⑦ サイバー・フィジカル異常検知

日本電信電話株式会社、 三菱電機株式会社

適用領域

IoT　ICTベンダー
製造　インフラ　流通
自治体行政　ビル・スマートシティ

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

■ **多数の制御プロトコルをその場の使い方に合わせて詳細に監視**
多数存在するOT分野の制御プロトコルの大部分に対し、監視対象システム個々でのプロトコルの使われ方の違いも踏まえた、きめ細やかな監視を実現

■ **独自プロトコルも対象に、未知も含むセキュリティ異常を迅速に検知**
独自仕様のプロトコルであっても、通信の特徴を自動的に学習し対応

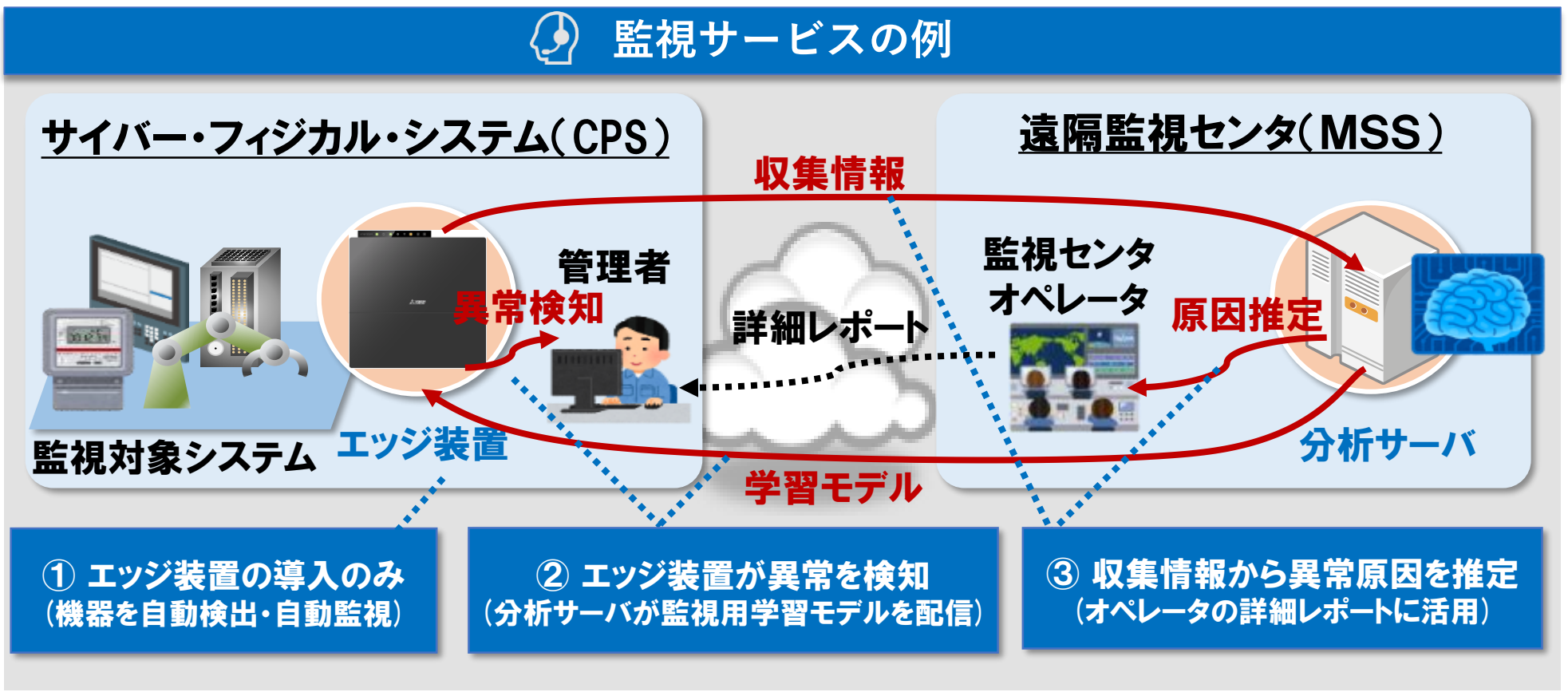
導入効果

■ **漏れなく迅速に異常・兆候を検知することで、運用者による先回りとなる素早い対応を可能とし、監視対象システムの継続的運用を支援**

■ **サイバー攻撃による回復困難な被害発生を未然に回避**

ユースケース

■ **オンプレ設置・自社運用から、監視サービスとしての利用まで、様々な導入・運用形態に対応**

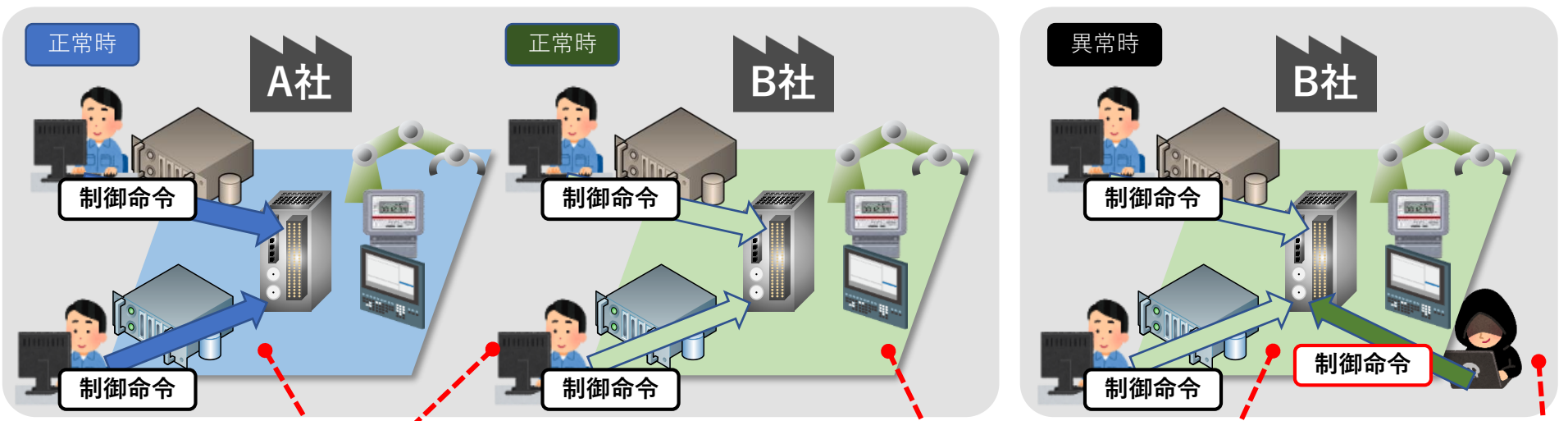


⑦ サイバー・フィジカル異常検知

日本電信電話株式会社、三菱電機株式会社

技術内容

