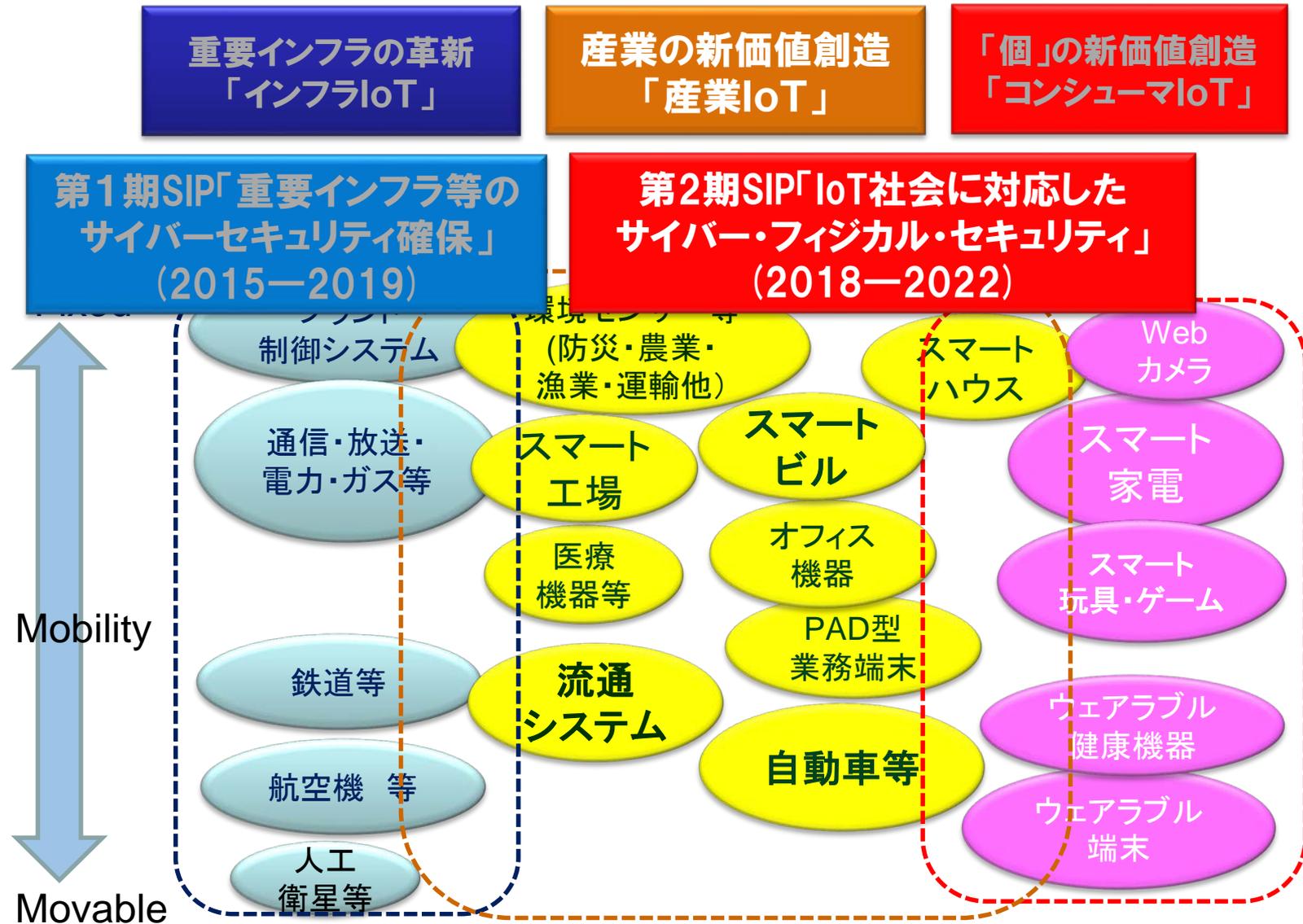


# 『IoT社会に対応した サイバー・フィジカル・セキュリティ』

---

内閣府  
プログラムディレクター  
後藤 厚宏

# 産業の新価値創造とサイバー・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対応は喫緊の課題

