⑧サイバー攻撃発生時の影響評価及び対処策実行支援

C
検証・維持

日本電気株式会社

サイバー攻撃を模擬した攻撃シミュレーションによってリスクアセスメントの自動化及びサイバー攻撃発生時の対処策案の検討を容易にし、サイバー攻撃発生時の対処策実行を支援します

技術の特長

■サイバー攻撃の影響を可視化

サイバー攻撃が引き起こす可能性のあるシステムや機器への影響を攻撃シミュレーションを用いることで分析。セキュリティ知識がなくても、運用者はサイバー攻撃リスクを把握可能

■リスクアセスメントを自動化

攻撃シミュレーションの結果をガイドライン*形式に変換。運用者のガイドライン対応を支援

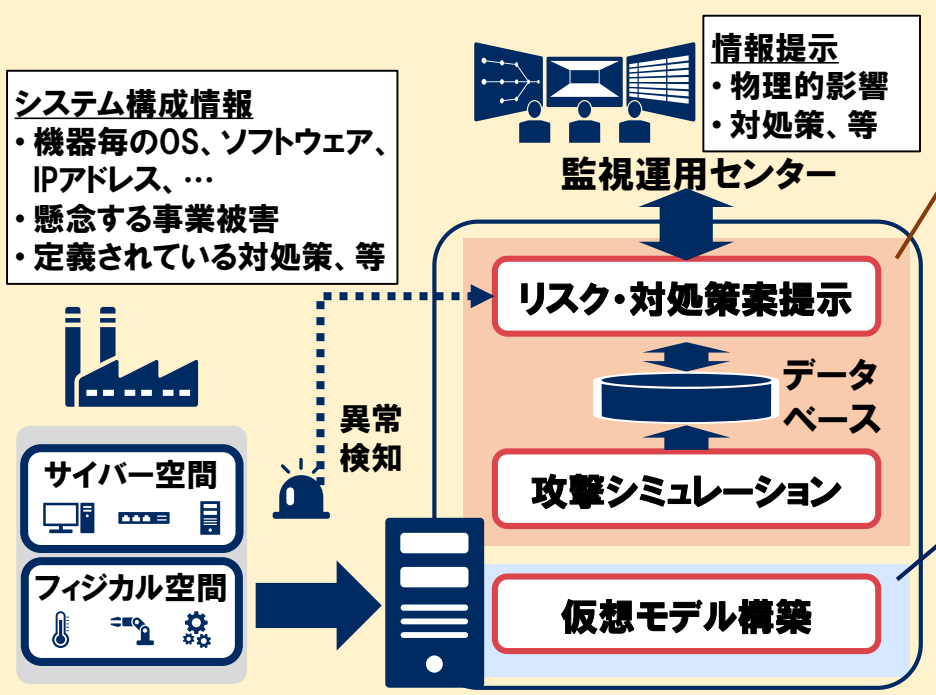
＊)IPA「制御システムのセキュリティリスク分析ガイド」

■サイバー攻撃に対する対処策案を提示

サイバー攻撃リスクに対する対処策案も攻撃シミュレーションを用いて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

サイバー攻撃対策の課題

課題解決のための研究開発技術概要



■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

技術のポイント

従来

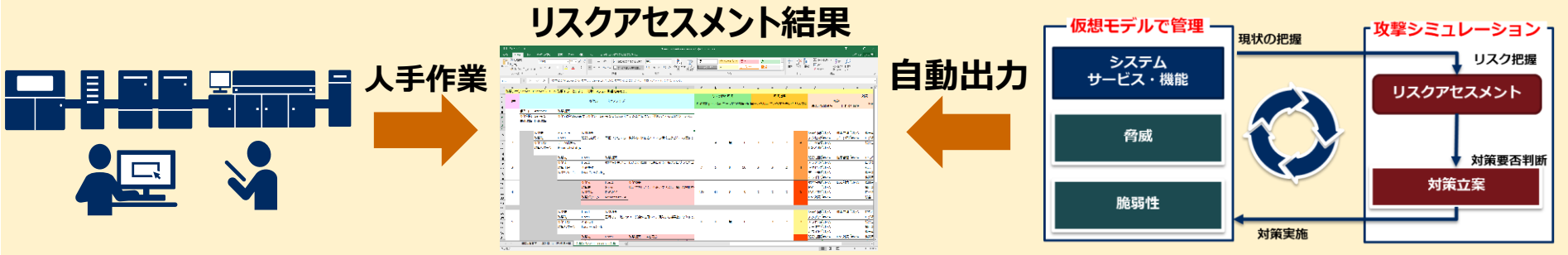
■実施者の能力によってリスク分析結果が異なる

人手でリスク分析を実施し発生し得るサイバー攻撃を検討。リスク分析結果に基づき対策を検討

本技術

■実施者の能力に依存せずに一様なリスク分析結果を実現

診断対象システムに発生し得るサイバー攻撃をシミュレーションにより探索。リスク分析結果及び対策案を自動で提示



利用シーン

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

①リスクアセスメント

日常的にOT/IoTシステムのサイバー攻撃リスクを診断、対処を実施

②サイバー攻撃発生時

サイバー攻撃発生時に、異常情報と攻撃シミュレーション結果を基に対処を実施

必要な情報

・サイバー側の分析

機器毎のOS、インストールソフトウェア、IPアドレス情報

・フィジカル側の分析

PLCプログラム、配管計装図