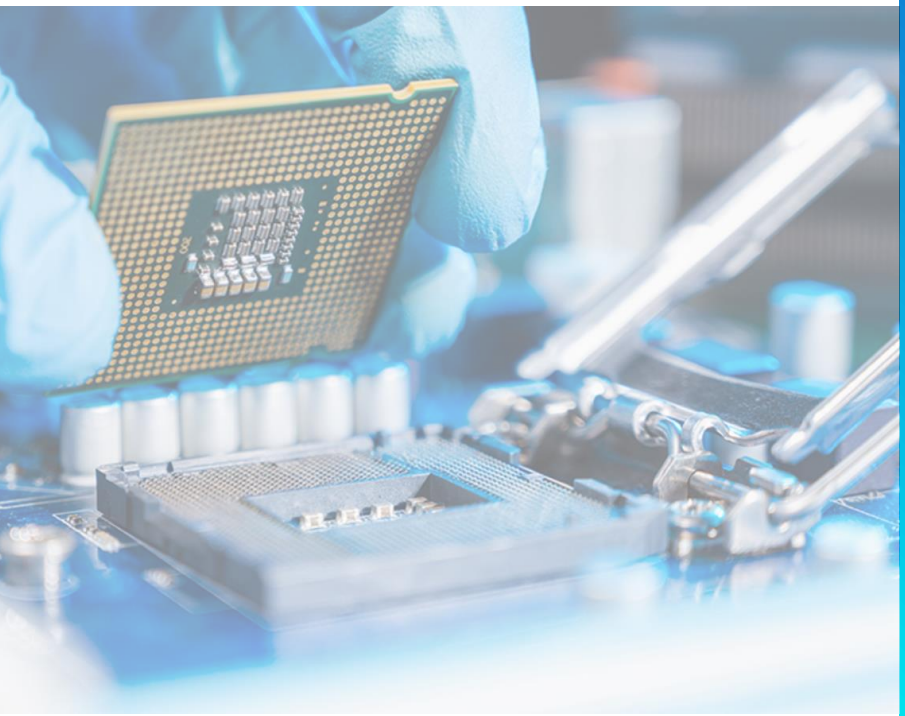
FUJITSU

製造業が狙われている！
今、必要なサイバー攻撃対策

～企業の生命線となる IT/OT 環境を
両面から守る方策とは～



目次

1. なぜ今、製造業がサイバー攻撃に狙われているのか？

数年前は金融業がターゲットになっていましたが、攻撃が多様化/高度化した今、攻撃者は様々な方法で利益を得ることができるようになってきました。その多様化、高度化した攻撃とは、どのようなものなのか。そして、こうした攻撃をどのように防げば良いのか、その内容をお伝えします。

さらに、IT と OT 環境における安全と、安定の重視という相反する性質を持つ環境を、その両面において防御するための考え方とその手法についてまとめました。

1.1 ウイルスとは何か

まずは、少しウイルスの話から始めましょう。

新型コロナもウイルスですね。ウイルスは細菌とは違い自分だけでは生きられないという特性があります※1。この特性は、まさにコンピュータウイルスも同じです。自己増殖しないものも含めて悪さをするソフトウェアという意味ではマルウェアといいます。マルウェアは、コロナウイルスが”人“という生物の分類に寄生するように、”Windows”のような固有の OS に寄生するのです。

つまり、様々な OS が多数存在すると、マルウェアはなかなか寄生できない（寄生できる宿主にたどり着けない）のです。だから、工場専用のコンピュータなどは感染しにくいのです。よって、オープン化したシステム、つまり Windows などが中心となった現在のシステムの課題はそこにある訳です。近年では様々な制御システムは Windows で動いていますので、そこに寄生するマルウェアが問題になってきています。これが、製造業においてサイバー攻撃が問題となっている要因の一つなのです。

※1 参考：広辞苑, 一般財団法人 新村出記念財団, 発行所 株式会社岩波書店， 2022 年 2 月 10 日 第七版, ISBN978-4-00-080131-7

