滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R５年度 No. 5
今、注目のサイバーセキュリティに関する情報をお届けします。

DDos攻撃への対策について

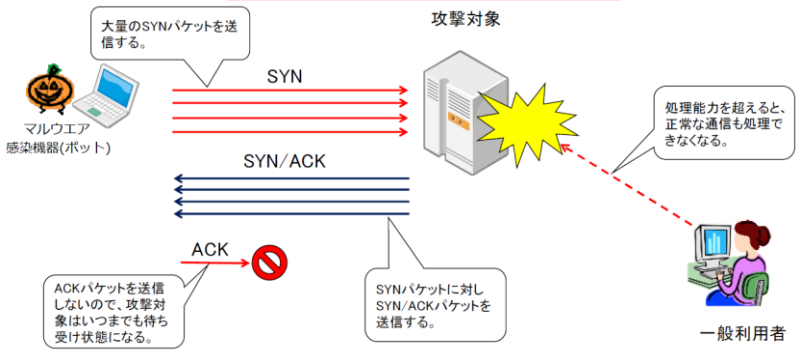
DDos攻撃とは

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

TCP(SYN)フラッド攻撃



★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。

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。

脆弱性無料点検実施中

※詳しくは
コネクトSHIG@No.1にて

«CS情報SHIG@»OSやアプリを最新のものに更新し、定期的にウイルスチェックしましょう。

滋賀県警察本部　サイバー犯罪対策課　警備第一課　077-522-1231(代表)詳細は県警webページで　→