セキュリティ

ITマネジメント（内部統制）

DDoS攻撃の脅威からWebサイトを守る ～負荷分散だけでない、CDN導入のメリット

Webサイトがビジネスにおいて大きな役割を担うようになった今、その存在を脅かすDDoS攻撃は企業にとって大きなリスクとなっています。ただDDoS攻撃の対策は難しいことも事実であり、多くの企業が頭を悩ませています。このDDoS攻撃からビジネスを守るために、具体的にどのような対策を講じるべきでしょうか。

Point

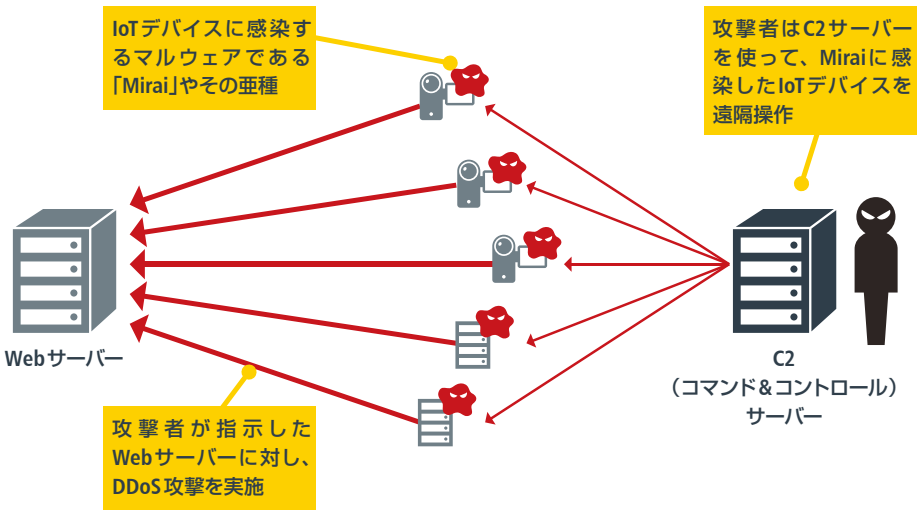
- **DDoS攻撃は増加し続けており、世界中の企業がターゲットになっている**
- **Webサーバー側での防御だけでは十分な効果を期待することは難しい**
- **CDNサービスの活用が有効なDDoS攻撃対策として期待されている**

相次ぐDDoS攻撃の被害

顧客とのコミュニケーションやユーザーサポートの場、サービス提供のプラットフォーム、あるいは商品を販売するためのコマースサイトとしてなど、ビジネスにおけるWebサイトの役割は増え続けています。今後デジタルトランスフォーメーションが進めば、Webサイトは企業にとって今以上に重要な存在となっていくでしょう。一方でWebサイトの存在感が増せば増すほど、大きなリスクとなるのがDDoS（Distributed Denial of Service）攻撃です。

大量のデータを送りつけて正常なWebサイトの閲覧を妨害するDDoS攻撃には世界中の企業が苦しめられており、もちろん日本企業も例外ではありません。たとえばハクティビスト集団であるAnonymousは、OpKillingBayやOpWhalesと呼ばれる作戦において日本の官公庁や企業をターゲットに大規模なDDoS攻撃を行いました。DDoS攻撃を行うと企業を脅迫して金銭を要求する犯罪行為も広まりつつあり、実際に日本のある金融機関が脅迫されていたことが発覚しています。

このDDoS攻撃におけるトレンドとして、見逃せないのはIoT機器に感染するマルウェア「Mirai」の存在です。攻撃者はMiraiに感染したIoT機器を遠隔操作し、ターゲットとなったWebサイトに対してDDoS攻撃を行います。2016年秋には、セキュリティ情報を発信しているブログである「Krebs on Security」がこの手法によるDDoS攻撃の被害に遭い、Webサーバーがダウンするという事例が発生しました。注目された理由は攻撃規模の大きさで、600Gbps以上もの帯域が使われたとされています。

