サイバーセキュリティの置き薬

2023年
第9号

DDoS攻撃、ランサムウェア被害多発！セキュリティ対策を！

国内の事業者を狙ってDDoS（ディードス）攻撃が多発しています。

DDoS攻撃の一種として「DNSランダムサブドメイン攻撃」と呼ばれるものがあります。

「DNSランダムサブドメイン攻撃」とは、DNSの仕組みを悪用して、攻撃対象のドメイン名に対し、存在しないサブドメインを大量に生成した後、サブドメインの問合わせ要求処理をDNSサーバに行わせて応答不能にする攻撃のことです。

この攻撃が行われると、ウェブサイトが閲覧不能になるなどの被害を受け、運営するウェブサイトの種類によっては金銭的損失が発生します。

その他、富山県内の事業者において、ランサムウェア（身代金要求型不正プログラム）感染被害が発生しています。

事業の種類や規模に関係なく、セキュリティ対策の弱い事業者が狙われるため、これらの被害に遭わないよう下記対策を行いましょう。

被害に遭わないための対策

○　セキュリティ異常検知・遮断装置の導入、運用実施

CDN、WAF、DDoS攻撃検知対応のセキュリティ装置等を導入し、ネットワーク通信を監視して、異常を検知しましょう。

通信の異常検知時に遮断できる、運用担当者へ通知できる運用を行いましょう。

○　異常発生時の対策マニュアル等の整備

警察や平素から関係のある行政機関、保守業者等の連絡先をまとめ、異常時の対策マニュアルや業務継続計画（BCP）の整備、代替手段の確保を行いましょう。

○　DNSサーバのセキュリティ設定の見直し

外部の不特定のIPアドレスからの再帰的問い合わせに応答する（オープン・リゾルバ）設定を「許可しない」に設定しましょう。

○　セキュリティパッチの適用

ベンダーから提供されるOSやアプリケーションの脆弱性を解消するための追加プログラムを適用し、常に最新の状態にしましょう。

○　海外割当てのIPアドレスを遮断、フィルタリング設定の見直し

自組織の事業範囲を考慮し、海外対応が不要であれば、海外割当てのIPアドレスを遮断しましょう。

自組織から送信元IPアドレスを詐称したパケットが送信されないようフィルタリング設定を見直しましょう。

被害を受けた場合は、警察への通報をお願いします！

他の「置き薬」もご活用ください↓

【参考】
警察庁、内閣サイバーセキュリティセンター：DDoS攻撃への対策について
https://www.nisc.go.jp/pdf/press/20230501NISC_press.pdf
総務省：電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第二次とりまとめ
https://www.soumu.go.jp/main_content/000376396.pdf
警察庁：ランサムウェア被害防止対策
https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html