ビジネスの未来を守る

デジタル変革期にオペレーショナル インフラを守る

verizon business

ビジネスの未来を守る

イノベーションのスピードと安全性維持の両立は、綱渡りのように難しい課題です。ここでは、ビジネスを停滞させずに成長させるためのポイントを紹介します。

ビジネスにおける最大のチャンスには、しばしば最大のリスクが伴います。その最たる例がデジタル化の推進です。

デジタル変革は、生産効率の向上、製品品質の改善、顧客体験の向上、そして事業のレジリエンス強化を実現します。一方、デジタル化は、特に生産活動に重要なオペレーショナルテクノロジー（OT）領域において、意図しないサイバーセキュリティのリスクをもたらす可能性があります。

OTのセキュリティは、製造、石油・ガス、公益、物流など幅広い業種にとって最重要課題です。それはすべての業種が依存する重要なインフラにとっても不可欠であり、もちろん企業の利益にとっても同様です。

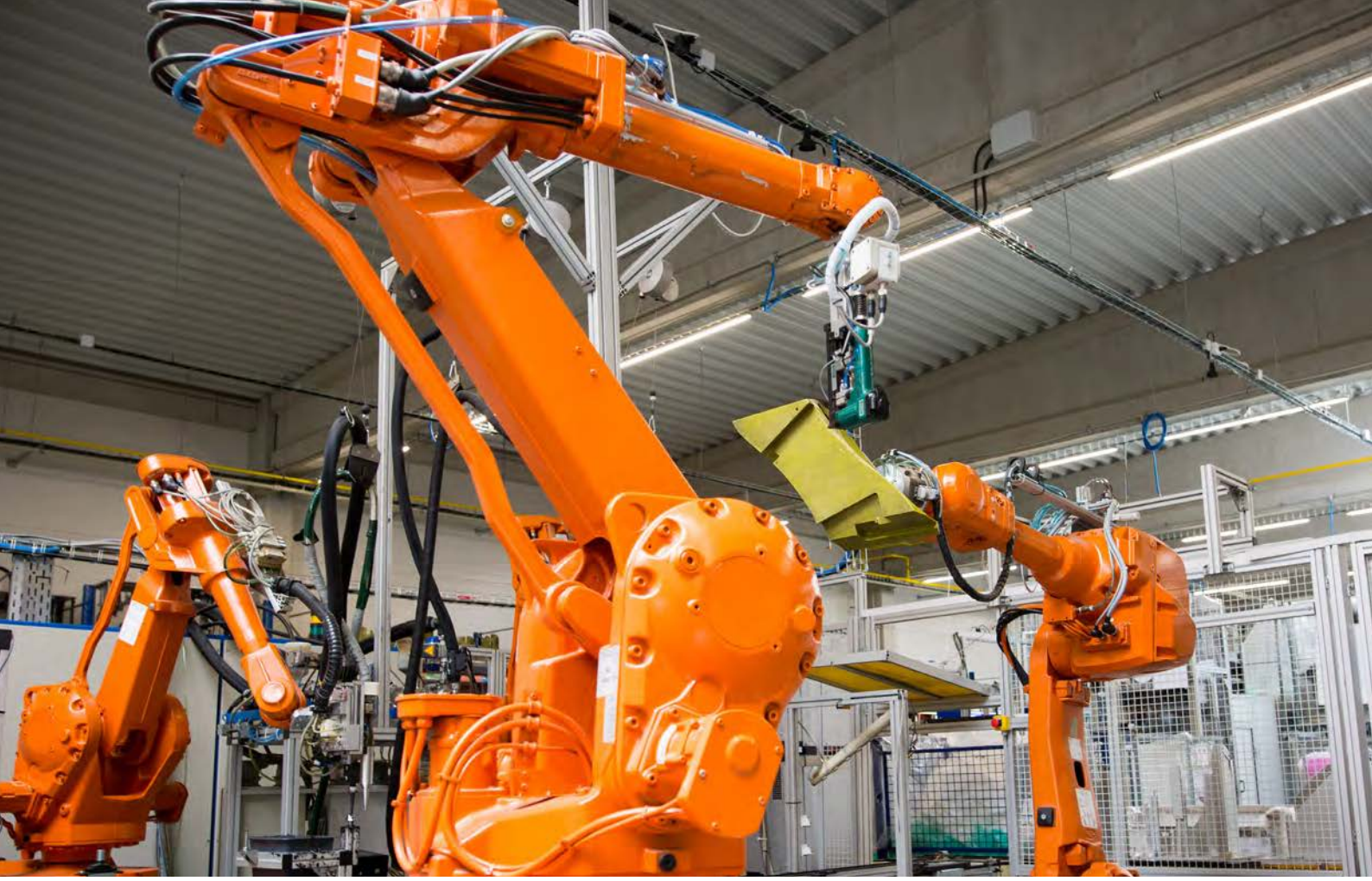
幸いにも、業種ごとに得られたデジタル化の重要な教訓の多くは、他業種にも応用することができます。つまり、ビジネスを無用なリスクにさらすことなくイノベーションを推進することが可能なのです。

それは、この課題を軽視してよいという意味ではありません。製造業が直面しているサイバーセキュリティの脅威は非常に現実的です。しかし、ここではデジタル化のメリットを享受しながらOTを保護するために実行できる、積極的かつ実用的な対策に焦点を当てます。

OTセキュリティに関する課題を認識していれば、それに対処することができます。ベライゾンはまさにお客様のビジネスを守り、成長させるためのサポートを提供します。

ベライゾンと共に包括的なサイバーセキュリティアプローチに取り組みましょう。

ベライゾンの包括的なITおよびOTセキュリティソリューションは、すでに世界中の多くの企業から信頼されています。私たちの包括的なサイバーセキュリティに対するアプローチは、お客様のビジネスニーズ、予算、デジタルトランスフォーメーションの目標に重点を置きます。



デジタル変革の必然性

読者の皆様にとっても、他の多くの製造業と同様に、デジタル変革が優先事項の上位にあると思われます。「マニュファクチャリング4.0（インダストリー4.0）」という概念が主流になって以来、この分野の変革のペースは加速しています。

> デジタル変革は、スループットを10％～30％向上させる可能性があります。
>
> 出典：McKinsey & Company, Preparing for the next normal via digital manufacturing's scaling potential, 2020

実際のところ、相互に"つながった"世界では、サプライチェーンに強靭性、俊敏性、最適化が求められています。そして、それは迅速なデジタル化を意味します。産業用モノのインターネット（IIoT）や人工知能（AI）などのテクノロジーは、急速に必須アイテムとなっています。これらを組み合わせることで、在庫を積極的に管理し、生産効率を向上させ、システム障害を軽減するために必要な透明性と連携が実現します。デジタルによる統合は顧客エンゲージメントの領域にも広がっており、満足度を高めてロイヤルティを強化するために必要な、リアルタイムのインサイト獲得とパーソナライゼーションを実現します。

デジタル化は運用効率の向上、さらには外部からの圧力への対応にも役立ちます。つまり、地政学的リスクや労働力不足により変化する需要に適応できる、柔軟でデジタル化されたオペレーションが必要なのです。デジタル化はまた、環境モニタリングの強化、エネルギーの最適化、規制遵守の実現も可能にし、消費者の期待とビジネス上の必然性の双方に合致します。

しかし、変革は必ずしもコストセンターである必要はありません。デジタル化は、無駄の最小化と予知保全による効率性の向上を通じて、大幅なコスト削減を実現します。ワークフローとプロセスのデジタル化は、価値をもたらしさらに多くのデータインサイトを生み出すことができます。これにより、より情報に基づいた意思決定が可能になり、市場の変化、規制の変更、予期せぬ事態への効果的な対応力が向上します。大きく変化する時代において、こうしたことはこれまで以上に重要です。

ただし、ビジネスが成長するにつれ、意図しない脆弱性が生じる可能性があることに注意する必要があります。

複雑さを増す脅威の状況

デジタルテクノロジーの応用拡大は、革新的な改善への扉を開いただけではなく、残念ながらサイバー攻撃の潜在的な脅威も拡大させています。

ITシステムとはこれまで独立していたOT環境の統合は、接続されたIIoTデバイスとAIの活用急増を伴って、防御しなければならない攻撃対象領域を大幅に拡大しました。

