生産的で安全な在宅勤務を可能に

――ゼットスケーラーのクラウドセキュリティソリューション

クラウドを使用して、
従業員の安全とセキュリティ、
生産性を確保

zscaler™

多くの組織が何年も前から、リモートワークを保護する最良の方法について議論してきました。前例のない状況に直面した今、早急なリモートワークの実現が企業に求められています。すべての従業員が在宅勤務を開始することになった場合、果たして本当に実行できるのでしょうか？

生産的で安全な在宅勤務を実現するための6つの要件

ビジネスレジリエンスの鍵は、従業員の健康を確保しつつ、オフィスにいるときと同様に、自宅でも生産的かつ安全を高めることです。このようなレジリエンスを実現するには、リモートアクセスソリューションが次のような要件に対応できなければなりません。

1. **すべてのアプリケーション**
   外部（インターネット、SaaS）および内部（データセンタ、Azure、AWS）のすべてのアプリケーションへの安全なアクセス

2. **クラウドアイデンティティアクセス管理**
   デバイス、内部および外部のSaaSアプリケーションの統合のための最適化

3. **高速のユーザエクスペリエンス**
   Microsoft TeamsやZoomなどのツールを使用した生産的なコラボレーション

4. **セキュリティとコンプライアンス**
   すべてのユーザのサイバー脅威からの保護と情報漏洩防止

5. **数日での導入**
   迅速な導入を可能にするアジリティとシンプルさ

6. **可視性とトラブルシューティング**
   オフネットワークのユーザの問題の診断に必要な可視性とツール

従来型 ITインフラストラクチャで 在宅勤務プログラムをサポートする場合の課題

迅速な拡張が不可能

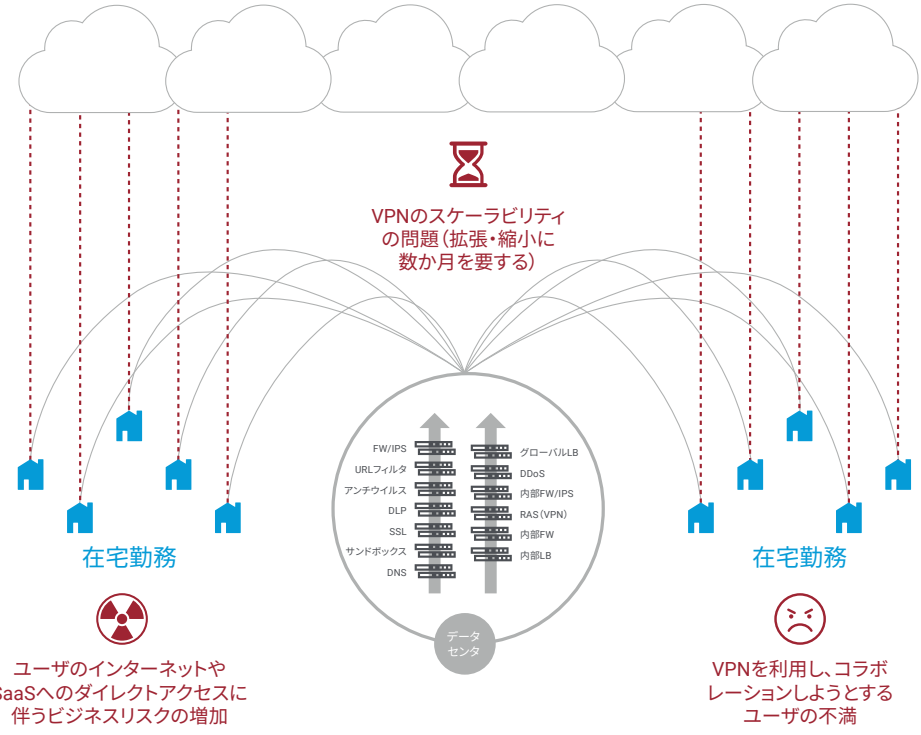
大人数の従業員を在宅勤務可能な状態にする際、VPNアプライアンスやゲートウェイアプライアンスを調達して構成を行い、ラックに収容してスタックを組み立てる形で対応しようとすると、ハードウェアサプライチェーンの混乱によって、数週間または数か月を要する可能性があります。このような遅延は従業員の生産性に影響し、結果としてビジネスパフォーマンスにも大きく影響します。回避策としてシングルテナントアプライアンスのVMを立ち上げると、複雑化が進むだけでなく、インターネットに公開されるすべてのファイアウォールが攻撃対象領域となり、最大規模のいくつものランサムウェア攻撃の入口となっていることから、リスクが高くなります。

