8. サイバー攻撃発生時の影響評価及び対処策実行支援

日本電気株式会社

セキュリティ専門家でなくてもシステムのリスク診断が可能
攻撃シミュレーションに基づいた対処策案を自動で提案

適用領域

半導体・実装 / 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

技術の特長

■ 攻撃シミュレーションを用いてシステムのリスク診断を自動化

実システムに影響を与えずにサイバー攻撃リスクの網羅的な診断を実施することが可能
リスク診断結果をIPA「制御システムのセキュリティリスク分析ガイド」の結果に変換して提示

■ サイバー攻撃に対する対処策案を提示

攻撃シミュレーションを用いてサイバー攻撃に対する対処策案とその有効性を自動で評価
対処策の有効性を容易に把握できるようになり、運用者の対処策決定・実行を支援

導入効果

■ セキュリティの知識が無くともリスク診断を短時間で実施

攻撃シミュレーションによりシステムへのサイバー攻撃やその対策を自動評価することで専門的な知識が不要。リスク診断に要する時間を従来と比較して約1/4時間に削減可能

■ セキュリティガイドラインで推奨されるリスクアセスメントを容易に実施

診断対象システムの資産（端末のOS、インストールソフトウェア）の情報及びネットワーク構成が把握できていれば、攻撃シミュレーションを実施可能（*分析精度向上には追加情報が必要）

