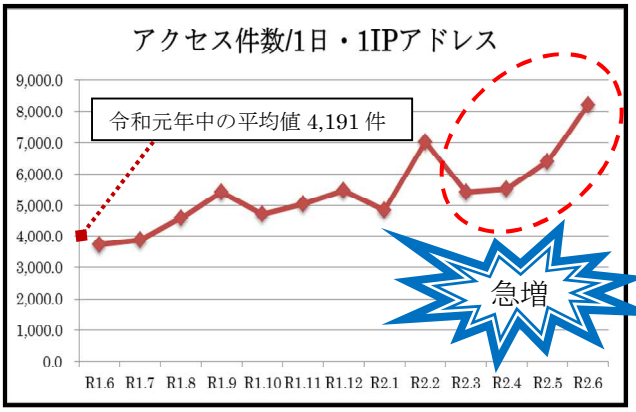
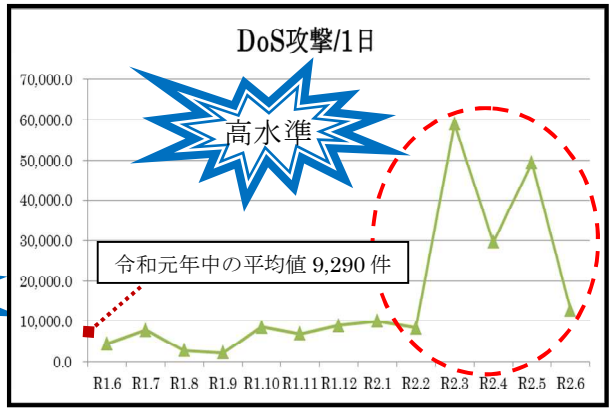
サイバーセキュリティの置き薬

2020 年
第 23 号

DoS攻撃が拡大しています！

警察庁がインターネットとの接続点で設置したセンサーの観測によると、攻撃と疑わしきアクセスが急増しています。また、その中で大量のデータを送りつけてサービス妨害を行う DoS 攻撃の検知数も非常に多い状況です。

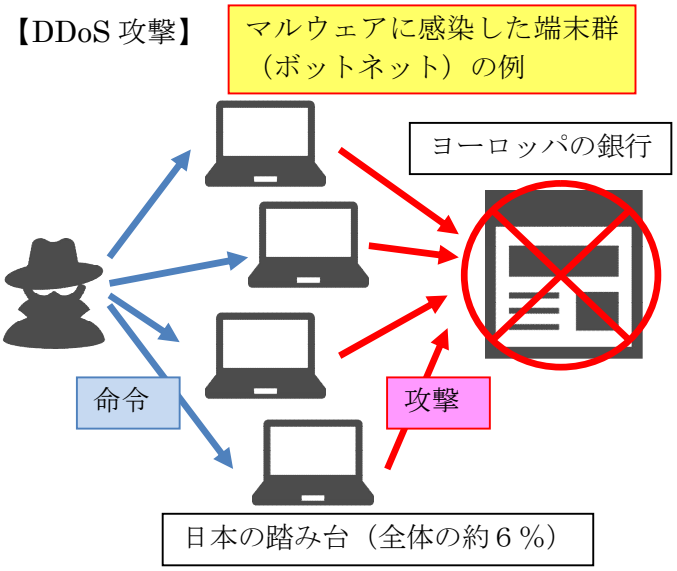




【参考】警察庁@police「平成 31 年 1 月期観測資料」～「令和 2 年 6 月期観測資料」
(https://www.npa.go.jp/cyberpolice/)

6月にはヨーロッパの大手銀行に過去最大規模の DDoS 攻撃（分散型の DoS 攻撃）が発生しました。攻撃のピーク時には1秒あたり8億 900 万パケットという大量の通信で、発信元は新たに観測された大量のボットネットからの通信でした。日本を発信元とする攻撃パケットは全体の約6%であり、国内の端末も踏み台として悪用されたと考えられます。

【DDoS 攻撃】



【対策】
- ○ OS やアプリケーションを最新化して脆弱性を塞ぐ。
- ○ セキュリティ対策ソフトを最新化して対応する。
- ○ 不審な IP アドレスからのアクセスを制限する。
- ○ CDN（コンテンツデリバリーネットワーク）でサーバ負荷を緩和する。
- ○ WAF（ウェブアプリケーションファイアウォール）で不審な通信を制限する。
- ○ 定期的に通信記録等を確認して不審な通信がないか確認する。

【参考】Akamai Japan Blog「パケット／秒ベースで史上最大規模の DDOS 攻撃を AKAMAI が緩和」
(https://blogs.akamai.com/jp/2020/07/)