サイバー攻撃対策通信

令和７年12月１日
令和７年度第８号
栃木県警察本部
警備部警備第一課
（サイバー対策センター）

DDoS攻撃へのセキュリティ対策

2024年から2025年の年末年始にかけ、航空事業者・金融機関・通信事業者等に対するDDoS攻撃によるとみられる被害が相次いで発生しました。
今後も年末年始に同種攻撃が発生する可能性は否定できません。
リスク低減に向けたセキュリティ対策をお願いいたします。

DDoS攻撃被害を抑える対策

☑ **まずは、取れる対策から進めていきましょう！！**

① **海外等に割り当てられたIPアドレスからの通信遮断**
世界各地のIoT機器を乗っ取り、標的事業者に大量のデータを送り付けていることが多いため、海外からの通信を拒否することにより緩和が可能

② **DDoS攻撃の影響を排除又は低減するための対策装置やサービスの導入**
WAF、IDS／IPS、UTM、DDoS攻撃対策専用アプライアンス製品等の導入

③ **CDNサービスの利用**
CDNサービスを利用する場合は、オリジンサーバのIPアドレスを隠匿する必要あり

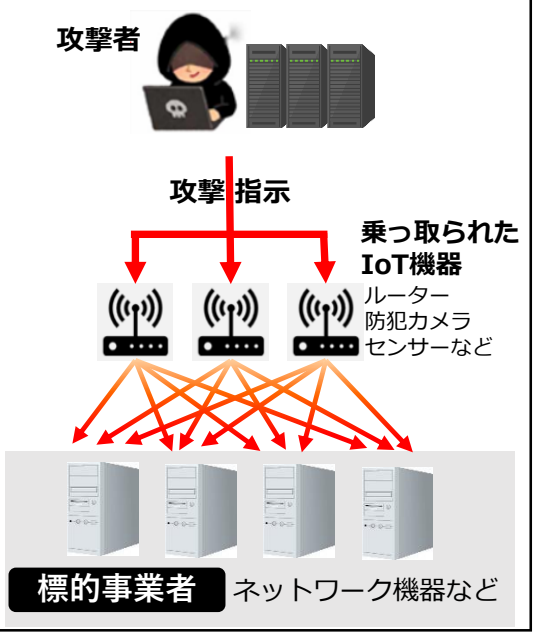
④ **サーバ、通信回線等の冗長化**
サービス継続のため機器等を複数準備

⑤ **サーバ等の設定の見直し**
サーバー、通信回線装置等の機能（パケットフィルタリング機能、3-way handshake時のタイムアウトの短縮、アプリケーションゲートウェイ機能等）を有効にする

DDoS攻撃被害を想定した対策

① **システム重要度に基づく選別と分離**
② **平常時からのトラフィック監視と記録の保存**
③ **異常通信時のアラート設定**
④ **ソーリーページ等の設定**
⑤ **被害発生時の対策マニュアル策定**

❒ **絨毯爆撃型DDoS攻撃**



年末年始に発生したDDoS攻撃は、「絨毯爆撃型」とみられています。
サイバー攻撃に加担することにならないよう、IoT機器の適切な設定やアップデートもお願いいたします。

栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER