Ksisnetだより

発行:Ksisnet事務局
令和4年8月23日
Vol.109

VPN機器を悪用した不正アクセスに注意！！

定期的にネットワーク機器のアップデートを行ってください

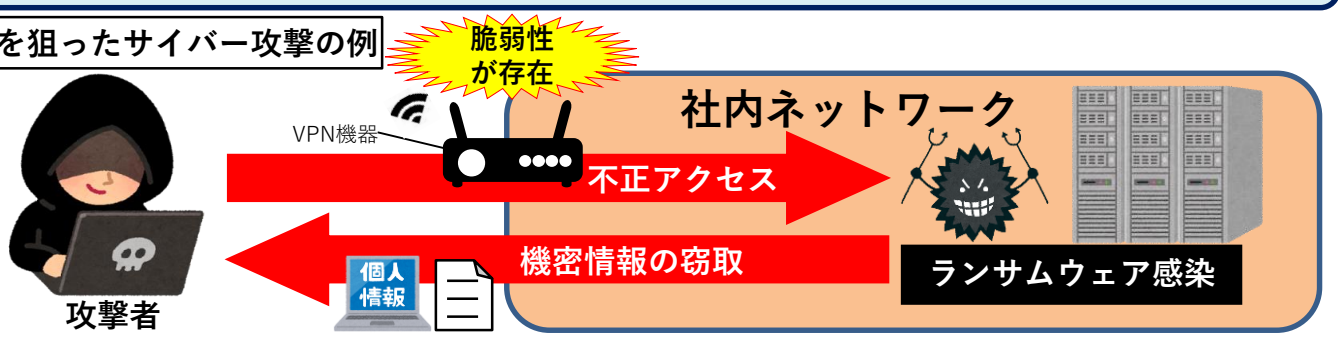
近年、組織の積極的なテレワークへの移行に伴い、自宅等からＶＰＮ経由で内部ネットワークにアクセスしたり、ウェブ会議サービスを利用して会議を行ったりする機会が増えています。

しかし、**ＶＰＮ機器の脆弱性を放置すれば、攻撃者に社内ネットワークに侵入され、ランサムウェアなどの不正プログラムに感染し、重要データが暗号化されたり、機密情報を窃取されてしまう可能性があります。**

まずは、インターネット機器のソフトウェアのバージョンを確認し、定期的な脆弱性診断を行い、アップデートを実行するなど対策強化をしてください。

※VPN･･･ネットワーク上に仮想の専用線を実現する技術（仮想プライベートネットワーク）

VPNを狙ったサイバー攻撃の例



全国的に、VPN機器から内部ネットワークに侵入され、ランサムウェアに感染する被害が多発しています。

【被害の予防（個人・組織）】

○ 最新アップデート（修正プログラム）の適用

・開発元から公開されている修正プログラムを適用し、脆弱性を修正しましょう。

○ 脆弱性関連情報の収集と対応

・常日ごろから情報セキュリティに関するニュースに関心を持ち、脆弱性が発表された場合は速やかに対応しましょう。

○ 多要素認証の実装

・ID・パスワード認証以外に、複数の認証を取り入れましょう。

○ ネットワークの監視および攻撃通信の遮断

・攻撃の疑いがある場合は、ファイアウォール等により通信遮断をしましょう。

○ セキュリティのサポートが充実しているソフトウェアを使う

・パッチの提供が早い等のサポートが充実したものを選びましょう。
・サポートの終了した製品の使用は避けましょう。

○ 一時的なサーバの停止

・すぐに修正プログラムが適用できない場合、一時的にサーバを停止してください。

参考　ＩＰＡ（情報処理推進機構）