CLOUDFLARE

ホワイトペーパー

ネットワークモダナイゼーションの戦略策定

本文

3 **レガシーネットワーク：デジタルモダナイゼーションを妨げる要因**

4 **プロセスの理解**

5 **ネットワークトラフィックの4つの主要経路**

6 **Cloudflareのコネクティビティクラウド**

7 **ネットワークモダナイゼーションの主要ユースケース**

7 ブランチ接続

8 外部公開されたインフラの保護

9 企業ネットワークの簡素化

9 DMZから移行

10 VPNからZTNAへ切り換え

10 LANへの過剰な信頼を排除

10 M&A時の接続を加速

11 クラウドの接続と安全確保

12 **次のステップ**

レガシーネットワーク：デジタルモダナイゼーションを妨げる要因

事業環境が急激に変化し得る世界で優位に立つには、俊敏性が不可欠です。しかし、俊敏性は単にリーダーシップと意思決定によって得られるものではありません。俊敏性は企業変革力にも懸かっているのです。システムは、破綻せず、柔軟に適応できるように確立しなければなりません。企業は、新たな収益モデルに合わせて再編成し、新アプリをサポートし、世界中で人々をつなげられなければならないのです。

俊敏性は、企業が競争優位の確立を目指してアップデートや改善を行うにあたり、デジタルモダナイゼーションプロジェクトの主たる期待成果としてまず掲げるものの1つです。従来型企業ネットワークの状況を見れば、俊敏性を優先成果物とするのも頷けます。企業ネットワークは、情報を伝達し、連携作業を可能にする上で極めて重要な役割を果たします。企業ネットワークはこれまで、変化に頑強に抵抗してきました。それにはもっともな理由があります。元来、システムへの衝撃に耐えられるよう設計されたものですし、変革には多額の費用と大変な手間がかかるからです。

クラウドがデータセンターにもたらす影響など、徐々に起こるため予測と対策が可能な変化もありますが、ネットワーキングは市場外部要因によって急激に変化しており、突然変化することもあります。例えば、パンデミックの発生によって、リモートワークの機能をすばやく追加し、従業員の生産性を維持し、人のいないオフィスのアイドル状態のネットワークにかかる費用を考えつつコスト管理することが、一部企業にとっていかに難しかったかを痛感させられました。

一方、そうした困難にうまく適応しただけでなく、業績を伸ばした企業もあったことが判明しました。これは、正しい事業意思決定を下す能力が経営陣にあったからだけではなく、その企業の変革力と実行力の賜物です。CIOとしては、変化に対応し、将来のニーズをサポートできるようアップデートや改善を行い、IT部門が変革を抑制するのではなく加速できるように、戦略を策定する必要があります。

オンプレミスネットワークへの多額の投資を考えると、モダナイゼーションは簡単に決断できるものではありません。ネットワークモダナイゼーションのメリットを十分に実現するには、何が変わらなければならないのかを見極めるために、達成すべき成果をしっかり考える必要があります。

プロセスの理解

過去のネットワーク設計のベストプラクティスを振り返ると、ここまで複雑になったのも納得できます。何十年にもわたり、ネットワークは新テクノロジーを重ねることによって構築・強化されてきました。新世代のネットワーク設計や新たなイノベーションが出現するたびに、ネットワークは複雑化していったのです。簡素化の機会はなく、新テクノロジーの追加によって速度、耐障害性、セキュリティの確保が一層複雑化するのが通常でした。

クラウド型のネットワークサービスやセキュリティサービスが現れ、企業ネットワーク設計は今、次の世代交代期に差し掛かっています。企業は、クラウド型サービスをネットワークの延長として活用することで、新たなユースケースへの取り組みや、データセンターを遥かに超えるカバレッジの拡張、アプリケーションの保護を実現できます。これは、ネットワークを大幅に簡素化する機会です。というのは、サービス配信システムは既存ネットワークとクラウドプロバイダーPoPとの接続を活かして構築され、接続を切って新たなアプライアンスを挿入するわけではないからです。オンプレミスネットワークとクラウドサービスの間のネットワーキングは不変で、クラウドサービス内のサービスが挿入され、利用される形です。