例えば、OTシステムは、最新のセキュリティテクノロジーが必ずしもサポートしていない、レガシーの通信プロトコルに依存していることがよくあります。多くのOTデバイスには、パッチが適用されていない脆弱性が残っており、今日のITシステムに一般的に見られる堅牢なセキュリティ機能が欠如している可能性があります。さらに、OTデバイスの運用寿命が長いため、古いソフトウェアやファームウェアが長期間稼働している可能性があり、セキュリティギャップがさらに深刻化しています。

> ITシステムと独立していたOT環境の統合は…防御しなければならない攻撃対象領域を大幅に拡大しました。

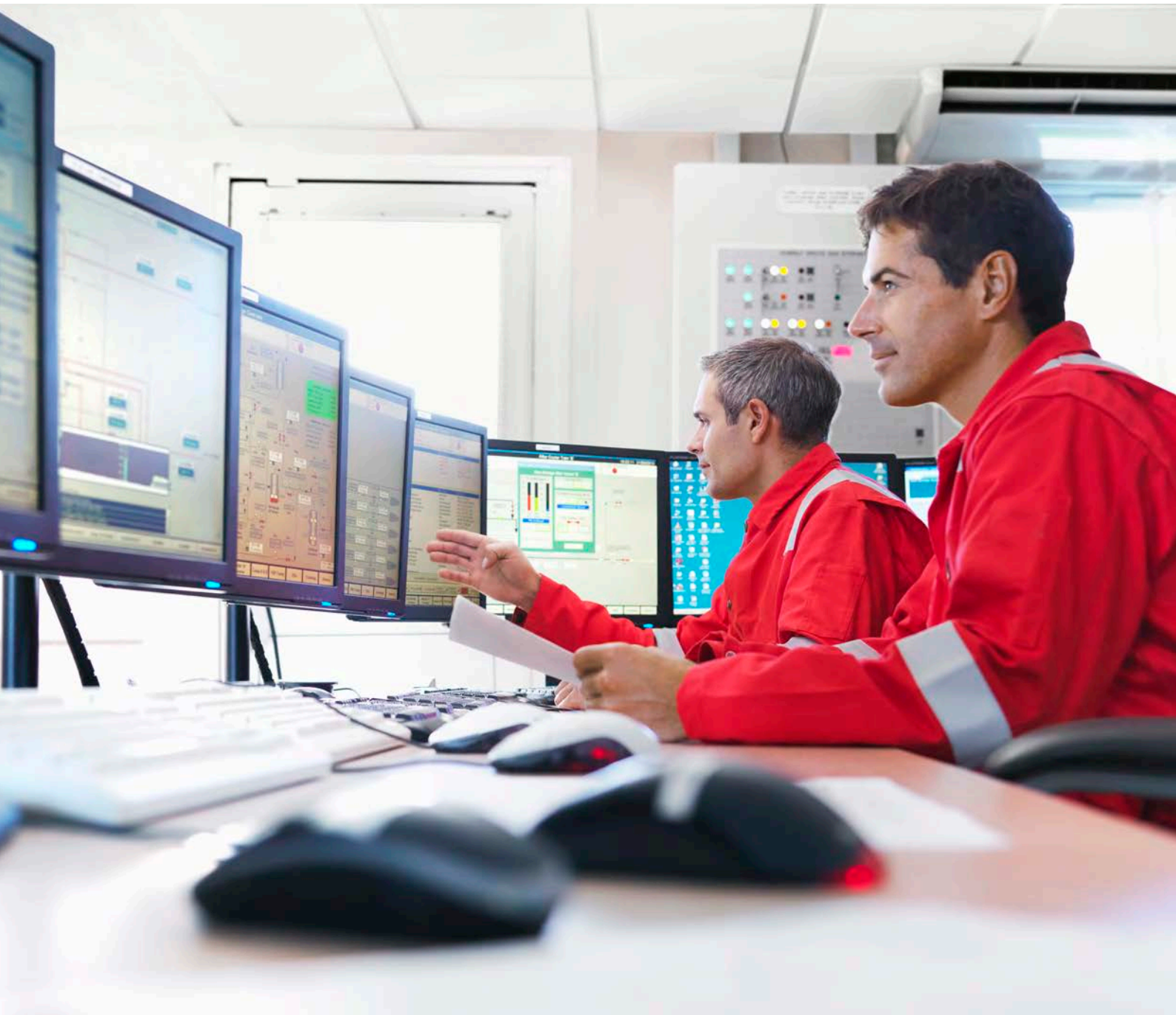
AIの登場は新たな攻撃ベクトルを生み出し、孤立したOTデバイスや機密データが外部、さらには人間以外の攻撃者に晒される可能性があります。これは少なくとも、より複雑なID管理環境を生み出すことになります。

