⑦ サイバー・フィジカル異常検知

C
検証・維持

日本電信電話株式会社、三菱電機株式会社

**サイバー・フィジカル・システム向けの高度な監視技術と初動対応支援によって
サイバー攻撃による回復困難な被害発生を未然に回避**

技術の特長

■ **空間的・時間的に漏れのない監視を実現する「即時監視」**
システム構成を常時監視し、構成変更に伴う監視の空白期間を最小化

■ **攻撃の兆候も含めた異常通信を検出する「即時検知」**
機械学習を用いた検知技術により多様な制御プロトコルに対して兆候を含め攻撃を検知

■ **未知の攻撃に対しても原因を推定する「即時支援」**
検知情報と様々なシステム情報（機器の定常通信パターン・作業計画等）を活用することによって、異常原因を推定し初動対応を支援

課題解決に向けた研究開発技術の概要

サイバー・フィジカル・システム（CPS）に対するサイバー攻撃による脅威は年々高まっており、物理的被害も実際に発生しています。サイバー空間からの攻撃で、大きな物理的被害を発生させることを特徴とするこの脅威には、即時の対処が鍵となります。

【複雑な防御対象】
システムを構成する多種多様な機器と動的に変化するCPS構成

【攻撃の進化】
システムの多様化と監視のわずかな隙を突いた高度な攻撃

【マルチドメイン】
ITとOTの融合によるインシデント対応の複雑化

監視空白期間を生まない監視

システム構成監視技術と高速・高精度な通信監視技術により、構成変更時の監視開始までの時間短縮と検知精度を両立。

独自プロトコルにも対応可能な異常検知

AIによりプロトコルに依存しない通信パターンを学習し、攻撃を兆候も含め検知。独自プロトコルにも対応が可能。

原因推定による初動対応支援

検知情報から異常箇所を特定し、さらにシステム情報と照合することで考えられる発生原因を推定。

導入イメージ

設備への導入

- ネットワーク機器のミラー設定によりセンサ装置がシステム内の情報を収集
- センサ装置が機器を自動検出後、直ちに監視を開始

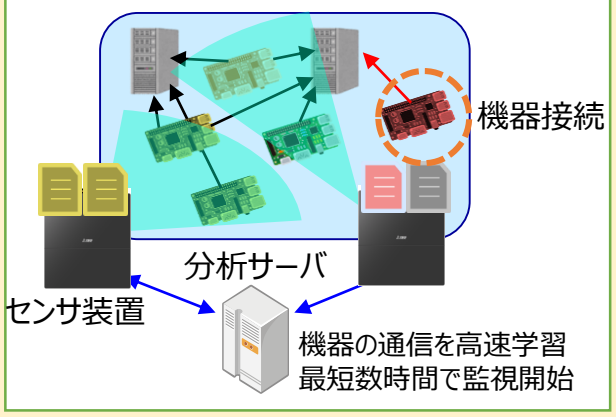
システム監視

- センサが収集した情報を用いた遠隔監視サービスを提供
- 監視に必要な人・物・時間をサービスとして提供

研究開発技術

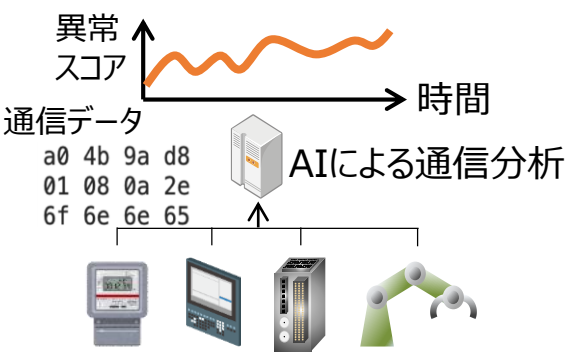
即時監視による漏れのない監視

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



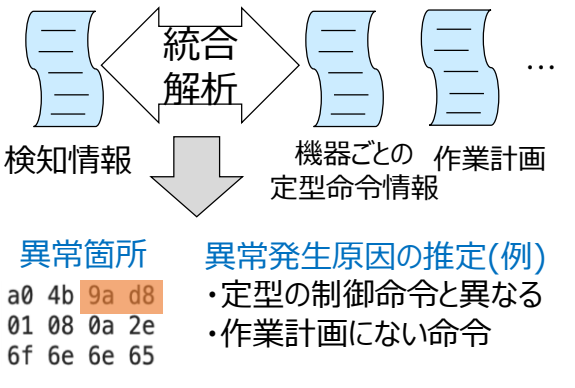
即時検知による通信異常検知

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



開発計画

監視開始までの時間の短縮、監視対象プロトコルの拡大、原因推定技術の分析精度向上により空間的・時間的に漏れのない監視と異常時の初動対応時間の大幅削減を目指す

2020年度	2021年度	2022年度	2023年度～
実験STEP1	実験STEP2	実験STEP3	
研究開発			実用化・商用化

問い合わせ先：
日本電信電話株式会社
NTTセキュアプラットフォーム研究所 E-mail: scpflab@hco.ntt.co.jp
三菱電機株式会社 E-mail: xs5n02@nh.MitsubishiElectric.co.jp