⑨ サイバー・フィジカル空間をまたがって流れる不正なデータの検知・対処

C
検証・維持

株式会社 日立製作所

IoTシステムにおける不正データに対して、一次対処にかかる時間を短縮し、
セキュリティ事故影響を低減

技術の特長

■多種多様な各IoTシステムの特性に応じた不正データ検知を実現
システム特性データを用いて不正データ検知の誤検知/見逃しリスクを低減

■サービス継続に適切な一次対処を自動実施
システムに合わせて柔軟かつ安全性の高い一次対処を自動実行する
不正データ対処技術により、サービスの可用性を改善

IoT:Internet of Things

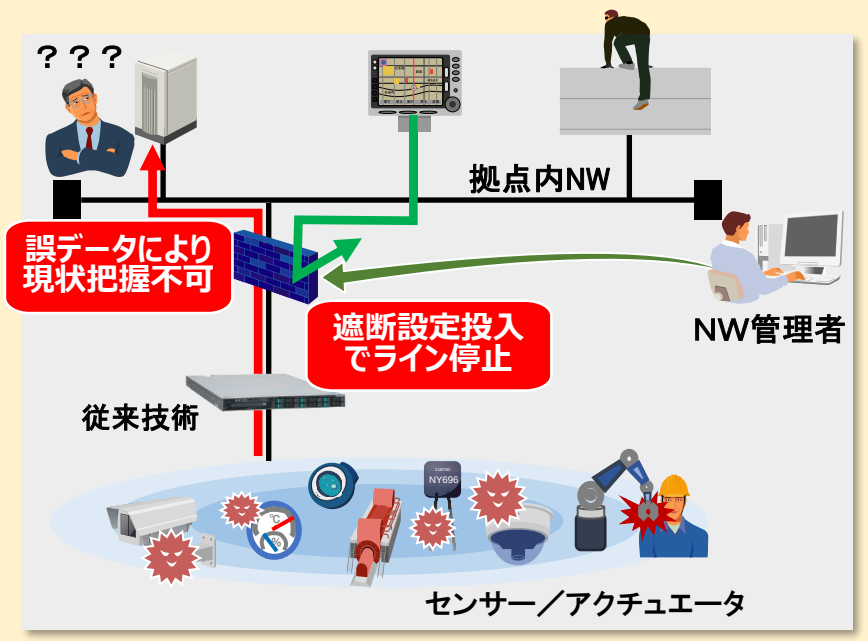
IoTシステムにおける課題と、本技術の特長

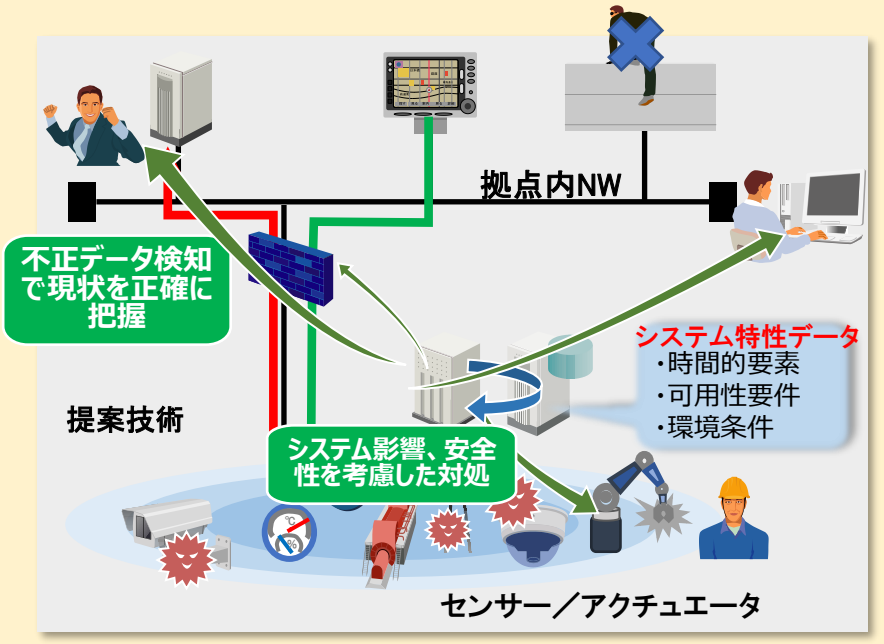
