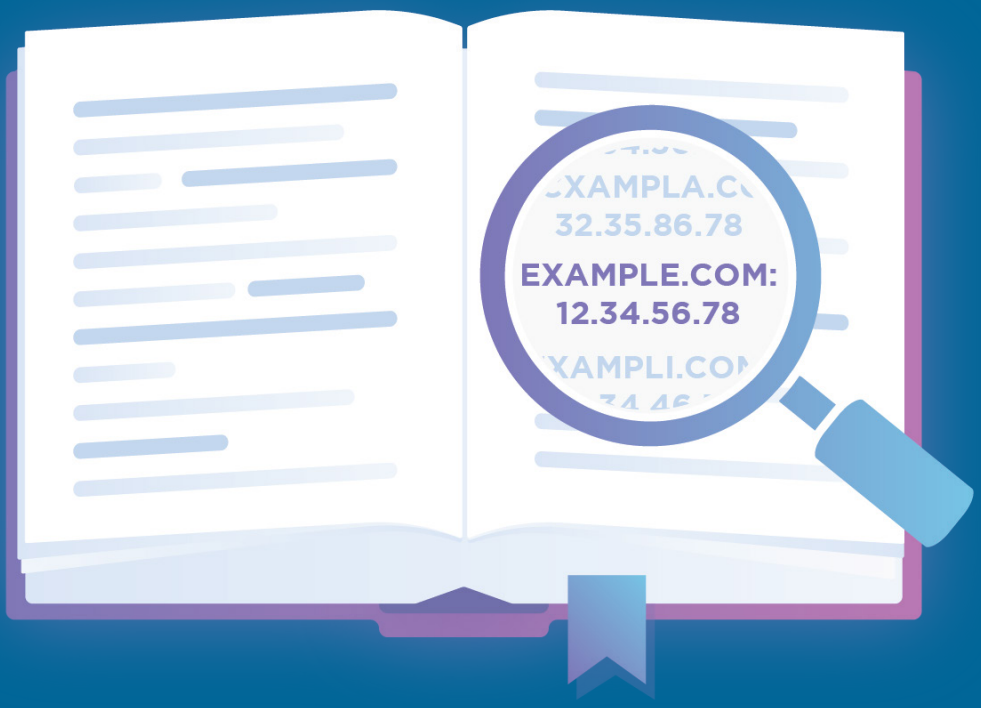
CLOUDFLARE®

DNSを活用して信頼性の高いデジタル体験を構築



enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE

I. エグゼクティブサマリー

Webサイトの速度はDNSの速さ次第です。サイト構築のしかたやホスト場所には関係ありません。

DNSを適切に実装して使えば、インターネットプロパティのセキュリティ、パフォーマンス、信頼性を大幅に改善できます。しかし、パフォーマンスを低下させたり、DNSサーバーを完全にダウンさせる恐れのある多様なサイバー攻撃が増えているにもかかわらず、DNSインフラストラクチャはそうした攻撃に対して非常に脆弱です。Webサイトのパフォーマンスと可用性に関するユーザーの期待が高まる中、攻撃によってDNSが単一障害点になるリスクがあります。

堅牢なサイトセキュリティ、パフォーマンス、信頼性を実現するには、統合型のDNSセキュリティとパフォーマンスを高めるために最適化された冗長性のあるDNSインフラストラクチャが必要です。

II. DNSのセキュリティ：企業のサイバーセキュリティの弱点

現在使用されているDNSインフラストラクチャは、インターネットアクセスが政府機関、科学者、軍部用に制限されていた1980年代に設計されたものです。システムのアーキテクトはセキュリティではなく、信頼性と機能性に重点を置いていました。[1]

その結果、現代世界のDNSサーバーは、スプーフィング、マルウェア、DNSトンネリング、DoS/DDoS攻撃など広範な攻撃タイプに対して脆弱です。こうした攻撃は発生頻度が増し、それに伴うコストも高額化しています。IDCの2019年版『Global DNS Threat』レポートでは、次のように報告されています。

- 組織の82%が過去2年間にDNS攻撃の被害にあった
- 帯域幅消費型から低シグナルまで、あらゆるタイプの攻撃が前年に比べ大幅に増加
- 攻撃1件あたりの平均コストは2019年に100万ドルを突破、前年比では49%アップ[2]

DNS攻撃は他のサイバー攻撃と同時に仕掛けられることが多く、セキュリティ担当者の注意をそらすための煙幕として使われることもしばしばです。Verizonの推定では、データ漏洩の約3分の1にDNS攻撃が関わっているといいます。[3]

セキュリティのためにDNSを最適化

DNSへの脅威は多種多様で、攻撃を効果的に軽減するには、以下を含めた統合型セキュリティ戦略が必要です：

- **DNSSECを有効化** DNSSECは暗号署名を使ってDNSレコードを検証する一連のセキュリティプロトコルです。サイトの署名がレコードと一致することを確認することによって、DNSリゾルバーはDNSサーバーから送られてきたデータの送信元を認証し、スプーフィングを防止します。

- **多層DDoS軽減を実装** レート制限、IPアドレスのホワイトリストやブラックリスト、接続追跡などでトラフィックをフィルタリングし、悪性リクエストをブロックしながら正規トラフィックを流します。DDoS攻撃の軽減は、セキュリティを強化するだけでなく、悪性トラフィックでDNSサーバーが過負荷になることを防いで信頼性とパフォーマンスも高めます。

- **DNSファイアウォールをデプロイ**（DNSフィルタリングとDNSブロッキングとも言います）これにより、既知の悪性ドメインからのアクセスをブロックします。

- **DNSロギングを有効化** DNSロギングは、ハッカーがDNSサーバーを改ざんしようとしている場合に警告し、DNSクエリや更新の問題を可視化します。

- **HTTPSを強制** Webサイトを常にHTTPSで読み込むようブラウザーに要求し、各サイトをSSL/TLS証明書で認証することによって、ドメインスプーフィングを防止します。

- **DNSサーバーを常時更新** 更新はしばしば重要なセキュリティパッチを含みます。

III. DNSのパフォーマンス：DNSルックアップが遅いと高遅延に

ユーザーがWebアセットにアクセスすると、デバイスはそのアセットのドメイン名をIPアドレスにマップするDNSリゾルバーに問い合わせた後、正しいIPアドレスをデバイスに返信します。ユーザーがブラウザーで新しいページにアクセスするたびに、少なくとも1度はDNSルックアップを行う必要があります。多くのページでは複数ドメインからアセットを読み込むため、数回のルックアップが必要になります。このプロセスはDNS解決と呼ばれ、リクエストされた各ドメインの解決に必要な時間はすぐに蓄積していきます。そのため、遅延を低く抑えるためにはDNS解決の速度を最適化することが重要なのです。

解決の速度を上げるための最適化がどのDNSプロバイダーでも行われているわけではありません。遅いDNSプロバイダーでは各DNSクエリーの解決に、120ミリ秒以上かかることもあります。[4] 最速のDNSプロバイダーはクエリーを20ミリ秒以内に解決します。たとえば、Cloudflare DNSは平均で12ミリ秒未満でクエリーを解決します。[5]

- 現代のWebユーザーは、デジタルアセットがたちどころに読み込まれることを望んでいます。ささいな問題であってもエンゲージメントやコンバージョン率に大きく影響しかねません。
- サイトの遅延がわずか100～400ミリ秒増えるだけでも、消費者行動に測定可能な影響を与えます。[6]
- 読み込み時間が1秒増えるだけでコンバージョン率が7%低下します[7]
- モバイルユーザーの約半数はアプリケーションが2秒以内に応答することを期待しています[8]
- Googleは、デスクトップとモバイル検索の両方でランキング要素にページ速度を採用しています[9]

パフォーマンスのためにDNSを最適化

ミリ秒単位の差が影響するマーケットプレースで優れたパフォーマンスを確保するために実行できることがいくつかあります。

- **グローバルなジオロケーションに基づくルーティングを使用** エンドユーザーとデジタルリソースの間が100マイル離れるごとに、約0.82ミリ秒の遅延が生じます。[10] そのため、訪問者を所在地域のDNSインフラストラクチャへジオステアリングすることが重要なのです。
- **最適なTime to Live（TTL）を見極め** TTLはDNSリゾルバーのキャッシングに間接的に影響します。低いTTLはパフォーマンスを悪化させますが、DNSベースの負荷分散に一役買う場合もあります。高いTTLはパフォーマンスを改善しますが、ダウンしてしまったキャッシュサーバーへユーザーをダイレクトする可能性があります。数多くの要素が関わっているため、万能の最適TTL値は存在しません。
- **エニーキャストを使用** エニーキャストを使用するDNSプロバイダーを探しましょう。エニーキャストは、世界中に分散された複数のDNSネームサーバーが同じIPアドレスをアドバタイズできるようにします。これによってDNS解決の速度が上がり、シームレスなDNSフェイルオーバー保護が提供されます。

DNSをネットワークエッジに移動する

11ミリ秒
平均的なDNS検索速度

5秒未満
で全世界にDNS伝播

IV. DNSの信頼性：冗長性がダウンタイムを回避する

遅延の問題は、放っておくとWebサイトが突然ダウンするという最悪のシナリオを引き起こします。ダウンタイムのコストは莫大で、着実に増大しています。データセンターが停止した場合の1分あたりの平均コストは、2010年には5,617ドルでしたが、2016年には8,851ドルまで上がっています。[11]

DNSの信頼性は会社の利益に直接かつ多大な影響を及ぼすため、どんな企業でも稼働率100%を目指さなければなりません。現実的でないように聞こえるかもしれませんが、企業が冗長性を重視した複数の対策で取り組めば不可能ではありません。

信頼性を確保するためのDNSの最適化

パフォーマンスと信頼性は頭と首のように密接につながっていて、一方がなければ他方は存在し得ません。信頼性を高めるために実行する対策のすべてが、パフォーマンスの強化につながります。たとえば、2つのDNSプロバイダーを利用すればページ読み込み時間が改善されます。これは、デフォルトでネームサーバーの解決が最速のDNSプロバイダーにより実行されるためです。

- **デュアル（プライマリ/セカンダリ）DNSプロバイダー** 単一プロバイダーのDNS設定では、全ユーザーがそのプロバイダーのネームサーバーセットから応答を受け取りますので、プロバイダー側の障害に対して脆弱になります。2つ目のDNSプロバイダーを追加することで、ドメインに使用できるネームサーバーセット数が倍増します。権威DNSプロバイダーが使えない場合は、クエリトラフィックはバックアップネームサーバーセットへ自動的にルーティングされます。
- **クラウドベースのDNS** 自社のDNSサーバーを管理できるだけの社内リソースや専門知識を持つ企業は、ほとんどありません。クラウドベースのDNSプロバイダーへアウトソーシングすれば、パフォーマンス、信頼性、セキュリティを強化し、コストを最小化し、社内のIT担当者を社内プロジェクトに回すことができます。
- **ネームサーバーのセグメンテーション** プロバイダーによっては、多数の顧客あるいは全顧客を同じネームサーバーレコードに集約している場合があります。顧客の一企業がDDoS攻撃に遭うと、そのネームサーバーを利用する他の企業も深刻な影響を受けます。ご利用のDNSプロバイダーがネットワークをセグメント化し、少数の顧客だけがネームサーバーレコードを共用するようになっていることを確認しましょう。
- **巨大なグローバルDNSノードネットワーク** ご利用のプロバイダーのDNSネットワークには、世界中に分散されたDNSノードが大量にあるべきです。1つのノードが故障すれば、トラフィックは残りのノードのいずれかへルーティングされます。グローバルネットワークでは、パフォーマンスを向上するジオステアリングも可能です。
- **グローバルとローカルの負荷分散** サーバーが過負荷にならないようにするだけでなく、1台のサーバーで障害が発生すると、ロードバランサーがトラフィックを別のサーバーにリダイレクトします。

V. 結論

動きの速い現在のデジタルマーケットプレースでは、数ミリ秒の読み込み時間の差がユーザーエクスペリエンスとコンバージョン率の良し悪しを左右します。Webサイトのパフォーマンスと信頼性は、DNSの解決速度によって決まりますが、DNSサーバーは広範なサイバー攻撃に対してあまりにも脆弱です。安全性と高パフォーマンス、稼働率100%を確保できるDNSインフラストラクチャを実現するには、セキュリティ、信頼性、パフォーマンスに対し統合されたアプローチが不可欠です。

VI. Cloudflareのサービス

Cloudflareは、本書で触れてきたベストプラクティスの多くを取り入れたエンタープライズグレードの権威DNSサービスを提供し、最速の応答時間、突出した冗長性、DDoS軽減とDNSSECを内蔵した高度なセキュリティを実現します。詳細情報や当社チームメンバーへのお問い合わせをご希望の方は、www.cloudflare.com/dns/をご覧ください。

巻末注

1. ICANN, “DNSSEC - What Is It and Why Is It Important?” https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en. 2020年1月27日にアクセス
2. IDC, “2019 Global DNS Threat Report,” https://www.efficientip.com/resources/idc-dns-threat-report-2019/. 2020年1月26日にアクセス
3. Global Cyber Alliance, “The Economic Value of DNS Security,” https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. 2020年1月27日にアクセス
4. Mann, Bill. “The Best DNS Servers for Speed and Privacy in 2019.” Blokt, https://blokt.com/guides/best-dns-servers. 2020年1月27日にアクセス
5. “DNS Performance Analytics and Comparison.” DNSPerf, https://www.dnsperf.com/. 2019年7月23日にアクセス
6. Brutlag, Jake. “Speed Matters,” Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. 2020年1月27日にアクセス
7. Rodman, Tedd. “Marketing & Web Performance: How Site Speed Impacts Metrics,” Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. 2020年1月27日にアクセス
8. Dimensional Research. “Failing to Meet Mobile App User Expectations: A Mobile App User Survey,” https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. 2020年1月27日にアクセス
9. “Using page speed in mobile search ranking,” Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. 2020年1月27日にアクセス
10. Sherman, Fraser. “Network Latency Milliseconds Per Mile,” Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile/ 2020年1月27日にアクセス
11. Priceonomics Data Studio. “Quantifying the Staggering Cost of IT Outages,” https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. 2020年1月27日にアクセス