1.2 なぜ、サイバー攻撃は攻撃者優位なのか

ここで、サイバー攻撃が攻撃者優位と言われていることについて考えてみましょう。

この原因は大きく 2 つに分けることができます。一つが攻撃の高度化、もう一つが攻撃の多様化です。攻撃の高度化とは、技術的な脆弱性が原因であり、多様化は、人的な脆弱性であるというように整理することができます。攻撃の高度化は、攻撃者しか知らないプログラムの穴（セキュリティホール）を突くことです。この様な高度な攻撃は守ることが非常に困難となります。一方、攻撃の多様化は、多様な方法によって人間の心理を突く攻撃です。この 2 つについて混同されることが多いため、ここで整理してお伝えしていきます。(図 1)

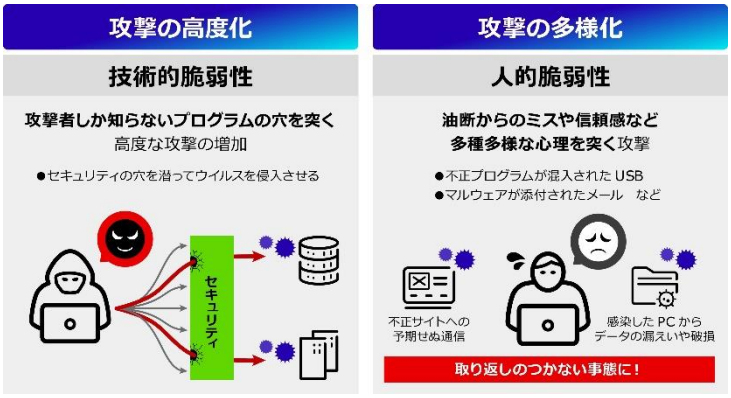


図 1：サイバー攻撃者の優位性

1.3 サイバー攻撃の高度化

ではまず、高度な攻撃について少し掘り下げて考えてみましょう。

高度な攻撃の代表例は、誰も知らないプログラムの脆弱性、つまり、「Zero Day」の脆弱性（日本語の「ゼロデイ」とは意味が異なります）を突く攻撃であって、つまりこうしたものが、「Zero Day Attack」と呼ばれます。「Zero Day Attack」は、元々は軍で検討される攻撃手法でした。しかし、現在は、ダークウェブから攻撃ツールとセットで入手することができてしまいますので、購入さえできれば誰でも攻撃を行えるものとなってしまっています。ただし、これは攻撃数としては少ないものであるとも言えます。(図 2)

高度な攻撃には、もう一つの特徴を持ったものがあります。それは、あえてオオゴトにしない攻撃です。これは、実は表にはあまり出てきませんので、よく分かっていない部分も多くあるところです。オオゴトにしないというのは、水面下で攻撃を進め、ずっと気づかれないままに仕掛けを行っていくということです。例えば、工場の歩留まりを下げる、つまり不良品を多くすることを水面下で行うということです。実際にこうした攻撃が見つかっている訳ではありません。しかし、攻撃者によってはこうしたことをする動機が十分にありますし、また、あってはならない様々なところで目的の分からないマルウェアが見つかっているために、こうしたことも疑われているのです。

1.4 サイバー攻撃の多様化

続いて多様な攻撃によって人的脆弱性、つまり人の弱みにつけ込んでくる最近の攻撃について、掘り下げて考えてみましょう。

まず一つ目として、ランサムウェアと脅迫の組み合わせです。「ランサム」自体が身代金要求という脅迫を意味するものなのですが、身代金を支払わなければ盗んだデータを暴露するという、二重の脅迫をしてくるようになってきています※2。さらに、支払に応じたら応じたで、”支払いに応じる企業”として闇市場に出回るターゲットリストに加えられてしまい、何度も攻撃を受けてしまう、ということにも繋がってしまいます。

二つ目として、ウイルス感染を『騙る』攻撃です。これは、皆さんの個人のパソコンにもよく来ているのではないでしょうか。例えば、『あなたにサイバー攻撃をしましたよ』というメールを送りつけるだけで、実際にはウイルスを送り込むなどの攻撃はしていないにもかかわらず、お金を騙し取ろうとする攻撃です。

また、少し似ている攻撃として、ポップアップで『あなたのパソコンはウイルス感染しました』と嘘の表示をさせる手口も出てきています※3。 こうしたことを知らない人は、かなり焦ってしまうのではないでしょうか。

