ホワイトペーパー

DDoS 攻撃に対抗する可用性と耐障害性を備えた DNS 設計

Akamai

はじめに

Edge DNS は、権威 DNS サービスを組織に提供します。これによって組織は、その Web サイトやその他のアプリケーションにエンドユーザーをつなげることができます。組織は、パフォーマンスに多大な関心を寄せている一方で、DNS の可用性と耐障害性の重要性について見落としがちです。特に、サービスを妨害し、エンドユーザーが接続できないようにする DDoS 攻撃が挙げられます。Akamai は、大規模な DDoS 攻撃を受けても可用性を維持できるように Edge DNS を設計しました。Edge DNS は、他に類を見ない世界規模、セグメント化された IP Anycast アーキテクチャ、複数の DDoS 制御機能を備え、必要に応じて他の Akamai サービスを活用することもできます。マネージド DNS サービスとして提供される Edge DNS は、パフォーマンスと可用性を最適な組み合わせで提供し、エンドユーザーが常に接続できるようにします。

統計データに関する注意事項

Akamai が Edge DNS を構築した元来の目的は、グローバル展開のコンテンツ・デリバリー・ネットワーク（CDN）ソリューションを支援する権威 DNS サービスを提供するためでした。Akamai は長年にわたり、大規模な DNS インフラストラクチャの拡張と可用性を実現するための最適な方法について、多くの教訓を得てきました。右に記載されている統計データの概要は、このプラットフォームの概算的な規模を表しています。ただし、統計データ単独では可用性と耐障害性に関する有益なガイダンスを提供できません。そのため、プラットフォームアーキテクチャ、具体的な DDoS 緩和機能、およびプラットフォームを攻撃から保護する際に Akamai が使用できる全体のリソースと合わせて検討する必要があります。

プラットフォームの統計データ

- 数千台のネームサーバー
- 1,000 か所を超える Point of Presence
- 140 を超える都市
- 40 を超える国

Akamai は、セキュリティ上の理由により、ネームサーバーの数や、Point Of Presence の数、場所、規模に関する具体的な詳細情報は公開していません。この方針は、攻撃を計画する際にそれらの情報を使用しようとする攻撃者から Akamai とお客様の両方を保護するものです。

アーキテクチャ

上記の統計データから分かるように、Edge DNS は、現在の市場で最も競争力のある他社の権威 DNS サービスよりもはるかに大規模です。ただし、サーバーおよび Point Of Presence の数、またはネットワークの総キャパシティーに関する統計データの概要は、グローバルプラットフォームの可用性と耐障害性の度合いを理解するためには不十分です。パフォーマンスのみを重視する他の DNS とは異なり、Akamai の Edge DNS は、パフォーマンスに加えて、DDoS 攻撃に対抗する可用性と耐障害性も考慮した設計となっています。そのため、ネームサーバー、Point of Presence、ネットワーク、およびセグメント化された IP Anycast クラウドなど、多層的な冗長性を備えたアーキテクチャが採用されています。

IP Anycast

Edge DNS を構成している数千台のネームサーバーは、1,000 か所を超える Point Of Presence に配置され、IP Anycast モデルで DNS クエリーに応答します。IP Anycast は、名前解決のために、エンドユーザーからのクエリーを一番近い Point Of Presence に誘導します。IP Anycast は、より高速な処理に加え、可用性と耐障害性について以下のいくつかの基本的な価値を提供します。ほとんどの権威 DNS サービスが IP Anycast を採用しているのはこのためです。

