CLOUDFLARE

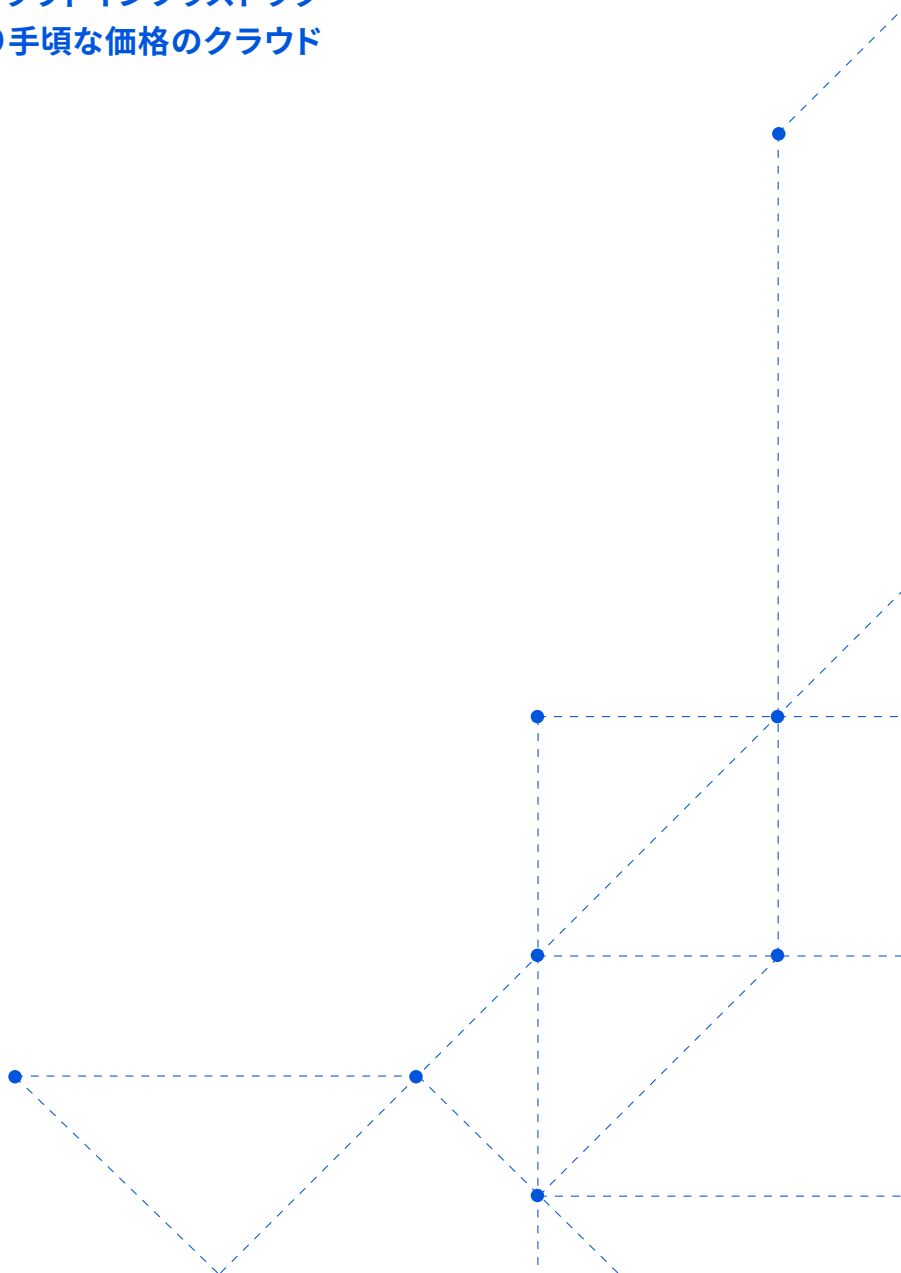
ホワイトペーパー

ネットワークアプライアンス機器の終焉

なぜ今がネットワークハードウェアから移設の時なのか

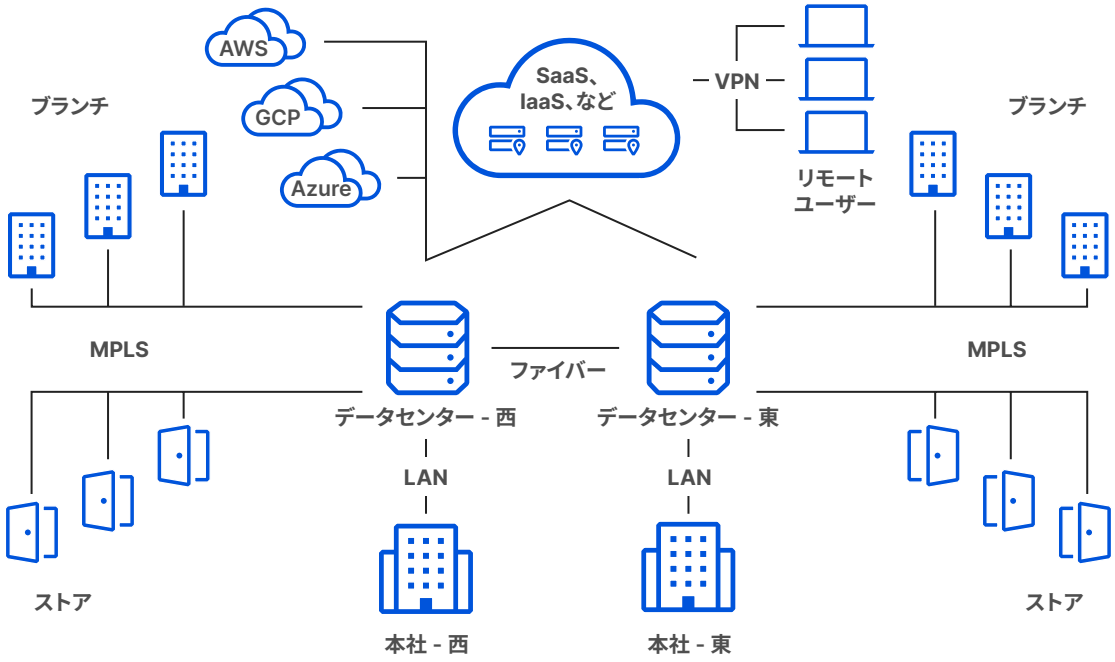
概要

ストレージおよびコンピューティングのクラウドへの移行中は、多くのネットワーク機能がオンプレミスで維持されるため、容量の制限、総所有コストの増加、サポートの課題、セキュリティに対するギャップが生じます。企業は、ハイブリッド型の勤務スタイルがニューノーマルになるにつれ、適正能力と効果的なセキュリティの確保に苦労しています。多くのトランスフォーメーションプロジェクトは、1年以上実行しているハードウェアバックログのためにこう着状態に陥りました。このホワイトペーパーでは、こうした課題を概説し、その結果を定量化し、ハイブリッドクラウドインフラストラクチャの速度とセキュリティを向上させ、より手頃な価格のクラウドベースのソリューションを提案します。



はじめに

クラウドへの移行は、インフラストラクチャのコストを削減し、データとアプリケーションの可用性を向上させ、スピーディな運用を高めるための効果的な戦略であることが実証されています。しかし、クラウドへの移行が一気に行われることはほとんどありません。多くの大企業で、マルチクラウドとオンプレミスのインフラストラクチャが複雑に混在しています。



このようなハイブリッドのインフラストラクチャは必ずしも悪ではありませんが、複雑さが増すことは否めません。具体的には、DDoS軽減、負荷分散、ファイアウォール、VPN など、さまざまなネットワーク機能がオンプレミスで維持されることになります。

従来のネットワークのハードウェア設備は、クラウド中心の世界で重要となる、インフラストラクチャのセキュリティ保護と加速化を担う水準には達していません。これらの設備の扱いにはいつも手を煩わされてきました。高価で、手に負えないほど多くの機材に、ケーブルが蜘蛛の巣のように絡み合っているのです。この中にクラウドを追加すると、セキュリティギャップ、パフォーマンスの低下、サポートの課題が即座に生じます。

