戦略的イノベーション創造プログラム SIP

『サイバー・フィジカル・セキュリティ対策基盤』

最先端のコア技術と各産業分野での技術実証の取組み状況

R&D on Cyber-Physical Security Infrastructure:
core technologies development and experiment plan in actual industries

2020年11月6日（金）

内閣府 SIP プログラムディレクタ（PD）
情報セキュリティ大学院大学　Institute of Information Security

後藤　厚宏　GOTO Atsuhiro

背景：IoTリスクとサプライチェーンリスク対応は喫緊の課題

SIP第2期の当初からの課題

IoTリスク：サイバー攻撃脅威が、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社会では、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

- 米国：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セキュリティ**認証制度**。
EUの顧客データの企業間流通に新たな**義務（GDPR）**

新たな課題

コロナウィルス・パンデミック：社会・経済へのインパクト

- 遠隔業務・在宅勤務等でのIoT活用の急増に対応できる**セキュリティ対策が急務！**
- サプライチェーンの寸断による経済活動停止リスク ⇒ **セキュアなサプライチェーンの復旧能力が鍵に！**

我が国の政策上の位置づけ

IoTサプライチェーンセキュリティ確保は、サイバーセキュリティ戦略の重要事項の一つであり、内閣府SIPが府省庁（総務省、経産省等）を取りまとめて技術開発を進める。

サイバーセキュリティ戦略（戦略本部）

- ◆ サイバー空間に係る認識
  - IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大
- ◆ 目的達成のための施策
  - 新たな価値創出を支えるサイバーセキュリティの推進（DX with Cybersecurity）
  - 多様なつながりから価値を生み出すサプライチェーンの実現
  - 安全なIoTシステムの構築

