データシート

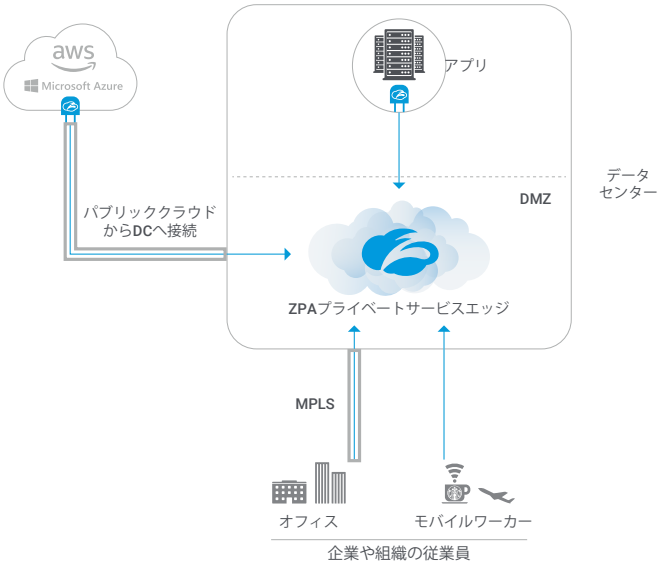
ZPAプライベートサービスエッジ

ZPA Private Service Edge

ゼロトラストネットワークアクセス（ZTNA）を
あらゆる拠点のユーザに対してオンプレミスで提供

ガートナーは多くの企業に対し、ゼロトラストネットワークアクセス（ZTNA）サービスの採用によるアイデンティティに基づいたプライベートアプリケーションアクセスの実現と、ネットワークアクセスの必要性の排除、そして、アプリケーションがインターネットに公開されるリスクの最小限化を推奨しています。ZTNAが注目を集めるようになった今、クラウド提供型のZscaler Private Access（ZPA）を導入して、あらゆる場所から接続するユーザに対して、プライベートアプリケーションへの高速かつ安全でシームレスな接続を提供する組織が増えています。

しかし、自社環境にアプリケーション接続サービスの展開を希望する組織も少なくありません。そこでゼットスケーラーでは、そのようなニーズに対応するサービスとして、ZPAプライベートサービスエッジを発表しました。ZPAサービスの追加機能としてご利用いただけるZPAプライベートサービスエッジは、お客様の組織がホスティングし、ゼットスケーラーが管理する、すべての機能を備えた、(お客様ごとの) シングルテナントのインスタンスであるブローカです。ZPAプライベートサービスエッジは、お客様のサイトまたはパブリッククラウドサービスのいずれかに置くことができ、ZPAクラウドサービスと同様、このオンプレミスのサービスによって、ポリシーが適用され、承認されたユーザと指定されたプライベートアプリケーションが結合されます。



ZPAクラウドサービスの機能をユーザに近い場所で提供

クラウド提供型のZPAサービスでは、ユーザがプライベートアプリケーションへのアクセスを要求すると、ユーザのトラフィックがインターネット経由でのクラウドデータセンタに転送されます。承認されたユーザとプライベートアプリがクラウドで連結されることで、両者が接続されます。この方法によってバックホールが排除されるため、ZPAは、オンプレミス、パブリッククラウド、あるいはプライベートクラウドで実行中のプライベートアプリケーションへのアクセスを必要とするモバイルユーザである従業員やサードパーティのユーザなどのリモートユーザに最適な選択肢です。また、オンプレミスのユーザが、オンプレミスで実行中のアプリケーションにアクセスしようとする場合、インターネットへの接続は不要であるように思えるかもしれませんが、ここでもZPAプライベートサービスエッジが最適な選択肢となります。

「ZPAによって、我々がこれまでに経験したことのない極めて詳細なレベルで、ネットワークで何が起き、誰がどのアプリケーションにアクセスしたかといった情報を瞬時に把握できるようになりました」

