作成　令和３年１月１４日

【F-CSNET 通信かわら版】
【表題：セキュリティ対策は「導入」＝「対策完了」ではない！】

中小事業者の皆様へ

１　「VPN」サービスを導入してテレワークを安全に

テレワークの普及により、通信データの暗号化等によって自宅や外出先等からでも会社の内部ネットワークに安全にアクセスすることを可能とするサービス「VPN」（ヴァーチャル・プライベート・ネットワーク、仮想施設網）に注目が集まりました。

２　「VPN」を利用すれば絶対安全？

一方、この「VPN」について、様々な製品で「ぜい弱性」に関する情報が公開されています。ぜい弱性情報の中には、「VPN の認証情報（パスワード等）」を第三者が取得可能となるものも含まれています。

つまり、このぜい弱性を悪用することにより、会社内部のシステムに侵入し、重要な情報を盗み取ることが可能となります。

３　ポイントは「ぜい弱性」を知り、必要な「手当て」を行うこと

どのような製品でも「ぜい弱性」は存在し得ます。ぜい弱性は、製品やサービスがリリースされた後に判明するものです。

「ぜい弱性」をメーカーが公表する場合その多くで「パッチ」（更新プログラム）が同時発表されます。

重要なのは、自社（個人）が利用している製品やサービスに関する「ぜい弱性」の存在を知り、早期に更新プログラムを実行して機器やサービスを最新の状態に保つということです。

４　セキュリティ対策は「導入」が「対策完了」ではない

これは、VPN サービスに限らず、あらゆる製品・サービスで同じことが言えます。

セキュリティ対策のために何か新しい製品・サービスを導入することは重要ですが、それまでに利用しているものが最新の状態であるか、会社全体、各個人（テレワークに使用する自宅のパソコンなども含めて）が確実に実施し、その習慣をつけることが重要といえます。

★　F-CSNET は、公的機関（九州経済産業局地域経済部情報政策課、福岡県警察本部生活

安全部サイバー犯罪対策課、福岡県商工部中小企業振興課）と、４つの中小事業者支援団体とが連携し、県内中小事業者を対象に、サイバー犯罪の被害防止等に的確に対応することを目的として発足したネットワークです。

★　福岡県警察サイバー犯罪対策課では、随時情報をホームページに掲載していますので、是非ご覧ください。

https://www.police.pref.fukuoka.jp/seian/cyber/index.html