サイバーセキュリティ2020（戦略本部）

- ◆ サプライチェーン全体のサイバーセキュリティ対策の強化

経産省の施策

- ◆ “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

総務省の施策

- ◆ “IoT・5Gセキュリティ総合対策2020”の推進技術

他　省庁

- ◆ 本SIPのWGには、NISC、総務省、経産省に加え、防衛装備庁が参加

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

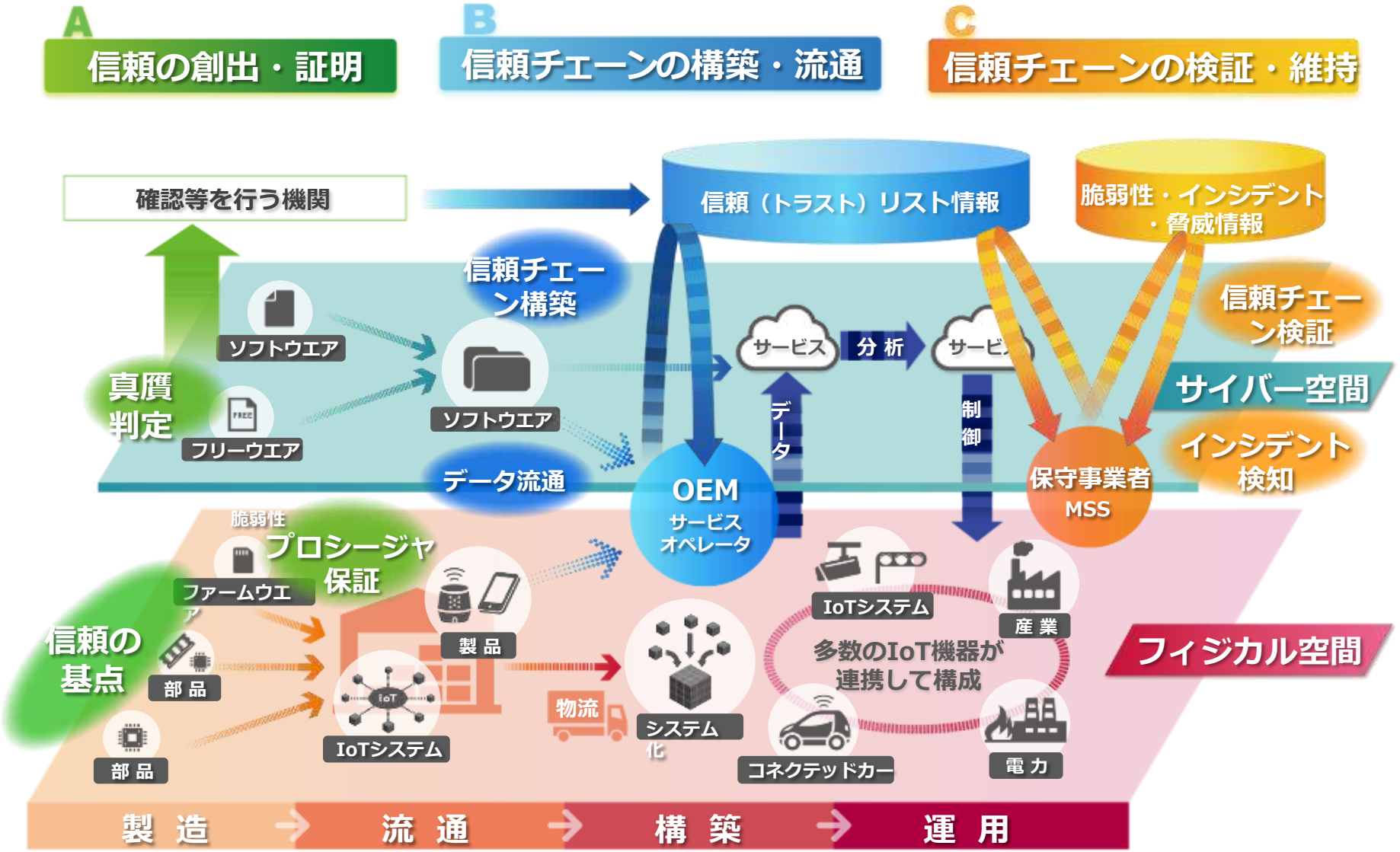
実施期間：平成30年度～令和4年度（2018年度～2022年度）

