ホワイトペーパー

ITリーダーがゼロトラストネットワークアクセスの戦略を検討すべき理由

データを保護しながらデジタルビジネスを実現

テクノロジはビジネスを前進し続けるために必要なエンジンのような存在として長い間捉えられてきましたが、現在ではさらに新たな効率性と収益機会を生み出せる、真のビジネスドライバーとして認識されています。そしてITリーダーの役割も同様に進化しており、CISO、CIO、CTOが経営幹部層の役職として認識され、テクノロジ関連のイニシアチブに注力し、これを主導する役割を担うようになっています。

こうした傾向の主な要因としては、AzureやAWS、Google Cloudなどのエンタープライズパブリッククラウドの導入の急増、および従業員が所有するモバイルデバイスの業務利用（BYOD）の普及が挙げられます。これらのテクノロジを活用することで、企業はビジネスプロセスを最適化し、製品やサービスをより迅速かつ総コストを抑えた状態で提供しています。

しかし、これに伴うリスクについてはどうでしょうか。

クラウドならびにユーザモビリティに向けたこのような傾向により、企業ネットワーク内のユーザと内部サービスを保護していた従来のセキュリティ境界は、もはや過去のものとなりました。

これにより、クラウドやモビリティをサポートする新しいITの予算を要求する際には、リスクとそれがビジネスの収益に与える潜在的な影響の関係性を経営陣に理解させることが不可欠となっています。データ漏洩や重要度の高いインフラストラクチャのダウンタイム、そしてブランドの評判の低下によるコストを明確に伝え、経営陣が理解できるビジネス価値に結び付けて説得する必要があります。

ITリーダーがまず取り組むべきことは、会社のリスクポートフォリオを理解し、自社がリスクの影響をどの程度受けやすいかを判断することです。また、ビジネスにとって極めて重要なアプリはSOC1またはISO 27001に準拠し、追加のセキュリティが必要となる場合もあり、これらは重要なインフラストラクチャと見なされます。さらに、中国のように他国から隔離しなければならない国もあります。従来のインフラストラクチャではパッチの継続的な評価が必要であり、ファイアウォールの設定に欠陥が1つでもあればビジネスにとって大きな問題となる可能性があります。

ITリーダーが克服しなければならない課題

鍵となるビジネスイニシアチブを推進し、ビジネス上のニーズとITの機能とのギャップを解消するために、ITリーダーは次のような課題を解決するのに役立つ適切なテクノロジを選ぶ必要があります。

1. 仕事を完了しやすくし、従業員のストレスを最小限に抑えること
2. 従業員および第三者に優れたユーザエクスペリエンスを提供すること
3. 生産性、知的財産、および企業の評判を脅かす可能性のあるリスクを削減すること
4. 動的に変化するビジネスを強化するために、適応性と敏捷性を持つこと
5. パブリッククラウドの採用によってデジタルトランスフォーメーションを加速させること

これらの目標を達成するテクノロジを見定めることは、あるソリューションが望ましい結果を出す代償として別のソリューションが複雑になってしまう可能性があるため、困難な課題と言えます。たとえば、クラウドサービスとモバイルテクノロジを採用することで、ユーザエクスペリエンスの合理化という目標は達成できますが、サイバーセキュリティ攻撃のリスクを最小限に抑えるという目標はどうでしょうか。ITリーダーは、新しいテクノロジ採用の加速化と、機密データのセキュリティの保証とのバランスを慎重に保たなければなりません。したがって、適切なテクノロジを適切なタイミングで選択することが重要となるのです。

ビジネスにとってのゼロトラストネットワークアクセスの価値

Gartnerは、柔軟でセキュア、そしてハイブリッドな働き方を実現する接続を提供するために、セキュリティサービスエッジ（SSE）戦略の一環としてゼロトラストネットワークアクセス（ZTNA）を採用することを推奨しています。ZTNAサービスは従来のVPNテクノロジを必要とすることなく、リモートおよびオフィス内のユーザにプライベートエンタープライズアプリケーションへのセキュアなアクセスを提供します。

ZTNAでは、アプリケーションの周囲にアイデンティティおよびコンテキストベースの論理アクセス境界が作成され、アプリケーションが外部から検出されなくなり、トラストブローカによって指定された一 連のエンティティへのアクセスが制限されます。接続の仲介にあたっては、指定されたユーザのアイデンティティやコンテキスト、ポリシー遵守状況をブローカが検証するため、アプリケーション資産がインターネットに公開されなくなり、攻撃対象領域が大幅に少なくなります。

Gartner

2025年までに、新しいリモートアクセスの導入の少なくとも70%がVPNサービスではなく主としてZTNAを利用して行われると予想されています。この割合は2021年末時点で10%未満であり、大幅な増加が見込まれます。

新しいテクノロジを採用する際に考慮すべき5つの重要な要素についてのこれまでの説明を踏まえ、ZTNAがそれぞれの実現にあたって果たす役割について解説します。

1. 生産性の向上：

オフィスで働くフルタイムの従業員の4人に3人が**今年辞職することを考えており、** パンデミックが引き金となって数千万人が転職を行った大規模な離職の動きに拍車がかかることが予測されています。労働力の大規模な再編に伴い、雇用主は人材の維持と誘致の方法を再考しており、ITリーダーはテクノロジを活用することで人材流出によるダメージを食い止め、今後に向けた業務の基盤を築くことができます。 使いやすいZTNAの機能により、ネットワークにログインするたびにVPNクライアントを起動する煩わしさを排除し、 生産性を高く保ちフラストレーションを最小限に抑えられるため、ユーザは大きなメリットを得られます。 また、クラウド配信型のソフトウェアのみからなるシンプルなZTNAは、容易に設定と導入を行うことが可能です。このシンプルさにより、IT部門はモバイルデバイス上でもセキュアなクラウドアプリケーションテクノロジを採用しつつ、ITスタッフならびに組織全体の生産性を最大限に高めることができます。

