令 和 ７ 年 ２ 月 ４ 日
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（注意喚起）

昨年12月から本年１月の年末年始にかけて、航空事業者・金融機関・通信事業者等に対するDDoS攻撃が相次いで発生しております。これらの攻撃はIoTボットネット等が用いられ、UDPフラッド攻撃やHTTPフラッド攻撃など、複数種類の攻撃が行われており、今後、大規模な攻撃が発生する可能性も否定できません。

各事業者におかれましては、これまでも様々なDDoS攻撃対策を講じられていることと思いますが、本紙も参考に、引き続きリスク低減に向けて適切な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。

また、各インターネット利用者におかれましては、ルータやIPカメラ等のいわゆるIoTデバイスがマルウェアに感染し、IoTボットネットに組み込まれてサイバー攻撃に加担することがないよう、これらのデバイスの設定やアップデートを適切に行っていただくようお願いいたします。

【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<u>以下の事項を参照の上、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。</u>

１ DDoS 攻撃による被害を抑えるための対策

① 海外等に割り当てられたIP アドレスからの通信の遮断

DDoS 攻撃はボットからの攻撃によって実施されることが多いため、ボットに感染している端末等が多い国やドメインからの通信を拒否することによってもDDoS 攻撃の影響を緩和することが可能であり、特に国内のみからアクセスを受ける情報システムであれば有効である。正規の通信への影響も考慮しつつ実施を検討する。また、同一のIPアドレスからのしきい値を超えた大量のリクエストを遮断する機能の利用についても検討する。

② DDoS攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入

WAF（Web Application Firewall）、IDS/IPS、UTM（Unified Threat Management）、DDoS 攻撃対策専用アプライアンス製品等を導入し、DDoS 攻撃を防ぐため必要な設定を行う。

③ コンテンツデリバリーネットワーク（CDN）サービスの利用

コンテンツデリバリーネットワーク（CDN）サービスを利用する場合は、元の配信コンテンツを格納しているオリジンサーバへ直接アクセスされることを防ぐため、オリジンサーバのIPアドレスを隠蔽する必要がある。

④ その他各種DDoS攻撃対策の利用

インターネットに接続している通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、DDoS 攻撃に係る通信の遮断等の対策を利用することも有用である。

⑤ サーバ装置、端末及び通信回線装置及び通信回線の冗長化

代替のものへの切替えについては、サービス不能攻撃の検知及び代替サーバ装置等への切替えが許容される時間内に行えるようにする必要がある。

⑥ サーバ等の設定の見直し

サーバ装置、端末及び通信回線装置について、DDoS攻撃に対抗するための機能（パケットフィルタリング機能、3-way handshake時のタイムアウトの短縮、各種Flood攻撃への防御、アプリケーションゲートウェイ機能）がある場合は、有効にすること。

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し、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その他の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及び監視記録の保存

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。また、監視記録の保存については、監視対象の状態は一定ではなく、変動することが一般的であり、監視対象の変動を把握するという目的に照らした上で保存期間を定め、一定期間保存する。

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 攻撃を受けた旨を連絡するため、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やユーザ向けのサービスが提供

不可となった場合のユーザへの周知手段の確保など、対策マニュアルや業務継続計画を策定する。

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。