令和５年５月１日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

DDoS 攻撃への対策について

DDoS 攻撃への対策について、各事業者において、これまでも様々な対策が講じられていることと思いますが、最近においても DDoS 攻撃による被害とみられるウェブサイトの閲覧障害が断続的に発生しており、引き続き対策が必要な状況にあります。

警察では、昨年９月における DDoS 攻撃の発生状況について下記のとおり分析しているところ、各事業者におかれましては、本分析結果を参考に、リスク低減に向けて適切にセキュリティ対策を講じていただくようお願いいたします。

【昨年９月に発生した一連の DDoS 攻撃の状況】

令和４年９月中、複数回にわたり、国内の政府関連や重要インフラ事業者などのウェブサイトに対する DDoS 攻撃が確認されました。この一連の攻撃について警察において分析した結果は以下のとおりとなっています。

□　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 アドレスであり、約１％の国内 IP アドレスについては、警察において対策を実施しています。

□　通信量の増加程度

DDoS 攻撃では断続的な通信量の増加が認められますが、一連の DDoS 攻撃においては、通信量の増加程度は、最も弱くて７Mbps 程度であり、最も強くて 100Gbps 程度の通信量の増加が確認されています。

□　DDoS 攻撃の手口

主に下記に挙げる３種類の DDoS 攻撃の手口が確認されています。

- 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
- UDP フラッド
  標的に偽の送信元 IP アドレスやランダムなポート番号を設定した UDP データグラムを大量に送りつける攻撃。攻撃元から直接攻撃する手法や、DNS キャッシュサーバの再帰的問い合わせ機能や NTP サーバへの時刻問い合わせ機能を悪用して、パケットを増幅させ、大量の DNS パケットを生成する手法も使われます。

なお、最近では Slow HTTP DoS 攻撃※についても確認されておりますので、こちらにも注意してください。

※　Slow HTTP DoS 攻撃は、DoS 攻撃の手口の一つであり、一般的な DoS 攻撃が大量のパケットを送信してネットワークの帯域やサーバの処理能力をひっ迫させるのに対し、本攻撃は、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です。

【リスク低減に向けたセキュリティ対策】

DDoS 攻撃への対策は、多くの費用と時間が必要なものもあり、また、全ての DDoS 攻撃を未然に防ぐことができるものではありません。しかし、上記のような DDoS 攻撃がなされた場合の備えとして、まずは下記事項を参照の上、各事業所で導入している機器やシステムの設定見直し及び脆弱性の有無の確認、ソフトウェアの更新など、身近な対策を進めてください。

１　DDoS 攻撃による被害を抑えるための対策

①　海外に割り当てられた IP アドレスからの通信の遮断

サービス対象者が国内に限られる Web 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する。

②　CDN、WAF の導入

CDN(Contents Delivery Network)や WAF(Web Application Firewall)などを導入し、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。

２　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、重要性に応じてシステムを分離することが可能か確認し、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ときに、SNS 等の媒体を利用して、サイト利用者に状況を通知する内容の投稿ができるように

するほか、別サーバに準備したソーリーページが表示されるように設定する。

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

DDoS 攻撃を受けた旨、警察や平素からやりとりのある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

通信事業者により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こと。

３　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。