Johnson Controlsのグローバルインフラストラクチャネットワークサービス担当ディレクタ Peter Daly氏

クラウドサービスと同様、ZPAプライベートサービスエッジは、Zscaler App（Z App）とApp Connectorとの接続を処理します。ZPAプライベートサービスエッジが導入されると、ゼットスケーラーのクラウドに登録され、ZPAプライベートサービスエッジによる、関連するポリシーと設定のダウンロードと適用が可能になり、パス選択の判断もキャッシュされるようになります。ZPAプライベートサービスエッジは、お客様のネットワーク環境にインストールされる軽量の仮想マシンもしくはRPMとして展開されます。セットアップが完了すると、ZPAプライベートサービスエッジは、ZPAクラウドサービスとまったく同じように動作します。オンプレミスのユーザやZPAクラウドサービスがない国のリモートユーザの場合、プライベートアプリケーションへのアクセスがZPAプライベートサービスエッジ経由で仲介されるため、常にシームレスで高速かつ安全なアクセスが可能になります。

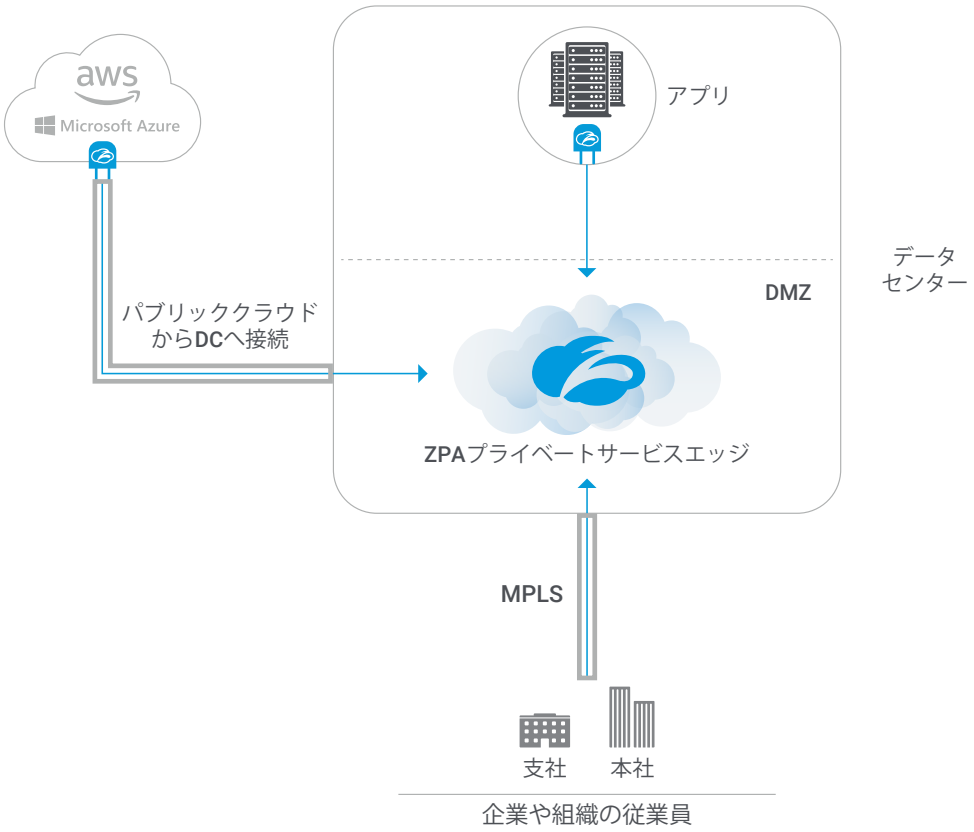
管理者はいつでも、ZPAを構成してプライベートサービスエッジとZPAクラウドサービスの両方が使用されるようにすることで、プライベートアプリケーションへの接続を必要とするユーザに最高のエクスペリエンスを提供できます。