リスクの増大

データセンタの内部アプリケーションへのアクセスにはVPNが必要ですが、インターネットやSaaSアプリケーションへのアクセスにも必要であるわけではありません。自宅で高速なユーザエクスペリエンスを求めるユーザは、適切なセキュリティコントロールを利用することなく、これらのアプリケーションにダイレクトアクセスするようになるでしょう。サイバー犯罪者はこの事実をよく認識しており、新たなランサムウェア、高度なソーシャルエンジニアリングの攻撃、標的型攻撃などを次々と仕掛けてきます。

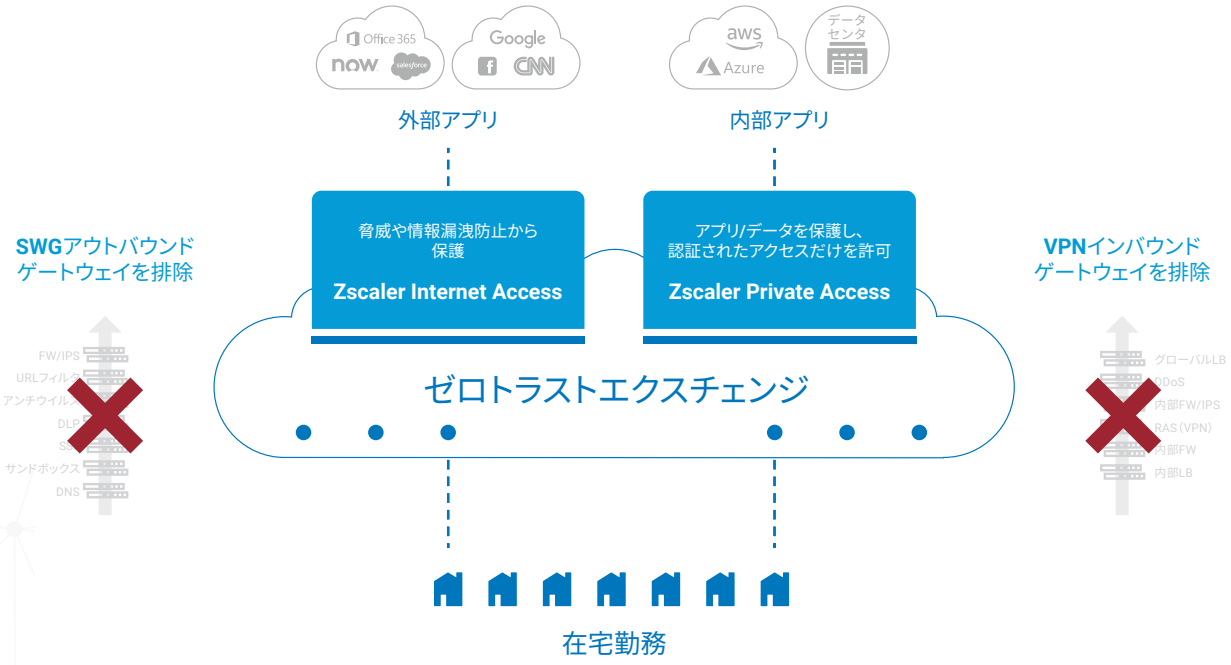
ユーザエクスペリエンスの低さ

Office 365やZoomなどのアプリケーションは、コラボレーションを推進し、さまざまな場所で働く従業員の生産性を向上させる上で重要な役割を果たします。課題となるのは、これらのアプリケーションやその他のSaaSアプリケーションがダイレクトアクセスを前提に設計されていることです。中央のインターネットゲートウェイへのVPN接続を利用してトラフィックをバックホールすると、レイテンシが発生し、ユーザの不満が募り、さらには、ユーザのコラボレーションの阻害要素となる可能性があります。



