⑤ 稼働中の機器の軽量型真贋判定

A
創出・証明

日本電気株式会社

性能やメモリ量に制約のあるIoT機器にも導入可能で、稼動中の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

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

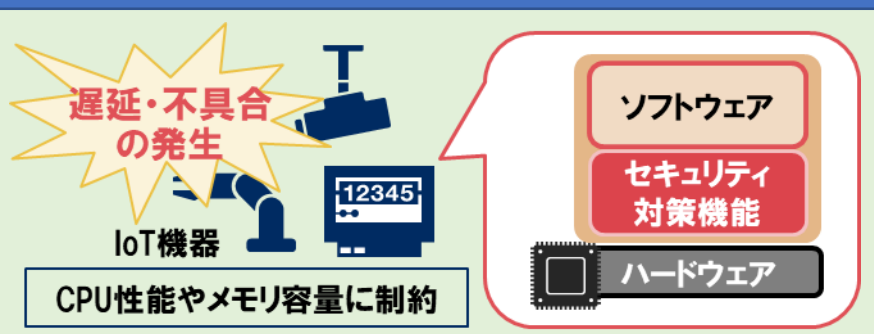
IoT機器の動作中にソフトウェアのプログラム自体の改ざんや処理順序の改ざんをリアルタイムに監視することで、長期間稼働し続けるIoT機器の安全性を向上。

■ 自動組み込みにより真贋判定機能の導入を支援

自動組み込みツールにより、対象IoT機器のソフトウェアへの真贋判定機能の導入を容易に。機器やソフトウェアのバージョンアップへの開発コストを低減。

IoT機器におけるセキュリティ対策の課題

課題：IoT機器本来の動作への影響懸念



対策すべきソフトウェア改ざんの主な攻撃手口
- メモリ上に展開されたプログラム自体の改ざん
- プログラムの実行順序の改ざん

課題：多種多様なIoT機器への導入コスト

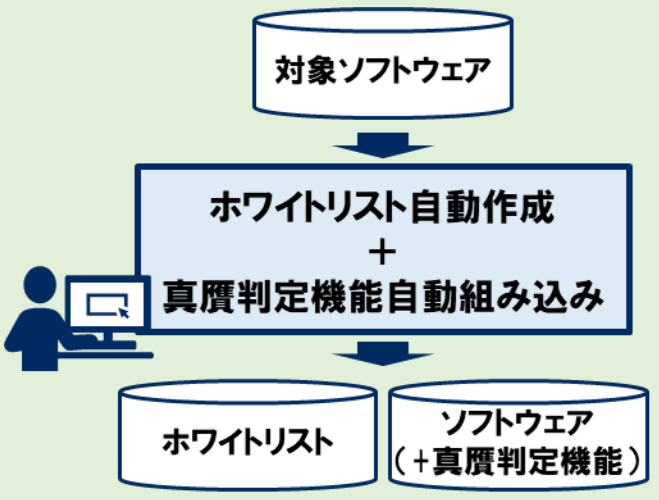
既存の真贋判定技術は、対象ソフトウェアに対応した判定基準（ホワイトリスト）が必要
（対象ソフトウェアのハッシュ値や、処理構造などを基に作成）

課題解決に向けた研究開発概要

開発フェーズ

ホワイトリスト生成技術

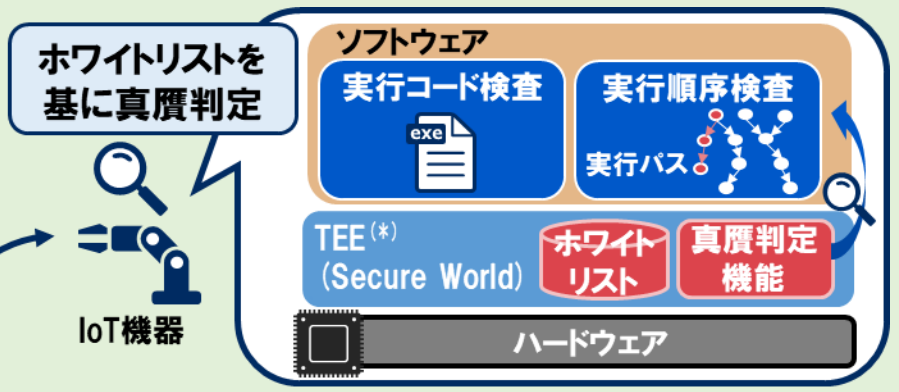
IoT機器の動作中に低負荷な検査を実現するホワイトリストを自動生成し、真贋判定機能も自動で組み込み



