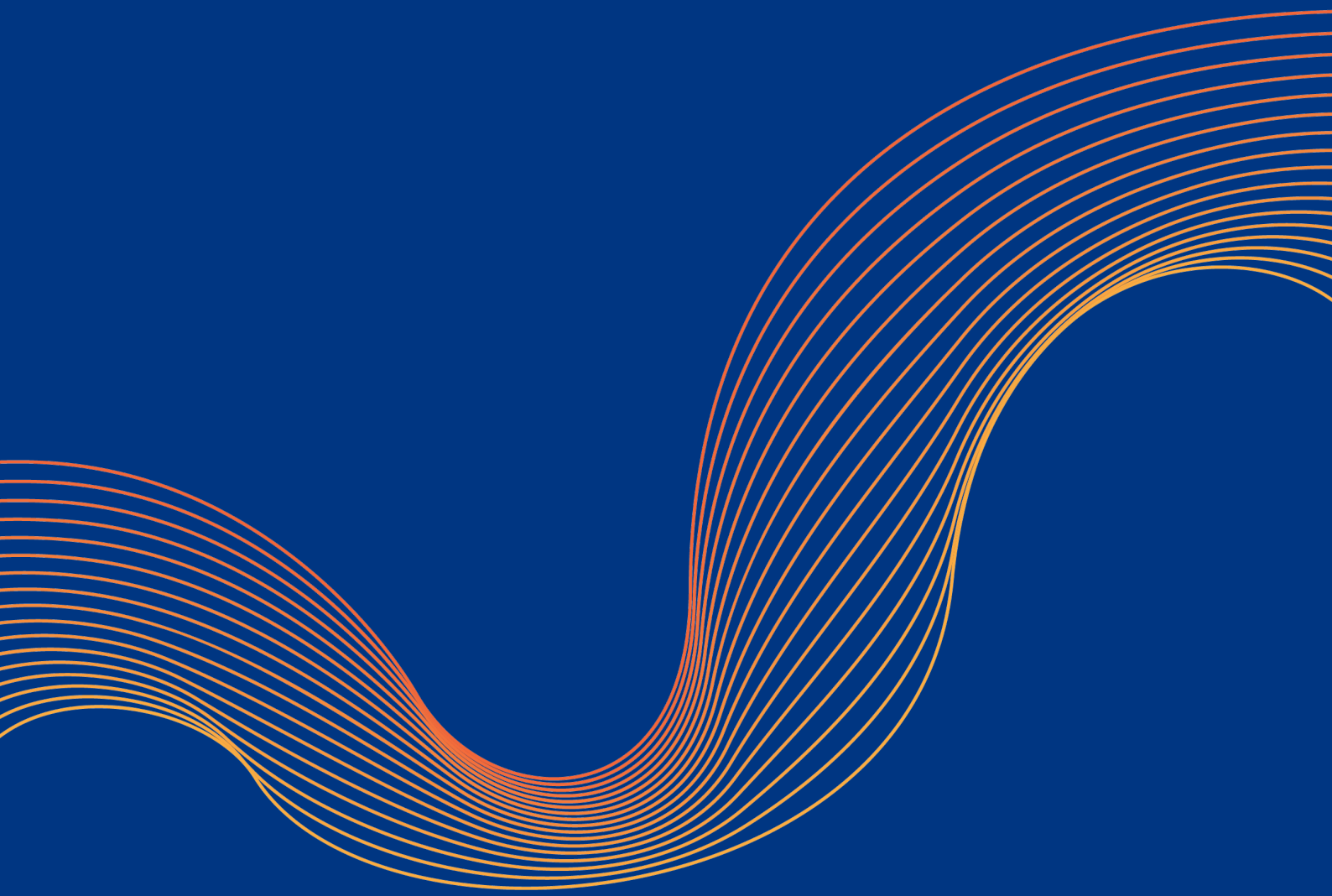
ホワイトペーパー

CLOUDFLARE

VPNをZTNAに置き換えることは可能か？3つのリモートアクセスアプローチを比較



03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

目次

はじめに

安全でシームレスなリモートアクセスはビジネスの支えとなります。リモートユーザーの生産性を高めるとともに、ユーザーとアプリケーションの機敏性と耐障害性を備えた接続性を維持するためにITチームが費やす時間を削減します。しかし、多くの組織にとってリモートアクセスは依然として課題のままです。

かつて、VPN接続といえば数人のリモートユーザーが企業ネットワークに短時間だけ接続するためのシンプルな手段でした。しかし、以前よりも従業員の働く場所が分散し、組織がリモートユーザーの接続を長時間安定的に保つ必要が出てきたことにより、パフォーマンスの遅さ、セキュリティリスクの高まり、拡張性に関する懸念など、このアプローチの欠陥が浮き彫りにされてきました。

リモートアクセスのニーズが増えるにつれて、従来のVPNの実装から、より安全で機能性の高いリモートアクセスソリューションへと移行する組織が増えています。ゼロトラストネットワークアクセス(ZTNA)は、特定のアプリケーション、プライベートIP、ホスト名の周囲に安全な境界を作り、デフォルトで許可するVPN接続を、IDとコンテキストに基づきアクセスを許可するデフォルトで拒否するポリシーに置き換えます。

2020年は、リモートアクセス利用全体の約5%が、主にZTNAによって提供されました。従来のVPNアクセスが抱える限界と、より正確なアクセスやセッションコントロールを届ける必要性から、2024年までにはその割合が40%になると予測されています。[1]

VPNと比較して、ZTNAが企業にもたらす利点は機能の拡張性を含めても明らかに優れていますが、多くの組織はVPNインフラストラクチャーを完全に置き換えることはできないと考えています。しかし、ZTNAが以前よりも堅牢になり、VPNの問題点が多くなるにつれて、この考えは急速に変化しつつあります。このペーパーでは、VPNとZTNAのリモートアクセスソリューションを比較し、利点と限界を明らかにし、移行プロジェクトで最も考慮すべき重要な点に焦点をあてます。また、CloudflareによるZTNAの提供方法について説明し、既存のVPNインフラストラクチャーから、リモートユーザーにとってより高速で安全なZero Trust接続への移行の推奨手順をご紹介します。

[1] Riley、Steve、MacDonald、Neil、Orans、Lawrence.「Market Guide for Zero Trust Network Access」ガートナーリサーチ、https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access。2021年6月21日現在。詳しくは表1をご覧ください。

アプローチ#1：従来のVPN

VPNは、数十年にわたって、組織が一定のプライバシーとセキュリティを保護しながらリモートユーザーが企業ネットワークへ接続するために使用してきました。VPNは、ユーザーが、攻撃者によってデータをのぞかれたり盗まれたりする可能性のある公共のインターネットで機密情報にアクセスにする代わりに、暗号化された接続を通して安全に社内リソースにアクセスできるようにします。

最も一般的な2つのVPN実装モードは、クライアントベースVPNとクライアントレスSSL-VPNです。それぞれに利点と課題があります。

クライアントベースVPNは、暗号化されたトンネルを経由してリモートユーザーをプライベートネットワークに接続します。この接続はソフトウェアアプリケーションまたはクライアントを通じて確立されます。ネットワーク内のリソースへの永続的なアクセスを得るために一度だけユーザー名とパスワードを使って認証する必要があります。

利点：いったん接続すると、ユーザーはラテラルムーブメント（横展開）自由にできるため、アプリケーションにアクセスし社内ホストに接続することによって簡単に複数のリソースに素早くアクセスできます。

