CLOUDFLARE

電子書籍

ダウンタイムの防止：DDoS防御モデルガイド

本文

クリックしてセクションに飛びます

はじめに：ハイブリッドワークの世界におけるDDoS防御

平均的な企業は、現在、1,400を超える異なるクラウドサービスを使用しています[1]—これは、より優れた、より高速なアプリケーションとカスタマーエクスペリエンスに対する需要の高まりに牽引されています。しかし、クラウドトランスフォーメーションの副産物は、以下に挙げる攻撃対象領域の拡大です：デジタルサービスがより増えるということは、攻撃者が悪用する「エントリーポイント」もより増えるということです。攻撃対象領域も、ハイブリッドワーク（オフィス内勤務とリモートワークの組み合わせ）で拡大してきました。—ハイブリッドワークは何年もの世界的なパンデミックに伴い必然的に生じたのです。

これらのすべての要因は、リソースに乏しい企業への圧力を増大させています。ITチームとセキュリティチームは、より回復力のあるアプリケーションとネットワークを提供する必要があるだけでなく、場所に関係なく、進化する脅威からユーザーとデバイスを保護する必要もあります。

これらの脅威の一部には、より頻繁かつ長期にわたるより大規模な分散サービス妨害（DDoS）攻撃が含まれます。2023年2月、Cloudflareは過去最大のHTTPS DDoS攻撃（71 Mrps）を検出し、軽減しました。また、当社のデータは、2022年に大容量のDDoS攻撃（100 Gbpsを超える攻撃）が前四半期比で増加していることを示しています。

今日の経済とハイブリッドワークの現状により、企業はDDoS防御を再評価する必要があります：
ダウンタイム、データ窃盗、ネットワーク侵入、財務損失のリスクが大きすぎます。

調査によると、60%を超える障害で10万ドルを超える費用がかかり、15%の障害で100万ドルを超える費用が発生しています[2]。ある例では、一連のDDoS攻撃によるダウンタイムにより、ある企業は1,200万ドル近くの損失を被りました[3]。

こうした現実により、DDoS防御はあらゆる規模の組織にとって非常に重要です。そして、これまでの手動のアプローチではもはや十分ではありません。攻撃を仕掛けるのは人間ですが、実行するのはボットです。勝つためには、ボット同士で戦わせる必要があります。検出と軽減は、可能な限り自動化する必要があります。

この電子書籍は、以下の内容を取り上げます：

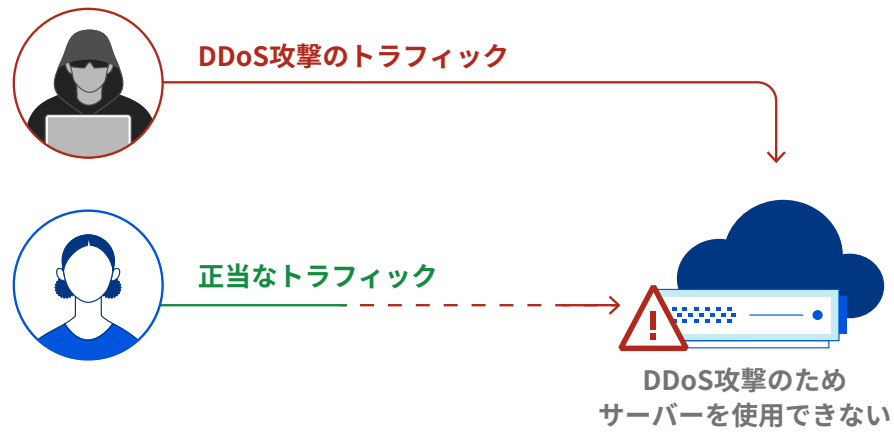
- クラウドベースのDDoS攻撃対策のさまざまなモデル
- 常時接続のクラウドスクラビングの制限を克服
- どのようにフォーチュングローバル500の企業がCloudflareでランサムDDoS攻撃を阻止したのか

