WHITE PAPER

OT 環境で実現する SD-WAN のメリット

概要

OT（オペレーショナルテクノロジー）のデジタル化に伴い、インターネットやクラウドとの安定した接続の重要度が高まっています。低速で高価な従来の WAN インフラストラクチャの後継ソリューションの候補として、ソフトウェア制御による WAN（SD-WAN）が登場しましたが、インターネット接続された情報テクノロジー（IT）と OT のコンバージェンスに伴い、可視性を向上させることで、分散するすべてのオペレーションの可視化、リモートでの展開、容易な管理を可能にすることが求められています。しかしながら、最も重要なのは、セキュリティ制御を強化し、OT に固有の増加し続ける攻撃からの保護を可能にすることです。

IT / OT のコンバージェンスがもたらす可能性とリスク

工業、製造、重要産業の分野では、OT システムと IT テクノロジーのコンバージェンスが進み、新たな効率性と機能が提供されるようになっています。ところが、このような連携の強化により、OT のこれまでとは違う特性に対応する新たなツールやソリューションが求められるようになりました。

デジタル化に伴い、OT が接続された組織では、複雑さとリスクが増大し、OT 管理に拡張ネットワークインフラストラクチャの全体像が必要とされるようになりました。今日、半数を大きく上回る組織（78%）で、OT 環境を部分的にしか一元管理できていないのが現状であり[1]、完全な可視性なしにはインフラストラクチャの見えない部分を保護することはできません。

IT と OT のコンバージェンスが進んだ結果、OT システムを隔離して保護していた「エアギャップ」はほとんど消滅しました。これは、IT への侵入が可能な脅威であれば、OT 側の脆弱で潜在的に価値のある標的にも到達できることを意味し、サイバー犯罪者に、垂直方向（OT 環境の外側から内側）だけでなく、水平方向の移動も許すことになります。侵入者を直ちに発見できる可視化ツールがない場合、被害が拡大する傾向にあり、イベントチェーンにおける攻撃者の初動から資産が最初に侵害されるまでの時間が、一般的に分単位で測定されるのに対して、発見までの時間は多くの場合月単位に及ぶことからも明らかです[2]。

運用、トレーニング、レポートを簡素化し、全体のコストを削減するには、IT と OT の両方の環境で二重の役割を果たす新しいインフラストラクチャも必要になります。異なるベンダーの多様なツールや製品を追加することで生じるインフラストラクチャの複雑さは、設備投資（CapEx）を増加させるだけでなく、導入、管理、監視の過剰な作業を担当者に強いることにもなり、結果として、運用経費（OpEx）も上昇します。

従来の WAN 接続は高コストを強いられる

多くの OT 企業の継続的な課題であるコスト削減の達成において、既存の WAN インフラストラクチャは大きな機会となります。従来の WAN では、高価な MPLS 回線や衛星回線が主に利用されてきましたが、一元的な制御と可視性を可能にする目的でトラフィックがオンプレミスのデータセンターにバックホールされるため、セキュリティのボトルネックにより、パフォーマンスに影響します。

企業のリモート環境の接続手段として広く利用されるようになった SD-WAN は、LTE（Long-Term Evolution）、DSL（Digital Subscription Line）、ケーブルなどのさまざまな商用インターネット接続を使用し、MPLS / 衛星回線を置き換えることで、大幅なコスト削減を可能にします。アプリケーションのパフォーマンスとユーザーエクスペリエンスの品質を確保するため、SD-WAN は、パフォーマンス（遅延やジッターなど）と接続コストに基づいてトラフィックのルーティングを管理することで、高信頼性かつ高品質の接続を実現します。

多くのエキスパートが、重要インフラストラクチャへの攻撃、すなわち、ボットネットによる OT ネットワークへの DDoS 攻撃、クラウドサービスを利用する製造システムへの攻撃、サードパーティーベンダーが侵害されてサイバー犯罪者による重要部門の攻撃に発展するサプライチェーン攻撃が増加すると予測しています[3]。

OT に固有の物理的ニーズ

OT 組織は、空調を完備するビルが立ち並ぶ大規模キャンパスからカーペットも敷かれていないリモートの小規模施設まで、あらゆる規模のあらゆる環境を運用しています。通常の IT 機器では耐えられない、次のような過酷な物理条件の環境もあります。

- 変電所
- 石油採掘場
- 工場
- 水力発電所
- 倉庫 / 配送センター
- 空港
- 船舶

SD-WAN を採用する組織が増加していることから、OT 環境のニーズを満たす機器があれば、OT 環境にも採用が拡大することが期待されますが、そのためには、産業、製造、重要インフラストラクチャなどの過酷な環境条件（石油採掘場、変電所、組立ライン、海上貨物など）を想定して設計された耐久性のある SD-WAN 機器が必要です。

SD-WAN は、迅速な導入、クラウドアプリケーションへの高速接続、統合管理による IT オーバーヘッドの削減など、OT の複数の課題を同時に解決し [4]、生産性の向上も可能にします。マルチクラウドアーキテクチャのクラウドサービス（Microsoft 365、Oracle Cloud、AWS 内のアプリケーションなど）に接続するオンサイトのユーザーが直接アクセスできるため、中央のデータセンターに置かれたファイアウォールを経由してインターネットに接続する、より低遅延ではるかに優れたユーザーエクスペリエンスが実現します [5]。

SD-WAN とセキュリティに対する疑問

OT 環境においては、クラウドやインターネットのリソースへの直接アクセスのセキュリティへの影響が一般的な SD-WAN の導入環境より大きくなる可能性があります [6]。従来の WAN から SD-WAN に移行すると、インターネットに接続されたトラフィックが一元的なセキュリティチェックの目的でデータセンターにバックホールされなくなるため、リスクがさらに増大します。ほとんどの SD-WAN は残念ながら、ルーティングテクノロジーを採用しており、トラフィックの最良の接続パスを探すことに主眼を置いて設計されています。昨今の SD-WAN ソリューションは、ほとんどセキュリティが組み込まれていません。

OT が利用されている業種は標的型攻撃の対象になっているため、OT の脆弱性のいかなる増加も深刻な問題となります。大多数の組織（90%）が 1 年以内に少なくとも 1 回の OT システムへの侵入を経験し、65% が 3 回以上も侵入されています [7]。

攻撃によって生じる OT の機能停止や中断は、生産性、効率性、さらには安全性にも大きく影響します。今日、多くのマルウェア攻撃が、脆弱な産業用制御システム（ICS）、監視制御システム（SCADA）、安全システムなどを標的として特別に設計されるようになっています [8]。重要インフラストラクチャ（水力発電所、原子力発電所、石油やガスのパイプラインなど）が標的になり、侵入が成功した場合、人命や環境に直接影響する可能性があります。

産業用ネットワークでは、制御センターやクラウドアプリケーションへの接続を保護、優先し、OPC UA（Open Platform Communications Unified Architecture）、MQTT（Message Queuing Telemetry Transport）、HTTP などの IIoT（産業用 IoT）や IoT の通信プロトコルを活用するスマートセンサーを保護する必要があります。プロセス制御ネットワークから企業の IT ネットワークやインターネットへのテレメトリや制御情報の転送には、Modbus、BACnet、SafetyNET などの本質的に安全でないプロトコルが使用されており、これらを異なるセグメントに配置してインスペクションし、優先させ、保護する必要がありますが、一般的な SD-WAN ソリューションは、これらの重要なセキュリティ機能を備えていません。

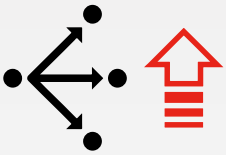
リモートの導入、管理、監視

SD-WAN の OT 環境への適応にあたり、もう 1 つの重要な問題として、技術者が少数あるいは不在であることが多いリモート環境に実装する必要があり、作業が困難になる可能性が挙げられます [9]。リモート環境への実装では、SD-WAN ソリューションがセキュリティポリシーを順守することで、システムが動作を開始した瞬間からサイトが保護されるようにする必要があります。