課題：

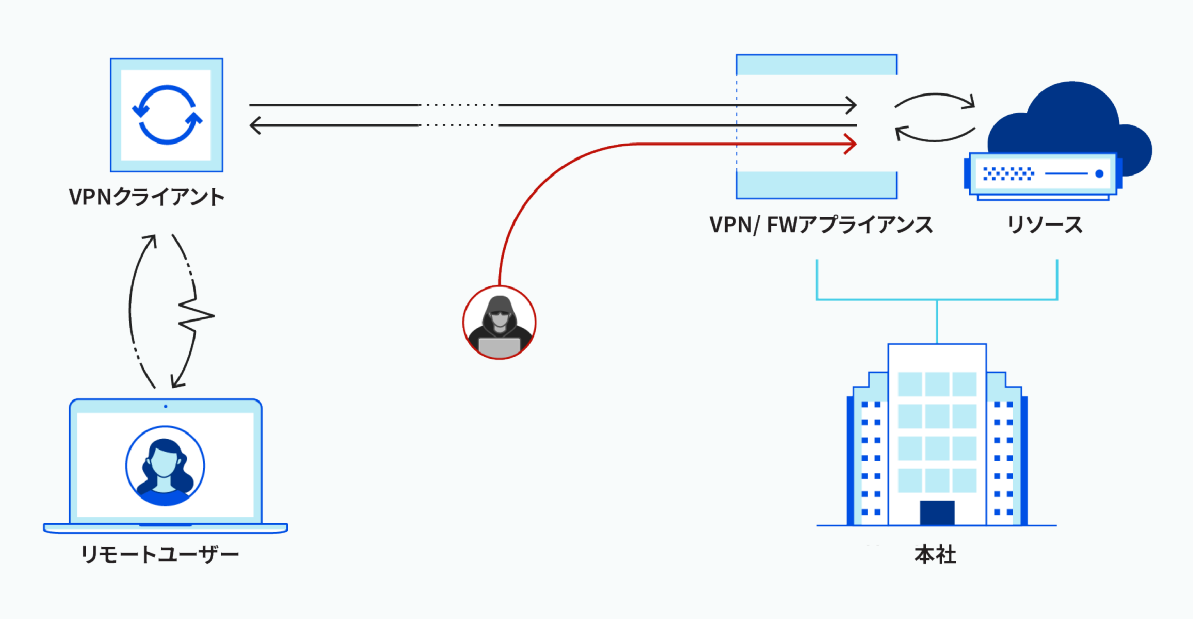
- **移動するユーザーやモバイル端末のための設計ではないこと。**ユーザーが移動すると、場所ごとにワイヤレスネットワークが変わり、ノートパソコンやモバイル端末もシームレスに再接続します。しかし、VPNクライアントは再接続を滑らかに行うのが得意ではないため、ユーザーは繰り返しVPNクライアントを強制的に再起動し再認証しなければならなくなり、生産性が失われ、IT部門のサポートが必要になる頻度が増えます。
- **可視性の低さ。**この方法では、データセンターの社内ファイアウォールの背後にあるVPNクライアントから、VPNインフラストラクチャーが暗号化されたトンネルを終了します。これらの接続については記録されるものの、どのアプリケーションユーザーがアクセスしたかや、アプリケーション内で何を行ったかが明らかになるような、アプリケーション別の集中型の記録は行われません。

クライアントレスSSL-VPNポータルは、数人のリモートユーザーをプライベートネットワーク内にある数個のブラウザベースアプリケーションへの接続を可能にします。この接続はVPNサービスを実行するネットワークアプライアンスに組み込まれたWebサーバーを使用することにより可能になります。

利点：デバイス上のクライアントを使用する代わりに、あらゆるWebブラウザからポータルのSSL証明書を使用して暗号化されたHTTPS接続を確立することで、管理下にないデバイスを使用する外部委託先も対象とすることができます。

課題：

- **セキュリティの懸念。**データセンター内のほとんどのVPNの設定ではユーザーに完全なアクセス権が付与されているため、請負業者などの非従業員に機密情報を扱うリソースやアプリケーションへの無制限のアクセスを付与したくない組織にとって問題になります。
- **同時多数接続に対応した設計になっていないこと。**最近のクラウドサービスとは異なり、ポータルのWebサーバーは増加する需要に合わせて自在に拡張することはできません。かわりに、さらに多くのネットワーク機器を設置し、負荷分散を行ってポータルを拡張しなければなりません。その拡張はしばしば大掛かりで、複雑で、残りのアプライアンスの機能が有効活用されない可能性があるため効果的ではありません。
- **クライアントレスSSL-VPNポータルはファイアウォールポートとWebサーバーを攻撃にさらします。**管理者は、社内アプリケーションにアクセスするためのポータル画面を提供しているWebサーバーに対して、インバウンド用のファイアウォールポートを開く必要があり、それによって外部からの脅威にさらされることになります。開いたポートとWebサーバー自体の両方をDDoSおよびWebアプリケーション攻撃から守る必要がありますが、この接続方法を安全に保つためにはより複雑な設定と高額な費用が必要になります。



