

DDoS攻撃を軽減するための 5つのベストプラクティス

急速に進化するDDoS攻撃から保護を行い、
全レイヤーの脆弱性に対処する方法

I. エグゼクティブサマリー

分散型サービス拒否(DDoS)攻撃は、依然として、全世界の企業に対してサイバー犯罪者が使用し、財務、業務、そして評判に甚大な損失をもたらす最も効果的な手法の1つです。この攻撃には様々な形態がありますが、目的は常に標的とするサーバー、サービス、ネットワークに大量のトラフィックを送りつけて正常な機能を奪うことであり、不正アクセスしたデバイスやネットワークを利用します。

企業が防御を強化すれば、サイバー犯罪者は複数のアプリケーションやサービスを標的とする新たな攻撃タイプでそれに応酬します。こうした攻撃のいくつかは、Open Systems Interconnection (OSI) モデルの第3層と第4層を新しい方法で標的とし、毎秒1.3 TB以上のネットワークトラフィック急増が生じます。そのほかの攻撃は、セキュリティ網をかいくぐって1つまたは複数のサービスゲートウェイとアプリケーション層を標的とするように設計された低速の第7層攻撃です。

DDoS攻撃に関連する困難を乗り切るためには、全ての層で全ての脅威に対応できる包括的なアプローチが必要となります。しかし、セキュリティを強化してもパフォーマンスを犠牲にしては意味がありません。オンプレミスのソリューションはその一部を実現することは可能ですが、より堅牢なソリューションとしては、パフォーマンスを担保しつつ、ネットワークエッジで機能するスケーラブルでクラウドベースの緩和策によって、最大限のアジリティと無制限の容量を提供することが好ましいでしょう。

PART 1

DDoS攻撃とは？

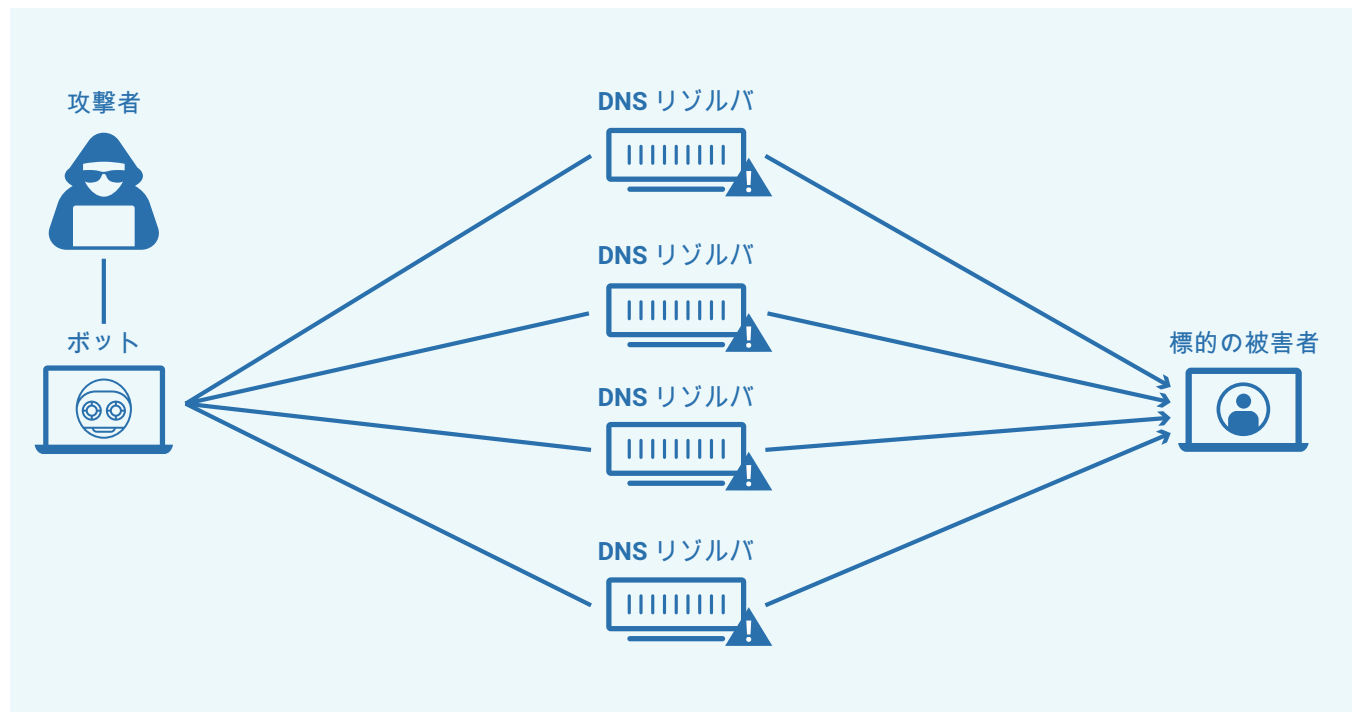
分散型サービス拒否(DDoS)攻撃とは、標的となるサーバー、サービス、ネットワークを大量のインターネットトラフィックで圧倒することで、そこを通過する通常のトラフィックを妨害する悪意のある攻撃のことです。こうした攻撃が影響を及ぼすために、脅威アクターと呼ばれる攻撃者は、オンラインのコンピューター、ルーター、IoTデバイス、その他のエンドポイントを制御し、攻撃トラフィックのソースとして活用します。このようなマシンはマルウェアに感染し、リモートコントロールで起動される「ボットネット」で兵器化されます。

