eBook

CIO向けガイド

セキュアなデジタルトランスフォーメーションの加速化

迅速かつ安全に実現するための5つのポイント

ITが直面する新たな現実

クラウドアプリケーションの採用を進め、インターネットトラフィックが大幅に増加している組織にとって、モバイルファーストコンピューティングは戦略的イニシアチブとなっています。

IT部門にとって、デジタルトランスフォーメーションはメリットもある一方でデメリットもありますが、心配する必要はありません。

セキュアなデジタルトランスフォーメーションの実現に必要不可欠な5つのポイント

1 老朽化したインフラストラクチャを更新する ›

2 支店からのインターネット接続を安全に行う ›

3 さまざまな場所のモバイルワーカーを安全に接続する ›

4 Microsoft 365のユーザエクスペリエンスを向上する ›

5 M&Aに伴うIT統合を簡素化する ›

老朽化したインフラストラクチャを更新する

約30年にわたって、多くの組織はユーザをデータセンタのアプリケーションに接続するために、複雑なネットワークを構築してきました。そして、そのすべてを保護するために、多数のネットワークセキュリティアプライアンスに投資してきたのです。脅威は常に進化しているため、老朽化したインフラストラクチャの更新や再開発、新しいセキュリティコントロールの追加が必要になり、ネットワークの複雑さやコストはさらに増加しています。

ユーザやアプリケーションがネットワークを離れ、クラウドに向かうトラフィックが増えたことで、このような従来型ネットワークモデルによる対応が困難になってきています。

今こそ、セキュリティニーズの解決とユーザの直接接続を可能にする、目的を考慮して設計された新しいアプローチを採用し、セキュリティをクラウドに移行する時です。

最初に取り組むべきこと

- **SASE（Secure Access Service Edge）アーキテクチャの使用:** 詳細は、Gartnerが発行するレポート「**The Future of Network Security is in the Cloud**」や「**Gartner Magic Quadrant for Secure Web Gateways**」で紹介されています。
- **ネットワークトランスフォーメーションの促進:** CSaaS（Cloud Security-as-a-Service）を活用して、ハブ&スポークから「Direct-to-Cloud」に移行します。
- **ハードウェアやソフトウェアの 段階的な廃止:** 技術者を面倒な作業から解放し、日常的な管理やメンテナンスを削減します。

成功事例

SIEMENS

クラウドが新たなデータセンタとなり、世界192か国、35万人のSiemensユーザにとってインターネットが新たな企業ネットワークになりつつあります。Siemensは、クラウドを前提に構築された、時間や場所に制限がないアプリへのセキュアかつ高パフォーマンスなアクセスを提供する最新ネットワークアーキテクチャによって、大幅なコスト削減を実現しました。

「トラフィックをバックホールすることなく、インターネットへのダイレクト接続を利用することで、70%のコスト削減を達成できる見込みです。」

Frederik Janssen
IT戦略&ガバナンス担当バイスプレジデント
Siemens

支店からのインターネット接続を安全に行う

新しい支店や店舗をオンラインにするには、どれ位の時間が必要でしょうか。新しいサイトをハブ&スポークネットワークと統合するには、多くの時間とリソースが必要になります。 さらには、オンラインになった後に、増加する帯域幅の需要にファイアウォールが追いつ けず、WANコストが上昇し、ゲートウェイが圧迫されると、トラフィックのボトルネックや レイテンシといった問題に直面する可能性もあります。レガシーネットワークでは、十分なスピードで拡張を実現することはできません。

SD-WANへの移行によって支店の運用を簡素化し、ローカルインターネットブレイクアウトを可能にし、SD-WANの価値を完全に実現するには、セキュリティをデータセンタからネットワークのエッジに移動させる必要があります。

最初に取り組むべきこと

- **クラウドへのセキュリティの移動:** データセンタ、クラウドサービス、オープンインターネットのいずれが送信先になっても、すべてのトラフィックをインスペクションします。
- **「資産を持たない」支店づくり**: すべての場所にローカルインターネット接続を展開し、可能であればMPLSを排除します。
- **支店のIT担当者との協業:** ビジネスの視点に立ってトランスフォーメーションを推進するようにします。

成功事例

AutoNation

米国最大手の自動車小売業者であるAutoNationは、360のローカルブレイクアウトの確立によって、高速かつセキュアなインターネットアクセスをユーザに提供できるようになりました。AutoNationはZscalerの採用によってコストを削減し、新しい拠点を容易にオンラインにつなぎ、さらにインラインSSLインスペクションやサンドボックスを始めとする機能でセキュリティを強化しました。

「Zscalerの採用によって、360の支店に設置されていたルーターとエンドポイントを大幅に削減できました。」

Ken Athanasiou
CISO兼バイスプレジデント
AutoNation

さまざまな場所のモバイルワーカーを安全に接続する

さまざまな場所で働くユーザがアプリケーションに接続できるようにするには、VPNテクノロジを利用してネットワークをユーザの場所まで拡張する必要がありました。しかしながら、セキュリティの観点から、トラフィックをデータセンタにバックホールする必要があるため、エクスペリエンスが低下し、多くの場合リモートユーザがVPNやセキュリティを回避するようになり、ビジネスリスクが増大します。このような理由から、Gartnerは60%の組織が2023年までにVPNを段階的に廃止し、ZTNA（ゼロトラストネットワークアクセス）ソリューションに移行すると予測しています。[1]

エンドポイントセキュリティだけで高度な脅威に対応することはできません。サービスエッジセキュリティクラウドを利用することで、どのようにユーザを保護し、優れたユーザエクスペリエンスを提供できるのでしょうか？

