戦略的イノベーション創造プログラム（SIP）

【日立製作所】

1－3　侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化

動作監視解析技術

可用性が重視される制御システムにおいて気づきが難しい不正な動作を早期に検知します

特長　微細な挙動変化を監視、システムの免疫力を強化

① 正常業務に紛れた不正な動作を検知します

既存の技術で検知しにくい不正な動作であっても、制御システムで発生した小さな変化をとらえ、検知します（統合健全性判定技術）。

② 制御システムの特性に適した監視を行います

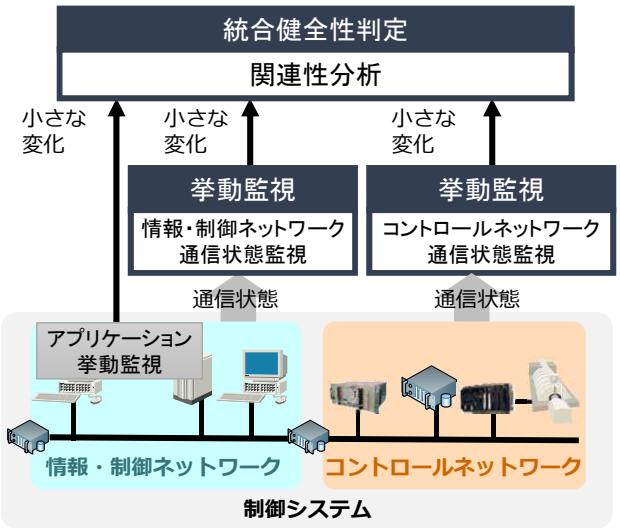
通信状態から制御システムの特性を学習、モデル化し監視することで小さな変化を検知します（挙動監視技術）。可用性が重視されるシステムに対しても、影響を最小限に導入可能です。

現在の重要インフラシステムでの課題

近年未知のウイルスが次々と生み出されるとともに、侵入方法も巧妙化しているため、侵入防御・攻撃防御技術だけで、すべての侵入を防ぐことは難しくなっています。また、外部ネットワークに直接つながっていない制御システムにおいても、侵入・攻撃リスクは高まっています。そのため、万一侵入された場合に備え、制御システムに適した侵入・攻撃検知技術が必要とされています。

課題を解決する技術

統合健全性判定技術



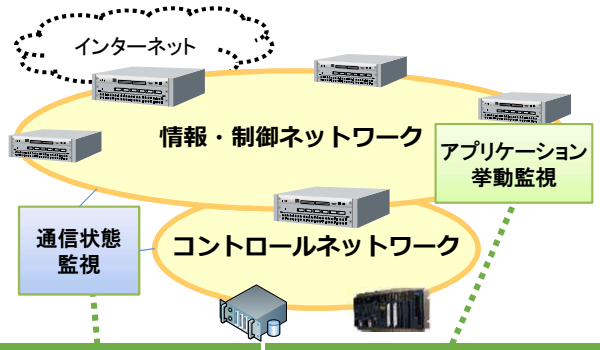
小さな変化を使って不正な動作を統合判定

小さな変化の関連性を分析することで、単一の変化だけでは見逃してしまう不正な動作を浮き彫りにしたり、過度な不正判定を抑制したりします。

挙動監視技術

制御システムに適応

制御システムの特性に応じて正常状態を学習しモデル化します。適用先に応じて通信状態監視・アプリケーション挙動監視を選択可能です。



通信状態監視

通信状態をリアルタイムに監視し、モデルと比較して、小さな変化を検知します。

アプリケーション挙動監視

通信状態に現れない機器内の活動をとらえ、小さな変化を検知します。

実施状況/スケジュール

重要インフラ事業者と協働した検証を2017年度末に実施しており、先行して研究開発が完了した技術に関して2017年度に製品化済みです。（製品：Hitachi Anomaly Detector）
製品化後も引き続き連携した活動を実施しており、現在実施中の研究成果も今後製品化予定です。

【日立製作所】

戦略的イノベーション創造プログラム（SIP）

1－3　侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化

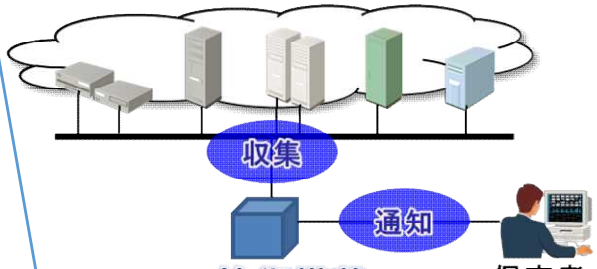
先行して研究開発が完了した技術を製品化　－ Hitachi Anomaly Detector －

SIPサイバー先行研究開発技術　多層監査膜

業務をホワイト化した複数の監査アルゴリズムを多層化

日立が長年積み上げてきた制御システムに対するノウハウを生かし、多角的な視点で業務をホワイト化

新旧機器が混在するシステム



セキュリティ監視製品
Hitachi Anomaly Detector

<特長> ① 業務に着目したアルゴリズムにより、未知の脅威をリアルタイムに検知
② 業務通信を分析し、正常な業務通信を"ゼロ"から自動で学習
③ システムに接続された機器の型やOSのバージョン等に依存せず導入可能

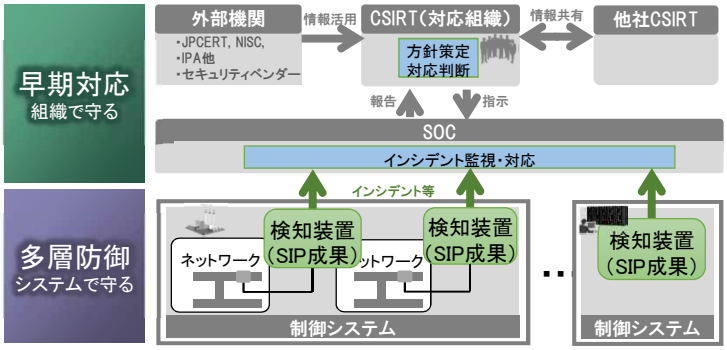
システムの安全稼働を守る

研究開発技術の適用方法

フェーズごとのガイドライン

- 設計
- 構築(確認)
- 構築(事前準備)
- 構築(導入)
- 運用

セキュリティシステム設計／構築方法や組織体制、運用設計等のポイントを解説

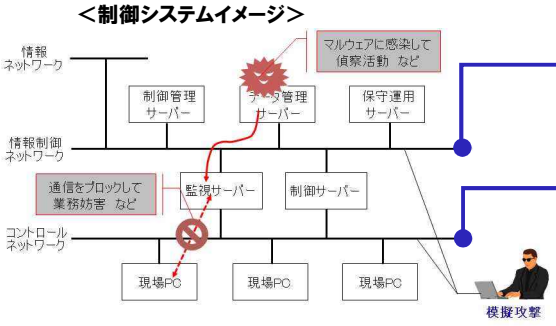


・現場の制御システムに検知装置を配置し、微細な変化を漏らさずインシデントとして検出
・SOC2) で各種インシデントを監視、統合的に判断して早期対応

展示概要

○検知装置で検知したインシデントの表示や運用方法を体感してください。

＜制御システムイメージ＞



＜検知装置構成例＞

① 模擬攻撃を実施

② 検知された模擬攻撃が運用画面に表示され、運用者視点でのオペレーションを実施

1) OT：Operational Technology
2) SOC：Security Operation Center