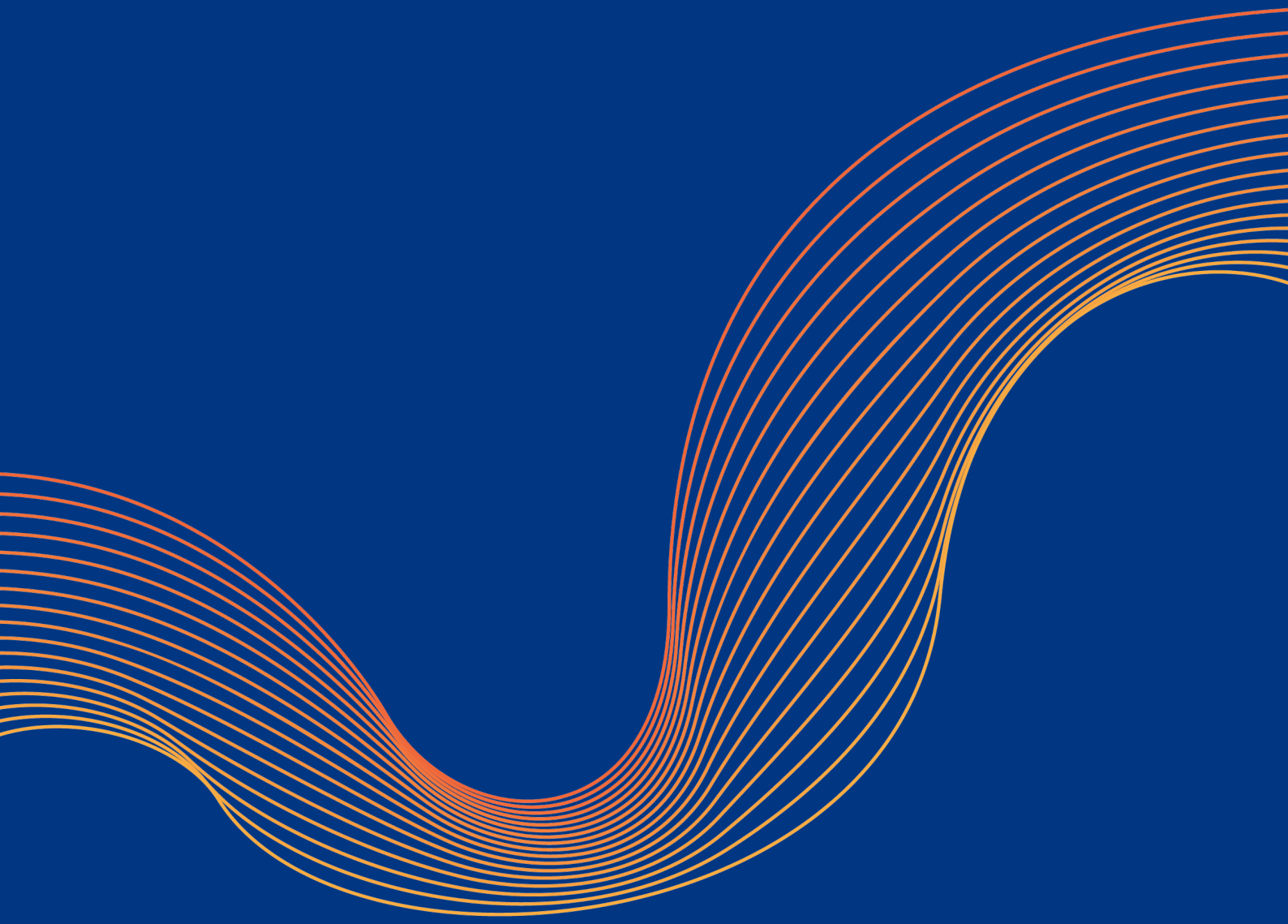
ホワイトペーパー

CLOUDFLARE

Magic Transitの ユースケースと リファレンスアーキテクチャ



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

目次

はじめに

本ドキュメントの目的は、Cloudflare Magic Transitの主要なアーキテクチャ、機能、およびネットワークデプロイメントオプションについて説明することです。Cloudflare Magic Transitは、インターネットに接続されたネットワークインフラストラクチャ向けの、BGPベースのDDoS攻撃対策およびトラフィック高速化サービスです。

第2章

Magic Transitとは？

DDoS攻撃からネットワークインフラストラクチャを保護するには、強さと速さの独自の組み合わせが必要です。帯域幅消費型攻撃は、ハードウェアボックスと帯域幅に制約のあるインターネットリンクを簡単に圧倒します。また、ほとんどのクラウドベースのソリューションは、トラフィックを中央のスクラビングセンターにリダイレクトするため、ネットワークのパフォーマンスに大きな影響を与えます。

Cloudflare Magic Transitは、オンプレミス、クラウド、ハイブリッドのネットワークをDDoS攻撃から保護し、トラフィックの高速化を実現します。250都市に広がるデータセンターと 100 Tbpsを超える軽減能力により、Magic Transitは、発生元に近い攻撃を世界平均で3秒未満で検出し、軽減できます。その一方で、パブリックインターネットよりも高速にトラフィックをルーティングできます。

簡単に説明すると、Magic Transitは次のように動作します。

接続: Border Gateway Protocol（BGP）のインターネットへのルートアナウンスやCloudflareのエニーキャストネットワークを使い、カスタマートラフィックをソースに一番近いCloudflareのデータセンターに統合します。

保護とプロセス：全てのカスタマートラフィックに対して攻撃の検査を行います。攻撃を検出した際には高度で自動化された軽減技術が即座に適用されます。負荷分散や次世代ファイアウォール、コンテンツキャッシング、サーバーレスコンピューティングなどといったその他の機能もサービスとして提供されます。