ユースケース

対象

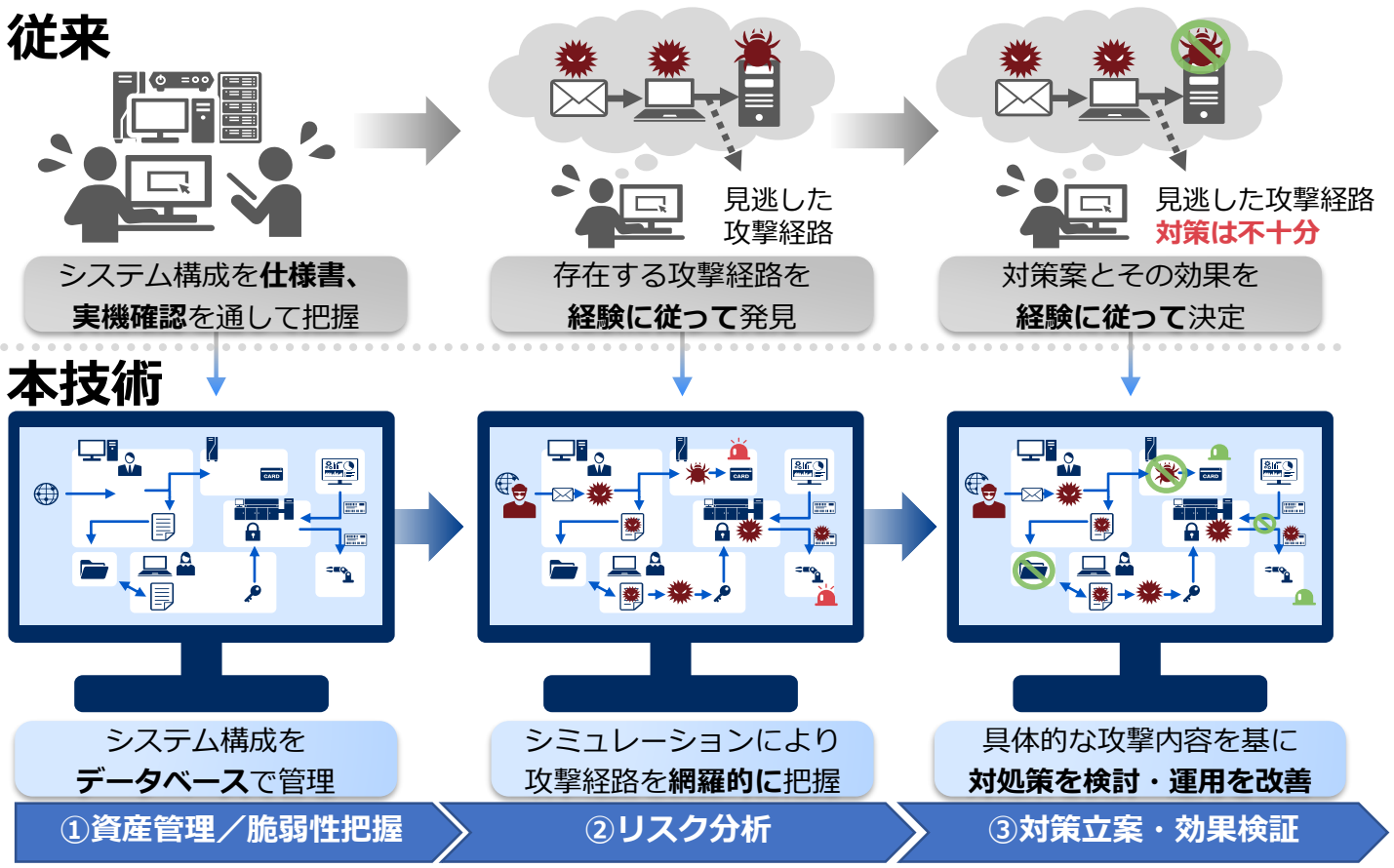
製造（工場）、流通、ビル等の分野のOT/IoTシステム

利用シーン

日常的にIoTシステムのサイバー攻撃リスクを診断、対処を検討

必要な情報

機器毎のOS、インストールソフトウェア、ネットワーク構成など

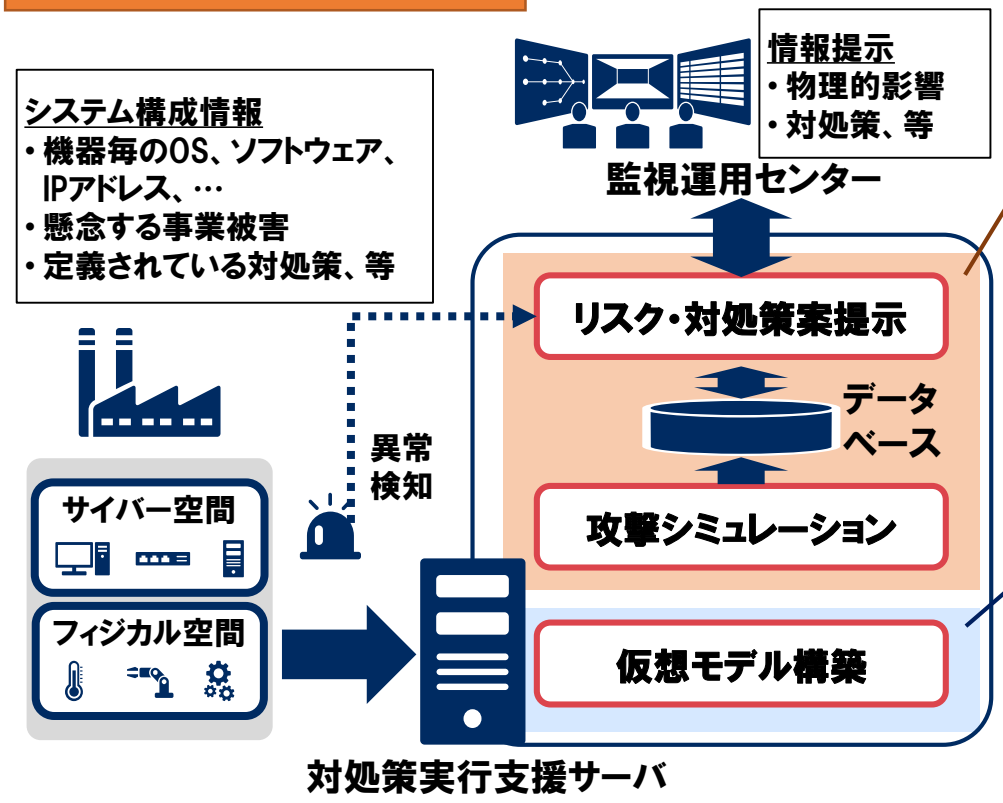


8. サイバー攻撃発生時の影響評価及び対処策実行支援

日本電気株式会社

技術内容

研究開発技術の概要



■ **対処策実行支援技術**
仮想モデル上で攻撃シミュレーションを実施することで、サイバー攻撃の影響や対処策の有効性を評価。実システムで異常が検知されれば、評価した結果を基に対処策案を運用者に提示

■ **仮想モデル構築技術**
実システムを用いずにサイバー攻撃リスクを分析するための仮想モデルを構築

解決する課題

■ **各種ガイドラインではリスクアセスメントを推奨**し、その結果に基づいて対策することを提案している

製造工場・ビルを構成する機器は、数百～数千台も存在するため、リスクアセスメントの実施は難しい

人手でのシステム検査は、時間と工数を要する

既存ツールでは、システムの被害はわからない

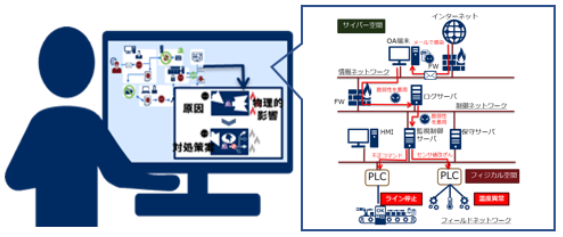
大規模環境への対応

被害の分かり易さ

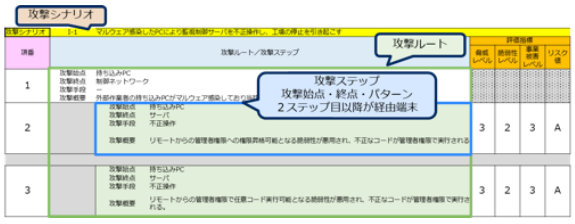
■ **C2③では、リスクアセスメントの運用者の負荷の低減**を目指しセキュリティへの対処を支援

どの環境でも適応可能にするため数千台規模に対応し、システムの被害を誰もが容易に把握可能にする

数千台規模の攻撃シミュレーション



ガイドラインに則った分析レポート



問い合わせ先

日本電気株式会社
Email: nec-sip2-ac2@secl.jp.nec.com