



HTTPキャッシュ バイパス フラッド

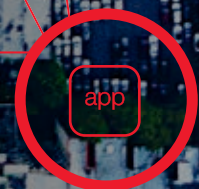
DNS NXDOMAIN攻撃

アプリのセキュリティを第一に考える

# DDoSは新しいスパム

大参事をただ迷惑なものに変える3つの戦略

TCP SYNフラッド攻撃





# 概要

## DDoS攻撃がますます大規模かつ複雑になり、蔓延するほど、サービス停止や不安が付きまとう将来になるように感じる

最新のInformation Security Forumの報告書『Threat Horizon』によると、DDoS攻撃を原因とするサービス停止は、組織が現在直面している最大のセキュリティ脅威の1つです。<sup>1</sup>

10年ほど前、誰もが不安を感じていたのは別の問題でした。それはスパムです。2009年、毎日送信される2,000億件以上の電子メールの約80%は、ナイジェリアの王子を名乗る寄付の依頼、オンライン薬局からの医薬品広告、そして「自宅で手軽にお金を稼ぐ」方法の紹介でした。すべてのスパム電子メールのほぼ半分は、フィルタを通り抜け、世界中の電子メールボックスはスパムで溢れていました。この状態がしばらく続き、電子メールを諦めなければならないようにも思えました。

現在、迷惑メールへの対策が改善されたことで、スパムは迷惑メールフォルダに追いやられ、たまに送られてくるナイジェリアの王子を名乗る人からの要請も他の何よりも笑える要素となりました。実際、これらの悪巧みのいくつかは笑って済ませることができます。スパムは、たまに気付く程度で日常生活を破壊することはない背景の雑音、迷惑なものになり下がりました。

しかし、私たちはまだDDoS問題を完全に掌握できたわけ

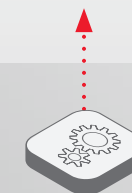
ではありません。もしナイジェリアの王子本人かもしれない誰かから、DDoS攻撃を仕掛けると脅迫する、ありえないようなメールを受け取ったとしたら、ただ笑って済ませる、または無視するわけにはいかず、真剣に受け止めなければなりません。今年、攻撃者は、あらゆる分野のさまざまな組織を標的としました。その目的は、政治的な出来事に影響を与えるため、ビットコインや従来の金融取引を混乱させるため、さらに一部の日常業務をオンラインにしているが大規模な大量攻撃への対策が取れていない企業を狙いランサムウェアを使って利益を絞り取るためです。<sup>2</sup>

DDoSがすぐにはなくならないことは明らかです。サービスの可用性およびビジネスの継続性を維持したいのであれば、攻撃および動機が進化しているように、私たちも進化する必要があります。

<sup>1</sup> <https://www.cio.com/article/3185725/security/9-biggest-information-security-threats-through-2019.html>

<sup>2</sup> <https://securelist.com/ddos-attacks-in-q2-2017/79241/>

## サービス拒否は、アプリケーション スタックのすべてのレイヤに影響



### アプリ サービス

- 厳しい（リソース消費型）URL 攻撃
- SLOWLORIS（ローアンドスロー）攻撃
- GETフラッド攻撃
- HTTPキャッシュ バイパス フラッド攻撃



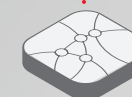
### アクセス/アイデンティティ

- セッション スプーフィング攻撃
- アカウント ロックアウト フラッド攻撃
- アカウント乗っ取り攻撃



### TLS/SSL

- SSLフラッド攻撃
- SSL再ネゴシエーション攻撃
- SSLプロトコルの悪用



### DNS

- DNSアンプ攻撃
- DNSリフレクション
- DNSキャッシュ ポイズニング
- DNS NXDOMAIN攻撃



### ネットワーク

- TCP SYNフラッド攻撃
- UDP & ICMPフラッド攻撃
- FIN/RSTフラッド攻撃
- ネットワーク プロトコルの悪用

## スパムは制御できたのに、 なぜDDoSはなくならないのか？

簡単に言えば、DDoSは予測が困難だけでなく、正当なリクエストと悪意のあるトラフィックの区別も困難であるため、その対処が難しいからです。どのようなネットワークにも複数のトラフィックの難所および脆弱な領域があり、現在のマルチベクトル攻撃は、さまざまな戦略が駆使され、ますます巧妙化しています。