ZPAプライベートサービスエッジの一般的なユースケース

ZPAをオンプレミス環境に拡張することで、次のような多くのユースケースで多大なメリットがもたらされます。

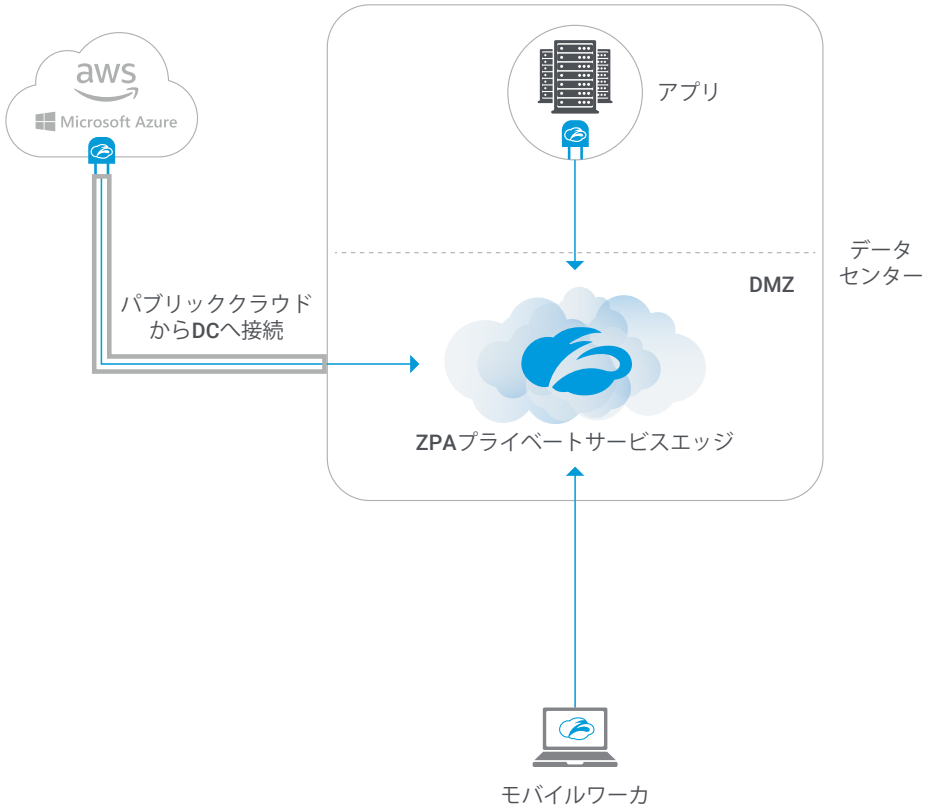
オンプレミスの従業員のためのゼロトラストネットワークアクセス

オンプレミスまたはパブリッククラウドで実行中のアプリケーションにアクセスする、本社やブランチオフィスのユーザの場合、トラフィックがZPAパブリックブローカに渡された後にローカルで実行中のアプリケーションに戻すというやり方は、まったく意味のないものです。ZPAプライベートサービスエッジは、オンプレミスのユーザとオンプレミスのアプリケーションの間のローカルブローカとして機能するため、ユーザの処理が高速になり、ネットワーク管理者の複雑さが軽減され、最小限の権限アクセスを提供することでビジネスデータのリスクが軽減されます。



リモートワーク環境向けのローカルサービスエッジ

ZPAブローカが存在しない国（アルジェリアなど）では、リモートユーザが国外（ドイツなど）で実行中のZPAブローカに接続し、本社でオンプレミスで実行中のアプリにアクセスする必要があります。ZPAプライベートサービスエッジがあれば、このようなリモートユーザがオンプレミスで実行中のアプリケーションにアクセスすると、ZPAが自動的にユーザごとの最速パスを判断し、ジョブに最適なブローカを選択します。