標的となるサーバーやネットワークのIPアドレスが特定されると、各ボットは、容量制限を超過させることを意図して、標的に同時にリクエストを送信します。その結果として、通常のトラフィックに対するサービス拒否につながります。各ボットが正当なデバイスであるため、攻撃トラフィックと正規トラフィックを分離することは非常に困難です。

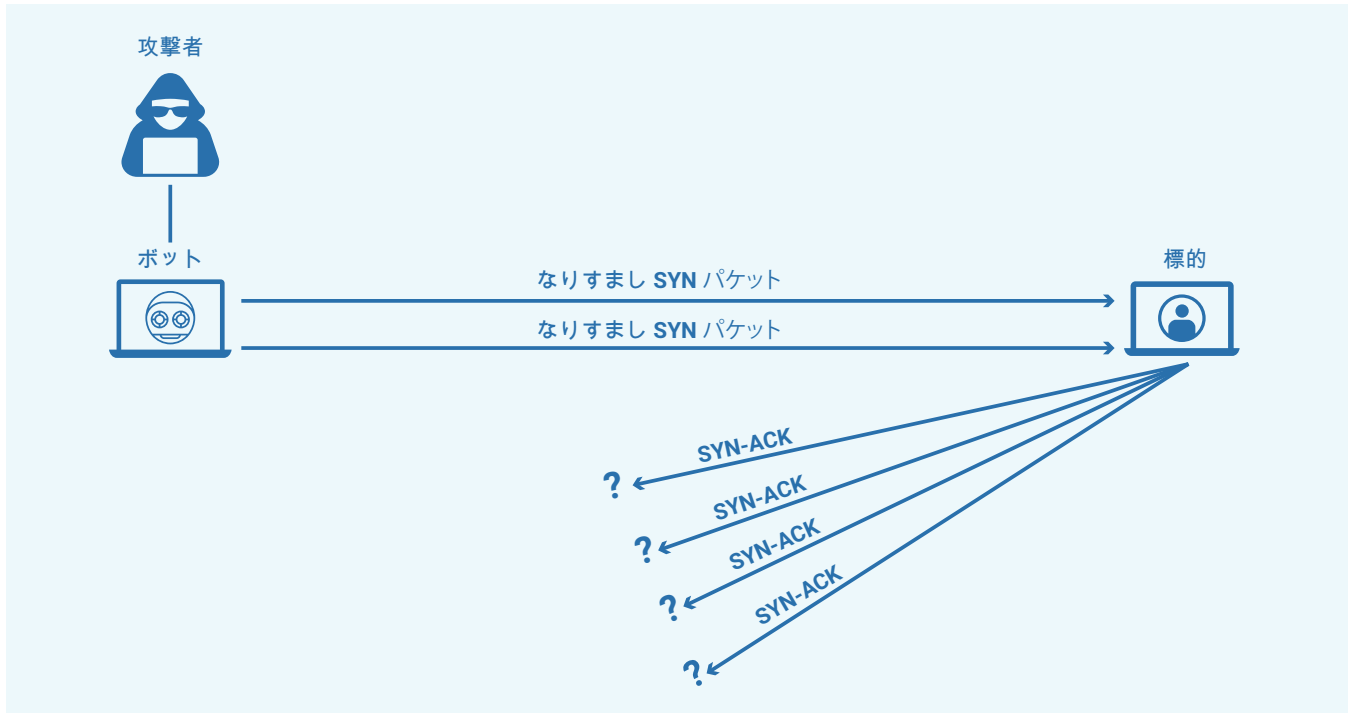
DDoS攻撃の種類

DDoS攻撃はネットワーク接続のOSIモデル内にある個別の7階層のどれでも標的にできます。こうした攻撃すべてが悪意のあるトラフィックにより標的の閉塞を引き起こしますが、三つのカテゴリーに分類できます。

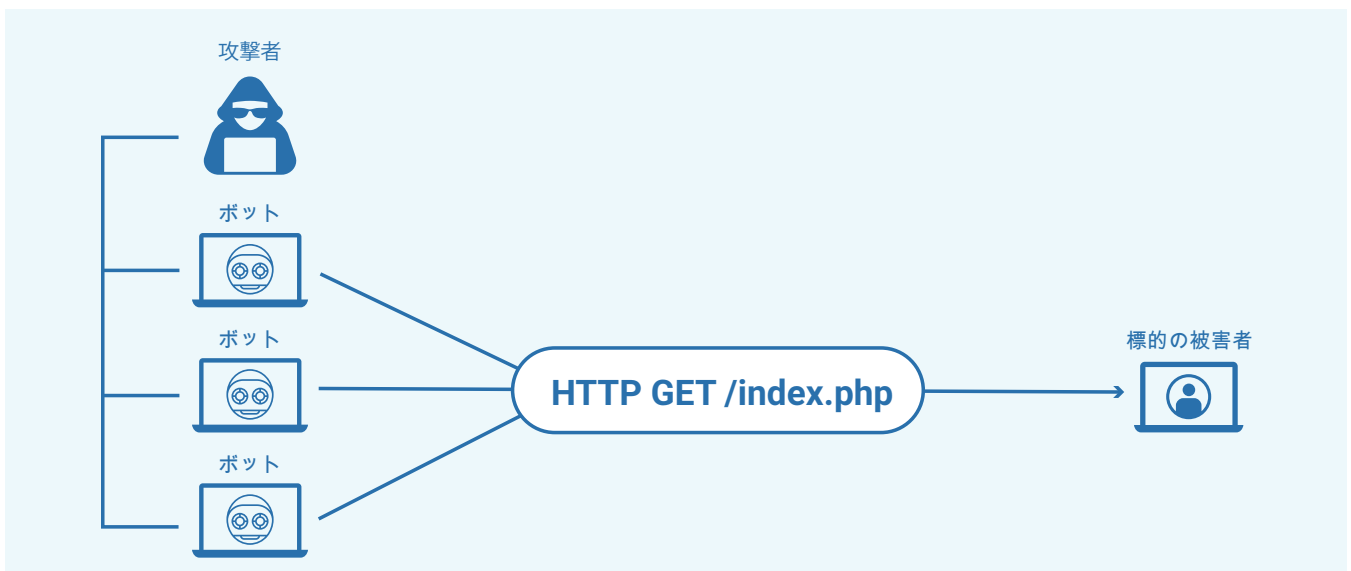
帯域幅消費型攻撃: この攻撃は、ネットワークを標的とし、webパフォーマンスを低速化、正規ユーザーのアクセスを低下させることで、サイトと大規模なインターネットの間で輻輳を発生させるようにデザインされています。そして、ビット/秒 (Bps) で測定される巨大なトラフィックサージを作り出すためにDNS増幅その他のテクニックを採用します。



プロトコル攻撃: プロトコル攻撃の目的は、OSIモデルのレイヤー3(ネットワーク)とレイヤー4(トランスポート)の脆弱性を標的とすることで、webサーバーまたは、ファイアウォールやLoad Balancerを含む、中間リソースで利用可能な容量すべてを消費します。こうした攻撃には、SYNフラッド攻撃、Ping of Death攻撃、Smurf DDoS、フラグメントパケット攻撃があり、すべてパケット/秒(Pps)で測定されます。



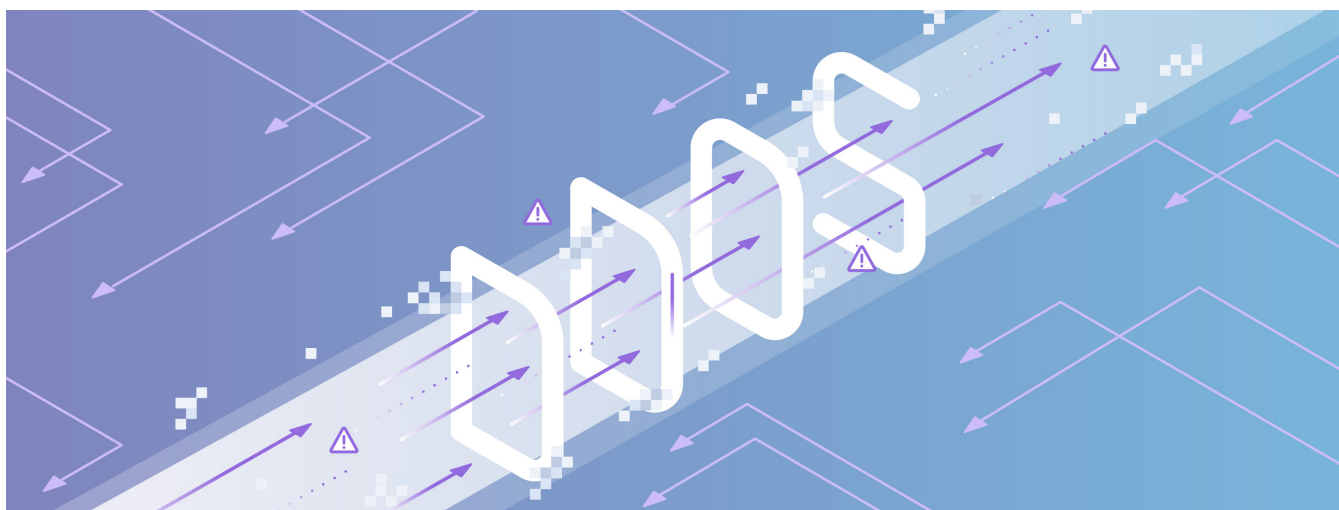
アプリケーション層攻撃: この攻撃は、時にアプリケーション層(レイヤー7) DDoS攻撃と呼ばれることもあり、サーバー上でWebページを作成したり、HTTPまたはHTTPSリクエストに応答して配信する層を標的とします。一度に多数のコンピューターのWebブラウザで繰り返し更新を実行するのに似ていて、この結果生成される大量のHTTPまたはHTTPSはリクエスト/秒(Rps)で測定されます。



こうした攻撃タイプには重複するものもあります。たとえば、プロトコル攻撃の一部は、帯域幅消費型攻撃でもあります。そして、脅威アクターが同時にプロトコルスタックの複数の層を標的にしたり、攻撃対象が取る対策に基づいて攻撃ベクトルを替えるマルチベクトル型攻撃があります。さらに、多くのマルチベクトル型攻撃は、データ漏えいやそのほかの犯罪を隠蔽するために設計された偽装行為にすぎません。

DDoS攻撃がどのようにビジネスに被害を及ぼすか

DDoS攻撃によりオフラインになってしまうと、収益、カスタマーサービス、そして基本的なビジネス機能に悪影響が及ぶ可能性があります。攻撃の目的が、サイトやネットワークに不具合を生じさせること、トラフィックをライバル企業に回すこと、企業データ窃盗を隠すこと、または単に最大限の風評被害を引き起こすことのいずれであれ、ユーザーに非難される対象はあなたの事業であることがほとんどです。平均的なDDoS攻撃は、小規模企業で12万3000ドル、大企業で200万ドル以上の被害をもたらします¹。そして攻撃は止まりません。世界中でDDoS攻撃の数は、2020年の1190万件から2022年までに1450万件以上に増加すると見られています²。



PART 2

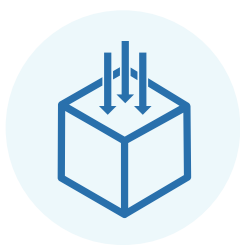
進化するDDoSの課題 どう対処するのか

一般的に、DDoS攻撃から保護するには次の能力が必要となります。

- トラフィックスパイクが、攻撃によるものかユーザーからの需要の高まりによるものかを区別する
- 正当なトラフィックを中断させることなくボットネットから送信されるトラフィックをブロックする
- サービス拒否を防止するために管理可能なチャンクに分割することで、残りのトラフィックを最適にルーティングする
- 継続的に悪意のあるパターンのトラフィックを分析し、適応的かつ強化された防御の開発に役立てる

今日、二つの新しい傾向が現れ、これらすべてをさらに困難なものとしています。

帯域幅消費型攻撃の規模拡大



- 100Gbpsを超える帯域幅消費型DDoS攻撃が2018~2019年に967%の急増³
- 2018年にGitHubをオフラインにさせた攻撃のように、毎秒1.3 TB規模のDDoS攻撃が当たり前になり
- 2020年のはじめ、1件の帯域幅消費型ネットワーク層DDoS攻撃が、92Gbpsに達し、1038万パケット/秒 (Mpps) を記録⁴
- 多くの帯域幅消費型DDoS攻撃は数分間で終わる一方、何時間も継続するものも。帯域幅消費型攻撃を受けた企業の73%が24時間以内に再び標的に⁵

攻撃の複雑性が増加



- 4分の3⁶のDDoS攻撃で、複数のベクトルが標的に
- レイヤー3とレイヤー4を標的とするDNS増幅と、レイヤー7を狙う大量のHTTP/Sの組み合わせは、マルチベクトル型DDoS攻撃の一例
- 攻撃が複雑になるほど、軽減も困難に。攻撃者の目的は、正当なトラフィックと悪意のあるトラフィックを可能な限り混ぜ合わせることでその区別をさらに難しくすること
- トラフィックをドロップまたは制限しようとする軽減策は、攻撃がこの対応策を回避するように適合すると効果なし

こうした要件と進化する傾向に基づき、企業が優先すべきDDoS対策に関する5つのベストプラクティスをご紹介します。

PART 3

DDoS対策に関する ベストプラクティス



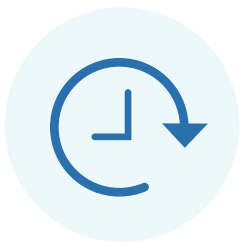
1 保護対象に合わせた戦略作り

webサーバーを保護することが目的であれば、リバースプロキシで攻撃者がサーバーのIPアドレスを特定して攻撃することを防止できます。攻撃者はリバースプロキシしか標的にできません。さらに複雑な第7層攻撃に関しては、web application firewall (WAF) が、リバースプロキシとして機能して特定タイプの悪意のあるトラフィックから標的とされたサーバーを守ることができます。独自のリバースプロキシを構築し展開する企業もありますが、これには集約性の高いソフトウェアとエンジニアリングリソース、さらに物理的なハードウェアへの多額の投資を必要とします。

リバースプロキシの便益を得る、最も簡単かつ費用対効果が高い方法の一つとして、コンテンツ配信ネットワーク (CDN) の利用があります。Global Server Load Balancingを備えたCDNを活用すれば、運営するサイトを世界中のいくつかのサーバーに分散できます。これなら、パフォーマンスに影響なく、DDoS攻撃をソースにより近いところで軽減できます。

ネットワークのインフラストラクチャの保護が目的ならば、Border Gateway Protocol (BGP) の再ルーティングを利用して悪意のあるトラフィックがフィルターにかけられるスクラブセンターへとトラフィックをリダイレクトすることができます。とは言え、地理的に離れていて数が限られているスクラブセンターにトラフィックすべてを再ルーティングすると、かなりのレイテンシーが発生することにもなりかねません。

このため、十分な規模のクラウドベースのDDoS対策ソリューションをお勧めします。クラウドベース軽減策では、自律システム番号 (ASN) は、緩和策プロバイダーが通知するため、トラフィックは配信元サーバーに向かう代わりに、直接スクラブへとルーティングされます。トラフィックは、攻撃のソースにより近いところでフィルターにかけられ、レイテンシーもさらに削減できます。

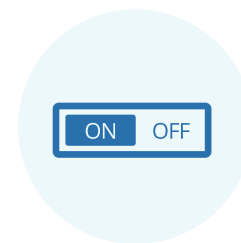


2 二つの最重要メトリクスを優先する—容量と緩和時間

サイトの機能性に影響を与えずにDDoS攻撃を緩和するために既存の容量を評価します。DDoS攻撃によって引き起こされるトラフィックのスパイクを吸収する従来のアプローチは、オンプレミスのサーバーファームを構築する方法でした。しかし、これは経費の規模が急激に大きくなり、最も堅牢なエンタープライズレベルのインフラストラクチャでも、日によって規模が大きくなる帯域幅消費型攻撃を前にして、圧倒される可能性が高いでしょう。

Rate Limitingが役に立つかもしれませんが、パフォーマンスを低速させ、インフラストラクチャが過負荷になる場合、やはり停止という結果になるかもしれません。たとえ数秒でも可用性が低下することで、収益や生産性の面で大きな損失が出るかもしれない場合、緩和時間 (TTM) が最優先事項になります。TTMの短縮のために、停止発生時にトラフィックが代替サイトへと確実にフェイルオーバーしなければなりません。しかし、これも、インフラストラクチャが圧倒されてしまえば機能しません。

ここで再び、より効果的なアプローチとなるのが、規模や複雑性にかかわらず、どんなDDoS攻撃からも保護できる無制限容量を提供するクラウドベースの軽減ソリューションを展開することです。そして、急速に進化するDDoS攻撃を軽減する最大限の敏捷性を実現するために、ネットワークエッジでサービスが利用できるようにします。



3 常時稼働 VS. オンデマンド保護

オンデマンド軽減サービスの場合、トラフィックはDDoS攻撃の可能性を検出するまで、通常通りに流れます。検出された時点でトラフィックはクラウドの軽減サービスへと再ルーティングされ、フィルターにかけられ、配信元のサーバーへと戻されます。DDoS対策料金は、必要な時だけ支払い、管理も追加のリソースも不要です。ただし、特に緩和時間ではトレードオフがあります。トラフィックスパイクがある程度のThresholdsに達して初めて攻撃の分析が開始し、誰かが手動で緩和サービスを作動させるため、攻撃を阻止するまでにより時間がかかります。

それと比べて、常時稼働の緩和はサイトトラフィック全てを継続的にルーティングし、フィルターをかけます。そのため、クリーンなトラフィックだけが常時、お客様のサーバーに到達します。オンデマンドサービスよりも費用は高くなりますが、常時稼働の緩和は中断なく保護を提供し、サーバーを手動で作動させる必要がないため、応答時間が速くなります。さらに、DDoS攻撃の増加を鑑みると、定額制の常時稼働の緩和サービスは、絶え間ない攻撃に常に直面している企業にとっては、実は経費削減となるかもしれません。



4 セキュリティのためにパフォーマンスを犠牲にしない

DDoS攻撃は停滞と停止を引き起こし、パフォーマンスを低下させるだけでなく、企業の持続可能な成長を達成する能力まで損ないます。今日のデジタル消費者は、webサイトとアプリケーションの読み込みは瞬時に行えて、決してオフラインにならないことを期待しています。平均的なユーザーは30ミリ秒でレイテンシーが気になり、読み込み時間が1秒でも長くなると、コンバージョン率は7%も低下します⁷。

また、レイテンシーは生産性も損ねます。最良の場合でも、平均的な従業員はネットワークが応答するのを待つのに、年間1週間分の時間を無駄にしています⁸。フォーチュン1000入りする企業における、ダウンタイムによる平均総コストは年間12億5000万〜25億ドルです⁹。パフォーマンスを低下させず、DDoSから守るには、慎重にバランスをとることが必要となります。

