ホワイトペーパー

OTセキュリティへの包括的アプローチ

オペレーショナルテクノロジー（OT）の新たなサイバーセキュリティ課題

verizon business

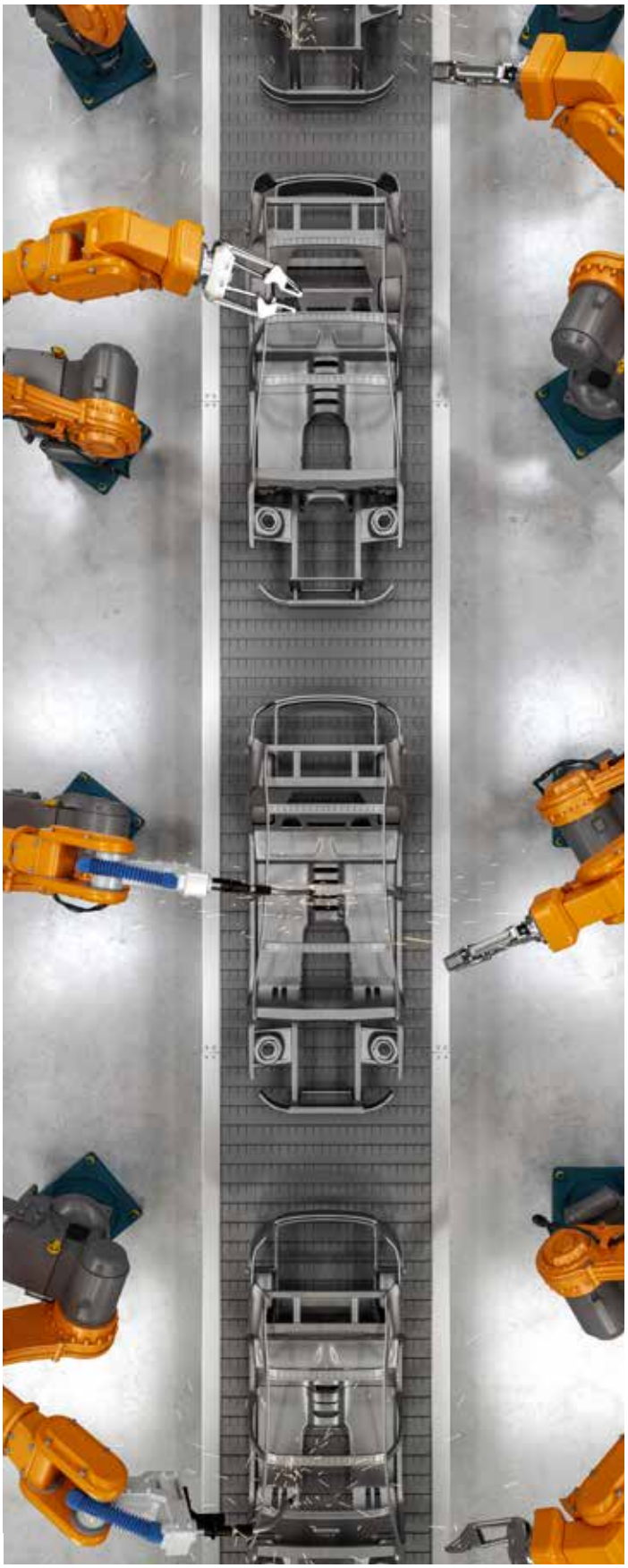
インダストリー4.0の進展によって形成された今日の産業環境では、スピード、安全性、そしてレジリエンスを兼ね備えたサービスとシステムが求められています。組織はOTセキュリティを最優先事項とし、あらゆる潜在的な問題に対処するための適切な監視および対応の体制を確立する必要があります。

なぜなら、OTアプリケーションとOTデバイスを相互接続することで組織は強化されますが、悪意あるユーザやサイバー攻撃者の侵入経路を拡大してしまう可能性があるからです。

従来、OTネットワークはセキュリティと信頼性の観点から、ITネットワークやインターネットから独立していましたが、今やその前提は崩れています。

このホワイトペーパーでは、統合されたOTネットワークをビジネスリスクではなくビジネスを支える力として位置づけ、その安全を守る方法を解説します。

OTセキュリティ市場では、資産の識別、脅威と脆弱性の検知に重点が置かれていますが、防御の重要性を忘れてはなりません[1]。



インダストリー4.0における サイバーセキュリティの再考

インダストリー4.0、つまり第四次産業革命は物理、デジタル、そして生物的領域の境界を曖昧にするテクノロジーの融合を特徴としています。

この新たな環境では、組織は自律ロボット、ほぼリアルタイムのリモートコントロール、エッジコンピューティング、高度な接続のテクノロジーなど、あらゆるものの導入を進めています。クラウドと密接に絡み合っているこのような進化した運用には、セキュリティアーキテクチャを根本から見直すことが求められます。例えば、厳格なセキュリティコントロールにはゼロトラストアクセスが必須となるでしょう。