問題は、一口にクラウド型のネットワーキング・セキュリティプラットフォームといっても、構築のしかたはさまざまで、違いを見分けるのは必ずしも容易でないという点です。多くは、モダナイゼーションの過程におけるメリットが限定的です。違いを理解して、複雑さの元凶を別の元凶に置き換える結果とならないように、ネットワークモダナイゼーションの目標をマッピングする必要があります。

ネットワークトラフィックの4つの主要経路

ネットワークモダナイゼーションプロジェクトの範囲を評価する際は、自社ネットワークが膨大な数のタッチポイントをカバーし、その中には同一のインフラストラクチャと交差するものもあれば（例えば、インバウンド、アウトバウンド、末端間のトラフィックが自社のコアネットワークを通過）、そのインフラの外で運用されるもの（パブリッククラウドネットワーキングなど）もあることを考慮しましょう。

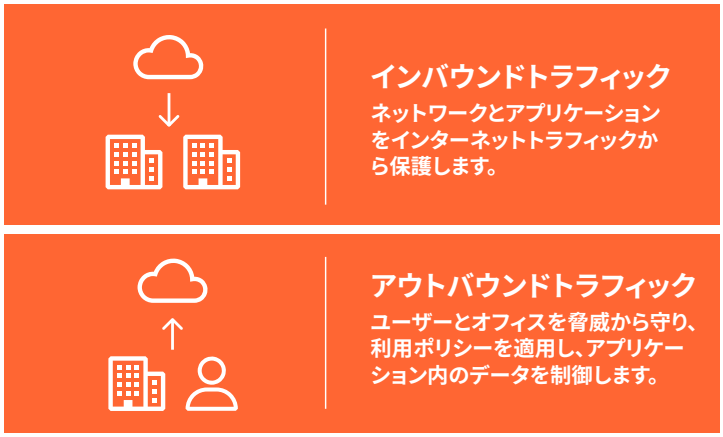
インバウンドトラフィック：ネットワークの一部がインターネットに露出するため、インバウンドの防御を維持して、ビジネスを機能不全に陥らせたり悪用したりする試みから保護しつつ、正規ユーザーからのトラフィックを許可する必要があります。従来の境界型防御では、過負荷に陥って分散型サービス妨害攻撃への対応能力が必要になる可能性があります。

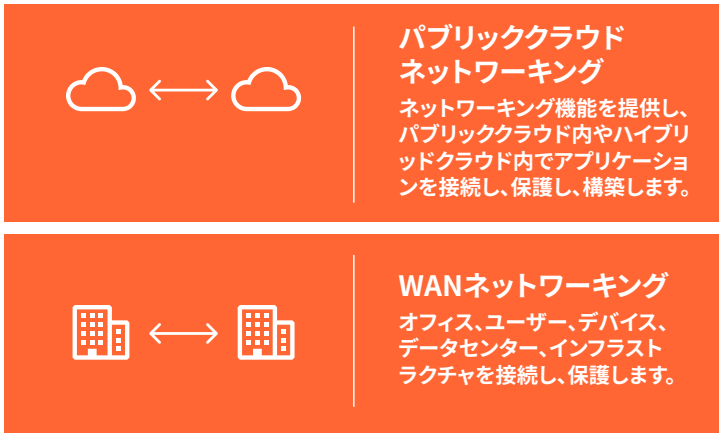
アウトバウンドトラフィック：インターネットアプリやクラウドアプリへの接続では、脅威やデータ流出からの保護など、安全なビジネスユースのための防護柵となるポリシーが必要です。ユーザーのロケーションが変化するため、企業はさまざまなアウトバウンド通信保護テクノロジーを組み合わせて実装してきました。ファイアウォールなどのオンプレミスアプライアンス（ユーザーがネットワーク上に居る場合）やDNSリゾルバー、SWGやCASBなどのクラウドプロキシ（ユーザーが遠隔地に居る場合）などです。

WANネットワーキング：WANとその対象範囲（キャンパス、支社など）は、クラウドファーストイニシアチブやIoTデバイスをサポートするために再設計が進められています。そして、従来のネットワーク構成は、データセンターへのバックホールをやめてインターネットへ直接接続するアーキテクチャへと変わりつつあります。この分野のネットワーキングが急激に進歩する一方で、セキュリティの挿入は逆に複雑化しています。多くの場合、内部トラフィックの経路はエッジに展開されたセキュリティアプライアンスに依存したままで、それが企業の変革推進を妨げています。

