OT セキュリティ訓練事例

株式会社小松製作所（コマツ）様

海外の生産拠点とともに確認した、OTインシデント対応の基本動作
コマツが進める、各拠点の「もしも」に備えた取り組み

製造現場を狙うサイバー攻撃の脅威が高まるなか、海外に拠点を持つ企業には、インシデント発生時に現地で初動を判断し、関係者と連携できる体制が求められている。特に OT（Operational Technology：工場の生産設備や制御システム）領域では、安全や生産への影響を踏まえた判断が必要となるため、平時から対応の考え方を共有しておくことが重要だ。

では、国や地域によって言語や法規制、設備、組織体制、日常の運用が異なる海外拠点で、共通する初動や判断の考え方をどのように共有すればよいのか。建設・鉱山機械のフルラインメーカーである株式会社小松製作所（以下、コマツ）は、工場の OT 環境におけるサイバーインシデントが疑われる事態を想定し、海外の生産拠点を対象とした訓練を実施した。

海外展開の背景には何があったのか。拠点ごとの違いを前提に、どのように訓練を設計したのか。訓練設計の工夫、実施を通じて得られた気づき、今後の展望について聞いた。

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
川越 靖之氏

生産本部 生産技術部に所属し、DX 推進グループの業務を兼務。FSIRT を担当している。2026 年に生産技術部へ異動して以降は、海外拠点向け OT セキュリティ訓練の推進に携わる。それ以前は国内工場側の立場で、訓練を受講する側として OT セキュリティ訓練に関わってきた。

国内訓練を海外へ

コマツはこれまで、製造現場のインシデント対応力を高めるため、国内工場で OT セキュリティ訓練を実施してきた。2024 年は、OT 環境特有の脅威への理解を深めるとともに、サイバーインシデントが発生した際の対応手順や役割分担を確認した。翌 2025 年には、工場で実際に使用されている AGV（Automatic Guided Vehicle：自動搬送装置）をシナリオに取り入れ、より複雑な事態を想定した内容へと訓練を発展させた。

こうした国内での取り組みを踏まえ、次の展開先として検討していたのが海外の生産拠点だった。サイバー攻撃の脅威は国や地域を問わず存在する。加えて工場においても、異常の検知、影響範囲の把握、操業継続・停止の判断、社内外と連携して対応する必要があり、海外の生産拠点との間でも、その基本動作の認識を共有することが重要であった。

津田氏は、海外の生産拠点へ訓練を展開した背景を次のように説明する。「国内で訓練を実施した後、その次の段階として海外拠点に展開することは、自然な流れでした。サイバーセキュリティ上の脅威は、国や地域を問わず存在するため、OT 領域においてもグローバルで基本的な考え方を共有しておく必要があります。」

今回の海外の生産拠点向け訓練は、日本の本社側が海外拠点の対応を細部まで定めて、一律に管理することを目的としたものではない。各拠点で設備や組織体制が異なることを前提に、参加者が OT セキュリティの責任者や担当者としてインシデント発生時に主体的に対応できるよう、基本的な対応の流れや判断の観点を共有し、それぞれの拠点で必要な備えを自ら考えられるようにすることを目指した。

「OT セキュリティで何が重要なのか、どのような準備が必要なのかを海外拠点と共有することが、今回の主な目的でした。日本からすべてを管理するのではなく、訓練の経験から、それぞれの拠点で必要な備えを考えてもらいたいと考えました。」と川越氏は目的について語る。

共通の基本を軸にした訓練設計

訓練の設計では、海外拠点に共通して必要となる考え方を明確にすることを重視した。参加者には共通のシナリオを提示し、そこで示される状況や判断を、自らの拠点に置き換えながら討議してもらう構成とした。特定の組織体制や詳細な手順を前提とするのではなく、各拠点で実際に対応を検討する際のベースとなる判断軸を共有することを意図した。

訓練のシナリオは、国内で 2024 年に実施した訓練内容をベースに作成した。脅威の本質や、異常発生時に求められる基本的な行動は、国内と海外で大きく変わらないと考えたためである。ただし、国内向けの資料をそのまま英訳するだけでは、海外の参加者に意図が十分に伝わらない可能性がある。そこでコマツとラックは、国内訓練の基本的な流れを維持しながら、日本固有の要素を調整し、各海外拠点が自らの設備や組織体制に照らして検討できる内容へ整えた。ラックは、セキュリティ訓練の設計ノウハウと OT セキュリティの専門性を活かし、海外拠点で共通して用いるシナリオへの調整や、OT 特有の判断ポイントの整理をした。

例えば、当局への報告要否や報告先、手続きは国や地域によって異なるため、日本の機関名や手続きを前提とした記述は一般化した。地域ごとの違いは、シナリオを全面的に作り替えるのではなく、注釈や補足説明で対応した。訓練で伝える中心的なメッセージは共通化しながら、各拠点の実情にも配慮できる構成とした。「拠点ごとに法規制や設備、体制が違うのは当然ですので、共通して押さえるべき基本動作を軸にして、日本を前提にした部分は一般化し、あとは各拠点が自らに照らして考えられるようにすることを心がけました。」と津田氏は説明する。

訓練は、事前学習のeラーニングと当日のオンライン訓練の2部構成とした。事前学習には、国内で 2025 年に実施した訓練のeラーニング動画を英語化したものを用いた。内容は、セキュリティの基礎、IT と OT の違い、インシデント発生時の対応の考え方で、当日のシナリオ討議に入る

© 2026 LAC Co., Ltd.