2. 優れたユーザエクスペリエンスの提供：

今日、ユーザはオフィス内や自宅、あるいは外出先など、あらゆる場所から業務を行っています。多くの場合、こうしたユーザの中には従業員とサードパーティが混在しており、どちらもデバイス、場所、ネットワークに関係なく、アプリケーションへのスムーズなアクセスを期待しています。ZTNAは各ユーザに迅速かつ完全にシームレスな体験を提供し、VPNや不便なログイン手続きを不要としつつ、エンドポイントエージェントを用いることなくサードパーティのユーザとあらゆる種類のデバイスをサポートします。さらに、プライベートアプ

リへのポリシーベースのアクセスを活用するクライアント不要のZTNAを利用すれば、ユーザが場所に関係なく任意のデバイスからアプリケーションに接続でき、生産性の向上を図れます。

3. リスクの軽減：

セキュリティは依然としてクラウドの採用とリモートワークにおける懸念事項であり、慎重に対処しなければビジネスにとって極めて重要なアプリやインフラストラクチャに対する攻撃の可能性を高めてしまう可能性があります。VPNやファイアウォールなど、従来型のネットワーク中心のテクノロジは過度な信頼を前提にしているため避けるべきです。これらのソリューションはリモートユーザをネットワークに直接配置するため、VPNサーバーがインターネットからのインバウンド通信を受け取る必要があり、これによってVPNがランサムウェアのトロイの木馬となってしまいます。つまり、リモートかローカルかにかかわらず、ユーザはネットワーク経由で水平方向にアクセスできるのです。これは、脆弱なセキュリティ慣行を行っている可能性がある従業員とサードパーティの両者に当てはまります。ZTNAはゼロトラストベースのポリシーを使用し、アイデンティティとデバイスポスチャに基づき、パブリッククラウド、プライベートクラウド、またはデータセンタで動作している特定のプライベートアプリへの接続を承認されたユーザにのみ提供します。接続性を提供することが主な特徴であったZTNAは、内部の脅威や高度な攻撃者からアプリケーションを保護する完全に統合されたセキュリティへと進化を遂げ、組織全体のセキュリティポスチャの改善を促進することが可能となりました。

4. クラウド配信による敏捷性と拡張性：

今日、従業員やデバイス、アプリケーション、およびトラフィックの数は増加の一途をたどっていますが、クラウド配信型のZTNAのサービスはベンダーによってホストされているため、規模の拡大はIT部門の懸念事項ではなくなりました。需要が増加した際には、ZTNAはその分の追加の負荷を自動的に処理します。パブリッククラウド導入のプロジェクトを遅らせる原因となる、追加のハードウェアや仮想ファイアウォールを導入する必要はありません。ZTNAを活用することで、ITリーダーの成功に不可欠な優れた敏捷性と拡張性を得られます。

5. デジタルトランスフォーメーションの加速：

現在、クラウドとモビリティは大半の企業内チームにおける優先事項となっています。しかし、適切ではないソリューションを適用すると、グローバルなユーザベース全体でクラウドを安全に活用できるまでに数か月から数年かかることがあります。その原因の1つは、従来のネットワークおよびセキュリティテクノロジを使用して、管理されていないデバイスからのクラウドアプリへのアクセスを提供することにまつわる複雑さです。ZTNAはソフトウェアを使用して複雑さを低減し、導入時間を数か月または数年からわずか数時間へと短縮します。そのため、ZTNAを通じ、組織はクラウドとモビリティの改善によるメリットを迅速に得ることができます。

> “クラウド移行の過程でさまざまな変化を切り抜けてきたことが、今後のあらゆる事態に対処できるという強い自信につながりました。この経験は今後も長期にわたって糧となり、いずれは古くから続いてきた考え方を変えることにもなるでしょう。私たちは、テクノロジが持つこのような影響力に加え、当社の人材が持つ困難への対応力や創造性を示しながら、新しい働き方の検討を始めています。”
>
> **– Alex Philips氏**（National Oilwell & Varco、最高情報責任者）

ZTNAについて

ZTNAサービスは企業のITリーダーにとって有益なツールです。Zscalerでは、Zscaler Private Access（ZPA）と呼ばれるZTNAサービスを開発しました。本サービスはグローバルクラウドを利用し、内部アプリケーションへのシームレスでセキュアなアクセスを提供します。コストがかさみがちなIT部門を経営の救い手へと変えられる本サービスをお試しください。

Paychexのエンタープライズテクノロジサービス担当シニアマネージャであるCarlo Cong氏が語る、吸収合併に伴うIT統合の際のZTNAによる簡素化と加速化についての詳細をご確認ください。

CMA-CGNの事例を見る

ZscalerのZTNAソリューションを7日間無料でお試しください。

7日間のZTNAデモを開始する

ZTNAに関するお問い合わせ先はこちら：sales@zscaler.com

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、数多く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150拠点以上のデータセンタに分散された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。

+1 408.533.0288
Zscaler, Inc. (HQ) - 120 Holger Way - San Jose, CA 95134
zscaler.jp