Zscaler Private Access for Microsoft Azure

Azureの内部アプリへの
セキュアリモートアクセス

zscaler™

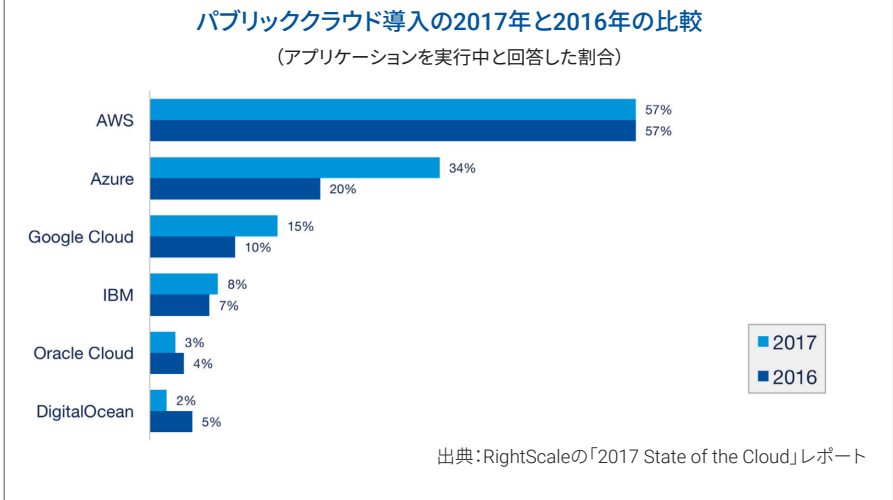
新しいクラウド時代へのセキュアアクセス

企業がAzureに移行する理由

Microsoft Azureは、グローバルなITトランスフォーメーションに欠かせない存在になっています。企業はAzureを使用することで、グローバルで柔軟性の高い相互接続されたMicrosoftネットワークを活用し、Infrastructure as a Serviceで実行することで、コストと複雑さを削減できます。Azureクラウドは、アジリティを提供し、柔軟な拡張を可能にしつつ、変化するビジネス要件に常に対応できるようにすることで、企業を支援します。

企業はこれらのさまざまなメリットを認識するようになっており、内部アプリケーションのAzureへの移行を中心に、アプリケーショントランスフォーメーションイニシアチブを積極的に推進しています。このような移行によって、企業におけるAzureの利用が急増し、現在、43%の企業がAzureでアプリケーションを実行しています。

Azureにはユーザにとってもさまざまなメリットがあり、モバイルユーザは、場所やタイムゾーンに関係なく、アプリケーションやサービスに簡単にアクセスできます。ユーザの生産性の最大限の向上に加えて、クラウドの利便性は、ユーザの考え方にも変化をもたらしました。クラウドアプリケーションへのシームレスなアクセスを経験したリモートユーザは、Azureクラウドでホスティングされる内部管理アプリケーションを含むすべてのアプリケーションに「クラウドのような」ユーザエクスペリエンスを期待するようになりました。



RightScaleの「2017 State of the Cloud（2017年版クラウドの現状）」レポートによると、企業におけるMicrosoft Azureの利用が2017年に急増しました。

アプリケーションがクラウドに移行したにもかかわらず、今もリモートアクセスにデータセンタが利用されるのはなぜでしょうか?