1. The Forrester Wave™:Operational Technology Security Solutions, Q2 2024; Forrester

しかし、これを負担と捉えるべきではありません。むしろ、ビジネスアーキテクチャの簡素化および最適化を進める新たな機会とも捉えられます。この再構築のメリットの1つは、分析のための膨大なデータセットを収集できることです。これは、インシデント対応から製品の改善まで、あらゆる業務の強化に役立ちます。

進化するビジネスの推進力がもたらす新たなリスク

OTの進化

組織がさらなる効率化を追求する中、OTはクラウド上でITと連携する方向へ進んでいます。また、企業はセキュリティ管理とコスト効率の観点から、予知保全や自動化のためにAIを活用し始め、サードパーティとの協業モデルを再考し始めています。

> 80%のCIOが、俊敏性とインサイト主導のビジネスのために、2028年までにAIと自動化を導入する見通しです。
>
> 出典：**CIO Predictions** in Asia/Pacific* for 2024 and Beyond Revealed by IDC

ITとOTの融合が生むリスク

従来の典型的なOTシステムは、サイバーセキュリティを考慮して設計されていないため、ITとOTのネットワーク間での相互接続が増すと、攻撃対象領域が拡大してしまうのです。

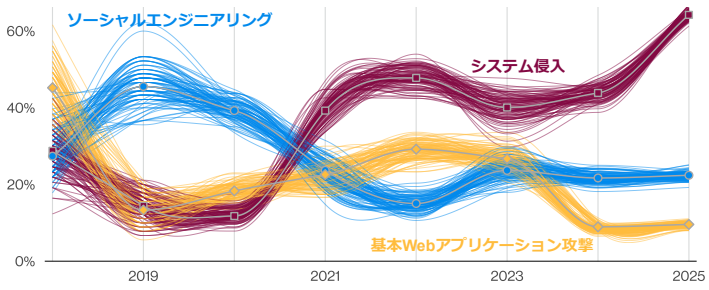
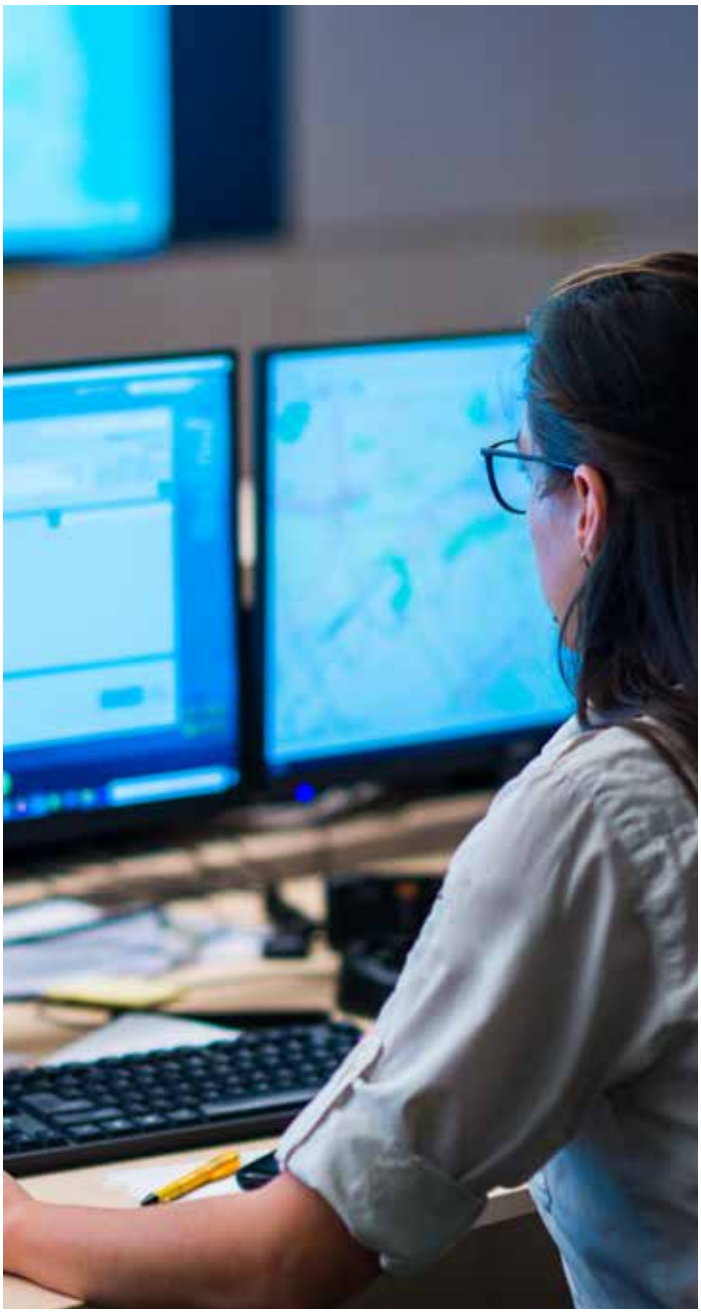