◆セキュアな Society 5.0 の実現に向け，様々なIoT機器を守り社会全体の安全・安心を確立するため， IoTシステム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『**サイバー・フィジカル・セキュリティ対策基盤**』の開発と実証を行う。

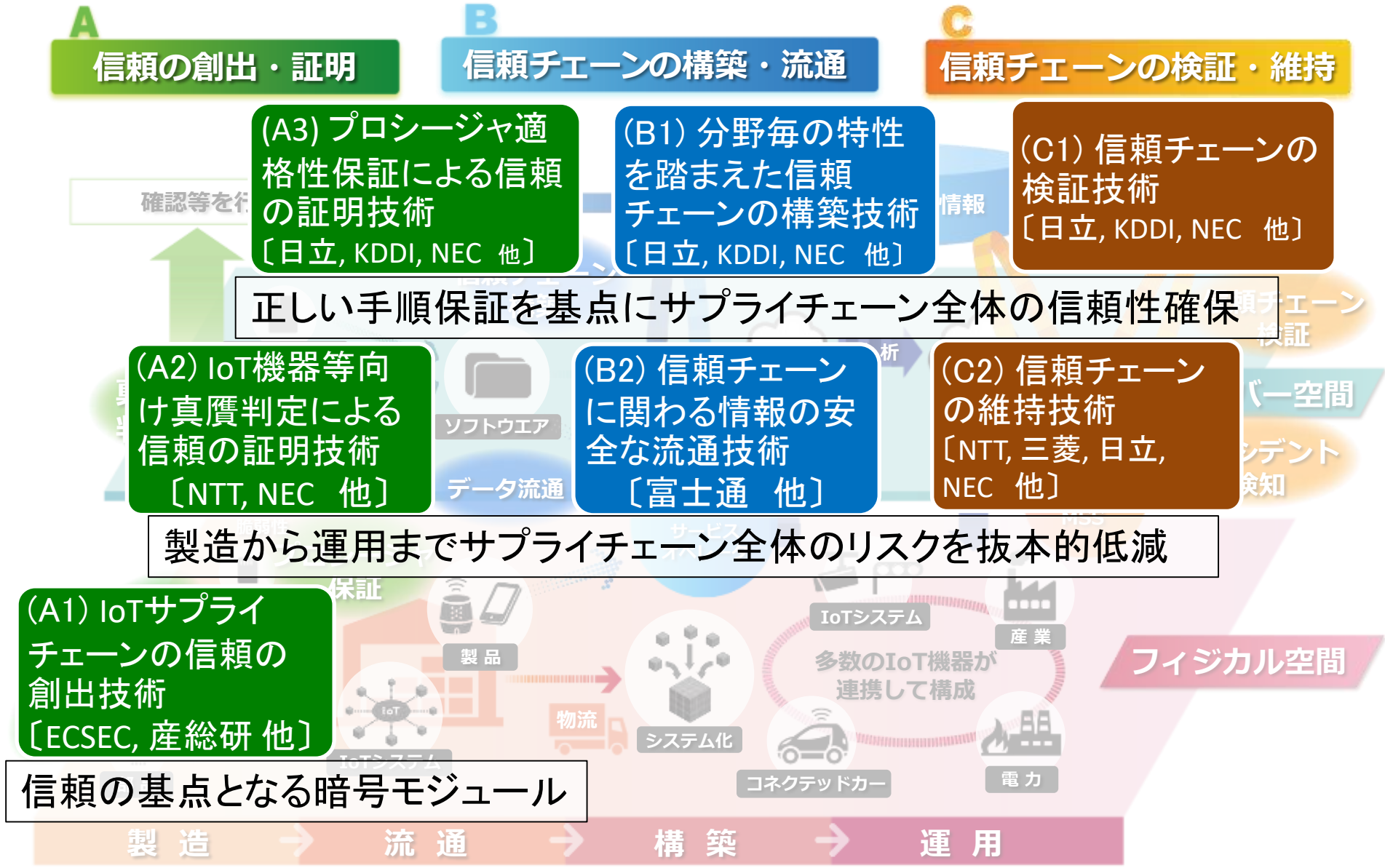
- サイバー脅威に対するIoTシステム・サービスの強靱化に向けた対策基盤の**コア技術**を開発する。
- 製造・流通・ビル等のサプライチェーンでの**実証**を通じて対策基盤の有効性を確認する。
- 多様な社会インフラやサービス，幅広いサプライチェーンを有する産業分野において本対策基盤の**社会実装を推進**する 。

