稼働中のIoT機器の軽量プログラム真贋判定

日本電気株式会社

稼動中のIoT機器のソフトウェアに対する真贋判定により、改ざんの有無を検証します

適用領域

IoT

ICTベンダー　製造　インフラ

流通　ビル・スマートシティ

技術の特長

■ CPU性能やメモリに制約のある稼働中のIoT機器の動作を監視

IoT機器のソフトウェアプログラムへ組み込むことで、機器のメモリ上のソフトウェアプログラムの改ざん、及びプログラムの実行順序の改ざんをリアルタイムに監視。

■ 機器の動作への影響を最小限に抑制する判定基準リストを自動生成

対象のIoT機器のソフトウェア構造を分析することで、機器のソフトウェアに適した検査タイミングや検査範囲を決定し、真贋判定の基準となる判定基準リストを自動生成。

導入効果

■ セキュリティ対策機能の導入が困難であったIoT機器を常時監視

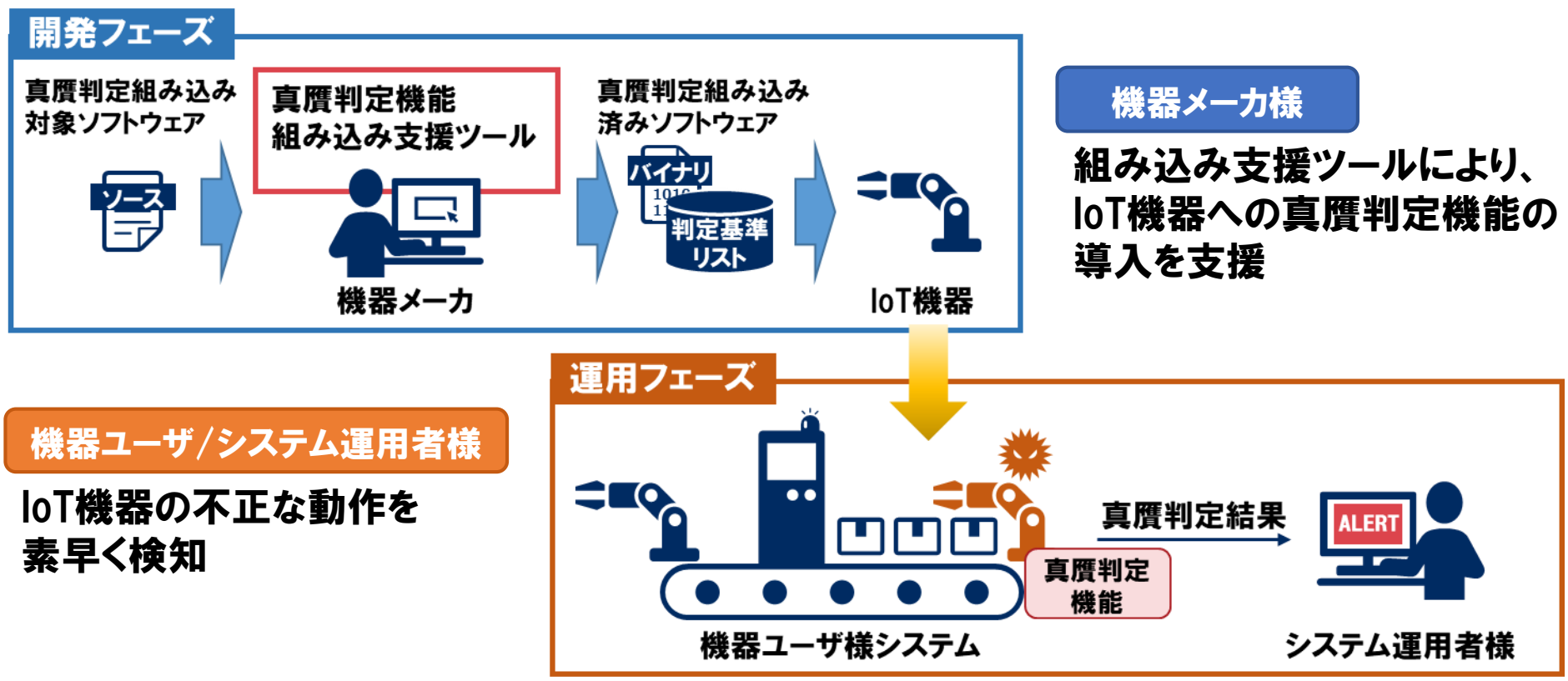
システムの末端に配置され、長時間稼働し続けるIoT機器の動作をリアルタイムに監視することで、システム全体の安全性を向上。

■ 判定基準リスト自動生成技術により、真贋判定機能の導入を支援

対象IoT機器のソフトウェアに対する判定基準リストの自動生成を含む組み込み支援ツールにより、真贋判定機能の導入を容易に。ソフトウェアのバージョンアップに伴う開発コストを低減。