- **可用性** – IP Anycast では、異なるネットワークロケーションにある複数のネームサーバーが 1 つの IP アドレスに対するクエリーに応答できます。Edge DNS は、IP Anycast を活用することで、複数のデータセンターでの DNS 名前解決を組織に提供するだけでなく、世界規模で負荷分散することにより可用性も向上させます。加えて、ドメイン名解決全体の機能に影響を与えることなく、個別の物理サーバーや Point Of Presence 全体をオフラインにすることが可能です。
- **規模** – Edge DNS のインフラストラクチャは、多くの Point Of Presence に分散している多数の物理サーバーで構成されているので、大量の DNS リクエストへの応答にも常に確実に応答できる、大きなコンピューティングリソースを組織に提供します。また、多くの場合、Edge DNS はリソースを他の Akamai サービスと共有しているため、Point Of Presence の多くで、かなりの余剰ネットワークキャパシティーを利用できます。これらの要素により、Edge DNS は、スタンドアロンの DNS サービスよりもはるかに大きな規模で、DNS フラッドやその他の DDoS 攻撃に対応できます。
- **分散** – IP Anycast は、規模の拡大を可能にするだけでなく、Edge DNS が複数の Point Of Presence やさまざまなネットワークロケーションにわたってトラフィックを分散できるようにします。これらの Point Of Presence の地理的な場所やネットワーク展開を考慮することで、特定の地域やネットワークへの小規模な攻撃の影響を抑え、他の地域のクライアントシステムの可用性を維持することができます。

IP Anycast の活用は、Akamai に限ったことではありません。エンドユーザーからの DNS クエリーを複数のネームサーバーが解決できるようにすることで、IP Anycast はあらゆる DNS サービスに対して名前解決の可用性を向上させます。しかし IP Anycast であっても、耐障害性はプラットフォーム全体の規模によって制限されたままであり、大規模な DDoS 攻撃は依然としてクラウドベースのプラットフォームを圧倒することができます。さらに、複層的なアーキテクチャを用意しないと、小規模な攻撃であっても特定の地域の DNS サービスを停止させ、多数のエンドユーザーが使用できない状態となり、それらのユーザーが接続するすべての Web サイトの可用性に影響が及ぼされる可能性があります。

Edge DNS クラウド

攻撃に対する耐障害性をさらに向上させるために、Edge DNS はネームサーバーと Point Of Presence を複数の IP Anycast クラウドに分割します。Edge DNS クラウドは、専用のネームサーバーと Point Of Presence、および関連するネットワークキャパシティーと接続性で構成されています。すべてのクラウドがそれぞれ独立して機能するため、Edge DNS は可用性、規模、分散性の面で複数のスタンドアロン DNS プロバイダーに相当する可能性があります。

Edge DNS の IP Anycast クラウドは、多様なアーキテクチャを提供します。同一のクラウドは 2 つとありませんが、それぞれは大まかに 2 つの設計方針に沿って設計されています。それは、パフォーマンスと可用性です。

- **パフォーマンス** – パフォーマンスクラウドは、世界中の 100 か所以上に分散された Point Of Presence を内包し、各 Point Of Presence はいくつかのネームサーバーで構成されています。図 1 に示すように、パフォーマンスクラウドは、より速いルックアップ時間とより優れた本来の性能を提供するために、エンドユーザーおよび地域のインターネット・サービス・プロバイダー（ISP）に近い多くの場所に小規模なネームサーバー群を展開します。ただし、小規模な Point Of Presence は、コンピュータリソースとネットワークキャパシティーが比較的小さいため、当然のことながら DDoS 攻撃への耐障害性は低くなります。
- **可用性** – Edge DNS は多数の可用性クラウドを保持します。図 1 に示すように、可用性クラウドは Point Of Presence は少ないですが、1 つ以上のアンカー領域があります。アンカー領域には、大量の専用ネットワークキャパシティーおよび複数のネットワークとの接続性を備えた 1 つの中央データセンターに何百ものネームサーバーを含むことが可能です。アンカー領域は、DNS リクエストや他のネットワークトラフィックの急増に対応するための規模を可用性クラウドに提供します。可用性クラウドは、世界中のユーザーに対して許容水準の処理能力を維持するために、アンカー領域に少数の小規模な Point Of Presence を追加します。