研究開発内容：信頼チェーンによるIoTサプライチェーンのセキュリティ確保

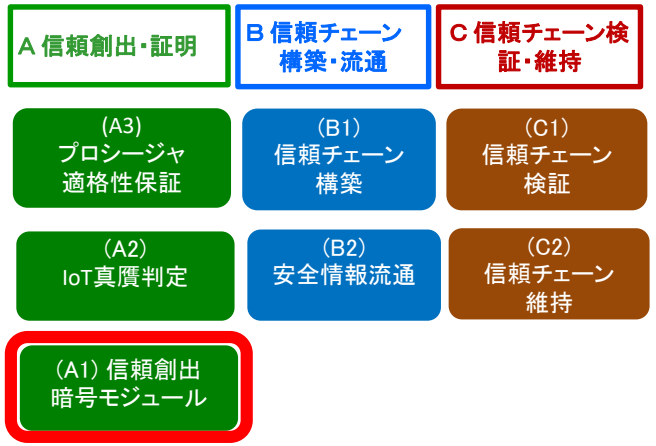
IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い，信頼のチェーンを構築・維持することで，IoTシステム・サービス及びサプライチェーン全体のセキュリティを確保



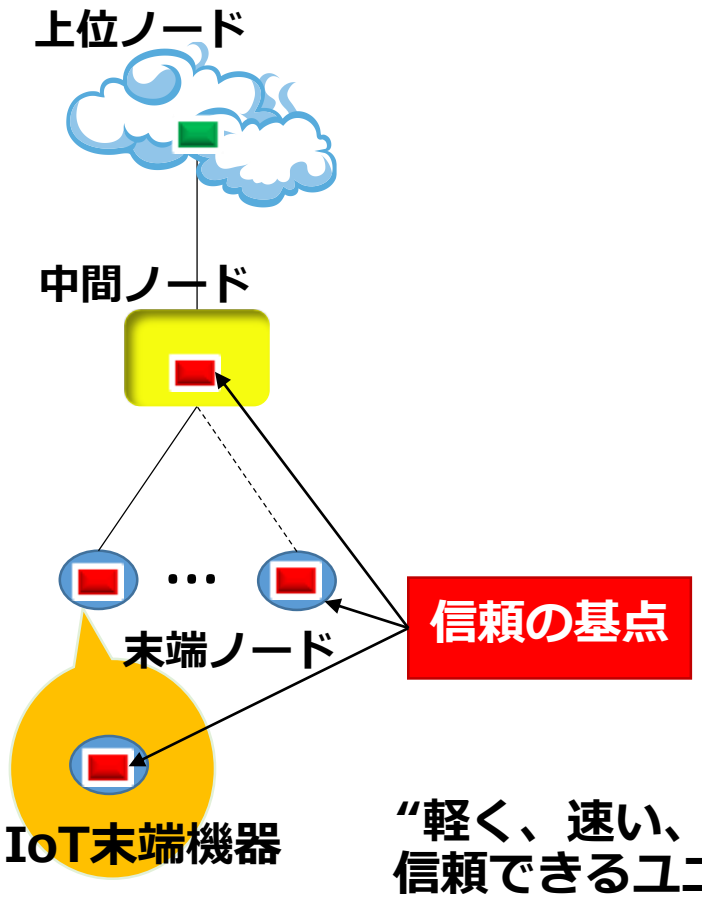
研究開発サブテーマ


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
(A3) プロシージャ適格性保証による信頼の証明技術
〔日立, KDDI, NEC 他〕
(B1) 分野毎の特性を踏まえた信頼チェーンの構築技術
〔日立, KDDI, NEC 他〕
(C1) 信頼チェーンの検証技術
〔日立, KDDI, NEC 他〕
正しい手順保証を基点にサプライチェーン全体の信頼性確保
(A2) IoT機器等向け真贋判定による信頼の証明技術
〔NTT, NEC 他〕
(B2) 信頼チェーンに関わる情報の安全な流通技術
〔富士通 他〕
(C2) 信頼チェーンの維持技術
〔NTT, 三菱, 日立, NEC 他〕
製造から運用までサプライチェーン全体のリスクを抜本的低減
(A1) IoTサプライチェーンの信頼の創出技術
〔ECSEC, 産総研 他〕
信頼の基点となる暗号モジュール
ソフトウエア
データ流通
製品
物流
システム化
IoTシステム
多数のIoT機器が連携して構成
産業
電力
コネクテッドカー
フィジカル空間
製造
流通
構築
運用

