OT セキュリティ訓練事例

株式会社小松製作所（コマツ）様

サイバー攻撃の矛先が IT だけでなく OT（Operational Technology：工場の生産設備や制御システム）へと広がる今、製造現場においても脅威への備えが求められる時代となってきている。建設機械・鉱山機械の大手メーカーの株式会社小松製作所（以下、コマツ）は、製造現場のサイバーセキュリティ対策を一層強化する取り組みとして、「OT セキュリティ訓練」に力を入れている。

製造ラインのみならず自動搬送装置（Automatic Guided Vehicle：以下、AGV）を訓練シナリオに取り入れるなど、工夫を凝らして訓練に取り組んだ津田氏と大久保氏に、導入の背景や訓練設計の考え方、得られた成果、今後の展望とこれから FSIRT を展開する企業へのアドバイスを聞いた。

本社総務部 リスクマネジメントグループ 主査
津田 隼人氏

システムエンジニアとして経歴をスタートし、2008 年にコマツに入社。人事部門のシステム担当、教育研修部門を経験しリスクマネジメントグループに配属。CSIRT の事務局を担当。
教育分野の知見を活かし、OT セキュリティ訓練を担当。

生産本部生産技術部 副部長
大久保 雅生氏

1992 年入社後、生産技術部門に配属。
2023 年から生産本部の DX 推進の GM を兼任、また生産本部に FSIRT を立ち上げ推進。
FSIRT のマニュアル作成、OT セキュリティ訓練を担当。

コマツのサイバーセキュリティ戦略

コマツは、情報セキュリティを IT の枠にとどまる技術課題ではなく、経営上の重要なマテリアリティのひとつとして位置づけている。2025 年から 2027 年の中期経営計画では、マテリアリティマップの上位に「プライバシーとデータ保護、サイバーセキュリティ」を設定し、成長戦略の 3 本柱のひとつである「経営基盤の革新」においても AI や DX の推進などの経営インフラ強化と並び、「BCP（サイバーセキュリティ／規制対応）」を重要な取り組みのひとつとしている。

出典 コマツ「新中期経営計画 公表資料」より抜粋

コマツがこの課題への対応を一層強化した背景には、国内外で製造業を含む多くの企業や組織がサイバー攻撃により業務や生産活動に深刻な影響を受けた事例が相次いだことにある。こうした状況を受けてコマツは情報セキュリティの事故対応を担う CSIRT（Computer Security Incident Response Team）に続いて、工場の OT 環境を対象とする FSIRT（Factory Security Incident Response Team）を整備し、サプライチェーン全体を視野に入れた体制づくりを進めている。

保護すべき情報資産とシステムが拡大する一方で、組織のリソースには限りがあるため、優先順位の設定が欠かせない。コマツは生産、開発、販売、および IT 部門などの管理部門が連携して、サイバーセキュリティの強化を全社的な活動として取り組んでおり、津田氏は「サプライチェーン全体を視野に入れ、全社的な視点でどの領域をどのように守るべきかを検討していくことが重要です。」と語る。

セキュリティを自らの課題として捉えるセキュリティ訓練

コマツは 2024 年度と 2025 年度、2 年連続で OT セキュリティ訓練を実施した。2024 年度は、OT 環境特有の脅威の理解、工場でサイバー攻撃が発生した場合の対応手順や役割分担、受講者が自ら考え理解を深めることなどを目的として、講義と訓練を組み合わせた教育を実施した。翌 2025 年度は、ネットワークと生産設備が直結する環境で発生する可能性のあるサイバーインシデントをリアルに体験できるよう、AGV をシナリオに組み込んだ、より実践的な訓練へと発展させた。津田氏は、「2 年連続で OT セキュリティ訓練を実施した理由のひとつは、DX 化が進む工場で起こり得るサイバーインシデントを現場の誰もが当事者として判断・対応できるようにすることでした。」と語った。

また、情報セキュリティの CIA（機密性・完全性・可用性）において、OT 環境では制御対象となる生産設備や部品・製品を安定的に稼働させるため、可用性を重視する傾向がある。ただし、それは機密性や完全性を軽視するという意味ではなく、人の安全確保と設備の継続稼働を最優先に、可用性・完全性・機密性のバランスを取ることが求められるということである。IT 環境では「即時遮断」や「封じ込め」といった対策が一般的

だが、OT 環境では必ずしも最適解となるとは限らず、安全と稼働のバランスを考慮した判断が重要となる。こうした IT と OT のセキュリティ思想の違いを理解し、共通認識を持つことも初年度の目的のひとつであった。

2 年目となる今回は、工場で日常的に稼働している AGV をシナリオのスコープに含め、実際に現場で起こり得るインシデントを題材にした。「安全を最優先としつつ、近年はネットワークにつながる機器が増えたことで、IT と OT の境目が無くなってきており、サイバーセキュリティの重要性が一段と高まっています。」と大久保氏は語る。