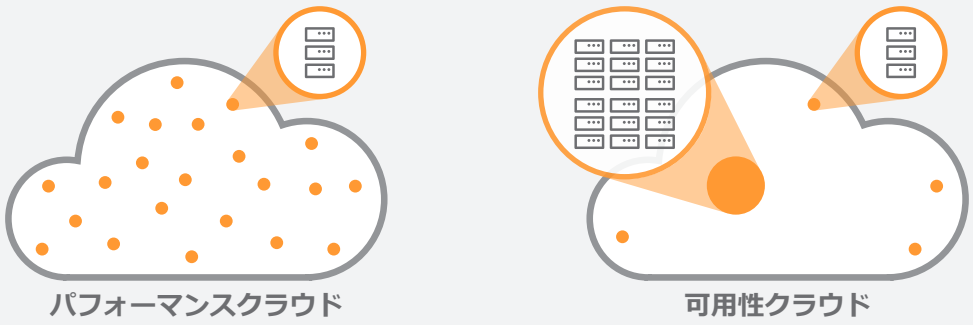

図 1：Edge DNS は、さまざまなアーキテクチャの複数の DNS クラウドを組み合わせることで、DDoS 攻撃に対抗するパフォーマンス、可用性、および耐障害性を最適なバランスで提供します。

セグメント化されたアーキテクチャ

Edge DNS は、単一の IP Anycast クラウドで権威 DNS サービスを運用している他のプロバイダーとは根本的に異なる可用性を提供します。IP Anycast により、プラットフォーム全体ではなく特定の地域にのみ影響を及ぼす小規模な攻撃を受けているときに、サービスが全体的なアップタイムを維持することができるため、すべてのプロバイダーにとっていくつかの可用性の利点がもたらされます。ただし、局地的な停止は、その影響が及ぼされた地域のエンドユーザーと、それらのユーザーと接続するためにそのサービスに依存している組織に影響を及ぼします。さらに、世界中の攻撃システムが生成するトラフィックによる大規模な DDoS 攻撃は、プラットフォーム全体を停止させる原因となる可能性があります。

多数の多様な IP Anycast クラウドがあるため、Edge DNS は 1 つ以上のクラウドを失っても機能を継続できます。この特性により、単一のクラウドアーキテクチャと比較すると、DDoS 攻撃に対して高い可用性と耐障害性を提供します。また、複数の IP Anycast クラウドを運用する利点として、プラットフォーム全体のサブセクション間でトラフィックをセグメント化することで、大規模な DDoS 攻撃を受けても、その影響を緩和できます。例えば、ある 1 つの Edge DNS IP Anycast クラウドに対する攻撃は、そのクラウドを構成する物理的なネームサーバーと Point Of Presence に誘導されます。セグメント化されたアーキテクチャによって、攻撃の影響は他の IP Anycast クラウドから分離されるため、個々のクラウドやお客様が DDoS 攻撃を受けていても、Edge DNS はすべての地域でプラットフォームの可用性を維持できます。

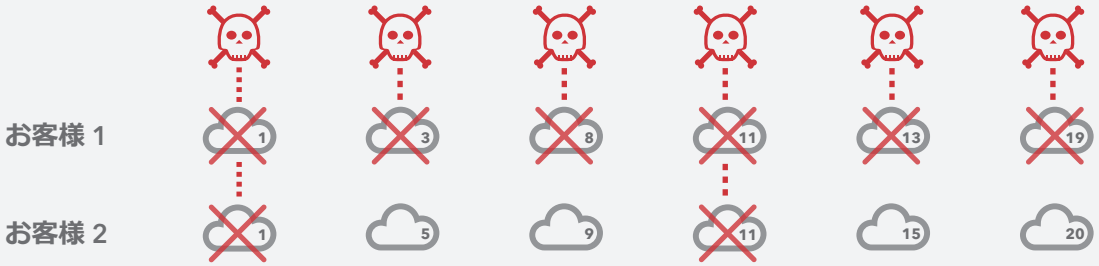

図 2：Edge DNS は、パフォーマンスクラウドと可用性クラウドの固有の組み合わせとしてお客様にネームサーバーを提供することで、他のお客様への攻撃からの巻き添え被害を最小限に抑えます。

Edge DNS のセグメント化されたアーキテクチャがもたらすメリットは、プラットフォーム全体の耐障害性を高めるだけではありません。特定のお客様が使用しているネームサーバーが攻撃された場合に、他のお客様への巻き添え被害のリスクも緩和できます。Edge DNS では、すべてのお客様に複数の Edge DNS クラウドが割り当てられますが、その際、パフォーマンスクラウドと可用性クラウドを固有の組み合わせで割り当て、他のお客様と同じ組み合わせにならないようにします。図 2 に示すように、このような分散は、お客様 1 とお客様 2 の間でのネームサーバーと IP Anycast クラウドの重複を最小限に抑えます。また、別のお客様に割り当てられた IP Anycast クラウドが大規模な DDoS 攻撃の明確な標的となった場合でさえ使用できるネームサーバーが、どのお客様にも存在するようになります。