**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リスク: IoT機器が社会インフラへサイバー攻撃

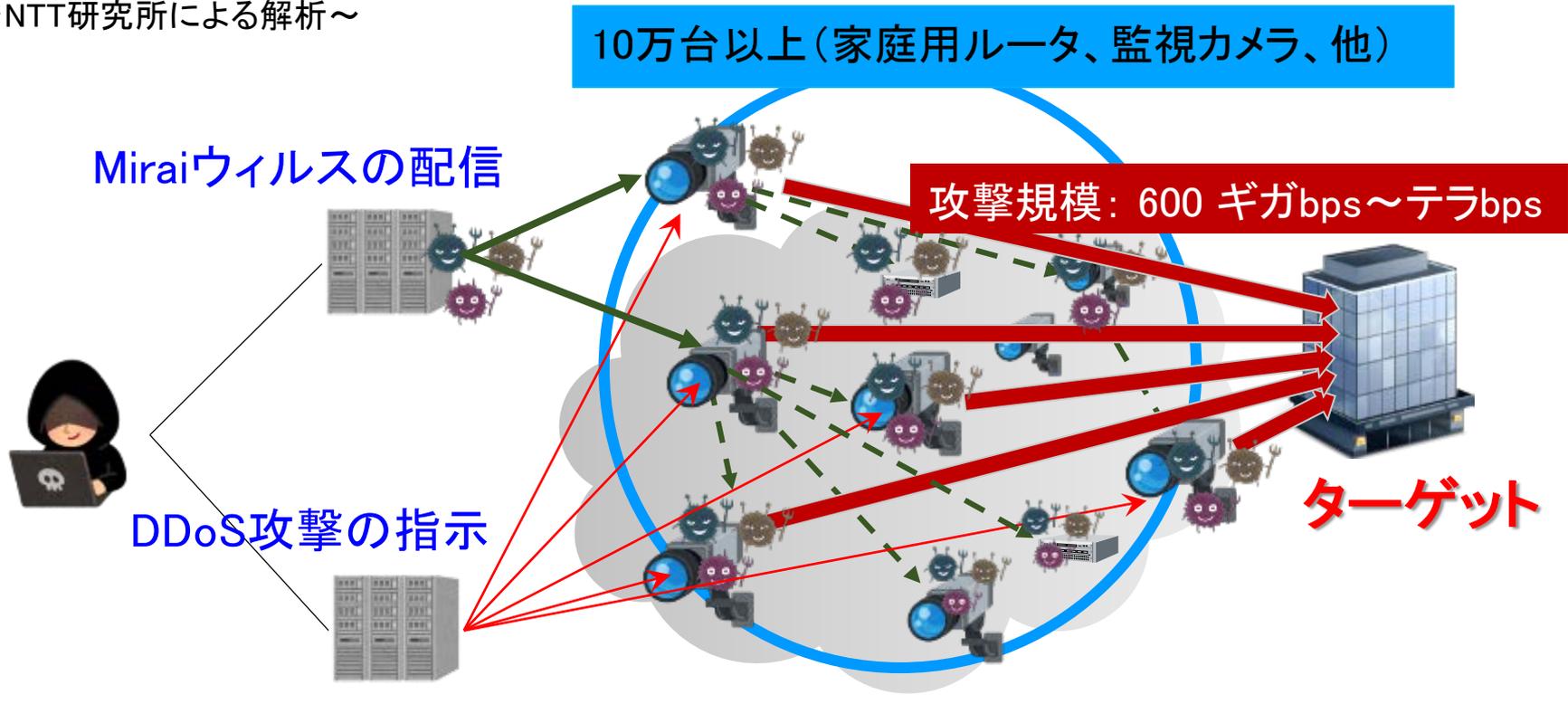
## ■ Miraiの事案: 脆弱性のあるIoT機器が大規模DDoS攻撃の踏み台