前述したように、多くの企業はトラフィックをスクラブセンターにリダイレクトして攻撃を緩和しようとしませんが、通常スクラブセンターはトラフィックソースや配信元サーバーから遠く離れていて、攻撃に匹敵するレイテンシーレベルをまねくボトルネックを作り上げます。このため、DDoS攻撃をブロックするために、限定的なスクラブセンターサービスを利用することは現実的な選択とは言えません。さらに速い応答時間を求めるなら、世界各地で攻撃ソースに対して物理的に近いロケーションで検出と軽減を実行する機能を備えたクラウド軽減サービスをご検討ください。



5 攻撃者の一歩先を行くために賢い選択を

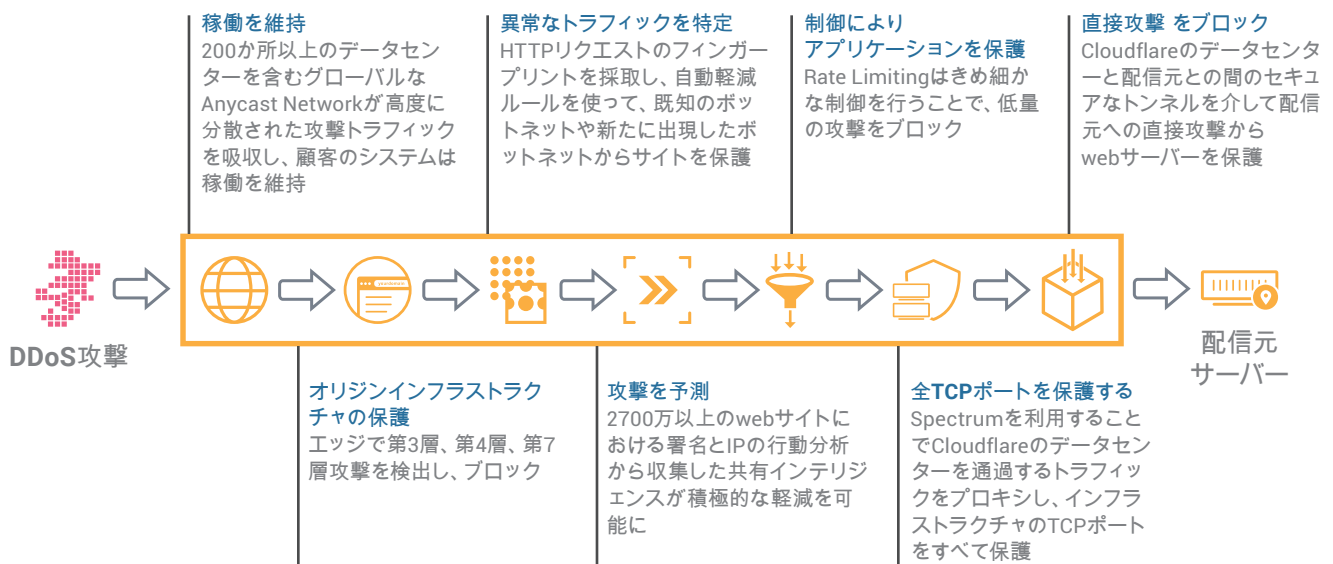
複雑さを増すDDoSに勝つために、単なる階層型アプローチ以上のものが必要となります。今後起こる攻撃を防ぐために必要なインテリジェントで適応力の高い防御を開発するために必要になる悪意のあるパターンについて継続的にトラフィックを分析する必要があります。進行中のDDoS攻撃は、次の攻撃に打ち勝つための秘訣です。

クラウドベースの軽減策を評価する際、容量や転送速度、フィルター速度以上を見るだけでなく、そのサービスが、どのような情報の入手に活用できるのを見ることも大切です。緩和ネットワークがさらに大きく堅牢になるほど、進化する攻撃パターンについて提供できる情報は豊かになります。—そしてこうしたサービスはより先制的になります。

Cloudflareのサービス

Cloudflareの階層型セキュリティアプローチは、複数のDDoS対策機能と組み合わせられて一つのサービスとなり、悪意のあるトラフィックによる混乱を防止しながら、良好なトラフィックの通過を許可し、webサイト、アプリケーション、API、ネットワーク全体を維持し、高い可用性とパフォーマンスで実行しています。