パブリッククラウドネットワーキング：企業が複数のクラウドにアプリケーションを構築するにつれ、ポイント間のネットワーキングとセキュリティの設定を確立して維持することが、ますます難しくなります。ネットワーキングの設定と管理は時間とリソースを食います。時間はプロジェクト開発に費やした方がいいはずです。

上記のトラフィック経路のいずれにも、企業が自社ネットワーク内に実装したテクノロジーやクラウドから利用するテクノロジーが数多く使われています。モダナイゼーションプロジェクトは複数方向のトラフィック経路に関わるため、4方向すべてについてネットワークモダナイゼーションの全過程を計画しなければなりません。アーキテクチャで失敗して十分な変革成果が出せず、複数の個別テクノロジーで未達のユースケースに取り組まざるを得ない事態を回避するために必要なことです。



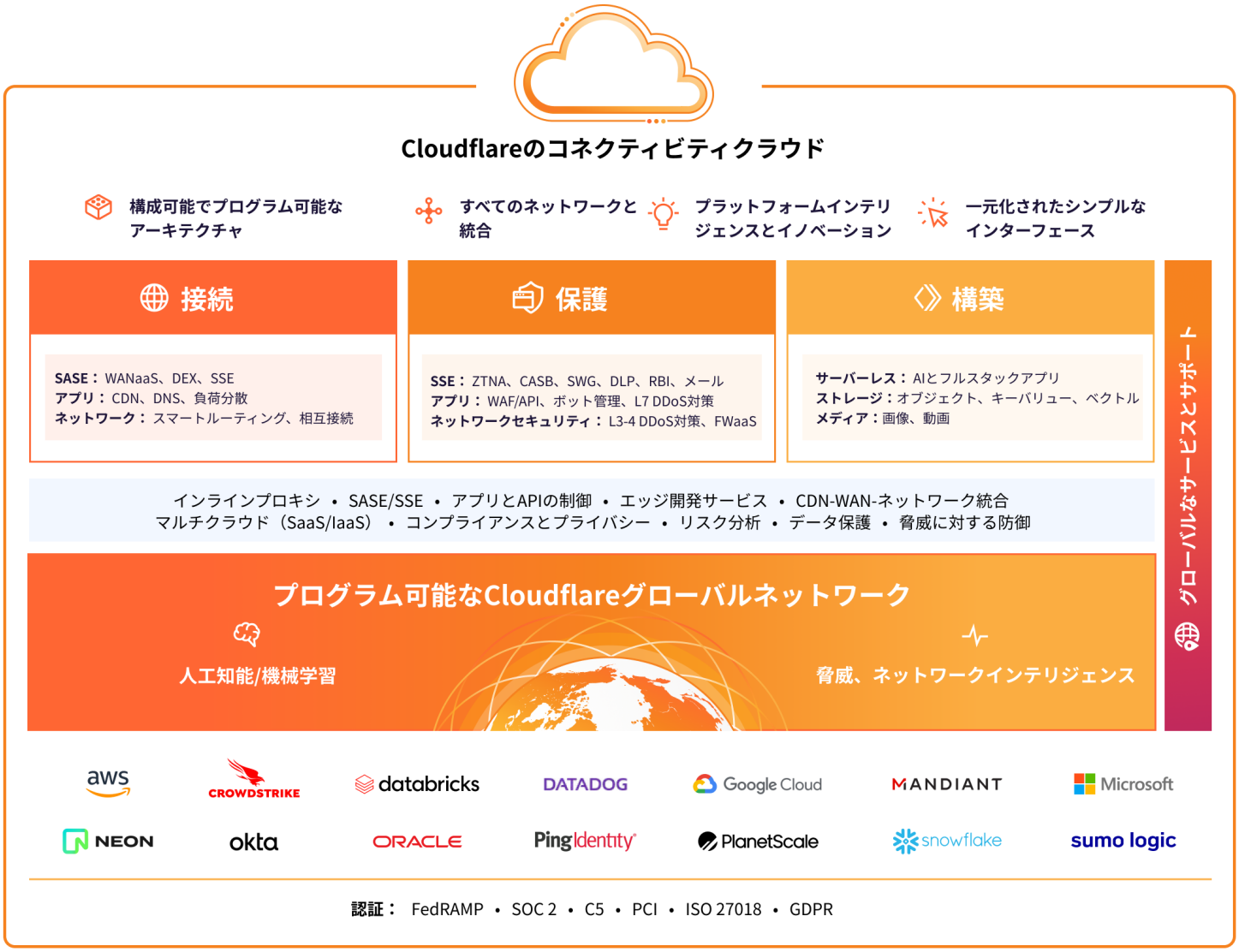


Cloudflareのコネクティビティクラウド

貴社ネットワークのモダナイゼーションに、Cloudflareコネクティビティクラウドのご利用をご検討ください。Cloudflareコネクティビティクラウドは、コンポーザブルでプログラム可能なアーキテクチャの使用を原理として構築されており、ネットワーキングとセキュリティのサービスを貴社のユーザー、クラウド型ビジネスインフラ、アプリケーションに提供します。コンポーザブルでプログラム可能なため、貴社のモダナイゼーションにおける現在および未来のニーズに対応できます。

Cloudflareを使えば、アプライアンスを挿入しなくてもサービスを有効化するだけで機能を追加し、新たなユースケースをサポートできます。Cloudflare Anycastデータセンターへの接続はそのままで、統一の管理インターフェイスでサービスの設定と展開を行い、トラフィックを処理することができます。現在のニーズを満たしつつ、将来のユースケースとネットワークモダナイゼーションの全過程をサポートするプラットフォームを整備できるのです。

グローバルなインフラストラクチャを増築する代わりに、当社のインフラをご利用ください。Cloudflareグローバルネットワークを経由することで、超高速配信のメリットをご享受いただけます。ほぼすべてのサービスプロバイダーとクラウドプロバイダーに直接接続するCloudflareネットワークを利用すれば、世界のインターネット人口の95%へ約50ミリ秒圏以内に到達可能です。



ネットワークモダナイゼーションの主要ユースケース

まず、ビジネスへのインパクトが大きく、貴社にとって最も有意義な便益をもたらすユースケースから始めましょう。企業にはそれぞれビジネスに応じた優先順位がありますので、以下のユースケースは順不同です。どういった道筋を選ぼうとも、大事なのは、短期的ニーズを満たしつつ、ネットワークモダナイゼーションをサポートするようなアーキテクチャを基盤として構築することです。

	モダナイゼーションプロジェクト
ブランチ接続 コストを削減、ユーザーエクスペリエンスを向上	• MPLSからコネクティビティクラウドへ移行 • SD-WANからコネクティビティクラウドへ移行
外部公開されたインフラの保護 投資したファイアウォールとDMZの耐用年数を延長	• ネットワークファイアウォールへの負荷を軽減 • DMZセキュリティをコネクティビティクラウドへ移行
企業ネットワークの簡素化 ゼロトラスト実装によりセキュリティを強化、資本的支出を削減	• DMZを縮小または撤廃 • VPNからZTNAへ切り換え • LANへの過剰な信頼を排除 • M&A時の接続を加速
クラウドの接続と安全確保 アプリに各クラウドの強みを利用	• アプリを構築し、保護 • 開発者サービスを利用してコア機能を集約

ブランチ接続

WANネットワーキングの主要素の1つは、支社オフィスや店舗などの小規模サイトの接続で、ユーザーとデバイスをアプリケーションへどう繋ぐかが重要になります。従来の「ハブアンドスポーク」アーキテクチャでは、高価なMPLS回路を使ってサイトをデータセンターにつないでいましたが、クラウドアプリをサポートするニーズが高まり、ブロードバンドでインターネットへ直接接続するアーキテクチャを使う企業が増えています。

SD-WANはネットワーク接続の信頼性を高める狙いでしたが、セキュリティの挿入に関しては完璧とはいえません。たいていのSD-WANアーキテクチャは、重いエッジアプライアンスとローカルファイアウォールでSD-WANファブリックにセキュリティポリシーを適用し、SSE/SASE統合はアウトバウンドトラフィックにしか使いません。

ブランチ接続にCloudflareのコネクティビティクラウドを使って、レガシーサービスの補強か代替かにかかわらず、移行の全過程をサポートしましょう。Cloudflareでは、「エッジを軽くクラウドを重く」の原理に基づくアーキテクチャを使い、ネットワーキングとセキュリティのサービスを提供しています。Cloudflare Magic WANで、ネットワークロケーション（支社オフィス、小売店舗、工場など）をつなぐサイト間接続を促進しましょう。Magic WANは、企業ネットワーク全体に安全で高性能な接続とルーティングを提供し、コストを抑え、運用に伴う複雑さを軽減します。セキュリティに関しては、Cloudflare Magic FirewallをMagic WANと共にシームレスにデプロイでき、基幹・末端（North-South）、末端間（East-West）を問わず、Cloudflareのネットワークを経由するトラフィックにネットワーク制御ポリシーを適用することができます。

外部公開されたインフラの保護

企業ネットワークとDMZはアドレス指定可能でインターネットに露出しており、攻撃者が害を及ぼさないようにする対策が必要です。完璧な世界なら、従来のネットワークファイアウォールで検査し、迷惑トラフィックをことごとく排除できるでしょうが、どのファイアウォールにも能力の限界（使用できる帯域幅、CPU使用率、セッションカウントなど）があります。攻撃者が成功するかどうかは、単に規模の問題です。つまり、企業がネットワークプロトコルの各階層を運用する能力を圧倒するほどのノイズを生成できれば、攻撃者の勝ちです。

それは、単にトラフィックの量だけではありません。インバウンドトラフィックを受け入れることは、未認証や事前認証済みのトラフィックに対し攻撃対象領域を開くことです。アプリケーションやオペレーティングシステムに欠陥があれば、システム上にアカウントを持たない攻撃者でも悪用できます。別の漏洩から得た既知のユーザーネームとパスワードをログインに使うクレデンシャルスタッフィングも、大きなリスクです。DMZでゼロトラスト原則をアプリケーションに適用することにより、インターネットへの露出を減らし、あわよくば露出を排除することができます。

企業は、深層防御の原則を適用し、外部公開インフラの上流で悪性トラフィックを吸収することにより、ネットワークの保護を強化できます。Magic Firewall内蔵のCloudflare Magic Transitは、CloudflareのAnycastネットワーク経由でデプロイされ、企業の玄関口として、悪性トラフィックや不要トラフィックをフィルターで排除し、クリーンなインバウンドトラフィックのみを配信します。

ネットワークファイアウォールがアプライアンスでDDoS軽減を行うとしても、接続処理はやはり行い、それから排除する形になります。Cloudflareを使えば、当社のネットワークがお客様のプレフィックスをブロードキャストし、本来境界ファイアウォールへ向かうであろうトラフィックを誘導します。Anycast技術で当社の全データセンターに負荷を分散することによって、効果的にDDoS攻撃を吸収しています。ボットネットを構成するデバイスが最寄りのAnycast PoPを見つけ、そのPoPがMagic TransitとMagic Firewallのポリシーに従ってトラフィックを処理します。

企業ネットワークの簡素化

簡素化は、モダナイゼーションの数多くの便益実現に寄与します。ITチームは、故障するコンポーネントが少ない設計のネットワークであれば、それだけ信頼性を高められますし、アクセス権限に関してゼロトラストですべて拒否のアプローチをとることによって安全性を高められます。

ネットワーク簡素化のため、以下の手段をご検討ください。

DMZから移行

ネットワークのDMZはゼロデー攻撃に対して特に脆弱で、運用が難しい領域です。攻撃者は内部ネットワークにアクセスしなくてもDMZ内のサーバーと交信できるため、企業は攻撃や不正利用を防止するために絶えず警戒しておかなければなりません。

ただ、DMZは確かにこれまで重要な役割を果たしてきましたが、今でも必要でしょうか？ネットワーク構成要素としてのDMZの重要性は低下しています。アプリケーションの構築やホスティングは他の方法でも可能だからです。

- 一般公開用のアプリの場合は、ワークロードをパブリッククラウドに移すことで経済的、技術的便益が得られます。
- SaaSを使えば、一般公開アプリや非公開アプリの多くは、お客様が管理するインフラで稼働する必要はまったくありません。

以上を踏まえ、セキュリティとネットワーク設計の観点から、DMZの必要性を減らす、もしくはなくす方法を考えることから始めるのが実利的でしょう。運用上合理的なだけでなく、DMZをサポートするネットワークインフラ（ファイアウォール、WAF、ロードバランサーなど）をなくせば、アーキテクチャが大幅に簡素化されます。

DMZ内に置かれた非公開アプリへのアクセスを、従業員、パートナー、請負業者に拡張する場合はどうでしょうか？それらのアプリをプライベートネットワーク内に隔離して、従業員やパートナーにはゼロトラストネットワークアクセス（ZTNA）でアクセスを拡張する方が安全でしょう。

ZTNAなら、アプリケーションへのインバウンドネットワークトラフィックを排除することによって、攻撃対象領域を効果的に縮小することができます。ZTNAでは、リソースへのアクセスをコンテキストに応じてCloudflareのコネクティビティクラウド経由で中継するため、ネットワークファイアウォールのポートを開く必要がなく、誰が何のリソースにアクセスできるのかをセキュリティチームが完全に把握できます。

VPNからZTNAへ切り換え

アプリケーションへのアクセスにVPNを使うことは、やがてなくなるでしょう。ユーザーがインターネットやクラウドにアクセスするのに長い長いトンネルを経なければならないというのは、ネットワーク設計の観点からみて非実用的です。ユーザー（と侵害された可能性のあるエンドポイント）をVPNでネットワークに乗せるのは、重大なセキュリティリスクでもあります。

VPNの機能はアプリケーションアクセスだけではありません。企業が、エンドポイント管理やサーバー主導通信など、エンドポイントとの幅広いネットワーク接続を必要とするシナリオもあります。そういったユースケースでは従来、VPNのネットワーク接続が双方向に使われており、早期に上市されたZTNA製品が伸び悩む要因となりました。選択肢のなかった企業は、ZTNAをVPNと併用したのです。

ネットワークインフラをモダナイズ（最新化）する企業は、CloudflareのZTNAでそれらの機能を統合できます。Cloudflareなら、典型的なZTNAのユースケースと、サーバー主導や双方向のトラフィックの両方をサポートできるからです。それらの機能は、VPNの必要なくアプリケーションにアクセスできるようにし、セキュリティ強化とさらなる簡素化を進めるのに役立ちます。

LANへの過剰な信頼を排除

ハイブリッドワークの導入で、オフィスでも他の場所でも働き方に大差はなくなってきています。実際に、ユーザーは頻繁にコーヒーショップやシェアオフィスの信頼できないパブリックネットワークを利用し、オフィスで働くのと同じように仕事しています。

オープンなパブリックネットワークはある意味、ゼロトラストを具象化したものと言えます。誰も特権的アクセスをもたず、誰も、何物も信頼できないのですから。シェアオフィス、ホームオフィス、コーヒーショップでゼロトラスト原則を実行できるなら、企業ネットワークからも信頼を排除できないでしょうか？

信頼の排除に必要なのは、ネットワーク設計の進歩ではなく簡素化です。認証済みユーザーのための昇格アクセス権を設け、リソースへの接続を開始する際にネットワークポリシーを適用するよりも、ネットワーク全体が信頼できないという前提に立つ方が遥かに安全でしょう。企業は、SASEでセキュリティを記述することで必要なアプリケーションにアクセスできますし、ネットワークそのものの信頼性を仮定せずとも、適切なセキュリティ対策でアクセスの安全を確保することができます。ゼロトラストはネットワークに信頼を付加するものではありません。むしろ、過去のように明示的で過剰な許可を与えるのではなく、より良く、より安全な状態に達するまでの間、信頼を除去することです。

M&A時の接続を加速

企業は、他の手段ではすぐに手に入れられないビジネスリソースや能力を取得するツールとしてM&Aを利用します。その機会を活かすためには、すばやく実行して、M&A後の会社が両社を足した合計より良いものとなるようにしなければなりません。しかし、2社のアプリケーションやその基盤を成すインフラストラクチャがすんなり噛み合うことは稀なため、IT部門はなかなか前に進めないのが通常です。

M&A時の接続を加速するには、アプリケーションへのアクセスはネットワーク統合とは別個のタスクと考えるのがよいでしょう。コンバージドネットワークアーキテクチャの設計は何年もかかる可能性がありますが、アプリケーションアクセスがそんな遠いマイルストーンに依存する必要はないのです。

というのは、信頼できるユーザーが使っているのが信頼できないネットワークであっても、アプリケーションへのアクセスが必要なことに変わりはないという初日の状況は、実質的にゼロトラストのユースケースだからです。Cloudflare Oneを使ってアクセスを拡張すれば、コンバージドネットワークへのアクセスを待たずともM&Aのための接続が可能になります。

クラウドの接続と安全確保

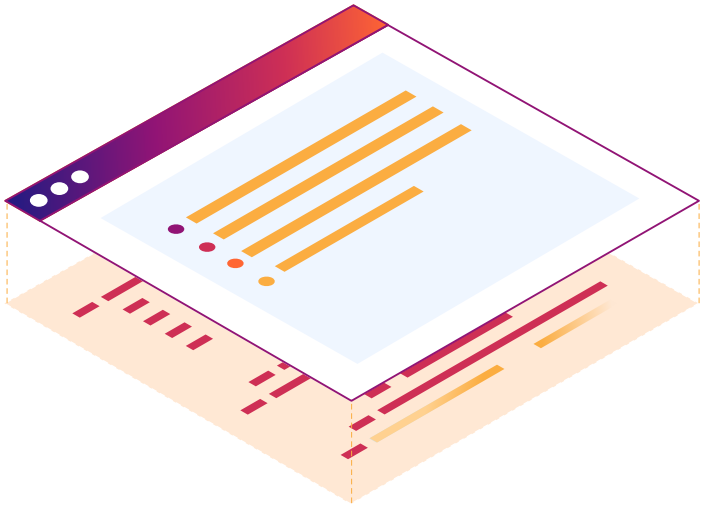
クラウド開発は進化しており、1つのクラウドのコンポーネントを別のクラウドで再利用できると有益でしょう。すべての企業がやがてはマルチクラウドになり、パブリッククラウドネットワーキングの管理も必要になってくるでしょう。アプリ開発はその性質上、縄張り意識の強い分野で、各部門のDevOpsは使い慣れたツールを好みます。全クラウドの接続を管理する組織的能力の開発は、全く異なる枠組みで構築された複数のツールセットに関わるため、複雑な作業になります。

さらに、マルチクラウドの複雑さのもう1つの側面として、ハイブリッドクラウドという領域があります。ハイブリッドクラウドは、オンプレミスのプライベートクラウドと仮想プライベートクラウドを組み合わせたものです。ネットワークは、AWS Direct Connectのような専用ネットワーク接続で構築されることもあり、その場合は高コストで、単一クラウド限定になる可能性があります。企業がマルチクラウドアプリケーションを構築するとしても、各クラウドへの専用ネットワーク接続の費用が発生する状況を望むとは限りません。

ネットワーキングとセキュリティをアプリからアプリへ直接構築するのではなく、Cloudflareをパブリッククラウドネットワーキングサービスの調整と接続にご利用ください。Cloudflareのコネクティビティクラウドは、広範なCloudflareネットワーク経由でクラウド間を移動するトラフィックのトランジットに最適で、そういったアーキテクチャで理想的な役割を果たすと、当社では考えています。お客様はパブリッククラウドネットワーキングを管理する能力を得、ワークロード接続の設定もCloudflareで調整できるようになります。

当社のパブリッククラウドネットワーキングは、配線調整だけではありません。当社のアーキテクチャは一歩進んで開発者サービスも提供しており、マルチクラウドアプリケーションの構築や統合にご利用いただけます。この開発者プラットフォームは、オープンソースとオープンスタンダードで構築された基盤技術の豊かなエコシステムを提供します。開発者プラットフォームは、全要素をお使いいただくことも選んでお使いいただくこともでき、クラウドによって特定サービスに利用が限定されることはありません。

次のステップ



ネットワークモダナイゼーションの次の段階へ進まれる際は、Cloudflareへお知らせいただければ、戦略策定を支援させていただきます。当社は、数千のお客様と緊密に連携をとりながら、各社アーキテクチャからCloudflareコネクティビティクラウドへの移行をお手伝いしてきました。

詳細については、次のページをご覧ください。
http://www.cloudflare.com/ja-jp/

© 2024 Cloudflare Inc.All rights reserved.
Cloudflareロゴは、Cloudflareの商標です。その他、
記載されている企業名、製品名は、各社の商標また
は登録商標である場合があります。

enterprise@cloudflare.com | cloudflare.com/ja-jp

REV:BDES-5483.2024JAN30