【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~



# IoT+サプライチェーン リスク: JEEP事例

■BlackHat2015で公表

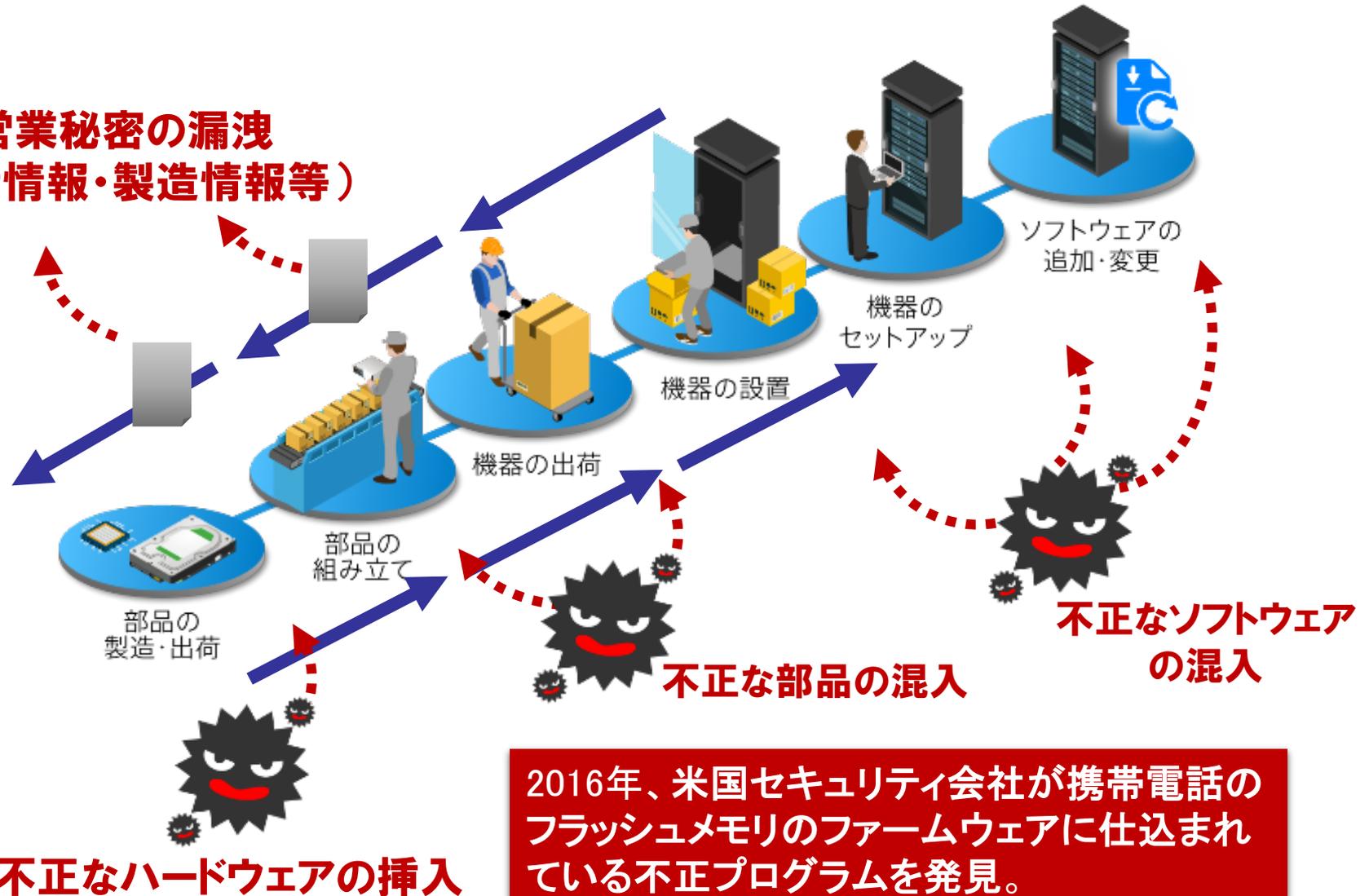
■リコール140万台で多額の損害が発生



画像.ブレーキ不能で溝に(出典:WIRED)

# サプライチェーンリスク:「混入」「改ざん」「漏洩」

営業秘密の漏洩  
(設計情報・製造情報等)



