SIP「IoT社会に対応した サイバー・フィジカル・セキュリティ」シンポジウム2019

～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～

2019年10月31日（木）13:30～17:00

ベルサール神田 イベントホール

主催：内閣府、NEDO

内閣府 Cabinet Office, Government of Japan

NEDO 新エネルギー・産業技術総合開発機構 New Energy and Industrial Technology Development Organization

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

― 目次 ―

【全体・複合】
プロジェクトの位置づけと展示の全体像 ・・・・ 4
サプライチェーンの信頼回復への挑戦 ・・・・ 6
サプライチェーンにおける組織を越えた信頼の可視化 ・・・・ 7
【信頼の創出・証明】
IoTサプライチェーンの信頼の創出 ・・・・ 8
社会実装につながるSCUアプリケーションシステムの構築 ・・・・ 9
運用を含むIoTサプライチェーンのハードウェアトロージャン対策 ・・・・ 10
安価なIoT機器に組込めるSCUを対象としたセキュリティ保証スキームの構築 ・・・・ 11
OT/IoTシステムの特性に対応可能な真贋判定 ・・・・ 12
稼働中の機器の軽量型真贋判定 ・・・・ 14
サプライチェーンにおけるVCPの適格性検証 ・・・・ 17
サプライチェーンにおけるデータの適合性判定 ・・・・ 18
サプライチェーンにおけるヒトの適格性判定 ・・・・ 20
【信頼チェーンの構築・流通】
サイバー空間のデータ流通保証 ・・・・ 22
【信頼チェーンの検証・維持】
サイバー・フィジカル異常検知 ・・・・ 24
サイバー・フィジカル空間を跨って流れる不正なデータの検知・対処 ・・・・ 26
サイバー攻撃発生時の影響評価及び対処策実行支援 ・・・・ 28

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

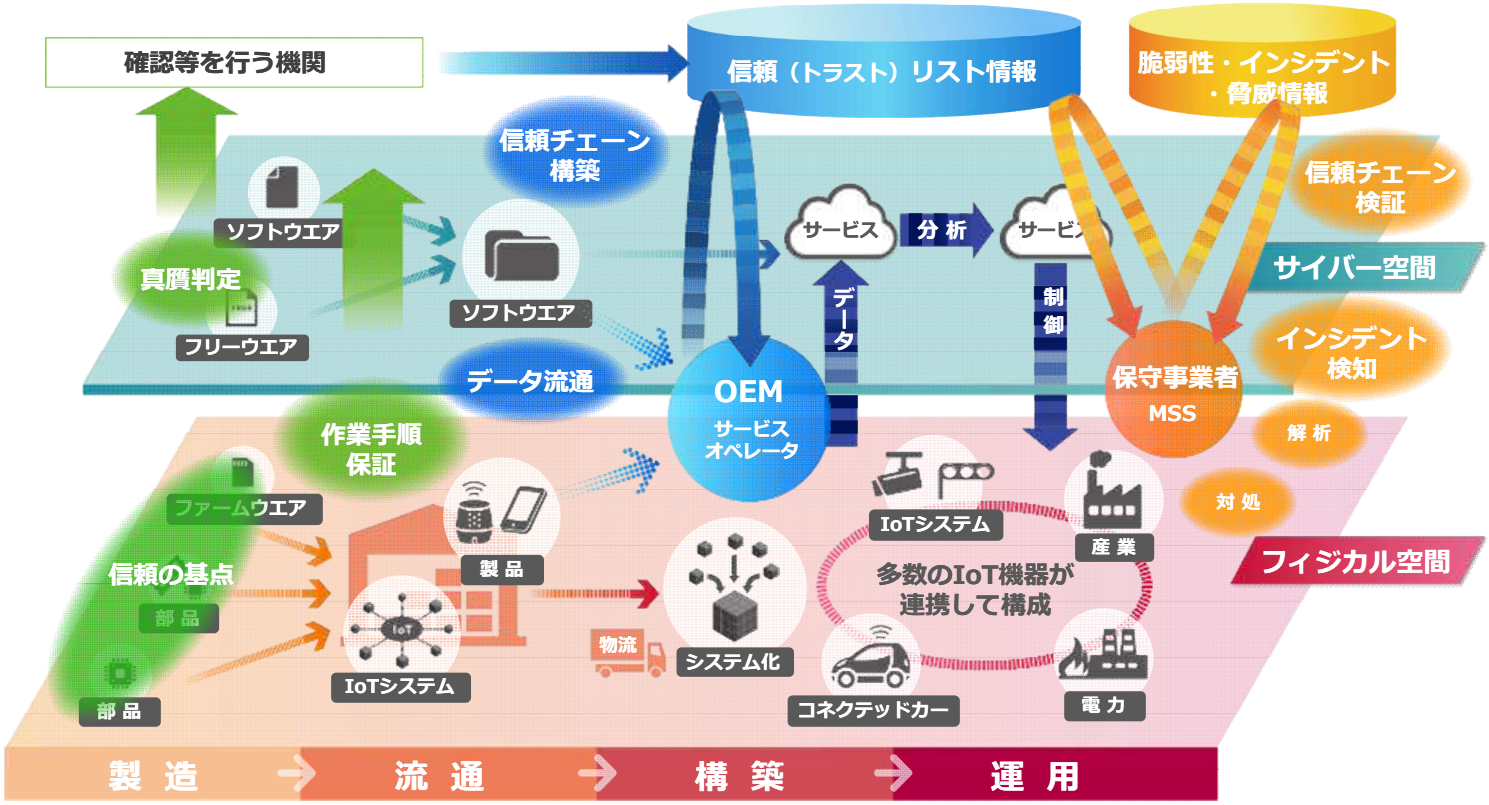
多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

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

展示会場の紹介

展示ブースのレイアウト

展示項目一覧と展示内容

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

展示場所	対応ページ	出展者	展示タイトル	利用シーン	技術	効用のポイント
①	8-11	ECSEC 産総研 他	・IoTサプライチェーンの信頼の創出 ・社会実装につながる SCUアプリケーションシステムの構築 ・運用を含むIoTサプライチェーンの ハードウェアトロージャン対策 ・安価なIoT機器に組込めるSCUを対象とした セキュリティ保証スキームの構築		A	格上のセキュリティ 組込み機器対応セキュア暗号ユニット(SCU)エンジン 供給者の意図に反してハードウェアに組込まれる恐れのある悪意の機能を排除、検出 セキュリティ評価の厳密さと開発工数のバランス確保
②				ハードウェアトロージャン対策	A	
③				監視カメラ統合管理	A	
④	24-25	NTT 三菱電機	サイバー・フィジカル異常検知	サイバー・フィジカル・システムに対するセキュリティ異常の監視・分析	C	異常の影響が物理空間に及びうるシステムを対象とした高い「即時性」を備えたセキュリティ監視が可能
⑤	28-29	NEC	サイバー攻撃発生時の影響評価及び対処策実行支援	サイバー・フィジカル・システムの運用中	C	サイバー攻撃リスクの可視化 対処策の提示・計画立案支援 継続的なリスクアセスメント
⑥	26-27	日立	サイバー・フィジカル空間を跨って流れる 不正なデータの検知・対処	サイバー・フィジカル・システムの運用中	C	データ異常の高精度検知(誤検知・見逃しリスク低減) システム特性情報を活かした対処法の決定
⑦	12-13	NTT	OT/IoTシステムの特性に対応可能な真贋判定	OT/IoT機器の入出荷時・運用開始後の改ざん検知	A	OT/IoT機器のサプライチェーンとライフサイクルの全体を通じてソフトウェア改ざんを常時確認可能
⑧	14-15	NEC	稼働中の機器の軽量型真贋判定	IoTシステムの起動時/運用中	A	起動時/稼働中の常時監視 自動組込み/自動復旧による運用支援
⑨	22-23	富士通	サイバー空間のデータ流通保証	サイバー空間の「つなぐ」から「運営」までのライフサイクル	B	客観的情報に基づく相互認証:正しい相手とつなぐ 脅威対策標準の配備/検知時の一時対処 脅威対処情報の交換
⑩	7	日立	サプライチェーンにおける組織を越えた信頼の可視化	顧客へのサービス提供模様 (自動車販売営業店)	BC	保証書、能力情報等による信頼チェーンの構築 ライフサイクルを意識した運用方式
⑪	6	日立	サプライチェーンの信頼回復への挑戦	サイバーとフィジカルが信頼でつながる社会	ABC	信頼の確保:価値創造過程の監視と証明可能性 信頼チェーン:個々の「セーフティ」と「信頼性」を連鎖
⑫	17	日立	サプライチェーンにおけるVCPの適格性検証	顧客へのサービス提供模様 (工場での生産ライン)	A	ヒト、データ、プロシージャの適合性の統合による信頼の創出と証明
⑬	18-19	KDDI研	サプライチェーンにおけるデータの適合性判定	工場ライン ビルメンテナンス	A	データの適切な管理
⑭	20-21	NEC	サプライチェーンにおけるヒトの適格性判定	工場ライン	A	ヒトの適格性を保証することで信頼を創出 ヒトの資格や行動情報とその取扱条件の検証

【（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

紹介ブースNo

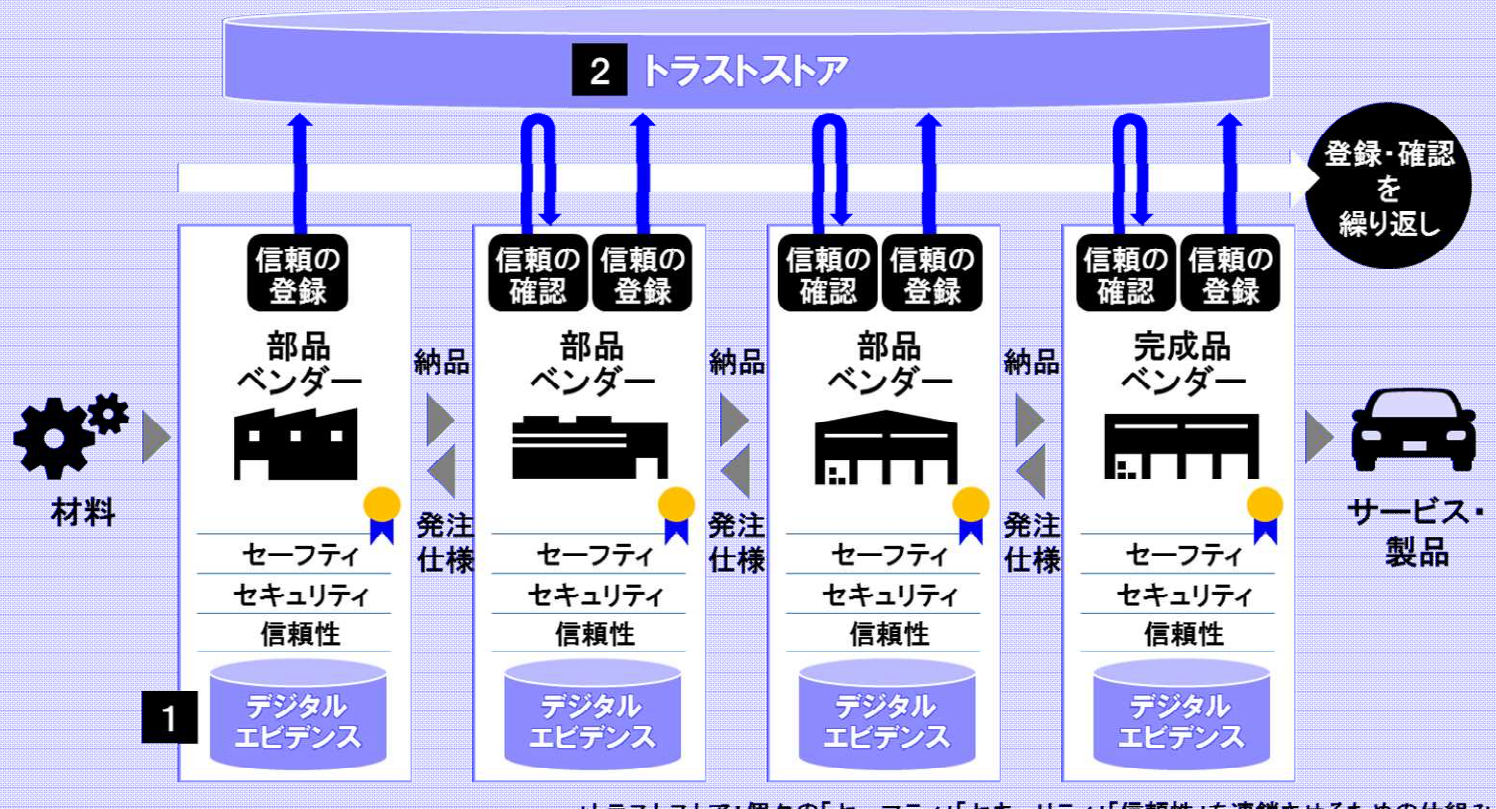
⑪ヒトの適格性判断
⑫データの適格性判断
⑬プロシージャの適格性判断

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

紹介ブースNo

⑭信頼チェーンの可視化



*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

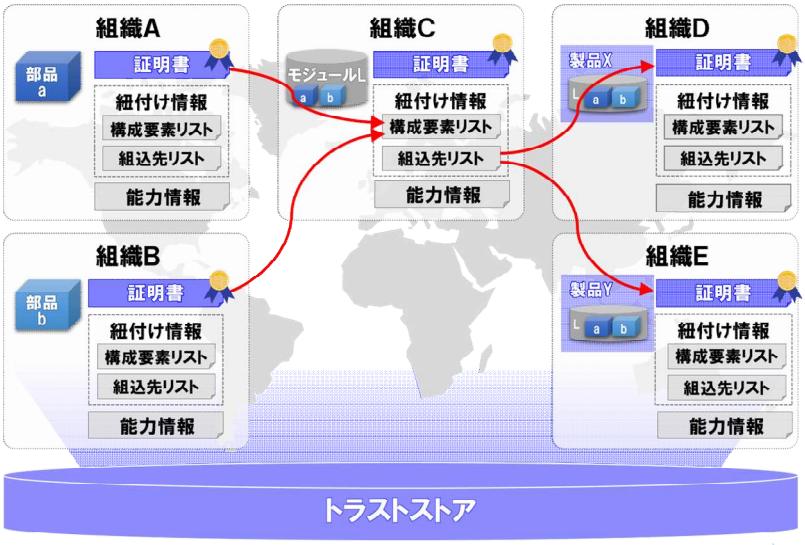
■**ライフサイクルを意識した運用方式**
製品・サービスのライフサイクルに対応