（A1）信頼の創出のコア技術：セキュア暗号ユニットSCU



Internet of Things



信頼できるサービス・サプライチェーン

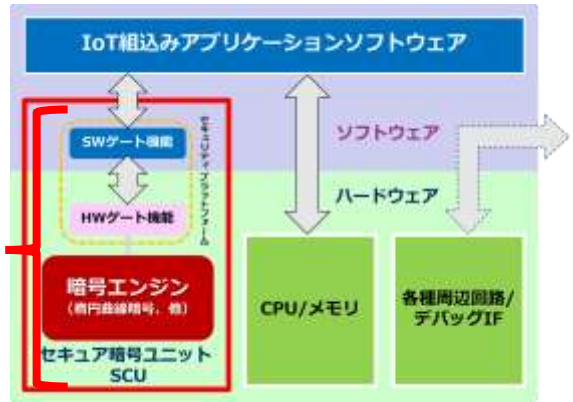
信頼できるシステム

信頼できるIoT機器

IoT機器をサイバー攻撃から守る

SCU搭載ICチップ

例：SCU入り１チップマイクロコントローラ



“軽く、速い、強い”
信頼できるユニット

SCU

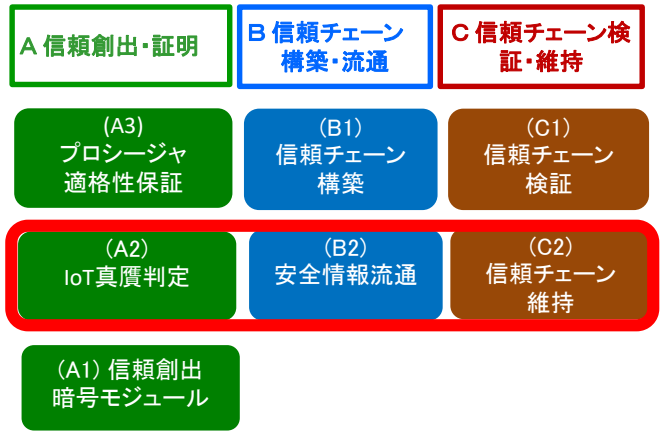
セキュア暗号ユニット

IoT末端機器向けセキュリティチップの３要件で世界トップを目指す

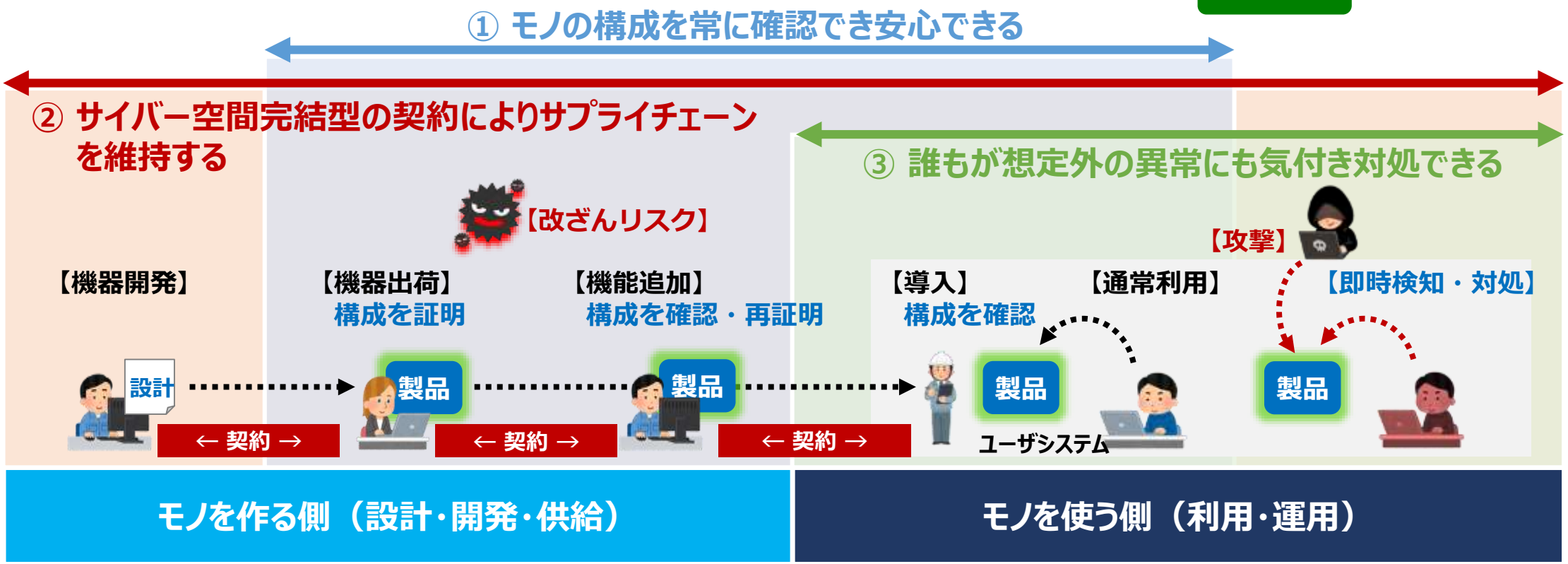
1. セキュリティ機能：公開鍵暗号機能、アクセス制御、耐タンパー実装
2. セキュリティ保証：第3者認証スキーム、認定スキーム
3. 性能・リソース：処理速度、消費電力、小サイズ（楕円曲線暗号処理で、世界最小、世界最少消費電力、世界最速の個別記録）

（A2･B2･C2）製造から運用までサプライチェーン全体のリスクを抜本的低減

① サプライチェーンと運用を通じて、**モノの構成を常に確認でき安心**できる
② 事業状況の変化に応じて、**サイバー空間でスマートに契約**できる
③ 高度なスキルを要求することなく、**誰でも想定外の異常に気づき対処**できる