図1：製造業におけるデータ漏洩/侵害の主な攻撃パターンの経時的変化

出典：2025年度DBIR

この傾向はすでに顕著に表れています。ベライゾンの2025年度データ漏洩/侵害調査報告書（DBIR）によると、2020年以降、世界的にシステム侵入が大幅に増加しています。 特に製造業では、この1年で著しい増加が見られました。この業種ではデータ漏洩/侵害も大幅に増加しており、中小企業では今年、1,607件が報告されています。

金銭目的の外部攻撃者が依然として主な脅威となっている一方で、スパイ活動が製造業におけるデータ漏洩/侵害の約20%となっていることは注目に値します。これは前年のわずか3%から大幅な増加です。



レガシーシステムとパッチ未適用システム

多くのOT環境では、ベンダーのサポートが不足しているか、全くサポートされていない、旧式のオペレーティングシステムやソフトウェアに依存しています。ダウンタイムや生産停止への懸念から、OTシステムのパッチ適用やアップデートが難しい状況になっています。

可視性と資産管理の欠如

組織では、多くの場合、接続されているOT資産の正確な管理ができておらず、リスク評価が困難になっています。シャドーOTデバイス（管理外のOTデバイス）や文書化されていないエンドポイントは、未知の脆弱性をもたらす可能性があります。

ランサムウェアとサイバー脅威

ベライゾンの2025年度DBIRによると、ランサムウェア攻撃が製造業におけるデータ漏洩/侵害で最も大きな影響を与えています。攻撃者は、ITとOT間の脆弱なセグメンテーションを悪用し、そこから展開して他の業務に損害を与える傾向があります。

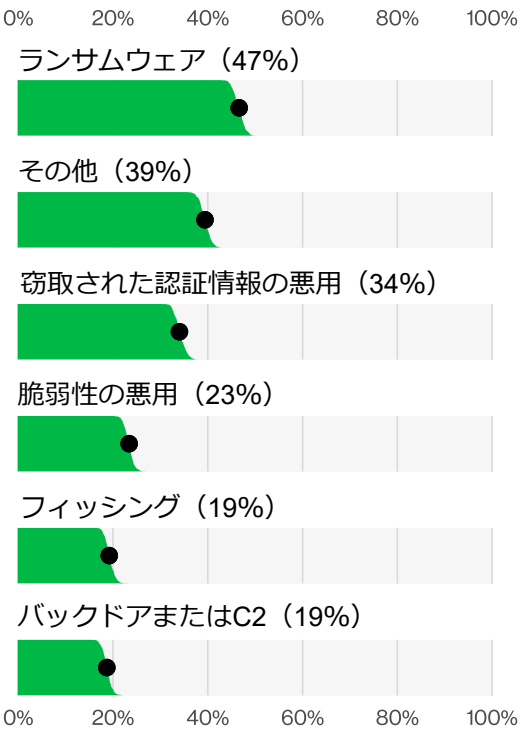


図2：製造業におけるデータ漏洩/ 侵害の主な攻撃の種類

出典：2025年度DBIR

2025年度のDBIRで調査対象となった全データ漏洩/侵害のうち、ランサムウェアによるインシデントは44%に上り、前年の32%から増加しています。しかし、この増加にもかかわらず、支払われた身代金の中央値は15万ドルから11万5000ドルに減少しています。これは、身代金の支払いを拒否する被害組織が増加したことに関係している可能性があります。

ランサムウェアは、中小企業（SMB）におけるデータ漏洩/侵害の88%を占めており、特に深刻な影響を与えています。一方、大企業では39%に留まっています。

複雑な規制とコンプライアンス

組織は、米国国立標準技術研究所（NIST）、IEC 62443、サイバーセキュリティ・社会基盤安全保障庁（CISA）のガイドラインなど、複数のサイバーセキュリティフレームワークと業界規制に準拠する必要があります。グローバルサプライチェーン全体にわたるコンプライアンス確保は、特に中小企業にとって、さらに複雑な課題となります。