高速かつ安全な在宅勤務を可能にするには、専用のセキュリティクラウドが必要です

アプリケーションやインフラストラクチャのクラウドへの移行を進める組織においては、迅速に、いつでも効率的に移行する必要があることから、アジリティは、大きな優位性につながる要素となります。ビジネスを中断させる恐れのある予期しない出来事が発生した場合、このニーズはさらに大きなものとなります。マルチテナントプラットフォームとしてゼロから構築されたゼットスケーラーは、新しい世界、すなわち、クラウドが新たなデータセンタであり、インターネットが新たなネットワークである世界への安全な移行を可能にします。ゼットスケーラーのプラットフォームサービスは、あらゆる状況と規模、さらには、自宅やオフィスなどのさまざまな場所で、どのようなデバイスからでも、ビジネスを遂行できるようにすることを目標に開発されました。セキュリティをお客様に近づけるために、世界中に150以上のデータセンタがあり、クラウドのキャパシティは日々増加しています。



- **動的に拡大・縮小できる**、クラウドネイティブでマルチテナントのアーキテクチャ
- **6大陸の150箇所**に分散するグローバルなデータセンタ
- **すべての主要インターネットエクスチェンジとの**数百のピアリング
- **大量の暗号化されたトラフィックの完全インスペクションを可能にする、**プロキシベースのアーキテクチャ
- **クラウドは毎日120,000以上**の一意のセキュリティアップデートを15分ごとに受信し、オンデマンドで40以上の外部脅威をフィード
- **クラウドは毎日950億のトランザクション**を処理し、AIとMLのモデルを適用することで、新たな脅威も特定してブロック
- **クラウドのいずれかの場所で検知された脅威から**すべてのユーザを保護

ゼットスケーラーを活用してセキュアで快適な在宅勤務を実現

すべての内部アプリ（DC、AWS、Azure）と外部アプリ（SaaS、インターネット）への安全なアクセスを可能にします

在宅勤務でも高い生産性を維持するには、オフィスで働く場合と同じレベルのセキュリティと快適なアクセスが必要です。内部アプリへのアクセスにはVPNが必要ですが、パフォーマンスの低下やVPN接続の切断などの問題が発生した場合、ユーザがVPNをオフにし、適切なセキュリティコントロールを回避してインターネットやSaaSアプリケーションにアクセスする可能性があります。もちろん、そのようなリスクを回避する方法はあります。ゼットスケーラーは、ログインやログアウトを必要としないシームレスなユーザエクスペリエンスをリモートユーザに提供します。ネットワーク接続が変更された場合もアクセスは継続し、クラウドで直ちにセキュリティが適用されます。

VPNを排除することで、セキュリティとユーザエクスペリエンスが向上します

ゼットスケーラーは、最新アプローチによるアプリケーションアクセスの保護を可能にすることで、使用量の急増によってパフォーマンスに多大な影響を与える、VPN経由のトラフィックのバックホールの問題を解決します。ゼットスケーラーを利用すると、ユーザは、世界中の150箇所のデータセンタに分散するゼットスケーラーのクラウドを経由してアプリケーションに接続されます。接続する場所にかかわらず、包括的なセキュリティとポリシーの適用によってユーザが保護されます。ゼットスケーラーを採用すれば、インバウンド VPNゲートウェイインフラストラクチャの拡張に必要な高いコストを排除できるだけでなく、段階的に廃止することができます。

