デジタルトランスフォーメーション時代のSD-WAN

ネットワークセキュリティを複雑化せずにビジネスアジリティを実現

WHITE PAPER

概要

ほとんどの組織では何らかの形でデジタルトランスフォーメーション（DX）が進められており、どのように製品やサービスを市場に投入し、最終的にどのような価値を顧客に提供するかということについて、変革が起きています。しかし、DX イニシアチブの促進にはネットワークオペレーション業務を複雑化するという弊害もあります。ビジネスクリティカルなサービスは複数のクラウドに分散しています。このことが潜在的なパフォーマンスの問題の原因となっており、特にその傾向は支社において顕著になっています。

この現状を踏まえると、SD-WAN（Software-Defined Wide-Area Network）テクノロジーが瞬く間に台頭してきたことも不思議ではありません。残念ながら、SD-WAN は DX のパラドックスの例となっています。革新的なテクノロジーにはビジネスをさらなる高みへと引き上げる潜在能力がありますが、それらのテクノロジーによって攻撃対象領域が拡大し、組織が重大なリスクにさらされる可能性があるからです。そのため、SD-WAN の導入は、他の DX への取り組みと同様にセキュリティトランスフォーメーション（SX）を伴うものでなければなりません。この場合の SX とは、古くなった原則を再検討し、データセンターを超えて保護を拡大し、可視化と制御を一元管理するために、セキュリティアーキテクチャを統合することを意味します。

デジタルトランスフォーメーションによって、ますます多くのサービスがクラウドに移行するようになっており、その結果、従来のネットワークアーキテクチャは隅に追いやられ、SD-WAN が注目を集めています。

DX の課題

今日の企業における IT 分野の最も重要なビジネストレンドが、DX であることに間違いありません。DX によって、企業はアジリティとスケーラビリティをより迅速に改善可能となります。これは、多くの業界で極めて重要な要素です [1]。DX は、デジタル対応のエンタープライズを超越した、完全なデジタルエンタープライズを実現します。デジタルエンタープライズとは、「ハイパーコネクテッド、アダプティブ、インテリジェント、アジャイルな特性を備え、新しい業務プロセス、ポリシー、組織との高度な統合が可能な革新的能力をもたらすテクノロジーを活用する」企業を意味します [2]。

DX は、企業毎に若干異なるように思われますが、ほぼ確実にハイブリッドクラウドアーキテクチャへの依存度が高まることが特徴です。このことは、ネットワークオペレーション部門にとって、既存のオンプレミスリソースを複数の外部クラウドネットワークと組み合わせ、ユーザーがどこにいるかを問わず、そういったリソースやアプリケーションの可用性とパフォーマンスを確保しなければならないことを意味します。

DX のネットワーキングニーズに対応する SD-WAN

ますます多くのサービスがクラウドに移行するに伴い、「従来のネットワークアーキテクチャは、クラウド優先の組織のワークロードを処理するようには構築されていない」[3] ことが明らかになってきています。その結果、他の重要な DX テクノロジーとして、SD-WAN が急速に成長しています。この「急速」という言葉は、SD-WAN を表現するものとしてよく見かけられます。IHS Markit による調査では、74% の企業が 2017 年に SD-WAN を試験導入し、その多くが今年に入ってからこのテクノロジーを本格的に導入配備していることが明らかとなっています [4]。

SD-WANは、本社から離れた場所で働くユーザーにクラウドアプリケーションへの高性能のアクセスを提供するため、支社におけるネットワークのアジリティを改善し、以前は不可能だったレベルの自動化を促進します。具体的なメリットとしては、以下のようなものがあります。

1. **クラウドへの直接アクセス：**SD-WANは、バックホール、つまりクラウドと支社のすべてのトラフィックをデータセンター経由でルーティングする処理を不要にします。これにより、すべてのユーザーがその所在地を問わず重要なクラウドサービスに直接アクセスできるようになります。
2. **アプリケーションパフォーマンスの改善：**ビジネスクリティカルなトラフィックや、VoIP（Voice over Internet Protocol）などのリアルタイムサービスが優先され、最も効率的なルートを経由するようにSD-WANを構成することができます。トラフィックの送信オプションがいくつかあれば、回線のオーバーロードによるパケット損失や、トラフィックの混雑が原因のレイテンシーの低減に役立ち、パフォーマンスやユーザーエクスペリエンスが向上します[5]。
3. **ビジネスアジリティの強化：**ネットワークプランナーは、従来のWANのように追加のMPLS（MultiProtocol Label Switching）用の帯域幅を導入展開するために、数週間または数か月も前から計画を立てる必要がなくなります。また、複数の支社で充分なネットワークパフォーマンスを確保しなければならないことが原因で、他のDXイニシアチブの進行が妨げられることもなくなります。
4. **コスト節約：**SD-WANを利用することで、既存のMPLS回線だけでなく、LTEやブロードバンドで接続するパブリックインターネットを含めた複数のチャネル経由で、効率的にトラフィックをルーティングすることができます[6]。その結果、新たにMPLS帯域幅を追加するコストを抑制可能になります。

