DDoS攻撃への対策について（概要）

警察庁 National Police Agency　NISC

> ➢ **DDoS攻撃とは、攻撃者などが不正に操作した多数のパソコンなどから、攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃。**

●最近のDDoS攻撃に見られる特徴と対策

【特徴】

■ 攻撃元IPアドレス

攻撃元となるIPアドレスは、**約99%が海外に割り当てられたIPアドレス**
（約１%の国内IPアドレスは警察において対策を実施。）

■ 通信量の増加程度

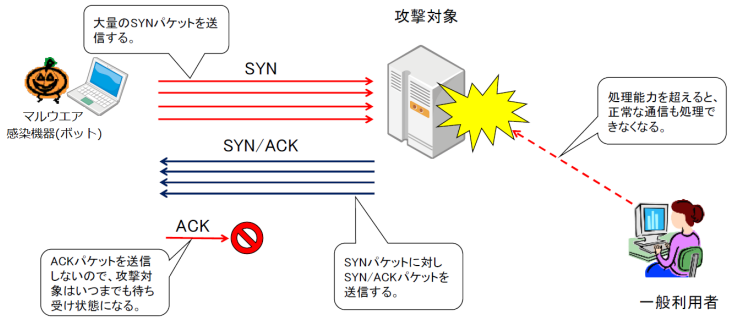
最大で100Gbps程度の通信量の増加が確認。

■ DDoS攻撃の手口（主なもの）

・TCP（SYN）フラッド
TCPの接続要求を行うSYNパケットのみを大量に送りつけて放置し「応答待ち状態」を大量に作り出す攻撃。

・HTTPフラッド
標的に（大量の）HTTPリクエスト（データ送信要求）を送りつける攻撃。

＜TCP(SYN) フラッド攻撃＞



このほか、Slow HTTP DoS攻撃※についても確認されているので注意が必要。

※　Slow HTTP DoS攻撃は、DoS攻撃の手口の一つであり、特定のTCPセッションを長期間継続することにより、Webサーバのセッションを占有してアクセスを妨害するもの。

【対策】

1　海外に割り当てられたIPアドレスからの通信の遮断
利用対象者が国内に限られるサイトの場合は、海外に割り当てられたIPアドレスからのアクセスを制限。

2　CDN、WAFの導入
CDNやWAFなどの通信量を制御するためのサービスを導入し、DDoS攻撃を防ぐため必要な設定を行う。

3　サーバ設定の見直し
同一IPアドレスからのアクセス回数を制限、タイムアウト設定を見直す。

●リスク低減に向けた取り組み

1　DDoS攻撃による被害を想定した対策

①　システムの重要度に基づく選別と分離

コストをかけてでも守る必要のあるサービスと、一定期間のダウンタイムを許容できるサービスを選別することで、それぞれの対応方針を策定するとともに、事業継続に重要なシステムは狙われやすいシステムとネットワークを分離することも検討する。

②　平常時からのトラフィックの監視

平常時のトラフィック状況を知っておくことで、異常なトラフィックを早期に発見できる。

③　異常通信時のアラートの設定

異常な通信が発生した際に、担当者にアラート通知が送られるようにする。

④　ソーリーページ等の設定

サイトの接続が困難、若しくは不能となった時に、別サーバに準備したソーリーページが表示されるよう設定する。

⑤　通報先・連絡先一覧作成など発生時の対策マニュアルの策定

警察や関係行政機関等の通報先についてまとめておくとともに、サーバやインターネット回線が使用不能となった場合の代替手段の確保など、対策マニュアルや業務継続計画を策定する。

⑥　プロバイダ側での対策可否の検討

利用している通信事業者の提供しているサービスについて、インターネット上流で通信流量抑制が可能かどうかを確認するとともに、通信事業者が提供するDDoS防御サービスへの加入も検討する。

2　DDoS攻撃への加担（踏み台）を防ぐ対策

①　オープン・リゾルバ対策

管理しているDNSサーバで、外部の不特定のIPアドレスからの再帰的な問い合わせを許可しない設定にする。

②　セキュリティパッチの適用

ベンダーから提供されるOSやアプリケーションの脆弱性を解消するための追加プログラムを適用する。

③　フィルタリングの設定

自組織から送信元IPアドレスを詐称したパケットが送信されないようフィルタリング設定を見直す。

<u>オープン・リゾルバを悪用した攻撃</u>