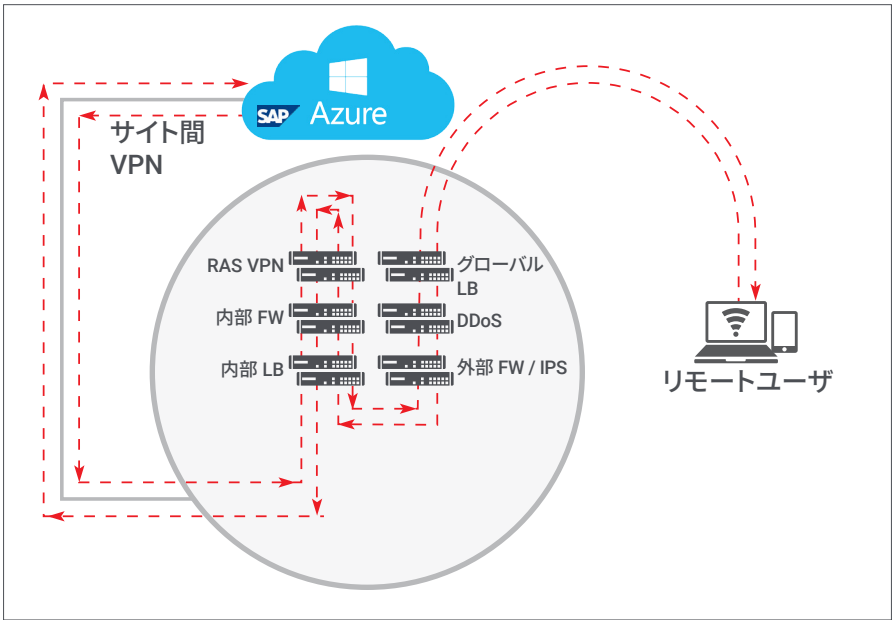
企業とそのユーザがアプリケーションをクラウドに移行するメリットを手に入れるためには、今こそリモートアクセスの再考が必要です。初期の時代のセキュリティは、データセンタに置かれたデータとそこで動作するアプリケーションの保護を中心とするものでした。セキュリティアーキテクトは、ネットワークの周囲に安全な境界を構築することが保護の最良の方法であると考えました。そこで、多くのセキュリティチームにおなじみの城を堀で囲む形のアーキテクチャが誕生しました。

ネットワークという点で見れば、1つのデータセンタでの内部アプリケーションのホスティングは、城を堀で囲む形のセキュリティアーキテクチャに適した方法です。そしてこのことは、アプリケーションにアクセスするためには、リモートユーザやブランチオフィスのすべてのトラフィックがデータセンタにバックホールされることを意味します。多くの場合、このデータセンタは世界の別の場所に存在します。

現在、かつてはデータセンタに存在していたアプリケーションのAzureクラウドへの移行が進んでいます。これにより、保護する必要があるアプリやデータが境界の外側に存在することになり、かつては安全だった境界という概念は崩壊します。トラフィックを中央のデータセンタにルーティングするハブ&スポーク方式では、Azureで動作するアプリを効率的に運用できません。ところが、今日のリモートアクセスソリューションは今も、トラフィックを最初にデータセンタにルーティングするということを前提にしており、有効な代替手段がないことから、多くの企業で今もリモートアクセスVPNが利用されています。

1990年代以来、内部アプリケーションへのリモートアクセスを提供する唯一の手段として、リモートアクセスVPN（仮想プライベートネットワーク）が利用されてきました。ところが、内部アプリがAzureなどのクラウドプロバイダに移行し、アクセスするリモートワーカも増えたことで、データセンタ経由でのトラフィックのルーティングは有効な方法とは言えなくなりました。

> DMZとVPNは、1990年代のネットワークを前提に設計されたものであり、デジタルビジネスの保護に必要とされるアジリティが欠如しているため、有効な手段ではなくなりました
>
> ガートナー
> 2016年9月



リモートユーザからインターネットへのトラフィックが遅くなるのは、クラウドからオープンインターネットに向かう前にデータセンタのセキュリティスタックにルーティングされ、帰りも同じ経路を逆戻りするためです。

リモートアクセス VPNの課題

ユーザエクスペリエンスの低さ

Azureクラウドで実行中のアプリケーションにアクセスしようとするユーザは、リモートアクセス VPNにログインする必要があります。トラフィックは、Azureに直接送られるのではなく、データセンタ経由でルーティングされます。

高いコストと複雑さ

リモートアクセス VPNには複数のゲートウェイアプライアンスが必要です。そのため、データセンタごとに同じ構成のゲートウェイを置く必要があり、結果として、複数の地域で拡張するのが困難になります。リモートアクセス VPNは、柔軟性、シンプルさ、コスト削減など、クラウドの価値の阻害要素となります。

攻撃のリスク

リモートアクセス VPNはリモートユーザをオンネットワークにするため、ネットワークがマルウェアや信頼されていないユーザデバイスに起因するその他のセキュリティ攻撃の標的になる可能性があり、攻撃者が水平移動して複数のアプリに被害が拡大する恐れがあります。