検知 IoTデータの多様化で従来技術ではデータ改ざん検知困難

対処 NW/現場の分担制約で本来必要な一次対処を迅速に実行できない

検知 システム特性を用いた不正データ検知で誤検知/見逃しリスク低減

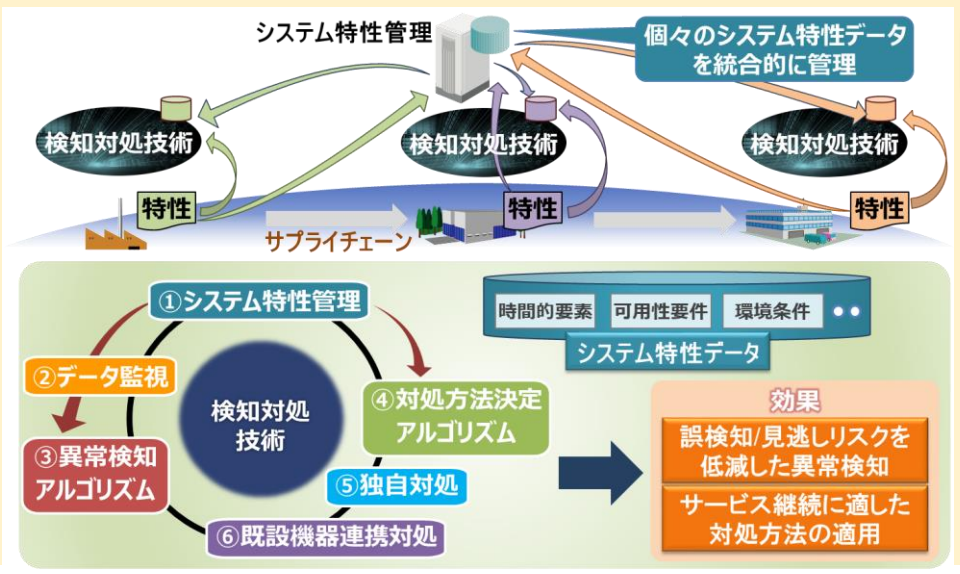
対処 現場で設定した安全性の高い一次対処を自動実行し、サービス可用性改善





NW:ネットワーク

課題解決のための研究開発技術概要

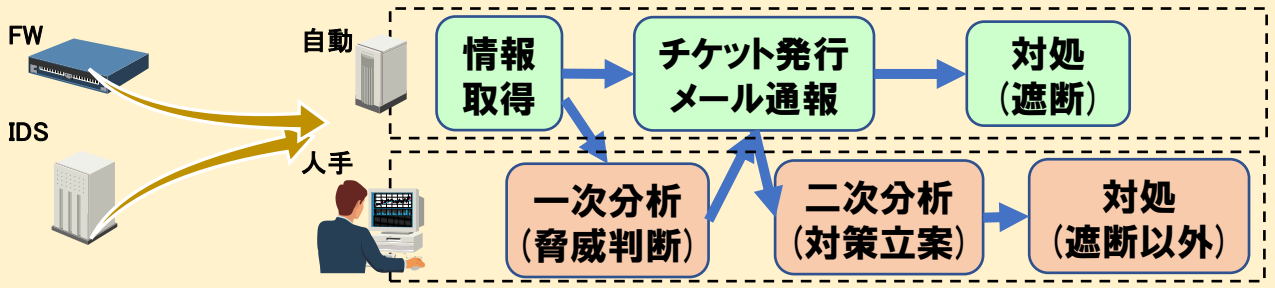


IoTシステム特性情報の活用

(1) IoTシステム特性情報を集約管理
(2) システム特性情報を異常検知・対処アルゴリズムに活用
(3) セキュリティと安全両面の侵害度を加味した一次対処判定