サードパーティおよびサプライチェーンのリスク

多くのベンダー、請負業者、サプライヤーが関与することで、接続されているOTネットワーク全体に複数のサイバー攻撃ポイントを生み出すことになります。あらゆる種類のリモートアクセスには、ID管理とゼロトラストアクセス管理による厳格な制御が不可欠です。

スキルと人材のギャップ

OTセキュリティの専門知識を持つサイバーセキュリティのエキスパートが不足しています。また、新規採用のスタッフは、サイバーセキュリティに関する認識が不足している可能性があり、その結果、内部脅威や人的ミスのリスクが増大するおそれがあります。

OTセキュリティ戦略の構築

NIST CSF、NIST 800-53、ISO 27K、IEC 62443、NIST 800-82、北米電力信頼度協議会重要インフラ保護基準（NERC CIP）などのフレームワークは、あらゆるサイバーセキュリティプログラムの管理に対する一貫したアプローチの提供や、組織に最適化されたカスタマイズのOTセキュリティ戦略の構築に非常に役立ちます。

図3：包括的なOTセキュリティ戦略の要素

出典：ベライゾン

簡素化されたOTセキュリティ戦略には、少なくとも以下の要素をガバナンス構造に組み込む必要があります。

- 保有機器、経過年数、サポート終了情報、ソフトウェアまたはファームウェアのバージョンを把握するための包括的な資産管理フレームワーク
- セキュリティ上の弱点やギャップを特定するための、OTネットワークに対する定期的なセキュリティ評価
- クラウド上のアプリケーションへの簡素化されたアクセスが可能な、IT DMZ（非武装地帯）を備えた多層ネットワークアーキテクチャ
- OTネットワークの検知能力を向上させるための継続的な脅威監視。これによりネットワーク層とアプリケーション層の両方を網羅し、YARA（Yet Another Recursive Acronym）ルールを用いてOT特有のマルウェアを検出します。
- 早期の攻撃検知と防御を可能にするOT特化型脅威インテリジェンス。これは、公開および政府機関の脅威インテリジェンス、業界固有の脅威フィード、オープンソースおよびコミュニティのフィード、ベンダーおよび民間の脅威フィードの組み合わせで構成されるものです。
- 脅威の早期検出を可能にする、適切に設計されテストされたインシデント対応計画（IRP）

OTセキュリティフレームワークの変革フェーズ

次ページの図は、理想的なOTネットワークセキュリティ構築プロセスの例です。ベライゾンが支援させていただく場合も、基本的にはこのステップに沿って実施いたします。

お客様は、自社のニーズと運用成熟度に最も適したフェーズから開始することが可能ですが、並行してOTガバナンスと組織における以下の領域に重点を置く必要があります。

- イノベーションおよび将来の開発に関わる組織的側面
- 企業および事業部門レベルでの経営戦略立案と実行
- OTプランニングと実行を成功させるために、工場またはグループごとにOT推進リーダーを選出

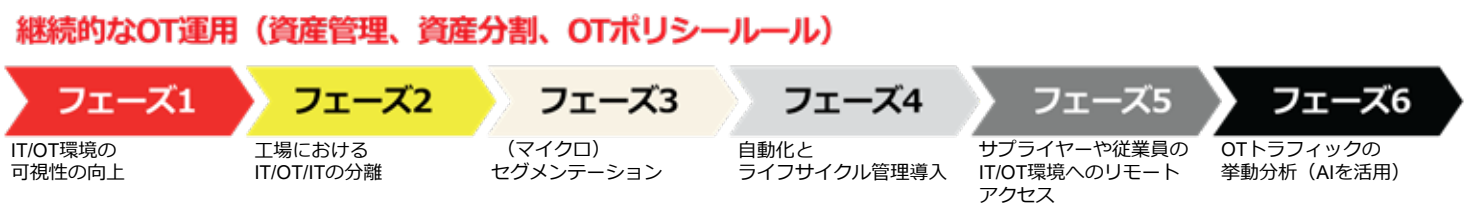


図4：OTセキュリティフレームワークの変革フェーズ
出典：ベライゾン

フェーズ1：OT環境の可視性の向上

ベライゾンのセキュリティコンサルティングサービスは、工場や倉庫などの環境におけるITおよびOTデバイス間の相互接続状況を明確化することを目指します。これは、包括的な工場資産の確認と評価を通じて実現されます。OTデバイスとそのリスク要因の完全な可視化のため、現地またはリモートで実施されます。