VPNはリモートユーザーのために基本的なレベルのプライバシーを提供しますが、その設計にセキュリティや拡張性についての考慮はありません。従来、組織は、数人のリモートユーザーが企業ネットワークに短時間だけ接続するためにVPNを使用していました。しかし、リモートワークが普及するにつれて、VPNの問題が増大し始めています。

- **パフォーマンスの遅さ。**VPNインフラストラクチャーにトラフィック量や従業員による同時接続に対応するだけの処理能力が不足している場合、ユーザーはインターネット接続速度の低下を体感します。さらに、VPN用の機器がユーザーと、アクセスしようとしているアプリケーションサーバーの両方から遠い場所に設置されている場合、伝送時間が長くなり遅延が発生します。
- **企業ネットワークが攻撃に対して無防備になること。**VPNは一般的に「城と堀」モデルを採用しています。このモデルでは、ユーザーはいったんネットワークに接続すれば、すべての企業リソースへの自由なアクセス権を与えられます。重要なインフラストラクチャーやデータへのアクセスを制限する方法が組み込まれていないため、組織は次世代ファイアウォールやネットワークアクセス制御などの高額で複雑なセキュリティーサービスを構成せざるを得なくなります。そうしなければ悪意のあるラテラルムーブメントに対し脆弱なままになり、大規模なデータ漏洩につながります。

ホステッドVPNサービスの課題

一部のベンダーは、VPNサービスを実行するネットワークアプライアンスをパブリッククラウドに移行し、1つ以上のデータセンターで仮想マシンとして稼働させています。VPNは、追加的なセキュリティサービスとバンドル（またはデイジーチェーン方式で接続）してもしなくても構いません。

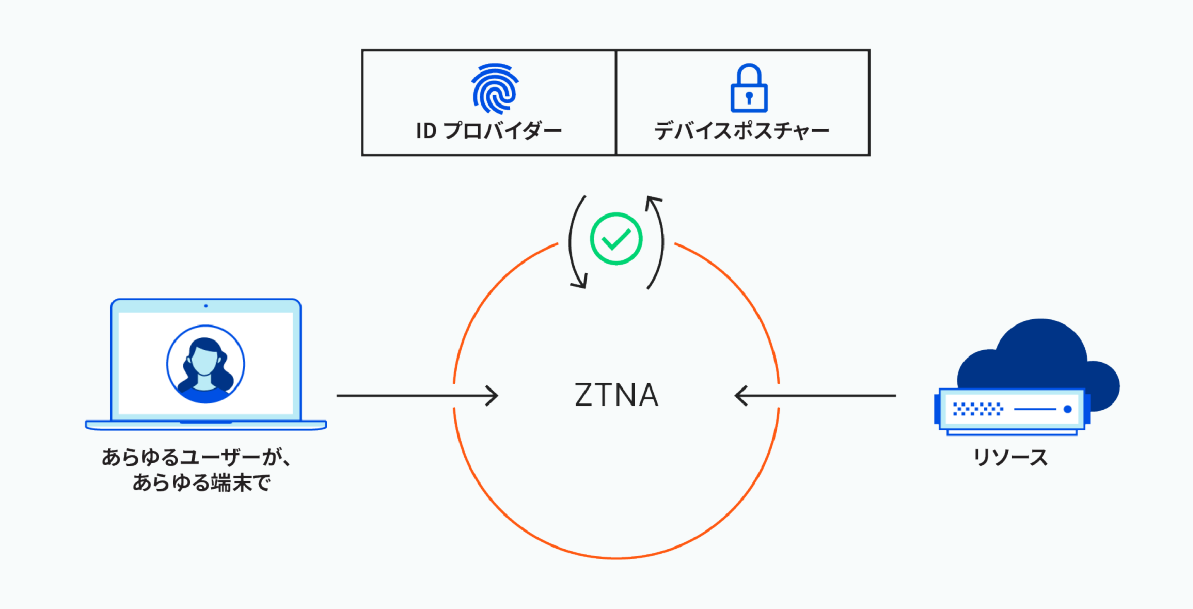
VPNをクラウドに置くことで、ハードウェアVPNアプライアンス固有の拡張性の問題が一部解決するように見えるかもしれません。しかし、そうしたとしても、いくつかの重大なセキュリティと拡張性の課題が発生します。