### ボリユーメトリック攻撃

私たちが頻繁に目にしている攻撃で、対象者のインターネットのアップストリーム リンクを制圧し、その意図するユーザ ベースにサービスを提供できなくなるように、ネットワークに大量のトラフィックを送り付けます。



### リソース ボトルネック攻撃

インターネット トラフィックの50%以上がSSL/TLSを使って暗号化されているため、TLS ASICなどの暗号インフラストラクチャへの需要が急増しています。<sup>4</sup> 攻撃者は、ネットワークの復号機能を制圧して、必要なセキュア チャンネルを介してサービスを利用できないようにします。



### 複合攻撃

多くの攻撃は、さまざまな攻撃ベクトルを混ぜ合わせ、これらを同時に実行して、インフラストラクチャで最も弱いリンクを探し、それを利用します。



### ローアンドスロー攻撃

攻撃者の利用が増えているのは、アプリケーションレイヤのリソースに対するローアンドスロー攻撃です。これは、リソース集中型のデータベース クエリなどの弱点を悪用してサービスを利用できないようにします。このような攻撃は、従来の対策方法では検知および対抗が困難です。



### ビジネス ロジック攻撃

ネットワークまたはアプリケーションの脆弱性を狙わない攻撃もあります。攻撃者によっては、ボットを使って電子商取引サイトで不正取引を行い、正当な顧客へのサービスを拒否し、コストを上昇させます。

<sup>4</sup> <https://f5.com/Portals/1/PDF/labs/R065%20-%20REPORT%20-%20The%202016%20TLS%20Telemetry%20Report.pdf>

DDoS攻撃を引き起こす動機は、政治的能動主義<sup>5</sup>、卑劣な報復行為<sup>6</sup>、および予想通りの金銭目的などさまざまです。<sup>7</sup> DDoSは、他の攻撃から注意をさらすために使用されることもますます増えています。これは、一般に「陽動作戦」と呼ばれる戦略です。サービスをオンライン状態に保つために大量のトラフィックと格闘している間に、攻撃者はその防御をいくぐり、企業データ、機密情報またはその他の貴重な財産を盗みます。DDoS攻撃は、IDSやロギング サービスなど、このような活動を検知するはずの既存のセキュリティ コントロールを制圧する場合にも使用できます。これらが制圧されると、ネットワークの他の部分が脆弱なままになります。

さらに状況を悪化させていることに、DDoS攻撃を仕掛けること

が、ますます安く簡単になっています。約\$100もあれば、6分間、125 Gbpsの攻撃を仕掛けることができます。この規模の攻撃でも十分に、ほとんどの組織のアップストリーム キャパシティを制圧できます。<sup>8</sup> このようなわずかなコストで、DDoS攻撃は、個人的な恨みでも動機があれば誰にでも利用できます。つまり、論理的にはすべての人がリスクにさらされています。

<sup>5</sup> <https://www.csoonline.com/article/3054652/security/political-state-ments-largely-behind-ddos-attacks.html>

<sup>6</sup> <https://www.csoonline.com/article/3180246/data-protection/hire-a-ddos-service-to-take-down-your-enemies.html>

<sup>7</sup> <http://www.zdnet.com/article/ransomware-ddos-now-top-threats-as-hackers-look-for-big-paydays/>