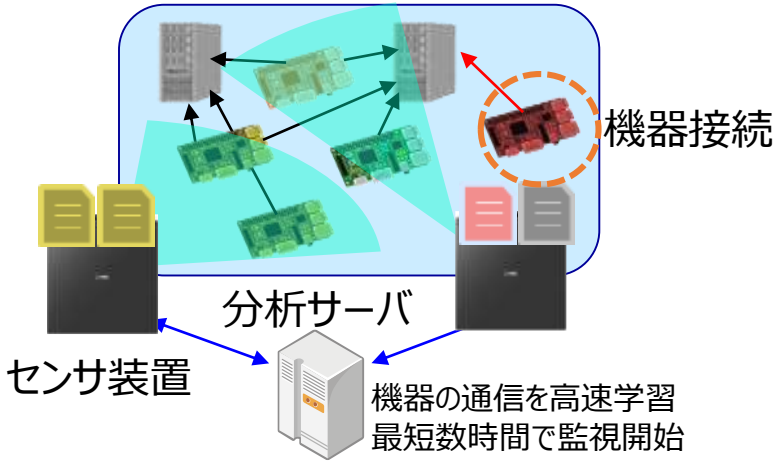
【モノ（製品）を作るプロセスと使うプロセスの「信頼」を確保、維持】



C2①「誰もが想定外の異常に対処できる」サイバーフィジカル異常検知

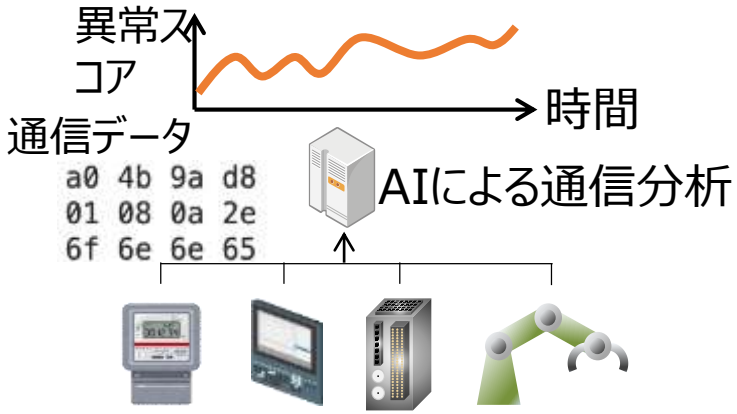
即時監視による漏れのない監視

システム内の通信を監視し、構成変化も即座に検知して対応



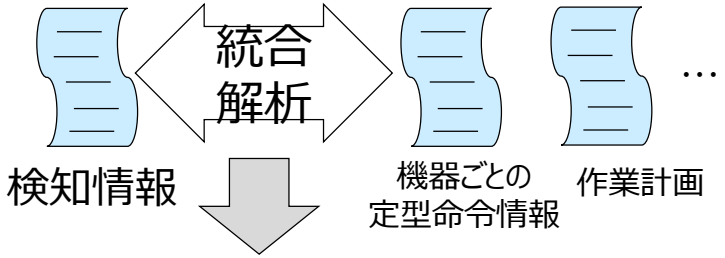
即時検知による通信異常検知

プロトコルに依存しない通信パターン学習により多様な環境で異常検知が可能



即時支援による原因推定

パケット内の異常箇所を特定し、さらに考えられる発生原因を推定

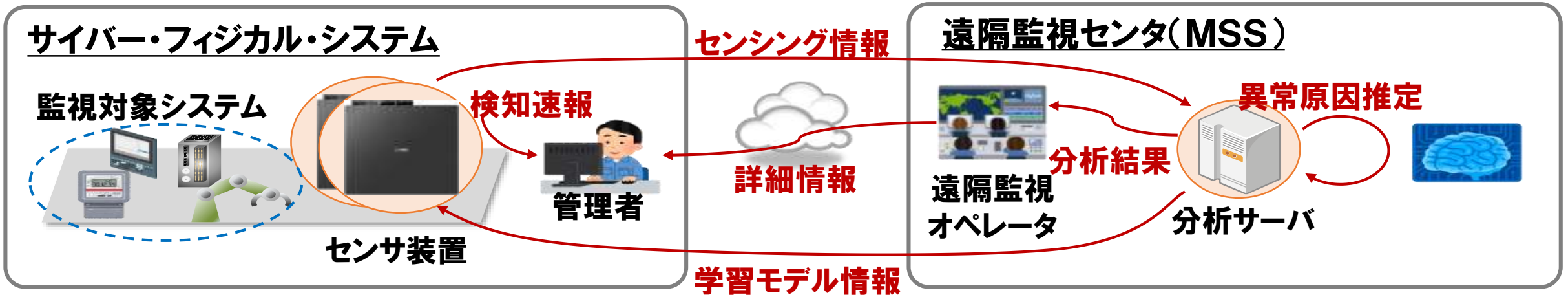


異常箇所

a0 4b 9a d8
01 08 0a 2e
6f 6e 6e 65

異常発生原因の推定(例)