フェーズ2：ITとOTの分離

ベライゾンはお客様と協力し、基本的な保護制御を活用してOTネットワークをITネットワークから分離します。

この分離作業は、物理あるいは仮想ファイアウォールの導入または再利用によって実現します。少なくとも、以下のセキュリティコントロールを有効にする必要があります。

- 脅威防御
- マルウェア対策
- ドメインネームシステム（DNS）保護

ベライゾンの認定エキスパートがセキュリティコントロールの実装と設定をサポートし、マネージドサービスチームがベライゾンのセキュリティオペレーションセンター（SOC）から運用を監視します。

フェーズ3：マイクロセグメンテーション

OT環境内のセグメンテーションを実施します。これは、企業施設全体で再利用可能なカスタムブループリントを作成することで実現され、標準化と簡素化を促進します。このフェーズでは、セキュリティゾーニングとポリシーの明確化が図られます。ベライゾンのセキュリティコンサルティングサービスが、既存のセキュリティコントロール（フェーズ2）に基づいてこれらのブループリントを開発し、実装します。

フェーズ4：自動化とライフサイクル管理導入

このフェーズでは、利用可能なツール、チケットシステム、またはスクリプト開発を活用して、シームレスなOTセグメントルールの作成および更新のための特定OTプレイブック開発を開始します。

また、デバイスを必要なセキュリティコントロールに準拠した状態に維持するためにライフサイクル管理が導入されます。適切なメンテナンスが不可能なデバイスは、専用セキュリティゾーンに隔離されます。

フェーズ5：サプライヤーや従業員のOT環境へのリモートアクセス

このフェーズでは、ゼロトラスト（need-to-know原則）ベースでの最新のリモートアクセスサービスを導入します。その後、従業員や様々なサプライヤーのアクセス制御を実装し、エージェントベースおよびブラウザベースのソリューションをサポートします。

フェーズ6：高度な（主にAI主導）セキュリティコントロールと自動化の有効化

AIを活用したセキュリティコントロール、例えばデータ損失防止（DLP）、侵入防止システム（IPS）、ユーザおよびエンティティの行動分析（UEBA）サービスは、ITおよびOTストリームにおける可視性をさらに高めることができます。これらの情報は、OTプレイブックの新規作成や既存プレイブック更新に活用できます。また、OTインシデント対応サービスの改善や、OT欺瞞ベースの防御サービス開発にも役立ちます。

OT環境向けの推奨運用モデル

ベライゾンは製造業の変革プログラムの経験を活かし、新しい時代にふさわしい組織モデルを提案することができます。

下の図は、ベライゾンがこれまでのIT/OT変革プログラムで活用し大きな成功を収めたモデルを示したものです。

もちろん、これはすべての組織に有効な万能モデルではありません。短期的な目標達成には、望ましいビジネス成果に合ったモデルの採用が求められるかもしれません。また、明確な長期ビジョンの実現には、組織とすべての業務プロセスの再構築が必要な場合があります。

提案された組織モデルでは、グループの最高情報責任者（CIO）が、全社横断のテクノロジーと関連リソースを一元管理し、事業部門に提供される共通サービスの責任を負います。各事業部門には、部門固有のOTを担当する最高技術責任者（CTO）またはCIO機能が設置されます。

事業部CIOは所属部門に報告する一方、グループCIOにはマトリクス方式で報告し、同時にCIO委員会にも参加します。CIO委員会の目的は、テクノロジーに関する全社的な整合性とガバナンスを確立することです。最高情報セキュリティ責任者（CISO）は、CIO委員会のメンバーとしてセキュリティ機能の責任を負います。

セキュリティサービスプロバイダーであるベライゾンは、マネージドトランスフォーメーションおよび運用引継ぎサービスをはじめとする、マネージドセキュリティサービス全般の提供が可能です。これにより、お客様は自社の差別化領域に注力できるようになります。