クラウド IAM（アイデンティティ /アクセス管理）との統合による条件付きアクセスを設定できます

企業のアプリケーションやデータをクラウドに移動するには、どの従業員にどのクラウドリソースへのアクセスを許可するかをより詳細にコントロールする必要があります。クラウド IAM（アイデンティティ /アクセス管理）ソリューションは、アイデンティティと認証のサービスを一元化することで、ITチームがクラウド環境とそのセキュリティを詳細にコントロールし、どのユーザがどのアプリケーションにいつアクセスしているかを追跡できるようになります。ゼットスケーラーは、Azure AD、Okta、Pingなどの主要 IAMベンダと密接なに統合によって、コンテキストアクセスポリシーを適用します。

> ZPAは、DB Schenkerの事業継続計画において極めて重要な役割を果たしてきました。今では、従来のVPN接続に戻りたいと考える従業員はいません。

DB SCHENKER

グローバルインフラストラクチャサービス担当シニアバイスプレジデント、Gerold Nagel氏

数週間・数か月単位ではなく、数日で運用を開始できます

ゼットスケーラーは100%クラウドのサービスで、アプライアンスのインストール、構成、管理が不要であるため、高速かつ容易に導入できます。ゼットスケーラーのクラウドでホスティングされるビジネスポリシーに基づいて、ユーザのトラフィックがローカルでゼットスケーラーに転送され、ユーザは、 Microsoft IntuneなどのMDMシステム経由の簡単に配布できる軽量のアプリであるZ Appを利用でき、Webアプリの場合はブラウザだけあればすぐにアクセス可能です。

ゼットスケーラーは、アイデンティティプロバイダとの統合によって、 ACLやIPアドレスに頼ることなくユーザを認証し、コンテキストアクセスを適用します。小さいVMで、フロントエンドの内部アプリであるApp Connectorと内側から外側へのマイクロトンネルを使用して、ユーザを承認されたアプリに接続します。ゼットスケーラーがすべてのルーティングとロードバランシングを処理するため、インフラストラクチャの拡張を心配する必要はありません。

従業員とデータをインターネットのサイバー脅威から保護します

サイバー犯罪者は、新しいマルウェア、高度なソーシャルエンジニアリングによる攻撃、標的型攻撃などを次々と仕掛け、通常はセキュリティ境界の背後に置かれている企業ネットワークを利用しているユーザが自宅で働くようになっていることを十分に認識しています。ゼットスケーラーは、世界中に分散するクラウドにセキュリティを移行し、インターネットの完全セキュリティスタック（高度な脅威保護、 SSLインスペクション、情報漏洩防止、サンドボックス、リモートブラウザ分離、 CASB）をユーザに近づけることで、高速かつ安全なユーザエクスペリエンスを実現します。ユーザがどこに接続するかにかかわらず、ユーザを追いかけ、セキュリティポリシーが適用されます。

ユーザの問題の診断に必要な可視性と迅速なトラブルシューティングを提供します

全従業員が在宅勤務で働き、その多くが管理対象外のデバイスを利用し、ネットワークがインターネットとなると、ネットワークアクティビティを監視できるかどうかが重要な課題になります。ユーザやアプリケーションのリアルタイムの可視性に加えて、パフォーマンスの問題の原因をすばやく特定するには、ユーザのデバイスやアプリケーションのあらゆる場所で何が起きているかを正確に把握できる必要があり、そうすることで、修正アクションを実行できるようになります。

> ゼットスケーラーを利用することで27,500人のユーザ全員がリモートワークを開始できると説明したとき、NOVの経営陣は驚きを隠せない様子でした。
>
> **National Oilwell Varco、CIO、**Alex Philips氏

ゼットスケーラークラウドセキュリティプラットフォーム

ゼットスケーラーのサービスは100%クラウドで提供され、インターネットアプリやクラウドアプリ、データセンタ内のプライベートアプリ、パブリッククラウドやプライベートクラウドへの高速かつ安全で信頼性の高いアクセスを提供します。アクセスのベースとなるSD（Software-Defined）ビジネスポリシーが、接続する場所や使用するデバイスに関係なくユーザを追いかけ、適用されます。

