デジタル化する工場のサイバーセキュリティ(1)

工場(OT)環境の類型整理とOTセキュリティ

PwCコンサルティング合同会社 シニアマネージャー 上村 益永

はじめに

デジタル化が進む昨今、サイバー攻撃は企業活動の根幹を成すOT(Operational Technology:生産ラインやシステムの制御・運用技術)環境に及んでいます。日本国内においても工場をはじめとするOT環境でのサイバーセキュリティインシデント(以下、OTセキュリティインシデント)が発生していることは周知の通りです。PwCは、企業の存在意義すらも脅かすOTセキュリティインシデントおよびその発生を防止するOT環境におけるサイバーセキュリティ(以下、OTセキュリティ)を重要な経営課題と捉えています。本稿では、OT環境の類型化を通じて、OTセキュリティ管理の在り方の検討、および取り組みにおける留意点をお伝えします。

OT環境の類型整理

(ア)OT環境の大別

一般に、OT環境である工場や研究所では産業制御システム(ICS: Industrial Control System)が使用されていることから、OTのサイバーセキュリティは従来の情報セキュリティやITセキュリティとは別の取り組みとして考えられることが多いです。これまではTCP/IP(Transmission Control Protocol/Internet Protocol)の脆弱性を利用した情報システムへのサイバー攻撃が主流であったこと、情報管理やIT環境の所管部門とOT環境の所管部門が異なる企業が主流であることが、その主な理由です。

OT環境は、大別するとFA(Factory Automation)環境とPA(Process Automation)環境に分類できます。FAは、主に物理的な組み立て・加工などを行うプロセスを自動化することを目的としたシステムからなる環境です。一方、PA環境は、主に化学的な合成・精製などを行うプロセスを自動化することを目的としたシステムからなる環境です。

その他にもBA(Building Automation)や送電網、通信網など、ICSを使用したサービスシステムは多数ありますが、そうした環境はユーザーにサービスを直接提供するために使用されているなど、いわゆる工場や研究所といった企業内部の事業活動に使用される環境とは異なる性質を持つため、ここでは取り扱わないこととします。

なお、本稿はOTセキュリティに係る環境全体の類型化に焦点を当てる目的から、例外が多数存在することは認識した上で一般論に終始しています。

(イ)FA環境とPA環境の特徴と主な違い

OTセキュリティを大局的に考えると、全ての環境で可用性が最優先であるといった誤解や、構成変更が難しいことから技術的な対策は何もできないといった錯覚に陥ることがあります。しかし、実際のOT環境は個々に性質が異なり、OA(Office Automation)環境のように全体として1つの傾向を語ることは難しいと言えます。FA環境とPA環境に大別するだけでも、一般に下表(図1)のような違いがあります。

図1:OT環境の類型整理

カテゴリ	指標	参考)OA環境	FA環境	PA環境
機能や実状	構成変更の容易性	容易	比較的容易	困難
	要求される出力品質精度	低(ベストエフォート)	高	中
	規格	TCP/IP	TCP/IP+固有プロトコル	TCP/IP+固有プロトコル
	運用体制	IT部門で全社的に一元化	製造部門ごとに細かく分散	運用ベンダにて一定程度一元化
セキュリティ	守るべき対象	情報資産	プロセスおよびプロセスを担う設備	プロセスおよびプロセスを担う設備
	最優先されるセキュリティ要素	機密性	可用性	完全性
	セキュリティ侵害時の影響	データの損失	環境・安全・製品・設備の侵害	環境・安全・製品・設備の侵害

