製造業に必要なセキュリティ対策

狙われる生産現場ー
今、製造業に必要なサイバー攻撃対策とは

サイバー攻撃が多様化/高度化した今、攻撃者は製造業をターゲットにしてきている。だが可用性を重視したOT では常に最新化が必要な ITとは正反対の環境にあり、IT の防御手法ではなかなか対策が進まない。 IT/OT 環境を両面から守る方策とは？

製造業においては OT（Operational Technology）と呼ばれる、工場内の機器を制御するための技術がある。これはコンピューター機器やネットワークなどいわゆる IT (Information Technology) と同じような技術が使われるが、その的や指すものは異なっている。そのため、多くの現場では IT と OT の衝突のようなことが起きているというのが実情だろう。

近年、OT がオープン化した技術をベースにするようになり、IT 環境に対する攻撃がそのまま OT 環境に大きく影響するようになってきた。攻撃は技術的に高度になるだけでなく、人の心理を突くような人的脆弱（ぜいじゃく）性も悪用され、攻撃の多様化も進んでいる。OT 環境では「最新の状態にアップデートする」ことは難しく、「多種多様な防御手法を導入する」こともシステムの不安定さを誘発し、IT 環境と同じ方法では対策がなかなか進まない。これが、情シス部門と製造部門の摩擦を生む原因なのではないだろうか。

だがサイバー攻撃が激化する今こそ、IT 部門とOT 部門は協力していかなければならない。本稿では、IT/OT それぞれのスペシャリストが「いま製造業が狙われている現状」「セキュリティ視点における製造業の課題と対策強化ポイント」「OTで可視化が必要な理由」を解説している。製造業にとって生命線ともいえる IT/OT 環境を両面から守る方策についてお届けしよう。

製造が狙われているーその理由は？

最新のサイバー攻撃ではさまざまな脆弱性を悪用し、侵入できないと思われていた場所へ不正に入り込み、悪意ある行動が行われている。

報道が多く行われてきた「ランサムウェア」は、単にデータを暗号化し身代金を要求するだけでなく、支払わなければデータを公開すると脅すなど、複数回の脅迫を行うことが当たり前

富士通株式会社
インフラ＆ソリューションセールス本部
プロモーション統括部
デジタルプロモーション部
マネージャー

斎藤　建氏

になった。また、そのような直接的な攻撃だけでなく、利用者をだますようにパソコンの画面上に偽のポップアップメッセージ「ウィルスが検出されました」と出すことや、マルウェアが入ったUSBメモリを物理的にばらまくなどの方法もある。攻撃が多様化することで、直接金銭を奪取することから脅迫やデータ取得などによる間接的な搾取へとターゲットが移行しつつある。その移行先の一つが、急激に攻撃が増加している「製造業」なのだ。

富士通の斎藤建氏は、「サイバー攻撃に関する報道は公表しづらいことが多く、実際には " 針の先 " 程度しか伝えられていない」と表現する。特に製造業においては、止まってはならない OT を抱えている。クラウドを活用しつつ DX を進めるというスピード第一の IT と、慎重にことを進め安全が第一である OT では話が合わないことも多い。

しかし、製造業の機器も最新のテクノロジーが利用されており、例えば電子顕微鏡というモノの制御のため、オープンな OS であるWindows が使われることも多い。もはや ITとOT はセットであり、IT 部門と OT 部門それぞれが協調しつつ、それぞれのやり方を選ぶことで、企業全体を守る方法が求められているのだ。

富士通株式会社
インフラ＆ソリューションセールス本部
プリセールス統括部
NWセキュリティセールス部
シニアマネージャー

松山　啓介氏

製造業を取り巻く環境

製造業においても、スマートファクトリーを始めとする新たな潮流が具体化している。IT/OT 環境をダイレクトにネットワーク接続することで、工場内の機器から上げられるデータはSaaS/クラウドサービスと連携し、取引先を含めたサプライチェーンで共有、連携される。一方で、このようにITとOTがつながることで、工場におけるサイバー攻撃のリスクが高まっている。

富士通の松山啓介氏は「この状況を、攻撃者はしめしめと思っている」と述べる。製造業におけるリスクは IT につながるOTだけでなく、サプライチェーンへの影響も懸念される。松山氏はサイバー攻撃において最も懸念される手法である、標的型ランサムウェア攻撃とサプライチェーン攻撃を例に紹介する。

これまでの多くのランサムウェア攻撃では、暗号化のためのマルウェアを添付したメールを不特定多数にばらまき、そのうち１つでも実行されればよいといった考え方で行われていた。しかし今では文字通り「標的型攻撃」が行われる。