> 我々が提供する重要な要素の1つが、アプリ単位のアプローチです。このアプローチによって、過剰なアクセスを付与せずユーザが必要とするものを提供することが可能です。
> ZIAとZPAの組み合わせによって、はるかに柔軟にサービスを提供できたほか、拡張もとても簡単で、すべてのトラフィックを処理することができました。
>
> Takeda
>
> **Takeda Pharmaceutical、CSO、**Mike Towers氏

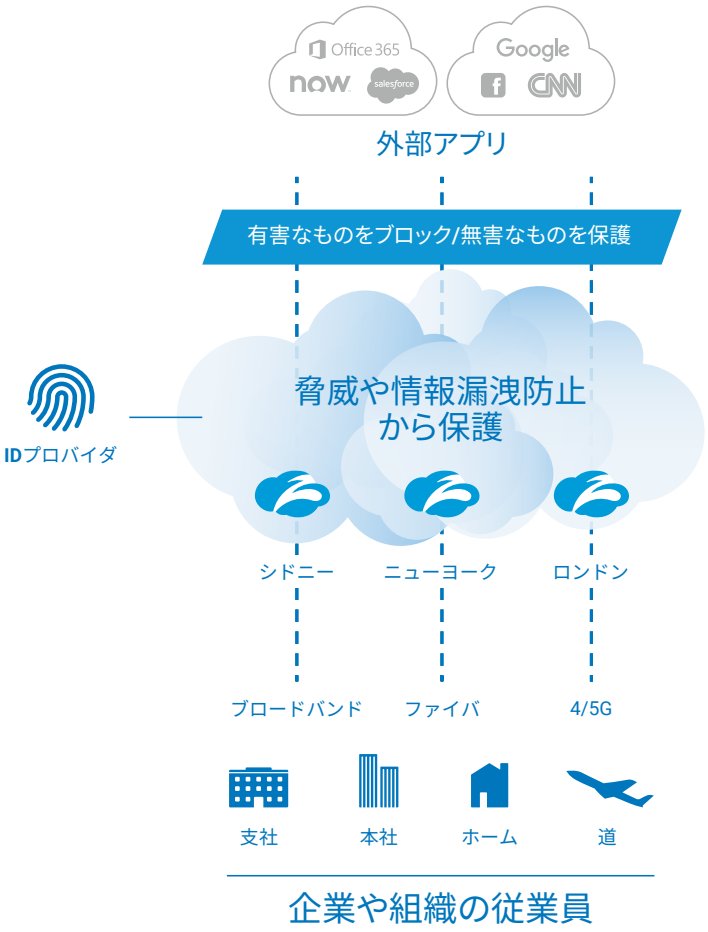
Zscaler Internet Access（ZIA）とZscaler Private Access（ZPA）は、ゼットスケーラーのクラウドセキュリティプラットフォームを構成し、アウトバウンドやインバウンドのセキュリティゲートウェイをクラウドに移行します。ゼットスケーラーをインターネットへの最初のホップにすることで、すべての接続が保護され、ユーザが接続する場所やアプリケーションがホスティングされる場所に関係なく、ポリシーが適用されます。

Zscaler Internet Access：SaaS（Security stack as a Service）

ZIA（Zscaler Internet Access）は、アウトバウンドSecurity-as-a-Service全体をクラウドから提供することで、従来型のセキュアWebゲートウェイアプローチのコストと複雑さを解消します。セキュリティをグローバルに分散するクラウドに移行することで、ゼットスケーラーはインターネットゲートウェイをユーザに近づけ、高速のユーザエクスペリエンスを実現します。組織は、場所に関係なく、すべてのオフィスやユーザにまで簡単に保護を拡張でき、ネットワークやアプライアンスのインフラストラクチャを最小限にすることができます。