■**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

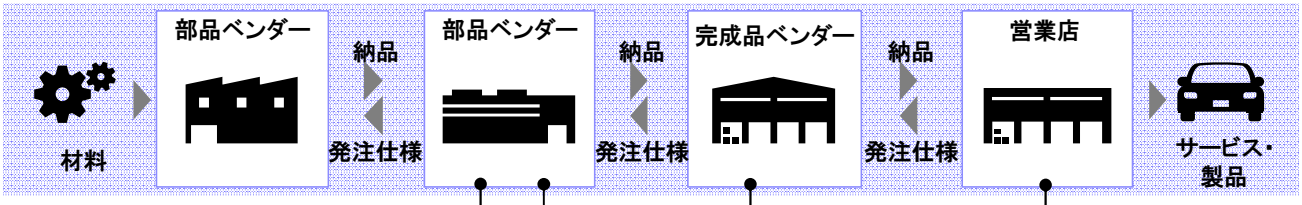
サプライチェーンの信頼性確認のイメージ



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

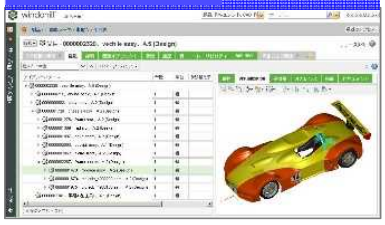
「信頼チェーン」がどのように使われるのか、部品ベンダー、完成品ベンダー、営業店のシステムを模擬した環境で、サプライチェーン全体の信頼を確認できる世界をご紹介します。



生産支援システム

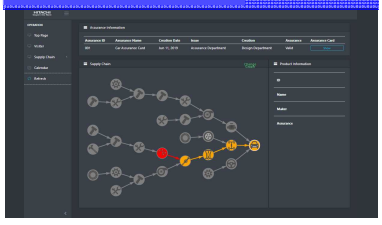
日系のシェア工場で使われている
生産システム上に利用イメージを
実現しています。

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

創出・証明

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)**

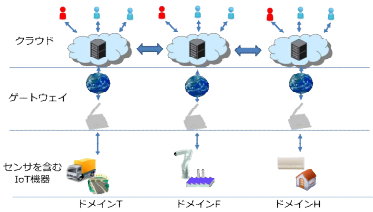
信頼のチェーン(連鎖)を構築するため、多種・大量の小型IoT機器にコスト、性能面共に適用可能な信頼の基点実装(信頼の創出)技術の研究開発

■ **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

(2020年頃まで?)

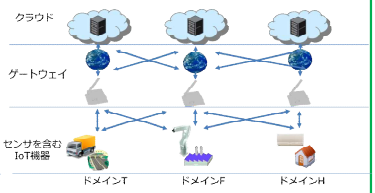


やや閉じたIoT

■現在はドメイン、あるいは事業主毎に、垂直統合でIoTアーキテクチャが構成されている。

■ドメイン間、あるいは事業主間で、クラウドを介した部分的な情報交換が行われる。

(2030年頃には)

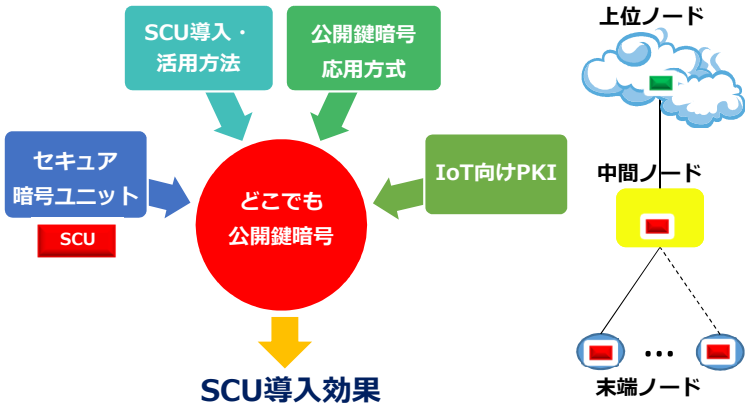


オープンなIoT

■ドメイン、事業主を問わず、IoTの様々なレイヤ間でデータ流通のメッシュ化、サービスの多層化、仮想化が進む。

■複数のステークホルダが多様に繋がる究極のIoTに向かって展開する。

理想:公開鍵暗号が末端まで使える



SCU導入効果

■ 共通鍵暗号しか使えない場合に比べ、格上のセキュリティを達成可

■ 多数の末端ノードの鍵管理・セキュティ管理コストを圧倒的に削減可

■ 大規模IoTの利便性とセキュリティの両立に大きく貢献

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。

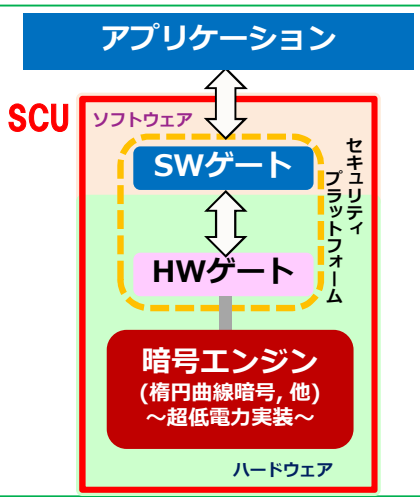
■ **ハードウェア暗号エンジン**

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

【電子商取引安全技術研究組合、産業技術総合研究所、他】

社会実装につながるSCUアプリケーションシステムの構築

創出・証明

想定モデルシステムを構築し、公開鍵暗号エンジンを搭載したSCUを社会実装を促進

ポイント

- 様々な想定されるモデルシステムに適した暗号を用いた機器間相互認証等を高速エンジンで実装
- 主な想定されるモデルシステムを構築し、SCUアプリケーションシステムの構築と実用化技術の実証
- 公開鍵暗号エンジンを搭載したSCUの社会実装を促進

モデルシステム1

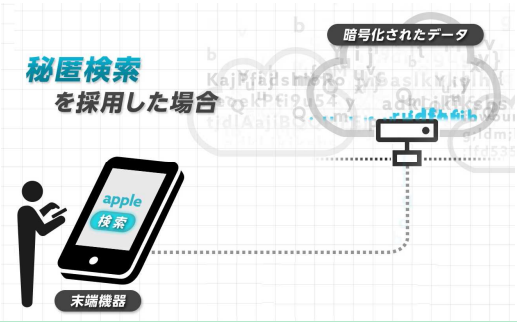
一般組込み機器用 SCUアプリケーションモデルシステム

モデルシステム2

極小組込み機器用 SCUアプリケーションモデルシステム

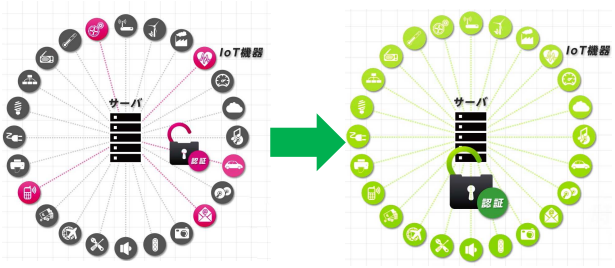
モデルシステム3

秘匿検索用 SCUアプリケーションモデルシステム



モデルシステム4

集約署名用 SCUアプリケーションモデルシステム



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、神戸大学 、他】

運用を含むIoTサプライチェーンのハードウェアトロージャン対策

創出・証明

供給者の意図に反してハードウェアに組込まれる恐れのある悪意の機能を排除、検出

技術の特長

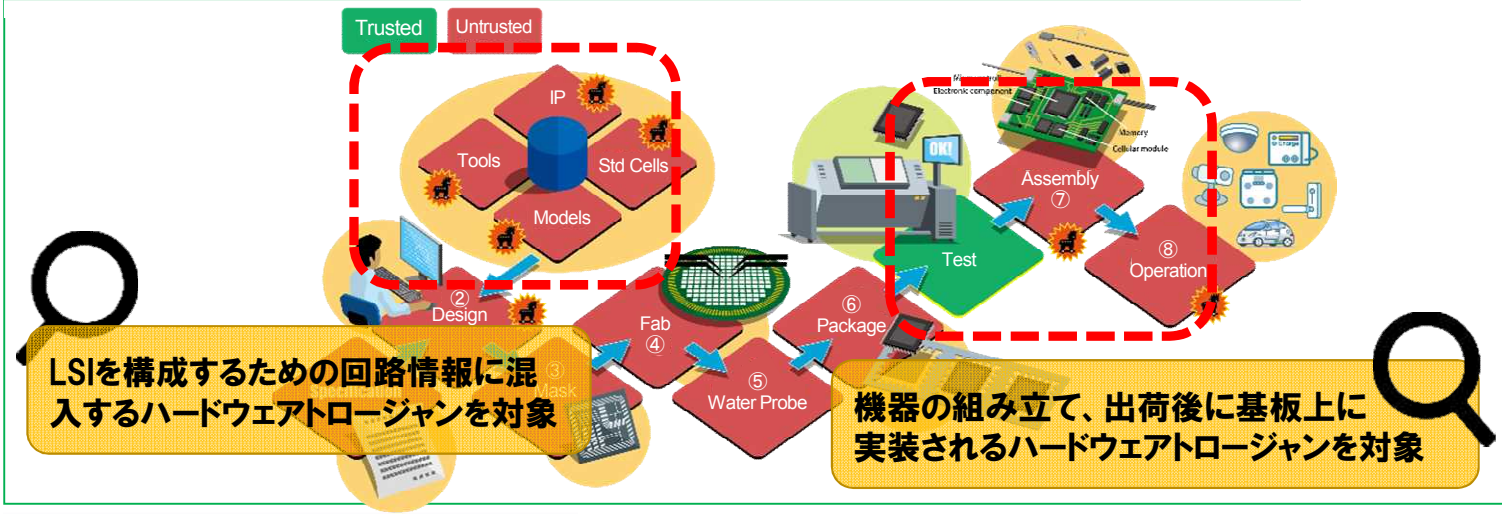
■ ハードウェアトロージャン検知技術

機器の製造過程及び出荷後に機器を構成する基板上に実装される可能性のあるハードウェアトロージャンを検出し、信頼の起点となるハードウェアのセキュリティを確保

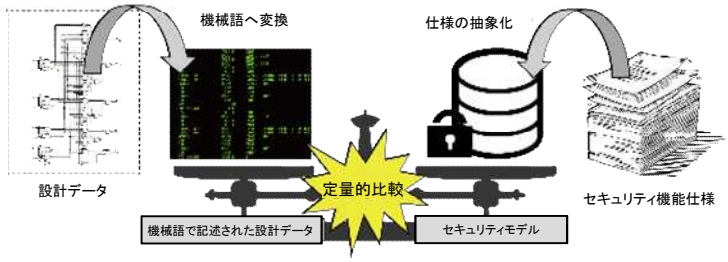
■ LSI設計IPのHT形式検証技術

ハードウェアIPコアの論理記述検証とソフトウェアのセキュリティ検証に用いられる形式検証を統合し、ハードウェア・トロージャンフリーなIC設計を保証する技術に関する基礎理論を構築

サプライチェーンにおいてハードウェアトロージャンが実装されるタイミング



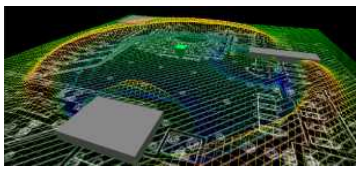
LSI設計IPのHT形式検証技術



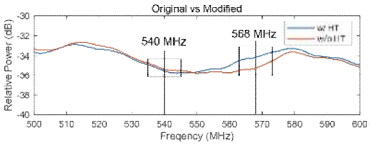
半導体チップ設計の際に第三者から購入する設計IPにHTが混入している場合を想定し、形式検証技術で設計IP内のHTを検知する方法を基礎理論として開発し、実証

ハードウェアトロージャン検知技術

時間領域計測による検知



周波数領域計測による検知



SCUに搭載した**アクティブセンサ**を用いて周囲をセンシングしIC及び周囲の**電気的な変化を計測**することで**HTの実装**された**位置を検出**・**動作を抑止**

奈良先端大、神戸大学、東北大学、横浜国立大学、
電子商取引安全技術研究組合（ECSEC）

安価なIoT機器に組込めるSCUを対象としたセキュリティ保証スキームの構築

創出・証明

網羅的な脅威分析で、セキュリティ要件を明確化し、セキュリティ評価の厳密さと開発工数のバランスを確保

技術の特長

■ **セキュリティのレベル分け**

IoTの安価な末端ノードに対し、セキュリティ実装の確からしさのレベルの分け方とセキュリティの示し方の妥当性を確保

■ **セキュリティ保証スキーム**

信頼の基点となるハードウェアを組込む機器に最適なセキュリティ保証スキーム（セキュリティ評価技術と認証の仕組み）を構築

SCU搭載IoT機器のセキュリティ保証

信頼の基点となる暗号ハードウェアを組込む1チップマイコン等を軸とした、高信頼な機器を妥当なコストで開発する基盤を構築

IoT機器の脆弱性評価／攻撃手法の集約

- Physical Attacks
- Overcoming sensors and filters
- Perturbation Attacks
- Retrieving keys with DFA
- Side-channel Attacks
- Exploitation of Test features
- Attacks on RNG
- Java Card applications
- Software Attacks