サイバー攻撃を受けた際に、生産設備の稼働を継続すべきか停止すべきかを判断するのは、設備担当者でなければ難しい領域であるため、CSIRT、FSIRT、現場部門の連携が不可欠である。そのため、工場トップから現場メンバーまでを対象に、工場の現場の実情に即した教育の実施と、実際に現場で稼働している生産設備を想定したシナリオを組み合わせた訓練を実施することが望ましい。現場の知見と専門部門の知識を結びつけ、組織全体でインシデントに備える仕組みづくりこそがコマツの目指す方向だ。その背景には、CSIRT、FSIRT、現場部門などの組織間連携をさらに深めていく必要があるという共通認識があり、こうした意識が OT セキュリティ訓練を継続的に進める原動力となっている。

コマツとラックが取り組んだOTセキュリティ訓練

2025 年度の訓練では前回に引き続きコマツとラックが連携して、コマツの OT 環境に合わせた実践的な机上訓練シナリオを新たに制作した。コマツは生産設備の構成や現場の業務フロー、専門用語など OT 環境ならではの詳細情報を提供し、ラックはそれを踏まえて訓練用シナリオに落とし込んだ。

実際のインシデント対応では、設備担当、CSIRT、情報システム部門、ベンダーなど複数の組織が迅速に同時並行で動く必要がある。両社は綿密な議論を重ね、判断の流れや情報共有のプロセスを具体的に再現できるように設計し、現場での対応を忠実に再現できる訓練内容に仕上げた。また、参加者が受け身にならず議論や判断に加われるよう、設問は報告書の作成などの演習ではなく、討議を中心とした形式を採用。その結果、現場の一人ひとりが自らの立場で考え、判断し、部門間の連携のプロセスも体験することができた。津田氏は次のように振り返る。「コマツには、工場を含めた組織構造、業務フロー、インシデント対応の手順、専門用語があります。こうした組織の動き方や用語などを正確に共有することに注力しました。ラックとの協働を通じて相互理解を深め、コマツの現場の実情に即したシナリオを構築できたと思います。」

実際に参加者からは「設備の不具合とサイバーリスクを、どう切り分けるかを考える必要性を体感できた」「何を確認し、どこへ報告するのかが明確になった」といった声が寄せられた。一方で「初動で本当に気づけるか不安」「自分たちの判断と模範解答との差の確認が重要」といった意見もあり、現場部門や FSIRT だけでは判断が難しい場面や CSIRT では把握しきれない現場の状況など、OT 環境特有の難しさと対応力を高める上での示唆が多く得られる機会となった。また、関係する部門全てが協働してインシデントに対応する重要性を認識することがこの訓練の目的のひとつであり、これらの目的を踏まえた上で「現場の感覚に自然になじむ」シナリオを共創できたことは、両社にとって大きな成果となった。

コマツが訓練パートナーにラックを選んだ理由は、過去に依頼した IT 環境の訓練における高い品質と柔軟な対応力を高く評価していたためであり、OT 環境向けの訓練においても同様に細部までカスタマイズできると考えたことが決め手となった。実際に工場設備や組織体制の詳細情報を共有し、シナリオを共同で作り込むことで、参加者が「これは自分たちの現場そのものだ」と実感できる訓練となった。

工場を守る、FSIRT訓練のロードマップと今後

「FSIRT 訓練に着手したい企業が最初に取り組むべきことは、インシデント対応体制とマニュアルの整備です。」と津田氏は語る。たとえ FSIRT を構築済であっても「各段階における責任の所在、判断プロセス、および報告経路」が明確になっていない場合、組織は緊急時に適切に動くことができない。マニュアルを整備し、関係者間で共有した上で、マニュアルに基づくインシデント対応手順の実効性を検証する訓練を実施することが重要である。また、OT 環境は IT 環境と異なり、設備の特徴や安全要件を熟知した現場の設備担当者でなければ判断できない場面も多く、訓練では現場の責任者や担当者の訓練参加が必要不可欠である。

一方、「工場のサイバーセキュリティに取り組みたいが、何から始めればよいのか分からない」という企業においては、まず自社の OT 環境のリスクを把握することが重要となる。DX やスマートファクトリーの進展によって、OT 環境は外部のインターネット環境と接続されつつあり、従来の閉じた環境に比べてサイバー攻撃を受ける可能性が高まっている。生産を止めないことは工場の重要な使命のひとつであり、生産継続がサイバー攻撃の脅威に晒されている可能性があるという事実を、経営層と現場の双方が共有することが OT セキュリティ対策の出発点になる。

今後コマツが注力するのは、国内で実施した OT セキュリティ訓練を海外の工場にも展開することである。津田氏は、「グローバルの生産拠点でも脅威の性質や対応の基本プロセスの差は大きくないと考えています。国内で作り込んだ訓練シナリオをベースにすれば、同様の効果を上げる訓練の実施が可能だと考えています。」と語る。このようにコマツは国内で構築した OT セキュリティ訓練をグローバル全体に展開していく予定である。ラックはこれまでの経験を活かし、今後も支援のパートナーとしての貢献が期待されている。

［お問い合わせ］
株式会社ラック
サービス紹介ページ https://www.lac.co.jp/education/course/ot_introduction.html