- 定型の制御命令と異なる
- 作業計画にない命令



（A3・B1・C1） 正しい手順保証を基点にサプライチェーン全体の信頼性確保

サプライチェーンの『Resiliency』,『Flexibility』、事業活動の『説明責任』を果たす仕組み

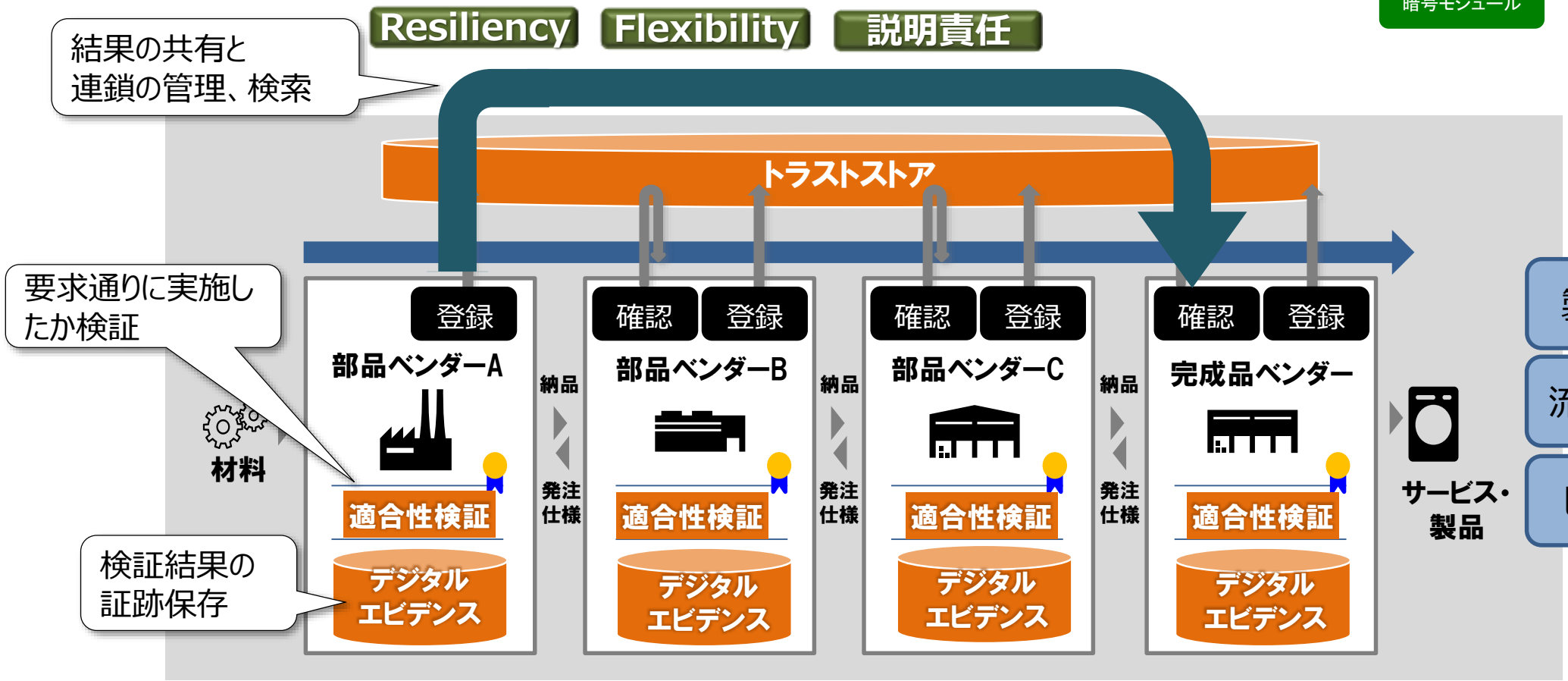
1. サプライチェーン上の生産活動が規程どおりに行われたかを検証 **（適合性検証）**
2. 適合性の検証結果の根拠をデジタルエビデンスとして保存、検索 **（デジタルエビデンス）**
3. 適合性の検証結果をサプライチェーン全体で共有、トレーサビリティ確保、検索 **（トラストストア）**

A 信頼創出・証明 | B 信頼チェーン構築・流通 | C 信頼チェーン検証・維持

(A3) プロシージャ適格性保証 | (B1) 信頼チェーン構築 | (C1) 信頼チェーン検証

(A2) IoT真贋判定 | (B2) 安全情報流通 | (C2) 信頼チェーン維持

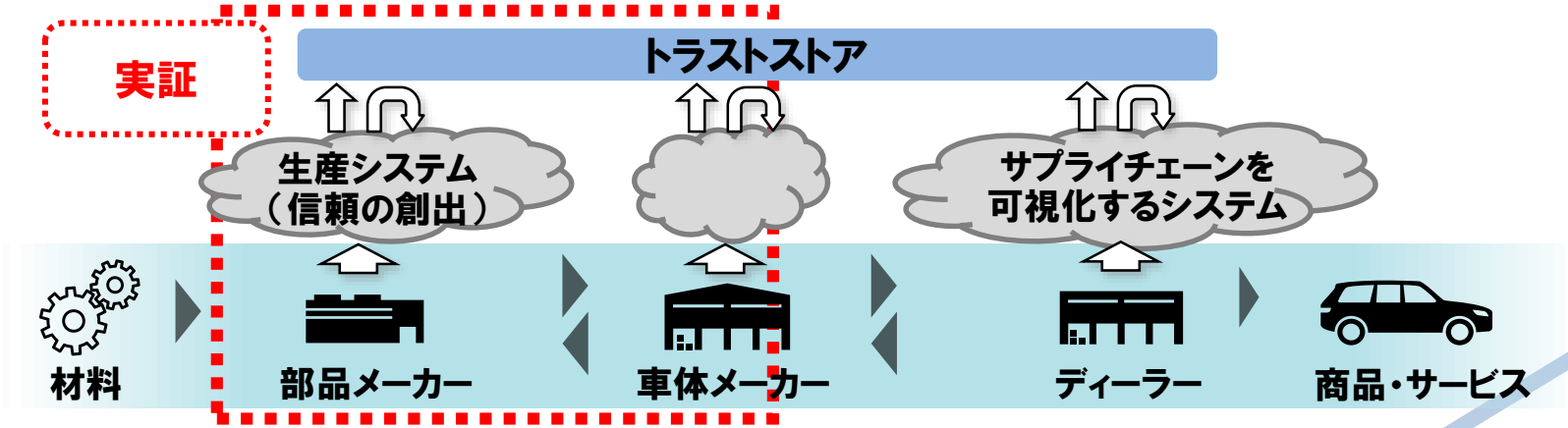
(A1) 信頼創出 暗号モジュール



実証実験

- 製造 (海外工場)
- 流通(企業間取引)
- ビル （サービス業)