クラウドベースのDDoS軽減アプローチの理解

このDDoS攻撃は、インターネットトラフィックの洪水でターゲットまたはその周囲のインフラストラクチャを圧倒することにより、ターゲットのサーバー、サービス、またはネットワークの通常のトラフィックを妨害しようとする悪意のある試みです。効果的なDDoSソリューションは、この「トラフィック渋滞」がいつ、どこで、どのように発生しているかを正確に伝え、悪意のあるトラフィックを吸収して再ルーティングしながら、正当なトラフィックを妨害しないようにします。保護されていないインターネットプロパティとネットワークと相まって、トラフィック量の多い宛先はすべて一般的なターゲットになります。

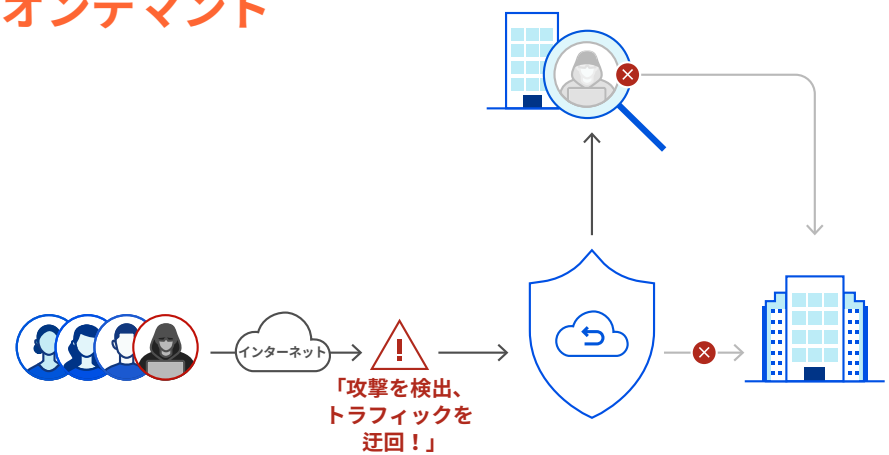
DDoS攻撃は新しいものではありませんが、それを阻止するには新しいアプローチが必要です。アプリケーションのクラウド移行に伴い、オンプレミスのDDoSソリューションの市場も縮小し、[4]代わりに、より多くの組織がDDoS攻撃対策のためにクラウドに目を向けています。

クラウドベースの保護にはさまざまな種類があり、クラウドプロバイダーは、組織のアプリケーションとインフラストラクチャの前に配置され、すべてのトラフィックをスクラビングセンターに転送して「クリーンアップ」します。正当なトラフィックのみがユーザーに送り返されます。この「クラウドスクラビング」モーションは、次の***オンデマンド***または***常時接続***のいずれかの方法で有効にできます。



**正当なユーザーへのサービスを拒否する
アプリケーション層DDoS攻撃の図**

オンデマンド

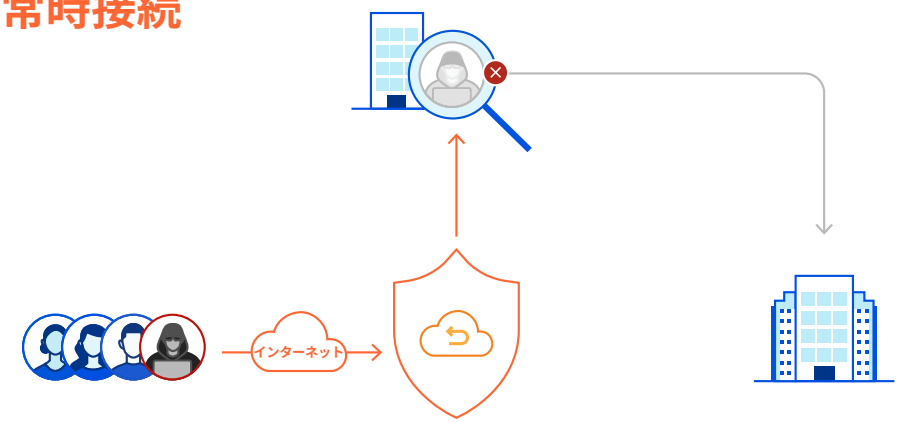


「平時」には、オンデマンドのクラウドスクラビングにより、すべてのトラフィックがリダイレクトされずに、確実にアプリケーションとインフラストラクチャに到達します。アクティブなDDoS攻撃の状況では、トラフィックは、クラウドスクラビングプロバイダーに転送されます。