多種多様な制御プロトコルに対し、監視対象システム個々の正常の基準を自動把握し、制御命令や設定値のわずかな違いも異常として迅速に検知できるアノマリ監視技術



同じシステムでもA社とB社では、正常/異常の定義は異なる

B社固有の制御命令や設定値に対し、わずかな違いの発見が求められる

攻撃に対し迅速さが鍵

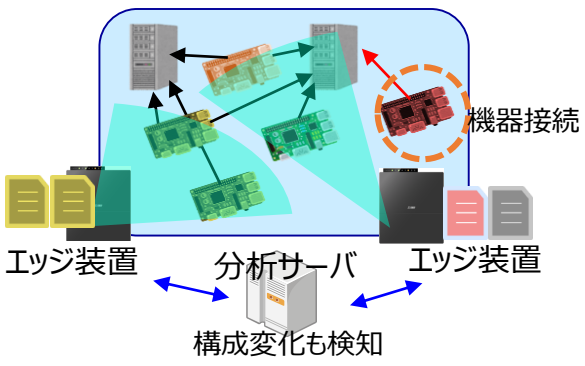
システム個々の正常基準を定義でき、詳細かつ迅速な監視手段の実現が課題

本課題の解決技術

「多種多様な制御プロトコルへの対応」と「即時性」を両立する技術

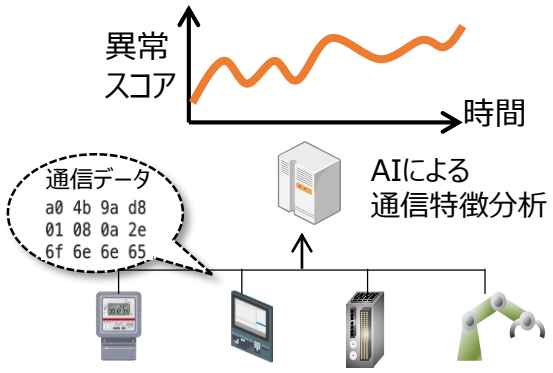
即時監視

通信の監視で構成変化も即座に検知、CPSに特有なバースト的通信でも分析性能を犠牲にしないエッジ処理



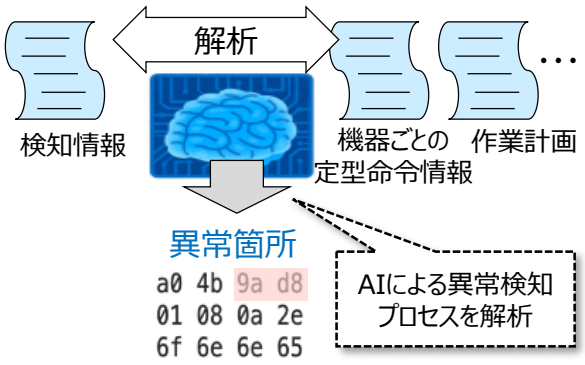
即時検知

通信特徴を自動学習することによって、独自仕様も含む多種多様なCPSプロトコルに対応



即時支援

異常検知のきっかけとなったパケット内の異常箇所を自動特定し、発生原因を推定



問い合わせ先

日本電信電話株式会社　社会情報研究所　Email: solab@hco.ntt.co.jp
三菱電機株式会社　Email: xs5n02@nh.mitsubishielectric.co.jp