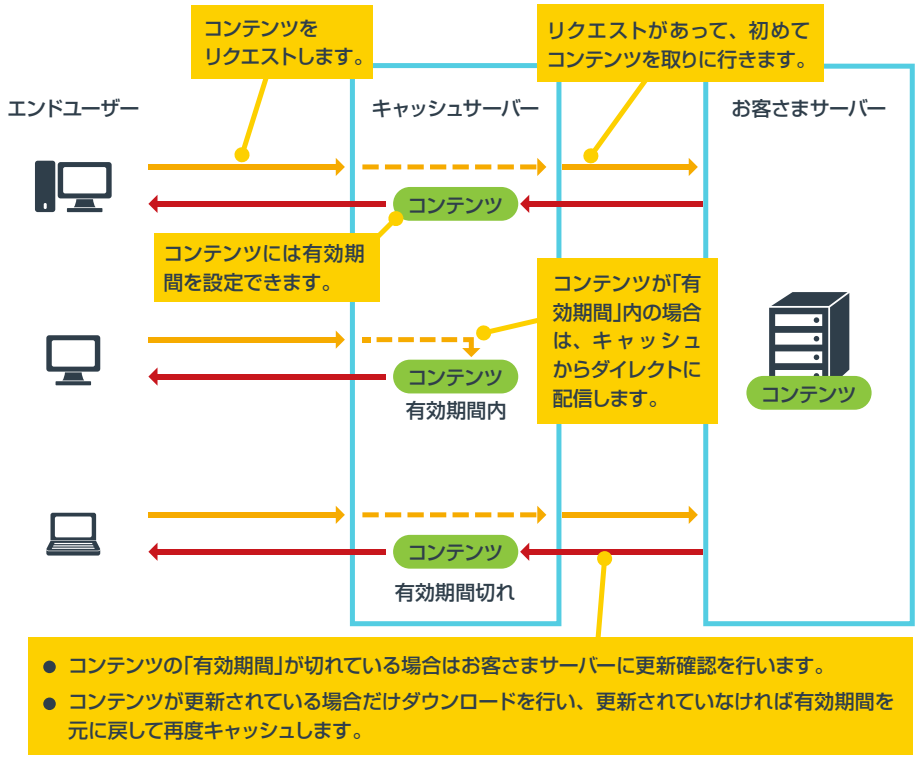


DDoS攻撃の防御が難しい理由

DDoS攻撃でやっかいなのは、対策が極めて難しい点です。たとえばWebサイトへの不正侵入を試みるサイバー攻撃であれば、通常のアクセスとは異なる異常な通信を検出したり、あるいは特定した攻撃元からのアクセスを遮断したりすることで対策することが可能です。しかしDDoS攻撃は正常な通信で大量のデータをサーバーに送り込むため、正常な通信と見分けることができません。また攻撃元も多数存在するため、そのすべてをリストアップしてアクセスを遮断することも難しいのが実情です。

仮にサーバー側で何らかの対策を行ったとしても、インターネットに接続している回線が詰まってしまうという問題もあります。DDoS攻撃によって大量のパケットが送り込まれ、それによってインターネット接続回線の帯域が消費されてしまうと、正当なユーザーもWebサイトにアクセスすることは不可能になります。つまりサーバーにダメージを与えなくても、大量の通信によって回線を詰まらせることができればDDoS攻撃は成功になるわけです。

このように対策が難しいDDoS攻撃からWebサイトを守るため、脚光を浴びているのがCDN（Contents Delivery Network）と呼ばれるサービスです。これは世界中に配置されたキャッシュサーバーを利用してWebサイトのコンテンツを配信するというサービスであり、もともとWebサイトのレスポンス向上を目的として利用されていました。

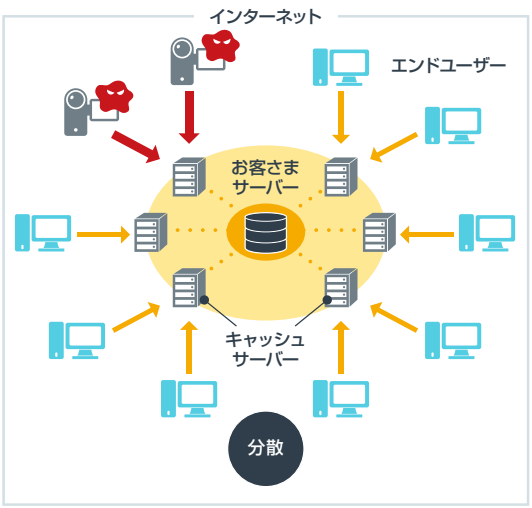


たとえば日本にサーバーがあるWebサイトにアメリカからアクセスすると、ネットワーク遅延の影響のため、日本からアクセスするよりもレスポンスは低下してしまいます。しかしCDNを利用すれば、もっとも近い位置にあるキャッシュサーバーからコンテンツを取得するため、たとえアメリカなど海外からのアクセスであっても高速なレスポンスで快適にアクセスすることが可能です。CDNサービスでは、独自に構築したキャッシュサーバーやそれに紐付くネットワークを利用し、顧客のコンテンツを世界中のユーザーに届けています。

DDoS攻撃対策として脚光を浴びるCDN

では、なぜCDNがDDoS攻撃対策として有効なのでしょうか。DDoS攻撃を受けると、攻撃者に操られている世界中のコンピューターからデータが送り込まれます。しかし、CDNを使っていれば接続先はキャッシュサーバーとなり、自社で運用しているWebサーバーやインターネット接続回線への影響は最小限に留められます。これによって正当なユーザーのWebサイトへのアクセスも可能となり、DDoS攻撃の被害を避けられるというわけです。

Webサイトの運用負荷の軽減にも大きな効果が見込めます。CDNを利用すれば、ユーザーからのアクセスに対して世界中のキャッシュサーバーで応答する形となるため、自社のWebサーバーに大きなリソースを割かなくても、多数のユーザーからのアクセスに対応することが可能になります。これによってサーバー台数を削減できれば、運用負荷の軽減につなげられます。またインターネット接続回線の帯域も節約できるため、Webサーバー運営コストの適正化が図れます。



- キャッシュサーバーから代理配信するため、自社で用意するのは最低限の設備で良くなる。
- キャッシュサーバーの無限大のキャパシティーを利用するため、設備増設自体が必要なくなる。
- エンドユーザーになるべく近いキャッシュサーバーが自動で選択されるため、海外ユーザーの表示速度が格段に上がる。
- DDoS攻撃で大量にアクセスがあっても、接続先はキャッシュサーバーのため、被害は最小限に留められる。

NTTコミュニケーションズでは、「コンテンツデリバリーネットワークサービス」のプランの1つである「プラン2［セキュリティソリューション］」において、DDoS攻撃対策にも有効なCDN環境を提供しています。これを利用することでWebサーバーにおけるセキュリティ対策を強化できるほか、世界各国に配備されたキャッシュサーバーを利用することでレスポンスの改善も図れます。グローバル全体でのWebプラットフォームとして利用すれば、各国で個別に運用していたWebサーバーを集約し、コストの最適化を実現するといったことも視野に入ります。

このように、CDNはWebサイトの運営においてさまざまなメリットをもたらします。DDoS攻撃の不安を払拭したい、あるいはWebサーバーの運用が負担となっているといった課題を抱えているのであれば、CDNは有効なソリューションとなります。