例えば、VPNにファイアウォールと追加的なセキュリティー機能を組み合わせたフルNGFW（次世代ファイアウォール）をホストする組織を考えてみましょう。NGFWはバンドルサービスとして提供されているので、特定の機能だけを個別に要求に応じて拡張することはできません。ひとつの機能を拡張するために、サービス全体の拡張が要求されます。そのためにはまた、各VMで行われる少量の計算を負荷分散するためにより多くのVMを稼働させる必要も出てきます。これは非実用的かつ非効率的なソリューションだというだけでなく、組織のリモートアクセスを継続的に拡張する必要があるため、費用が高くなる傾向があります。

アプローチ#2：ゼロトラストネットワークアクセス(ZTNA)

ゼロトラストセキュリティはVPN特有の多くの課題を回避します。ゼロトラストセキュリティはネットワーク内外のどのユーザーやデバイスもデフォルトで信頼しない原則に基づいています。データ漏えい、内部からの攻撃、その他の脅威のリスクと影響を軽減するため、ゼロトラストアプローチは以下のことを行います。

- すべてのログインとリクエストを認証および記録し、
- 全ユーザーおよびデバイスの厳格な検証を要求し、
- 各ユーザーおよびデバイスがアクセスできる情報を、IDとコンテキストに基づいて制限し、
- エンドツーエンドの暗号化を追加して、ネットワーク内のアプリケーションおよびデータを分離します。



VPNと同様、ZTNAの構成にはいくつかの方法があります。

1. **クライアントレス（またはサービスを起点とする）ZTNA**は、クライアントを使用する代わりに既存のブラウザを使用し、安全な接続を作成してユーザー端末を認証します。従来、クライアントレスZTNAはHTTP/HTTPSプロトコルを使用するアプリケーションに限定されていましたが、互換性が急速に進化しています。[2]
   - **利点：**クライアントレスZTNAはリバースプロキシ接続を使用して、閲覧許可されていないアプリケーションやデータへのユーザーによるアクセスをブロックし、管理者による管理により大きな制御権と柔軟性を与えて、アプリケーションへの直接アクセスを防止しています。
2. **クライアントベース（またはエンドポイントを起点とする）のZTNA**では、まずユーザー端末にソフトウェアをインストールしてから、制御するエージェントと認証されたアプリケーションとの間に暗号化された接続を確立します。
   - **利点：**クライアントベースのZTNAは、管理者はアプリケーションにアクセスするユーザーのデバイスポスチャー、所在地、リスクコンテキストに関するより多くのインサイトを把握できます。そのため、より細かいポリシーを作成して適用することができます。また、この方法はHTTP/HTTPSに限定されないため、SSH、RDP、VNC、SMB、およびその他のTCP接続を含むより広範囲の非HTTPアプリケーションへのアクセスに使用できます。

[2] *2021年6月時点で、CloudflareのZTNAソリューションはSSHおよびVNCアプリケーションへのクライアントレスアクセスをサポートしており、今後RDPのサポートも予定しています。*

ZTNA実装の課題

ZTNAには従来のVCPNより明らかに優れた点がありますが、リモートユーザーのネットワークアクセス保護への欠陥のないアプローチというわけではありません。企業がZero Trustを採用するメリットとデメリットを比較するとき、直面する可能性がある課題には以下のようなものがあります。

ソリューションが真のクラウドネイティブではない。

ベンダーがクラウドベースのZTNAを提供していない場合、顧客は自社のデータセンターにソフトウェアをデプロイする必要があることになります。その場合、瞬時に拡張を行えることや、スループットの限界が無いなどの主要な利点を失うことになります。

ベンダーがクライアントベースおよびクライアントレスZTNAオプションを提供していない。

この場合、リモートデスクトップ、SSH、ファイル共有など、HTTP以外のアプリケーションにユーザーを接続する必要がある組織にとっては価値が限定的なものになります。

複雑で時間を要する設定。

ポリシーオーケストレーションや（Terraformなどのツールを使用した）自動化のサポートを提供していないベンダーの場合、ID プロバイダーで既に行われている設定に加えて、管理者により多くの手動作業が発生する可能性があります。