信頼の基点に対するセキュリティ保証スキームの整備／構築

SCUを信頼の基点として用いたIoT機器のセキュリティ確保

ユーザフレンドリー志向で作成：
・ガイドライン
・チェックリスト

低消費電力・高安全な暗号技術搭載機能の確実な活用

厳密な保証

SCUに対するセキュリティ保証スキーム

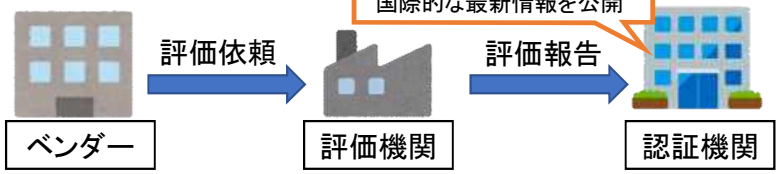
対象IoT機器に組込まれる暗号モジュールが**確かにSCU**であることを認定

・SOGIS
・JEDS
・JHAS

海外機関

SOGIS[*1]における脆弱性評定(AVA_VAN)や**評価保証レベルEAL**[*2]等の議論動向を踏まえ、SCU搭載機器のセキュリティ保証のあり方を検討

脆弱性や攻撃手法に関する国際的な最新情報を公開



[*1] Senior Officials Group Information Systems Security
[*2](Evaluation Assurance Level)

⇨ 製品を認証

国立研究開発法人産業技術総合研究所（AIST）

【日本電信電話】

OT/IoTシステムに対応可能な真贋判定

創出・証明

多様なOT/IoT機器に対応可能な真贋判定により不正ソフトウェアが混入しにくいサプライチェーンを実現

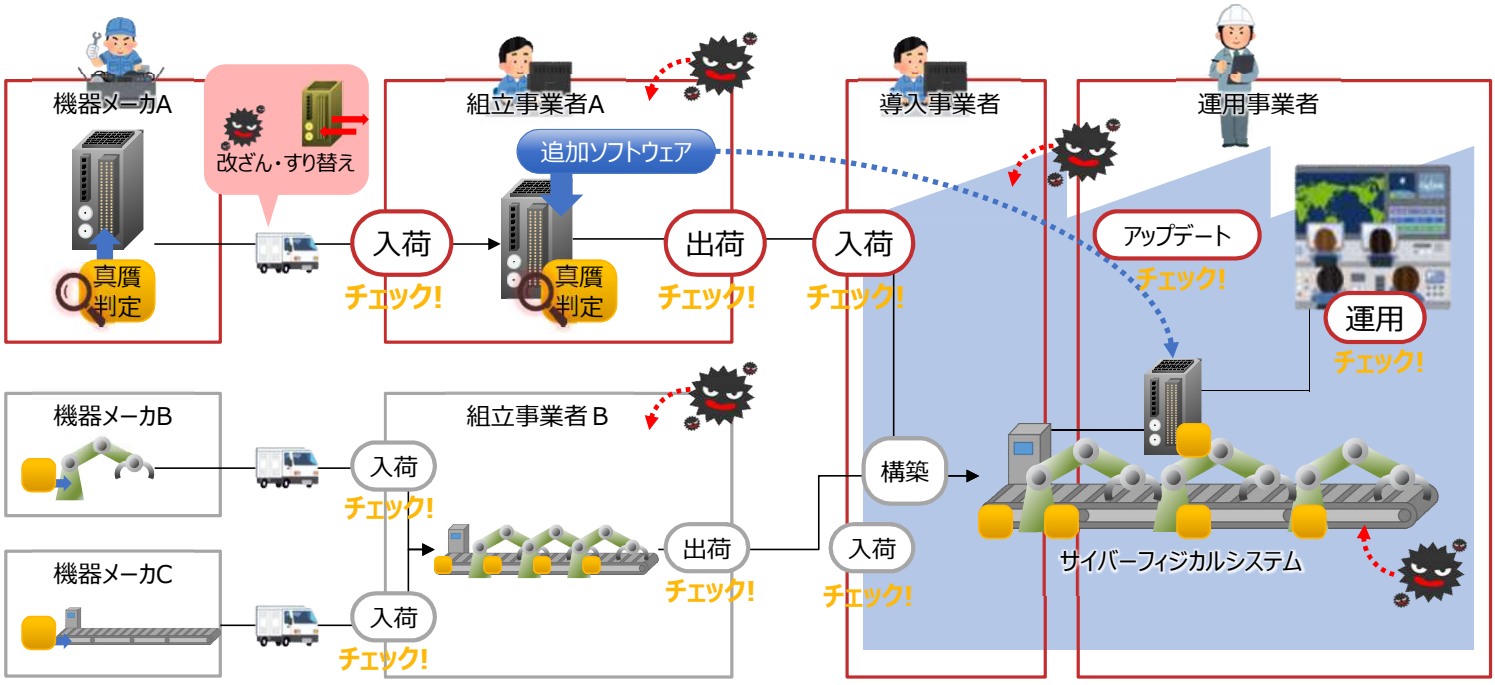
技術の特長

■ **機器の運用時だけでなく流通時も容易に判定可能**
多様なOT/IoT機器内で安全確実に動作する判定機能により、ソフトウェア完全性確認を自動化（サプライチェーン常時判定技術）

■ **出荷後の構成変更に合わせ判定基準を最新化しセキュアに共有**
流通時及び運用開始後の各過程で加わるソフトウェア構成変更に対して、判定基準を安全に更新（構成変更対応技術）

■ **セキュリティ専門家でなくても正しい判定基準を作成可能**
多様なOT/IoT機器の判定基準をツールにより正確かつ容易に作成（判定基準作成技術）

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を確立



出荷後の機器の完全性を確認
機器に実装された真贋判定機能により、出荷後もユーザが機器の完全性を確認でき、セキュリティアップデート等を安全確実に実施できます。

製造から納品まで改ざん・すり替えを検知
各事業者が入出荷時に真贋判定を行い早期に改ざんを検知することで、不正ソフトウェアが混入しにくいセキュアなサプライチェーンを実現できます。

運用時のシステムの完全性を確認
各機器の真贋判定機能を連携させることで、多様な機器群で構成されるサイバーフィジカルシステム全体の改ざん検知を可能にします。

本研究開発テーマの背景

Society5.0の実現に向け、工場のスマート化やIoT機器の普及により、汎用ハードとソフトウェアを用いた機器開発が増加し、機器の製造、導入、運用の全過程で「不正機能の混入」のリスクが高まっています。このような中で、安全な製品を供給し安全に機器を運用するためには、機器の製造時や運用時だけでなく、サプライチェーンも含めたライフサイクル全体を通して機器の正しさ(真贋)を常に確認できる必要があります。

利用イメージ

入荷時の確認

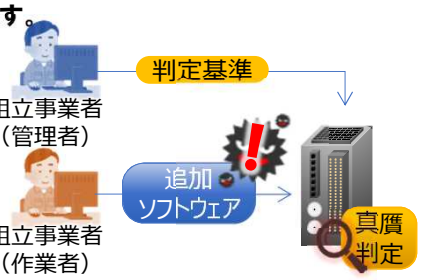
機器の配送時等に、不正なソフトウェアをインストールされる、機器をすり替えられるなどのリスクがあります。

機器メーカが定義した基準に基づいて、正しい機器に正しいソフトウェアがインストールされていることを確認できます。

出荷時の確認

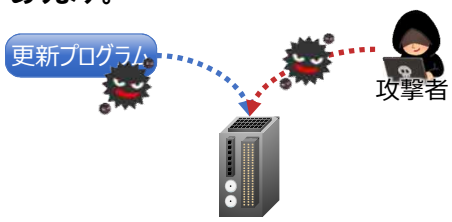
機器への機能追加時に、作業ミス・内部不正・作業環境汚染等により、機器が改変されるリスクがあります。

管理者が定義した判定基準に基づいて、作業が正しく実施できたことを確認できます。

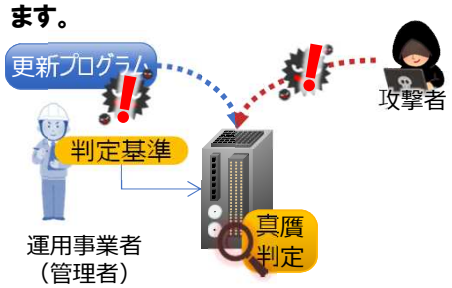


運用時の確認

機器の運用時に、外部からの攻撃、更新プログラムの改ざんが起こるリスクがあります。

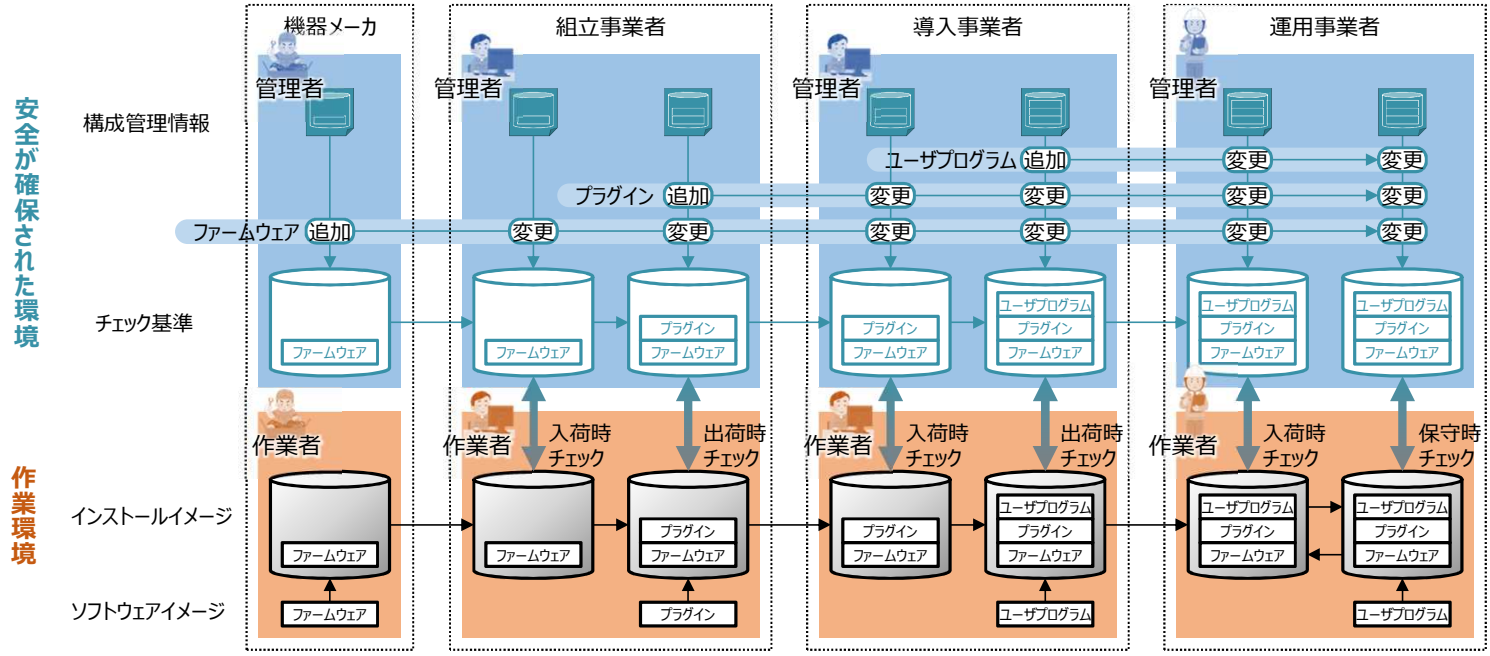


管理者が定義した判定基準を使って、意図しないソフトウェア変更を検知できます。



技術のポイント

流通時及び運用開始後の各過程におけるソフトウェア構成変更に合わせて、正しい機器の状態を安全が確保された環境で管理し、常に最新の判定基準を共有できるようにします。このことによりサプライチェーンを含む機器のライフサイクル全体にわたり、機器の真正性および完全性が確認できるようになります。



稼働中の機器の軽量型真贋判定

創出・証明

性能やメモリ量に制約のあるIoT機器にも導入可能で、稼動中ソフトウェアの「改ざん検知」を行うことで安全性を担保

技術の特長

■ **起動時だけでなく稼働中にもIoT機器を常時監視**

メモリ上のソフトウェア実行コードの真贋判定をIoT機器の動作中に行うことで、長期間稼働し続けるIoT機器の安全性を向上

■ **自動組込、自動復旧により運用を支援**

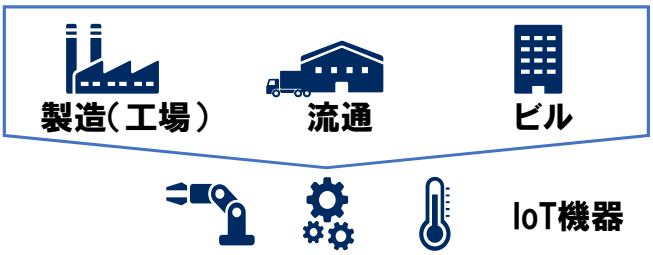
自動組み込みツールにより、機器やソフトウェアのバージョンアップがあっても導入可能。「贋」と判定された場合は改ざん領域を自動復旧することで、開発・復旧フェーズのコストを最小化