人的脆弱性を突く攻撃の三つ目として、USB 攻撃があります。これは昔からあるものですが、USB 攻撃を侮らないでください。この攻撃はある意味では最強とも言われており、軍のレベルでも再三やられている手法です※4,5。(図２)

※2 参考：事業継続を脅かす新たなランサムウェア攻撃について, IPA, https://www.ipa.go.jp/files/000084974.pdf, 2020/8/20
※3：攻撃内容は、筆者が確認したものを基に解説、再現
※4 参考：サイバー戦争 終末のシナリオ 上, ニコール・パーロース著, 発行所 株式会社早川書房, 2022 年 8 月 15 日発行
※5 参考：ゼロデイ, 山田敏弘著, 発行所 株式会社文藝春秋, 2017 年 3 月 20 日発行

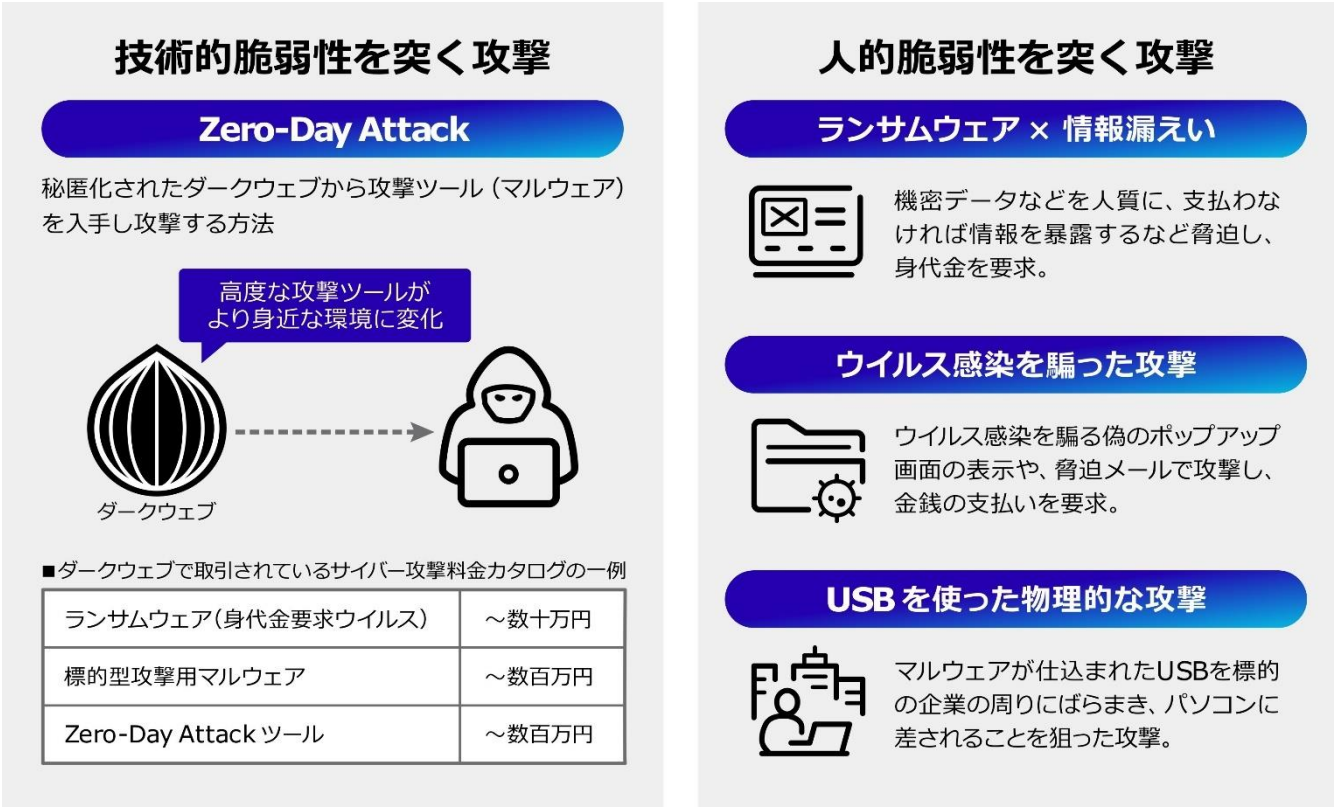


図２：技術的脆弱性と人的脆弱性の攻撃手法

1.5 金融業から製造業へ

このように様々な攻撃手法が出てきているために、攻撃者から見ると間接的にお金を取り易くなったと言っていいでしょう。少し前のサイバー攻撃は、金融機関が狙われ金銭を奪われていた、というところがありました。しかし最近は、金融機関の防御が堅くなったこと、また、様々な攻撃が可能になったことによって製造業が狙われるようになってきたということが言えます※6。

※6 出展:How Ransomware Attacks Impact the Manufacturing Industry, xorlab, https://www.xorlab.com/en/blog/how-ransomware-impact-manufacturing, 2023 年 1 月 13 日採取