インバウンドトラフィックが事前に設定されたしきい値（例えば、リンク容量の70%）を超える場合、または大規模な攻撃が検出された場合、オンデマンドのクラウド軽減モードが有効になり、トラフィックは処理のために最も近いスクラビングセンターに転送されます。

VS

常時接続



この人の手を基本的に介さないクラウドスクラビングへのアプローチは、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てトラフィックをルーティングします。

常時接続モデルは、サービスを中断することなく、検出から軽減までの時間を最小限に抑えることができます。

オンデマンドと常時接続の技術は、どちらも異なる利点がありますが、それぞれ、異なる状況において、制限がある場合があります—詳しくは、次のセクションで説明します。

クラウドスクラビング方法の一般的な制限

オンデマンドクラウドスクラビングの課題

攻撃に対する反応の遅れ：

- オンデマンドでは、DDoS攻撃時にクラウドプロバイダーにトラフィックを再ルーティングする必要があります。攻撃に手動で対応する時間に加えて、このネットワークスイッチが行われるまでに数分かかる場合があります（例：サービスをオンにするようにプロバイダーに伝える）。オンデマンド保護が時間内にオンにならない場合、大きな影響を与える可能性があります。

長期的にはコストが増加：

- オンデマンドクラウドプロバイダーは、攻撃のトラフィックのバイトごとに課金することがよくあります。料金は使用した分を支払いますが、組織がDDoS攻撃をより頻繁に経験する場合、結果的に費用が高くなる可能性があります。

潜在的な、すり抜ける攻撃：

- 使用率のしきい値を超えないDDoS攻撃は検出されず、正当なトラフィックに影響を与えるネットワークリンクを混雑させる可能性があります。
- また、ネットワークリンクは、SSLやアプリケーションレベルでの上位レイヤープロトコル攻撃を監視しません。

常時接続のクラウドスクラビングの課題

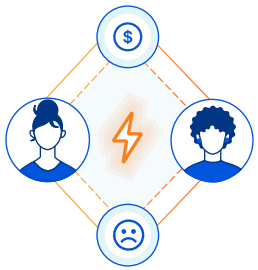
ネガティブなユーザーエクスペリエンスにつながる遅延問題：

- 多くのクラウドDDoS軽減プロバイダーは、攻撃のトラフィックの発信元から遠く離れたネットワークトラフィックのスクラビングに特化した一連の遠隔データセンターを持っています。スクラビングセンターが少ないことは、一般的に、遅延がより大きくなるということです。また、このトラフィックのバックホールは、遅延を発生させ、顕著な遅延を生む可能性があります。
- DDoSスクラビングに特化したデータセンターでは、多くの場合、ネットワークレイヤーのみを検査します。Webアプリケーションファイアウォールやコンテンツキャッシングなど、その他のレイヤー上に存在する機能の場合、このトラフィックは通常、代替データセンターで処理され、さらなる遅延をもたらします。

より高い総所有コスト：

- ネットワーク容量が限られている常時接続のクラウドスクラビングソリューションは、より高い価格という形で、帯域幅の制限を顧客に転嫁する可能性があります。専門サービス料金が上乗せされる場合もあります。

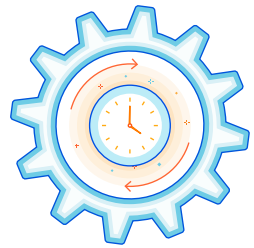
時は金なりの場合：ダウンタイムと遅延がビジネスにどのような影響を与えるのか



組織の91%は、ビジネスの損失、生産性の中断、修復作業により、**1時間あたりのダウンタイムのコストが最大30万ドルに上る**と述べています[5]

遅延を経験した**ゲーマーの44%は、プレイ中のゲームを終了して**後で再試行することで対応します—一方、**24%はゲームを終了して他のゲームをプレイします**[8]