AIツールをトレーニングし、活用していく中で、インフラへの侵入やデータの不正利用を防ぐための新たなセキュリティ機能と対策が必要になる可能性があります。企業が、多様な拠点にまたがってデータを生成、準備、処理、保管する必要性のバランスを取る上で、データ主権は重要な考慮事項となります。大量のデータを必要とするAIツールから知的財産と個人情報を保護することも最優先事項です。

準備を怠ると、大きな損失を被る

サイバー攻撃者は、製造業が操業停止に対して許容が極めて低いことも、企業の知的財産には大きな価値があることも知っています。製造業におけるシステム侵入が2025年に急増し、報告された件数が2024年からほぼ倍増したことは、決して驚くべきことではありません（ベライゾン、2025年度データ漏洩/侵害調査報告書（DBIR)による）。

- **フィッシングとソーシャルエンジニアリング**は、従業員を騙して機密情報を漏洩させたり、不正な操作を実行させたりするために利用され、多くの場合、ITネットワークとOTネットワークの両方にアクセスできる個人をターゲットにします。
- **サプライチェーン攻撃**は、サプライヤーとパートナーの複雑なネットワークの脆弱性を悪用します。
- **産業用制御システム（ICS）**への攻撃は、特に重要なインフラと生産オペレーションの妨害を狙った高度な攻撃です。
- **ゼロデイ攻撃**は、これまで知られていなかったテクノロジーの脆弱性を悪用するものであり、持続的かつ進化し続ける危険性をはらんでいます。
- 生産環境内の**管理されていない、かつセキュリティ対策が施されていないIoTデバイス**も、サイバー攻撃の侵入経路となります。



> 製造業におけるシステム侵入は2025年に急増し、報告された件数は2024年からほぼ倍増しました。
>
> 出典：ベライゾン、2025年度データ漏洩/侵害調査報告書（DBIR)

攻撃は、金銭的な損害に加え、生産活動への重大な影響、貴重な知的財産や機密データの窃取、物理的資産への損害、およびコンプライアンスに影響を及ぼす可能性があります。重要なインフラ分野では、このような攻撃が公共の安全そのものを脅かす事態に発展することさえあります。

これらのサイバーセキュリティの課題への対応は、複数の要因によって複雑化することがよくあります。急増するOTおよびIIoTデバイスの資産管理を正確かつ最新の状態に保つことは、大きなハードルとなる可能性があります。また、IT分野と比較して、OTやIIoTインフラへの攻撃に特化した脅威インテリジェンスは不足しています。IT環境と生産環境の間に存在する優先順位と文化の根本的な違いは、OTにおけるサイバーセキュリティ対策の効果的な導入を阻害する要因にもなります。

企業がデジタル変革の一環としてITとOTの連携強化を目指す場合、セキュリティ対策も整合させる必要があります。

世界中の製造業が取り組むべき課題

製造業は、複雑かつ地理的に分散したITおよびOT環境が数多く存在します。これらの複雑なシステムには、最新テクノロジーとレガシーテクノロジーが混在し、相互接続された膨大な数のデバイスが含まれるため、セキュリティ管理において大きな課題が生じています。

こうした大規模かつ複雑なオペレーションでは、高度で統合的なサイバーセキュリティのアプローチが求められます。

これまで分断されていたネットワークや運用文化を統合し、ITとOTの部門間に存在する文化および業務的なギャップを克服することが、統一されたセキュリティ体制を構築する上で重要です。

製造業は、複雑でしばしば長大なサプライチェーンに依存しています。このグローバルなサプライネットワークは相互に接続されているため、サプライチェーンのどの部分でセキュリティ侵害が発生しても、事業全体に連鎖的な悪影響が生じる可能性があります。製造業では、すべてのサプライヤーが厳格なセキュリティポリシーに従って事業を運営し、リスクを最小限に抑える必要があります。