2. IT と OT の文化の違い

そこで、製造業の環境を、考えてみましょう。

製造業は、IT（情報システム）と OT（制御システム）の 2 面性があることを考えておく必要があります。例えば、IT は DX を進めていますが、OT はとにかく止まると一大事です。また、IT では新規性が求められますが、OT では昨日と今日とで変わることを良いとされず、トラブルの元をそれで予見したりします。さらに、IT はクラウド活用を促進していますが、OT は外部接続を一部のみにすべきでしょう。また、IT はスピード第一で、OT では安全第一というように、常識が大きく異なるのでそれぞれの部門において、なかなか話が合いません[※7]。

※7 参考:製造業のサイバーセキュリティ, 佐々木弘志著, 発行所 株式会社 日科技連出版社, 2021 年 4 月 26 日発行, ISBN 978-4-8171-9734-4

2.1 IT セキュリティと OT セキュリティ

そうなると、セキュリティの面でも、いろいろと違いがでてきます。ウイルスに対しても、OT 環境ではウイルスチェックは基本的にできませんので、混入防止が大事です。OT ではパッチ適用もできませんので外部と遮断するか、もしくは監視が大事です。ウイルスに感染しても、OT では簡単にシステムを止めることもできません。(図 3)

OT の分かりやすい例としては、電子顕微鏡が挙げられます。端末とセットになっています。これでは、簡単には入れ換えもできません。製造業にサイバー攻撃の狙いが移ってきている中で、IT と OT では考えることが違うということから IT と OT のそれぞれに必要な対策を取っていくことが求められる訳です。