リモートユーザトラフィックは、ゼットスケーラーの軽量のZ AppまたはPACファイルを経由してゼットスケーラーのクラウドに転送されます。Zscaler Internet Accessは、ユーザとインターネットの間に位置し、SSLも含め、複数のセキュリティ技術のトラフィックのすべてのバイトをインラインでインスペクションするため、Webやインターネットの脅威からの完全な保護が可能になります。**クラウドサンドボックス**、**次世代ファイアウォール**、**情報漏洩防止（DLP）**、**ブラウザ分離**、**CASB**をサポートするクラウドプラットフォームを利用することで、今すぐ必要なサービスから始め、ニーズの拡大に合わせてその他のサービスの利用も追加できます。

詳細については、ZIAの**データシート**をお読みください。

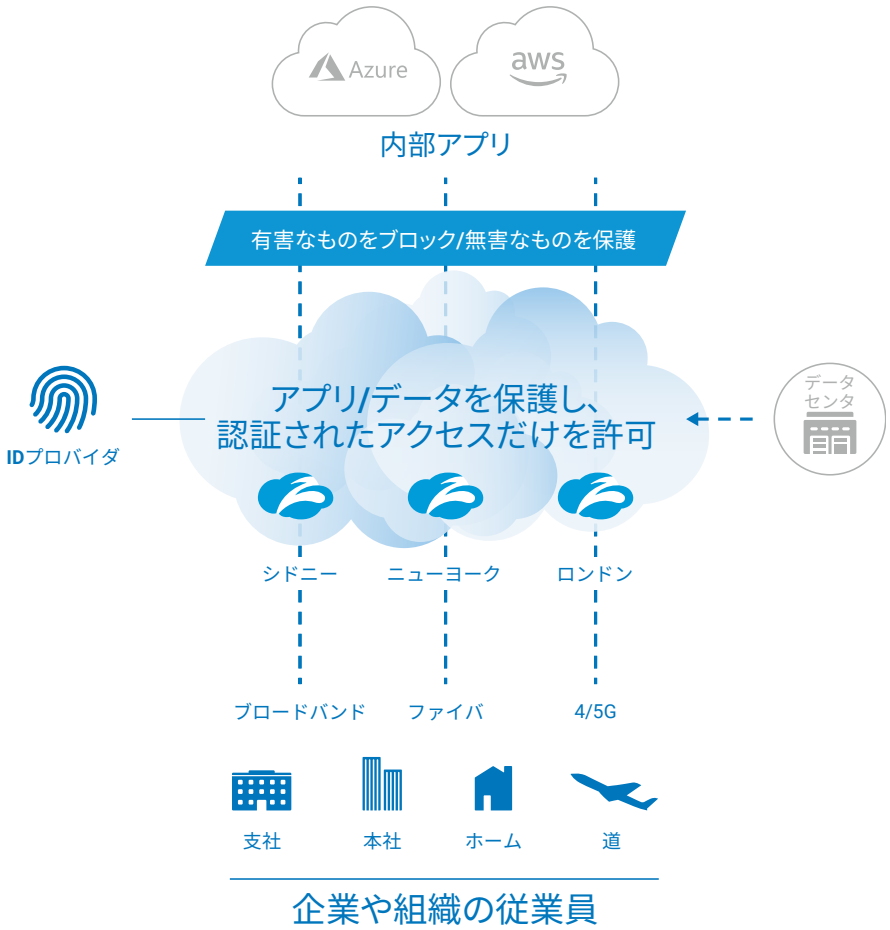


Zscaler Private Access：VPNに代わるスケーラブルな選択肢

ZPA（Zscaler Private Access）は、データセンタやパブリッククラウドの内部管理アプリへの高速かつ安全なアクセスをユーザに提供します。ZPAを利用することで、バックホールや面倒なログインを必要としない、シームレスなユーザエクスペリエンスが実現します。VPNを起動してアプリケーションにアクセスする必要はなく、すぐにアクセスしてアプリケーションを利用できます。ZPAアーキテクチャは、セキュリティにも多くのメリットももたらします。IPアドレスが外部に公開されないため、DDoS攻撃の標的になることはありません。さらには、ユーザがオンネットワークにならないため、マルウェアの水平移動や拡散のリスクも軽減されます。

