FUKUOKA POLICE 70th ANNIVERSARY

F－CSNET通信かわら版

令和６年8月 号外

VPN機器の脆弱性等を悪用した攻撃と対策

VPN機器の脆弱性や設定不備を悪用した攻撃により、本来権限を持たない第三者が不正なVPN接続をし、企業内のネットワークに侵入する不正アクセス事件が発生しています。
今一度、VPN機器のセキュリティ状況等を確認しましょう。

令和５年に都道府県警察から警察庁に報告された**ランサムウェア被害**においては、その感染経路のその**約６割が「VPN機器からの侵入」**となっています。

出典：警察庁広報資料　「令和５年におけるサイバー空間をめぐる脅威の情勢等について」

■ 被害防止・軽減対策 ■

VPN機器のファームウェアのバージョンが古い、テストアカウントを放置する等の理由による被害が確認されています！

- 重要！ VPN機器の脆弱性情報の把握、**ファームウェアのバージョンアップ**、修正プログラムの適用
- 重要！ 適切な認証管理（**テストアカウント等不要なアカウント削除**、多要素認証の導入、特定IPアドレスからのアクセス許可・拒否、認証試行回数の制限等）
- セキュリティ機器等による攻撃通信の監視と不審な通信の検知・遮断
- システム再構築に備えた適切なバックアップの取得
- BCP（事業継続計画）の策定とインシデント対処体制の確立

VPN機器に限らず、パソコンやサーバのOS、利用しているソフトウェア等はバージョンアップをして常に最新の状態に保ちましょう。

ランサムウェアや不正アクセス等のサイバー犯罪の被害に遭われた場合は、最寄りの警察署に通報・相談してください。

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、X（旧Twitter）やホームページに掲載していますので、ぜひご覧ください。

【X】（旧Twitter）　【ホームページ】