IoT機器の真贋判定における課題

メモリ上の実行コードのハッシュ値を用いたホワイトリストによって稼動中の真贋判定を行う技術があるが、実用面で以下の課題がある

① 機器やソフトウェアのバージョン毎に必要となるホワイトリストの作成コストが大きい
② 実行コードの検証に加えて、その実行順序の検証も必要
③「贋」と判定された後の復旧コストが大きい

利用産業と利用シーン



製造（工場）、流通、ビル等の分野の様々なIoTシステムで利用されているIoT機器に導入でき、稼働中のIoT機器の完全性を監視

課題解決に向けた研究開発技術の概要

①開発フェーズ

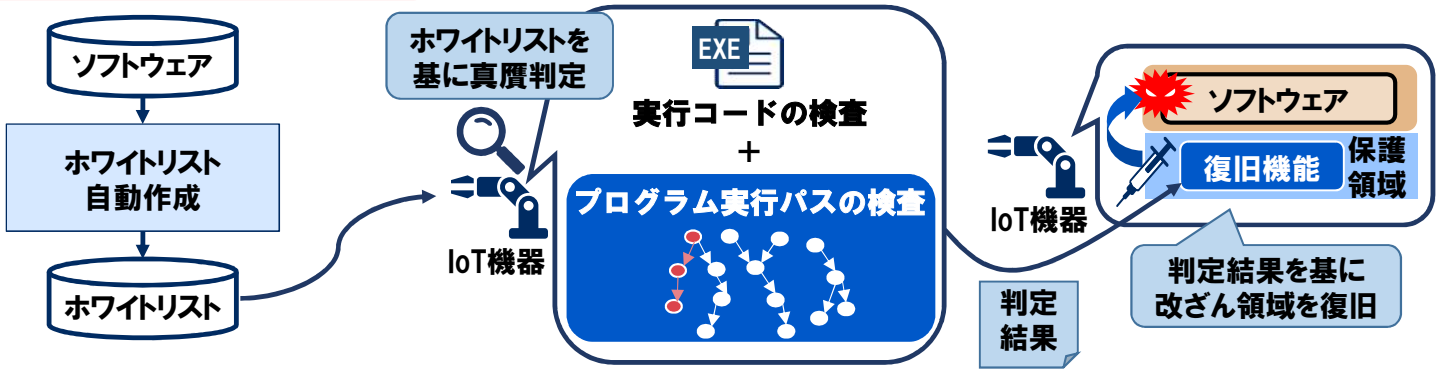
ホワイトリスト生成技術
IoT機器の動作中に低負荷な検査を行うためのホワイトリストを自動生成

②検知フェーズ

真贋判定の精度向上技術
実行コードと実行順序（実行パス）を同時に監視し、判定精度向上

③復旧フェーズ

自動復旧技術
改ざんされたソフトウェアを正常な状態に戻すことで、IoT機器を自動復旧



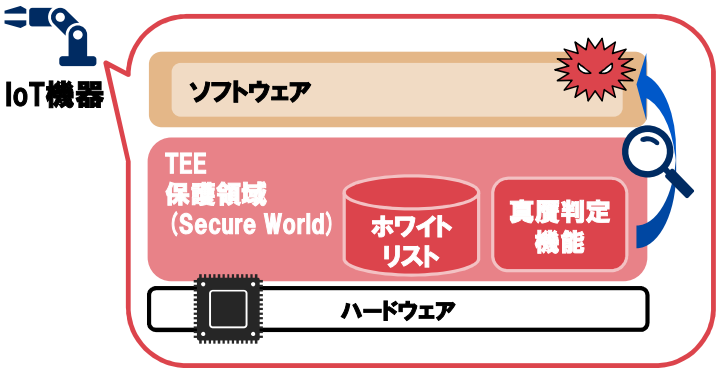
稼動中のIoT機器で真贋判定を実現

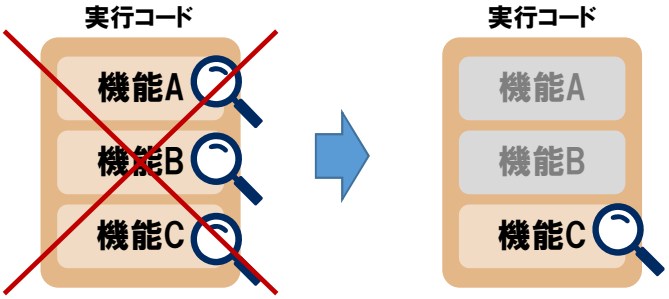
■ 軽量性

ソフトウェアの制御等による複雑な振る舞いの監視ではなく、実行コードと実行順序のみを監視するシンプルな方式
メモリ上に保護領域を作成するTEE(*)に組み込むことで保護コードが不要となり、軽量化を実現

■ 高速性

ソフトウェアの構造を把握し、これから実行される機能が格納されているメモリ領域を特定することで、その領域のみを検査
検査領域を絞り込むことで、IoT機器の動作に影響を与えない高速な真贋判定を実現





実行コード全体の検査は処理負荷が高い

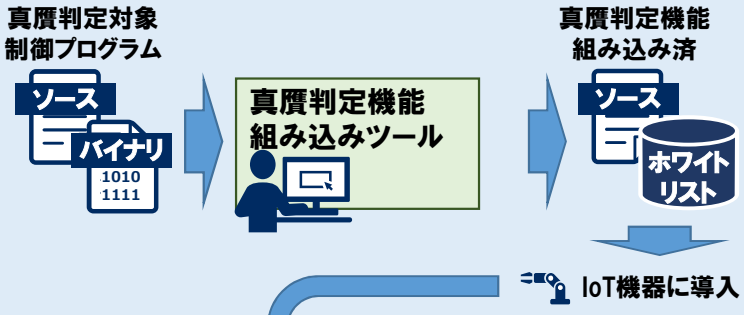
検査領域を絞り込むことで処理負荷を削減

(*) TEE: Trusted Execution Environment

研究開発技術の利用イメージ

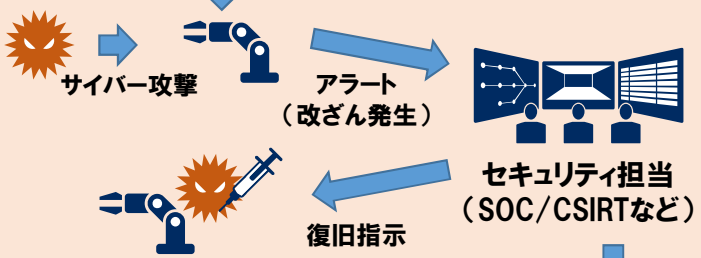
機器メーカ

- 対象とするIoT機器の制御プログラムのソースコードとバイナリを開発ツールに入力することで、真贋判定機能を自動組み込み
- 真贋判定機能を組み込んだ制御プログラムをIoT機器に導入



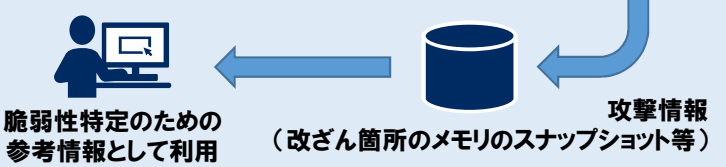
ユーザ企業

- サイバー攻撃により改ざんが発生すると、リモートの管理コンソールにアラートが表示
- 管理コンソールから復旧を行うと、IoT機器が正しく動き始める



機器メーカ

- サイバー攻撃を受けたIoT機器から収集した情報を基に脆弱性を修正



[メモ]

サプライチェーンにおけるVCPの適合性検証

創出・証明

ヒト、データ、プロシージャの適合性の統合による信頼の創出と証明

技術の特長

■ **適合性検証**
検証の基準情報としてVCP*モデルを定義し実績情報と適合性検証の実行

■ **デジタルエビデンス**
信頼の起点となるデジタルエビデンスを保存

*VCP:Value Creation Process

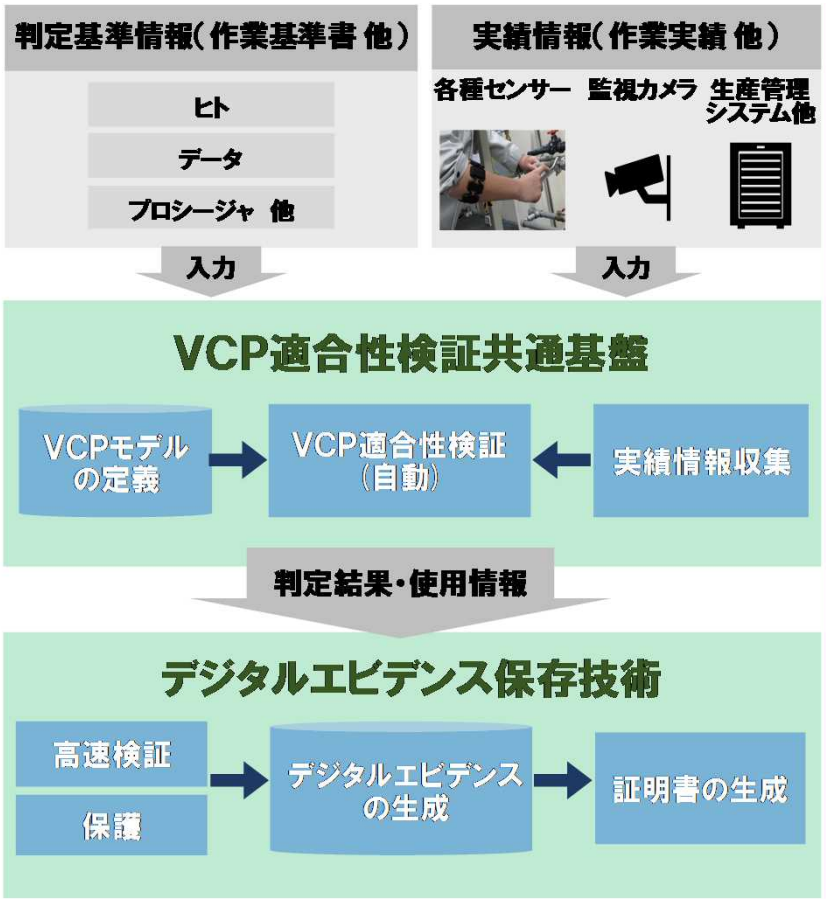
効果

本技術を活用することにより、サプライチェーンにおけるVCPの適合性検証

■ **企業価値、CSRの向上**
①不正な改ざん・作業等の検知・抑止ができ、企業のコンプライアンス対策に寄与
②第三者へ説明するための根拠として、企業の説明責任を果たすことで企業価値、CSRの向上に寄与

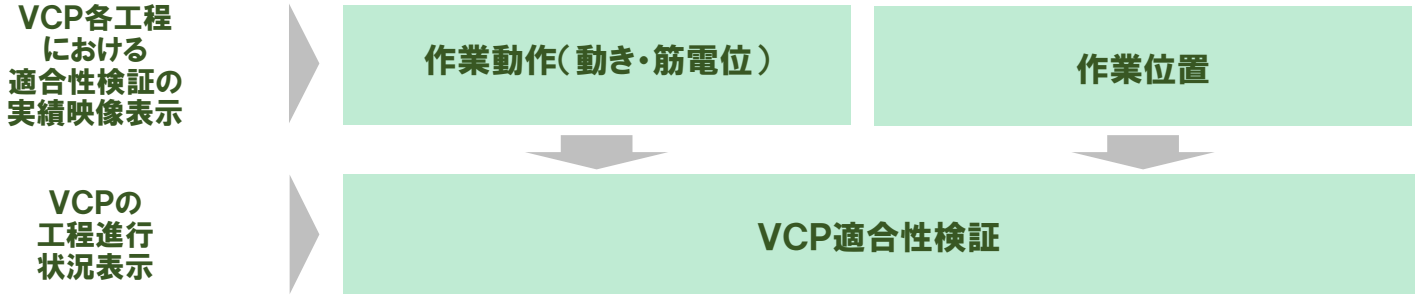
■ **利用シーン**
サプライチェーン上でのヒト、データ、プロシージャの適合性検証とエビデンスの保存

信頼の創出と証明のイメージ



VCPの適合性検証デモンストレーション

本デモでは、VCP適合性検証を実行するシステムをご紹介します。デモのイメージとしては、製造現場における部品組立を想定し、各工程での適合性検証を行い、最終的にはVCP適合性検証を実施し、検証結果とその使用情報をデジタルエビデンスとして出力する一連の流れをご紹介します。