ネットワークセキュリティの低下を招くSD-WAN

DXにおけるSD-WANネットワークアーキテクチャのメリットについて、議論の余地はありません。しかし、SD-WANには明らかなデメリットもあります。SD-WANが導入され、ローカルでインターネットにアクセスする各拠点では、攻撃対象領域が拡大することに加えて、ネットワークセキュリティチェーンにおいて脆弱なリンクが増えることになります。SD-WANの導入以前から、支社のセキュリティレベルは本社に比べて低いことが多いため、既存の問題をさらに悪化させます。

74%の企業が2017年にSD-WANを試験導入し、その多くが今年に入ってからこのテクノロジーを本格的に導入配備しています[7]。

もちろん、DXに端を発するテクノロジーの大半が組織の攻撃対象領域を拡大するため、多くの場合セキュリティはDXイニシアチブにとって最大の障壁と見なされます[8]。SD-WANの導入をはじめとするすべてのDXイニシアチブを成功させるためには、対応するSX（セキュリティトランスフォーメーション）が不可欠です。

SXがセキュアなSD-WANを実現

SXには、長年にわたって適用されてきたエンタープライズセキュリティ関連の原則の再検討が不可欠です。たとえば、境界ベースのセキュリティモデルの場合、新たなクラウドサービスが展開される度に有効性が低下するため、SD-WANではまったく機能しません。また、SXではセキュリティを後付けで考えるのではなく、DXのプランニング段階で組み込む必要があります。DXイニシアチブ、計画、展開を担当するすべてのチームが、セキュリティバイデザイン（Security by Design：計画的なセキュリティ導入）、セキュリティバイデフォルト（Security by Default：初期段階からのセキュリティ導入）の原則に従わなければなりません。

SD-WANの導入に関しては、ネットワークセキュリティ部門とネットワークオペレーション部門がソリューションに関する意思決定プロセスを共有し、最終選考が完了した時点でセキュリティ戦略を実施する必要があります。従来、これらのチームはサイロ化されており、場合によってはお互いが競い合うように業務を行うこともあります[9]。しかし、チームが連携することによって、以下のようにSD-WANを取り巻く真のセキュリティ上の懸念事項に戦略的に対処できるようになります。

- DXイニシアチブの推進とSD-WANインフラストラクチャによって拡大する攻撃対象領域のセキュリティを確保する[10]
- マルウェアのネットワークへの侵入や拡散を防ぐ[11]
- リモートの事業拠点で不足する熟練のITセキュリティ担当者の業務を補完する
- ネットワーク全体の可視化とエンタープライズ全体のセキュリティの一元管理を実現する

SD-WAN には、必然的にセキュリティトランスフォーメーションを伴います。つまり、境界の保護をはじめとする、長年にわたるエンタープライズセキュリティの原則を再検討する必要があるのです。

統合こそ SX 実現の鍵

最近のある調査によると、大手の組織ではサイバー攻撃関連の不正侵入が 2 年間で 20 件発生しており、そのうちの 4 件でセキュリティが侵害され、データの損失やウイルス感染などの被害が発生していることが明らかになっています [12]。問題の一部として挙げられるのが、典型的な攻撃を検知するだけで 6 か月以上（197 日）も要しており、その間に攻撃者が組織内で自由に水平移動（ラテラルムーブメント）が可能であることです [13]。このような脅威の大部分は、従来のセキュリティ対策の回避を意図した高度な攻撃です。SD-WAN やその他の DX イニシアチブを戦略的に展開しなければ、そういった脅威の問題をさらに悪化させることになります。

DX を推進するために SD-WAN を導入する際には、SX も同様に重要であることを考慮しなければなりません。SD-WAN ではネットワークトラフィックがデータセンターを迂回するため、ネットワークセキュリティアーキテクチャを拡大する必要がありますが、その結果セキュリティアーキテクチャのサイロ化を招いてはいけません。万全のセキュリティを備えた SD-WAN ソリューションを採用することで、セキュリティをネットワークに統合し、複数の拠点を持つ分散型のエンタープライズ環境全体を保護することが可能になります。その結果、一元的な可視化と制御、セキュリティプロセスの完全な自動化、脅威インテリジェンスの動的な共有、ネットワークの耐障害性の向上がすべて実現します。

過去 2 年間で 20 件のサイバー攻撃による不正侵入が一般的な企業に被害を及ぼしています。不正侵入の検知に 6 か月以上も要していることから、従来のセキュリティパラダイムは崩壊し、組織はデータの盗難、ランサムウェア、業務オペレーションの停止などのリスクを抱えることになります。

