戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

IoT社会に対応したサイバー・フィジカル・セキュリティ 取組概要

－ 目次 －

戦略的イノベーション創造プログラム（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

～Society 5.0を支えるセキュアなIoTサプライチェーンの実現を目指して～

内閣府　プログラムディレクター　後藤　厚宏（情報セキュリティ大学院大学　学長）

管理法人：国立研究開発法人新エネルギー・産業技術総合開発機構　実施期間：2018年度～2022年度

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『サイバー・フィジカル・セキュリティ対策基盤』の開発を行い、実稼働するサプライチェーンに組み込み実用化することで、サイバー脅威に対するIoT社会の強靭化を図る。

研究開発テーマ

A 信頼の創出・証明

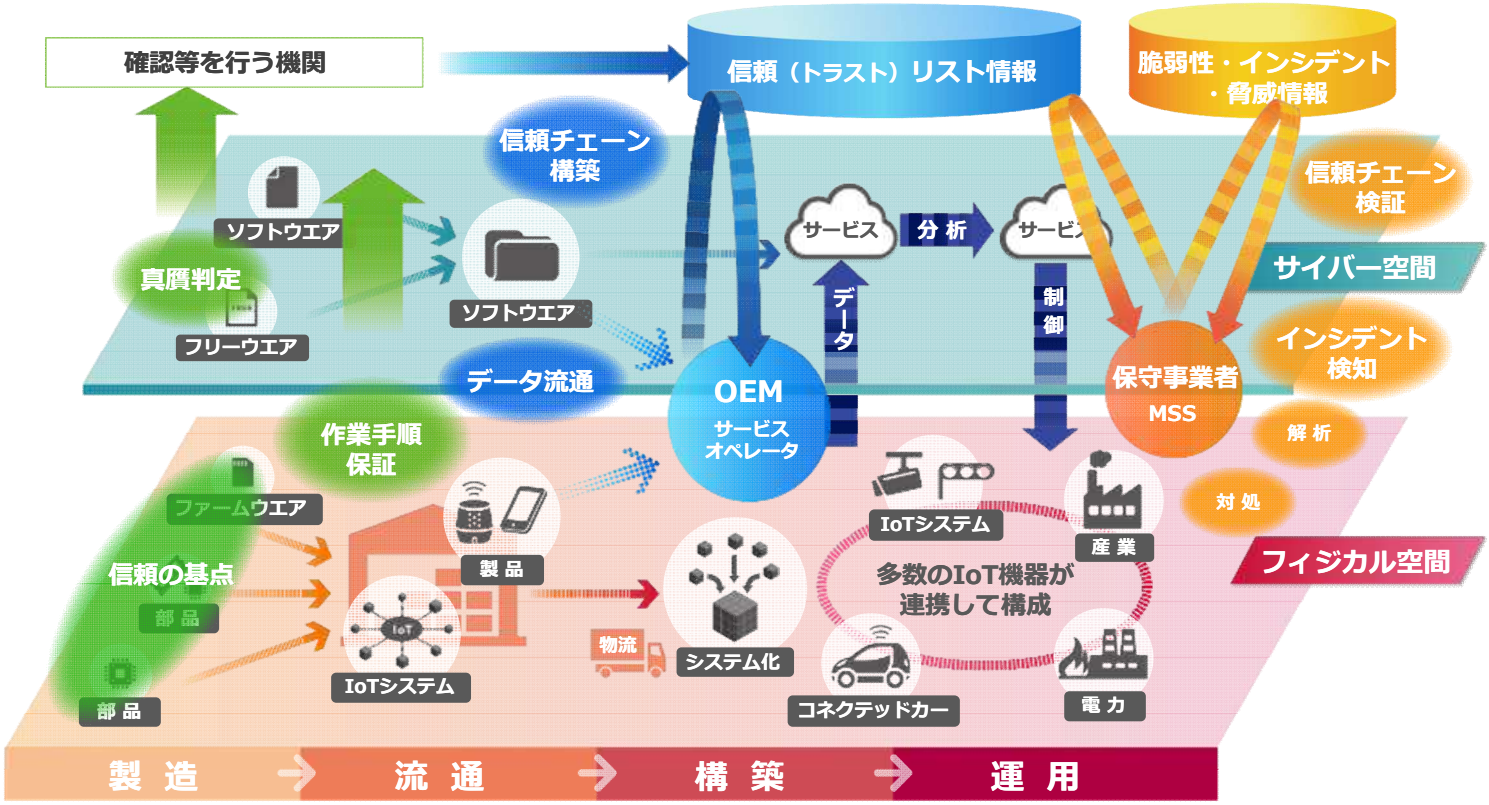
多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