リモートアクセスに対するCLOUDFLAREのアプローチ

リモートアクセスの保護と拡張は、面倒なセキュリティソリューションを積み重ねたり、パフォーマンスのトレードオフを生み出したり、不要な費用を発させない、シームレスなプロセスであるべきです。Cloudflareは、以下の利点と共に、あらゆるリモートアクセスのユースケースを取り扱えるようにチームをサポートします。

- **ユーザーと管理者のための簡単でリスクのないオンボーディング。**Cloudflareなら、既存のIDプロバイダーやエンドポイント保護プラットフォームを容易に統合することができ、Zero Trustポリシーを適用して企業のアプリケーションやリソースへのアクセスを制限することができます。
- **クライアントベースおよびクライアントレスZTNAのデプロイメントの柔軟性。**Cloudflareは、ウェブ、SSH、VNC、（および近い将来に対応予定のRDP）アプリケーションへの接続のためのクライアントレスのサポート、ならびに非HTTPアプリケーションおよび社内IP用プライベートルーティングのためのクライアントベースのサポートを提供します。

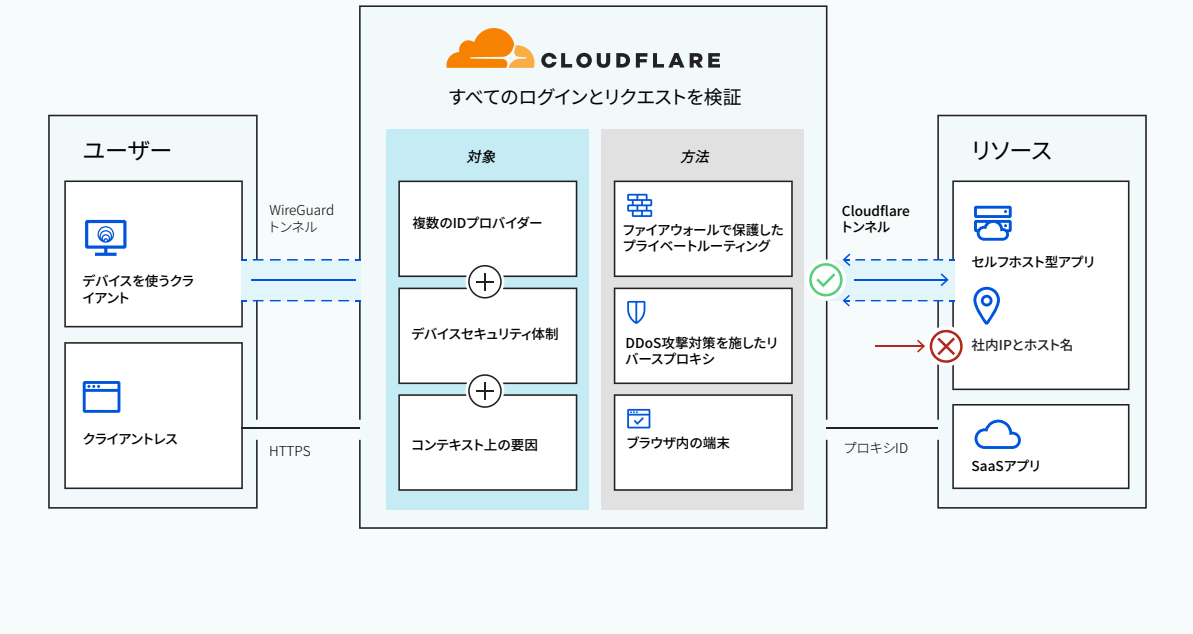


表1：Cloudflareによるリモートアクセスの課題への対応

⚠ 問題	✓ ソリューション	⚙ Cloudflareの実装
拡張の難しさ	グローバルエッジネットワーク	クラウドネイティブではないVPNサービスとZTNAサービス両方にとって拡張性の課題は悩みの種であり、リモートユーザーにアプリケーションやデータにアクセスすることを困難にします。 Cloudflareのグローバルエニーキャストネットワークは、VPNよりも高速なユーザー接続を提供するだけでなく、あらゆる規模のリモートの従業員が必要に応じて、安全かつ迅速に企業のリソースに接続できる環境を提供します。管理者は時間のかかる追加設定をする必要なありません。
モバイル端末との互換性の低さ	軽量クライアント	VPNおよびZTNAソリューションは、多くの場合モバイル端末やローミングデバイスでパフォーマンスが低くなるIPSecおよびSSLプロトコルを利用しています。 Cloudflare Warpクライアントは、より新しいWireguardプロトコルを採用しています。このプロトコルはユーザー空間で動作し、従来のオプションよりも高速なユーザーエクスペリエンスを提供しながら、より広範囲のOSオプションのセットをサポートします。CloudflareのWarpクライアントは、Windows、MacOS、iOS、Android、そして近日Linux端末で構成可能です。
DDoS攻撃対策が組み込まれていない、または脆弱	業界最先端のDDoS攻撃対策を内蔵	DDoS攻撃対策が組み込まれていない場合、多くの場合組織では追加的なセキュリティサービスを次々と繋ぎ合わせる必要があり、これによって構成の複雑さ、拡張性の問題、セキュリティの課題が発生します。 Cloudflareの67+ Tbpsネットワークは、あらゆるZTNAモードに対応したDDoS攻撃対策を内蔵し、最大規模の帯域幅消費型攻撃からもネットワークを保護します。
プロトコルの限界	非ウェブアプリのサポート	✓ モード互換性：SSH/VNCアプリケーション用クライアントレスZTNA、その他すべての非ウェブアプリケーション用クライアントベースZTNA。
ネットワークファイアウォールが組み込まれていない	内蔵のネットワークファイアウォール	企業ネットワークが拡大するにつれて、組織がバランスを取らなければならないセキュリティハードウェアも積みあがっていくことから、費用／パフォーマンス／セキュリティがトレードオフ関係になる原因となります。 Cloudflareでは、管理者はエッジでネットワークファイアウォールポリシーを適用できるようになり、ネットワークに出入りするどのデータを許可するかなどの詳細な制御を可能にするとともにトラフィックの流れの可視性を高めます。 ✓ モード互換性：クライアントベースZTNA
詳細な制御ができない	セキュアウェブゲートウェイ（SWG）を搭載	制限なくアプリケーションを使用できることは、組織にとって重大なセキュリティの問題を起こす可能性があります。厳格なポリシーがない場合、ユーザーが機密データやその他の企業リソースにアクセスして改ざんする恐れがあります。 CloudflareはZTNAとSWGを組み合わせることで、管理者がアプリケーション内でユーザーおよびデバイスのアクセス権に関してよりきめ細かな制御を行うことを可能にし、ユーザーおよびロールベースのグループだけが必要なリソースにアクセスできるようにしています。 ✓ モード互換性：クライアントベースZTNA