<sup>8</sup> <https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/>

DDoS攻撃は、既存のセキュリティ コントロールの制圧に使用され、ネットワークの他の部分を脆弱のままにすることができる

# \$ 100

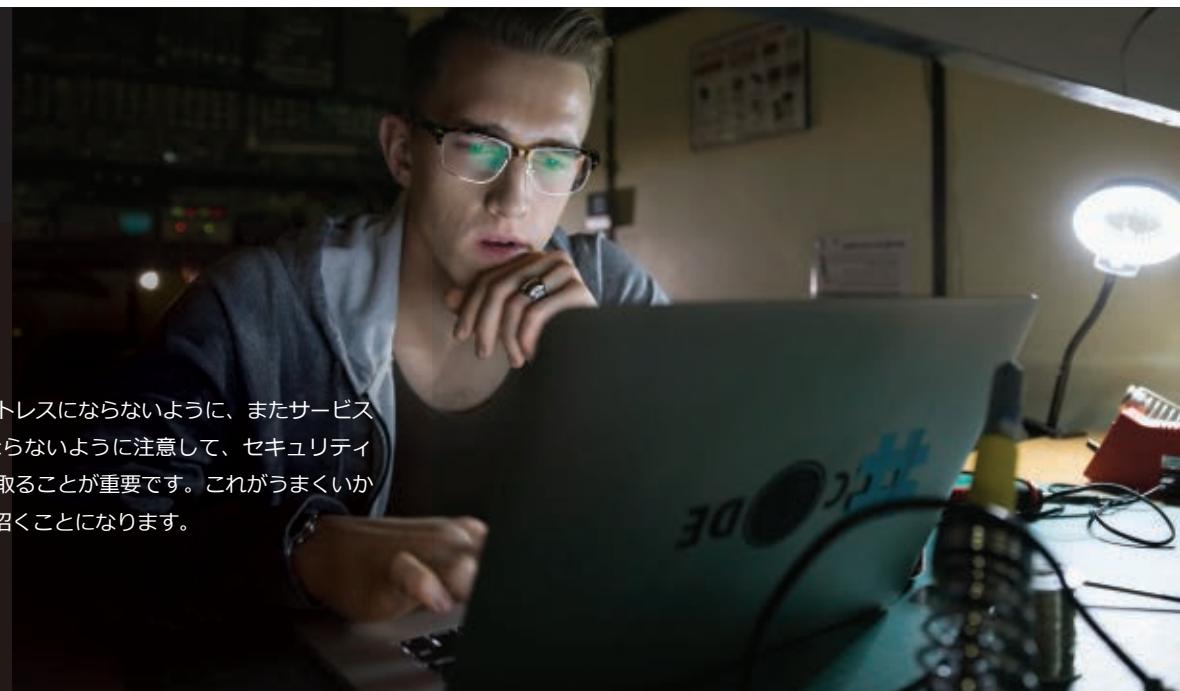
\$100もあれば誰でも6分間、125 GBPSの攻撃を仕掛けることができる


重要なことは、顧客のストレスにならないように注意してセキュリティ コントロールのバランスを取ることに

## 自分自身で「DoS」を招かない

通常、分散型サービス拒否（DDoS）と言えば、大規模なボットネットを利用した大量攻撃のことです。しかし、注意しなければならないのは、攻撃者は、顧客に企業への不満を感じさせれば、システムを完全に制圧する必要がないということです。サービスの停止またはサービス レベルの低下だけでも、顧客が取引を止める、または顧客が競合企業のサイトに移る十分な理由になります。

これを踏まえて、顧客のストレスにならないように、またサービスの継続的な利用の妨げにならないように注意して、セキュリティ コントロールのバランスを取ることが重要です。これがうまくいかないと、自らが「DoS」を招くことになります。






# DDoS対策能力を上げる ための3つの戦略

これらの進化を続けるDDoS攻撃は防御が困難です。コスト バランスを取るだけでなく、需要およびトラフィックの急上昇に合わせてスケールアップする必要があり、さらに十分なサービス レベルを顧客に継続的に提供する必要があります。また、柔軟なスケールダウンによりコストを最小限に押さえる必要もあります。これらの問題は、どの組織でも必ずどこかの時点で考えなければならないことです。いくつかの先進的な企業は、

頻繁に、およびランダムにシミュレーション攻撃を内部的に仕掛けて、インフラストラクチャの耐性をテストしています。<sup>9</sup> 必要は発明の母と言います。対処が難しいDDoS攻撃に取り組む中で、すべての人のDDoS対策能力が自然と向上し、ネットワークおよびアプリケーション アーキテクチャの耐性が強化されていくというメリットがあるかもしれません。

<sup>9</sup> <https://medium.com/netflix-techblog/tagged/simian-army>





ネットワークおよび攻撃の高度な可視化は、攻撃をより効果的に管理するためのコントロールの微調整が必要になるときに非常に有益です。

## 1 行動分析および行動学習はDDoS攻撃の軽減に役立つ

システムがセルフトレーニングにより、トラフィック行動を分析して、DDoS攻撃を認識し自動的に停止してきたとしたら素晴らしいことです。スマート ソリューションならこれが可能です。サービスの状況および進行中のトラフィック パターンを継続的に監視することで、高度な防御技術は、行動分析およびマシン ラーニングを利用して、数多くのデータ ポイントから標準的なトラフィックの状況および基準を理解できます。異常なトランザクションまたはワークフローの識別、疑わしいクライアントの影響を軽減するための措置の実施、およびデータの絞り込みによるプロセスの漸次的な改善は、さらに実現に向かっています。ここで1つ注意すべきことがあります。行動分析はレイヤ7のDDoS攻撃を止める上では有用ですが、大規模な大量フラッド攻撃に対する防御にはあまり実用的ではありません。不要なトラフィックにより、正当なリクエストが押し流されるだけです。

ネットワークおよび攻撃の高度な可視化は、攻撃をより効果的に管理するためのコントロールの微調整が必要になるときに非常に有益です。たとえば、顧客ベースの90%が米国にあり、米国以外のIPアドレスから大量の攻撃トラフィックが送られていることが分かった場合、顧客ベースの最も広範囲におけるサービスの可用性を守るために、攻撃を受けている間は米国以外のすべてのトラフィックをブロックすることが必要になる場合があります。フラッド攻撃が収まったら、このような制御を緩めて全体的な可用性を元に戻すことができます。

あるいは、特定のIPアドレスまたは特定の種類のマルウェアからアプリケーション レイヤ リクエストが繰り返し送られ

ていることがわかった場合、ネットワーク レイヤでこれらのクライアントからのトラフィックをブロックして、処理しないこともできます。また、これらのリクエストの影響を軽減するために、サービス品質 (QoS) ポリシーを実装することもできます。

# 33%

2017年、全組織の33%が少なくとも1回のDDoS攻撃を受けていました<sup>10</sup>

スマート ソリューションを利用することで、トラフィックの基準を確立し、そのトラフィックを管理するパラメータを設定して、事前に定義しておいた条件に基づき制御を自動的に強めることができます。行動分析およびフィンガープリントは、任意のリモート エンドポイントの意思、つまり人間かボットか、善か悪かをより詳細に可視化でき、これが、トラフィックを適切に分類する上で役に立ちます。

<sup>10</sup> <https://www.techrepublic.com/article/33-of-businesses-hit-by-ddos-attack-in-2017-double-that-of-2016/>

## 2 クラウド スクラビングは、攻撃を受けている間でもビジネスをオンライン状態に維持

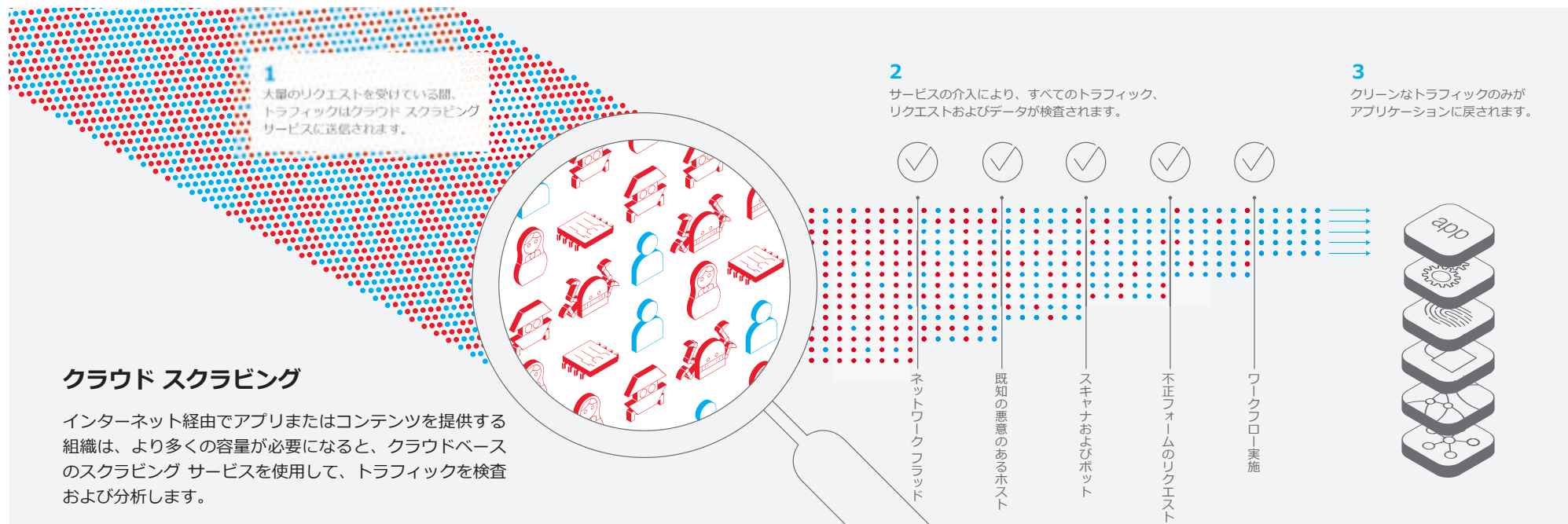
飽和に満たない認証ベースのアプリケーションレベルの攻撃なら、一般的に、常時稼働のクラウドまたはオンプレミス ソリューションで対応できますが、大規模な大量攻撃の場合、最強の防御能力がなければ簡単に制圧されてしまいます。そのため、敵の攻撃量を超える容量でデコ入れする計画が必要になります。ここがクラウド スクラビングの出番です。