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



研究開発の背景

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リスクとサプライチェーンリスクへの対応は喫緊の課題

【（株）日立製作所、日本電気（株）、（株）KDDI総合研究所】

サプライチェーンの信頼回復への挑戦

創出・証明　構築・流通　検証・維持

製品・サービス不正を防ぎ、信頼でつながる社会へ

コンセプト取り組みの紹介

サイバーとフィジカルが密接に連携する超スマート社会Society 5.0における「信頼」を生み出す、私たちが考えるセキュリティの形です

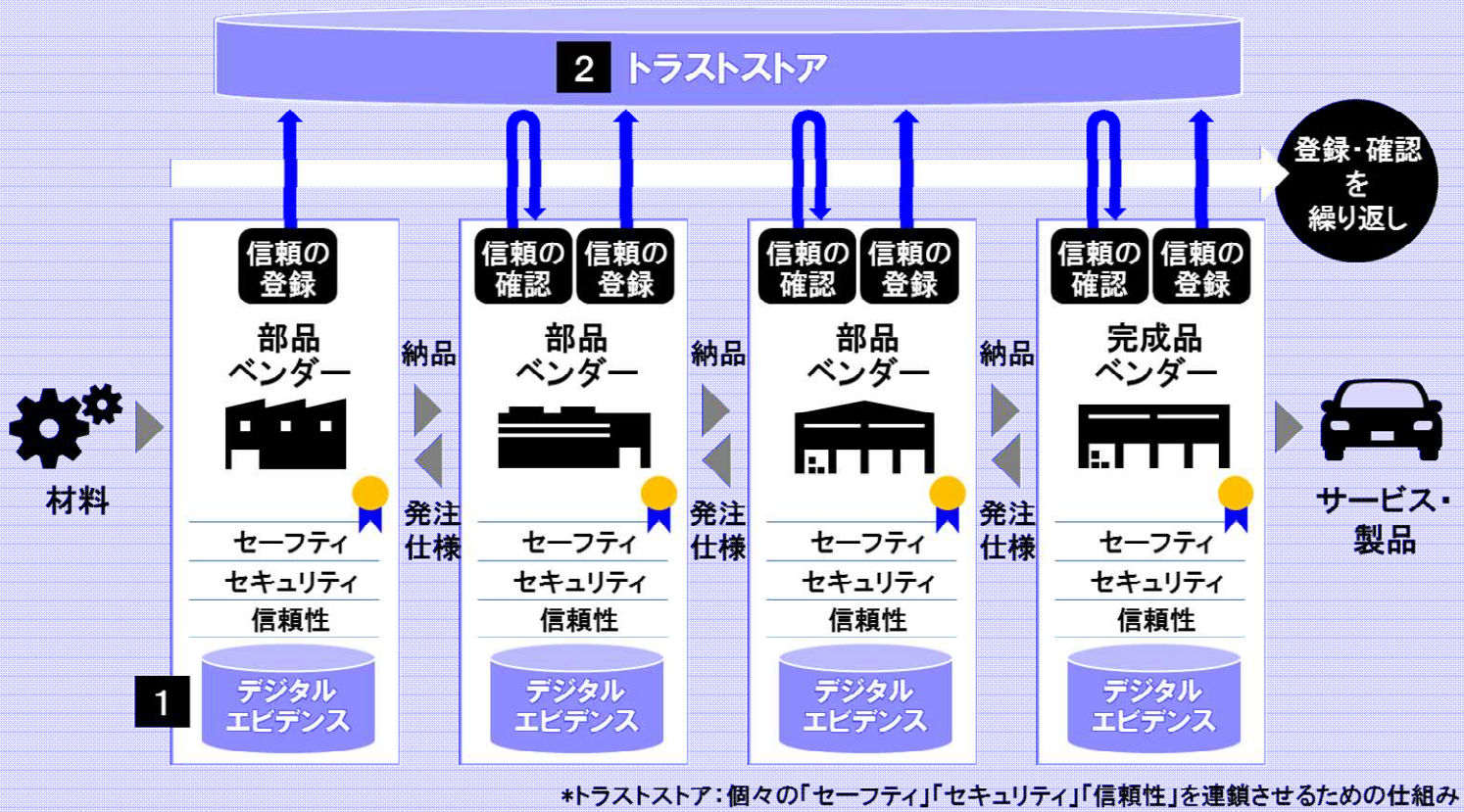
Society 5.0の未来のカタチ

1 信頼の創出

- サプライチェーン上の工程が基準・ルールどおりに行われたかを確認
- デジタルエビデンスに裏付けされた証明可能性による柔軟な信頼性確保

2 信頼チェーン

- 個々の「セーフティ」「セキュリティ」「信頼性」をトラストストア*で相互参照し連鎖
- サプライチェーン全体で「信頼性」確保



*トラストストア：個々の「セーフティ」「セキュリティ」「信頼性」を連鎖させるための仕組み

【（株）日立製作所】

サプライチェーンにおける組織を越えた信頼チェーンの可視化

構築・流通　検証・維持

信頼情報の登録、連鎖による信頼チェーンの構築および検証

技術の特長

■**信頼チェーンの構築**
証明書、能力情報、紐付け情報により構築

■**トラストストア利活用インターフェース**
事業者がトラストストアを利活用するための
インタフェースを提供

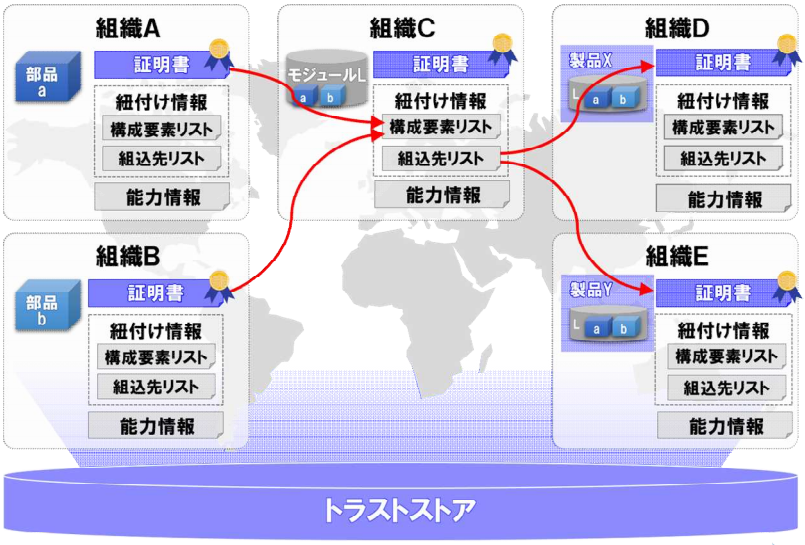
■**ライフサイクルを意識した運用方式**
製品・サービスのライフサイクルに対応

■**信頼チェーンのグランドデザイン作成**
運用・制度・仕組みに関わる将来像を作成

効果

①サプライチェーン全体における信頼性が確認できる
②事業者が容易に利活用できる
③さまざまな事業者が長期的に使うことができる
④異なる業界や国を跨いで信頼性が確認できる

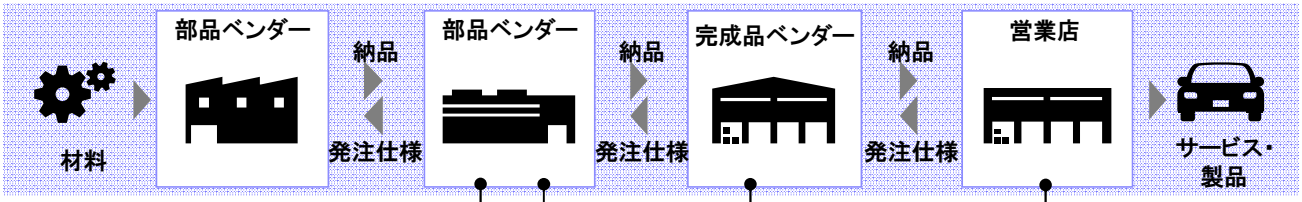