それでは、どのように動作するのでしょうか？ ZPAは、指定されたユーザと指定されたアプリの間に1つのセキュアセグメントを作成し、許可されたユーザだけが特定のプライベートアプリケーションにアクセスできるようにします。Zscaler Adminコンソールで定義したビジネスポリシーに基づき、アクセスが許可されます。ZPAは、高速かつシームレスなユーザエクスペリエンスを実現します。VPNクライアントにログインする（そしてセッションを開始するたびにそれを続ける）ことなく、ノート PC、携帯電話、またはタブレットでZscaler Appを開くだけで、高速のローカル接続を利用できます。

詳細については、ZPAの**データシート**をお読みください。



短時間で簡単に使い始められるゼットスケーラー

ゼットスケーラーのサービスは100%ソフトウェアベースで、数日で導入できます。

Z App Connectorを展開

小規模のVMがデータセンタ、パブリッククラウド、またはプライベートクラウドのプライベートアプリケーションの前に配置されます。

Zscaler App（Z App）をインストール

この軽量アプリは、MDM（モバイルデバイス管理）ソリューション経由での配布が可能で、ユーザのデバイスポスチャを保証し、安全なマイクロトンネルをゼットスケーラーのクラウドにまで拡張します。

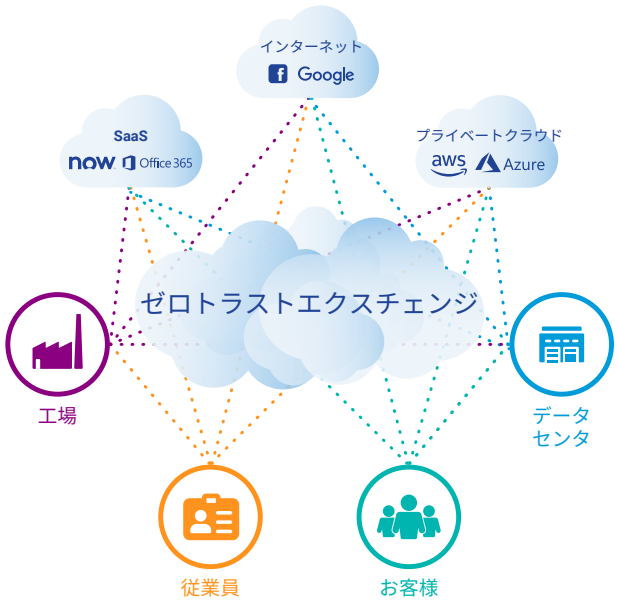
Zscaler Adminコンソールでポリシーを構成

アクセスポリシーの設定が完了すると、あらゆる場所にいるユーザにポリシーが適用されます。

従業員を保護し、組織を保護

アプリケーションやインフラストラクチャのクラウドへの移行、ユーザのオフネットワークへの移行に合わせて、ゼットスケーラーは、常時オンのクラウド配信型セキュリティを提供してきました。現在、Forbes Global 2000の400を超える企業がゼットスケーラーを利用し、ユーザ、アプリケーション、デバイスのすべての接続を保護しつつ、高速のユーザエクスペリエンスを提供しています。

生産的で安全な在宅勤務が実現すれば、WANインフラストラクチャやネットワークセキュリティに対する考えが広がり、さまざまな検討を始められるはずです。ネットワークが中心ではなくなった、現代のクラウドとモバイルの世界においても、ネットワークベースのセキュリティインフラストラクチャに投資し続ける理由があるのでしょうか？



ゼットスケーラーのクラウドは、
ゼロトラストエクスチェンジとして動作し、
Any-to-Anyの安全な接続を可能にします

ゼットスケーラーのサービス、および在宅勤務のイニシアチブを
安全に実現する方法については、以下をご参照ください

https://www.zscaler.jp/solutions/work-from-home

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp