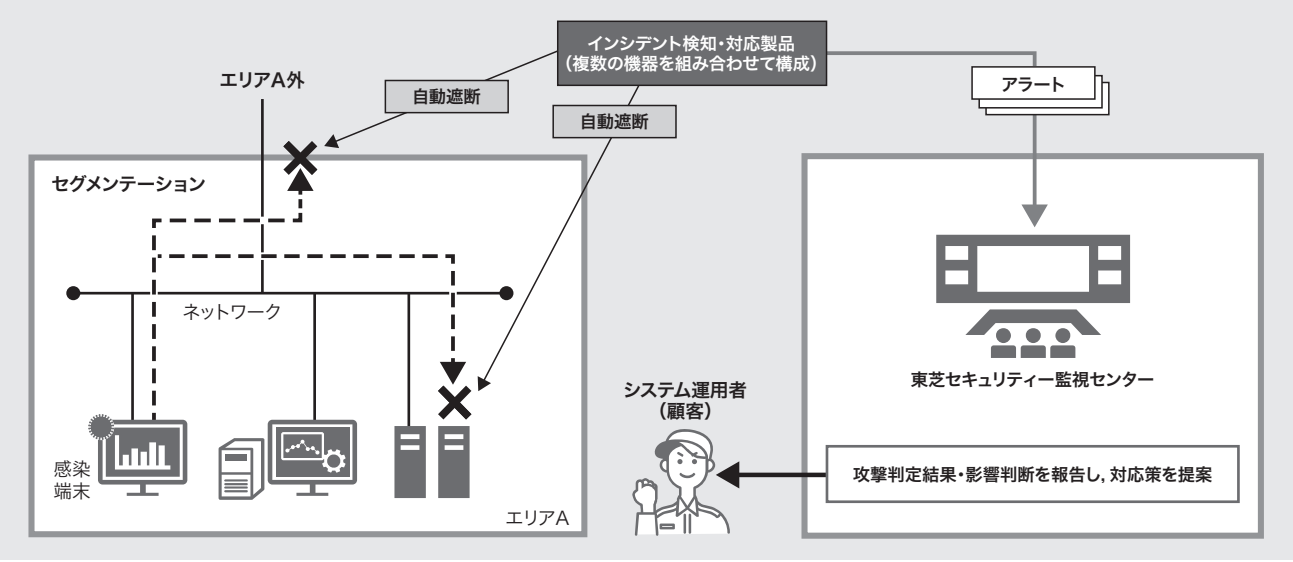
社会インフラ・製造システムのサイバーレジリエンスを強化する攻撃検証・監視運用技術

Attack Emulation and Monitoring Operation Technologies for Enhancing Cyber Resilience of Social Infrastructure and Manufacturing Systems



顧客の制御システム運用におけるセグメンテーションと検知・自動遮断及び監視運用連携によるインシデント対応支援

Outline of security support service for customer's control system providing incident response through network segmentation, and incident detection and automatic isolation functions in conjunction with remote operation center

近年, 国内では制御システムが持つ防御機能を巧みに回避するランサムウェアにより, 製造業が製品の出荷停止に追い込まれる事案(インシデント)が発生している。海外では, AIを悪用した高度なサイバー攻撃が電力・ガス・水道などの重要インフラに及びつつあり, 産業や国民生活への影響が懸念されている。

こうした状況の中, 政府は2025年5月にサイバー対処能力強化法を成立させた。これは, 重要インフラを運用する特定社会基盤事業者(以下, 重要インフラ事業者)に対し, インシデント発生時だけでなく, その兆候を把握した場合にも, 攻撃痕跡を政府に報告する義務を課している。また, 重要インフラ事業者に製品を提供するベンダーにも, "セキュリティ要件適合評価及びラベリング制度(JC-STAR)"などの公的認定要件を満たす製品の提供に加え, 重要インフラ事業者と連携したセキュリティー確保が求められている。

東芝は, これに先立ってPLC(Programmable Logic Controller)などの自社製品を含むシステム検証環境を構築するとともに, 模擬攻撃を実施できるホワイトハッカー人材を社内で育成し, この環境を利用した最新の脅威動向に基づく出荷前検証を, 導入予定のインシデント検知・対応製品に対して実施している。また, 製品運用の段階では, 重要インフラ事業者・製造事業者向けに2020年から提供してきた監視運用サービスのノウハウを活用し, サイバー攻撃リスクの分析・判断を迅速化する取り組みを進めている。

研究開発においても, 当社事業領域を中心に収集した攻撃や脅威の知見と, 保守や停止リスクに関する制御システム特有の知見を活用し, インシデント発生時の影響を的確に評価し, 迅速に対応策を提案できる枠組みの確立を進めている。例えば, ランサムウェアの感染事案では, 1台でも感染すると影響が急速に拡大するおそれがある。そこで, 製造ラインにおいてネットワーク分離(セグメンテーション)を設計するとともに, 複数のインシデント検知・対応製品を組み合わせ, 感染端末の通信を自動で遮断することで, 他エリアへの二次感染を防止する仕組みを構築した。これにより, 工場への導入コストと監視運用の負担を抑えつつ, 製造停止リスクを大幅に低減できるようになった。

今後も, 攻撃耐性の高い製品の供給と監視運用サービスを通じて, 制御システムのレジリエンスを向上させていく。

小椋　直樹　OGURA Naoki
総合研究所 AIデジタルR&Dセンター セキュリティ基盤研究部