SX を推進してセキュアな SD-WAN を実現

SD-WAN の導入は、企業の支社ネットワークにおいて具体的なバリューをもたらす絶好の機会となります。その導入に際して、IT やセキュリティの責任者は以下の点に留意することが重要です。

- SD-WAN は、多くの組織における DX 推進の根幹となる
- SD-WAN は、支社でのクラウド利用促進、アプリケーションパフォーマンスの改善、ビジネスアジリティの強化、コスト削減など、具体的なビジネス価値をもたらす
- 多くの場合、SD-WAN は攻撃対象領域の拡大を招き、最も脆弱なセキュリティリンクとなる可能性がある
- SD-WAN のセキュリティを確保するには、SX が不可欠である
- セキュア SD-WAN 実現の鍵は、統合である

[1]「Digital transformation and the CIO: Everything you need to know today（デジタルトランスフォーメーションと CIO：今すぐ知っておくべきこと）」、Michael Krigsman 著、ZDNet、2018 年 5 月 25 日発行（英語）：https://www.zdnet.com/article/digital-transformation-and-the-modern-cio/
[2]「Digital transformation reimagines everything（すべてを変えるデジタルトランスフォーメーション）」、Benson Chan 著、Strategy of Things、2017 年 9 月 7 日発行（英語）：https://strategyofthings.io/digital-transformation
[3]「A digital-first enterprise needs SD-WAN（デジタルエンタープライズには SD-WAN が必要）」、Kelly Ahuja 著、Network World、2018 年 6 月 7 日発行（英語）：https://www.networkworld.com/article/3280226/a-digital-first-enterprise-needs-sd-wan.html
[4]「Enterprises are moving to SD-WAN beyond pilot stages to development（試験段階を経て SD-WAN の本格導入に移行するエンタープライズ）」、Andy Patrizio 著、Network World、2018 年 5 月 7 日発行（英語）：https://www.networkworld.com/article/3269858/enterprises-are-moving-sd-wan-beyond-pilot-stages-to-deployment.html
[5]「How does SD-WAN manage real-time network performance?（SD-WAN におけるリアルタイムのネットワークパフォーマンス管理）」、Lee Doyle 著、TechTarget SearchSDN、2018 年 1 月 9 日発行（英語）：https://searchnetworking.techtarget.com/answer/How-does-SD-WAN-manage-real-time-network-traffic-performance
[6]「Traditional WANs vs Next Gen SD-WAN（従来の WAN と次世代の SD-WAN の比較）」、Infosecurity、2017 年 12 月 12 日発行（英語）：https://www.infosecurity-magazine.com/opinions/traditional-wans-next-gen-sd-wan/
[7]「Enterprises are moving to SD-WAN beyond pilot stages to development（試験段階を経て SD-WAN の本格導入に移行するエンタープライズ）」、Andy Patrizio 著、Network World、2018 年 5 月 7 日発行（英語）：https://www.networkworld.com/article/3269858/enterprises-are-moving-sd-wan-beyond-pilot-stages-to-deployment.html
[8]「Security Implications of Digital Transformation Report（デジタルトランスフォーメーションがセキュリティに及ぼす影響に関するレポート）」、フォーティネット、2018 年 7 月 26 日発行（英語）：https://www.fortinet.com/blog/industry-trends/security-implications-of-digital-transformation-report-.html
[9]「Driving the Convergence of Networking and Security（ネットワーキングとセキュリティの融合の促進）」、Erin O’ Malley 著、SecurityWeek、2018 年 5 月 15 日発行（英語）：https://www.securityweek.com/driving-convergence-networking-and-security
[10]「Warning: security vulnerabilities found in SD-WAN appliances（SD-WAN アプライアンスで見られる脆弱性の警告）」、Steve Garson 著、Network World、2017 年 11 月 28 日発行（英語）：https://www.networkworld.com/article/3238725/warning-security-vulnerabilities-found-in-sd-wan-appliances.html
[11]「What are the options for securing SD-WAN?（SD-WAN のセキュリティを確保するための選択肢とは）」、Lee Doyle 著、Network World、2018 年 7 月 12 日発行（英語）：https://www.networkworld.com/article/3285728/what-are-the-options-for-securing-sd-wan.html
[12]「Security Implications of Digital Transformation Report（デジタルトランスフォーメーションがセキュリティに及ぼす影響に関するレポート）」、フォーティネット、2018 年 7 月 26 日発行（英語）：https://www.fortinet.com/blog/industry-trends/security-implications-of-digital-transformation-report-.html
[13]「Advanced Threats in Financial Services and Retail: A Study of North America & EMEA（金融サービスと小売業における高度な脅威：北米および EMEA に関する考察）」、Ponemon Institute、2015 年 5 月 28 日発行（英語）：https://www.ponemon.org/blog/ponemon-institute-releases-new-study-on-the-efforts-of-retail-companies-and-financial-services-to-improve-the-time-to-detect-and

FORTINET
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