高速化： クリーンなトラフィックは、スループットを最適化するためにCloudflareの低遅延ネットワークリンクを経由してルーティングされ、IPトンネル (GREまたはIPsec) またはプライベートネットワークインターコネクト (PNI) を経由してオリジンネットワークに渡されます。Magic Transitは、Cloudflareのトンネルエンドポイントに Anycast IPアドレスを使用します。つまり、どのデータセンターのどのサーバーでも、同じトンネルのパケットをカプセル化およびカプセル化解除できます。トンネルとカプセル化の詳細については こちらを参照してください。

エニーキャストを使ってネットワークに復元力をつける：

Magic Transitは、ネットワークトンネルのエンドポイントにエニーキャストのIPアドレスを使用します。つまり、お客様のネットワークからCloudflareへとつながる1本のトンネルが、すべてのCloudflareグローバルデータセンター（チャイナネットワークを除く）へとつながります。しかし、これによってルーターに負担がかかることはありません。ルーターから見れば、単一IPエンドポイントを使用した1本のトンネルに過ぎないからです。

このトンネルのエンドポイントが技術的に1つのIPアドレスにつながるものであって、特定のデバイスにつながる必要がないというのが、これが機能する理由です。外部ヘッダーを削除して、内部パケットをルーティングできるデバイスであれば、このトンネル経由で送信されたパケットを処理できます。

ネットワーク障害や他の問題が発生した際、トンネルは自動的にフェイルオーバーします。お客様のネットワークパフォーマンスへの影響はゼロです。

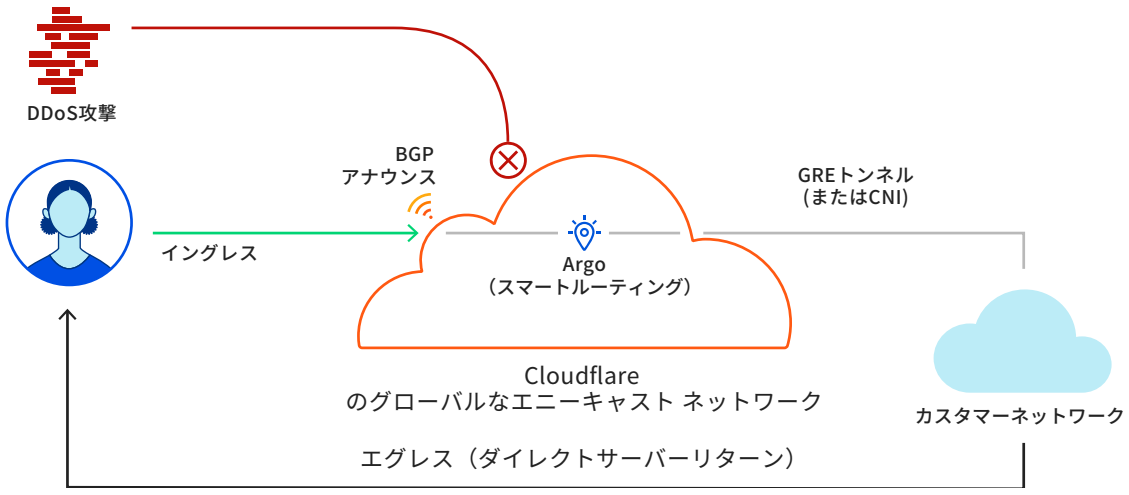


図1：Magic Transitの概要

第3章

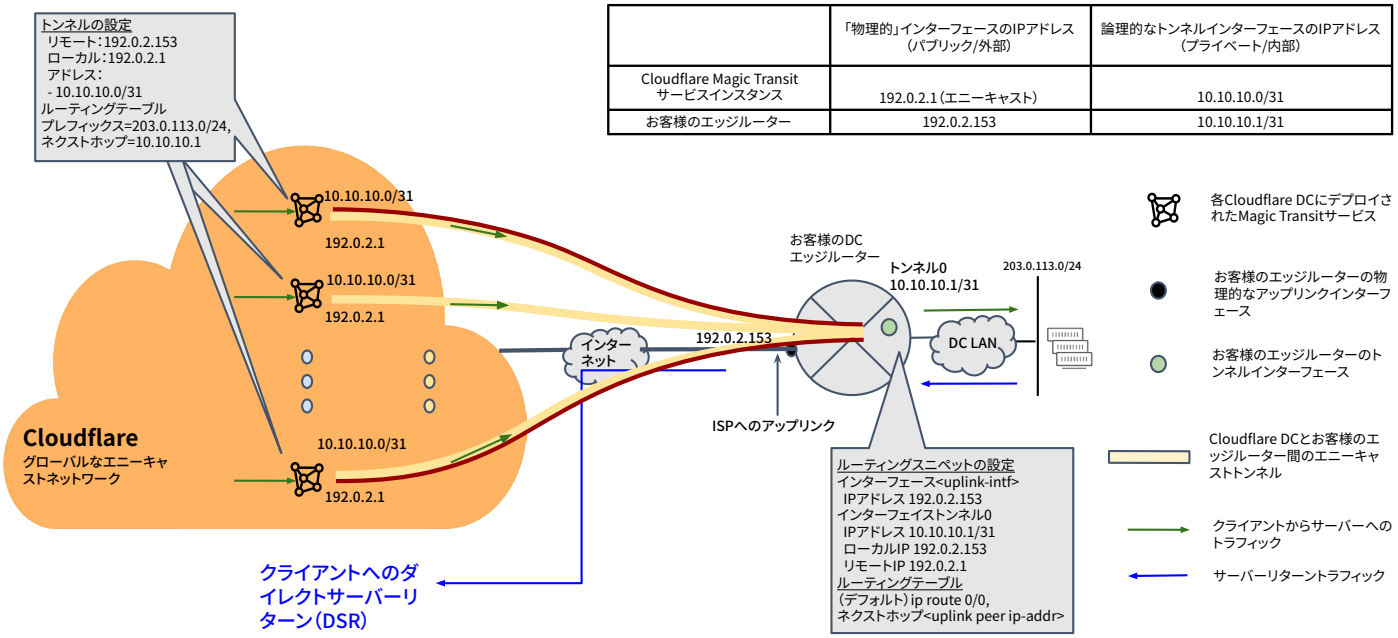
3.1 Magic Transitの導入アーキテクチャ

デフォルト設定（イングレスのみ、ダイレクトサーバーリターン）

デフォルトでは、Magic Transitは、イングレス方向（インターネットからカスタマーネットワークへ）のトラフィックのみを処理します。クライアントへのサーバーリターントラフィックは、エッジルーターのデフォルトルーティングテーブルに基づいて、お客様のDCエッジルーターからインターネット/ISPへのアップリンクを経由してルーティングされます。このサーバーリターントラフィックは、トンネルを経由してCloudflareを通過することはありません。これはDSR（ダイレクトサーバーリターン）と呼ばれています。