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。

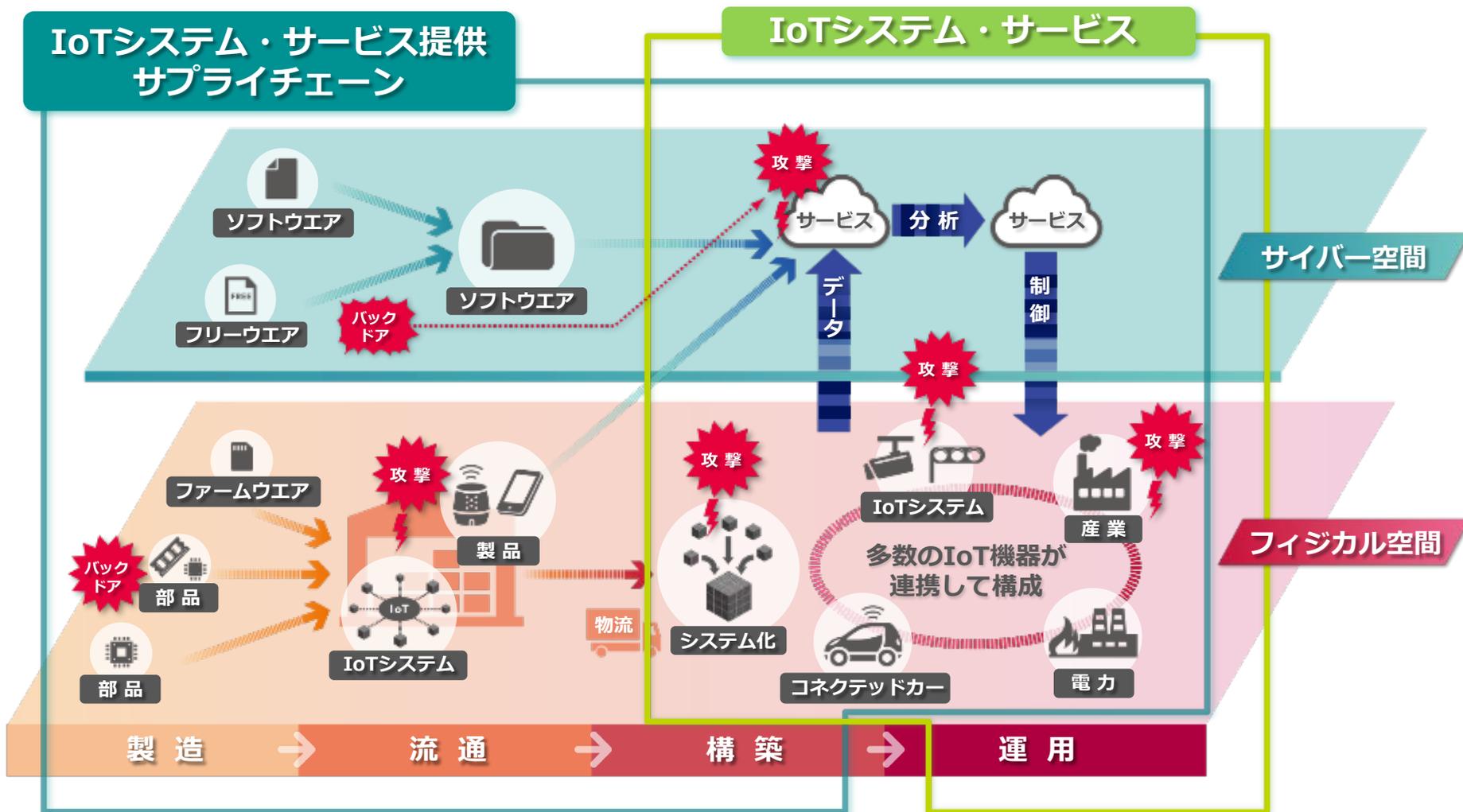
# サイバー・フィジカル・システムのセキュリティ課題

サプライチェーンのセキュリティ確保

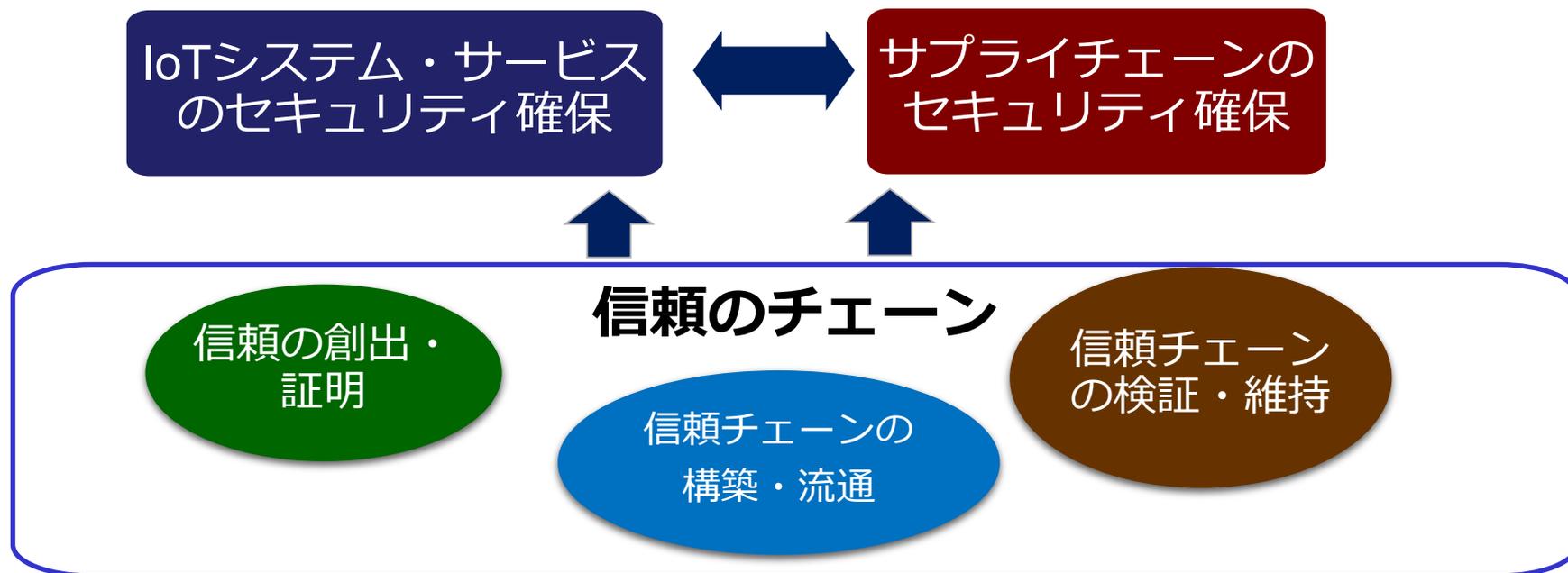
IoTシステム・サービスのセキュリティ確保

IoTシステム・サービス提供  
サプライチェーン

IoTシステム・サービス

