サイバー攻撃対策通信
（令和７年第11号）

令和７年12月２日

福岡県警察

年末年始の情報セキュリティ対策について

長期休暇の時期は「システム担当者が長期間不在になる」等、普段とは異なる状況になるため、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまう可能性が高くなります。

利用者の方々にありましては、被害の発生防止に備え、年末年始の前後に以下のチェック項目を確認しましょう。

また、昨年末は複数分野においてDDoS攻撃が発生しております。システム管理者の方にありましては、裏面の【DDoS攻撃対策のお願い】をご確認いただき、同攻撃への備えを再確認いただくよう推奨いたします。

長期休暇前後のチェック項目

年末に確認

- □ **持出ルールの確認・遵守**
  パソコン等の機器やデータを持ち出す場合、ルールを確認しましょう。
- □ **使用しない機器の電源OFF**
  使用しないパソコン等の機器は電源をOFFにしましょう。
- □ **データの整理（不要データの削除、必要データのバックアップ）**
  ウイルス感染や紛失、盗難等によって情報漏洩等の被害が発生しないようにしましょう。

年始に確認

- □ **持ち出し機器のウイルスチェック**
  組織内で使用する前に必ず確認しましょう。
- □ **各種アップデートの実施**
  最新の修正プログラムを適用し、脆弱性等の改善を行いましょう。
- □ **不審メールへの対応**
  休暇中はもちろん、特に休暇明けの溜まったメール開封には注意しましょう。

困ったら、担当者に報告、連絡、相談しましょう！

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）

ＤＤｏＳ攻撃対策のお願い

警察庁
National Police Agency
令和7年12月

- 令和６年から７年の**年末年始**にかけ、交通・金融機関などの重要インフラ事業者において、**DDoS攻撃が相次いで発生**しました。
- これらの攻撃の特徴を基に、**対策をまとめました**ので確認をお願いします。

攻撃の特徴

- ✓ **長時間**にわたる攻撃＆**サービス提供に影響する部分**を集中的に狙う
- ✓ **オリジンサーバのIPアドレスを直接標的**にすることで、CDNを回避
- ✓ 対策の状況を観測し、**攻撃手法を変化**
- ✓ 最大で**220Gbps**の大規模なDDoS攻撃
- ✓ ぜい弱性を放置＆サポート切れの**無線ルータやIPカメラなどを踏み台**に利用

➡ **攻撃リスク低減＆攻撃を想定した対策が必要！！**

対策

※セキュリティ担当者の方向けの内容となります。

👉**アクセスを監視し攻撃を検知・遮断する機能を持つ対策装置**や**サービスの導入**

👉**各種機器の<u>DDoS攻撃対策の設定の再確認</u>**

- ・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DNS設定の見直し
- ・複数の対策による攻撃への耐性確認

👉**サーバ装置、端末、通信回線装置及び通信回線の<u>冗長化</u>**

👉**<u>本社・支社使用のIoT機器の再確認</u>（踏み台としての悪用防止）**

- ・ぜい弱性の解消のためのファームウェアの更新
- ・ぜい弱性の解消のためのパッチの適用
- ・サポート切れになっていないか等の再確認

DDoS攻撃が発生した場合に<u>警察への相談・通報ができるよう、あらかじめ攻撃発生時の対応要領やBCPの確認をお願いします。</u>

参考資料

サイバー警察局便り（R5 Vol.20 ）IoT機器への注意喚起【警察庁】
https://www.npa.go.jp/bureau/cyber/pdf/Vol.20cpal.pdf