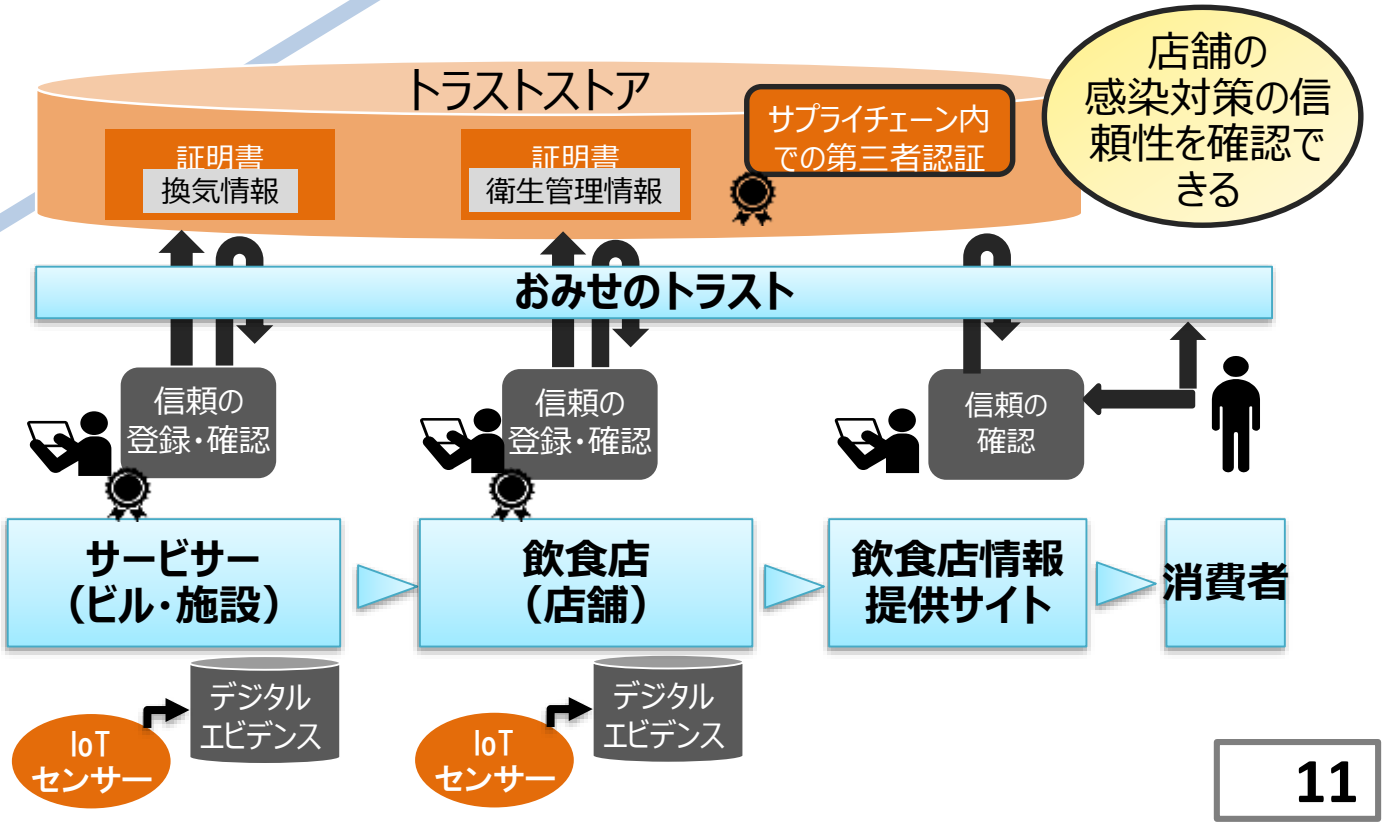
（A3・B1・C1） 製造分野とビル分野での実証実験



ビル（サービス業）

タイのアマタ工業団地にある工場

製造 (海外工場)



まとめに代えて

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

海外動向の調査

製造・流通・ビル分野等での実証

（2020年）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）**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

府省庁による制度設計・グローバルな調整

サプライチェーン向けガイドライン整備

NIST SP-800やWP29などに沿う**セキュリティ施策の導入**

個人データの企業間流通における**GDPR準拠**

引き続き、

招待講演と技術テーマ毎の

グループディスカッションへのご参加を

お願いいたします