運用フェーズ

低負荷な真贋判定技術

プログラム本体の改ざんに加え、実行順序（実行パス）の改ざんも低負荷に監視し、真贋判定精度を向上



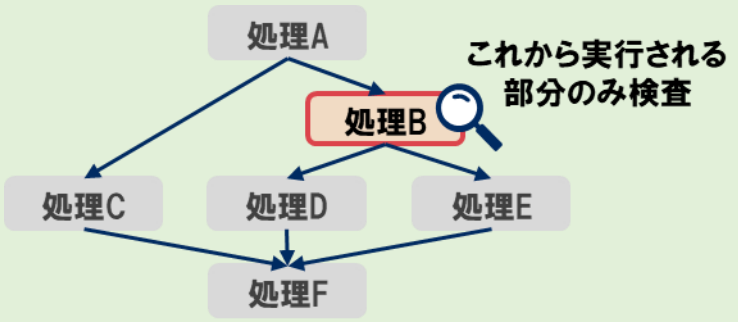
(*) メモリ上の保護領域であるTEE (Trusted Execution Environment)を活用した軽量実装

技術のポイント

高速性　ソフトウェアの構造に基づく検査範囲とシンプルな判定処理で負荷を削減

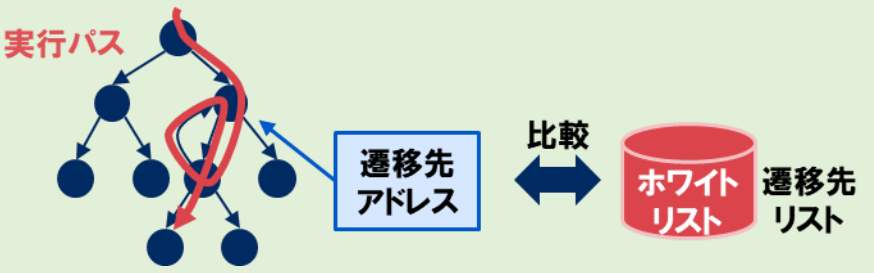
■ 実行コードに対する真贋判定

- 従来技術は、検査対象の実行コード全体/一部を定期的に検査するため、検査時間が課題
- 本技術は、実行コードの処理順序を考慮した限定的な検査領域により、検査時間を短縮

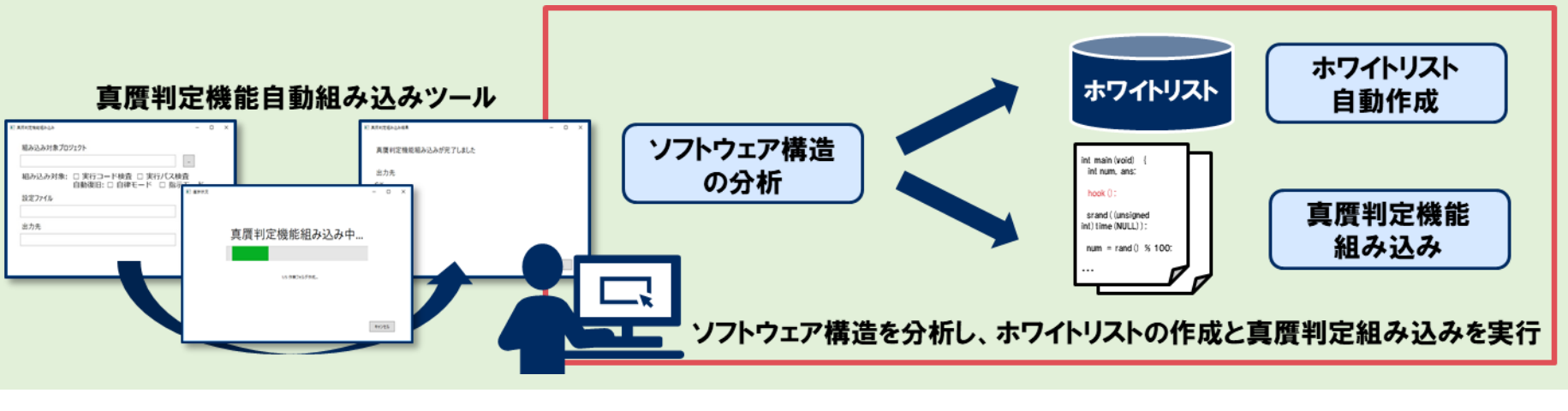


■ 実行パスに対する真贋判定

- 従来技術は、処理順序を管理するメモリ領域を複製する等により、オーバヘッドが大きな課題
- 本技術は、処理上問題ないと想定される遷移先（ホワイトリスト）を基に検査し、オーバヘッド削減