Zscaler Private Accessによるクラウドへのダイレクトアクセス

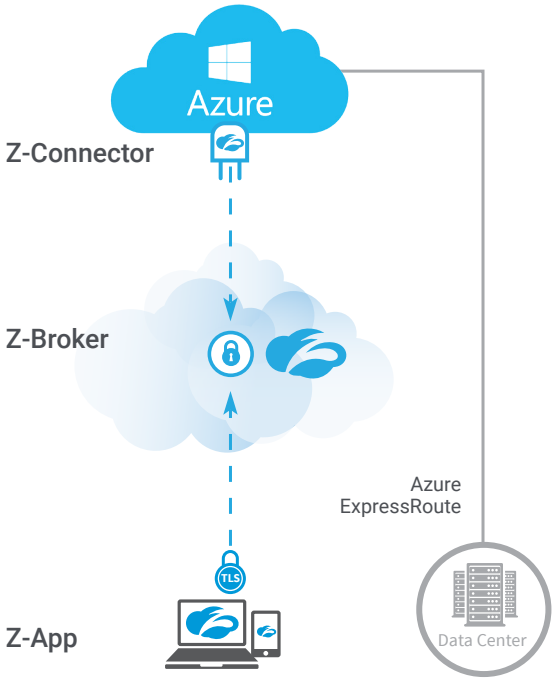
Zscaler Private Access（ZPA™）は、ゼットスケーラークラウドを使用した内部アプリケーションへのセキュアリモートアクセスを可能にする、ゼットスケーラーの革新的サービスです。ZPAによって、データセンタを中心とするリモートアクセスVPN主導の考え方から脱却し、最新のクラウドベースのアプローチに移行できます。

ZPAは、リモートユーザに内部アプリケーションへのアクセスに必要なシームレスなユーザエクスペリエンスを提供しつつ、シンプルなセキュリティによって、企業に必要とされるセキュリティを提供することで、ネットワークトランスフォーメーションの成功に大きく貢献します。

Z-Connector：
アプリの前面に置かれる（内側から外側への接続）

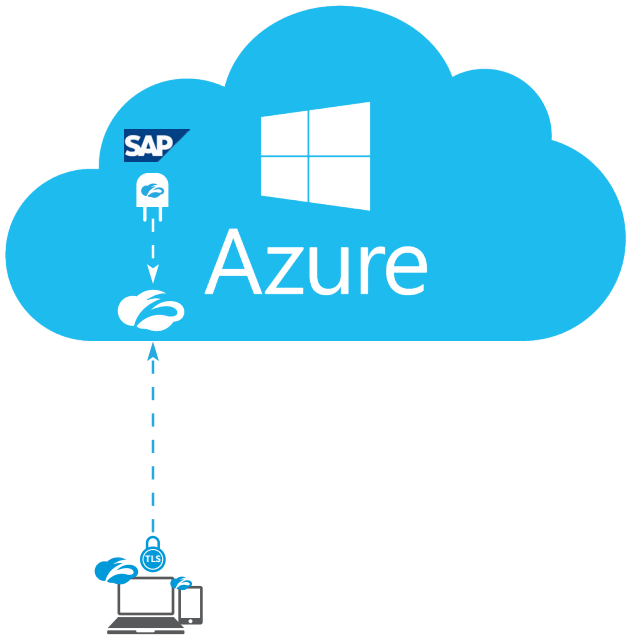
Z-Brokers：
ユーザからアプリへのセキュア接続

Z-App：
アプリへのアクセスを要求



Zscaler Private Access for Azure

多くの企業が現在、Azureクラウドのメリットと ZPAによって提供される強力なセキュリティとSDP（Software-Defined Perimeter）の両方を手に入れています。ZPAを使用すると、リモートアクセスVPNアプライアンスが不要になり、それに関連する落とし穴も解消されます。ZPAソリューションは、クラウドへのダイレクト接続をすべてのユーザに提供し、リモートアクセスゲートウェイ経由でルーティングすることなく、Azureで動作するアプリに迅速かつシームレスにユーザを接続します。