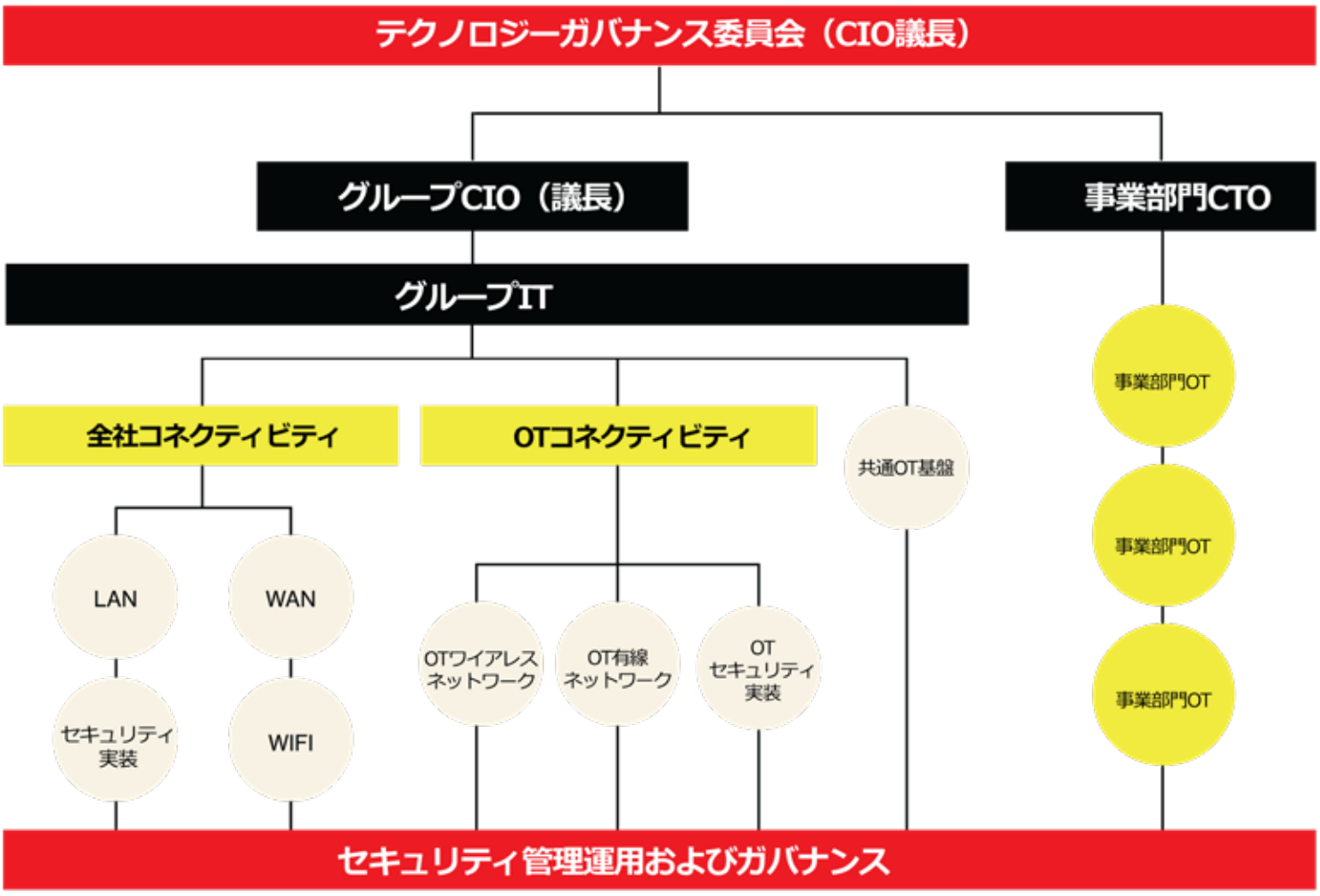


図5：共通/グループテクノロジー運用モデル
出典：ベライゾン

結論

OTセキュリティに対するこうした包括的なアプローチにより、企業はビジネスニーズと予算に対応した適切なセキュリティ体制を実現できるのです。ベライゾンは、お客様がサイバー脅威への万全の備えを確立するためのお手伝いをいたします。

詳細はこちら

ベライゾンによるサイバー脅威の軽減およびお客様のビジネスの保護ついては、ベライゾンのアカウントマネージャーにお問い合わせいただくか、verizon.com/business/ja-jp/solutions/secure-your-businessをご確認ください。

著者および寄稿者

著者

Marc Borking、ベライゾンビジネス、コンサルティングサービス、OT SME兼主席セキュリティコンサルタント

寄稿者

Ashish Khanna、シニアディレクター兼EMEAセキュリティコンサルティングサービス責任者

Stephen Young、セキュリティコンサルティングサービス、ディレクター

Beat Kueng、EMEAセキュリティソリューションアーキテクチャ担当アソシエイトディレクター

Chris Zijderveld、セキュリティコンサルティングサービス、アソシエイト ディレクター

Ali Akl、EMEAセキュリティコンサルティングサービス、リスクおよびレジリエンス責任者

David Samreth、コンサルティングサービス、主任コンサルタント

ケーススタディ：
グローバルで展開する製造業

グローバルで展開するこの製造企業では、オペレーション全体で自動化の導入を進める中、ITシステムとOTシステム間の通信量が急増し始めましたことが明らかになりました。これに伴い、セキュリティリスクの増大および攻撃対象領域の拡大が顕在化しました。人、データ、インフラの保護に重点を置きながら成長を続けるために、まず同社はプロアクティブな対策として、既存のOT環境の包括的なセキュリティ評価を実施し、いくつかの重要課題を特定しました。

