

令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について



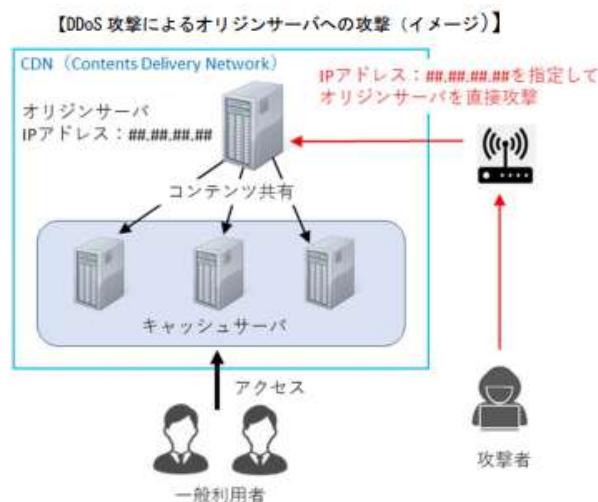
情勢と概況

政府機関、金融機関等の重要インフラ事業者等におけるDDoS攻撃とみられる被害や、ランサムウェア被害報告件数は高水準で推移しているが、サイバー攻撃を想定した業務継続計画（BCP）を整備済の組織は少ない。

重要インフラ事業者等に対するDDoS攻撃

● 攻撃事例

- DDoS攻撃に対し事業者が遮断措置を講じた場合でも、状況に応じて手口を変化させ、攻撃を継続する事例を確認した。
- IPアドレスを指定し、ウェブコンテンツのオリジナルデータが保存されているオリジンサーバを直接標的にすることで、アクセスの分散によって負荷軽減を実現しているCDN※を回避する攻撃が複数の事案で確認された。※Contents Delivery Network

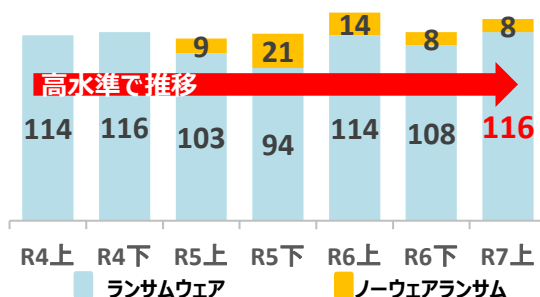


○ 対策

- オリジンサーバに対するCDNを経由しないアクセスの遮断
- 組織外にオリジンサーバのIPアドレスが露見しないようなDNS設定の見直し
- 海外に割り当てられたIPアドレスからの通信の遮断
- アクセスを監視し攻撃を検知・遮断する機能を持つような対策装置やサービスの導入
- サーバ装置、端末、通信回線装置及び通信回線の冗長化等 が求められる。

ランサムウェアの情勢

- 令和7年上半期に警察庁が把握したランサムウェア被害件数は、116件（前年比+2件）発生。
- 前年と同様に中小企業が狙われる状況が継続。
- RaaS による攻撃実行者の裾野の広がりが、対策が比較的手薄な中小企業の被害増加につながっていると考えられる。



サイバー攻撃を想定した業務継続計画（BCP）の推進

- ランサムウェア被害企業・団体のアンケート調査結果では、BCPを整備済の割合は6%だった。
- ランサムウェアによるデータ暗号化は、調査・復旧作業や広報のあり方も、災害時とは異なる対応が求められる。
- そのため、サイバー攻撃を想定したBCPを事前に準備しておくことが望ましい。
- ランサムウェア対策を紹介する政府広報啓発動画「中小企業で被害多数 ランサムウェア」



政府広報啓発動画

【参照】警察庁 広報資料「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

福岡県警察サイバー攻撃対策隊（公安第一課第七係）電話番号：092-641-4141（内線：5986）