有名なeコマース企業の場合、ダウンタイムは1分あたり最大**220,000ドル**に上る可能性があります[6]



IT部門の意思決定者の64%は、より迅速かつ簡単なカスタマーエクスペリエンスを提供する必要性が**「技術インフラストラクチャにとってかなりの、または大きな負担」だと述べています**[9]

買い物客の90%は、サイトが「適切な時間内に」読み込まれないと**サイトを放棄し、57%はサイトを離れて同じような小売店から購入します**[7]

クラウドベースのDDoS防御の約束を最大限に実現し、ー障害による収益損失を保護

インテリジェントなグローバルネットワークを搭載した統合クラウドプラットフォームがDDoSの脅威からどのように保護するのかを次に示します。

オンデマンドのクラウドスクラビングは人間の介入に依存するため、軽減への対応に時間がかかります。その一方、常時接続のクラウドDDoS攻撃対策はより包括的です—しかし、常時接続のクラウドDDoSベンダーの多くは、ユーザーエクスペリエンスに遅延をもたらす遠隔のスクラビングセンターに依存しています。

Cloudflareは、統合セキュリティプラットフォームでこれらの制限に対処します—これには、DDoS攻撃対策の3つのレイヤー（レイヤー3、4、および7）と、オンプレミス、クラウドホスト型、およびハイブリッドネットワークのトラフィックアクセラレーションが含まれます。攻撃トラフィックはソースの近くで軽減されるため、エンドユーザーはシームレスで高性能なエクスペリエンスが得られます。

ネットワーク利用のセキュリティ

Cloudflareは**197 Tbpsのネットワーク容量**を持つ**データセンターを285を超える都市に展開しています**（その一方、ある有名な常時接続のDDoS軽減サービスは、40未満のスクラビングセンターを展開し、20 Tbpsのネットワーク容量となっています）。

攻撃はお客様のネットワークに到達する前に当社のネットワークによって自動的に吸収され、ほとんどの悪意のあるトラフィックは**3秒未満**でブロックされます。バックホーリングは必要ありません。

ユーザビリティ、視認性、セルフサービス

CloudflareのDDoS攻撃対策はサービスとして提供されます。これは、資本的支出への投資やハードウェアのライフサイクル管理は必要ないということです。

さらに、**セルフサービス可能**で、**単一のダッシュボード**にカスタム設定機能を搭載しています。

大規模な脅威インテリジェンス

さらに理解して、さらに保護：Webのほぼ20%がCloudflare上で実行されています。当社のお客様は、当社のグローバルネットワークの規模とインテリジェンスの恩恵を受けています。それは、**1日あたり1,120億件を超えるサイバー脅威をブロックします**。

高度な機械学習モデルにより防御力が常に向上するため、お客様に代わって新たな脅威の先を行くことができます。

業界が認めたDDoS防御

Cloudflareは、**DDoS攻撃対策の2022年GigaOm Radarレポートでリーダーに選出されました。**このレポートでは9つの異なるベンダーを評価し、Cloudflareが総合的に最高位にランクされました。Cloudflareは、**The Forrester Wave™: DDoS軽減ソリューション、2021年第1四半期でも「リーダー」**に選ばれました。