では次から、製造業が受ける攻撃について、見ていきましょう。

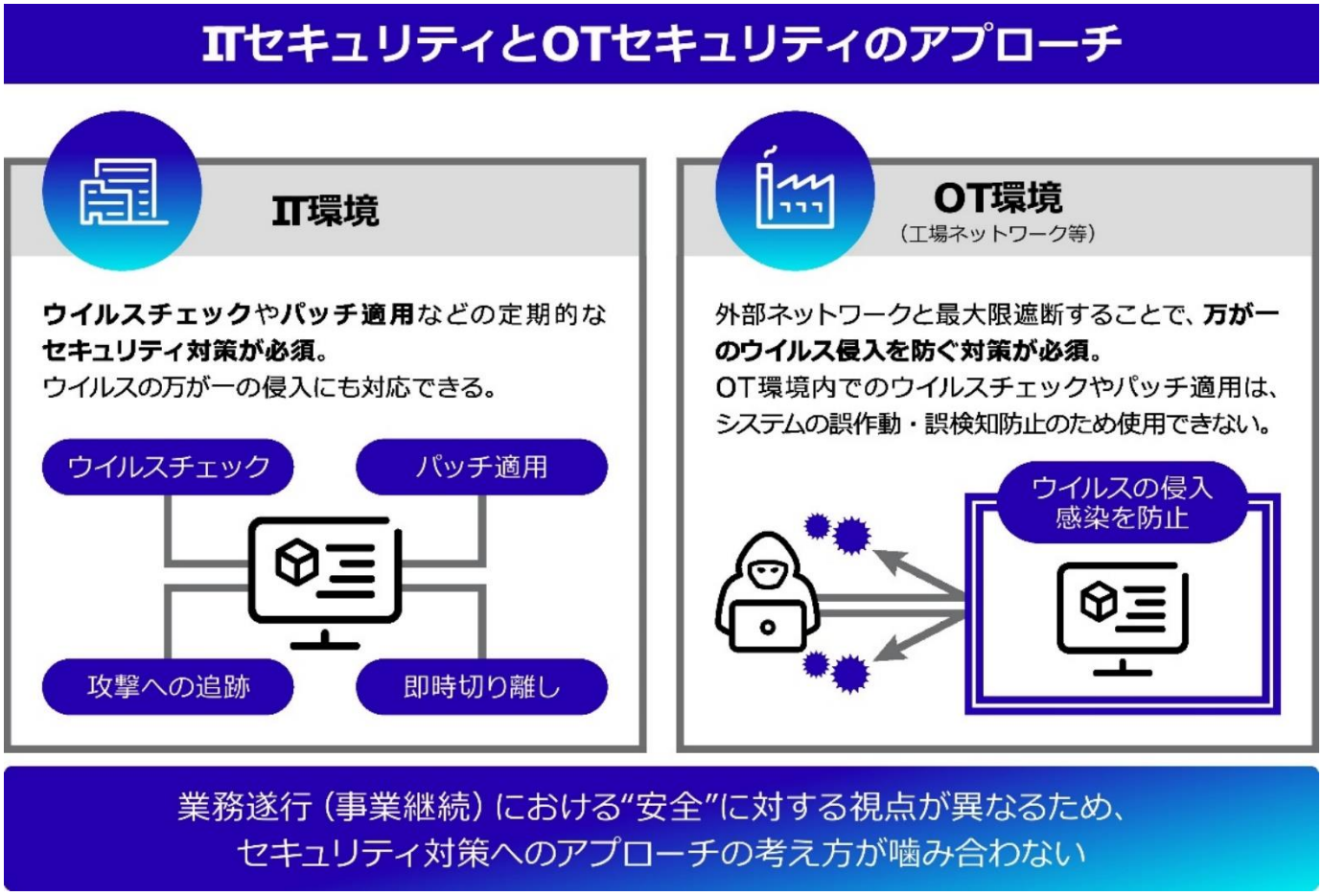


図 3 ：IT セキュリティと OT セキュリティ

2.2 製造業が受ける攻撃

製造業が受ける攻撃として、IT 環境から入ることがあります。よって、IT 環境をしっかりと守ることが、工場を守ることにも繋がります。例えば、昨今のテレワークを狙って、攻撃者は VPN 装置の脆弱性を突いて ID 窃取を行うことがあります。または、メールなどで端末にマルウェアを送り込み、その端末に脆弱性があると開封することでマルウェアに感染し、バックドアを仕掛け、端末に侵入してくるということもあります。そこから、攻撃の拡散を行います。最終的に個人情報を窃取したり、工場を停止させたりということを行います。(図４)

このような攻撃は、関連会社や子会社を経由してくるということもあります。いわゆるサプライチェーン攻撃というものです。対策の弱いところを狙って、攻撃者は攻撃を仕掛けてきます。