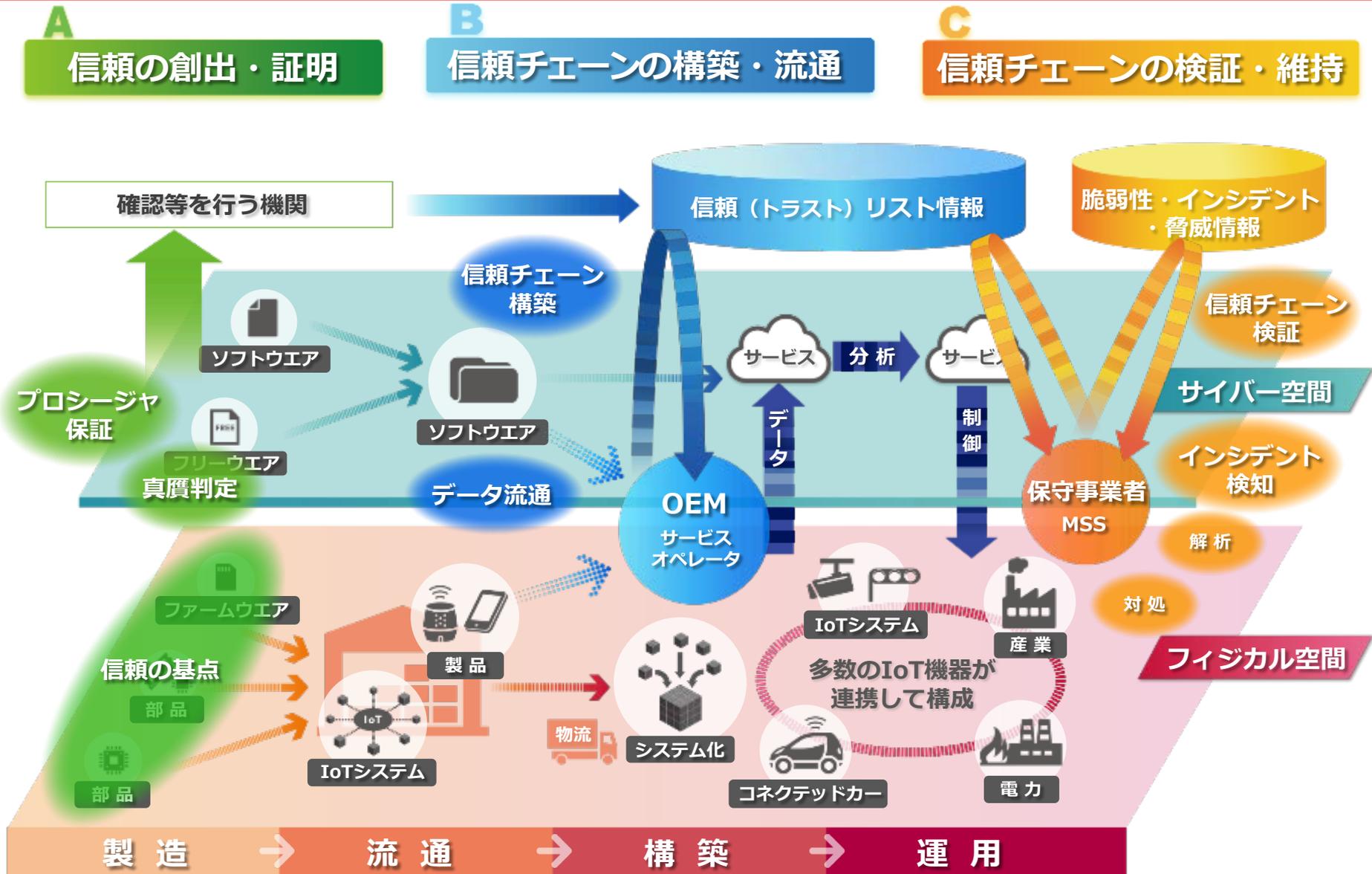


# 「信頼のチェーン」によるセキュリティ確保



- ◆ 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



# 実フィールドを持つ事業者と連携し社会実装へ

2018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

2020年

**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

2022年

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**

# IoT・サプライチェーンセキュリティのグローバル動向

- ◆ IoTセキュリティ: 米・欧・日でフレームワーク議論が活発化。民間でフレームワークを支える技術開発が個々に進んでいる。
- ◆ サプライチェーンセキュリティ: 政府調達(防衛含む)・インフラ調達での議論・取組みが活発になっているが、それらを支える技術開発は本格化していない。