サプライチェーンにおけるデータの適合性判定

創出・証明

データの取り扱いに関する「正しさ」を保証

技術の特長

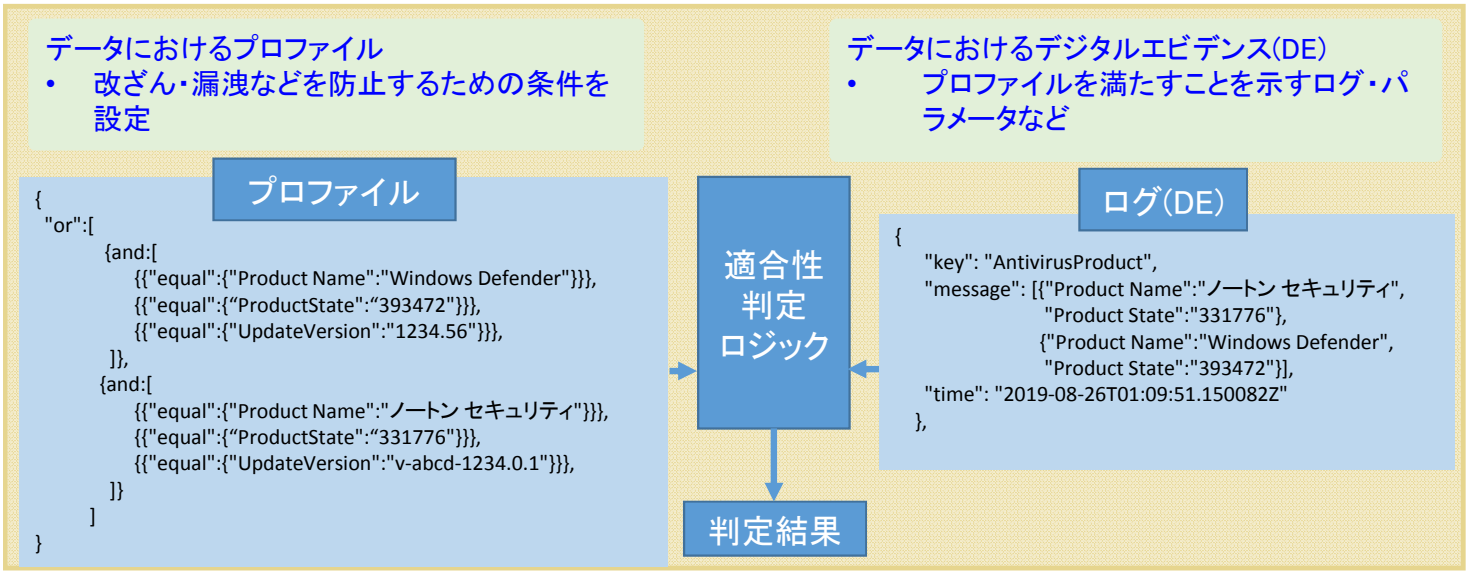
■ データの正しい取り扱いをルール化
改ざん・漏洩などの防止の条件をプロファイルとして設定
■ 操作ログ・端末の環境情報などをセキュアに取得・保管
データにおけるデジタルエビデンス(DE)として取得・保管
■ 適合性判定
プロファイルとDEを比較し自動判定

効果

ねらい:データの安全な管理を保証することで信頼を創出
利用シーン:サプライチェーン上でのデータやり取り
脅威:データの改ざん・漏洩・窃盗など

データの適合性判定のイメージ

プロファイル(判定条件)の例
セキュリティソフトがインストールされており、最新版に更新されている
適合性判定ロジック
①プロファイルで指定された条件を抽出
②対象のログを検索し条件と判定



サプライチェーンにおけるデータの適合性判定

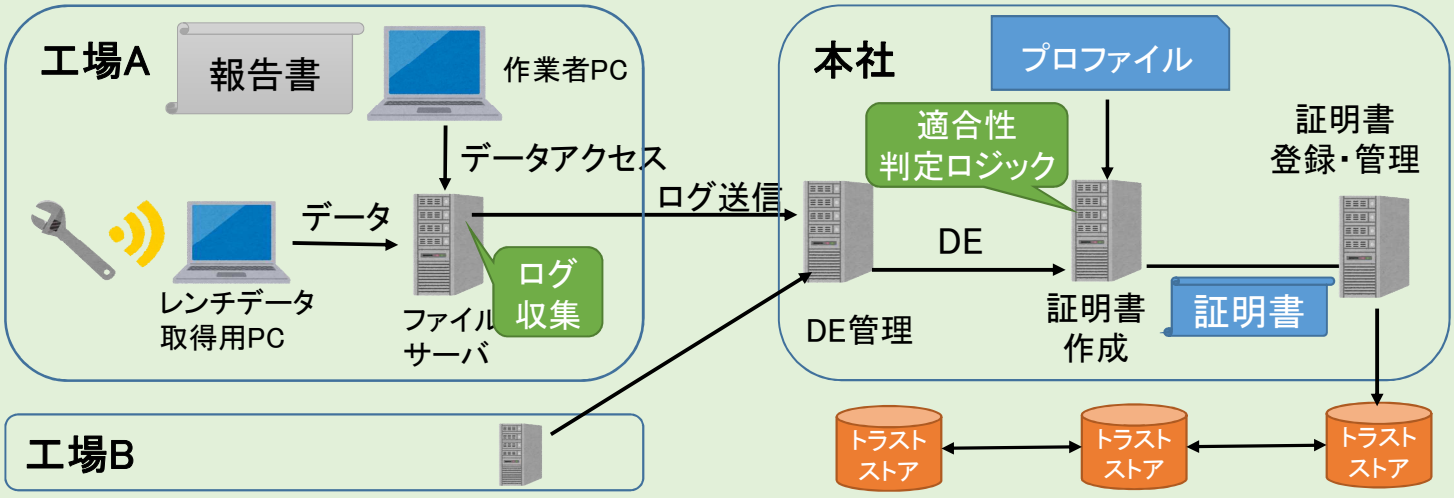
創出・証明

データの取り扱いに関する「正しさ」を保証

データの取り扱いに関する「正しさ」の保証の実施イメージ

- データの取り扱いには、データアクセス、データ取得、データ送信、データ格納などがあり、それぞれ「正しさ」の確認が必要
- 証明書によって各組織における正しさを証明
- デジタルエビデンス（DE）を「正しさ」の根拠として管理
- トラストストアによって、組織ごとの正しさをまとめ、全体としての正しさを証明

工場における活用例(デモ)



ビル管理への応用例

組織	役割	証明対象のデータ
エレベーター製造	製造・遠隔監視	仕様・監視データ
監視カメラ製造	製造	仕様・保守履歴
空調機器製造	製造	仕様・保守履歴
施工業者	ビル建設	設計図面
メンテナンス業務	作業・報告	作業データ
警備業務	監視	監視カメラデータ・入退履歴

問い合わせ先：https://www.kddi-research.jp/inquiry.html

サプライチェーンにおけるヒトの適格性判定

創出・証明

ヒトによるサービス提供・製品製造の信頼性確保

技術の特長

ヒトの適格性を判定し、証明書を発行

■ヒトの適格性の特性に応じた扱い

有効期限や更新条件の異なるヒトの属性情報をタイムリーに取得・参照

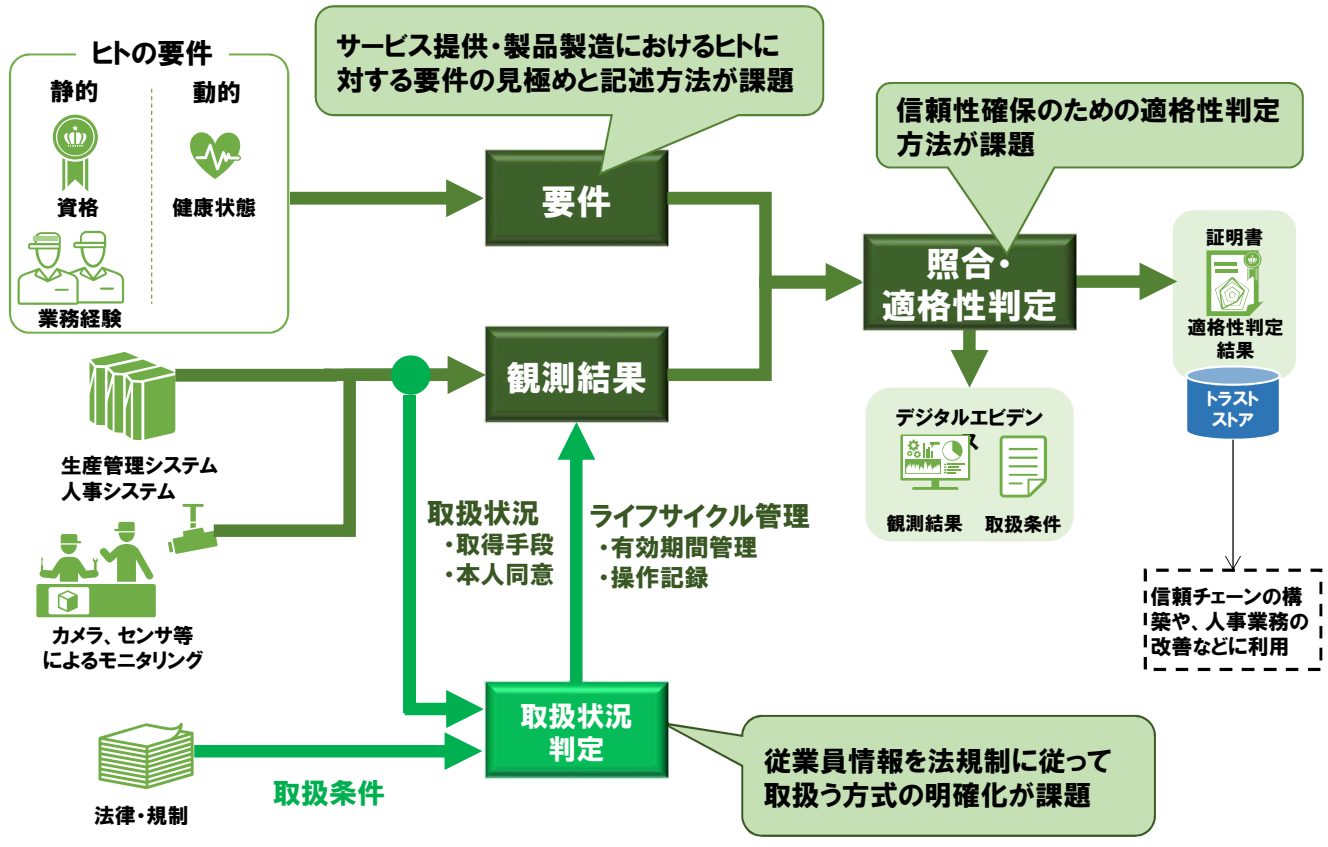
■従業員情報の取扱い

従業員情報を外部へ開示するため、法規制・規定に従った情報取扱を実施

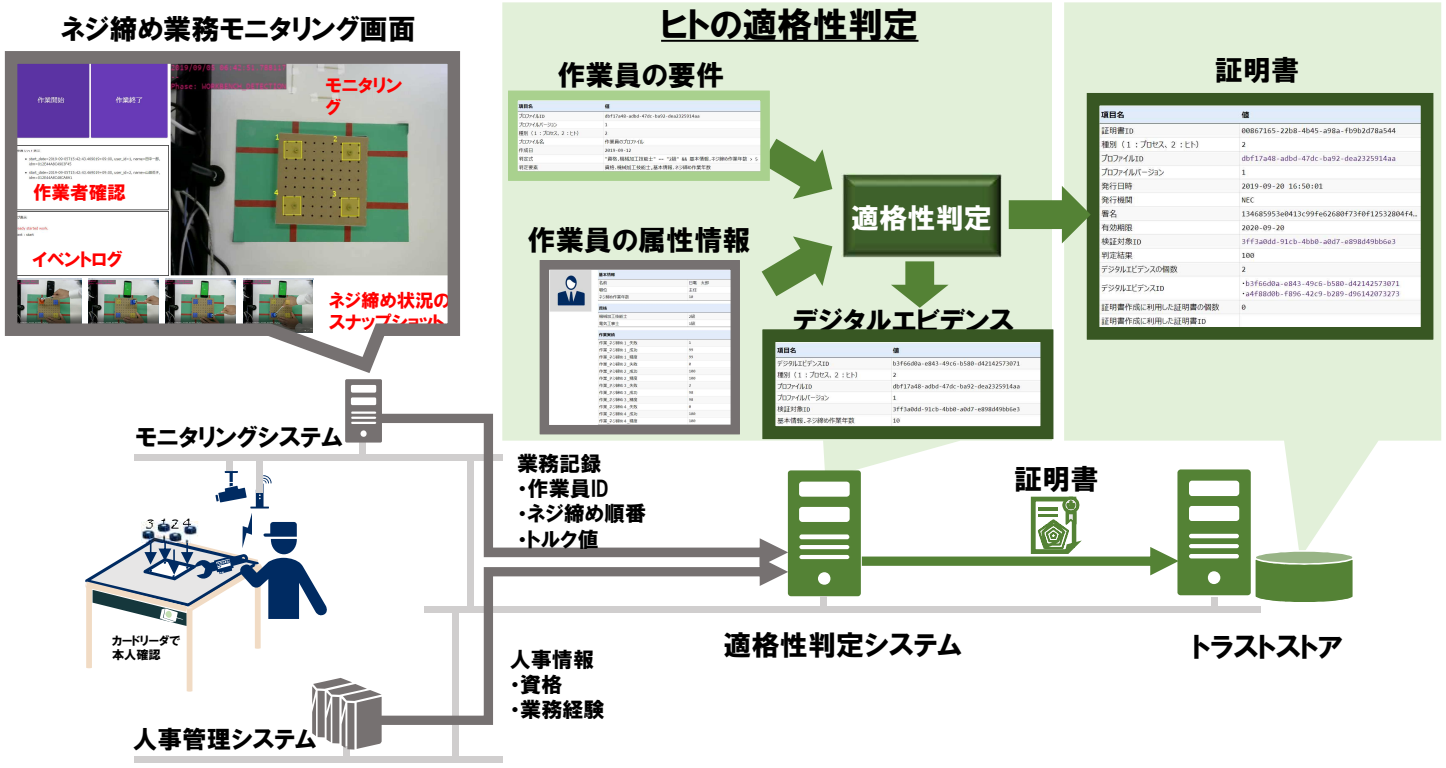
効果

①適格性を満たさなかった業務を見える化し、サービス・製品の安全性維持に貢献
②信頼チェーン構築による問題発見の効率化促進
③トラストストア利活用による人事業務の改善