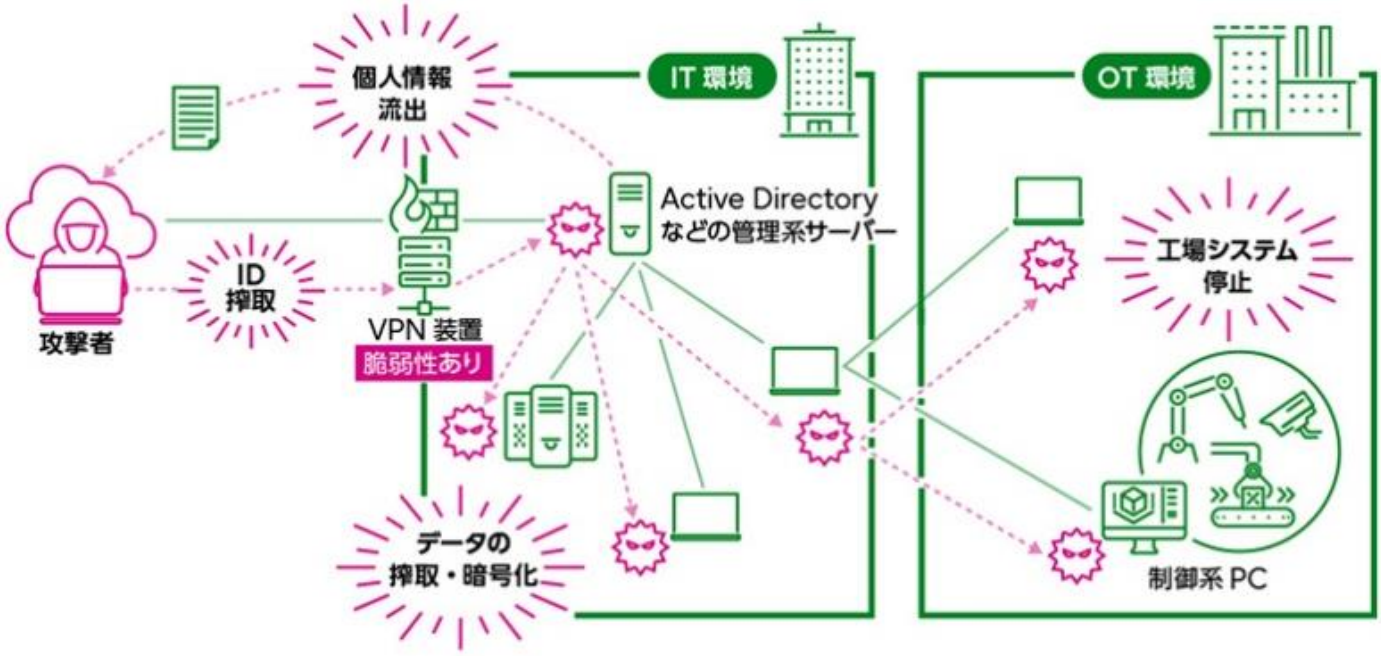


図４：製造業への攻撃手法

3. 製造業における対策

弱いところを狙われないようにするためには、脆弱性をしっかりと潰し、弱さを見せないようにしておくということが重要です。さらにユーザ端末やそれを踏み台としてサーバーに入ってこられないような対策も必要です。その上で、OT セキュリティを強化していくと良いでしょう。(図５)