95か国200都市以上に広がるデータセンターと37Tbpsを超えるネットワーク容量を持ち合わせるCloudflareは、DDoS攻撃をソースの近くで軽減し、先進国において、インターネット接続人口の99%に100ミリ秒以内でデータを配信可能です。



高速で自動化された緩和策

限られたスクラップセンターでのボトルネックに依存する従来のソリューションとは違い、当社のポイントオブプレゼンスはグローバルにセキュリティサービスをホストし、規模や複雑性にかかわらず、あらゆるDDoS攻撃から保護しています。これには分散型サーバー全体にトラフィックを分散させてネットワークに吸収させる機能が含まれます。

グローバル規模の脅威インテリジェンス

CloudflareのDDoS対策を支えているのは、Cloudflareのグローバルネットワークによるインテリジェンスで、毎日2700万以上のwebサイトを保護し、そこを通過する10億を超える固有のIPに対処しています。このインテリジェンスが、最も高度化した攻撃から保護する独自の見張り台としての役割を果たしています。

コストパフォーマンスに優れた保護

Cloudflareのプランすべてで、DDoS攻撃に対して無制限かつ定額制の軽減を提供しています。攻撃の大きさに関わらず、追加料金なし、そしてネットワークトラフィックの攻撃によるスパイクに対するペナルティもありません。

使用と管理が簡単

Cloudflareの常時稼働でクラウドベースのDDoS保護は、直感的な操作が可能なインターフェースに基づいて構築されており、DDoS攻撃の規模や複雑さにかかわらず、ユーザーが数回クリックするだけで、迅速かつ簡単にインターネットプロパティを保護することができます。

セキュリティとパフォーマンスの統合

CloudflareのDDoS攻撃対策は、Web Application Firewall、ボット管理、Magic Transit、Load Balancer、CDNその他のセキュリティやパフォーマンスソリューションとシームレスに統合し、学習し、動作するよう設計されています。

自社の方法でデータ分析

Cloudflare AnalyticsならCloudflareの統合ダッシュボードやGraphQLを通じてご自身でDDoS攻撃のイベントを分析できます。また、Cloudflareログを主要なサードパーティのSIEMと統合して、既存のビジネスプロセスとシームレスに統合できます。

まとめ

DDoS攻撃に関連する困難を乗り越えるために効果的な戦略は、すべての層ですべての脅威に対応する包括的なアプローチが必要です。オンプレミスのソリューションはその一部を実現することは可能ですが、すぐに経費がかさんでしまいます。より堅牢なソリューションとしては、パフォーマンスを担保しつつ、ネットワークエッジで機能するスケーラブルでクラウドベースの緩和策によって、最大限のアジリティと無制限の容量を提供し、DDoS攻撃の規模や複雑さにかかわらず、保護できることが好ましいでしょう。

脚注

- 1 Kaspersky Labs, "DDoS Breach Costs Rise to Over \$2M for Enterprises Finds Kaspersky Lab Report," Kaspersky Labs, February 22, 2018
- 2 Crane, Casey, "The 15 Top DDoS Statistics You Should Know in 2020," Cybercrime Magazine, November 16, 2019
- 3 DeNisco Rayome, Alison, "Major DDoS attacks increased 967% this year," TechRepublic, April 24, 2019
- 4 Avital, Nadav, "2019 Global DDoS Threat Landscape Report," Security Boulevard, February 5, 2020
- 5 Cook, Sam, "DDoS attack statistics and facts for 2018-2019," Comparitech, August 20, 2019
- 6 Ibid
- 7 Stein, Jake, "Behind the Buzzword: The Reality of Real Time," InformationWeek, September 5, 2019
- 8 Tyson, Mark, "Users Lose a Full Working Week Every Year Due to Slow Computers," Hexus.net, October 2013
- 9 "IDC Study - The cost of downtime," Tech Republic, September 30, 2017



+81 3 4510 1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

© 2020 Cloudflare, Inc. All rights reserved.
Cloudflareのロゴは、Cloudflareの商標です。その他の会社名および商品名はそれぞれ関連する各企業の商標です。

改訂: 200330