リモートワークを安全に促進

ゼットスケーラーによる事業継続ソリューション

zscaler™

今最も重要なのは、従業員やコミュニティのメンバの健康を守ることです。そのために企業にはコロナウイルス（COVID-19）感染のリスクを軽減するよう努力することが求められています。同時に、事業継続を保証し、とりわけ従業員が完全に社外で勤務する体制へ移行する場合は、生産性の維持にも努める必要があります。全従業員をリモートワークへと早急に移行する必要性に迫られている多くの企業は、このことによって大きな課題に直面することになります。

> クラウドファーストインフラストラクチャへの投資の回収を特に期待できるのは、VUCA [Volatility（揮発性）、Uncertainty（不確実性）、Complexity（複雑さ）、Ambiguity（曖昧さ）] 環境に適用できた場合である
>
> DB Schenker、CIO/CDO兼取締役、Markus Sontheimer氏

リモート管理が可能で、全員がリモートワークに対応できる組織もありますが、多くの企業では、従業員全員（場合によっては数十万人のユーザ）がリモートアクセスに移行した際、管理しているネットワークアーキテクチャに過剰な負荷がかかり、通常のIT管理に加えて処理が追いつかなくなる可能性があります。

リモートワークの急増を好機と考えるサイバー犯罪者も増えており、世界中の個人や企業を標的にする、**コロナウイルスに関連したサイバー攻撃** が増えています。攻撃者は、マルウェア、ランサムウェア、ボットなどを仕掛け、新しくリモートワークを始めた従業員とそれに伴って拡大する攻撃対象領域を悪用しています。

企業は、リモートワークへの移行の影響を十分に認識する必要があります。

帯域幅

リモートワークにVPNベースのインターネットエグレスを利用している企業は、予想外の問題に直面している可能性があります。ビデオコラボレーショントラフィックの急増によって、既存のインターネットエグレス接続が飽和状態に陥る恐れがあり、VPN接続が増えることで、インフラストラクチャの負荷が過剰になります。

セキュリティ

リモートワークの保護が必要です。従業員全員がリモートワークに移行した場合、必要なサービスやアプリへのアクセスにどのような影響があるでしょうか？　現在のセキュリティスタックはトラフィックの急増に問題なく対応できるのでしょうか？

ユーザーエクスペリエンス

Office 365などのSaaSアプリケーションには、最適化されたルーティングが必要ですが、ネットワークホップ数の増加とともに接続パフォーマンスのラグが大きくなります。VPNを経由して多数のリモートユーザがまずセントラルロケーションに接続する必要がある仕組みでは、この問題がさらに深刻化します。

コスト

どのようなソフトウェア、ITリソース、インフラストラクチャが新たに必要になるか、それらすべてのコストはどれほどか、試算する必要があります。

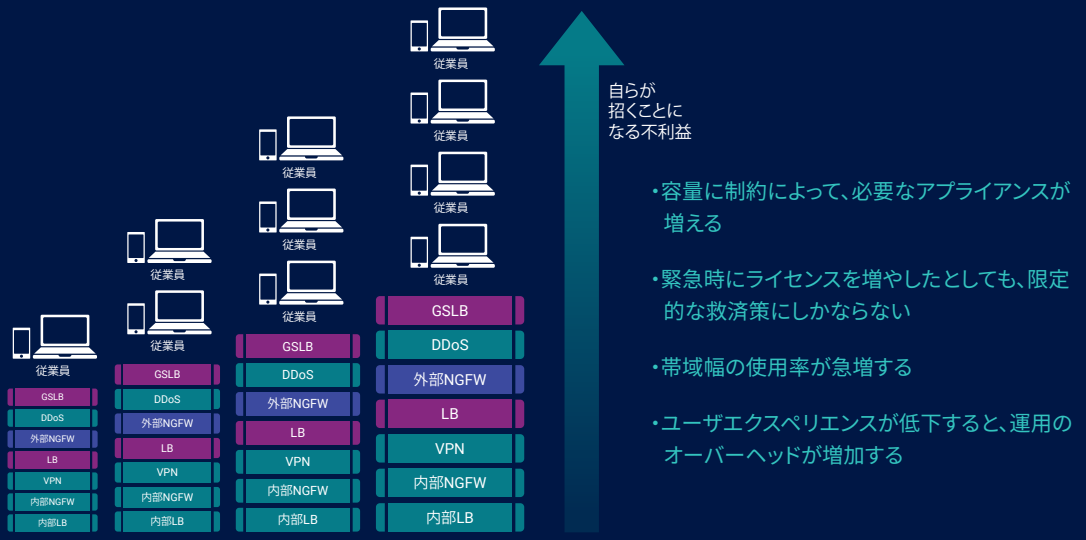
時期

リモートワークの運用モデルの導入までに数か月あるいは数年かかる可能性があることを考えた場合、リモートワークにどれほど早期に移行できるのか、またどのような戦略で移行を進めることになるのか、検討が必要です。