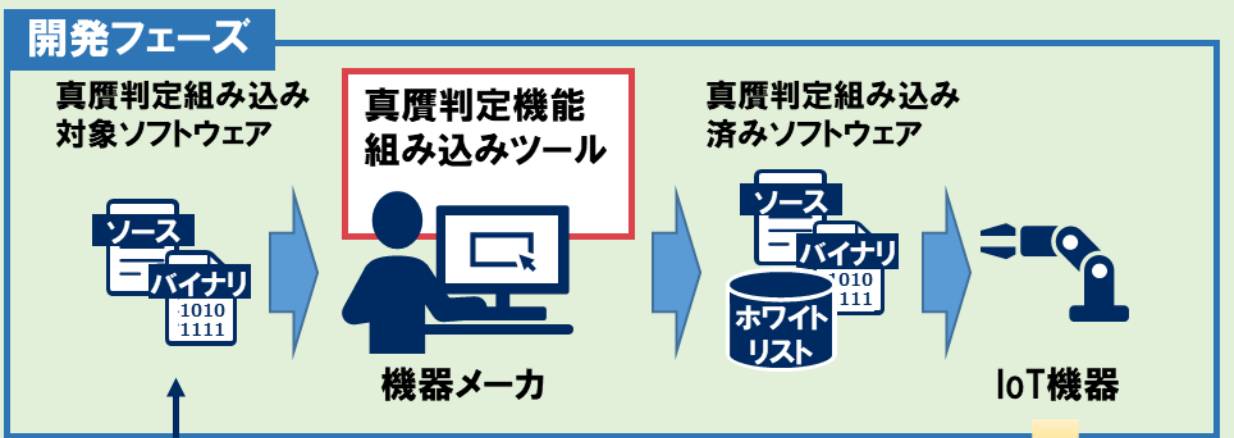


導入容易性　ソフトウェアを分析し、当該ソフトウェアに適した判定処理を自動組み込み



利用シーン

製造、流通、ビル等のシステム向けIoT機器への導入支援、及びIoT機器の安全な運用を実現

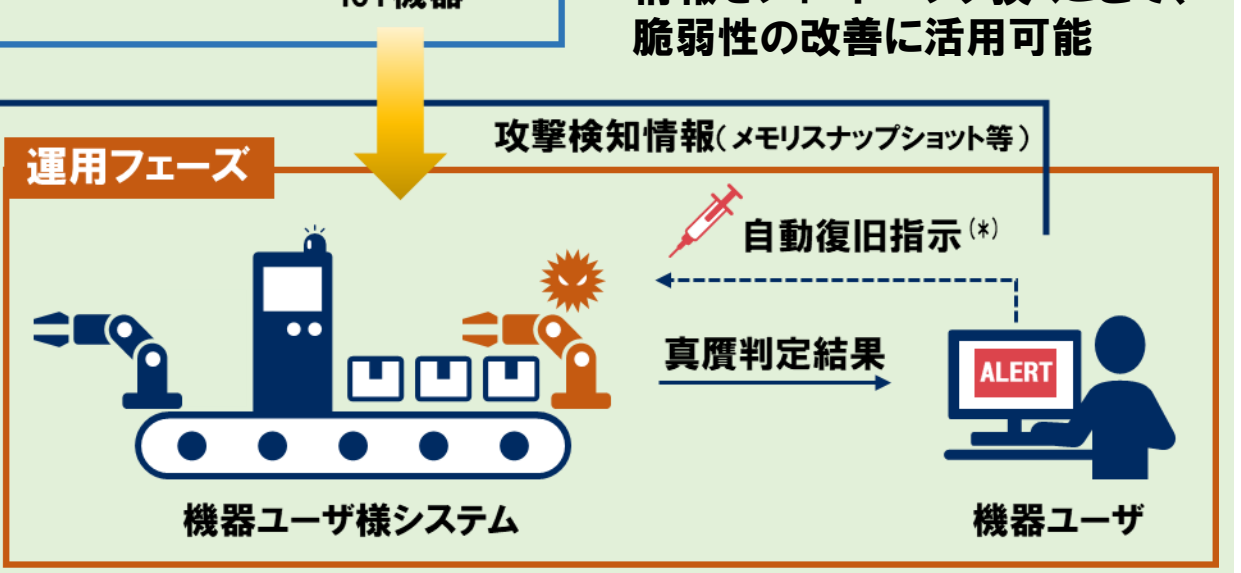


機器メーカ

- 自動組み込みツールにより、対象IoT機器への真贋判定機能の組み込みを支援
- 提供機器に改ざんが発生した場合、機器ユーザから攻撃検知情報をフィードバック頂くことで、脆弱性の改善に活用可能

機器ユーザ

- 真贋判定機能により改ざんを検知するとリモートの管理サーバがアラートを受信
- 真贋判定機能が搭載されたIoT機器をご利用頂くことで、機器の安全性を確認可能



(*) 改ざんされた実行コードの復旧機能についても研究開発中