TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2023年 第10号

VPN機器、メールセキュリティ機器等の総点検を！

～インターネットへ通信できる全ての機器のOSやファームウェアを最新版にアップデートしましょう！～

VPNの仕組み等を利用して自宅、外出先の業務用パソコンから自組織内ネットワークへ接続して業務を行う働き方やメールの添付ファイルによるサイバー攻撃への対処能力を高めるためのネットワークセキュリティ機器の導入が定着する一方、このような**機器のぜい弱性が放置された結果、サイバー攻撃を受けて業務停止や経済的損害を被る事案が後を絶ちません。**

警察庁は、サイバー攻撃被害の一例として、ランサムウェア(身代金要求型ウイルス)被害に遭った場合の業務停止期間と業務復旧費用等を含めた被害額を公表しており、**業務停止は概ね1か月、被害額は概ね1000万円**となっています。

サイバー攻撃を受けた原因の過半数が、**VPN機器等ネットワークセキュリティ機器のぜい弱性を放置したこと**です。

以下の対策を行って、自組織を守りましょう。

被害に遭わないための対策

○　使用機器のOS、ファームウェア更新情報の把握

ネットワークセキュリティ機器のメーカー(Fortinet(フォーティネット)、Cisco(シスコ)等)では、機器を稼働させるために利用するOSやファームウェア(基本ソフトウェア)の危険なぜい弱性(CVE-2023-27997、CVE-2023-20008、CVE-2023-20044)を修正した最新版のソフトウェアをメーカーホームページで配布しています。

最新版のソフトウェアを確認し、インストールしましょう。

また、Barracuda(バラクーダ)製のメールセキュリティ機器「Barracuda ESG」は、危険なぜい弱性(CVE-2023-2868)の対応として機器本体を交換するよう通知しているので、直ちに交換しましょう。

○　使用機器で動作するソフトウェアぜい弱性情報、サイバー攻撃の手口に関する情報収集を行う

JPCERT/CC、情報処理推進機構(IPA)等、セキュリティ関連のウェブサイトやニュース等を参照し、平素からぜい弱性情報やサイバー攻撃の手口に関して情報収集に努め、対処すべき情報があれば適宜対応しましょう。

被害を受けた場合は、警察への通報をお願いします！

【参考】
警察庁：令和4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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
内閣サイバーセキュリティセンター(NISC)：インターネットの安全・安心ハンドブック Ver5.00
https://security-portal.nisc.go.jp/guidance/pdf/handbook/handbook-all.pdf
情報処理推進機構(IPA)：情報セキュリティ5か条
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055516.pdf
JPCERT/CC
https://www.jpcert.or.jp

他の「置き薬」もご活用ください↓

サイバー犯罪注意喚起動画↓