法規制環境

法規制が厳しい業界では、緊急時に陥った場合でも、コンプライアンスルールが緩和されるとは限りません。新たにリモートワークを始めた従業員が誤って有害なアプリケーションにアクセスし、会社をコンプライアンスに違反させてしまう可能性があります。

リモートユーザの急増に伴い、VPNの課題も増加



1.VPNのユーザとトラフィックが増加すれば、エンタープライズネットワークの課題も増加します。

VPNテクノロジには、ゲートウェイアプライアンスとそれをサポートするインフラストラクチャ（上記の図1を参照）のスタックが必要であり、どちらにも、帯域幅やライセンス容量の制約が存在します。VPNの単一イングレスポイントモデルも外部攻撃対象領域となり、分散環境のアプリケーションへのユーザトラフィックのバックホールによって、パフォーマンスが低下します。

Zscaler Internet Access（ZIA）・Zscaler Private Access（ZPA）は、SaaS、インターネット、プライベートアプリケーションへのセキュアアクセスを前提に構築されたクラウド提供型サービスを使用することで、リモートワーカの課題の軽減を可能にします。

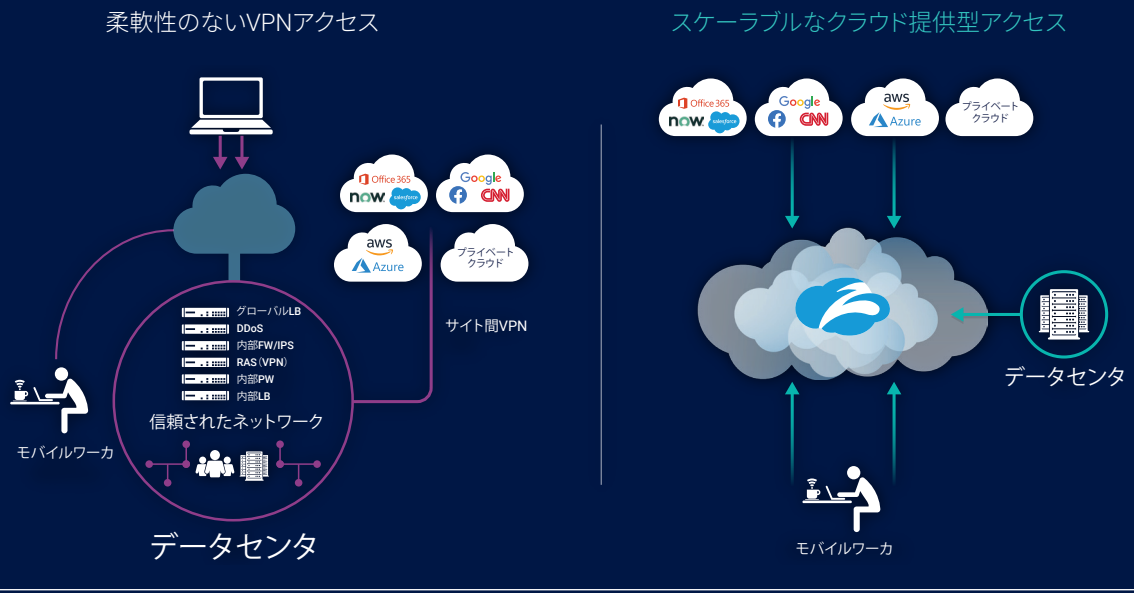


図2. セキュリティが保証されないVPNアクセスモデル（左）は、コストの増加と柔軟性の欠如、リモートアクセスの急増によってすぐに過負荷の状態に陥ります。ゼットスケーラー（右）などのクラウド提供型リモートアクセスは、優れたスケーラビリティによって、リモートワークの増加にも対応できます。