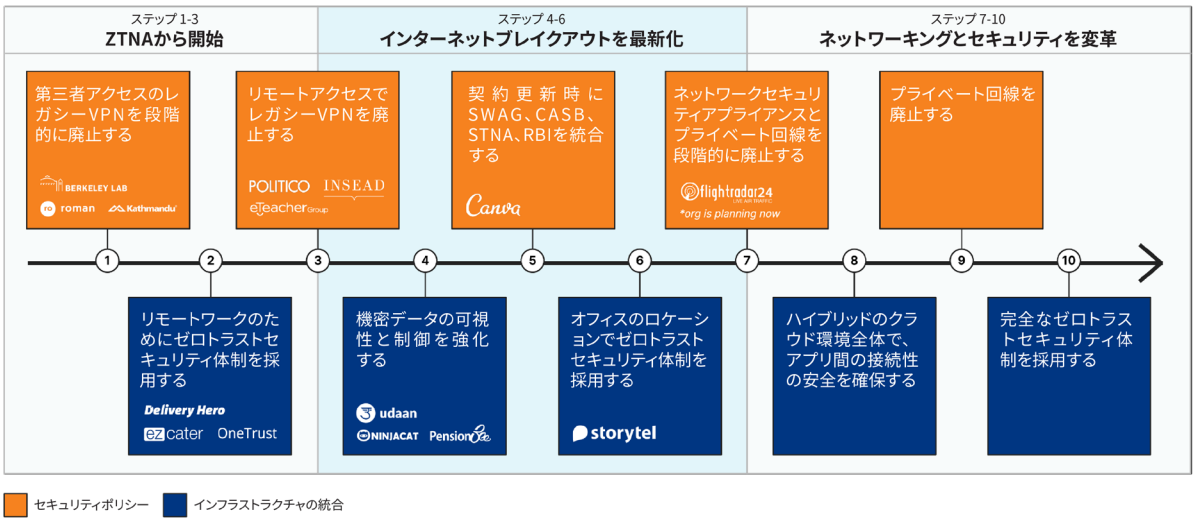
既存のVPNをゼロトラストネットワークアクセス(ZTNA)に置き換える

長く痛みを伴うVPNなしのセキュリティへの移行の渦中にいるITセキュリティリーダーにとって、Zero Trustの約束がむなしく感じられるかもしれません。しかし、プロトコルサポートや機能性のトレードオフを生むことなく、VPNをゼロトラストネットワークアクセス(ZTNA)に置き換えることは可能です。

推奨される移行の道すじはプロジェクトを推進する業務の優先順位によって異なります。

- アプリケーションへの高速な接続性が優先されるなら、**非ウェブアプリのクライアントベースZTNAを**最初にデプロイします。
- アプリケーションに対するアクセスルールのセキュリティ強化を重視する場合は、**Webアプリケーション**から始めます。

VPNの置き換えはネットワークトランスフォーメーション全体の最初のステップにすぎません。SASEモデルへの移行はあまりに圧倒的になる可能性があるため、当社の顧客がこれまでにとったアプローチに基づき、Zero Trustセキュリティへの共通する道のりを細分化しました。



VPNへの依存度を徐々に減らしながら最終的に置き換えるために、CloudflareのZero Trustプラットフォームがどのように役立つかについて詳細をご覧ください。

詳細を見る

実際のVPNとZTNAの比較と、Cloudflare Accessがアプリケーションのアクセスのセキュリティをどのように強化するかについてご覧ください。

デモを視聴する

付録

インターネットブレイクアウトを最新化

ZTNAの実装は、セキュアアクセスサービスエッジ（SASE）モデルのデプロイにおいて重要なステップです。**Cloudflare One**は、あらゆる規模のチームの企業ネットワーキングを簡素化し保護する包括的なNetwork as a Service（NaaS）ソリューションです。Cloudflare Oneを使用すると、組織は以下のことが可能になります。

- **Zero Trustアクセスの採用。**幅広いセキュリティ境界を、すべてのリソースにおけるすべてのリクエストに対する1対1の検証に置き換えます。ユーザーの場所やユーザーが誰であるかを問わず、企業アプリケーションへの接続すべてにZero Trustルールを適用します。
- **インターネットトラフィックの安全性を確保。**インターネット上の脅威の動きが急速な場合、脅威を阻止するにはより前衛的である必要があります。Cloudflare Oneは、スムーズかつ高速なユーザーエクスペリエンスを提供しながら、あらゆるサイトにZero Trustの「ブラウザの分離」を実施することにより、インターネット上の脅威からリモートの従業員を保護し、企業から貴重なデータが漏えいすることを防止するポリシーを適用します。
- **オフィスとデータセンターの保護と接続。**企業ネットワークは過度に複雑になっており、ユーザーのトラフィックが目的地に到達するまでに複数のホップを通過しなければならないケースが増えています。Cloudflare Oneでは、企業は一貫性のある統一されたクラウドプラットフォームを通じて、オフィスとデータセンターを保護することができます。

Cloudflare Oneの詳細は、10分間の紹介とデモをご覧ください。

お客様のネットワークを変える

もうすぐCloudflareの「Zero Trust」と「WAN as a Service」がひとつに統合され、従業員は働く場所にとらわれずに企業のリソースに安定してアクセスできるようになります。

現在、VPNおよびWAN製品は、従業員に社内のプライベートネットワーク内にあるリソースへのアクセスを許していますが、接続性とセキュリティのポリシーを別々に管理しなければなりません。

Cloudflareは統一されたコントロールプレーンを提供し、複数のポイントプロダクトを取り扱う必要なく、同じZero Trustセキュリティポリシーを従業員および職場全体により柔軟に適用可能にしています。

詳細は https://www.cloudflare.com/cloudflare-one/ をご覧ください。