このホワイトペーパーでは、クラウドに移行する世界でネットワークハードウェアを維持するリスクと落とし穴について概説し、よりセキュアで効果的なネットワークを構築するための戦略を提示します。

クラウド環境における ハードウェアのリスク

ネットワークハードウェア設備は、各機能が多岐に渡り、使用方法も企業ごとに若干異なります。

一般的な例：

セキュリティ

- DDoS攻撃対策
- ファイアウォール
- 仮想プライベートネットワーク
- 設定可能なポリシー

パフォーマンスと信頼性

- 負荷分散
- トラフィックの高速化/WAN最適化
- パケットフィルタリング
- トラフィック分析

このハードウェアをオンプレミスにデプロイすると、アーキテクチャには次の5つのリスクが生じます。**サプライチェーンの混乱、容量制限、高い総所有コスト、サポートの課題、セキュリティギャップです。**

最初の3つのカテゴリーは、最も洗練されたネットワークおよびセキュリティチームに対してでさえ常にある程度の課題を提起しています。他の2つは、クラウドへの移行によってさらに悪化しています。

サプライチェーンの混乱

すべての物理的製品のように、ネットワークハードウェアは様々なサプライチェーンの問題に対する脆弱性があります。材料のコストが上昇すると、特定の材料とコンポーネントの取得が難しくなるか、出荷プロバイダーが過負荷となり、ネットワークハードウェアの購入や交換が難しくなります。

残念ながら、このような問題は最近一般的になってきました。主な原因は新型コロナウイルス感染症パンデミックによる影響です。Gartnerのリサーチによれば、「パンデミック以前、一般的なリードタイムは4-6週でした。今では、200–300日が一般的となり、顧客に対する連絡の中で430日以上に言及している例もありました。」

これらの遅延には複数の要因があります。

- **ロジスティクスの問題:** 以前のサプライチェーンモデルには複数の障害点があります。最小の従業員で、セキュアかどうか定かではないテクノロジーに過度に依存し、最近の在宅勤務による課題があります。パンデミック中は、多くの工場が閉鎖され、運送企業は遅延を経験し、多くの種類のサプライチェーンの従業員の雇用と労働がより困難になりました。これらすべての課題のために、ハードウェアの製造や配送により長い時間がかかるようになりました。おそらくロジスティクスすべてにおける最大の難問は、それがリレー競争に似ていて、あなたの各組織が問題を経験していないとしても、あなたがチェーンを拡大するときにリンク切れの影響を受ける場合があるということです。
- **材料コストの上昇:** ネットワークハードウェアアプライアンスは多様な原材料に依存しています。需要が高いうえ供給が制限されているため材料コストは急騰しています。これは企業が自分のネットワークで必要なものを得るために長い時間待つ必要があるというだけでなく、支払い額の増大が顕著であることを意味します。残念ながら、これらの課題のため、Gartnerはハードウェアアプライアンスのリードタイムが2023年中高いままであると予測しています(出展)。

これらの課題すべてのために以下の結果が生じます。ハードウェアボックスを調達、保守、交換し続けると、間接費は増加し、実行時間よりも計画のための時間が増え、不確実な時代に物理的サプライチェーンのセキュリティを確保するためにセキュリティ上の懸念が増大します。ハードウェアボックスのロジスティクス、リードタイム、調達、格納に焦点を当てるより、組織は顧客のニーズを満たすことに焦点を当てることができるはずです。

容量制限

ネットワークハードウェア設備は、その性質上、予期せぬトラフィックの急増時に、そのトラフィックが正当であるかどうかにかかわらず、過負荷になってしまうことがよくあります。しかし、最近の傾向では、これらの限界点に到達することがより一般的な懸念になってきています。

分散サービス妨害(DDoS)軽減について考えてみましょう。史上最大規模のDDoS攻撃は、Microsoftによれば2021年11月に発生し、最大3.47 Tbpsに達したと言われています(出展)。DDoS攻撃は、市場で最も高度なDDoS軽減ハードウェアボックス(通常、このような攻撃を軽減するのに必要な容量の一部を提供する)に何度も過度の負荷をかけたことでしょう。

