AKAMAI ホワイトペーパー

DDoS 攻撃に対抗する可用性と耐障害性のための DNS 設計

Akamai
FASTER FORWARD

はじめに

Fast 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、そのウェブ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、処理能力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する Fast DNS を設計しました。この Fast DNS は、他に類を見ないほどの世界規模、セグメント化された IP Anycast アーキテクチャ、必要に応じて他の Akamai サービスを活用することのできる能力など、数々の DDoS 制御を備えています。Fast DNS は Managed DNS サービスとして提供され、組織とエンドユーザーを常に接続するために、処理能力と可用性の最適な組み合わせを提供します。

統計データに関する注意事項

Akamai が Fast 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。

プラットフォーム統計データ

- 何千ものネームサーバー
- 何百もの Point of Presence（POP）
- 90 都市
- 32 ヵ国
- 87 のネットワーク

Akamai は、セキュリティ上の理由により、ネームサーバーの数、または Point Of Presence（POP）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、Fast 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 POP の数、またはネットワークの総容量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には不十分です。従来から処理能力だけに焦点を合わせている他の DNS とは異なり、Akamai は、処理能力に加えて、ネームサーバー、POP、ネットワーク、およびセグメント化された IP Anycast クラウドなどの多層的な構造上の冗長性とともに、DDoS 攻撃に対抗する可用性と耐障害性を特に考慮して Fast DNS を設計しました。

IP Anycast

Fast DNS は、DNS クエリーに応答するために IP Anycast モデルを採用している数百の POP 上に展開された、数千のネームサーバーによって構成されています。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 POP 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 は、1 つの IP アドレスに対して行われるクエリーに対して、異なるネットワーク上にある複数のネームサーバーが応答できるようにします。IP Anycast を活用することにより、Fast DNS は、複数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を向上させます。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 POP 全体をオフラインにすることが可能です。

- **規模 —** 多数の POP にわたる多数の物理サーバーによって構成される Fast DNS インフラストラクチャは、大量の DNS リクエストに応答する際に常に信用できる、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、Fast DNS は他の Akamai サービスとリソースを共有することが多いため、POP のかなりの余剰ネットワークリソースにもアクセスできます。これらの要素により、Fast DNS は、DNS フラッドや他の形態の DDoS 攻撃に対応する規模を、スタンドアロン DNS サービスよりもさらに多く使用できます。

- **分散 —** IP Anycast は、規模の拡大を可能にするだけでなく、Fast DNS が複数の POP 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 POP 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 を利用しても、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にし、それらのユーザーが接続するすべてのウェブサイトの可用性に影響が及ぼされる可能性があります。

Fast 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、Fast DNS はネームサーバーと POP を複数の IP Anycast クラウドに分割します。Fast DNS クラウドは、専用のネームサーバーと POP とともに、関連するネットワーク容量と接続性で構成されています。すべてのクラウドはそれぞれ独立して機能するため、Fast DNS は可用性、規模、分散性の観点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。

Fast 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 箇所以上に分散された POP を内包し、各 POP 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。その代わりに、小規模な POP は、コンピュータリソースとネットワーク容量が少ないため、DDoS 攻撃への耐障害性が本質的に低くなります。

- **可用性 —** Fast 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 POP 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容量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 POP を追加します。