サプライチェーンの信頼性確認のイメージ



証　明　書：部品・モジュール・製品・サービスなどが信頼に適合していることを示す文書
紐付け情報：組織を越えた証明書のつながりを示す情報
能 力 情 報：証明書が何に適合しているのかを示す情報
（保有している資格、性能、規制、規格 など）
トラストストア：証明書、紐付け情報、能力情報を保持し、サプライチェーン全体の信頼性を確認できるようにしたもの

デモンストレーション展示：コンセプト取り組みの紹介

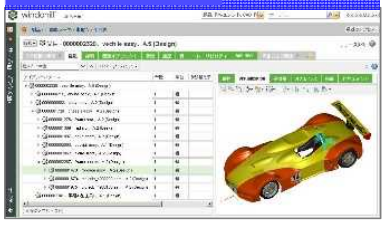
「信頼チェーン」がどのように使われるのか、部品ベンダー、完成品ベンダー、営業店のシステムを模擬した環境で、サプライチェーン全体の信頼を確認できる世界をご紹介します。



生産支援システム

日系のシェア工場で使われている
生産システム上に利用イメージを
実現しています。

製品管理システム



国内外の生産現場で利用実績の高い
BOM*／製品管理システム上に利用イメージ
を実現しています。
*BOM：Bill of Materials

営業店支援システム

将来の営業店で使われるシステムを
想像して、その上に利用イメージを
実現しています。

【電子商取引安全技術研究組合、産業技術総合研究所、他】

IoTサプライチェーンの信頼の創出

Society 5.0の基盤であるIoTシステム・サービス及びサプライチェーンのセキュリティ確保を実現し、信頼のチェーン(連鎖)を構築

技術の特長

■ **信頼の基点実装(信頼の創出)**

信頼のチェーン(連鎖)を構築するため、多種・大量の小型IoT機器にコスト、性能面共に適用可能な信頼の基点実装(信頼の創出)技術の研究開発

■ **セキュリティ保証スキーム**

信頼の基点に対するセキュリティ保証スキームの研究開発及び整備・構築し実用化・社会実装を推進

仮説:オープンなIoTへの展開が進む

理想:公開鍵暗号が末端まで使える

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。

電子商取引安全技術研究組合(ECSEC)、国立研究開発法人産業技術総合研究所(AIST)
横浜国立大学、東京大学、東北大学、神戸大学、奈良先端科学技術大学院大学、三菱電機