よくある事例として、テレワークで急激に活用が広がったVPN装置の脆弱性が狙われ、攻撃者がIT環境内に侵入するケースがある（図1）

攻撃者は侵入後、順次ウィルス感染・拡大を行い、IT 環境内を渡り歩いた先に見つけた機密情報（個人情報や機密データ）を暗号化し、盗み出す。さらに攻撃者は OT 環境につながることのできる IT 機器への攻撃もできてしまうのだ。

この事例では、VPN 装置に脆弱性が残っていたこと、IT環境内の管理サーバやユーザー端末を狙った攻撃に気が付けなかったことなどが課題として挙げられる。OT 環境ではサポート切れ OS も稼働していることが多く、脆弱性による感染を止められない。それを防ぐには、OT 環境における、OTならではの方法によるセキュリティ強化が課題として捉えられるだろう。

そして、もう一つの大きなポイントは「サプライチェーン攻撃」だ。ここでは技術的な課題というよりも、そもそも取引先を完全にコントロールするのは難しいということが一つの要因だ。松山氏は「取引先やその委託先の企業全てが、十分なセキュリティ対策を行えているわけではない。ある取引先のセキュリティ対策が不十分だった場合でも、自社ではそれを把握することが難しい。攻撃者がその取引先を見つけ出した場合、サプライチェーンを逆流し、自社にまで影響を及ぼす可能性がある」と述べる。