お客様の委任の管理

1 つの組織が長期にわたって複数の DDoS 攻撃を受けることはよくあります。Akamai はこれまで、数か月以上にわたる広範で持続的な攻撃活動を確認してきました。このような場合、Edge DNS のセグメント化されたアーキテクチャのおかげで、Akamai は攻撃対象になっていないお客様への影響を柔軟な方法で最小化できます。図 3 に示すように、Akamai は必要に応じて個々のお客様のクラウドを再割り当てすることで、攻撃による影響をさらに隔離できます。

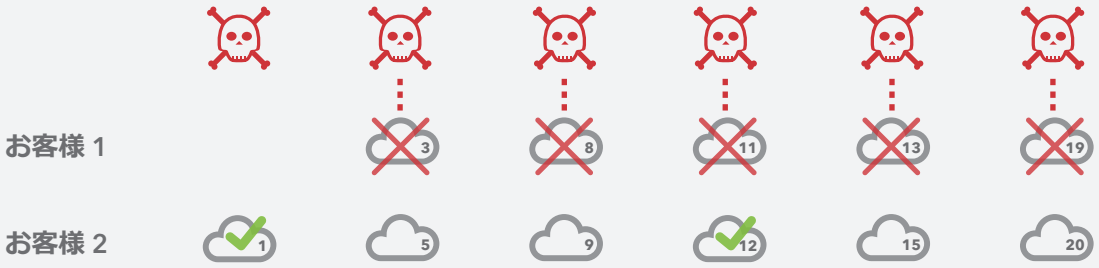

図 3：Akamai は、攻撃対象のお客様を個別のクラウドから移動させたり、攻撃の対象となっていないお客様の重複を最小限に抑えたりするなど、ネームサーバーの委任を管理することで、攻撃による影響をさらに最小化することができます（上記の図 2 と比較して）。

以下に例を挙げます。

- **攻撃対象となったお客様を特定のクラウドから移動させる** – Edge DNS のすべてのお客様は、他のお客様と IP Anycast クラウドを共有しています。そのため、あるお客様のすべての Edge DNS クラウドが攻撃の標的となった場合、他のお客様に割り当てられているクラウドの可用性にも影響を及ぼす可能性があります。通常の状況下では、再帰リゾルバーによって処理能力のより高いクラウドに自動的に切り替えられますが、持続的な攻撃の場合、Akamai は攻撃対象のお客様の IP Anycast を再割り当てすることで、攻撃対象でないお客様の可用性を回復させることができます。
- **攻撃対象外のお客様の重複を最小化する** — 場合によっては、Edge DNS の複数のお客様が、通常よりも多くの Edge DNS クラウドを共有していることもあります。このような場合、単一のお客様に対する大規模攻撃が、サービス全体は使用可能なままであるにもかかわらず、他のお客様の処理に重大な影響を及ぼす可能性があります。Akamai は必要に応じて、攻撃対象ではないお客様のクラウドを再割り当てすることで攻撃対象のお客様との共有を削減または除外し、攻撃対象ではないお客様のエンドユーザーの処理能力を回復させます。

多様なサーバー展開

Akamai は、各 Anycast クラウド内のさまざまな拠点に、そのクラウドの全体的な耐障害性を向上させるように設計された物理ネームサーバーを展開しています。Edge DNS クラウド内の拠点の多様性も、異なるネットワーク間でトラフィックをセグメント化する手段となります。これは、さまざまな状況で可用性を最大化するために役立ちます。以下に例を示します。