前に、参加者の前提知識を揃えることを狙いとした。英語化にあたっては、ラックが動画の英訳と英語音声の収録を担当した。当日の訓練でも、英語によるファシリテーションをラックが担当した。

OT特有の判断を踏まえ､｢異常の後にどう動くか｣

工場における設備の不調や普段と異なる動きは、不具合によるものであるのか、サイバー攻撃であるのかを見極めるのは難しい。訓練のシナリオでは、操作端末の応答が遅くなるという、一見ありふれた不具合から始まる。担当者が様子を見るなか、複数の端末で同じ症状が続き、再起動しても直らないことをきっかけに、上司がサイバー攻撃の可能性を疑い、FSIRT（Factory Security Incident Response Team）へ連絡する。訓練ではこの場面を起点に、現場の担当者から上司、FSIRT、地域の CSIRT、工場長や関係部門へと情報を上げ、組織として判断するまでの初動の流れを確認した。さらに事態が長引いた段階では、これらの関係者が緊急対策の体制を組み、外部の専門家とも連携して対応を判断する流れを扱った。

特に重要なのが、IT とは異なる OT ならではの判断だ。IT のインシデント対応は、検知したらまず切り離すなどで被害の拡大を止め、その後に対策と恒久対応へ進むのが基本である。これに対して OT では、直ちに止めることが前提ではなく、人の安全が確保できていれば、生産を継続しながら対応することも選択肢になる。被害が広がるリスクに応じて、監視の強化から設備の隔離、部分的な停止へと段階的に封じ込めを強め、継続か停止かは在庫や出荷、サプライヤーへの影響も含めた工場の BCP として、FSIRT が地域の CSIRT や IT 部門と連携して判断する。訓練では、こうした考え方を拠点を問わず共通の基本として確認した。

「人の安全に危険が及ぶなら、その場で止める。これは現場の判断で、承認を待つものではありません。安全が確保できているときに生産を続けるか止めるかは、設備を理解している FSIRT が状況を見極めたうえで、工場長など現地のマネジメントを交えて決めることになります。生産を止めれば、影響は自分たちの工場にとどまらず、サプライヤーや顧客、他の拠点にも及ぶからです。訓練では、技術的な対応だけでなく、マネジメントとどう情報を共有し、判断するかも確認しました。」と津田氏は振り返った。異常に気づいた人が、誰に何を伝え、関係者がどのように判断するか。そして、報告を受けた関係者がどの情報をもとに、どこまでの対応を判断するのか。訓練では、こうした一連の行動を具体的にイメージし、組織としての動きを確認した。

また、海外拠点向けの訓練は、複数の国と地域から参加できるオンライン形式で実施した。参加者の移動負担を抑えながら共通のシナリオを共有できた。海外の関係者を一か所に集めずに実施できたことは、今後の継続的な展開に向けた有効性を示した。

訓練から必要な備えを具体化

訓練後のアンケートでは、5 段階の総合評価で 4 以上が 96% を占め、インシデント発生時の行動を「イメージできた」とする回答も 89% だった。自由記述でも、「軽微な異常が大きなリスクにつながることを認識できた」「他拠点や他部門の観点を聞くことができた」といった声が寄せられた。ただし、コマツはこれを一度の訓練で完結する取り組みとは考えていない。訓練で確認した基本動作が各拠点の備えとして根付くには、定期的に訓練を重ねていくことが欠かせないためだ。

今回の訓練を通じて、参加者はインシデント発生時の基本的な対応を確認するとともに、自分たちの拠点で何を準備しておく必要があるのかを考える機会を得た。川越氏は、「訓練をすることで、『こういう準備をしなければならない』ということを、それぞれの参加者に感じてもらえたのではないかと思います。1 回の訓練だけで意識が変わったかを判断することはできませんが、必要な備えに気づいてもらうことが、大切です。」と語る。

訓練は、平時の備えを改めて見直す機会にもなる。シナリオで再感染の原因となったのは、最初の確認範囲から漏れていた端末だった。影響を受ける可能性のある設備やシステムを素早く見極め、確認漏れを防ぐには、設備やシステムの接続関係を示すネットワーク図や、初動対応上、把握しておくべき設備･システムの一覧が適切に更新され、必要な際に参照できる状態にしておくことが重要になる。どのシステムがどこにつながっているのか、異常が発生した場合に誰へ連絡するのかを平時から整理しておくことが、迅速な初動対応につながる。

共通の基本を軸に､各拠点が自ら備える

訓練で確認したのは全拠点に共通する基本的な考え方と対応の流れであり、それをそのまま各拠点に当てはめることは想定していない。拠点にはそれぞれ、設備や体制に応じた運用があるためだ。各拠点が自らの設備や体制を踏まえて必要な備えを整え、「もしも」のときに判断して動ける状態を目指す。

川越氏は、「共通の手順を示してそこに従ってもらうというよりも、必要なところは各拠点の設備や体制に合わせてアレンジしてもらい、自分たちで運用できる形にしていければと思っています。」と語る。

継続的な訓練で､より実践的な備えへ

設備やシステムの構成は変化し、サイバー攻撃の手口も巧妙になり続けている。組織や担当者が変われば、インシデント発生時の連絡先や判断の流れをあらためて確認する必要が生じる。平時には問題なく機能しているように見える体制も、実際に訓練してみることで、新たな課題が見えてくる。

コマツでは、国内外問わず、今後も訓練を継続する方針である。これまでの国内訓練では、AGV を取り入れた、より複雑なシナリオも実施してきた。次回以降の海外拠点向け訓練では、今回確認した共通の基本動作をベースに、より発展的な内容を実施していくことが期待される。訓練を重ねることで､想定していなかった課題を見つけ､平時の備えに反映する。その積み重ねが､いざというときに現場が迷わず動ける対応力につながっていく。

LAC

［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

● ラックおよびLACは株式会社ラックの登録商標です。　● 記載されている会社名、サービス名、製品名は、一般に各社の登録商標または商標です。

© 2026 LAC Co., Ltd.