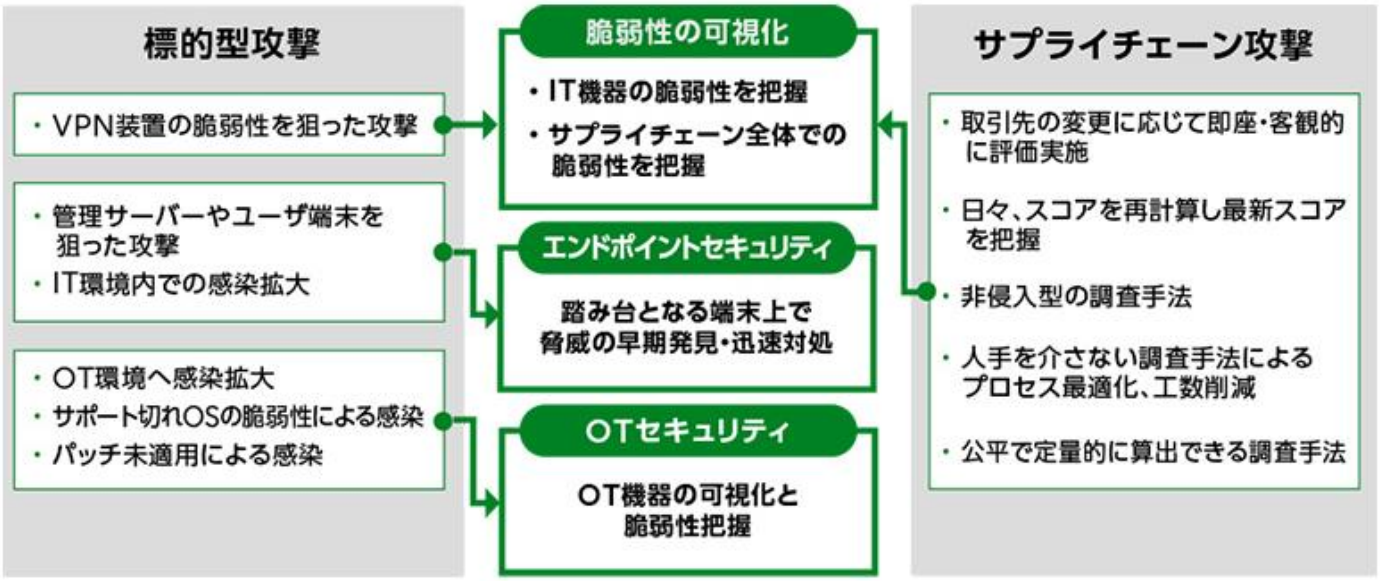


図５：標的型攻撃とサプライチェーン攻撃

3.1 IT 環境のセキュリティ対策

セキュリティ対策として行うことは多くありますが、直ぐにできることとしては、脆弱性をしっかりと潰しておくことがあります。そうした意味で、脆弱性を可視化し、その対策を打つということは大事です。

富士通では、サイバー攻撃の脅威からセキュリティのリスクを評価する「**セキュリティリスクレイティングサービス SecurityScorecard**」や、脆弱性を診断する「**脆弱性診断・管理サービス**」などを提供しています。

さらに、端末セキュリティを強化することも重要です。攻撃は端末から入ってくることが多いことから、端末で何が起こっているのかを迅速に検知し、テレワーク環境下においても遠隔で対処できることが必要となってきています。それを実現する仕組みが EDR(Endpoint Detection and Response)と呼ばれる対策です。富士通ではこれを実現するソリューションとして以下を提供しています。

- **Cybereason EDR サービス**
- **TrendMicro Apex One SaaS with XDR**
- **Palo Alto Networks Cortex XDR**

次に、工場を守るための OT セキュリティについて、解説します。

3.2 OT 環境のセキュリティ対策

生産現場というのはセキュリティに弱いものが多くあると捉えています。

生産現場に入り込んでくる脅威というものは、必ずしも生産現場そのものを狙ったものが全てではありませんが、実際に生産現場に入り込んでしまうと瞬く間に被害が広がってしまうリスクを秘めています。なぜなら、昨今の工場は既に様々なネットワークに繋がっていて、かつ脆弱なものが多いにもかかわらず、端末に簡単にウイルス対策ソフトを入れることができなかったり、セキュリティパッチを充てるための動作検証ができなかったりするためです。こういった実情を考えると、IT 領域もこれまで以上にしっかりと守りつつ生産現場のセキュリティ耐性も高めていくことが必要であると考えます。

そのためには、ソフトウェアに依存しない対策が有効です。その一つの方法として、ネットワークを外部から見るという対策があります。

富士通では、いつもの状態と違う「異常」を検知することにより、OT ネットワークを監視する「**OT ネットワークセキュリティ可視化サービス**」を提供しています。どの機器とどの機器が繋がっているかいつもの状態を把握したり、脆弱性を把握したり、さらには不正アクセスの検知を行います。(図６)

・いつもの状態を知る　(何が繋がっているのか/振る舞いとしてどこと繋がっているのか)