ゼットスケーラーによるセキュアリモートアクセスの実現

事業目標	戦略的能力	重要な戦術	ゼットスケーラーの使用
ネットワーク容量を確保する （例：回線帯域幅、ハードウェアメモリ、リソースなど）	企業には、帯域幅、ハードウェア、メモリなどの増加に対応できる動的スケーラビリティが必要であり、重要ではないトラフィックを排除または最小限にするためには、可視性も必要です。	時間帯、地理的な場所ごとにユーザネットワーク時間をスケジュールします。 ユーザの職種や役職（最高責任者、ITやカスタマサポートの担当者など）に高い優先度を設定し、必要な場合にいつでもネットワークにアクセスできるようにします。	**ZIAとZPAを導入し、インターネットのアプリやデータ、さらには、**パブリッククラウドプロバイダへのダイレクト接続を可能にし、ヘアピンルーティングを発生させることなく、すべてのトラフィックに会社のセキュリティポリシーが適用されるようにします。
最小限の導入オーバーヘッドで柔軟なスケーラビリティを構築する	運用担当者の負担を増やすことなく、リモートワークの従業員の急増に、可能な限り迅速に対応します。	クラウド対応アプリケーションへのアクセスを活用することで、アプライアンス、ライセンス、または地理的分散のボトルネックを解消します。	**リモートワーカをゼットスケーラーのグローバルクラウドプラットフォームへと移行**する方法であれば、数十人あるいは数十万人もの新規ユーザであっても、数週間あるいは数か月ではなく、数日で対応し、高信頼性のセキュアなアプリケーションアクセスを提供できます。
従業員によるアプリケーションやデータへのアクセスを保護する	リモートワークの従業員は、リモートでの作業中に、アプリケーションやデータにアクセスできなければなりません。	ID、職務、アクセス要件、地理的な場所に基づき、リモートワーカに適用する、会社やビジネスに固有のポリシーとセキュリティのルールを開発します。	ZPAとコネクタを展開し、Zscaler Appまたはブラウザベースのアクセスを使用し、**カスタムポリシーに基づいて、ユーザを許可されたアプリケーションに接続します。**結果として、アプリケーションやデータへのセキュアアクセスが可能になるだけでなく、外部に公開されるインバウンド接続が排除され、ネットワークの攻撃対象領域が少なくなります。
サードパーティによるアプリケーションやデータへのアクセスを保護する	契約社員、コンサルタント、ベンダ、パートナーについても、ネットワークを公開することなく、アプリケーションやデータへのアクセスを許可する必要があります。	許可されたアプリケーションに限定して、サードパーティによるアクセスを可能にし、ネットワーク接続を排除することで、水平方向の移動の可能性を最小限にします。	**ZPAのブラウザベースのアクセス**を活用することで、サードパーティのきめ細かいコントロールと可視化が可能になります — ソフトウェアをインストールする必要はありません。
データセンタやマルチクラウドのプライベートアプリケーションへのシームレスなアクセスを維持する	高コストのバックホールなく、ユーザがさまざまなバックエンド環境のアプリケーションにアクセスできるようにする必要があります。	複数のサイトに置かれたアプリケーションへの動的かつ安全なダイレクト接続を提供します。	ZPAコネクタを**複数のバックエンドアプリ環境に展開します。**動的パス選択によって、どのような場所であっても、すべてのリモートワーカに透過的で高パフォーマンスのアクセスが保証されます。
リモートワークの従業員のデバイスを保護する	企業は、自社のセキュリティ境界の外に置かれた、リモートワークの従業員のデバイスを保護する必要があります。	状況に応じてエンドポイントに適用する、それぞれのアクセスに固有のポリシーを開発します。	**Zscaler App**を、プッシュ方式、セルフサービスポータル、App StoreあるいはPlay Storeを利用して、すべてのエンドポイントに展開します。 ZIAを使用して、Zscaler Appの導入環境にポリシーを適用することで、リスク許容レベルに合わせた保護が保証されるようにします。
すべてのアウトバウンドトラフィックにSSL復号化を採用する	**インターネットやSaaSアプリ**へのすべてのトラフィックを検査して、ポリシー、脅威分析、検知、修復が適用されるようにすることで、脅威を発見し、侵入を防ぎます。	すべてのトラフィックカテゴリを調査する必要があるのか、あるいは、リスクプロファイルによって除外を許可するのかを判断します（PCI DSSやHIPAAコンプライアンスなど）。	**ゼットスケーラーの証明書を使用して、すべての場所、すべてのエンドポイントで、ZIAのSSL復号化**を有効にします（最も迅速な導入が可能）。
ファイルが有害かどうかを判断する	従業員は、社内と社外のどちらでも、たくさんのファイルをやり取りする必要があるはずです。	リスクの観点から、**サンドボックスで検査する必要がある**ファイルタイプや場所を判断します。判断にあたっては、会社や部門がサポートできる条件を考慮します。	ZIAを使用し、最も危険なファイルの種類に対して、**「any-any」のクリーンアップルールを有効にし、隔離（Quarantine）ファイルタイプを実装します。**
重要な企業データの流出を防止する	重要なデータが外部に持ち出されないようにする必要があります。	DLP（情報漏洩防止）ルールを見直して調整し、EDM（Exact Data Match）を実装して、重要なデータの移動をより慎重に制限します。	既定またはカスタムの**ZIA DLP**ルールを使用して、トラフィックフローに含まれる機密データを見つけます。

適切な計画と行動によって、COVID-19の感染拡大の影響を受ける企業であっても、重要なビジネス目標を達成しつつ、従業員の安全を確保することができます。**ゼットスケーラーのクラウドによって構築されたセキュアアクセスサービスエッジプラットフォーム**は、ローカルインターネットブレイクアウトによるダイレクト接続を可能にすることを前提に設計されており、企業（およびそのリモートワーカ）が不確実な状況が続く中でも業務を遂行できるようにします。

ゼットスケーラーは、**事業継続プログラム**を提供することで、前例のない今の状況に企業が対応し、安心して仕事を続けられる環境を従業員に保証すると同時に、生産性を維持できるようサポートしています。

リモートワークを今すぐ保護する

ゼットスケーラーについて

ゼットスケーラーは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、シンプルではあるものの力強い概念に基づき、設立されました。
ゼットスケーラーは現在、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。

zscaler™