ヒトの適格性判定アーキテクチャ



製造工場でのネジ締め業務における作業員の適格性判定



ヒトの適格性判定の技術開発に係る研究課題

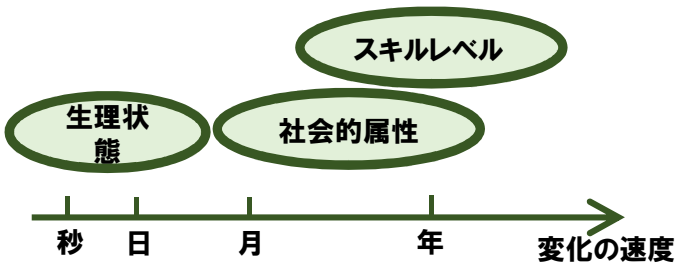
「ヒトの属性情報」に関する研究課題

- ヒトの適格性を判定するために検証すべき属性、その属性の表現形式、及びその属性の確認手法

本人同一性　資格　スキル　生理状態

IDカード

- ヒトの適格性の判定要件において、変化の速度が異なる様々な属性への対応



「従業員情報の取扱い」に関する研究課題

- 法規制・ガイドラインに従った、従業員個人情報の第三者への開示に当たって、消費者の個人情報とは異なる取扱いが必要である。
  - 消費者の個人情報取扱では、その利用目的等を明らかにした上で、本人同意が必要である。
  - 従業員の個人情報取扱では、本人同意だけでは不十分であるとみなされる。雇用主は従業員より立場が強いので、本人同意が自発的なものとはみなされないことがある。
- 例えば、欧州委員会の見解※では、従業員個人情報を利活用するには正当な理由をユースケース毎に明らかにする必要がある。

「正当な理由」の例：

- 雇用契約を履行するため
- 法的義務に従うため
- 雇用主の合法的事業 (legitimate interest) を推進するため

※Opinion2/2017, Article 29 working party, European Commission

【富士通】

サイバー空間のデータ流通保証

動的に構成・再構成される次世代サプライチェーンを支える安心・安全なデータ流通機構

構築・流通

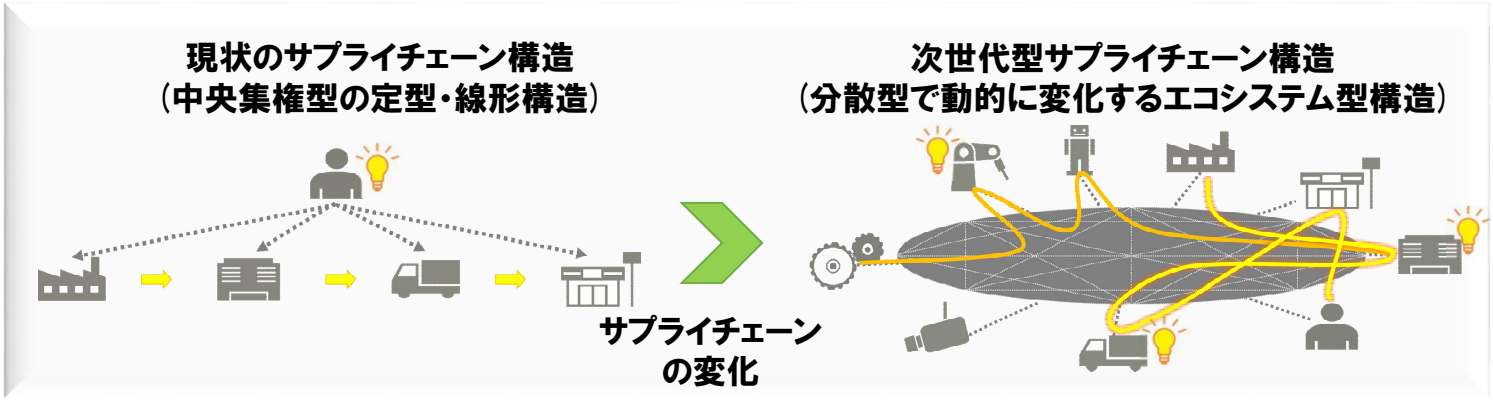
大規模・複数業種サプライチェーンの「つなぐ」から「運営」までのライフサイクルを通した安全性を確保

技術の特長

- **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**
  接続企業の合意形成をサイバー空間上で実施、
  安心・安全なサプライチェーンの動的な構成・再構成を迅速に実現
- **脅威対策の均質化によるデータ流通機構の安全性維持**
  脅威対策の均質化により対処を共通化、自律連携により迅速に脅威に対応

背景

Society 5.0の実現には、個々の参加企業が起点となり、商品の新たな付加価値を創造する権限分散型でダイナミックに変化するサプライチェーンの次世代化が必要



課題と解決策

次世代型サプライチェーンを支える安全なデータ流通を実現

中央集権型の次世代化に向けた課題

- サプライチェーンの変更には、主幹企業が各企業、及び企業間の調整を実施する必要があり、時間・労力を要し、機会損失が発生
- 各社独自の接続・セキュリティ対策により、サプライチェーン全体の均質なセキュリティレベルの維持が困難

権限分散型サプライチェーンで実現

- 権限分散型で動的に変化するサプライチェーンを構成するため、各々の企業が起点となって合意形成を行う「信用できる場」を形成する仕組み（Trustworthy Field Constructor）を提供
- 脅威への対処を共通化、自律的にサプライチェーン全体に共有・対処適用することでセキュリティレベルを維持する仕組みを提供

サイバー空間のデータ流通保証

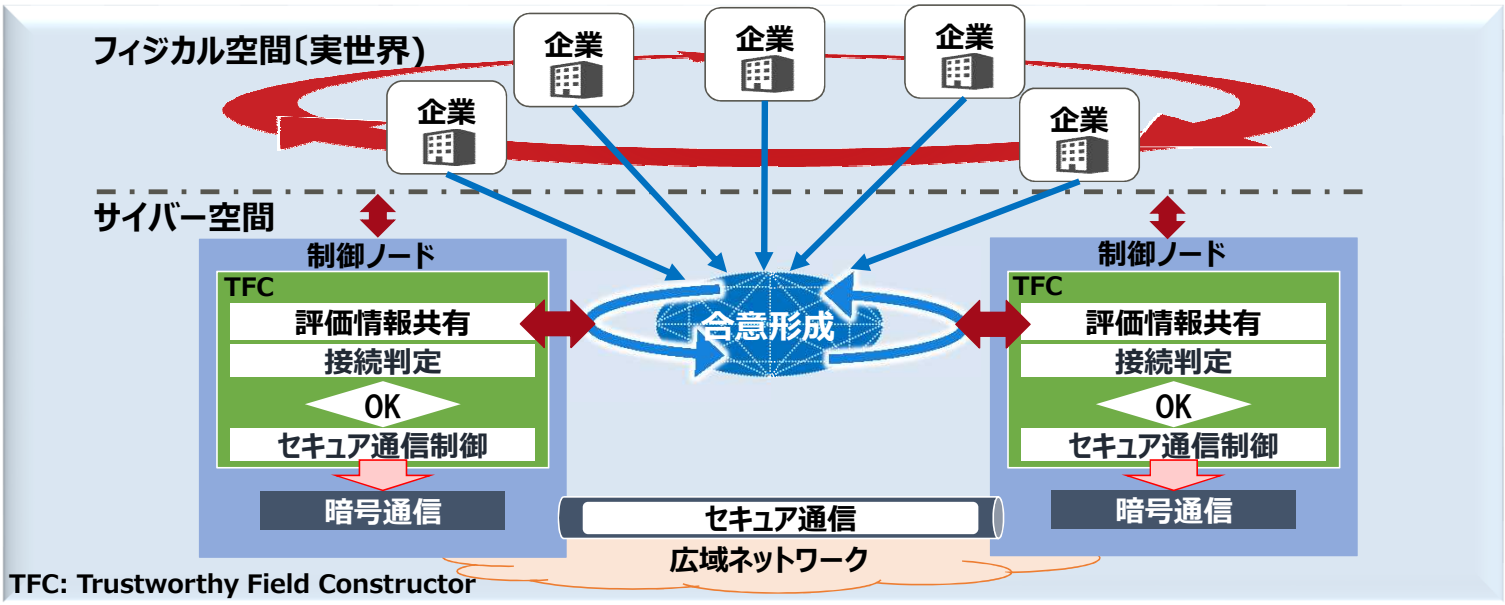
サイバー空間上の合意形成に基く安心・安全なデータ流通機構

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

◆技術の特長

・参加企業が評価項目を決めて情報を公開、相互に評価を行い合意形成

・公開された通信パラメータを用い、自動的に「信用できる場」を構成



セキュリティ維持技術の概要

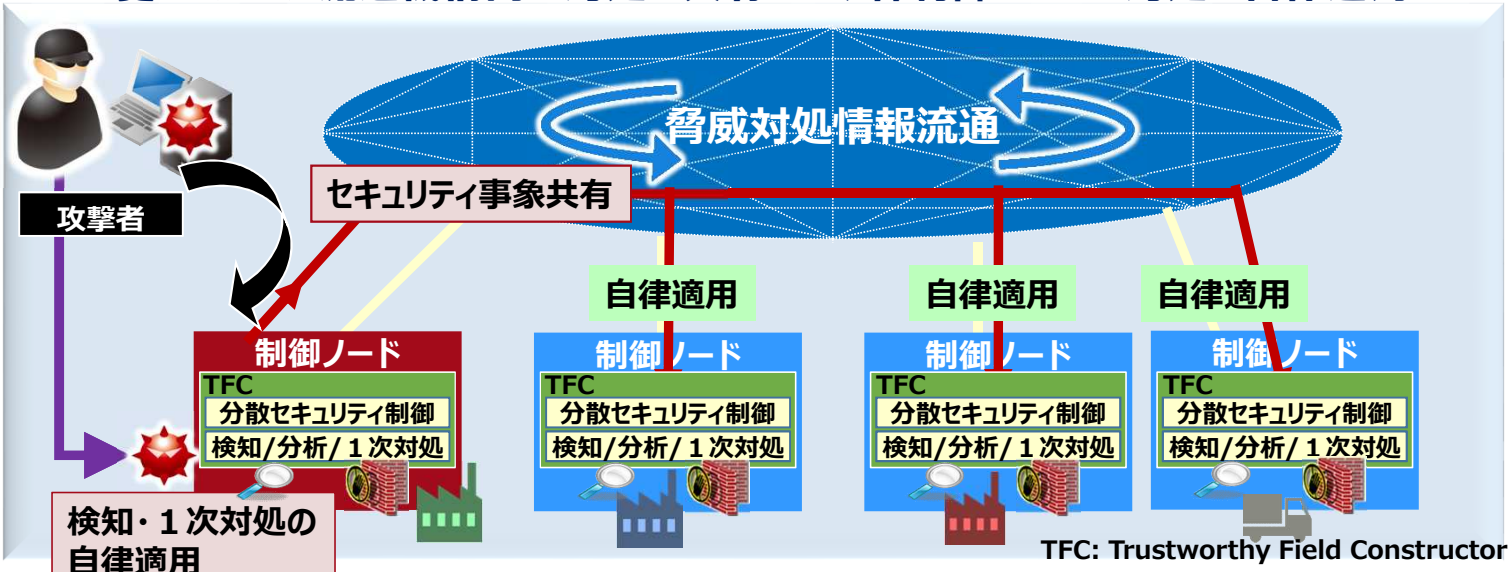
データ流通機構で脅威対策を標準化・配備することで、発生脅威に対する対処を共通化

対処を共有し、各制御ノードが自律的に対処適用することで、セキュリティレベルを維持

◆技術の特長

・制御ノード内の被害検知分析により、防御設定の変更など一次対処を自律適用

・更に データ流通機構内で対処を共有させ、各制御ノードが対処を自律適用



【日本電信電話、三菱電機】

サイバー・フィジカル異常検知

検証・維持

即時の監視・検知・対処支援を提供

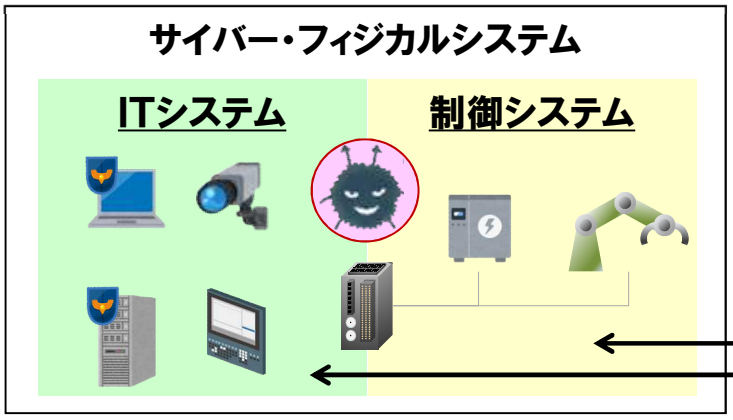
技術の特長

■ **導入直後から隙のない見守りを実現する即時監視**
機器の特徴に着目したセンシングと学習効率化によって、AIの学習期間に起因する監視空白期間の発生を回避（即時監視技術）

■ **被害の未然回避に役立つ即時検知**
サイバー攻撃の準備等に起因する微妙な変化（兆候）をも捉えることによって、回復困難な事態を未然に回避（即時異常検知技術）

■ **原因推定による異常対処への即時支援**
物理レイヤから管理レイヤ（システム運用計画等）に関する情報を活用することによって、異常原因を推定し異常対処を支援（原因推定技術）