・そこに脆弱性が含まれているのか

・影響度はどの程度か

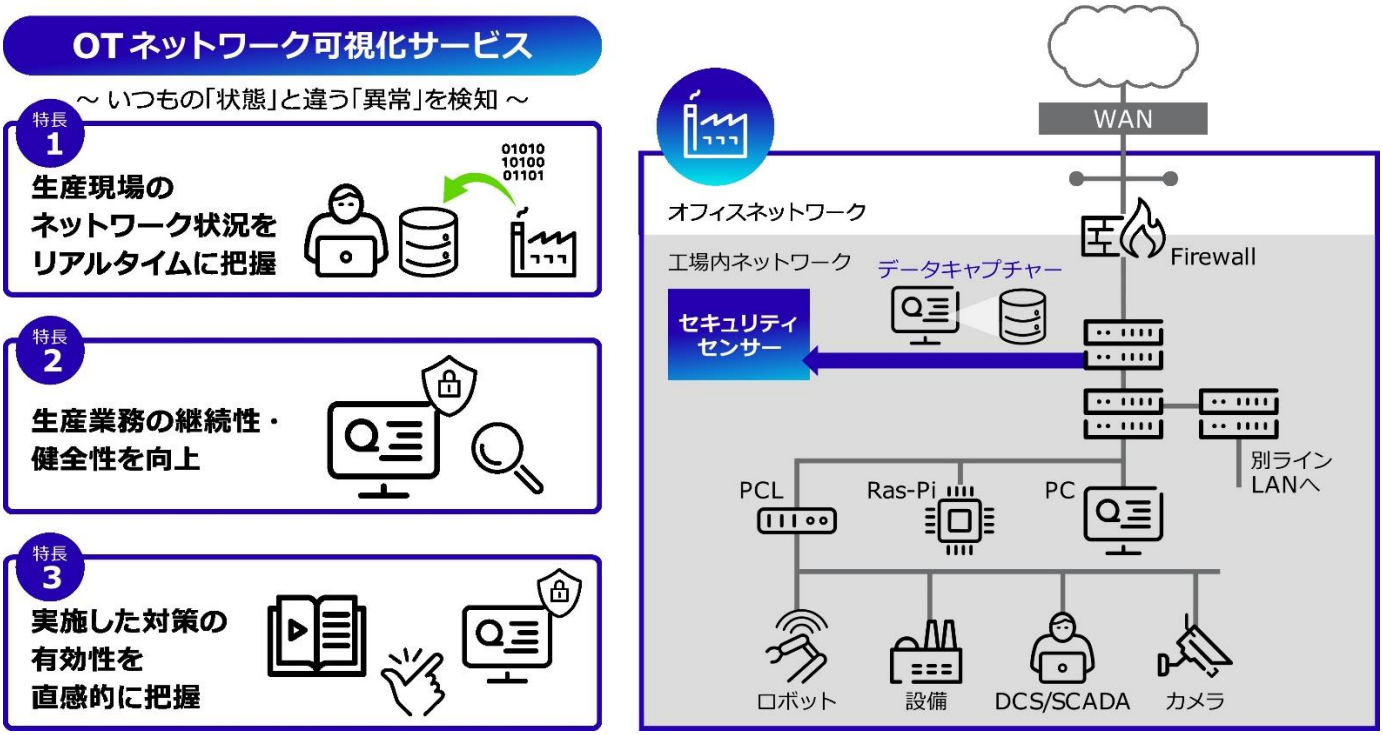


図６：いつもの「状態」と違う「異常」を検知（OT ネットワーク可視化サービス）

3.3 製造業におけるセキュリティ

現状を知り、そこから導き出されたリスク・脆弱ポイントをどの様に解決していくか、ネットワークのあり方も含めた構想を立案し、それにしたがって実際に環境を構築していくことが必要です。さらに、環境を作って終わりではなく、それを運用し、健全な状態を維持していくということまでお手伝いさせていただきます。

IT についても OT についても、セキュリティにおいては幅広く実施する必要があります。富士通では双方において総合的に対応できるよう、様々なソリューションをご提供しています。(図７)

図７：IT/OT ソリューション

さいごに

製造業をサイバー攻撃から守っていくためには、IT と OT のそれぞれの特性に応じたセキュリティが必要です。その両面を考慮した対応を行っていくことが必要であり、そのためには総合的に何をどこから行っていくべきなのか、検討していく必要があります。

製造業のセキュリティはこうした対応ができる富士通に、ご相談ください。

【ご参考】

OT ネットワークセキュリティ可視化サービス 詳しくはこちら

工場 IoT ネットワーク・セキュリティ 詳しくはこちら

Cybereason EDR サービス 詳しくはこちら

セキュリティリスクレイティングサービス SecurityScorecard 詳しくはこちら

お問い合わせ先

富士通コンタクトライン（総合窓口）

0120-933-200

受付時間 ：平日 9:00～12:00、13:00～17:30 (土曜・日曜・祝日・当社指定の休業日を除く)

富士通株式会社　https://www.fujitsu.com/jp/services/infrastructure/network/security/zero-trust/

【発行元】富士通株式会社
〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター