



VPNのパスワードが流出！

テレワークに欠かせない技術の一つVPN（仮想私設網）。比較的低コストで安全な通信が確立できるとして、社外に持ち出したPCや自宅のPC等を組織内部のネットワークに安全に接続させるための手段として定着していますが、複数の企業において、このVPNのパスワードが流出しているとの報道がなされました。

今回は、VPN機器の脆弱性を突いた攻撃により、暗証番号が流出したと考えられているようですが、たとえ修正プログラムを適用していたとしても、リスクはゼロにはなりません。社内システムに一度侵入されれば、重要機密情報が筒抜けになる可能性もあります。

最近では、システムに侵入されることを前提とした「ゼロトラスト」という対応が主流になりつつあるようです。生体認証などと組み合わせて本人確認を行う多要素認証の導入など、社内のセキュリティ対策が現在のままでいいのかを検討してみてもいいのではないでしょうか。

○ VPNとは？

Virtual Private Networkの頭文字を取った用語で、インターネット上に仮想の専用線を設定し、特定の人のみが利用できる専用ネットワークです。

低コストで実現可能で、比較的安全に通信を行うことができますが、情報漏洩のリスクはゼロにはなりません。

○ ゼロトラストネットワークとは？

「社内は安全である」という前提で境界を守る「ファイアウォール」や「VPN」というセキュリティ対策ではなく、「全て（内部・外部問わず全てのトラフィック）が信用できない（ゼロトラスト）ことを前提として、ユーザーがアプリケーションやサービスにアクセスする都度認証することで脅威を防ぐ」という考え方です。

Microsoft製品の脆弱性対策について



今年8月、マイクロソフト社は、マイクロソフト製品に関する脆弱性の修正プログラムを公表しています。

これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生するおそれがあります。

これらの脆弱性については、「Windows 8.1」や「Windows Server 2012 R2」も影響を受けるそうなので、早急に修正プログラムを適用してください！

長崎県警察本部サイバー犯罪対策課
095-820-0110 (3451・3452)
メール e103108@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！
友だち登録お願いします！

@387ojopi