ビジネス上の重要課題：

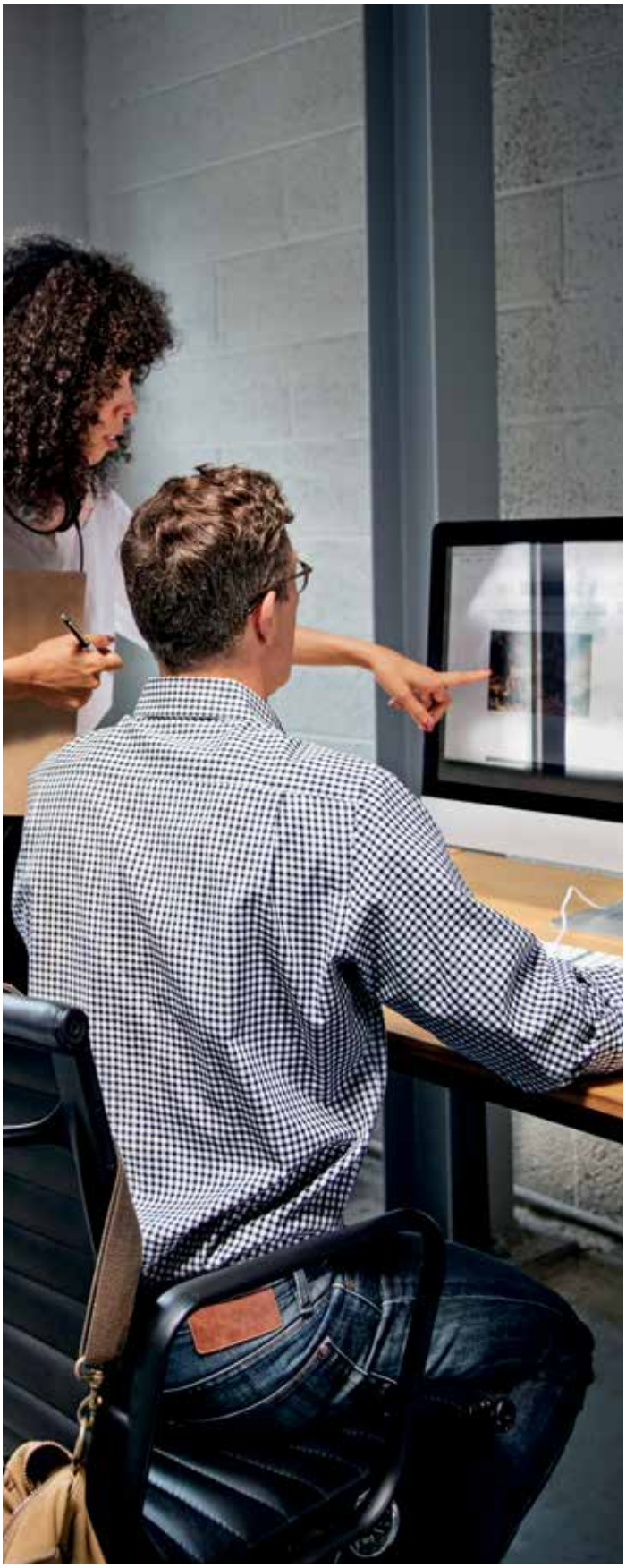
- 目的に合わなくなった既存のセキュリティインフの更新
- 現行アーキテクチャ、セキュリティ要件、セグメンテーションポリシー、業務フロー、デバイス、プロセスの明確化
- セグメンテーションの欠如によるセキュリティリスクの把握
- ビジネス資産保護のためのセキュリティコントロールの実装
- セキュリティ体制とポリシーの整合化
- 巧妙化するグローバルでのセキュリティリスクの軽減
- 将来の成長およびコンプライアンスに備えた環境の整備

ソリューション：

- 各工場でのオンサイト調査とOT評価を実施
- 構成管理データベース構築と適切なアーキテクチャ設計：セキュリティポリシーテンプレートおよびOT/ITセグメンテーションテンプレートの作成
- オンプレミスのファイアウォールを再利用または新規導入して、新しいポリシー、セグメントおよびゾーンを構成した上で、ベライゾンのマネージドセキュリティサービスへ運用委託
- 世界中のすべての工場（25拠点以上）にLANセグメンテーションを適用し、IoTを可視化
- 段階的なアプローチでセキュリティポリシーを微調整
- OTセグメンテーションの作成と簡素化のためにプレイブックを自動化

