

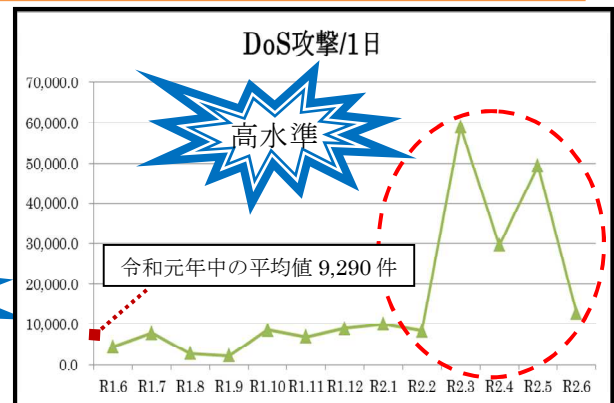
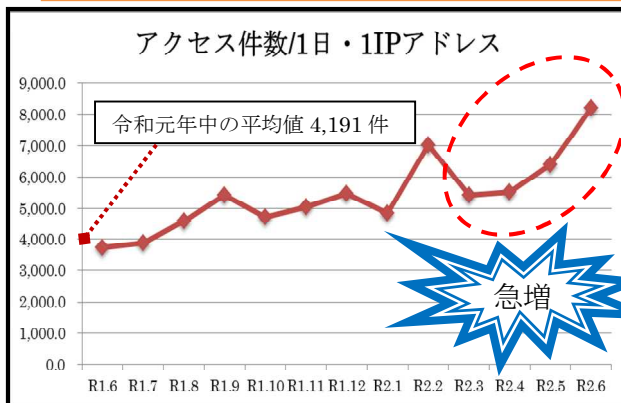


# サイバーセキュリティの置き薬

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。

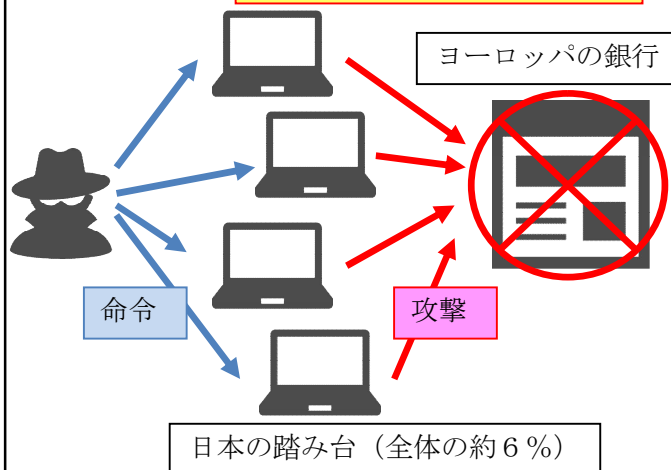


【参考】警察庁@police「平成31年1月期観測資料」～「令和2年6月期観測資料」  
(<https://www.npa.go.jp/cyberpolice/>)

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】

マルウェアに感染した端末群  
(ボットネット) の例



### 【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/>)