「コントロールし切れていないというよりも“コントロールしていない”のが実情だ。目を向けていない場所に目を向けねばならない」（松山氏）

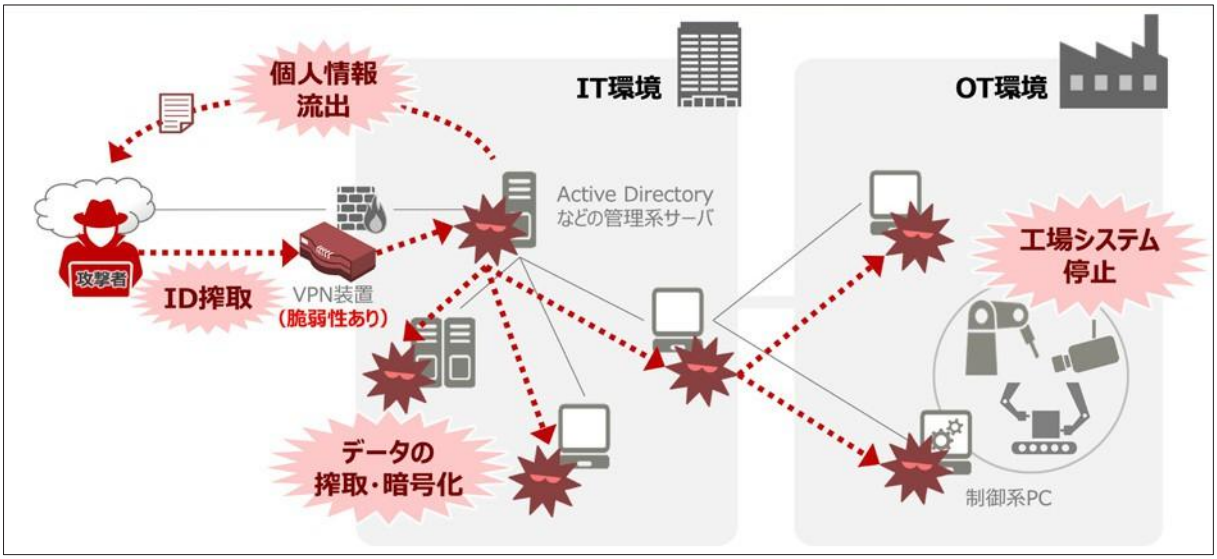

図1　攻撃者がVPN装置を侵入口とした例。このケースでは侵入口を起点としてOT環境にまで入り込まれてしまった

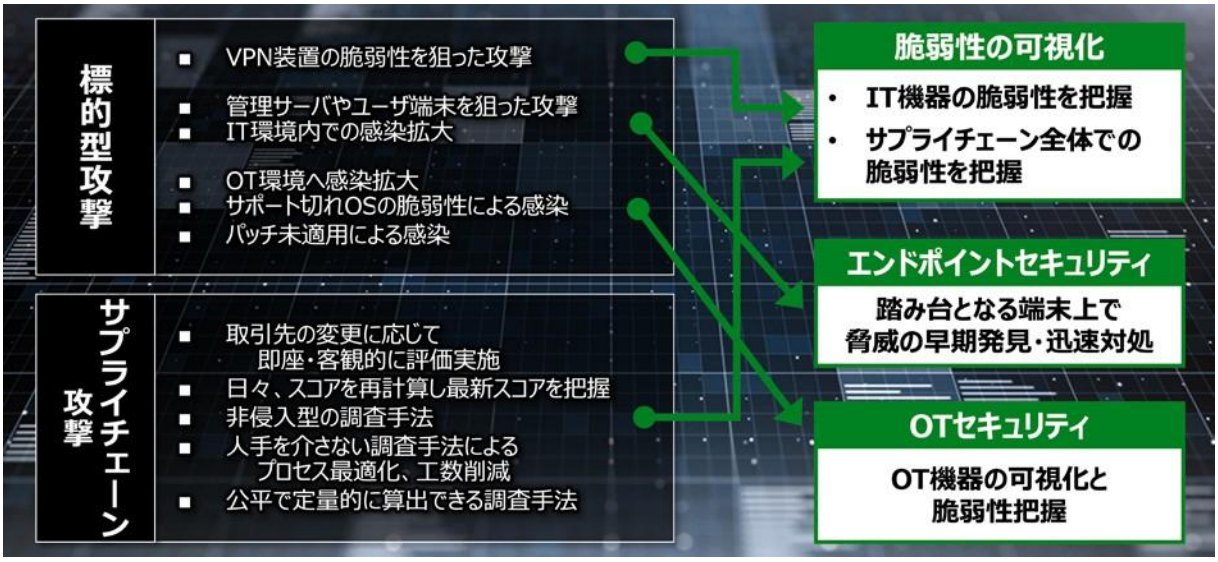

図2 富士通が考える、まず着手すべき「脆弱性の可視化」「エンドポイントセキュリティ」

このような現状がある中、松山氏は IT における対策として、まず行うべきは「脆弱性の管理」と「エンドポイントセキュリティ」だと述べる（図2）。脆弱性の管理はサイバー攻撃を成功させないためのもの、そしてエンドポイントセキュリティは万が一侵入された時のことを考え、被害を最小化する投資対効果の高い対策だ。

普段と違うことに気が付くためには ーOTで「可視化」が必要な理由

そして、OT部分にはOTにおける特徴を加味した対策が重要だ。これまでは生産現場のネットワークは分離されている前提で考えていたかもしれないが、その考え方を変えていく時期に来ている。

富士通の蛭田盛夫氏は「OT環境においてももはやスマート化、DX化のデータ活用が無視できず、何らかの形でネットワーク接続されていると考える。直接生産現場が狙われているわけではなくても、生産現場に脅威が入り込むとまたたく間に被害が出てしまう」と述べる。

だからこそ、生産現場を守らなければならない。生産現場を守るためには、セキュリティ耐性を高めるため、何がどのようなことをしているのか " いつもの状態 " を知っておくことが重要だ。「"いつも"を知っていれば異常に気付くことができ、異常に気付くことができれば対処ができる」と蛭田氏はアドバイスする。IT 環境と OT 環境がどこでつながっていて、どのような通信が行われているかを可視化することにつながるが、その可視化が必要な理由とは「いつも」を知るためなのだ（図3）。

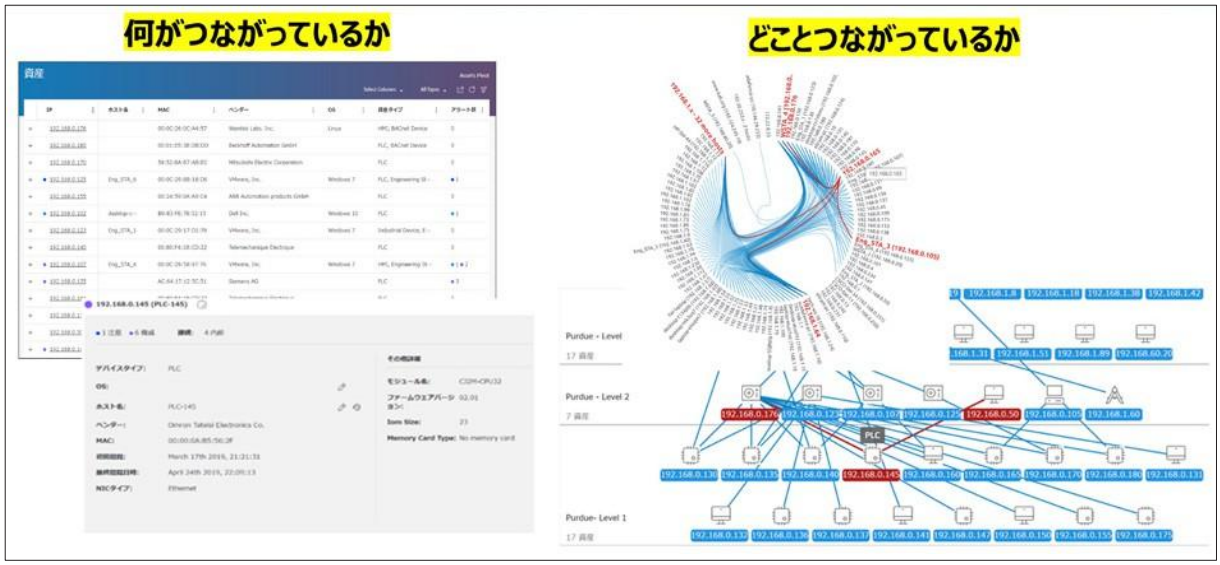

図3 セキュリティセンサーとしてOT ネットワークの可視化サービスを活用し、いつもの状態を知る

富士通株式会社
ネットワーク＆セキュリティ
サービス事業本部
サービスビジネス事業部
インテグレーション部
マネージャー

蛭田　盛夫氏

それを実現するために、富士通は OT ネットワークの可視化サービスを提供している。蛭田氏はこの特徴を「生産現場のネットワーク状況を、リアルタイムに把握できること。対応方法を提案することで生産業務の継続性、健全性を向上させること。そして対策の有効性を把握できるよう、スコア化することにある」と述べる。

具体的な機能を見ていこう。富士通のOTネットワークセキュリティ可視化サービスでは、自社OT機器の脆弱性を、CVE情報と呼ばれるリストと照らし合わせ、優先して対応すべき脆弱性を含む機器がどこにあるのかを把握することができる。また「MITRE ATT&CK（※注）」フレームワークで定義される攻撃の段階と手法における、どの部分に関連する異常なのかを確認でき、今あるリスクに気が付くことができるようになる。不正アクセスが行われていないかを把握するための「ユーザーアクティビティー分析」や、「IEC 62443/NIST-CSFなどのガイドラインの適合度合いをスコア化」する機能も提供され、これらを活用することで自社のOT環境を評価し、自分の現在値を把握することも可能だ。

セキュリティに強い企業が選ばれる時代に

もはやセキュリティはコストとして考えるものではなく、自社を強化し、自社の強みを増やすための「投資」だといえる時代だ。サプライチェーン攻撃に注目が集まる今、セキュリティ対策が十分な企業との取引を望むのは当たり前だろう。そのためには、さまざまな行動指針や国際規格に準拠し、IT部門とOT部門が協調して安全を作り出していること、そしてそれが理解されることが重要だ。

今やOTの領域でもICTの技術が無くてはならない存在になってきている。その意味では”ITの知見があるOT専門家" よりも、富士通のような“OTに精通したICT専門家”をパートナーに選定すべきだろう。また富士通ならば、可視化された状態から現状のリスク・改善ポイントの発見（アセスメント）、それらを解決するためのネットワークのありようも含めた対策立案（グランドデザイン）、グランドデザインにのっとったインテグレーション、それらを維持していく運用支援まで、DX化の土台となるネットワーク構築に必要なサイクルをワンストップで対応可能だ。

富士通は上記で紹介したサービス以外にもさまざまな対策ソリューションを持ち、組織のかたちに合わせた総合的な提案を得意としている。激化するサイバー攻撃への対策に動き出したならば、ぜひ一度相談してみてほしい。

※注　MITRE ATT&CK：MITRE（マイター社）が開発した、「攻撃者の行動を戦術や先方から分類したナレッジベース（ATT&CK：Adversarial Tactics, Techniques, and Common Knowledge」(2022/9/1掲載)

関連リンク

- ✓ サイバー攻撃から生産現場を守る 早期検知と迅速対応で事業継続を実現
- ✓ リスクを可視化し、工場DXを推進　生産現場の現状把握から未来のロードマップ策定までサポート
- ✓ DXを加速させる、安全なOTネットワーク　設計・構築から運用までワンストップで支援
- ✓ 端末やネットワークの挙動から不正な兆候を検知し、高度なセキュリティ運用を実現するXDRソリューション
- ✓ リアルタイムでサイバー攻撃の兆候を検知・防御し侵入後の対応も迅速に実現するEDRソリューション

※この冊子は、TechFactory（https://techfactory.itmedia.co.jp/）に 2022 年 9 月に掲載されたコンテンツを再構成したものです。
https://techfactory.itmedia.co.jp/tf/articles/2209/30/news013.html

※本記事中に記載の肩書きや数値、固有名詞等は掲載日現在のものであり、このページの閲覧時には変更されている可能性があることをご了承ください。
[2023年掲載]

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中4-1-1