Cloudflareは、セキュリティオペレーションセンター、対応の自動化、パフォーマンスなど15の基準で最高得点を獲得しました。

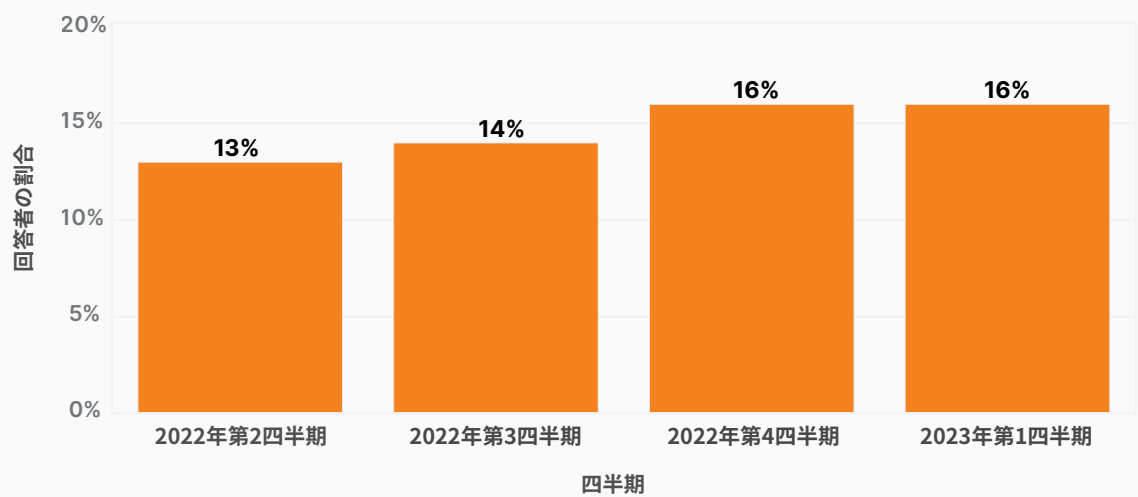
導入事例：ランサムDDoS攻撃の標的となったフォーチュングローバル500の企業

また、身代金脅迫として知られているランサムDDoS（RDDoS）攻撃は、悪意のあるグループが個人または組織をDDoS攻撃で脅して金銭をだまし取ろうとするものです。ランサムDDoSの試みの数は2022年を通じて着実に増加しました—2023年第1四半期には16%を超えるCloudflareのお客様が、DDoS攻撃の一部として脅威または身代金の要求を受けました。

ランサムウェア攻撃とよく混同されますが、ランサムDDoS攻撃は次のように動作が異なり、実行がより簡単です：被害者を騙してメールを開かせたり、リンクをクリックさせたりする必要はなく、また、ネットワークへの侵入や法人資産への足がかりを必要としません。サービスとしてのランサムウェアの可用性が高まっていることにより、攻撃者にとってランサムDDoSは労力が低く、リスクが低い選択肢となっています。

四半期別のランサムDDoS攻撃と脅威

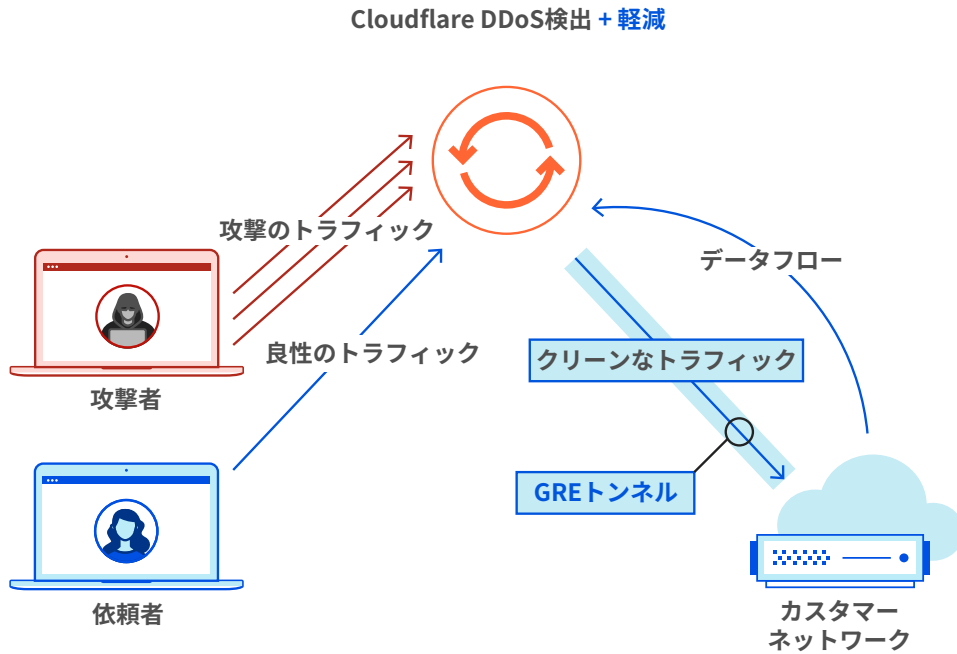
ランサムDDoS攻撃によって標的とされている、または脅威にさらされていると報告した回答者の割合



