セキュリティ脅威を招く落とし穴（第8回）

VPN自体に意外な“セキュリティリスク”も？

2022.12.16

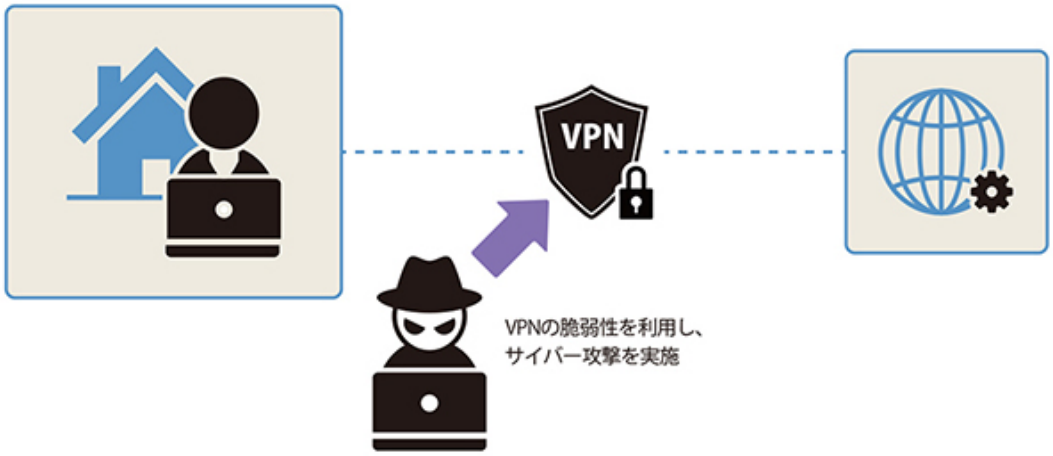
コロナ禍で外出が制限されることで生活や働き方は大きく変わった。その中でも最も大きな変化はそれまで一部の人のものとされていたテレワーク・リモートワークを多くの人が経験したことだろう。「オフィスに行かなければ無理」と思われていた業務なども在宅環境で行えるという認識が広まりつつある。一方で、インターネットに接続して仕事をすることで、サイバー攻撃を受ける可能性も高まっている。それらの回避方法として注目されるVPNだが、落とし穴はないのだろうか。

“VPNがあれば万全”というわけではない

VPNとは「Vutual Private Network」の略称で「仮想専用線」と呼ばれるものだ。イメージとしてはネットワーク上に仮想のトンネルを設け、特定の利用者だけが利用できるようにしている状態を指している。あくまでも仮想的に作られた専用線なので、物理的な専用線と比較してコストが安価で、柔軟性も高い。専用のトンネルを使い、通信内容も暗号化することでセキュリティレベルも高いレベルを保持できる。

不特定多数が利用するインターネットに比べて安全性が高く、コロナ禍でテレワーク・リモートワークが一気に普及する中で、通信の安全性を高めるためのもっとも身近な方法として多くの企業がこのVPNを導入するようになった。使い方も簡単で利用するシステムにより異なるが、例えば接続したい拠点に専用ルーターを設置しておき、ネットワーク接続設定からVPNの追加を選択してサーバー名やアカウント名、パスワードなどを入力しておくことで設定できる。

しかし、セキュリティ上のリスクも指摘されている。利用者が公衆回線網などから接続してしまうことでVPNの認証情報が盗み取られてしまったり、VPN機器自体の脆弱性が狙われたりすることもある。



総合的なセキュリティ対策が急務に… 続きを読む