サイバー・フィジカルシステムにおけるセキュリティ課題



【標的】
- 情報資産
- 物理資産

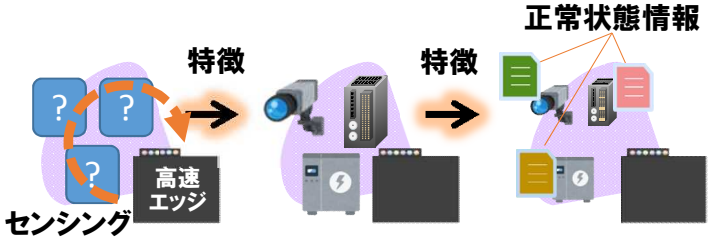
【被害】
- 機密性・完全性・可用性の侵害
- 物理的・人的被害

システム停止や品質低下による
ビジネス上の悪影響

セキュリティ異常の
早期検知が必要

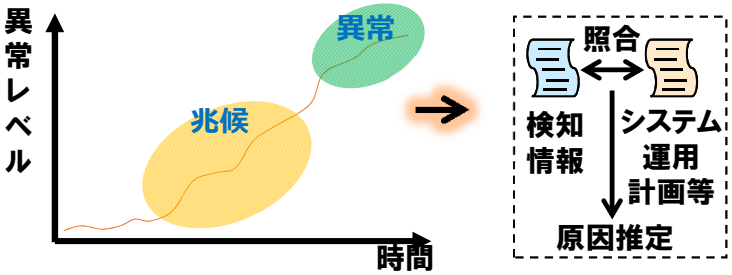
課題解決に向けた研究開発技術の概要

即時監視技術



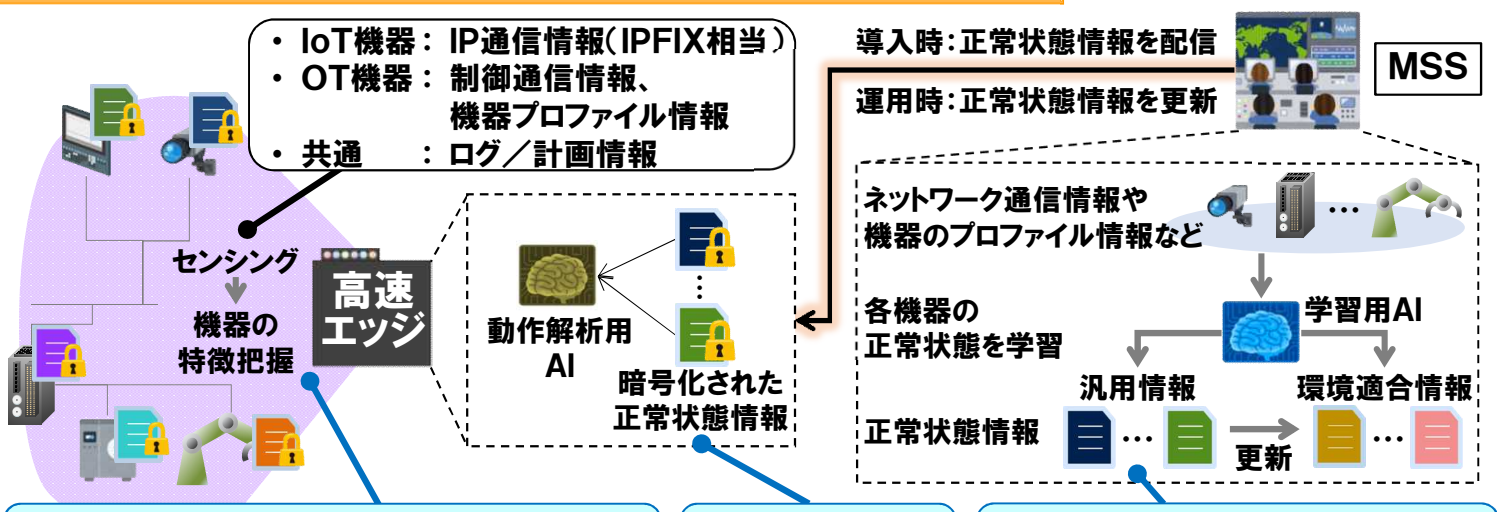
センシングにより把握した機器の特徴に基づき
正常状態情報を共有・適用して即時監視を開始

即時異常検知技術・原因推定技術



異常兆候の検知情報とシステム運用計画等の
活用による原因推定結果を事業者に通知

高速エッジとMSSの連携による即時監視の実現

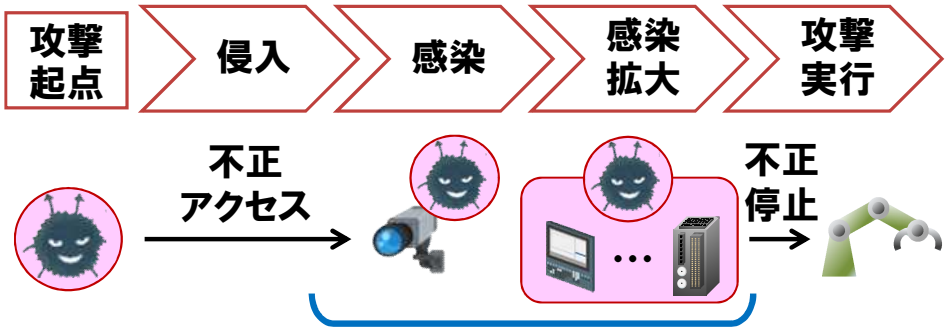


物理レイヤまで含み情報収集し、機器ごとに正常状態情報を適用し即時監視

正常状態情報を保護

高度な学習管理機能によって学習～共有・適用を最適実行

即時の異常兆候検知とその原因推定を兼ね備えた初動対応支援



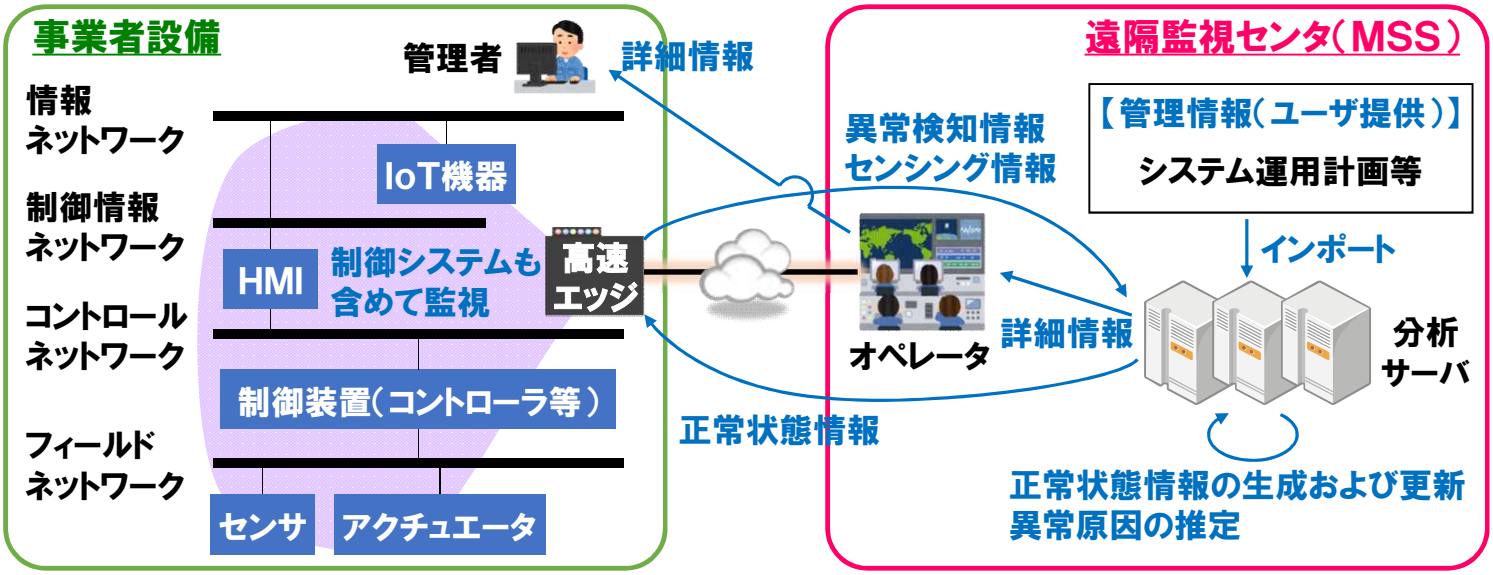
【管理情報（ユーザ提供）】
システム運用計画等

原因推定（例）：
運用計画にない停止であるため
異常原因はサイバー攻撃

AIが算出する機器ごとの異常レベルに対する時系列での変化傾向や機器間の相関等を解析し異常兆候を検知

兆候検知時に管理情報を分析し初動対応に有用な原因を推定

利用形態



【日立製作所】

サイバー・フィジカル空間をまたがって流れる不正なデータの検知・対処

検証・維持

監視対象のIoTシステムの特性を考慮した異常検知を行い、システム特性に応じ適切な対処方法を決定

技術の特長

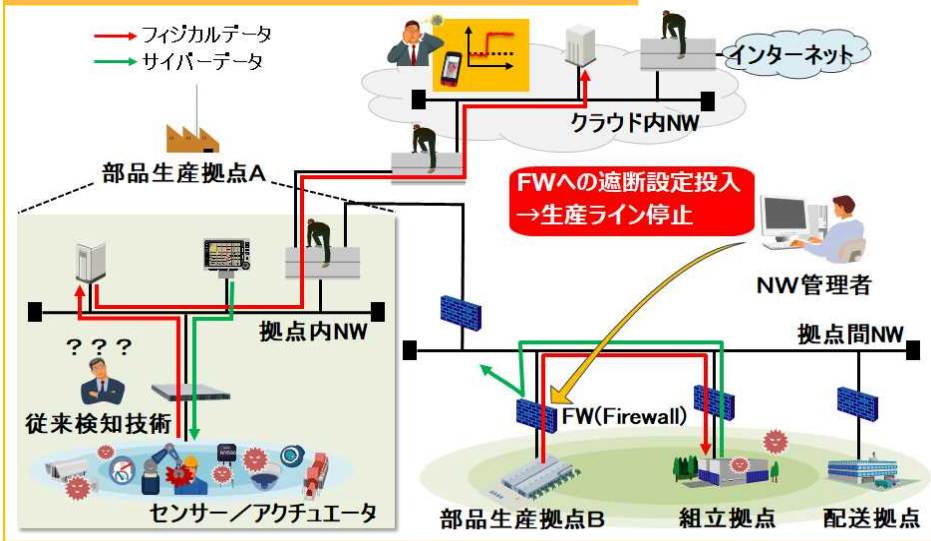
■ **誤検知・見逃しリスクを低減**

既存技術で検知しにくい不正なデータに対して、システム特性情報と照合することで、検知精度を向上

■ **サービス継続に適切な対処方法を決定**

システム特性情報を生かし、監視対象IoTシステムのサービス継続に適した対処方法を決定

IoTシステムにおける現状の課題



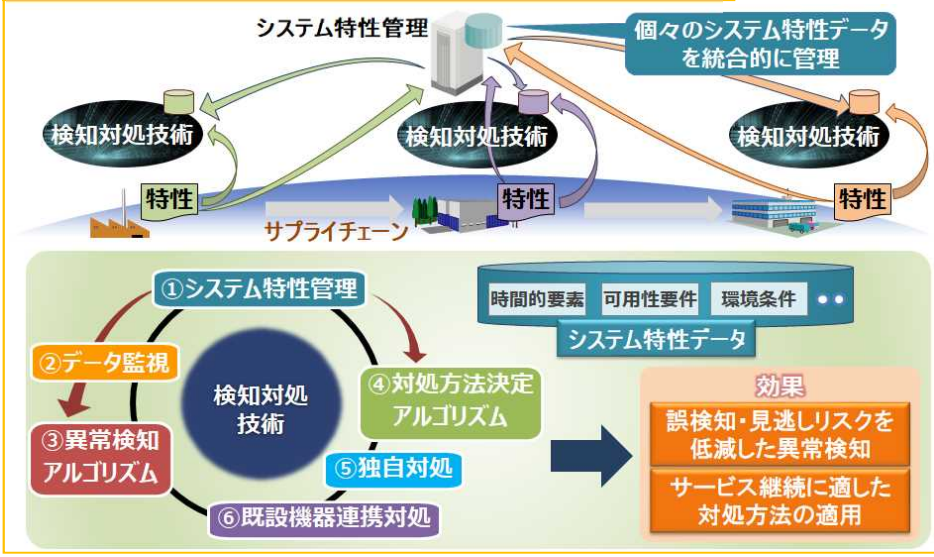
IoTデータ改ざん検知の課題

- 多種多様なデバイスへの追従が困難
- データの異常判定が困難

人手による対処時の課題

- 判断遅れによる被害拡大
- 人為ミスによる二次災害

課題解決のための研究開発技術概要



IoTシステム特性情報の活用

(1) IoTシステム特性情報を集約・管理

(2) システム特性情報を異常検知アルゴリズムに活用

(3) システム特性情報を対処方法決定アルゴリズムに活用

本研究開発テーマの背景

IoTシステムに迫る脅威

- 近年では、OT*1／IoTシステムもサイバー攻撃の危険にさらされている。
- インターネットにつながる各種IoTデバイスは、既に攻撃者に侵入されている可能性あり。
- サイバー・フィジカルデータを用いたサイバー攻撃は、従来の防御機構をすり抜け、IoTサービスに甚大な被害を及ぼす危険がある。

*1 Operational Technology

IoTデータ監視の必要性

不正侵入を完全に防ぐことは不可能

サイバー・フィジカルデータ改ざんにより

IoTシステム運用に甚大な被害の発生が想定

侵入後の特徴として

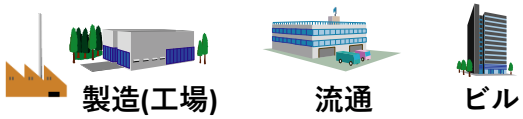
侵入から攻撃に至る前には、攻撃準備が行われる。
⇒ データに微細な変化が現れる。