インターネット経由でコンテンツまたはアプリケーションを提供する組織は、クラウドベースのスクラビング サービスを使用して、攻撃を受けている間でもビジネスをオンライン状態に保ち、ユーザへの影響を最小限に押さえることができます。スクラ

ビングとは、トラフィック、リクエスト、入力データなどを利用状況と妥当性の両方で検査および分析するプロセスのことです。トラフィックがオフサイトのスクラビング センターを通過するときに、継続的な分析により、悪意のあるリクエストがフィルタ処理で除外されます。このプロセスの最後で、すべての「クリーン」なトラフィックが戻されるので、正当なリクエストにサービスを提供し、通常通りに運用を続けることができます。

クラウド スクラビング サービスは一般的に、オンデマンドと常時稼働の2つのモデルのいずれかで提供されます。オンデマン

ド モデルでは、処理能力を超える量のトラフィック（莫大な量であっても、負荷のかかる量であってもリソース集中型のリクエスト）を受けている場合のみ、トラフィックがスクラビング センター経由で送信されます。常時稼働のクラウド スクラビング サービスは、企業に代わってこの処理をいつでも行うので、修復までの時間を短縮またはなくすることができます。また、常時稼働モデルは、家の庭で犬を飼うことで泥棒に狙われづらくなるように、獲物を探し回る潜在的な攻撃者の抑止手段の役割を果たす場合もあります。



### 3 DDoS対策の未来になり得る、 シグナリングとオンデマンドのハイブリッド防御

DDoSが効果的な手段として利益を挙げ続ける限り、攻撃ベクトルおよび戦略は進化を続けます。強力なソリューションは、ローアンドスロー攻撃からフラッド攻撃まで、あらゆる攻撃に対する防御能力を備えている必要があります。しかし、システムをどのように最適化すれば、攻撃を受けている間もシステムが効率的に機能し、ビジネスをオンライン状態に保つことができるでしょうか。

「シグナリング」は、オンプレミス設備とクラウド スクラビング サービスを統合することで、攻撃時の相互通信を可能にします。この技術により、オンデマンドのクラウドベース スクラビングを素早く起動でき、スクラビング サービスを介して攻撃トラフィックをシームレスにリダイレクトできます。これにより、最大

の大量攻撃が発生しても、アップストリーム接続が飽和することはありません。Internet Engineering Task Force (IETF) は、オンプレミス ソリューション、スクラビング サービスおよびその他のネットワーク要素やサービス間におけるリアルタイムのシグナリングに関する、標準に基づいたアプローチを開発する作業グループがあります。<sup>11</sup> この技術が成熟するにつれ、シグナリングはさらに効果的になり、包括的なDDoS対策戦略における最高の防衛線になるかもしれません。

現在使用しているソリューションによっては、ネットワークとアプリの保護にシグナリングを使用できるかもしれません。クラウド スクラビング サービスに手動で切り替える、またはポリシーおよびしきい値を介してシステムが自動的に切り替えるように

設定できます。この自動的な方法では、（特にSSLオフロードが必要なレイヤ7の防御に関して）準備とテストが必要になりますが、実際に標的になった場合には時間と労力を大幅に節約できます。

ここでの教訓は、すべてのDDoS対策戦略にも言えることです。最悪の事態になる前に計画と準備をしておくことです。トラフィックをスクラビング サービス間でシームレスに受け渡しする最適な方法をスクラビング プロバイダと協力して決めるまでに多少の時間を要しますが、このサービスを導入することで、いざというときに大きな助けとなります。

<sup>11</sup> <https://datatracker.ietf.org/wg/dots/about/>

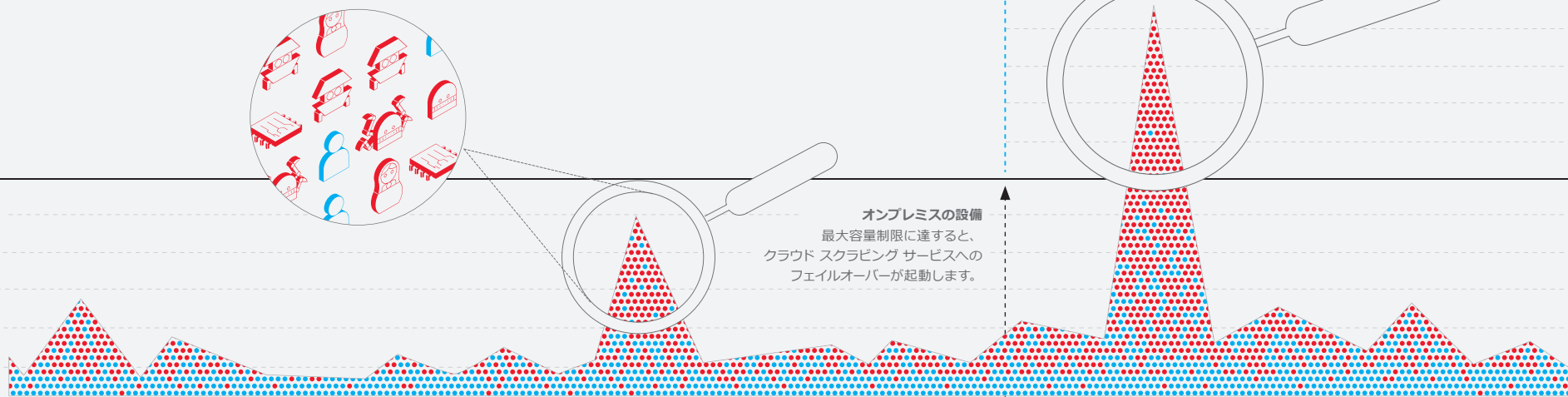
**シグナリング** この技術は、大量のトラフィックを受けているときにスクラビング サービス経由でトラフィックをシームレスにリダイレクトすることで、オンデマンドのクラウドベースのスクラビングを素早く起動できます。

#### クラウド スクラビング サービス

統合型ソリューションでは、トラフィックが急上昇すると、クラウド スクラビング サービスに切り替わります。

#### オンプレミスの設備

最大容量制限に達すると、クラウド スクラビング サービスへのフェイルオーバーが起動します。





## DDoS：迷惑ではあるが、大参事には至らない


シグナリングおよびスクラビング技術が進化するにつれ（またソリューションの適応性が高まるにつれ）、DDoS攻撃は効果が弱まり、攻撃者予備軍にとって魅力的ではなくなります。そして近いうちに、IoTボットネットから仕掛けられる1 Tb規模の攻撃は、たとえそれに気付くことがあっても、大参事には至らず、ただ迷惑に感じるだけの存在になる時が来るでしょう。

それでは、そこにいち早くたどり着くにはどのようにすれば良いでしょうか。多層防御のDDoS戦略を設計して事前に計画し、信頼できるセキュリティ プロバイダと協力して、大規模攻撃に備え

てください。事前に備えておけば、DDoS攻撃の脅威による眠れぬ夜から解放されときに、その努力が報われます。

組織に影響を与える脅威、およびそれらの対策の詳細については、[f5.com/security](https://f5.com/security) をご覧ください。

事前に備えておけば、DDoS攻撃の脅威による眠れぬ夜から解放されときに、その努力が報われる



多層防御のDDoS戦略を設計して事前に計画し、信頼できるセキュリティ プロバイダと協力して、大規模攻撃に備えてください。

## アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を保護することは、攻撃を受けるアプリを保護することにつながります。



### F5 ネットワークスジャパン合同会社

#### 東京本社

〒107-0052 東京都港区赤坂 4-15-1 赤坂ガーデンシティ 19 階  
TEL 03-5114-3210 FAX 03-5114-3201

お問い合わせ先：<https://f5.com/jp/fc/>

#### 西日本支社

〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階  
TEL 06-7222-3731 FAX 06-7222-3838