- **複数のネットワークを持つデータセンター内** – DDoS 攻撃に対する耐障害性を考える際には、キャパシティーと同様に、ネットワーク接続の多様性も重要な考慮事項となり得ます。大規模な DDoS 攻撃は、データセンターに到達する前に上流 ISP や他のネットワークを圧迫する可能性があるため、データセンター自体が影響を受けていない状態であっても、ネットワークの輻輳やサービスの停止を引き起こす可能性があります。攻撃の最中でも、可用性を保ち、エンドユーザーからの DNS クエリーに応答できるようにするため、Edge DNS では、キャパシティーが大きいだけでなく、複数のネットワークを介した接続性も備えたデータセンターにネームサーバーを展開しています。
- **ISP の分離** – 多くの場合、Edge DNS はネームサーバー群を個々の ISP のネットワークに直接展開します。これらのネームサーバーは、通常、IP Anycast のトラフィックをそのネットワーク内のみでブロードキャストし、それらの ISP のエンドユーザーに対してのみ DNS クエリーを解決します。このような形態は、特定のネームサーバー群がサービス提供できるエンドユーザーの数を制限することになるものの、IP Anycast クラウドがその ISP 外で攻撃の対象になった場合には、それらのユーザーの可用性を維持することが可能になります。攻撃者は、ネームサーバーを確認するために特定の ISP のネットワーク上にシステムを持たざるを得ません。その場合でも、通常、その 1 つのクラウドを保護するのに使用可能なキャパシティーは十分にあります。
- **ネットワークの多様性** – お客様には意図的に多様なクラウドが割り当てられます。たとえば、特定の ISP に固有のサーバー拠点を持つものであったり、広範な接続マシンを持つものであったりします。このようなアーキテクチャによって、所定のクライアントの再帰ネームサーバーは、利用可能な Edge DNS クラウドに必ず接続できます。

- **他の Akamai サービスと共有されるデータセンター内** – Akamai は、権威 DNS のほかにもさまざまなサービスを運用しているので、複数のサービスをサポートするデータセンターに Edge DNS ネームサーバーを展開できます。後に詳述しますが、これにより、大規模な DDoS 攻撃に対応する際に、Edge DNS が利用できるネットワークキャパシティーが増えます。他のサービスのために Akamai が用意しているパブリックピアリング調整や、専用ネットワーク容量も活用できるからです。

DDoS 制御

Edge DNS には、アーキテクチャの設計のほかにも、DDoS 攻撃の一種である DNS フラッドの影響緩和に役立つ制御機能がいくつかあります。大半の DDoS 攻撃が大量のトラフィックを使用してネットワーク網を圧迫するのに対し、DNS フラッドは正規の DNS リクエストを大量に生成し、物理ネームサーバー上のコンピューティングリソースやメモリーリソースを消費して実際のエンドユーザーからのクエリーに応答できなくします。Akamai は、以下のようにいくつかの方法で DNS フラッドから Edge DNS プラットフォームを保護します。

- **規模** – Akamai の権威 DNS サービスの規模は、他の競合 DNS ソリューションの何倍にも及びます。Edge DNS は、世界中の 1,000 か所を超える Points of Presence に配置された何千台ものネームサーバーを活用します。これは DDoS 制御に限ったことではありませんが、IP Anycast によって攻撃トラフィックがさまざまな地域およびネットワークに分散される一方、多数の物理ネームサーバーのおかげで Edge DNS は DNS リクエストの急増を吸収できるだけの十分なコンピューティングリソースとメモリーリソースを維持できます。

- **Rate Limiting** – Edge DNS には、Rate Limiting 機能があり、リクエスト量が設定しきい値を超えると、個々の IP アドレスからのリクエストを自動的にドロップできます。Rate Limiting は、DNS リクエストの急増による物理ネームサーバーのコンピューティングリソースとメモリーリソースの消費を防止します。また、大量のリクエストを生成する一方で比較的低い帯域幅を消費するような攻撃に対して役立ちます。Edge DNS の Rate Limiting は、その Edge DNS プラットフォーム固有のアルゴリズムで機能しているため、お客様による設定には対応していません。

- **DNS ホワイトリスト** – Akamai は、インターネットにおける当社の立場上、独自の可視性を有しており、インターネットにおける正規の DNS ルックアップの約 95% に対応する再帰リゾルバーの動作を把握できます。Edge DNS は、過負荷時には必要に応じて、ポジティブ・セキュリティ・モデルを使用し、DNS リクエストを既知の良好に動作する DNS リゾルバーのリストに制限します。

キャパシティー関連

DDoS 制御は、DNS フラッドによる影響の緩和には役立ちますが、他のタイプのネットワーク層 DDoS 攻撃に対応するためには、大量のトラフィックを吸収するために使用できる十分なネットワークリソースが必要になります。ここ数年、大量攻撃のリスクは劇的に増大しています。既知の最大規模の攻撃は、ピーク時の帯域幅が 1 Tbps を超えていました。

Akamai は、計測可能な指標を攻撃者に提供することを避けるため、Edge DNS プラットフォームのキャパシティーを公表していませんが、プラットフォームの規模に関するあらゆる面に継続的に投資を行い、インターネット上の新規顧客やトラフィックの増加に対応できるよう、Edge DNS のインフラストラクチャを拡大しています。クラウド・サービス・プロバイダーである Akamai は、サーバーを再利用して、新たな地域に迅速に DNS キャパシティーを展開する能力を備えています。トラフィックの急増を吸収できる大量のキャパシティーを保持しており、Edge DNS プラットフォーム上の通常のトラフィックで消費されているリソースは全体の 1% 未満です。Edge DNS は、DDoS 攻撃を緩和するために、必要に応じて他の Akamai プラットフォームのリソースを活用することもできます。

他の Akamai プラットフォームの活用

従来、大きな帯域幅を消費する DDoS 攻撃に耐える能力はネットワークキャパシティーで判断されますが、この方法は Edge DNS には使えません。Edge DNS は他の Akamai プラットフォームのリソースを活用できるからです。Akamai は DNS だけを扱う企業ではなく、Edge DNS 以外にも多様なサービスを提供しています。Akamai が運用するそれらすべてのサービスのうち、権威 DNS は他のサービスの運用のために重要ではありますが、全体的なトラフィックの観点では小規模なものにとどまっています。そのため、以下に示すように、Edge DNS は必要に応じて利用可能なキャパシティーをいくつかの手段で補充できます。

- **CDN からキャパシティーを借用** – 多くの場合、Edge DNS は、Akamai CDN 上で稼働する他の Akamai サービスが所属するサーバーと同じ Points of Presence 内にネームサーバーを展開しています。これらの Points of Presence は、かなり大きな帯域幅を消費するサービスに対応できる設計となっているため、多くの場合、非常に大きな容量を備えています。また、このような余力のおかげで、Akamai は必要な時に CDN から柔軟にキャパシティーを借りることができます。大規模な DDoS 攻撃を吸収できるようにするため、ほかのサービスは他の Points of Presence 経由で迂回させ、共有するネットワークキャパシティーを Edge DNS だけが使えるようにすることも可能です。
- **専用の緩和キャパシティー** – Akamai は、権威 DNS と CDN に加え、これらとは別に、専用の緩和キャパシティーと機能を備えた DDoS 防御サービスを運用しています。大規模な DDoS 攻撃を緩和する必要がある場合、その専用キャパシティーと DDoS 緩和ツールを活用するために、Akamai は個々のネームサーバーの身代わりを Prolexic スクラビングセンターで割り当てることができます。これにより、Edge DNS の外側にある Prolexic プラットフォームの DDoS 緩和容量が効果的に提供され、Edge DNS はエンドユーザーからの正当なクエリーに応答するためのリソースを維持できます。

複数の DNS ベンダー

Edge DNS は、多くの競合サービスの何倍もの規模の権威 DNS サービスを提供し、多数のセグメント化された IP Anycast クラウドで構成されたアーキテクチャにより耐障害性にも優れています。また、DDoS 攻撃から保護するために他の Akamai サービスのキャパシティーと機能を追加で活用することも可能です。これらのメリットに加え、Edge DNS は、組織の唯一の権威 DNS プロバイダーとして機能するために必要な可用性と耐障害性を提供することもできます。ただし、組織によっては、既存のソリューションと並行して Edge DNS を利用する場合もあります。マルチベンダー構成の場合、組織は既存の DNS レコード管理方法を維持しながら、Edge DNS による追加の可用性と耐障害性でプライマリー DNS ソリューションを補うことができます。

展開オプション

マルチベンダー環境で利用できるようにするため、Edge DNS は、以下に示すいくつかのオプションをサポートしています。

- **従来のセカンダリー** – すでに DNS プロバイダーを利用している組織は、既存の DNS ソリューションを補助するセカンダリーサービスとして Edge DNS を展開できます。このような組織は、引き続きプライマリープロバイダーを使用して DNS レコードを管理し、ゾーン転送または Edge DNS API を使用して Edge DNS を自動的に更新します。プライマリーソリューションとセカンダリーソリューションの両方がエンドユーザーからのクエリーに応答することができるため、さらなる可用性を提供します。
- **隠しマスター** – 社内の DNS ソリューションで DNS レコードの管理を継続することを希望する組織には、このオプションを推奨します。この隠しマスター方式では、Edge DNS は（唯一のセカンダリー DNS プロバイダーとして、または複数のプロバイダーの 1 つとして）、DDoS 攻撃に内部ソリューションを公開することなく、エンドユーザーのクエリーに応答できます。このような組織は、引き続きプライマリープロバイダーを使用して DNS レコードを管理し、ゾーン転送または Edge DNS API を使用して Edge DNS を自動的に更新します。
- **デュアルプライマリー** – 隠しマスターの考え方を少し変化させたものです。一部のクラウド・サービス・プロバイダーでは従来のゾーン転送機能の採用が廃止され、ゾーンレコードの変更にはそのプロバイダーの API や他のユーザーインタフェースを使用することがお客様に求められています。Edge DNS をプライマリーモードに設定し、Edge DNS クラウドを権威 DNS として追加すれば、このような手法に Edge DNS を活用できます。

セカンダリーとしての可用性の維持

セカンダリー DNS ソリューションとして展開している場合、Edge DNS がエンドユーザーからのクエリーに正確に応答するためには、プライマリー DNS ソリューションからのゾーン更新に頼らざるをえません。ゾーンファイルは一般的に、権威の開始（SOA）レコードにある有効期限のフィールドで管理される Time-to-Live（TTL）の期間について、セカンダリー DNS ソリューション上での有効性を維持します。プライマリーソリューションの停止の原因となる DDoS 攻撃は、停止期間が TTL 値を超えると、セカンダリーソリューションがクエリーへの応答を停止する原因ともなる可能性があります。この状況に対応するため、Edge DNS は、（1）TTL の有効期限が切れた後もゾーンファイルを保持し、（2）DNS レジストリが Edge DNS を指している限り DNS クエリーへの応答を継続します。その結果、プライマリーソリューションが使用できない場合でも、セカンダリー DNS ソリューションとしてさらなる可用性を提供することができます。

結論

現在、既知の最大規模の DDoS 攻撃は、ピーク時の帯域幅が 1 Tbps を超えています。この規模では、クラウドベースのサービスが使用できる総帯域幅を計算し、そのような攻撃に対する耐障害性の正確な指標を提供することは、もはや不可能です。また、小規模な攻撃でさえも地域レベルでの停止の原因となる可能性があります。Edge DNS は、お客様に 100% の可用性を提供するために、以下のような多層的なアプローチを採用しています。

- 世界各地に拠点を置き（ネームサーバー、Point of Presence など）、多くの競合サービスの何倍にも相当する膨大な規模を備える
- 耐障害性に優れたアーキテクチャ – セグメント化された多数の IP Anycast クラウドにより、攻撃の影響を隔離し、他のお客様やプラットフォーム全体への巻き添え被害を防ぐ
- DDoS 制御の展開能力や必要に応じてお客様の委任を再割り当てする機能など、DDoS 攻撃への対応を適切に管理する
- Akamai CDN や Prolexic DDoS 防御など、他の Akamai サービスを活用してキャパシティーを補充することで、どのような規模の DDoS 攻撃にも対応できるようにする

権威 DNS は、世界中のエンドユーザーを組織のオンラインプレゼンスに接続するミッションクリティカルなサービスです。Edge DNS は、単一の権威 DNS プロバイダーとして利用しても、また既存の DNS ソリューションと併用しても、Web サイトや他のインターネット接続アプリケーションへのグローバルなアクセスを維持するために必要な可用性を提供できます。