侵入 → 遠隔操作 → 探索 → 拡散 → 目的遂行

攻撃準備段階の動作を検知、さらに、
サービス継続性を考慮した対処の実現が重要

検知対処技術として研究・開発

利用産業と利用シーン



製造(工場)、流通、ビル等、
さまざまな分野で稼働中のIoTシステムにおいて、既設のシステムに手を加えることなく、セキュリティ監視に適用可能

期待される効用

- IoTシステムの可用性向上
- セキュリティ対策の早期適用
- サプライチェーンの信頼性の維持

【日本電気】

サイバー攻撃発生時の影響評価及び対処策実行支援

検証・維持

OT/IoTシステムに対するサイバー攻撃リスクを自動分析 攻撃リスク可視化と対処策案提示により対処実行支援

技術の特長

■ **サイバー攻撃の影響を可視化**

サイバー攻撃が引き起こす可能性のあるシステムや機器への影響を自動で分析。セキュリティ知識がなくても、運用者はサイバー攻撃リスクを把握可能

■ **サイバー攻撃に対する対処策案を提示**

サイバー攻撃リスクに対する対処策案も自動で評価。運用者の対処策決定・実行を支援

サイバー攻撃対策の課題

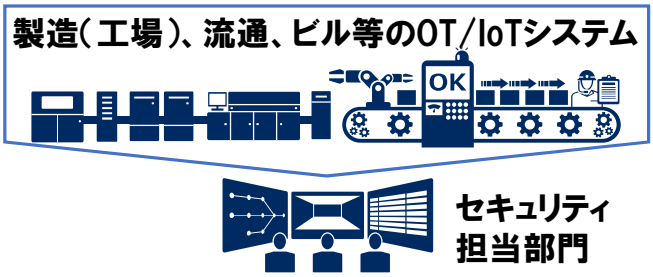
■ **サイバー攻撃による影響の把握**

システムで生じる事象や影響が及ぶ可能性の機器を把握するためには、サイバー攻撃に関する深い知識が必要

■ **対処策の有効性に関する事前評価**

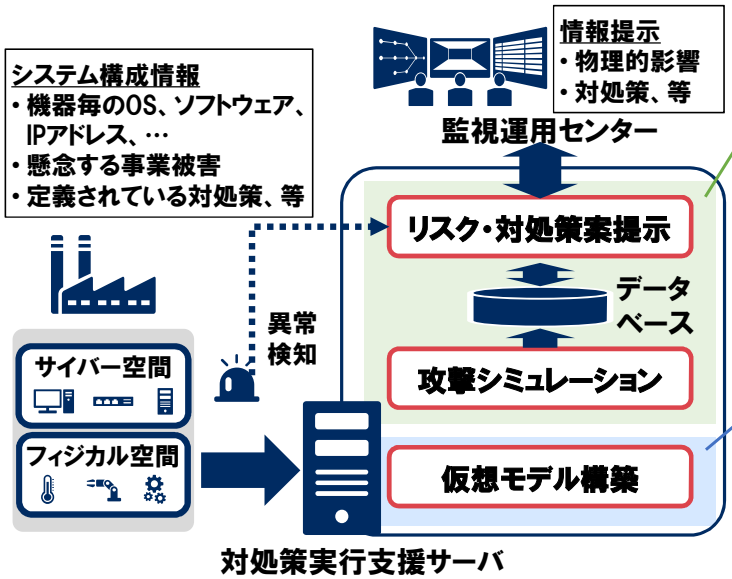
サイバー攻撃に対する対処策について、稼働中の実システムを用いた評価や机上での漏れのない評価は困難

利用産業と利用シーン



製造(工場)、流通、ビル等の分野のOT/IoTシステムにおける日常的なセキュリティ業務(リスク分析や対策立案等)やインシデント対応

課題解決に向けた研究開発技術の概要



■ **対処策実行支援技術**

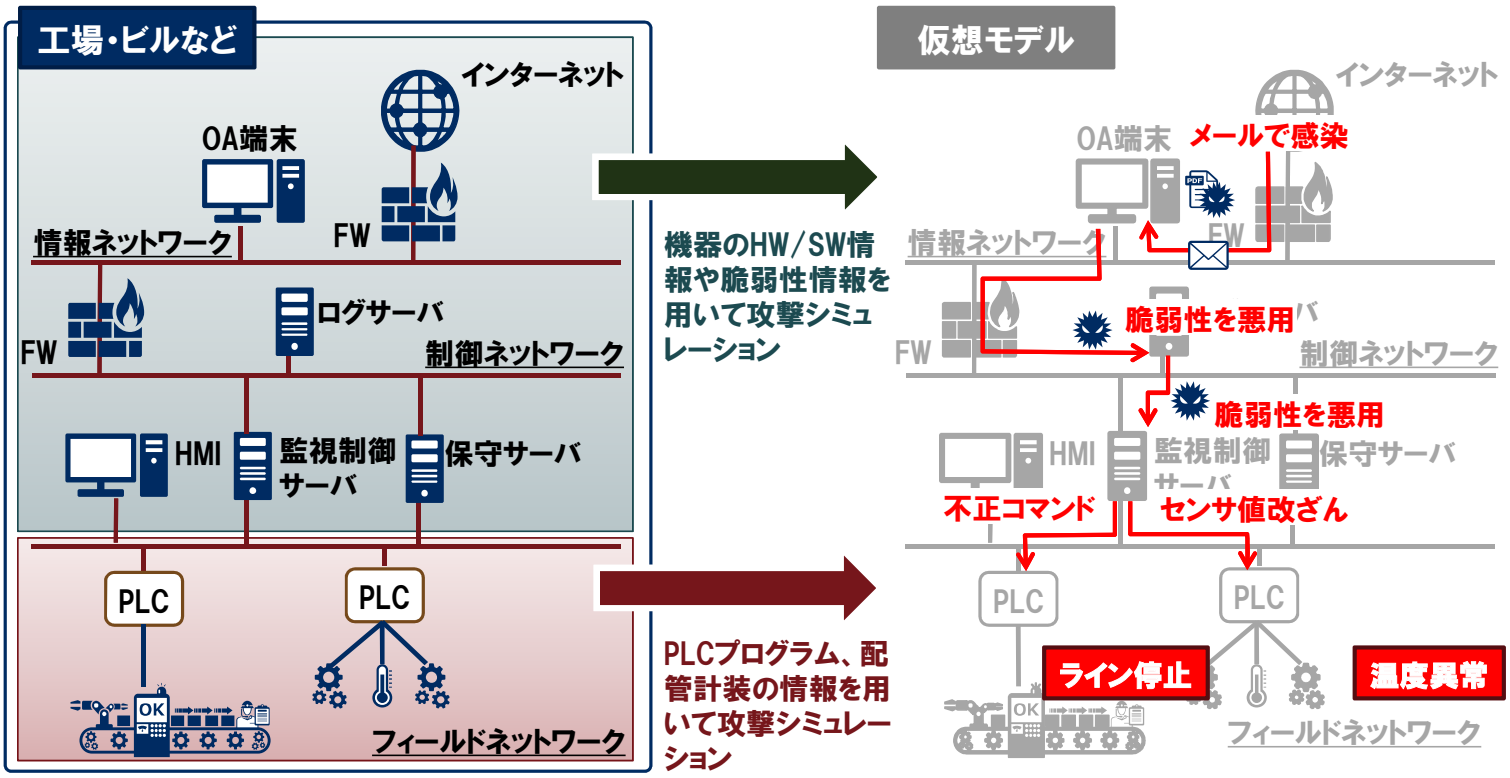
仮想モデル上で攻撃シミュレーションを実施することで、サイバー攻撃の影響や対処策の有効性を評価。実システムで異常が検知されれば、評価した結果を基に対処策案を運用者に提示

■ **仮想モデル構築技術**

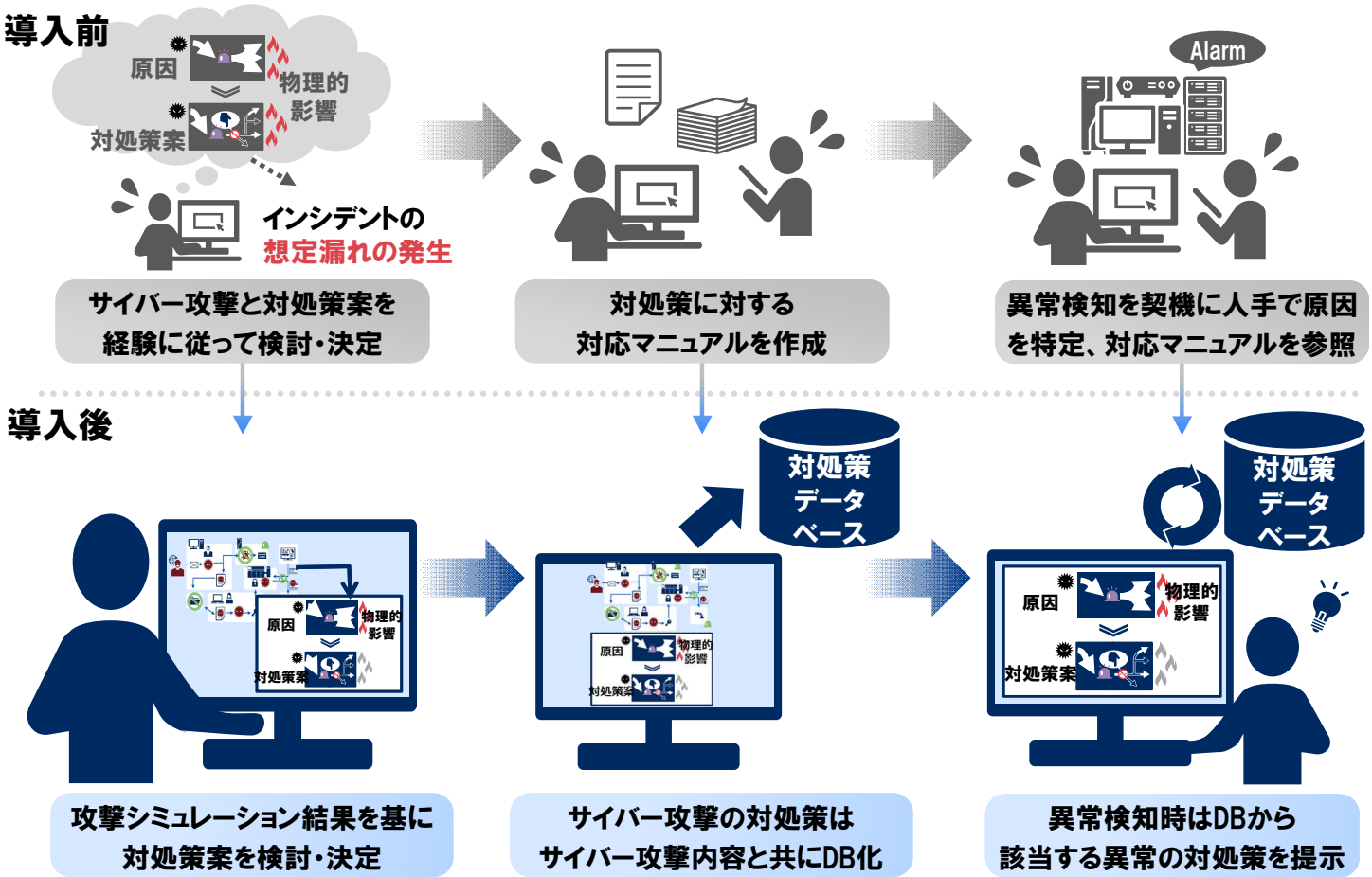
実システムを用いずにサイバー攻撃リスクを分析するための仮想モデルを構築

仮想モデル上での攻撃シミュレーション

サイバー攻撃リスクの分析に必要な情報を収集して構築した仮想モデル上で、システムに生じる可能性のある具体的な侵入・攻撃手口、その結果発生する影響を探索



対処策実行支援のイメージ



[メモ]

内閣府 Cabinet Office, Government of Japan

NEDO 新エネルギー・産業技術総合開発機構 New Energy and Industrial Technology Development Organization

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

SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」シンポジウム2019

～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～

13:00	開場	
13:30	開会あいさつ	内閣府　大臣官房審議官（科学技術・イノベーション担当）　髙原 勇
13:35	主催者あいさつ	NEDO　理事　今井 淨
13:40	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
14:00	招待講演①	「内閣官房におけるサプライチェーンのセキュリティ確保の取り組みとSIPへの期待」 内閣官房内閣サイバーセキュリティセンター　副センター長・内閣審議官 山内 智生 氏
14:20	招待講演②	「Software Supply Chain: A Collaborative Approach to Transparency」 米国商務省国家電気通信情報庁　サイバーセキュリティ戦略ディレクター アラン・フリードマン 氏
15:00	成果普及に向けたあいさつ	サブプログラムディレクター　瓜生 和久 情報処理推進機構　セキュリティセンター長
15:05	休憩・展示見学	
16:00	ミニ講演 研究開発チームによる研究内容の紹介	・セキュア暗号ユニットSCUを基点とするIoTサプライチェーンの信頼の創出（横浜国立大学） ・IoT機器等向け真贋判定による信頼の証明技術の研究開発（日本電信電話㈱） ・信頼チェーンに関わる情報の安全な流通技術の研究開発（富士通㈱） ・信頼チェーンの維持技術の研究開発（日本電気㈱） ・サプライチェーンの信頼性回復への挑戦 ～製品・サービス不正を防ぎ、信頼でつながる社会へ～（㈱日立製作所、日本電気㈱、㈱KDDI総合研究所）
16:55	閉会あいさつ	サブプログラムディレクター　今瀬 真 （大阪大学大学院　情報科学研究科　特任教授）

日時：　令和元年10月31日（木）　13:30～17:00
会場：　ベルサール神田　2Fホール
　　東京都千代田区神田美土代町7住友不動産神田ビル
参加費：　無料
定員：　200名

お問合せ先：　シンポジウム事務局　株式会社サイバー創研内
　　Tel: 03-3490-3181　sip2sympo_2019@cybersoken.com
主催：　内閣府、NEDO

シンポジウムHP　https://www.sip2-cyberphysicalsecurity.org/

SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」
シンポジウム2019