既存技術との比較

■従来の検知/対処技術例:SIEM/SOAR

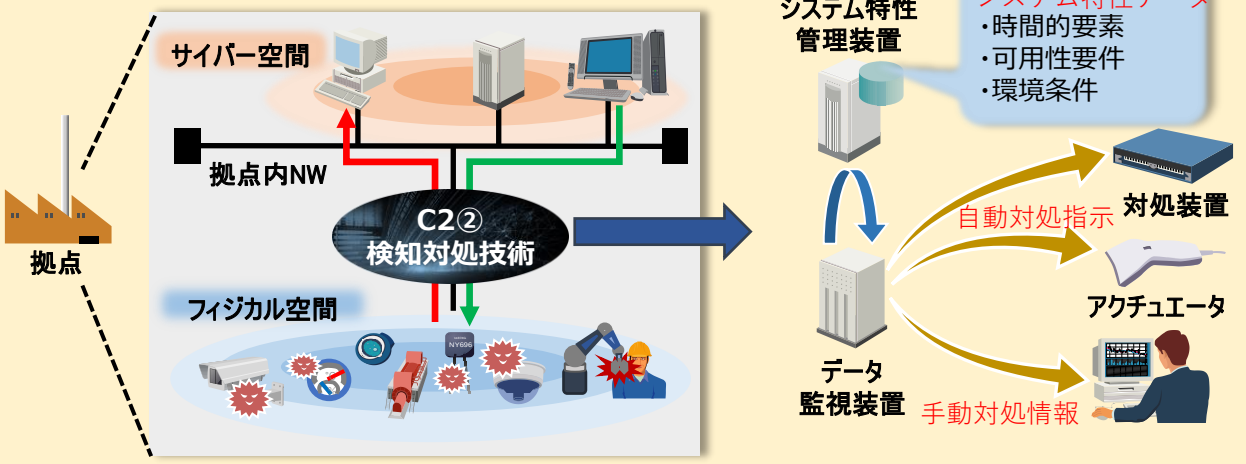


セキュリティ検知はFW/IDS/各種センサーに依存、現場ごとの特性を考慮しない検知

SIRTでのチケット・メール発行などを自動化。現場自動対処はほぼ遮断(隔離)のみ

■ 全体としてのMTTRは削減されるが、一次対処できる内容は限定される

■今回研究の検知/対処技術



システム特性データを活用した誤検知/見逃しリスクの低い不正データ検知

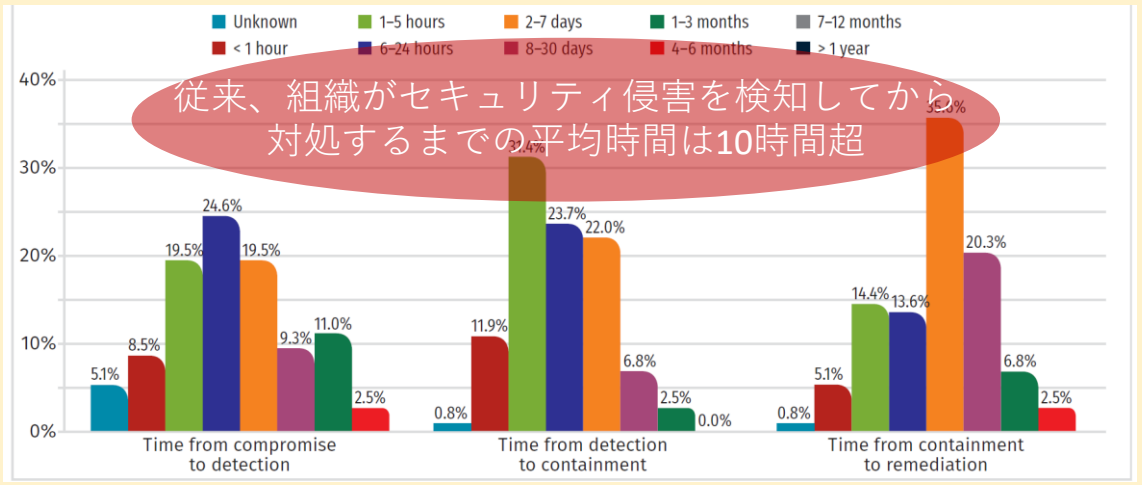
現場で可用性/安全性を考慮した自動一次対処を設定して、システム稼働率改善

■ 一次対処の迅速化により、システムとしての停止時間を大幅に低減

SIEM: Security Information and Event Management SOAR: Security Orchestration, Automation and Response
SIRT: security incident response team FW: FireWall IDS: Intrusion Detection System MTTR: Mean Time To Repairs

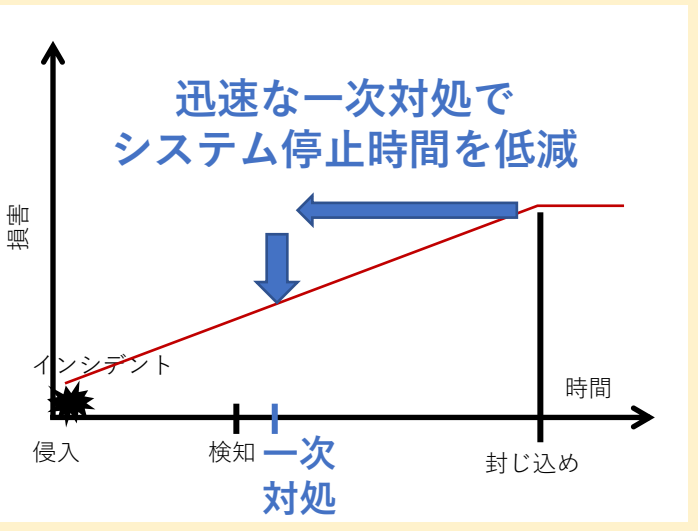
ベンチマーク

現場における一次対処比率を上げることで対処時間を低減し セキュリティ侵害に起因するシステム停止時間の大幅改善をめざす



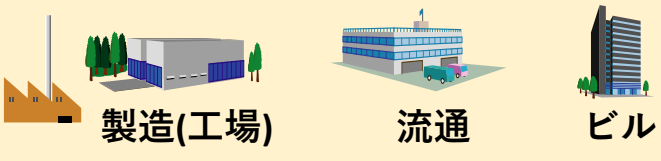
従来、組織がセキュリティ侵害を検知してから、対処するまでの平均時間は10時間超

出典: SANS 2019 Incident Response (IR) Survey: It's Time for a Change
Figure 2. Compromise to Remediation Times1



SANS: SysAdmin, Audit, Network, Security

利用産業と利用シーン



製造(工場)、流通、ビル等、さまざまな分野で稼働中のIoTシステムにおいて、既設のシステムに手を加えることなく、セキュリティ監視に適用可能

期待される効果

- IoTシステムの可用性向上
- セキュリティ対策の早期適用
- サプライチェーンの信頼性の維持