サイバー攻撃への対応を怠ると、この分野において非常に現実的で深刻な結果を招く可能性があります。企業だけでなく、その周囲の環境やコミュニティにも悪影響を及ぼします。例えば、オフィス業務が基本の企業であれば、サイバー脅威を封じ込めるためにシステムをシャットダウンするだけで済むかもしれませんが、冷却システムや電力システムといったOTシステムは安全確保のために稼働を継続しなければならない場合があります。物理的な産業災害を防ぐことは常に最優先事項です。

ITとOTの部門間に存在する文化および業務的なギャップを克服することが、統一されたセキュリティ体制を構築する上で重要です。

継続的なオペレーションという商業的な圧力は、セキュリティ対策の妥協につながることもあります。経営陣は必要なアップデートの実施やメンテナンスのためのシステム停止を躊躇し、サイバー攻撃に対する脆弱性を高めてしまう可能性があります。

また、最新のセキュリティテクノロジーや専門人材への投資を制限する予算上の制約に直面する企業も少なくありません。世界中に分散している多数の拠点や多様な事業部門にセキュリティリソースを効率的に割り当てることは、大きな課題となります。特に、サイバーセキュリティ予算がオペレーション全体ではなく、IT部門に集中している場合、これは顕著です。ビジネスのあらゆる領域に適切な保護を提供するためには、OTとITの予算を統合する必要があります。

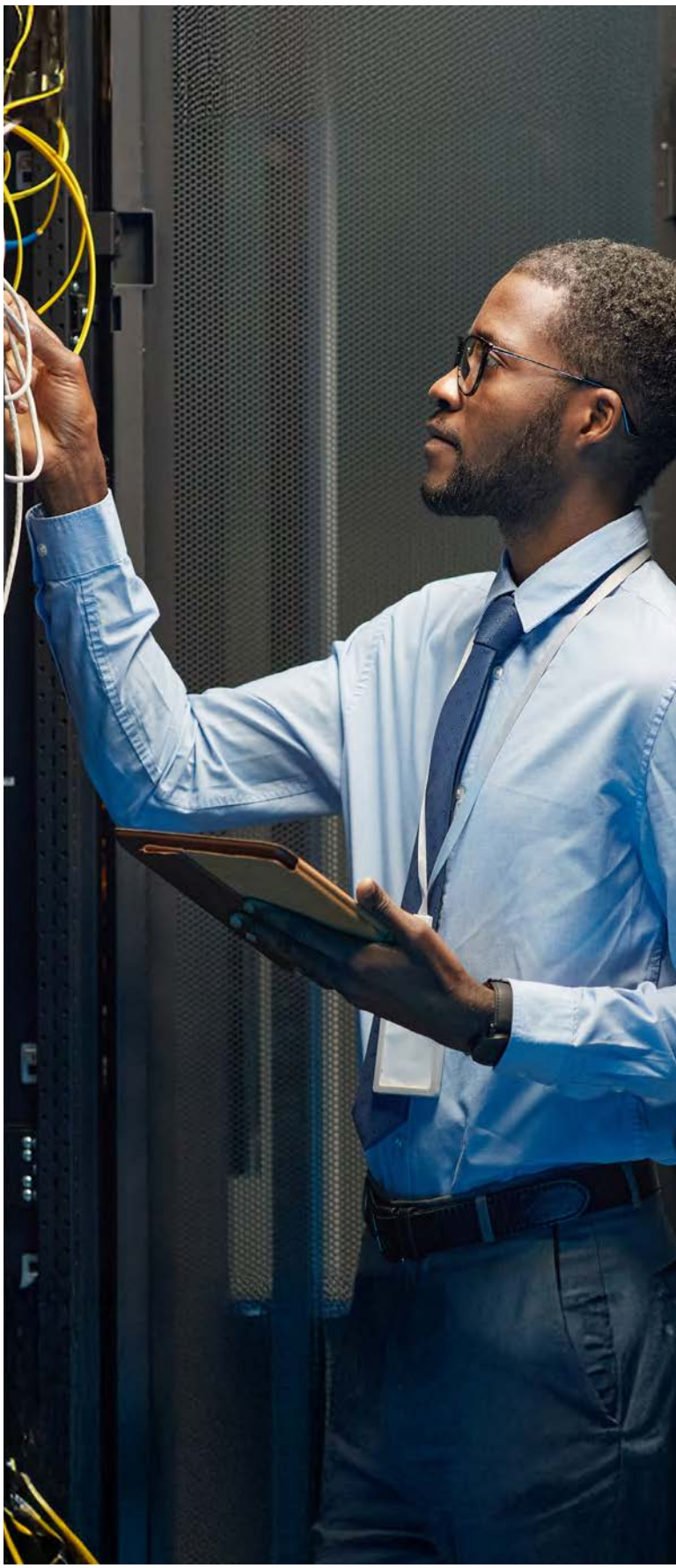
また、レガシーのOTシステムが生産プロセスに深く組み込まれているという問題もあります。これらの古いシステムはアップデートが困難でコストもかかるため、重大なセキュリティ上の脆弱性が生じる可能性があります。生産を中断ぜずに、OT環境におけるこうした技術的負債に対処するには、綿密な計画、専門知識、そして段階的な最新化へのアプローチが必要です。