図2のネットワーク図は、このようなMagic Transitのセットアップと、Magic Transitで保護されたトラフィックのエンドツーエンドのパケットフローを示しています。このセットアップのトンネルは、カプセル化にGREを使用します。

- Cloudflareは、トンネルエンドポイントのCloudflare側のエニーキャストIPアドレスのペアをお客様に提供します。これらは、Cloudflare独自のアドレス空間からパブリックにルーティング可能なIPアドレスです。エニーキャストIPアドレスのペアは、ネットワークの冗長性を確保するために2本のトンネルの設定に使用できますが、基本的な設定に必要なアドレスは1つだけです。上記の設定は、1本のトンネルを示しており、Cloudflare側のトンネルエンドポイントのアドレスは192.0.2.1です。
- お客様側のエニーキャストGREトンネルは、パブリックにルーティング可能なアドレスである必要があります。一般的には、お客様のエッジルーターのWANインターフェースのIPアドレスです。この例では、192.0.2.153です。
- トンネルインターフェースのIPアドレスは、RFC1918のプライベートアドレスです。これらはトンネルヘッダー内にカプセル化され、カプセル化されたパケットがインターネット上で転送された後、2つのトンネルエンドポイントデバイス（Cloudflareサーバとお客様のエッジルーター）によってカプセル化が解除された場合にのみ表示されます。



	「物理的」インターフェースのIPアドレス（パブリック/外部）	論理的なトンネルインターフェースのIPアドレス（プライベート/内部）
Cloudflare Magic Transit サービスインスタンス	192.0.2.1（エニーキャスト）	10.10.10.0/31
お客様のエッジルーター	192.0.2.153	10.10.10.1/31

図2：デフォルトのDSRオプションを使用したMagic Transit Tunnel（GRE）の参考構成

- これらのトンネルインタフェースアドレスは、それらが属する特定のMagic Transitサービスインスタンス内でのみ「ローカルに重要」です。したがって、お客様は、同じMagic Transitサービスインスタンス内に設定された他のトンネルのアドレスと重複しない限り、希望するRFC 1918アドレスを選択できます。
- ベストプラクティスとして、トンネルがポイントツーポイント接続であることを考慮すると、特定のトンネルに必要な2つのIPアドレスを割り当てるには、/31サブネットで十分です。上の例では、10.10.10.0/31サブネットが選択されています。トンネルインターフェースのCloudflare側を10.10.10.0/31、お客様のDCエッジルーター側を10.10.10.1/31としています。
- トンネルが設定されると、Magic Transitサービスインスタンスに静的ルートが設定され、指定されたお客様のプレフィックス宛のトラフィックが正しいトンネルに転送されます。
- お客様のプレフィックス203.0.113.0/24宛のトラフィックは、トンネルインターフェースのリモートエンド（Cloudflareネットワークから見たお客様側）が10.10.10.1であるトンネルにルーティングされます。
- これがDirect Server Return (DSR) のセットアップである場合、サーバーのリターントラフィックは、お客様のエッジルーターに設定されたデフォルトルート (ip route 0/0) に従って、インターネットからクライアントに戻る途中で、アップリンクピア（お客様のISPのルーター）に送信されます。

注記： ほとんどのISPがお互いのBGP広告で受け入れる最小のIPプレフィックスサイズ（つまり、最長のIPサブネットマスクを使用）は/24です。例えば、x.x.x.0/24またはy.y.y.0/23はOKですが、z.z.z.0/25はNGです。したがって、Cloudflare Magic Transitがお客様に代わって広告できる最小のIPプレフィックスサイズは/24です。

3.2 エグレスオプションを有効にしたMagic Transit

Magic Transitがエグレスオプションを有効にしてデプロイされている場合、お客様のネットワークからのエグレストラフィックはCloudflareのネットワーク上にも流れます。 このデプロイメントオプションでは、トラフィックフローの対称性を実現し、クライアントからサーバーへのトラフィックフローとサーバーリターントラフィックフローの両方がCloudflareネットワークを経由します。この実装により、Cloudflareのネットワークを利用することで、サーバーリターントラフィックにセキュリティと信頼性が加わります。

次のネットワーク図は、Magic Transitのエグレスオプションを有効にした場合の、エンドクライアントとカスタマーネットワーク間のエンドツーエンドのパケットフローを示しています。

- 「イングレス」のトラフィックフローは、ユースケース3.1と同じです。
- エグレストラフィックがMagic Transitで受信および処理されるには、トラフィックの送信元IPアドレスが、Magic Transitで保護されたIPプレフィクスの範囲内にある必要があります。また、送信先IPアドレスは、パブリックインターネットのルーティング可能なアドレス（RFC 1918以外のアドレス）である必要があります。

クラウドホスト型のサービス用に独自のパブリックIPアドレスを持ち込む（BYOIP）お客様にとっては、Magic Transitのエグレスオプションを利用することで、クラウドプロバイダーとの間でBYOIPサービスを購入・導入する必要がなくなります。さらにクラウド料金の削減や運用コストの低減など、付加価値を提供できることは注目に値します。

これを実現するために、クラウドプロバイダーのVPCとCloudflareネットワークの間に、Magic Transitにオンランプする IPトンネルを設定します。Magic Transitのエグレスオプションを使用すると、クライアントとサーバーの両方向のトラフィックがこれらのIPトンネルを通過します。トンネルパケット内のBYOIPアドレスは、外側のトンネルエンドポイントIPアドレスとトンネルヘッダーの後ろに隠され、VPCとCloudflareネットワーク間の基盤となるクラウドプロバイダーのネットワーク要素からは「見えない」ようになっています。

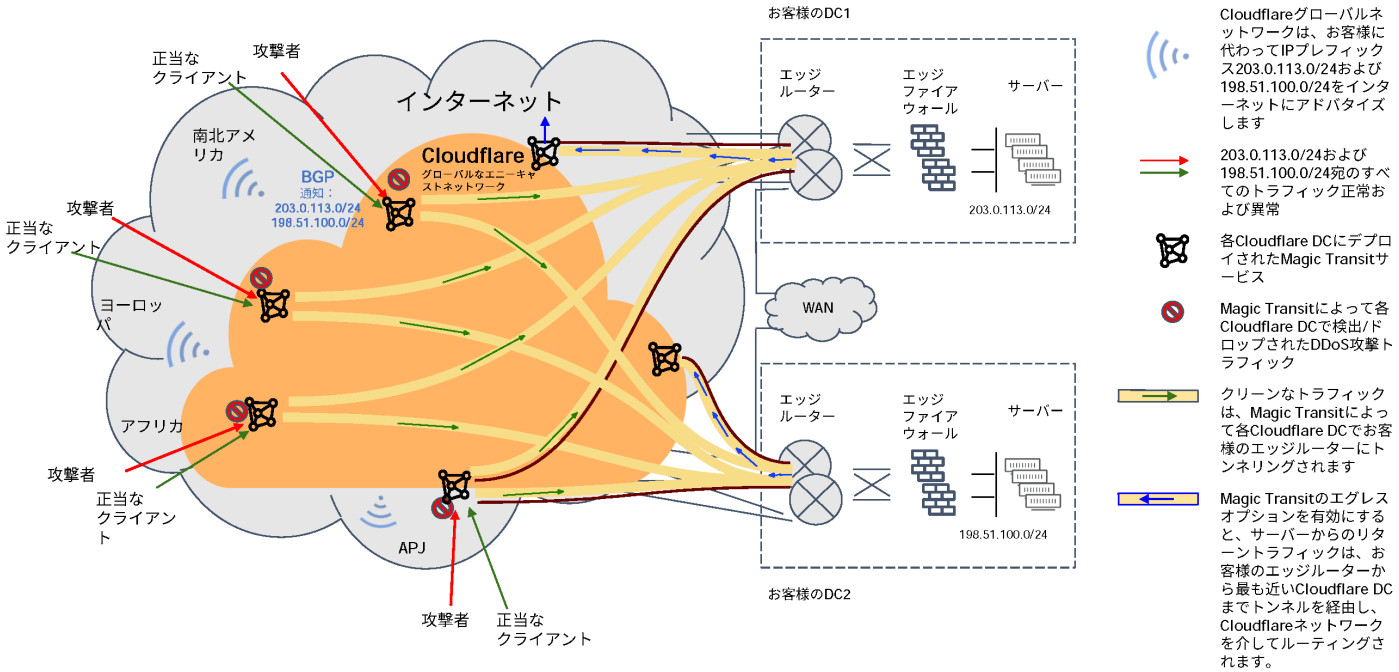


図3：Magic Transit（Egressオプション有効）

第3章

3.3 Cloudflareネットワークインターコネクト（CNI）経由のMagic Transit

Cloudflareネットワークインターコネクト（CNI）は、お客様のネットワークインフラストラクチャをパブリックインターネットを経由せずに直接Cloudflareに接続することで、信頼性、パフォーマンス、安全性を向上させることができます。CNIの詳細については[こちら](#)をご覧ください。

- CNIは、クロスコネクトプロバイダーによって一連のレイヤー2接続としてプロビジョニングされ、Cloudflareは、Cloudflare自身のインターネットルーティング可能なIPアドレスブロックからIPアドレスのペアを各接続に割り当てます。
- Cloudflareは、これらのリンクを設定し、CNIのオンボーディング中にリンク上でBGPピアリングセッションを確立するために、お客様と調整します。
- CNI経由で接続されているCloudflareネットワークとお客様のエッジルータ間でBGPセッションが立ち上がると、Cloudflare独自のプレフィックスがこのCNIリンクを経由してお客様のエッジルーターにアドバタイズされます。

図4は、CNI経由のMagic Transitの参照設定と、関連するパケットフローを示しています。

注記： ここでは、エグレスオプションを有効にしていないデフォルトのMagic Transitサービスの例を示しています。前のセクションで説明したように、Magic Transit Direct Server Returnモード（イングレスのみ）では、サーバーリターントラフィックは、お客様のエッジルーターによって、パブリックインターネットを介してISP経由でクライアントにルーティングされます。

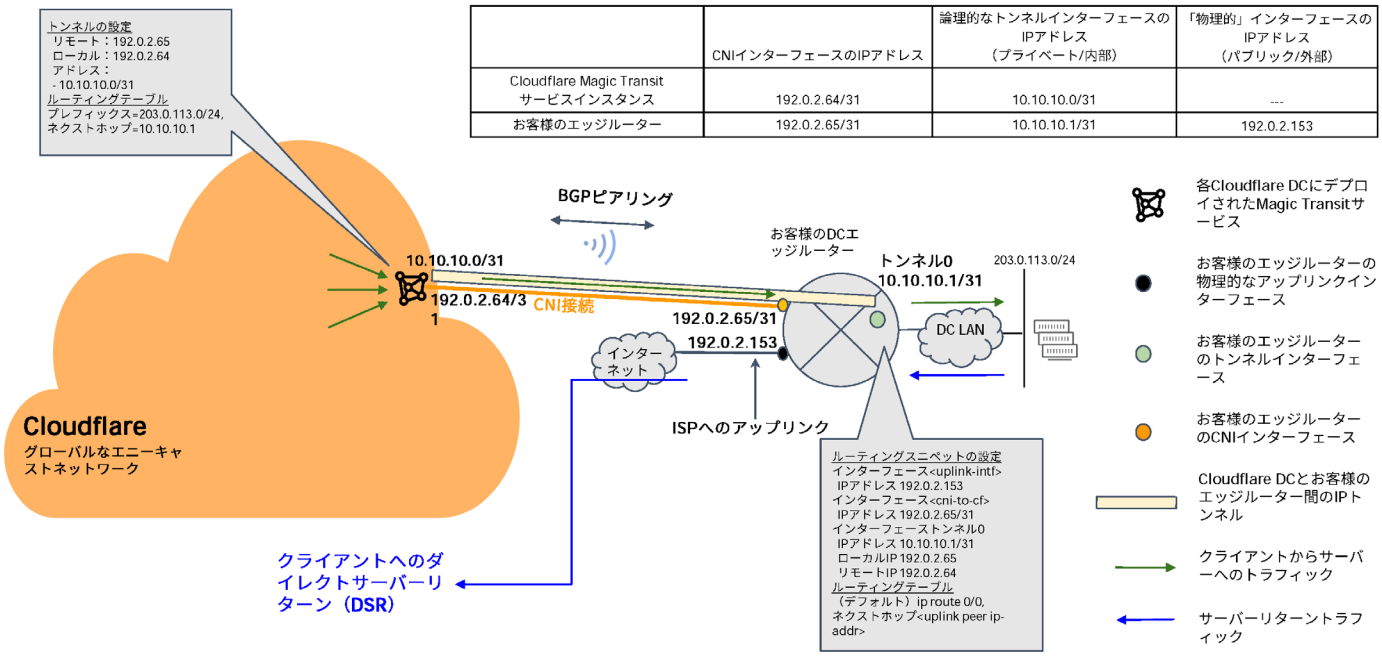


図4：Magic Transit over CNI（デフォルトのDSRオプション）の参考構成

第3章

Magic Transitのエグレスオプションを有効にして使用すると、サーバーリターントラフィックを、CNI接続で設定されたIPトンネルを経由して、Cloudflareネットワークを介してクライアントに送り返すことができます。図5はその一例を示したものです。

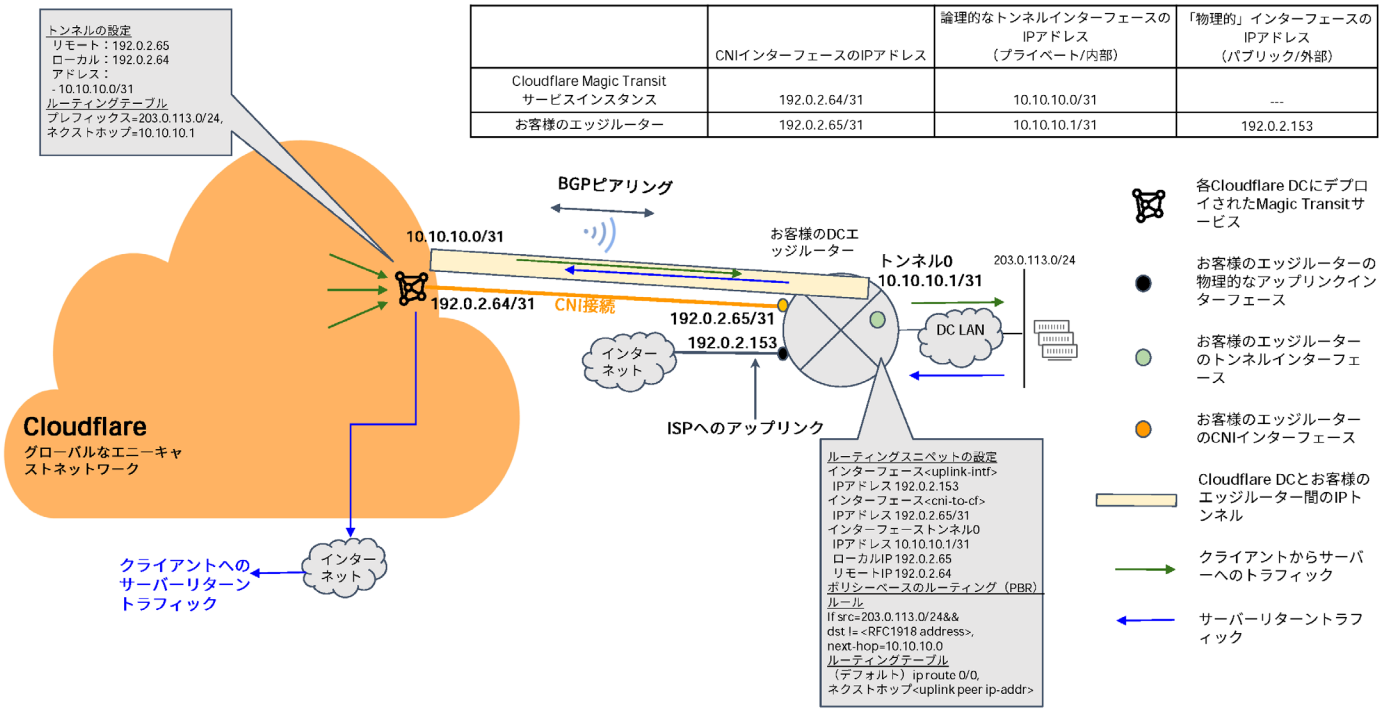


図5：Magic Transit over CNI（Egressオプション有効）の参考構成

3.4 パブリックのクラウドホスト型サービスを保護するMagic Transit

Magic Transitは、オンプレミスとクラウドでホストされているサービスを保護します。このユースケースでは、クラウドホスト型デプロイメント用の設定を説明します。

- この例では、特定のお客様が2つの異なるクラウドプロバイダー、および2つの異なる地理的リージョンに分散した2つのクラウドVPCデプロイメントを持っています。
- この例では、お客様の/24以上のプレフィクスが複数の小さい（サブネットマスクの長さが長い）プレフィクス（例えば/26）に分割され、異なるロケーションのさまざまなVPCに割り当てられます。Cloudflareネットワークから各VPCへのトンネルを確立すると、お客様はMagic Transitの設定で一元的に静的ルートを設定し、トラフィックを各VPCにルーティングできます。このような設定は、APIまたはUIダッシュボードを経由して行うことができます。

Magic Transitのエグレスオプションを使用すると、Magic Transitトンネル経由でCloudflareグローバルネットワークを介してエグレストラフィック（サーバーリターンやサーバーからインターネット）を送信することで、各クラウドプロバイダーのBYOIPサービス、関連する料金、管理・運用の煩雑さを回避できます。

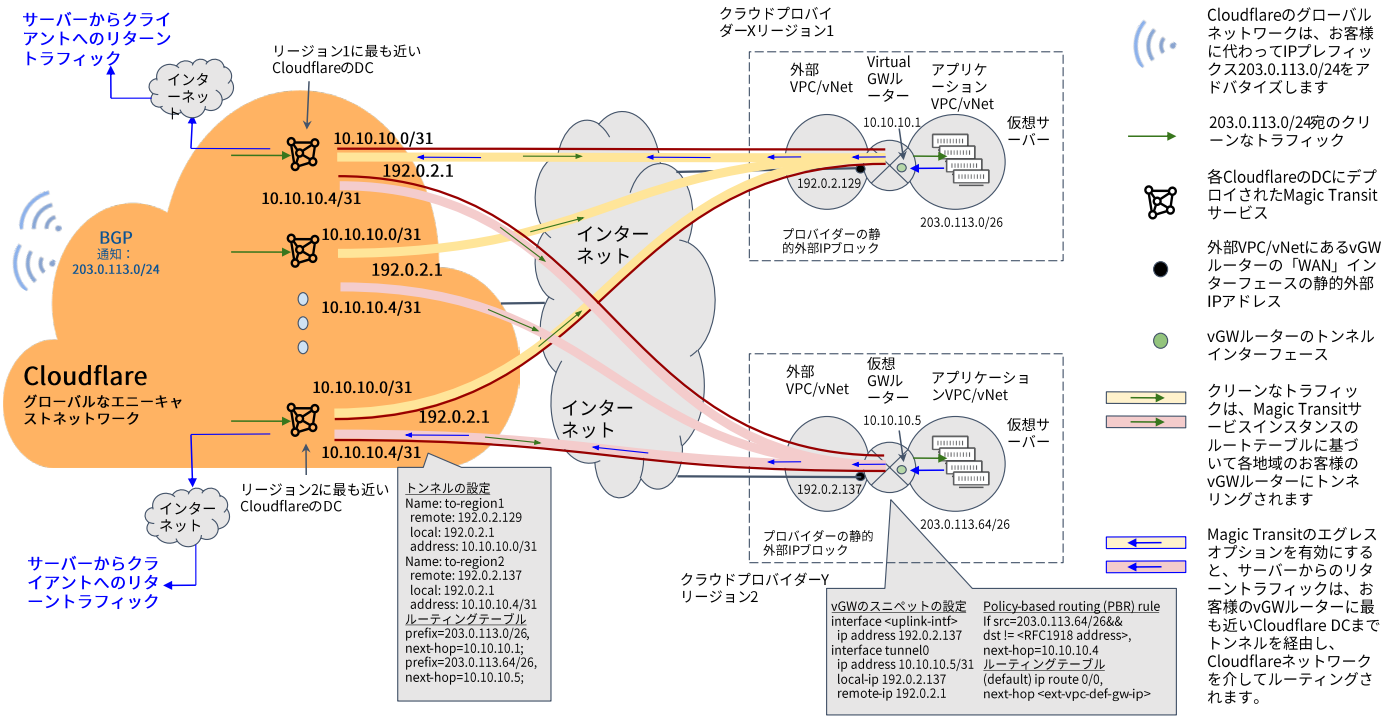


図6：Magic Transit（Egressオプション有効）でマルチクラウドベースのサービスを保護

3.5 Magic TransitとMagic WAN

Cloudflare Magic Transitサービスを使用すると、企業の外部向けサービスのトラフィック（南北方向のインターネットのルーティング可能なトラフィック）を保護およびルーティングすることに加えて、 Cloudflare Magic WANを使用して、企業のすべてのサイトを相互に接続する東西方向の「企業内」の内部トラフィック（RFC1918のプライベートアドレスなど）を保護できます。

Magic WANは、従来のWANアーキテクチャをCloudflareネットワークに置き換え、グローバルな接続性、クラウドベースのセキュリティ、パフォーマンス、制御を1つのシンプルなユーザーインターフェースで実現します。

Cloudflare Magic TransitとMagic WANのサービスを組み合わせることで、企業全体を対象とした、安全で信頼性が高く、パフォーマンスに優れたグローバルなNetwork-as-a-Serviceソリューションを実現し、東西および南北のトラフィックを保護し、高速化できます。

両方のサービスを同じサービスインスタンスにデプロイできます。また、外部のインターネットに接続されたネットワークと内部の企業ネットワークの管理とトラフィックフローを完全に分離しておきたい場合は、Magic TransitとMagic WAN用に異なるサービスインスタンスをデプロイすることもできます。

図7は、Magic TransitとMagic WANのサービスを別々のサービスインスタンスにデプロイした例です。

- この例では、GREトンネルを使用して、Cloudflareグローバルエニーキャストネットワーク経由でお客様のさまざまなサイトに接続します。Magic Transitサービスインスタンス用のCloudflareエニーキャストIPアドレスは192.0.2.1です。一方、Magic WANサービスインスタンスのアドレスは192.0.2.2です。Magic Transitサービスは、エグレスオプションで有効になります。
- Magic Transitサービスは、外部向けフロントエンドのクライアントサーバートラフィックを保護し、ルーティングします。Magic WANサービスは、内部アプリケーション、バックエンドのデータベース同期、支社からDC、支社から支社へのトラフィックなど、企業の内部トラフィックを保護し、ルーティングします。

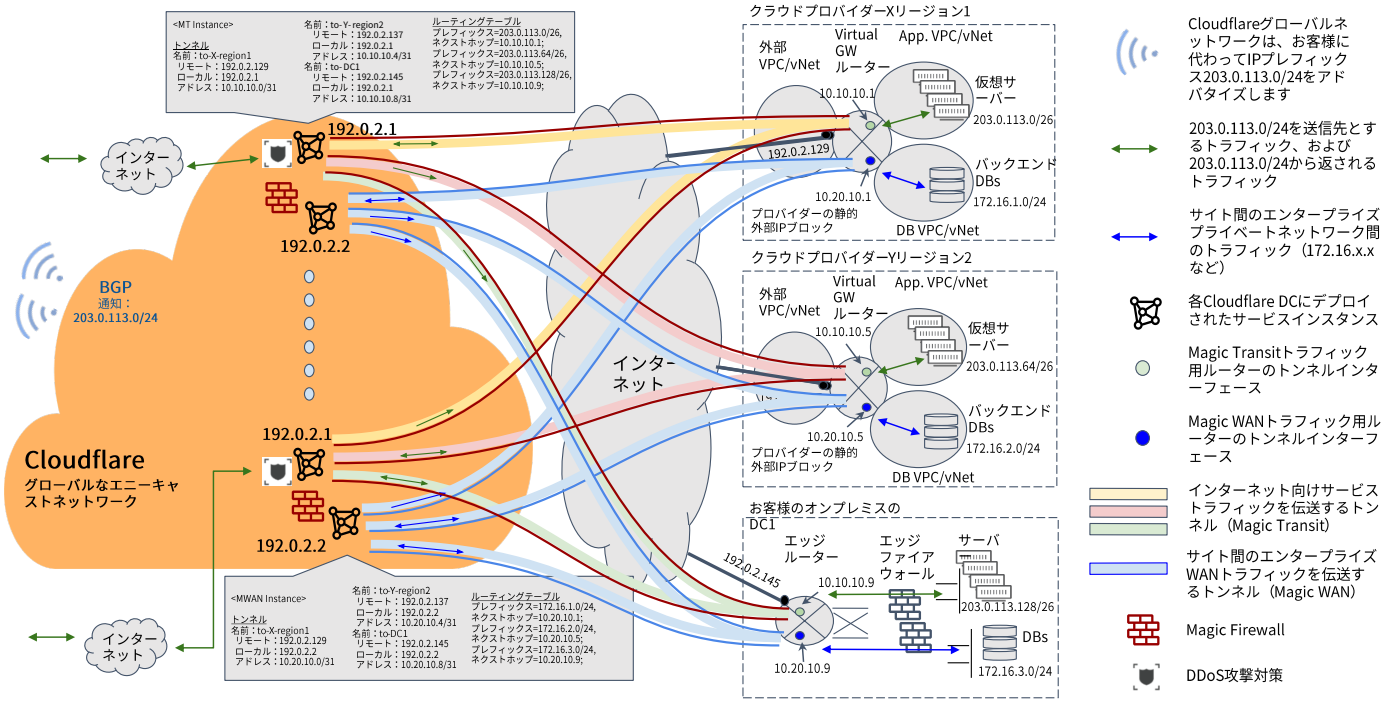


図7：Magic Transit + Magic WANが企業全体に与えるNetwork as a Service

3.6 Magic Firewall：企業ネットワークに到達する前の不要なトラフィックの制御とフィルタリング

Magic TransitがDDoS攻撃からお客様のサービスを保護する一方で、多くのネットワーク管理者は、他の不要なトラフィックや潜在的に悪意のあるトラフィックを制御し、ブロックしたいと考えています。Cloudflare Magic Firewallは、本社、支社、仮想プライベートクラウドなど、お客様のWAN全体に一貫したネットワークセキュリティポリシーを適用し、お客様が共通のダッシュボードから500ミリ秒未満できめ細やかなフィルタリングルールをグローバルにデプロイできるようにします。

Magic Firewallは、Magic Transitの一部としてデプロイ・設定されます。Cloudflareのエッジデータセンターを経由するすべてのイングレストラフィックは、Magic Transitによって送信先プレフィックスが保護されており、Magic Firewallによってフィルタリングできます。

Magic Firewallのルールでは、管理者は、IPパケットのヘッダーに含まれる一般的な5タプル（送信元/送信先IP、送信元/送信先ポート、プロトコル）の情報だけでなく、IPパケットの長さ、IPヘッダーの長さ、TTLなどの他のパケット情報に基づいて、ネットワークトラフィックを照合し、フィルタリングできます。また、Magic Firewallのルール（ジオブロッキング）を設定する際には、Cloudflareデータセンター/coloの名前、データセンターがある地域、国などの地理的な情報も利用できます。

Magic Firewallとその設定の詳細については、このブログ記事と当社の開発者向けドキュメントを参照してください。

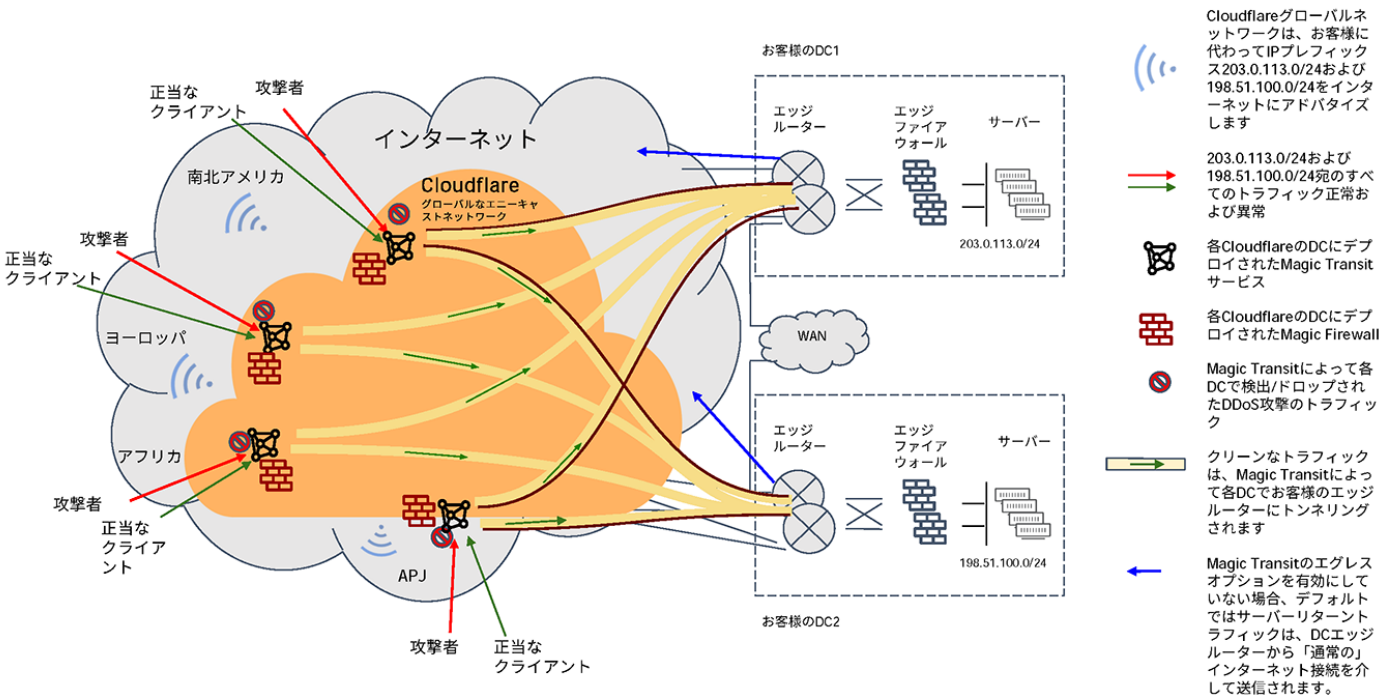


図8：Magic Firewallがインターネットエッジの望まないトラフィックや悪意のあるトラフィックをブロックブロック

第4章

常時稼働とオンデマンドのデプロイメントに関する注記

クラウドDDoS軽減サービスプロバイダーは、トラフィックの脅威を常に監視したり（常時稼働のデプロイメントモデル）、攻撃が検出された場合にのみトラフィックを再ルーティングしたり（オンデマンド）できます。この決定は、応答時間と軽減までの時間に影響します。また、場合によっては、遅延にも影響します。

オンデマンドのデプロイメントモデルでは、インバウンドトラフィックをネットワーク Edgeで監視・計測し、帯域幅消費型攻撃を検出します。通常のオペレーション時（平時）には、すべてのトラフィックが、遅延やリダイレクトなしに、アプリケーションやインフラストラクチャに直接到達します。トラフィックは、アクティブなDDoS攻撃の場合にのみ、クラウドスクラビングプロバイダーに転送されます。多くの場合、お客様はサービスプロバイダーにコールしてトラフィックをリダイレクトする必要があるため、応答時間が長くなります。

常時稼働モードは、DDoS軽減のためのハンズオフアプローチであり、攻撃を受けた際にお客様には何もしていただく必要はありません。組織のトラフィックは、平時であっても、脅威を検査するために常にクラウドプロバイダーのデータセンターを経由します。これにより、検出から軽減までの時間が最小限に抑えられ、サービスの中断がなくなります。

すべてのアプローチとデプロイメントオプションの中で、常時稼働方式は最も包括的な保護を提供します。

ただし、プロバイダーによっては、すべてのトラフィックをDDoS軽減プロバイダーのクラウド経由で転送すると、ビジネスに不可欠なアプリケーションにとって最適とはいえない遅延が発生する場合があります。Cloudflareは、常時稼働のデプロイメントであっても、攻撃による遅延のペナルティが発生しないように設計されています。エッジでトラフィックを分析することは、パフォーマンスに影響を与えずに大規模な軽減を行う唯一の方法です。

これは、エニーキャスト経由でトラフィックを取り込むと、トラフィックが最も近いCloudflareデータセンターにのみ移動して検査されるためです。データセンターは100カ国以上、250都市以上にあるため、近くで検査される可能性が高くなります。これにより、トロンボーン効果を取り除くことができます。

多くの場合、トラフィックは公共のインターネットを経由するよりも、Cloudflareを経由する方が速くなります。当社は、お客様が包括的なセキュリティを実現するためにパフォーマンスを犠牲にする必要はないと考えています。

第5章

まとめ

Cloudflareは、オンプレミス、クラウドホスト型、ハイブリッドの企業ネットワークを接続し、保護するための包括的なネットワークサービスを提供しています。Cloudflareは、お客様独自のアーキテクチャに合わせて、さまざまな接続およびデプロイメントオプションをご提供します。

- Cloudflare Magic Transitは、Cloudflareのグローバルネットワークの力を利用して、DDoS攻撃から組織を保護する、クラウドネイティブなネットワークセキュリティソリューションです。
- Magic Transitには、ビルトインのネットワークファイアウォールが搭載されており、お客様はオンプレミスのファイアウォールを段階的に廃止し、拡張性のあるサービスとしてネットワークセキュリティをデプロイできます。
- 企業の外部向けサービスのトラフィック（南北方向のインターネットルーティング可能なトラフィック）を保護・ルーティングするだけでなく、Cloudflare Magic WANを使用して東西方向の「企業内」の内部トラフィックを接続・保護することもできます。

Magic Transit、Magic WAN、またはMagic Firewallの詳細については、デモをご覧ください。