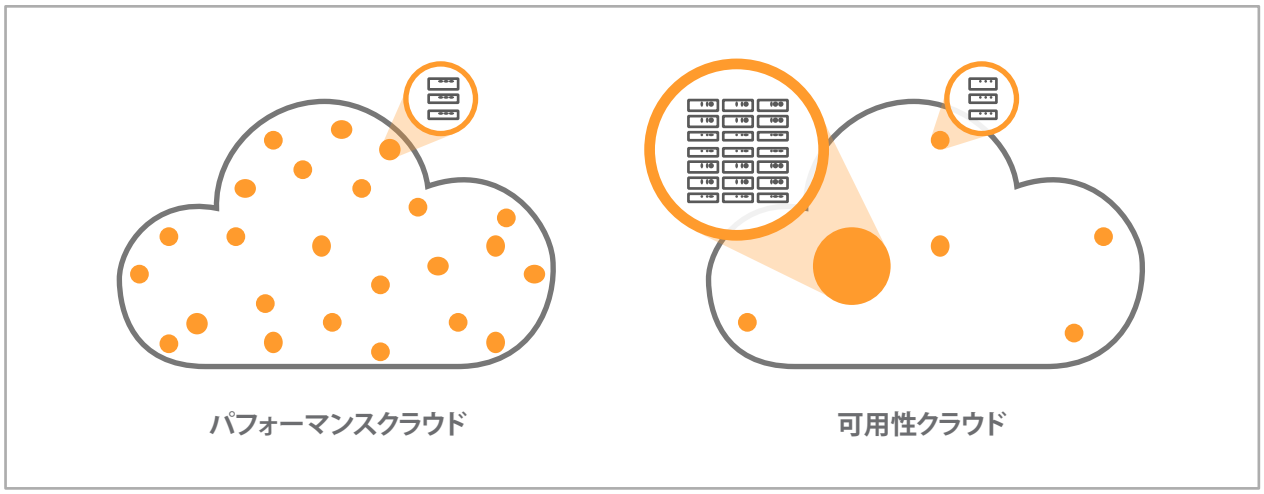

図 1：Fast DNS は、さまざまなアーキテクチャに複数の DNS クラウドを組み合わせて、DDoS 攻撃に対抗するパフォーマンス、可用性、および耐障害性の最適な組み合わせを提供します。

セグメント化されたアーキテクチャ

Fast 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比較して、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。

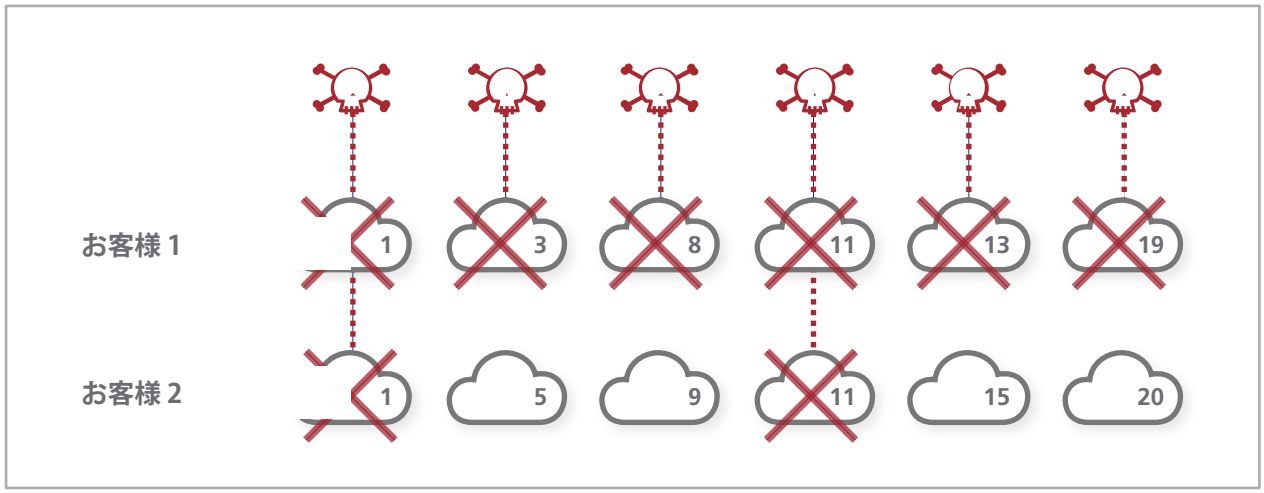

図 2： Fast DNS のすべてのお客様は、パフォーマンスクラウドと可用性クラウドの固有の組み合わせという形でネームサーバーのサービスをうけることで、他のお客様に対する構成からの巻き添え被害を最小限に抑えます。

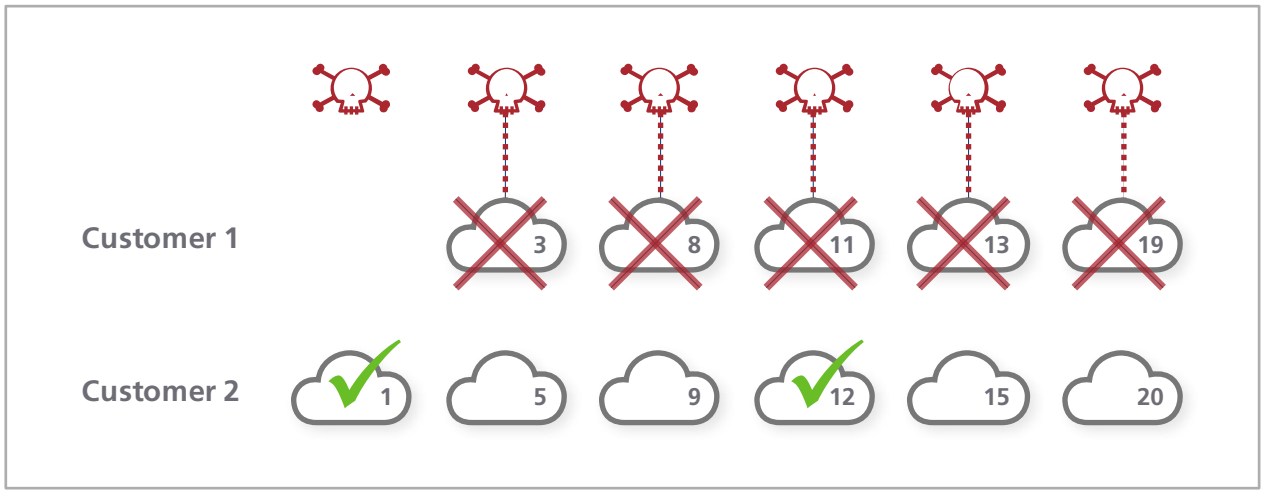

図 3：Akamai は、攻撃対象のお客様を個別のクラウドから移動させたり、攻撃対象外のお客様の重複を最小限に抑えたりするなど、ネームサーバーの身代わりを管理することで、攻撃による影響をさらに最小化することができます（上記の図 2 と比較して）。

多数かつ多様な IP Anycast クラウドによって、Fast DNS は 1 つ以上のクラウドを失っても機能し続けることができます。そのため、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ことで、大規模な DDoS 攻撃の影響さえも緩和するために、プラットフォーム全体のサブセクションでトラフィックをセグメント化することが可能になります。例えば、単一の Fast DNS IP Anycast クラウドに対する攻撃は、特定のクラウドを構成する物理的なネームサーバーと POP に誘導されます。セグメント化されたアーキテクチャは、その影響を他の IP Anycast クラウドから分離し、個別のクラウドまたはお客様が DDoS 攻撃を受けていても、Fast DNS がすべての地域でプラットフォームの可用性を維持できるようにします。

Fast DNS のセグメント化されたアーキテクチャは、プラットフォーム全体の耐障害性を向上させることに加えて、あるお客様が使用するネームサーバーが攻撃されている場合に、その他の個々のお客様への巻き添え被害のリスクも緩和します。Fast DNS は、すべてのお客様に複数の Fast DNS クラウドを、他のお客様と共有することのない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で割り当てます。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 つの組織に対する複数の DDoS 攻撃は長期間にわたって行われることが多く、Akamai はこれまでに、広範で数か月以上にわたる持続的な攻撃活動を確認してきました。このような状況において、Fast DNS のセグメント化されたアーキテクチャは、攻撃の対象とされていないお客様への影響を Akamai がさらに最小化する際に、優れた柔軟性を提供します。図 3 に示すように、Akamai は個々のお客様のクラウドを再割り当てし、必要に応じて攻撃による影響をさらに分離します。

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 —** Fast 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。その結果、あるお客様のすべての Fast DNS クラウドを標的とする攻撃は、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、持続的な攻撃に対しては、Akamai が攻撃対象のお客様の IP Anycast を再割り当てし、攻撃対象でないお客様の可用性を復元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 —** Fast DNS の複数のお客様が、通常よりも多くの Fast DNS クラウドを共有する場合があります。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、攻撃対象のお客様との共有を削減または除外するために攻撃対象ではないお客様のクラウドを再割り当てして、攻撃対象ではないお客様のエンドユーザーのため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。Fast DNS クラウドの多様な拠点によって、さまざまなネットワーク間のトラフィックをいっそうセグメント化することができ、異なる状況における可用性を最大限に高めることができます。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慮した場合、ネットワーク接続の多様性は、容量と同じくらい重要になる可能性があります。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。攻撃を受けている間でも可用性とエンドユーザーからの DNS クエリーに対応する能力を維持するために、Fast DNS はネームサーバーを、大容量であるだけでなく、複数のネットワークを介する接続を備えた大規模なデータセンターに展開します。

- **ISP の分離 —** 多くの場合、Fast DNS はネームサーバー群を個別の 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、その 1 つのクラウドを保護するのに使用可能な容量は、通常、十分にあります。

- **ネットワークの多様性 —** お客様には、多様なクラウドが意図的に割り当てられます。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。このアーキテクチャは、再帰ネームサーバーである既定のクライアントが、使用可能な Fast DNS クラウドに常に接続できるようにします。

- **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 以外のさまざまなサービスを運用することで、複数のサービスをサポートするデータセンターに Fast DNS ネームサーバーを展開することができます。後に詳述しますが、これによって、大規模な DDoS 攻撃に対応する際に、Fast DNS が大量のネットワーク容量にアクセスできるようになります。パブリックピアリング調整も、専用のネットワーク容量も、どちらも Akamai が他のサービスのためにすでに用意しているものです。

DDoS 制御

Fast DNS にはアーキテクチャ設計だけでなく、DDoS 攻撃のカテゴリーの 1 つである DNS フラッドと呼ばれる攻撃の影響緩和に役立つ制御機能がいくつか含まれています。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、以下に示すいくつかの方法によって、DNS フラッドから Fast 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 ソリューションの数倍あります。Fast DNS は、世界中の何百もの POP に展開されている何千ものネームサーバーを活用します。DDoS 制御に限定されたことではありませんが、IP Anycast が攻撃トラフィックを地域およびネットワークにわたって分散し、その一方で物理ネームサーバーが Fast DNS に DNS リクエストの急激な増加を吸収するのに必要な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提供します。

- **Rate Limiting —** Fast DNS には、Rate Limiting 機能が含まれているため、リクエストの量が設定したしきい値を超えた場合、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。Fast DNS の Rate Limiting 機能は、その Fast DNS プラットフォームに固有のアルゴリズムを使用するため、お客様による設定はできない点に注意してください。

- **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から、インターネット上での正規の DNS ルックアップの約 95% に対応する再帰リゾルバの動作に対して、独自の可視性を持っています。Fast 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 リゾルバのリストに制限します。

容量関連

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。2016 年はネットワーク層攻撃のリスクが劇的に増加し、既知の最大規模の攻撃ではピーク時の帯域幅が 1 Tbps を超えていました。

Akamai では、計測可能な指標を攻撃者に提供することを避けるため、Fast DNS プラットフォームの容量を公表していませんが、プラットフォーム規模のあらゆる面に対して投資を続け、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するために Fast DNS 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・プロバイダーとして、サーバーを再利用し、DNS 用の容量を新しい地域に迅速に展開する能力を備えています。Akamai はトラフィックの急増を吸収する大量の使用可能リソースを保持しており、Fast 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。Fast 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

高帯域幅の DDoS 攻撃に耐える能力を、ネットワーク容量を使用して見積もる従来の方法は、Fast DNS には通用しません。その第一の理由は、Fast DNS は他の Akamai プラットフォームのリソースを活用できるためです。Akamai は単なる DNS 企業ではなく、Fast DNS 以外の多くのサービスを運用しています。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、必要に応じて Fast DNS が使用できる容量を補充する機会がいくつか提供されます。

- **CDN から容量を借用する —** 多くの場合、Fast 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 POP 内にネームサーバーを展開しています。これらの POP は、かなり高い帯域幅を消費するサービスに対応するように設計されているため、多くの場合、非常に大規模です。また、これらは Akamai の他のサービスを他の Point of Presence サービス経由で迂回させ、大規模な DDoS 攻撃を吸収できるように Fast DNS だけが使用できる共有ネットワーク容量を作り出すことができるため、必要な際に CDN の容量を借用するための運用上の柔軟性が Akamai にもたらされます。

- **専用の緩和容量を展開する —** Akamai は、権威 DNS と CDN に加え、専用の緩和容量と機能を備えた DDoS 防御サービスを別個に運用しています。大規模な DDoS 攻撃を緩和する必要がある場合、その専用容量と 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、Fast DNS の外側にある Prolexic プラットフォームの DDoS 緩和機能が効果的に展開され、エンドユーザーからの正規のクエリーに応答するための Fast DNS のリソースを維持します。

複数の DNS ベンダー

Fast 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、多数のセグメント化された IP Anycast クラウドを備えた耐障害性に優れたアーキテクチャ、DDoS 攻撃から保護するために他の Akamai サービスの容量と機能を追加して活用する能力を提供します。Fast DNS はこれらのメリットとともに、組織の単一の権威 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します。ただし、一部の組織では既存のソリューションと並行して Fast DNS を展開することを選ぶかもしれません。複数ベンダーによる展開では、Fast DNS による追加の可用性と耐障害性を使用してプライマリー DNS ソリューションを補いながら、既存の DNS レコード管理手法を維持することが可能です。

展開オプション

Fast DNS では、Fast DNS をマルチベンダー環境に展開するために、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 —** 既存の DNS プロバイダーがある組織は、Fast DNS を既存の DNS ソリューションを補助するためのセカンダリーサービスとして展開できます。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 Akamai {OPEN} API を使用して Fast 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、この導入オプションを推奨します。この隠しマスター形態は、DDoS 攻撃に内部ソリューションを公開することなく、Fast DNS（単一のセカンダリー DNS プロバイダーとして、または複数のうちの 1 つとして）がエンドユーザーのクエリーに応答することが可能です。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 Akamai {OPEN} API を使用して Fast DNS を自動的に更新します。

- **デュアルプライマリー —** 隠しマスター概念の変形型です。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。Fast DNS は、プライマリーモードに設定し、Fast DNS クラウドを権威 DNS として追加することで、このような手法でも活用することができます。

注：Fast DNS の一部の詳細機能には、特定の導入オプションとの互換性がない場合があります。例えば、DNSSEC のサポートには特殊な考慮事項が必要となります。

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た場合、Fast DNS はエンドユーザーからのクエリーに正確に応答できるようプライマリー DNS ソリューションからのゾーン更新に依存しています。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）の期間に基づいて、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。Fast DNS は、(i) TTL の有効期限が切れた後もゾーンファイルを保持する、(ii) DNS レジストリが Fast DNS を指している限り DNS クエリーへの応答を継続することで、このような状況から保護します。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

現在の既知の最大規模の 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。Fast DNS は、お客様に対して 100% の可用性を提供するために、可用性に対して以下を組み合わせた多層的な手法を採用しています。

- 多くの競合サービスよりも数倍もの規模を備えた、ネームサーバーや POP などの海外拠点による膨大な規模
- 攻撃の影響を分離し、他の顧客とプラットフォーム全体への巻き添え被害を防ぐ、多数の分割された IP Anycast クラウドを備えた耐障害性に優れたアーキテクチャ
- DDoS 制御を展開する能力や、必要に応じてお客様の身代わりを再割り当てする能力など、DDoS 攻撃への対応の管理
- Akamai CDN や Prolexic DDoS 防御などの他の Akamai サービスを活用し、容量を補充して大規模な DDoS 攻撃にも小規模な DDoS 攻撃にも対抗する能力

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。単一の権威 DNS プロバイダーとして展開するか、既存の DNS ソリューションと並行して展開するかにかかわらず、Fast DNS は、組織のウェブ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のに必要な可用性を組織に提供します。