最初に取り組むべきこと

- **ZTNAアーキテクチャの採用:** ネットワークへのアクセス権限をユーザに付与することなく、アプリにアクセスできるようにします。
- **エッジへのセキュリティの移動:** 高速なユーザエクスペリエンスを保証しつつ、あらゆる場所から接続するユーザに同一のセキュリティを提供します。
- **アプリケーションへのアクセスの許可/拒否:** アイデンティティの一元管理によって許可または拒否することで、管理の複雑さが軽減されます。

成功事例

nab

オーストラリア最大の法人向け銀行であるナショナルオーストラリア銀行（NAB）は、より安全で優れたユーザエクスペリエンスを提供し、業務を合理化することを目指して、クラウドへの移行を開始しました。NABは現在、ゼロトラストを採用し、全従業員によるWFA（Work From Anywhere）を可能にする、将来にわたって使い続けられるネットワークインフラストラクチャを提供しています。

「従業員は自宅でPCの電源を入れ、オフィスにいるのとまったく同じように仕事を始められます。ログインの手順が追加されることも、セキュリティトークンを使う必要もありません。」

Steve Day
EGMインフラストラクチャ / クラウド / ワークプレイス担当
ナショナルオーストラリア銀行

Microsoft 365のユーザエクスペリエンスを向上する

ほぼすべてのユーザがMicrosoft 365を利用しているため、そのユーザエクスペリエンスは導入の成功度を測る重要な指標となります。ところが、Microsoft 365へのユーザトラフィックによってネットワーク使用率が大幅に増加するため、ファイアウォールの負荷が高くなり、ユーザエクスペリエンスが低下します。さらには、Microsoft 365によって、高価で複雑化の原因となるハードウェアのアップグレードが必要になることも多く、ファイアウォールの継続的なアップデートには困難が伴います。

高速かつ一貫性あるMicrosoft 365のエクスペリエンスが必要です。それを実現するため、 Microsoftは以下を推奨しています：

- Microsoft 365トラフィックの識別および区別
- ローカルでのネットワーク接続の送信
- バイパスプロキシの評価
- ネットワークヘアピンの回避

最初に取り組むべきこと

- **Microsoft365のトラフィックのルーティング:** Microsoftが推奨するローカルのインターネットブレイクアウト経由でMicrosoft365のトラフィックをルーティングします。
- **Microsoftが推奨する唯一のクラウドセキュリティベンダーの活用:** これにより、最速のユーザエクスペリエンスが実現します。
- **帯域幅の使用の合理化**: Microsoft 365のトラフィックが業務に無関係なトラフィックより優先されるようにします。

成功事例

KELLY SERVICES

Kelly Servicesは、ネットワークトランスフォーメーションによって、世界中の900か所に高速かつセキュアなダイレクトインターネット接続を提供し、Microsoft 365を始めとするクラウドアプリへの高速アクセスを可能にしました。同社は、MPLSの予算を60%削減したほか、インスペクション機能を強化し、ネットワークとポリシー管理を大幅に簡素化することができました。

「Zscalerを利用することで、Office 365のために全帯域幅の30%を確保できるだけでなく、それを50%以下に制限することでOneDriveのファイル転送ですべてがダウンするのを防止することもできます。」

Darryl Staskowski
シニアバイスプレジデント兼CIO
Kelly Services

M&Aに伴うIT統合を簡素化する

IT統合の複雑さは、M&Aを遅らせるだけでなく、業務を混乱させます。リスクを管理しつつ、 ユーザをオンボードまたはオフボードにし、ユーザが必要とするアプリケーションへのアクセスを提供する必要があります。このような複雑さに加えて、企業に新たに加わった、セキュリティ標準が緩やかであったり異なったりする部門との統合を進め、セキュリティを標準化する必要がありますが、その過程でリスクが高くなる可能性もあるため、常に細心の注意が必要です。

ネットワークインフラストラクチャのコンバージェンスを必要とすることなく、アプリケーションへのアクセスをユーザに提供し、ビジネスリスクを最小限に抑えることで、M&Aや関連アクティビティの所要期間を数年から数週間へと短縮できます。

最初に取り組むべきこと

- **ZTNAテクノロジの活用:** ユーザをオンネットワークにすることなく、アプリケーションにすぐにアクセスできるようにします。
- **アイデンティティに基づく段階的アプローチの採用:** 両社でM&Aに関連する活動を担当するユーザから始め、アクセスが必要なアプリケーションを決定します。
- **ユーザやアプリケーションのリストの拡張: 事業統合の進行と並行して進めます。**

成功事例

Fortune 500に名を重ねる米国の某医療機関は、ネットワークアクセスを前提としないアプリケーションアクセスを提供することで、統合タイムラインを9か月も短縮し、新しく買収または統合した組織のセキュアなオンボーディングを可能にしました。これにより、組織のM&Aインフラストラクチャが簡素化され、ITの複雑さが軽減されました。

Zscalerについて

Zscalerは2008年に、「アプリケーションがクラウドに移行されるなら、セキュリティもクラウドに移行する必要がある」という、シンプルで力強い概念に基づき、設立されました。Zscalerは現在、世界中の数千の組織のクラウド対応の運用への移行を支援しています。

CIOライブラリ

CIOによる、CIOのための役立つリソースについては、
以下を参照してください。

https://revolutionaries.zscaler.com/

または、営業担当者までお問い合わせください。

zscaler™ | Experience your world, secured.™

Zscalerについて
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、何千人ものお客様をサイバー攻撃や情報漏洩から保護しています。世界中で運用する150のデータセンタで動作するSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

03-4243-6320
Zscaler, Inc.(本社) - 120 Holger Way - San Jose, CA 95134
zscaler.com