トピックス

# DDoS攻撃からWebサービスを守る
## ―大規模化するDDoS攻撃の仕組みとその対策―

インターネットを利用した企業活動における重要基盤（ネットワークそのもの、DNS、Webサービスなど）に対するDDoS攻撃が大規模化している。その脅威からどのようにサービスを守るべきか。DDoS攻撃の動向と、筆者の業務経験に基づいた対策を紹介する。

NRIセキュアテクノロジーズ サイバーセキュリティサービス事業本部
サイバーセキュリティプラットフォーム部 上級ITセキュリティアーキテクト
神谷（かみや）　誠（まこと）
専門はネットワーク構築・運用全般とDDoS攻撃対策など

### 大規模化するDDoS攻撃の最新動向

DDoS（Distributed Denial of Service）攻撃とは、特定のネットワークやコンピュータへ複数のマシンから大量の処理負荷を与えることで機能を停止させてしまう攻撃である。最近は攻撃規模も回数も増え続けており、これは金銭を目的とした企業脅迫が増えていることが背景にある。

DDoS攻撃は複数の攻撃手法を混在させて行われることが多いが、大規模攻撃の手法として、数年前からUDP（インターネットなどで使われる、大量送信に向くプロトコル）を使ったリフレクター攻撃が利用される傾向にある。

「リフレクター」とは、送信元からの問い合わせに対し、反射的な応答を返すように動作するモノの総称で、ここでは攻撃によく使われるDNSサーバーがそれにあたる。DNSプロトコルによるリフレクター攻撃は「送信元を攻撃対象のIPアドレスに偽装」し、DNSリクエストをセキュリティの脆弱（ぜいじゃく）なDNSサーバーを経由して大幅に増幅させ、攻撃対象に大量のパケットを送り付ける攻撃である。プロトコルによって増幅率はさまざまであるが、数十倍から数百倍まで幅広い。また、UDP以外にも単純にHTTP/HTTPSでのリクエストを大量発生させる手法も依然として存在している。

### DDoS攻撃の影響と対策

一般的にDDoS攻撃の対象となりやすいのは、企業がインターネットを通じて一般ユーザーに提供しているWebサービスである。

一般ユーザーが企業のWebサービスを利用する際には、クライアント（ブラウザー）からWebサービスの「名前解決」を行い、リクエストを送信、Webサービスからのレスポンスを受信という流れになる。この流れのどこが欠けても、一般ユーザーから見た企業のWebサービスは利用不能と見なされてしまう。

この名前解決、リクエスト、レスポンスに対する具体的な攻撃手法とその影響、さらには対策について見てみたい。

### (1) 名前解決に対するリスク

企業のドメイン名を管理しているDNSサーバーに大量の名前解決の問い合わせが行われることにより、DNSサーバーの性能限界に達し、名前解決ができなくなる。また、DNSサーバーに至るネットワークの帯域をパンクさせることでも名前解決を不能にできる。

この対策としては、CDN（Contents Delivery Network：世界中のサーバーからエンドユーザーに最も近いサーバーを選び効率的にWebコンテンツを配信する仕組み）を利用した、クラウド分散型DNSによるドメイン管理サービスを利用することが挙げられる。このサービスにより、DNSがクラウド上に分散されることで、DNSの応答不能を回避できる。

### (2) リクエストに対するリスク

リクエストが到達できないように、Webサーバーに至るネットワークに大量のトラフィックを流入させ、帯域をパンクさせる方法もある。

また、帯域はパンクしないがHTTP/HTTPSの大量リクエストによりWebサーバーに至る途中経路に導入している「負荷分散装置」や、Webアプリケーションの脆弱性を利用した攻撃対策に特化した「WebアプリケーションFirewall」のリクエスト解析の処理能力が、性能限界に達してしまうことも考えられる。

これらの攻撃に対して、対策を挙げてみたい。リフレクター攻撃では主にUDPが利用されるが、企業が一般ユーザー向けに提供するWebサービスではUDPは利用しないケースも多い。契約しているプロバイダーに、UDPなど必要のないプロトコルをフィルターで通信拒否をしてもらうことは、コストも安く効果が高いと考えられる。

次に、高コストではあるが、CDNサービスプロバイダーが提供するDDoS攻撃の緩和サービスの効果が高い。また、WebアプリケーションFirewallをクラウド提供しているベンダーもあり、解析処理の性能枯渇に対して有用である。

その他に、DDoS攻撃を緩和する専用機器も世の中にいくつかあり、一定の効果は認められる。しかし、規模の見えない攻撃に備えて専用機器を維持運用していくことは費用対効果の面から見ると非常に負担が大きい上、機器の許容量を超える攻撃には耐えることができない。

### (3) レスポンスに対するリスク

Webサーバーの性能を超えるリクエストにより、Webサイトを応答不能に陥れる方法もある。この対策にもCDNによるWebサーバーのクラウド分散が最も効果が高い。

## 組織面へのリソース配分の重要性

これらサービスの適切な利用には、自社内に専門組織が必要である。また、大規模攻撃が発生した際の行動計画を作成し、定期的な訓練を実施すべきである。組織内CSIRT（Computer Security Incident Response Team）があれば、これらを担うのが理想であろう。DDoS攻撃への対策として、技術面だけでなく、組織運営へのリソース配分も重要となる。■