ユースケース

■ 製造(工場)、流通、ビル等の分野のIoTシステムにおける機器の正常動作を監視



稼働中のIoT機器の軽量プログラム真贋判定

日本電気株式会社

技術内容

■ IoT機器におけるセキュリティ課題と研究開発の概要

- IoT機器のサイバー攻撃リスクが増しており、攻撃を受けると影響はシステム全体に波及
- IoT機器は性能面の制約からセキュリティ対策機能の導入が困難

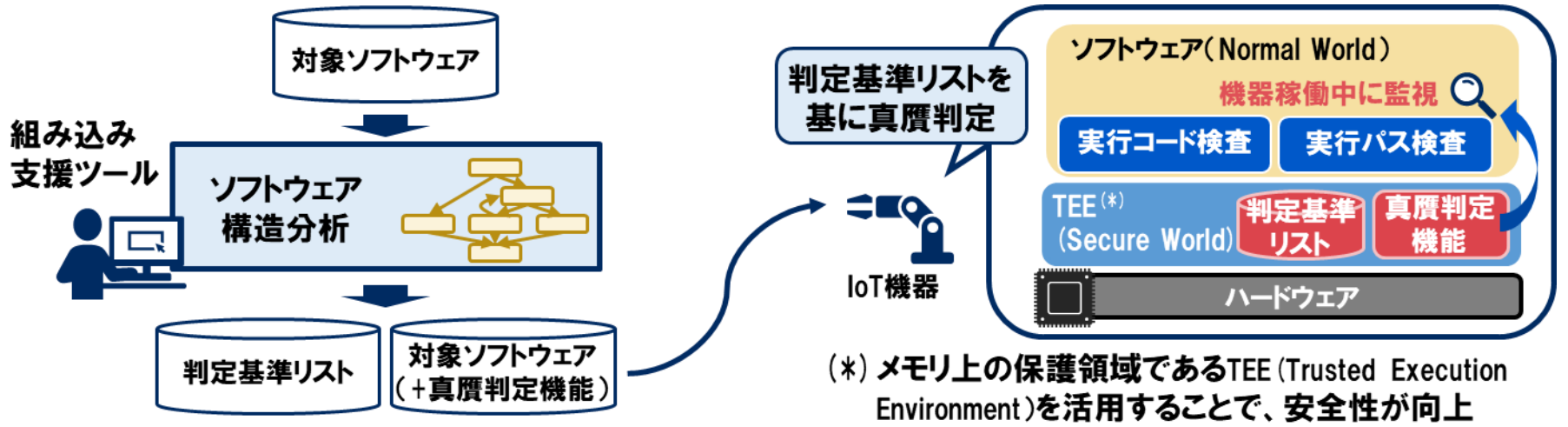
➡ IoT機器のソフトウェアに対する改ざんに着目し、機器の正常な状態（判定基準リスト）を基に、リアルタイムに監視を行う軽量な真贋判定技術を実現

開発フェーズ

判定基準リスト自動生成技術
対象ソフトウェアの構造を分析し、処理に基づいた検査タイミングの決定と判定基準リストの自動生成を実現

運用フェーズ

低負荷な真贋判定技術
メモリ上のプログラムの改ざんと実行順序（実行パス）の改ざんの有無を検査し、機器の正しい動作を監視

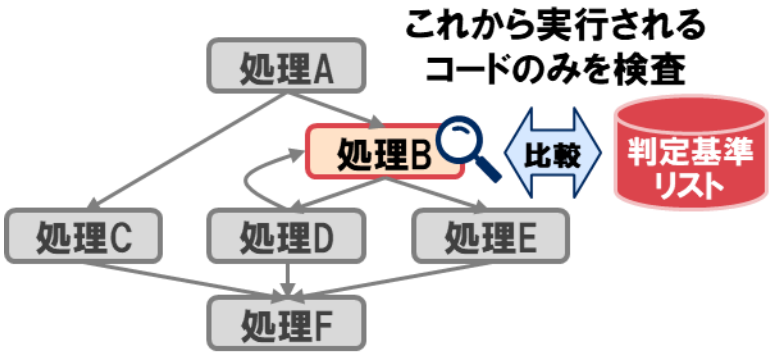


(*) メモリ上の保護領域であるTEE (Trusted Execution Environment)を活用することで、安全性が向上

■ 真贋判定対象

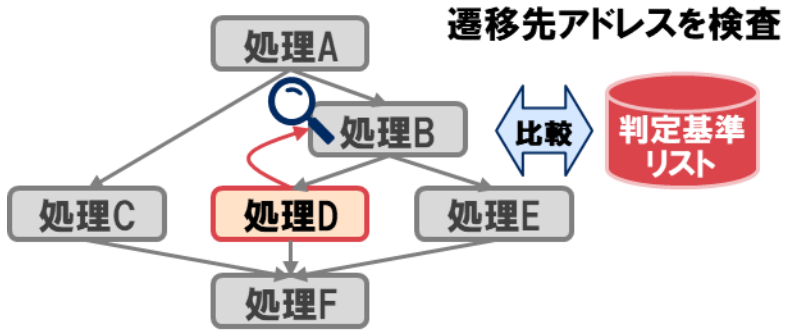
✓ 実行コードに対する真贋判定

- メモリ上に展開された実行コードを改ざんし、悪意のあるコードを組み込む攻撃を監視
- 処理順序に基づき、検査領域を限定することで、従来技術に比べ検査時間を短縮



✓ 実行パス（制御フロー）に対する真贋判定

- 処理の実行順序等を管理するメモリ領域を改ざんし、悪意のある処理に遷移させる攻撃を監視
- 処理の遷移先が起こり得ないアドレスでないかのみを検査することで、オーバヘッドを削減



問い合わせ先

日本電気株式会社
Email: nec-sip2-ac2@secl.jp.nec.com