滋賀県警察サイバーセキュリティ情報
R７年度 No.１３
サイバーコネクトSHIG@
今、注目のサイバーセキュリティに関する情報をお届けします。
Cyber connect shig@

年末年始のDDoS攻撃に御注意ください！！

令和６年末から令和７年初頭にかけて、通信、航空、金融機関といった重要インフラ事業者を対象としたＤＤｏＳ攻撃が発生しました。

これらの攻撃は、ＩｏＴボットネットなどが利用され、ＵＤＰフラッド攻撃やＨＴＴＰフラッド攻撃などの複数種類の攻撃が観測されており、今回も大規模な攻撃が発生する可能性が否定できません。

各事業者におかれましては、これまでも様々なサイバー攻撃対策を講じられておられることと思いますが、引き続き、リスク低減に向けて、適切なセキュリティ対策を講じていただきますようお願いいたします。

障害発生日	企業名	主な障害情報
R6.12.26	日本航空(JAL)	社外システムと通信しているシステムで不具合発生 自動チェックイン機が使用不可に
R6.12.29 R7.1.7	りそな銀行 関西みらい銀行など	「りそなグループアプリ」がつながりにくい現象発生
R7.1.2	ＮＴＴドコモ	「ｄメニュー」「ｇｏｏサービス」がつながりにくい
R7.1.5	日本気象協会	「ｔｅｎｋｉ．Ｊｐ」が利用しにくい状態に

攻撃の特徴

○　長時間に渡る攻撃と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（コンテンツデリバリーネットワーク）を回避する。
○　対策の状況を観測し、攻撃手法を変化させる。
○　最大で２２０Gbpsもの大規模なＤＤｏＳ攻撃を敢行。
○　脆弱性が放置されたり、サポート切れの無線ルータやＩＰカメラなどのＩｏＴ機器を踏み台（中継点）に利用する。

被害低減対策

○　ＤＤｏＳ攻撃対策の設定の再確認
・　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
・　一般にオリジンサーバのＩＰアドレスが露呈しないＤＮＳ設定の見直し
・　複数種類のサイバー攻撃に対する耐性確認
○　自組織におけるＩｏＴ機器の再点検（支店、関係先含む）
○　通信を監視し、攻撃を検知、遮断する機能を持つ機器やサービスの導入
○　サーバ、通信回線、通信機器の冗長化

あらかじめ、攻撃が発生した際の対応要領や事業継続計画の確認をお願いします。
実際に被害に遭われたり、予兆を検知した場合は、警察に御相談ください。

滋賀県警察本部　警備第一課　サイバー攻撃対策係　077-522-1231（代表）