2021年11月、史上最大のDDoS攻撃は最大3.47 Tbpsに達したと言われています。

すべての組織がこの規模の攻撃を引き付けるわけではありませんが、すべての組織が最も高度なDDoS軽減ハードウェアを実装可能または実装するわけでもありません。Cloudflareの報告によれば、帯域幅消費型攻撃は2022年の第1四半期に増加しました。実際、10 Mpps(百万パケット/秒)を超える攻撃は前四半期比300%以上増、100 Gbpsを超える攻撃は前四半期比645%増となりました(出展)。DDoS攻撃の警報が急に増加しているだけでなく、これらの種類の攻撃により高容量であると称する多くのハードウェアベース軽減ソリューションが過負荷状態になる可能性があります。

さらに、攻撃の規模には、データセンターに同時に到達する可能性のある正当なトラフィックは含まれません。トラフィックの多い期間、たとえば買い物が盛んに行われ、eコマースの1日のページビューが一夜にして平均2倍になる(出展)ブラックフライデーの週末に小規模な攻撃が届く場合、結果として生じるトラフィックの急増は、セキュリティハードウェアの限界点を超えるのに十分でしょう。

DDoS軽減は、オンプレミスハードウェアの容量制限の一例にすぎません。

その他の例には次のようなものがあります：

ロードバランサー: 個々のオンプレミスのロードバランサーは、正当なトラフィックが突然増加すれば、簡単に過負荷になります。この場合、追加のハードウェアのプロビジョニングとインストールに時間がかかることがあります。代替案は、最悪の事態に備えて十分な容量を維持しておくことです。しかし、この方法では、企業が大量のハードウェアを高いコストで継続的に運用する必要があります。

仮想プライベートネットワーク(VPN): VPNの使用状況を事前に予測することははるかに難しくなっています。多くの企業にとって、完全なリモート業務およびハイブリッド型業務はニューノーマルですが、多くのVPNは企業全体での連続使用を考慮されていないため、従来のVPNアプローチでは注意深い計画、保守管理が必要です。VPNを使用する従業員が多すぎる場合、接続や信頼性が損なわれます。さらに、VPNは性格上Zero Trust制御を考慮していないため、セキュリティの問題が浮上する可能性があります。その上、VPNが過負荷状態になると、企業は「スプリットトンネル」トラフィックとなりWebバウンドトラフィックはは VPNを通過せず、従業員のwebアクティビティを追跡および管理することが困難になります。

これらの問題に対する選択肢の1つは、新しい、大容量のハードウェアを購入することです。しかし、この方法は多くの別の問題を引き起こします。

所有コスト

容量の制限があるため、データセンターのハードウェアが高価であることは、特段驚くべきことではありません。たとえば、約100 GbpsのDDoS軽減容量を達成するために必要なハードウェアは、先行投資として40万～50万米ドルの費用を要します。

さらに、これらのコストは、ハードウェア設備の総所有コストの一部にすぎません。

次の費用を考慮してみてください：

- チームコスト: ハードウェアを購入、運用、保守してOSI参照モデルのあらゆるレイヤーを脅威から防御し、細心のWebサイトやインターネットアプリケーションで期待されるレベルのパフォーマンスと信頼性を提供するためには、これらのネットワーク機能の専門家から構成されるチームが必要です。これらの広範な専門知識を有するチームを構築するには、特にかつてないほど市場の労働力が逼迫している間は、とても高額な費用が掛かります。2022年のISACAの調査では、年次調査に参加した2000人のサイバーセキュリティ専門家のうち、63%がサイバーセキュリティの役職についておらず、これは前年より8%増加しています(出展)。
- メンテナンスコスト: ネットワークハードウェアの平均的なオンプレミスの有効期限は3～5年ですが、それらの全体期間の保障には追加の支出が必要です。技術革新の速度を考慮すると、これらのオンプレミスボックスの寿命を短くせざるを得ません。他の選択肢としては、製造元または第三者による計画外の予算計上されていない修理があります。また、ハードウェアの誤動作によりデータセンターのダウンタイムが発生する可能性があり、そうした事態のコスト平均は1分あたり8,800ドル以上です(出展)。
- 交換コスト: 3年ごとにハードウェア設備を交換するために、企業は初期投資の返済だけでなく、新しいハードウェアの配送料と設置に経費を費やす必要があります。多くの場合、これらの交換を遅らせると、誤動作が頻発し、追加の保守費用が増えます。

このモデルを、クラウドで配信されるネットワーキングサービスと比較してみましょう。小回りがきくチームで運用可能で、保守と輸送にかかるコストも不要です。企業が、経費のかかるアップグレードと誤動作の増加のどちらかを選ぶように迫られることもありません。

ハードウェアの誤動作により、データセンターのダウンタイムが発生する可能性があり、そうした事態の平均コストは1分あたり8,800ドル以上です。

課題のサポート

ネットワークハードウェア設備のサポートは、高コストというだけでなく、物流上の課題も抱えています。ハードウェアは、最新の脆弱性と攻撃戦略に対応するために、頻繁にパッチを適用する必要があります。このプロセスは、手動での実装に依存することが多く、人為的ミスの影響を受けやすいプロセスです。

企業が使用するハードウェア設備が多いほど、不注意、または重要なシステムに与える影響などの懸念により、パッチが最終的に無視される可能性が高くなります。最近の連合サイバーセキュリティ勧告で、アメリカ国家安全保障局(NSA)、米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)、連邦捜査局(FBI)は、パッチ未適用のネットワークデバイスにおける16の広く知られた欠陥が広範囲のキャンペーンで悪用されました(出展)。その悪用は小規模な商用ルーターから企業VPNに至る様々なオンプレミスデバイスに影響を与え、ネットワークトラフィックを操作してターゲットネットワークのデータをこっそり引き出す潜在的能力を攻撃者に与えます。

リストされた16の欠陥の大半が重度であると評価されても、パッチの適用と是正は単純なタスクではありません。実際、ハードウェアにパッチを適用させることは、非常に複雑であるため、企業が最新の状態を維持するのをサポートするためにさまざまな種類のソフトウェアが存在するといっても過言ではありません(出展)。

たった1つのパッチの見逃しが重大な結果につながることがあります。ハードウェアの脆弱性が続くだけでなく、パッチが一度リリースされれば、それに対応する脆弱性が、日和見主義の攻撃者にとって標的となる可能性がさらに高まるためです。この状況を、クラウドベースのセキュリティサービスと比較してください。クラウドベースのセキュリティサービスでは、脆弱性の修正とアップデートのインストールがデフォルトで自動的に行われ、クラウドプロバイダーのネットワーク速度によっては伝達にわずか30秒しかかかりません。

ハードウェアの管理に関するその他の課題は次の通りです。

- **トラブルシューティング:** ハードウェアのみの場合、トラブルシューティングでは多くの場合ITチームがロードバランサー、ファイアウォール、その他のオンプレミスアプライアンスを1つずつ取り外して、問題の発生個所を突き止める困難なプロセスを辿る必要があります。

  このプロセスは、クラウドサービスの同時使用によってさらに複雑になります。ハードウェアに依存する企業は多くの場合、一元化されたデータセンターとその個々の機器すべてを介してこれらのサービスへのアクセスを管理します。従業員が特定のサービスにアクセスできない場合、ITチームは問題を診断するために別の場所を確認します。Productivの最近のレポートによれば、それらの56%のSaaSアプリケーションが、シャドーIT、またはITの知識を持たずに取得された未承認または非管理対象アプリケーションに該当しており、この問題は規模と範囲の両方で急速に増加しています(出展)。
- **物理的なメンテナンス:** ハードウェア機器が故障した場合、ITチームはそれを物理的に取り外し、交換品を注文し、交換したものをテストし、再設置する根気のいる作業を行う必要があります。多くのグローバル企業の規模を考慮すると、注意を払う必要があるアプリケーションは世界の半分に及ぶ可能性があります。

セキュリティギャップ

企業が、最新かつ最大容量のオンプレミスハードウェアを継続的にプロビジョニングおよび保守するために必要なリソースを持っていたとしても、結果として生じるインフラストラクチャは依然として重大なセキュリティ上の欠陥に苦しむでしょう。特に、クラウドへの移行が進む世界では、この問題は顕著です。

従業員のアクセス管理について考えてみましょう。VPNハードウェアは、リモートで働く従業員のデバイスと内部データセンターでホストされているアプリケーションとの間に暗号化されたトンネルを確立できますが、このトンネルを確立した後のユーザアクティビティを監視およびセキュリティで保護することはできません。

従業員のデバイスがマルウェアにより安全性が損なわれる（た）場合、またはフィッシング攻撃によりVPN資格情報の安全性が損なわれる（た）場合、攻撃者はそのVPNアクセスを使用してさまざまな機密情報にアクセスできる可能性があります。フィッシングとマルウェアの両方が深刻なリスクを呈しており、攻撃者は顕著な金銭利益を獲得しています。FBIによれば、2021年にサイバー犯罪により69億ドルが損失しました。特に、ビジネスメール詐欺(BEC)により業務上の損失は24億ドルとなりました(出展)。

従業員のデバイスがマルウェアによって侵害された場合、またはフィッシング攻撃によってそのVPN資格情報が侵害された場合、攻撃者はそのVPNアクセスを使用してさまざまな機密情報にアクセスする可能性があります。

クラウドサービスおよびSaaSアプリケーションは、ハードウェア中心インフラストラクチャのセキュリティをさらに複雑にします。たとえば、ハイブリッドクラウドモデルでは、企業はオンプレミスとクラウドインフラストラクチャが混在した状態で使用しています。企業はセキュリティハードウェアをクラウドプロバイダーに単純に送信することはできません。自身のデータセンターのためにオンプレミスハードウェアを使用し続けることを願う場合、そのインフラストラクチャの各部によって保護する方法が異なるため、セキュリティチームにとっては、攻撃に対する可視性と管理能力が低下してしまいます。

クラウドベースのサービスは、データセンターとクラウドサービスを単一のソフトウェア定義のレイヤーに統合することで、これらの両方の課題を克服できます。

このアプローチの詳細な説明は、このホワイトペーパーでは割愛します。詳細については、次の記事を参照してください。

- Zero Trustネットワークとは?
- セキュアアクセスサービスエッジとは?

クラウドベースのセキュリティとパフォーマンスサービスの利点と課題

クラウドを介してネットワークサービスを提供することで、ハードウェアに関連する多くの問題（サプライチェーンの混乱、容量の制限、コスト、サポートの課題、セキュリティのギャップなど）を回避できます。

- **サプライチェーン:** 多くのクラウドベースのネットワークプロバイダーは、モダンなグローバルアーキテクチャに合わせてスケーリングし、サプライチェーンの問題の深刻性が低下するように設計されています。
- **容量:** クラウドの分散性とソフトウェア定義の性質により、企業はビジネス規模に応じて簡単に追加容量をプロビジョニングできます。
- **コスト:** ハードウェアの追加費用は存在しないか、もしくは事前に簡単に計画できるようになっています。さらに、クラウドサービスは、通常、設備投資ではなく、運営費に分類され、多くの企業にとって税制および会計上のメリットになります。
- **サポート:** 物流およびリソースのニーズは、サービスプロバイダーによって処理されます。さらに、更新が自動的に行われるため、パッチを見逃してしまうこともありません。
- **セキュリティ:** ソフトウェア定義のネットワーキングサービスでは、1つの保護レイヤーでさまざまなインフラストラクチャを統合できます。

ただし、クラウドネットワークサービスは、慎重にデプロイしなければ独自のリスクが発生することがあります。

リスク	説明
遅延	一部のクラウドベースのネットワーク機能は、DDoS軽減のためのスクラビングセンターなどの、特殊なクラウドベースのデータセンターに依存しています。これらのデータセンターへのトラフィックをバックホールすると、送信先サーバーが指す場所に応じて、かなりのレイテンシーが追加される場合があります。 この問題は、企業がネットワーク機能ごとに異なるプロバイダーを使用している場合にさらに複雑になります。トラフィックがプロバイダーからプロバイダーにホップする必要がある場合、遅延は数百ミリ秒単位になります。
サポート	企業が異なる機能に対して異なるプロバイダーを使用する場合、トラブルシューティングは依然として問題になります。どのプロバイダーが輻輳や停止の原因であるかを判別するのが難しくなるためです。
コスト	企業がさまざまな機能に対してそれぞれ別のプロバイダーを使用する場合、管理に必要な時間（とそれに伴う費用）は依然として高くなる可能性があります。

これらの問題を回避するために、次の戦略をご検討ください。

- **クラウドとオンプレミスの両方のインフラストラクチャで動作するプロバイダーを探す。**
  この機能により、ITチームとセキュリティチームは、一貫した制御を設定して、グローバルトラフィックを1つの場所で監視できます。また、より優れた回復性を持つアーキテクチャを構築するためにも役立ち、チームは市場の状況変化に応じて素早く方向転換することができます。
- **連携する複数のネットワーク機能を提供するクラウドプロバイダーを探す。**
  これにより、多くの場合、トラフィックが実行する必要があるネットワークホップの数が少なくなり、結果として遅延が減少するため、エンドユーザーエクスペリエンスが向上します。また、ネットワーク問題に関するトラブルシューティングを行う際に、複数ではなく1つの企業に連絡するだけであれば、もっと簡単になります。さらに、複数の機能をバンドルすると、多くの場合コストが下がります。
- **あらゆる場所から複数のネットワーク機能を実行できるクラウドプロバイダーを探す。**
  買収によってサービスポートフォリオを拡大するプロバイダーは、必ずしもこれらの新しいサービスを完全に統合するとは限りません。これは、特定の機能は特定のデータセンターを通してのみ提供されることを意味します。上述の問題を回避するためにも、ネットワーク全体にわたってこれらの機能を提供するプロバイダーを検討してください。
- **広いグローバルプレゼンスを持つクラウドプロバイダーを探す。**
  これにより、前述の場所の柔軟性がサポートされ、エンドユーザーの居場所を問わず、常にネットワークの近くにいることが保証されます。また、大規模なネットワーク面積により、DDoSトラフィックを吸収し、大容量を必要とする他のネットワーク機能を実行することが可能となります。

Cloudflareのサービス

企業は、ハードウェアの到着を待ったり、ほんの数年しかもたないコンピューターにさらに投資したりせずに、自分のネットワークトランスフォーメーションを加速させることができますか?
Cloudflareを使用します。

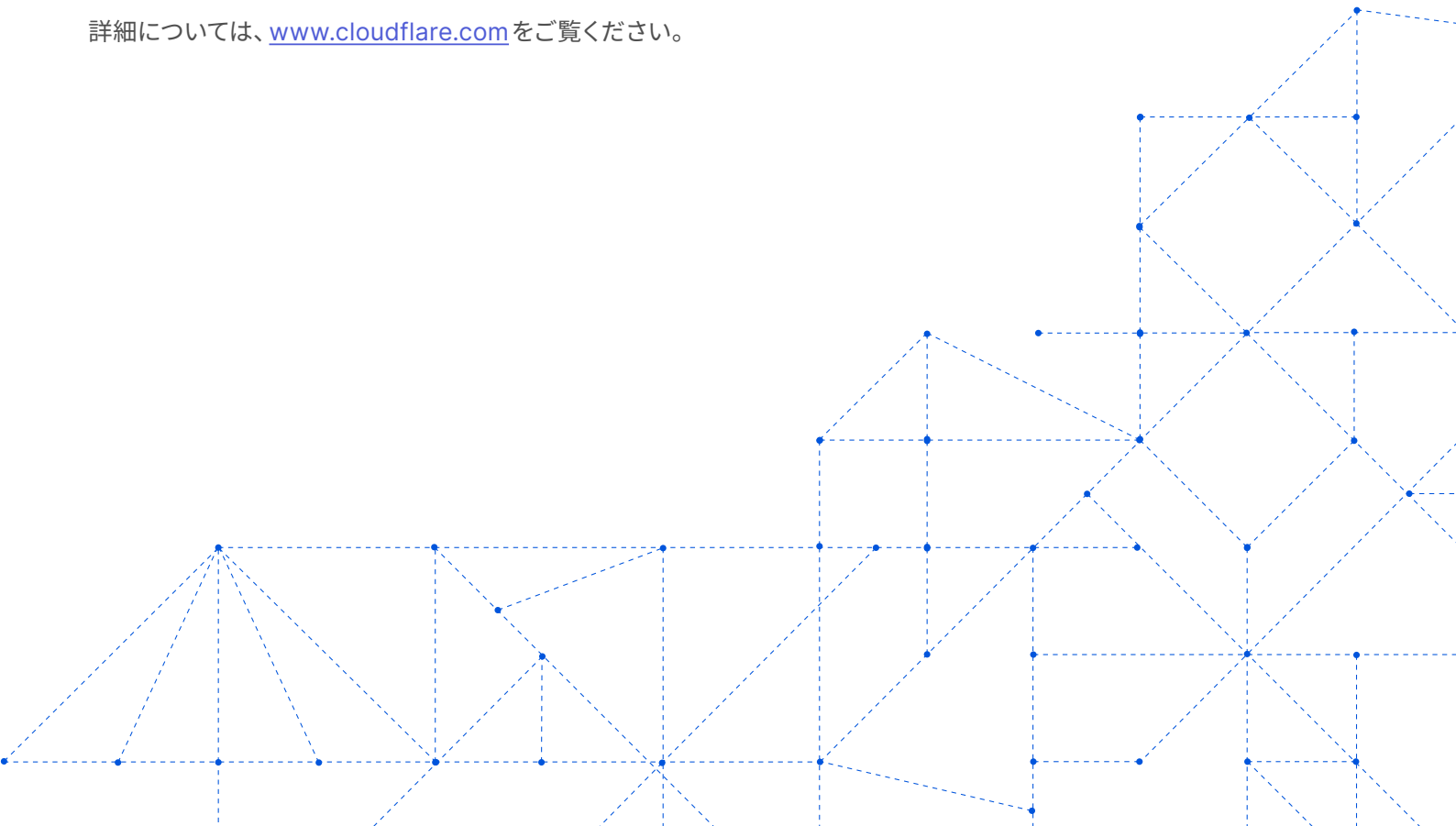
Cloudflareはさまざまなネットワークサービスを提供するグローバルクラウドプラットフォームです。これによりビジネスをより安全にしてアプリケーションのパフォーマンスを強化し、個々のネットワークハードウェアを管理する費用や複雑性を排除しています。Cloudflareのプラットフォームは、拡張可能で使いやすい統合型制御プレーンを提供し、オンプレミス、ハイブリッド、クラウド、サービスとしてのソフトウェア (SaaS) アプリケーションに対してセキュリティ、パフォーマンス、信頼性を提供しています。

重要なこととして、Cloudflareの270以上の都市グローバルネットワークにあるすべてのデータセンターでこれらすべてのサービスを提供できるため、クラウドの実装を複雑化する遅延が削減されます。あなたのネットワークスタックを効率化して、トランスフォーメーションを加速し、次に起きる脅威からネットワークを保護します。

詳細については、www.cloudflare.com をご覧ください。

「Dropboxは最近 "バーチャルファースト" 企業になりました。私たちはこの企業戦略が当社のセキュリティアプローチおよびネットワークアーキテクチャに影響を与える様子を観察してきました。私たちや他のリモート優先企業がこの「ニューノーマル」に適応する方法を学習するための、Cloudflareのサポートに感謝しています。」

Konstantin Sinichkin
Dropbox担当エンジニアリングマネージャー



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

REV:BDES-3313.2022JUN10