OT に固有の物理的ニーズ（続き）

上記のような場所では、OT 環境では一般的な次のような条件でも動作する、専用の電子機器が必要です。

- 温度の極端な変化
- 湿度
- 強い振動または日常的な振動
- 電磁波（EMI）
- 機器の設置スペース
- 110 V や 220 V 以外の電源での運用
- OT 業界の様々な法規制の認定



世界の SD-WAN 市場は 2024 年まで 168% 成長し、32 億ドルを超えると予測されています [10]。

サイバー犯罪者は、OT の従来の脆弱性と拡大する攻撃対象領域の新しい脆弱性の両方を同時に標的にすることで、攻撃の機会を最大限に活用します [11]。

さらに、セキュリティオペレーションセンター（SOC）は、各サイトの脅威レベルを監視し、IT と OT のネットワーク間のゲートウェイを管理し、システムを隔離して感染を特定し、マルウェアの拡散を最小限にするための一元的な可視性が必要です。

OT 向け SD-WAN に対する信頼性、セキュリティ、コスト効率のニーズ

あらゆる種類のサイバー犯罪者（ハクティビスト、国家が支援する攻撃者、犯罪組織など）が自らの目的のために OT システムを混乱させたり損傷させたりしようとしているため、組織は、デジタル化のメリットを最大限に活用しつつ、これらのテクノロジーが機密度の高い環境にもたらす新たなリスクを最小限に止める必要があります。

生産性とコスト削減は、あらゆる企業に不可欠な推進要素ですが、OT システムに依存する業種は、そのいずれかを業務の安全性やセキュリティより優先させるわけにはいきません。インターネットへの直接接続が OT 環境にもたらすリスクの増大に対抗するには、統合セキュリティ、一元的な可視性、リモート管理の機能を備えた SD-WAN が不可欠です。さらには、SD-WAN のメリットを今日の産業環境でも活用するには、OT の導入環境に固有の物理要件に合わせて、ネイティブに設計された耐久性のあるソリューションが必要です。

[1]「2020 State of Operational Technology and Cybersecurity Report」、フォーティネット、2021 年 4 月 13 日（英語）：
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2020-ot-cybersecurity.pdf

[2]「2019 Data Breach Investigations Report」、Verizon、2019 年 4 月（英語）：https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[3]「15 Cyber Threat Predictions for 2020」、Bruce Sussman 著、SecureWorld、2019 年 12 月 19 日（英語）：
https://www.secureworldexpo.com/industry-news/15-cyber-threat-predictions-for-2020

[4]「SD-WAN: More Than A Retail Solution」、Nirav Shah 著、Network World、2020 年 7 月 15 日（英語）：
https://www.networkworld.com/article/3566877/sd-wan-more-than-a-retail-solution.html

[5]「What Manufacturing CISOs Need to Know About SD-WAN」、Joe Robertson 著、LinkedIn、2019 年 12 月 20 日（英語）：
https://www.linkedin.com/pulse/what-manufacturing-cisos-need-know-sd-wan-joe-robertson/

[6]「SD-WAN: More Than A Retail Solution」、Nirav Shah 著、Network World、2020 年 7 月 15 日（英語）：
https://www.networkworld.com/article/3566877/sd-wan-more-than-a-retail-solution.html

[7]「2020 State of Operational Technology and Cybersecurity Report」、フォーティネット、2021 年 4 月 13 日（英語）：
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2020-ot-cybersecurity.pdf

[8]「Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems」、フォーティネット、2019 年 5 月 16 日（英語）：
https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-security%20trends.pdf

[9]「SD-WAN Isn't Just for Retail」、フォーティネット、2020 年 4 月 3 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-sdwan-isnt-just-for-retail.pdf

[10]「SD-WAN Market Expected to Increase 168 Percent by 2024」、BBC Magazine、2020 年 7 月 8 日（英語）：
https://www.bbcmag.com/breaking-news/sd-wan-market-expected-to-increase-168-percent-by-2024

[11]「Operational Technology: Why Old Networks Need to Learn New Tricks」、Derek Manky 著、Dark Reading、2019 年 12 月 31 日（英語）：
https://www.darkreading.com/application-security/operational-technology-why-old-networks-need-to-learn-new-tricks

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Promise-of-SD-WAN-OT-202109-R1