コンプライアンスのためのプライベートインフラストラクチャ

自然災害が多い国や厳しい法規制が適用される業種（銀行など）では、セキュリティサービスをクラウドでホスティングするのではなく、オンプレミスで実行することで、高可用性が保証されるようにする必要があります。ZPAプライベートサービスエッジは、ローカルで動作し、お客様の環境ですべての仲介を処理することで、国内の業界の規制へのコンプライアンスを可能にします。

「ZTNAによって、リソースへのアクセスコントロールが可能になることで、攻撃対象領域を抑えることができます。ZTNAによって隔離されることで、効率的な接続が可能になり、アプリケーションをインターネットに直接公開する必要がなくなります。インターネットは信頼できない転送手段と見なされ、サードパーティのプロバイダによってコントロールされるクラウドサービスや、自己ホスティング型のサービスといった仲介者を経由して、アプリケーションにアクセスするようになります。」

ガートナー、「ゼロトラストネットワークアクセス市場ガイド」
Steve Riley、Neil MacDonald、Lawrence Orans共著、2019年4月

ZPAプライベートサービスエッジの主なメリット

ネットワークセグメンテーションを必要とすることなく、ZPAの仲介サービスをオンプレミスで（アイデンティティに基づいて）ホスティングできるため、Zscaler Private Accessの既存または新規のお客様に多くのメリットが提供されます。

- **シンプルなセグメンテーション**

  「送信元 IP対送信先 IP」のポリシーから「ユーザ対ホスト名」のポリシーへと移行します。ファイアウォールのIPアドレスのリストをメンテナンスする、また、ローカルユーザやリモートユーザに異なるポリシーを設定する等といった、ネットワークセグメンテーションの複雑さを軽減します。ZPAプライベートサービスエッジによってポリシーフレームワークがよりフラットで管理しやすいものになります。

- **ハイブリッドクラウドとマルチクラウドの迅速な導入**

  ZPAプライベートサービスエッジは、データセンタまたはパブリッククラウドで動作します。したがって、プライベートアプリをAzure、AWS、Googleなどのパブリッククラウドサービスに移行した後も、アクセスポリシーを変更する必要はありません。

- **ローカルユーザへの最小限のアクセス権の付与**

  ゼロトラストネットワークアクセスがオンプレミスで可能になり、承認されたローカルユーザと指定されたアプリを仲介することで、1対1の接続が確立されるため、ネットワーク経由の水平方向のアクセスを防止し、リスクを最小限にできます。

- **高可用性**

  インターネット接続が十分に整備されていない地域では、ZPAプライベートサービスエッジによって大きなメリットがもたらされます。アクセスポリシーが数週間キャッシュされるため、インターネット接続が失われた場合もセキュア接続が可能になります。

- **高速でシームレスなユーザエクスペリエンス**

  リモートとローカルのどちらであっても、変わらないアクセスが提供されます。オンプレミスとパブリッククラウドの仲介のデュアルアクセス機能によって、オンプレミスで実行中のプライベートアプリにアクセスするローカルユーザや、ZPAクラウドブローカが国内に存在しない国のリモートユーザのエクスペリエンスが自動的に最適化されます。

- **コスト削減**

  内部ファイアウォールの利用を少なくすることで、新たな投資の必要性を回避できます。ローカルユーザによるアプリケーションへのアクセスを可能にするために、ファイアウォールを追加したり、新しいネットワークセグメントの作成したりする必要はありません。

- **コンプライアンス**

  このプライベートインフラストラクチャは、厳格な規制や標準によって、クラウドホスティング型テクノロジの使用が認められていない業種にも対応し、お客様のコンプライアンスを支援します。

ZPAサービスに関するご質問については、ゼットスケーラーにお問い合わせいただくか、**zscaler.jp/zpa**を参照してください。
ZPAプライベートサービスエッジの詳細については、**ゼットスケーラーのヘルプドキュメント**を参照してください。

ゼットスケーラーについて

ゼットスケーラーは2008年に、「アプリケーションのクラウド移行に伴って、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。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。

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