メリットと成果:

- ITとOTネットワーク、およびOTとOTのセグメント間を分離することで、サイバーリスクへの対応を強化
- ベライゾンのマネージドセキュリティサービスによるセキュリティデバイス監視の改善
- デバイスと業務フローの可視性の向上
- 新たな規制や世界的な脅威の状況に合ったコンプライアンス強化
- 将来の成長を支える新しいセキュリティ環境の構築



得られた教訓:

理論的には合意されていた内容でも、実践には必ず時間がかかります。これはほとんどのプロジェクトでよくあることです。今回のケースでは、クライアントはプロジェクト開始前にスコープを変更する必要がありました。そして、ゴーサインが出た後でも、必要なデータの収集、適切な人材の確保、適切なスイッチの選定、そして正しい構成の実装に予想以上に時間がかかりました。また、ビジネス上の優先事項における綱引きにより、リードタイムが長引くこともありました。

クライアントサイドからのサポート

一旦専任チームが編成されると、プロジェクトは加速し始めました。1か所の設定が完了すると、プロセスや設計、潜在的な問題に関して得られた教訓を次の拠点に適用でき、作業効率が向上しました。ネットワークにおけるトラフィックとデータの取得（SPANポート経由）も課題であり、マイクロセグメンテーションは業務への影響を考慮して時間を掛けました。資産におけるデータフローが常に把握できるとは限らず、拒否ルールを有効化する前に複数のファイアウォールログ分析を実行する必要がありました。さらに、旧式のスイッチが設定や追加負荷に対応できないため、資産の検出が困難でしたが、トラフィックをファイアウォール経由に切り替えることで解決できました。

連携、情報共有、参画、意欲喚起

連携の調整が極めて重要だということが明らかになりました。自動化では、プレイブックが設計どおりに機能することを確実にするため、さまざまなチーム間の連携が必要でした。

機器ベンダーは、多くの場合デバイスへの広範なアクセス権を持っていることがわかったので、アクセスをセキュアシェル（SSH）、リモートデスクトッププロトコル（RDP）、またはブラウザベースなどに制限する必要がありました。

アーキテクチャの変更をタイムリーに実施するためには、ベンダーへの明確かつ直接的なリクエストを行う必要があります。また、トラフィックの収集と分析には多くのリソースが必要となるため、適切な計画と予算確保が不可欠です。

フェーズ別変革の詳細

フェーズ1

- 主要な連絡先を明確にすることで、コミュニケーションを効率化し、すべてのプロジェクトの整合性を保つことが保証できました。
- 初期段階の要件洗い出しと構成は徹底的かつ細心の注意を払って行いました。
- ファイアウォール経由でデータをルーティングするソリューションの構築によって、ネットワークトラフィック取得の課題にうまく対処しました。
- プロジェクト開始日の調整はありましたが、これにより、より包括的で整合性のとれた最終計画を立てることができ、結果的には実装を成功させることができました。

フェーズ2

- ファイアウォールの初期導入時には、地域における制約や政府の規制に対処することが主な課題でした。
- すべての法的要件を満たし、全地域で法令に準拠した導入を確立できました。
- 初期のセグメンテーションでは慎重な段階的導入を実施しましたが、これは他の拠点に向けたスムーズで加速的かつ再現性のあるプロセスの開発に必要不可欠でした。

フェーズ3

- マイクロセグメンテーションの第2段階では、業務の中断を避けるために慎重かつ段階的なアプローチが必要でした。
- 成功の鍵となったのは、現地から得られるインサイトでした。
- 正確を期すために、詳細なファイアウォールログ分析を実行し、すべての資産フローの全容を把握しました。

フェーズ4

- さまざまなチーム間の連携が、効果的かつ効率的な自動化プレイブックの開発には不可欠であることが明確になりました。
- すべてのチームが同期することで、シームレスに機能するソリューションを構築することができました。

フェーズ5

- ベライゾンは、ベンダー向けのより統制されたアクセスモデルへの移行をサポートしています。
- これには、SSH、RDP、またはブラウザベースの方法のみにアクセスを制限する新しい標準ルールの確立が含まれます。
- この変更は、新しいアーキテクチャに完全に適合しながらベンダーのアクセスニーズが満たされるように、各ベンダーへの直接リクエストと協業を通じて実装されています。

フェーズ6

- ネットワークトラフィックの挙動分析により重要なインサイトが得られ、ネットワークアクティビティをより深く理解できるようになりました。

verizon business