今日のサイバー脅威についてグローバルな視点で把握しましょう。

ベライゾンが毎年発行している「データ漏洩/侵害調査報告書（DBIR）」は、進化するサイバーセキュリティの状況に関する信頼できる情報源であり、データ主導のセキュリティアプローチへのベライゾンの取り組みを反映しています。

サイバーセキュリティ侵害に関して信頼性の高い情報を提供するDBIRは、製造業をはじめとする様々な業種における主要なリスクを明らかにし、それらを軽減するためのエキスパートのアドバイスを提示しています。2025年度のレポートだけでも、22,000件を超える実際のインシデントを分析し、巧妙化する脅威への防御力を高める実用的なインサイトを提供しています。

ぜひ、今すぐ報告書をダウンロードしてください。



エンドツーエンドのサイバーセキュリティで、より安全なOT環境を実現

信頼できる専門パートナーの存在は、OTサイバーセキュリティの複雑さを大幅に軽減できます。

ベライゾンは、企業のサイバーセキュリティ対策の強化を支援してきた実績があります。ITインフラだけでなく、相互接続が進むOT環境も守るエンドツーエンドの保護を提供します。

ベライゾンは、豊富な経験と実績に加え、他のセキュリティリーダー企業と連携し、専門的なOTセキュリティを提供しています。こうした協業により、お客様がデジタル変革を進める中で、常に変化する特定のニーズに対応する最適なソリューションを提供します。

お客様のビジネスにとって重要なOTインフラを、業界最高水準のセキュリティで守りたいとお考えなら、ベライゾンが現地診断を実施し、費用対効果の高い即効性のある改善領域を特定することが可能です。

OTは、お客様のビジネスの心臓部です。今こそ、その守りを確かなものにしましょう。

ケーススタディ：近代的な製造業のセキュリティを確保

世界的なスピリッツ、ワイン、ソフトドリンクメーカーであるこの企業は、自社のセキュリティインフラがコネクテッドテクノロジーの進化に追いついていないことに気づきました。同社はベライゾンと連携し、セキュリティコントロールの緊急アップデートを実施し、変化するビジネス環境への適応、およびデータが実際に存在する場所に近い層でのセキュリティ強化を図りました。

ベライゾンが取り組んだこと

- 新しいオンプレミスファイアウォールの導入およびポリシー/ゾーンの再構成
- Verizon Managed Security Servicesによる管理業務の引継ぎ
- 世界中の20以上の工場向けにOTおよびIT LANをセグメント化
- 生産への影響を最小限に抑えながらセキュリティポリシーを相互適用

成果として実現したこと

- 将来の成長に向けた新しいセキュリティ環境の構築
- セキュリティデバイス監視の改善
- ITとOTネットワークの分離によるサイバーリスクの軽減
- デバイスと業務フローの可視性の向上

デジタル変革についてさらに詳しくお知りになりたい方は

業界のエキスパートによる重要なインサイトをお読みいただき、最新テクノロジーを統合して完全に"つながった"企業を実現する方法を、ぜひご確認ください。

ベライゾンの製造業向けソリューションの詳細

ベライゾンのイノベーションセンターで、製造業に競争力をもたらす最新の変革ツールを、ぜひご体験ください。

イノベーションセンターの詳細

OT環境を保護する方法についての詳細はこちらをご確認ください。

ホワイトペーパーをダウンロード