OTセキュリティにおける留意点

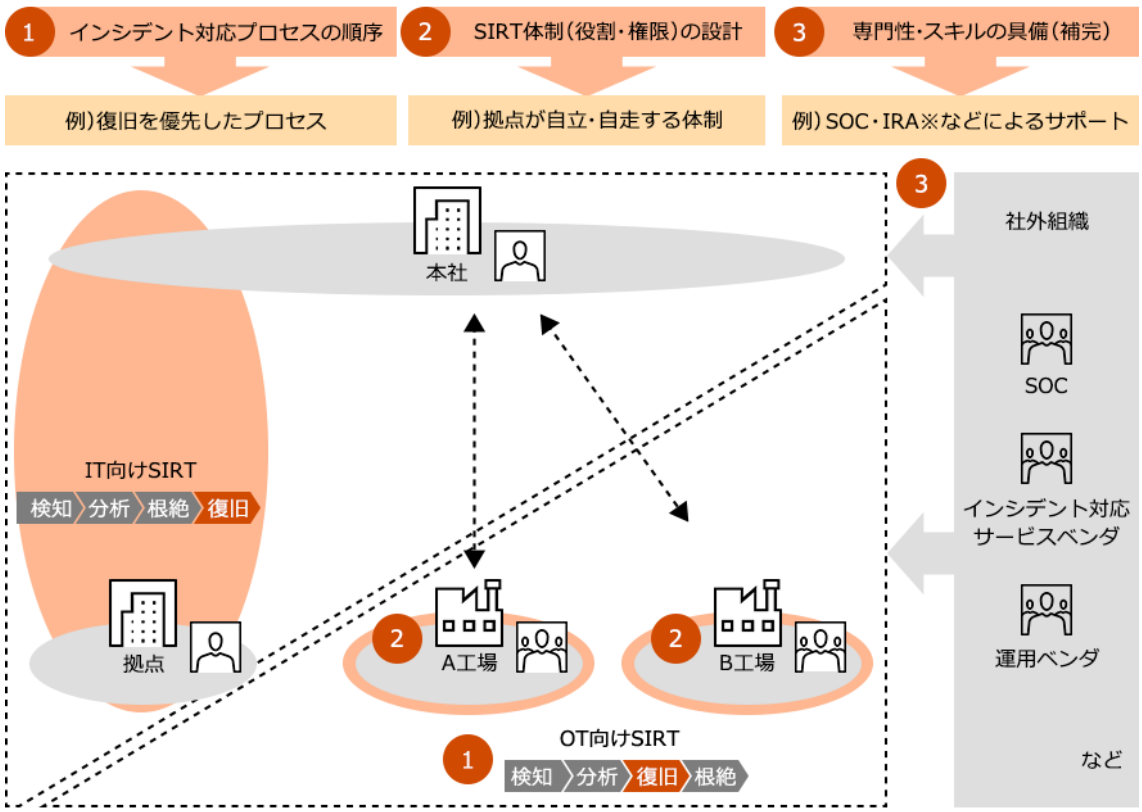
日本企業の多くは、これから自社のOTセキュリティ管理の在り方（体制、プロセス、技術的対策）の検討と、在り方の実現に向けた施策（制度や仕組み、対策製品の導入）の企画を進められることでしょう。その際、自社で保有する個々のOT環境が目指している機能や、実際の状況を適切に理解するとともに、従来の情報セキュリティ・ITセキュリティの考え方とOTセキュリティの考え方の違いを認識することが重要です。

例えば、インシデント対応態勢の在り方を考えてみましょう。プロセス面では、OT環境の特性に鑑みると、設備の稼働の維持または復旧を優先したいため、被害を受けた設備の隔離を前提としたプロセスではなく、稼働継続を前提としたプロセスとする必要があります。次に体制面では、OT環境はITのようにシステムやその管理が一元化されていないことから、状況把握や初動対応、切り分け、場合によってはトリアージなども、インシデントが発生している拠点の体制・人員で実施する必要があります。

しかしながら、こうした拠点の体制・人員は、本来セキュリティ管理を目的としたものではないため、セキュリティの専門性が経験・スキル面ともに不足します。その中で、トリアージや案件の切り分けといったセキュリティの知識・スキルを要するプロセスを有効に機能させるためには、拠点の体制・人員をサポートする外部サービスの利用や簡易的な判断基準の整備などの検討も必要です。（図2）

このように、すでに多くの企業が具備しているインシデント対応態勢1つを例に取っても、従来の情報セキュリティ・ITセキュリティとは随所で異なる対応が求められるであろうことが分かります。万が一、OTセキュリティの考え方を踏まえずOTセキュリティ管理に係る制度や仕組み、技術的対策を設計した場合、実効性が伴わないだけでなく、無駄な投資と運用コストを生じる懸念が強いと言えるでしょう。まさしくOTセキュリティの考え方に則った工夫が必要となるのです。

図2：インシデント対応態勢における留意点と検討例



※SOC：Security Operation Center
IRA：Incident Response Advisory

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com