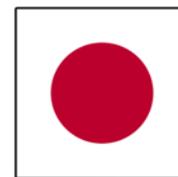
国  
米

- (官) DoD  
DFARS
- (官) NIST
- (民) AIAG



州  
欧

- (官) ENISA
- (官) UK  
DCMS
- (民) ECISO:  
ECSC



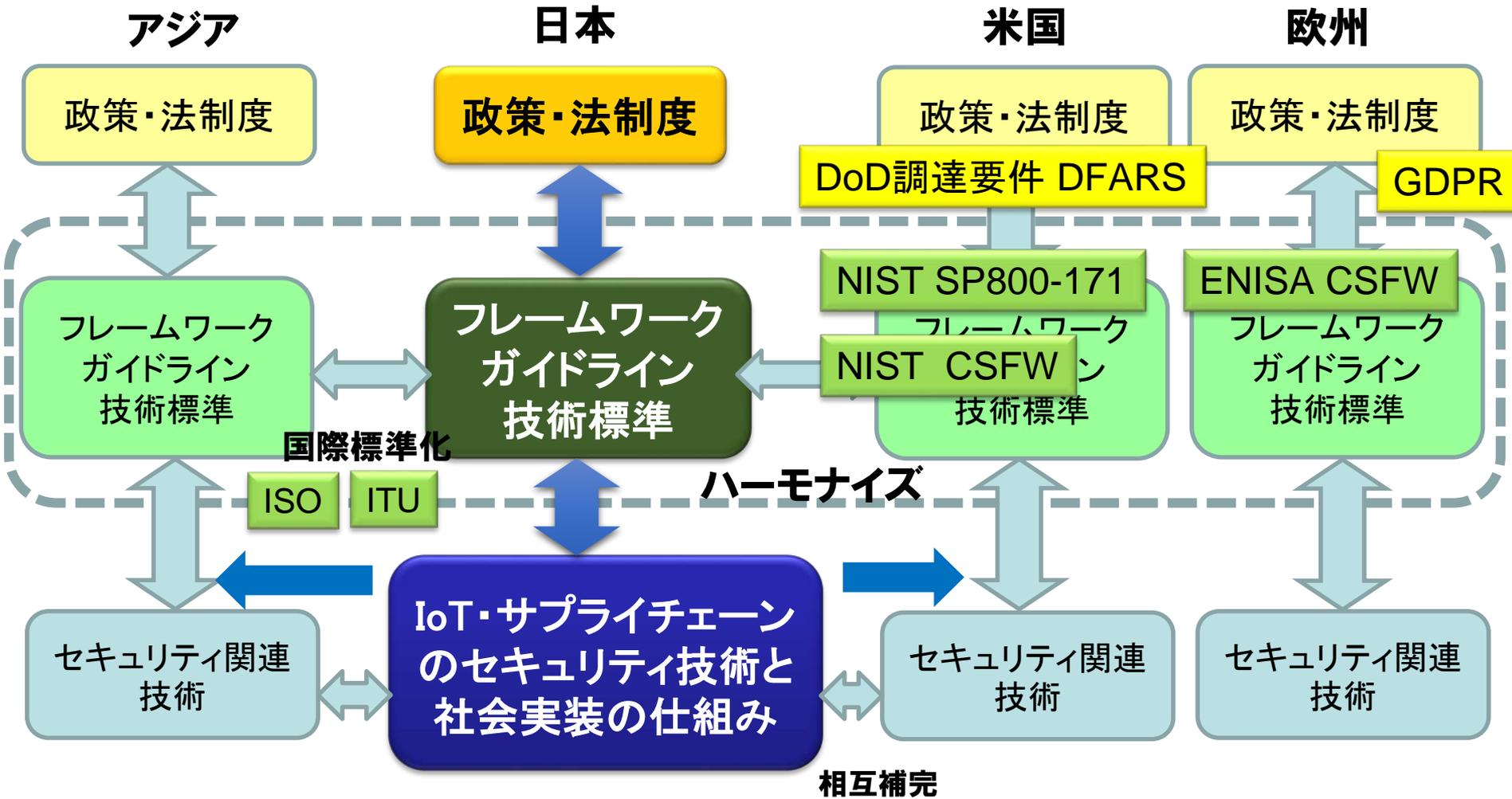
本  
日

- (官) NISC
- (官民) IoT推  
進コンソーシ  
アム
- (民) IPA

NIST: National Institute of Standards and Technology  
AIAG: Automotive Industry Action Group

ENISA: European Union Agency for Network and Information Security  
NCSC: National Cyber Security Centre  
DCMS: Department for Digital, Culture, Media and Sport  
ECISO: European Cyber Security Organisation

# 国際連携・関連府省庁の施策連携



# 研究開発の実施チーム体制