リモートユーザ向けのAzureのアプリへの高速アクセス

この共同ソリューションにより、ゼットスケーラーはMicrosoftのグローバルな機能を活用し、リモートユーザ向けにAzureに置かれたアプリケーションへの高速のクラウドダイレクトアクセスを提供できます。ZPAソリューションのコンポーネントであるZEN（Zscaler Enforcer Node）は、数百のデータセンタとグローバルロードバランサで構成されるAzureのネットワークで動作します。ZENは、モバイルユーザとアプリケーションの接続を仲介し、トラフィックをルーティングします。そして、Azureで動作し、アプリケーションの前面に配置されたZ-Connectorによって、ZENへの内側から外側への接続が提供されます。

ZPAとAzureの組み合わせにより、ユーザトラフィックは常にユーザの場所に基づき、最適パスで送受信されます。リモートユーザが最も近いアプリケーションにアクセスすることになるため、ユーザエクスペリエンスが向上し、生産性も向上します。

高速パフォーマンスだけでなく、シームレスなユーザエクスペリエンスも実現します。VPNでは、ユーザはアプリケーションにアクセスするたびにログインが必要ですが、ユーザのモバイルデバイスにインストールされたZ-Appを利用すれば、1度のログインでユーザが認証され、Azureのアプリケーションに迅速に接続されます。

ZPA for Azureを採用すべき理由

ZPA（Zscaler Private Access）とAzureのクラウドベースのセキュリティアプローチによって、データセンタからクラウドに環境が移行した場合であっても、内部アプリケーションへのアクセスを許可するユーザを判断できます。この共同ソリューションは、ZPAの4つの重要な原則に基づいて構築されています。

1 | **ユーザをオンネットワークにしない** – ユーザに企業ネットワーク全体へのアクセスが許可されることはありません。アクセスはアプリケーションに対して許可されるものであり、IPアドレスやACLによってポリシーを定義する必要はありません。

2 | **アプリケーションを公開しない** – 内部 IPアドレスがインターネットに公開されることはありません。内部アプリケーションは企業の「ダークネット」に置かれ、アクセスを許可されたユーザ以外に内部アプリケーションが公開されることはありません。

3 | **インターネットが新しいセキュアネットワークになる** – ZPAは、インターネットを活用することで、動的でアプリに固有のTLSベースのエンドツーエンド暗号化を可能にします。すべてのデータの機密性が維持され、お客様は独自のPKIを使用できます。

4 | **ポリシーによってアプリケーションレベルのセグメンテーションが提供される** – ユーザ対ネットワークのアクセスではなく、許可されたアプリケーションにのみアクセスが可能になり、アプリケーションセッションごとに専用のマイクロトンネルが作成されます。

優れたリモートユーザエクスペリエンス

- Azureに置かれたアプリへの高速アクセス
- ログインセッションごとにVPNクライアントの使用は不要
- Azureやデータセンタに置かれたアプリへのシームレスなユーザエクスペリエンス

管理の複雑さを軽減

- 1時間程度の容易な実装、VPNゲートウェイの設定は不要
- ネットワークではなく、アプリケーションのセグメンテーション
- Azure ADとの統合
- OktaなどのSSO（シングルサインオン）プロバイダとの統合
- Azure ExpressRouteとの連携

Azureに置かれた内部アプリへのセキュアリモートアクセス

- ユーザをオンネットワークにしない
- Azure上の特定のアプリケーションへのポリシーベースのアクセス
- 水平移動による他内部アプリケーションへのアクセスのリスクなし
- Azureで動作するすべてのアプリケーションの可視化
- 進行中のユーザアクティビティの可視化

ビジネス価値の向上

- ハードウェアの購入を不要にすることでコスト削減を実現
- リモートユーザの生産性の向上
- サービスモデルで運用コストがわかりやすく、予測が可能

> ゼットスケーラーによって、パブリックAzureクラウドやハイブリッドクラウドの環境への移行が簡素化されます

Microsoft Azure Networking担当バイスプレジデント
Yousef Khalidi氏

ZPA（Zscaler Private Access）とAzureを体験する

ZPAとAzureによって、内部アプリケーションへのアクセス方法が再定義され、これまでよりはるかに簡単な方法でクラウドを採用し、モバイルワークを始められるようになりました。この新しいソリューションによって、変更の阻害要因とされることが多いセキュリティが、内部アプリケーションのAzureへの移行を加速させるメカニズムになります。

詳細またはライブデモの視聴については、お問い合わせください。
www.zscaler.jp/company/contact

zscaler™

新しいクラウド時代へのセキュアアクセス