DDoS軽減にCloudflareを採用する前の2020年後半、フォーチュングローバル500の大手企業が、Lazarus Groupと名乗るグループ（北朝鮮政府が運営しているとされるサイバー犯罪グループ）**によるRDDoS攻撃の標的にされました。**攻撃者は当初、ビットコインを要求するメールを送信し、1週間で「支払い」を済ませる、さもないと2回目の大規模な攻撃が発生し、身代金が増加するというものでした。

身代金メモを受け取った後、グローバルデータセンターの1つへの大幅なトラフィックの増加に気付き、その企業は、オンデマンドスクラビングセンターサービスに連絡しました。ベンダーのサービスを有効にしてトラフィックをスクラビングセンターにリダイレクトするまでに30分以上かかりました。オンデマンドサービスを有効にしたことで、ネットワーク障害と複数のインシデントが起こりました。

最初の攻撃とオンデマンドプロバイダーの課題を受けて、企業は、Cloudflare Magic Transit—（ネットワークレイヤーのDDoS攻撃に対するCloudflareの常時保護）**を導入することを決定しました。**攻撃者達は二度目の大規模な攻撃を予告しましたが、それは起こりませんでした。



ネットワークレイヤーでのDDoS攻撃対策のためのCloudflare Magic Transit

「差別化の重要な点の1つは、既存のプロバイダーでは提供できなかったと思われる攻撃とトラフィックの分析です。自動的に軽減されていることについて知らなかった攻撃がわかります。」

インシデント対応およびフォレンジックチーム
フォーチュングローバル500の企業

まとめ

パンデミック後の時代にDDoS攻撃の頻度と複雑さが高まるにつれ、正当なトラフィックを維持して、収益を維持することが重要です。Cloudflareは、一般にその他のプロバイダーで起こる可能性がある遅延の問題や高額なコストを発生させることなく、攻撃から迅速かつ容易に保護できる機能を備えているため、常時接続のクラウド戦略を簡単に選択できます。

CloudflareによるネットワークDDoS攻撃に対する保護の詳細については、デモをリクエストしてください。

Zero Trust機能、DDoS軽減、ネットワークファイアウォール、トラフィックアクセラレーションを内蔵した単一のグローバルネットワークの詳細については、ここをクリックしてください。

ソース

1 Langrock、Sam。「クラウドでは攻撃対象領域の管理が複雑になってきています。」Recorded Future、2023年4月3日、
https://www.recordedfuture.com/the-cloud-has-complicated- Attack-surface-management

2「Uptime Instituteの2022年の障害分析では、障害頻度を抑制するための業界の取り組みが不十分であるため、ダウンタイムのコストとその結果が悪化していることが判明しています。」Uptime Institute、2022年6月8日、https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu、Catalin。「Bandwidth.comは、DDoS脅迫の試みを受け、最大1,200万ドルの損失を見込んでいます。」記録、2021年11月1日、
https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes、David、Blankenship、Joseph、他。「The Forrester Wave™: DDoS軽減ソリューション、2021年第1四半期」、Forrester、2021年3月3日

5 Didio、Laura。「企業のダウンタイムのコスト、」TechChannel、2021年9月30日。
https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6「Top US eコマースサイトのダウンタイムのコスト」、Gremlin、2023年5月8日にアクセス、
https:/ /www.gremlin.com/ecommerce-cost-of-downtime

7 Crets、Stephanie。「ほとんどのコンシューマーは、読み込みの遅いeコマースサイトを放棄します。」DigitalCommerce360、2020年8月21日。
https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre、Mathieu。「ゲーマーの44%はゲームを終了して遅延に対応—これを防ぐにはどうすればよいでしょうか？」PocketGamer.biz、2022年10月24日、
https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9「無限データと遅延を克服するための戦い」HazelcastとIntel、2019年11月。https://hazelcast.com/resources/infinity-data-report

enterprise@cloudflare.com | www.cloudflare.com

CLOUDFLARE