ITで働き方を変える（第6回）

安全なテレワーク実現。VPN構築法

2020.05.20

テレワークを成功させるポイントは、情報セキュリティの扱いだ。従業員の自宅やサテライトオフィスなど、ある程度決まった場所で働くケースでも、セキュリティの確保を考えなくてはならない。

在宅勤務最大の懸念は、通信環境のセキュリティ

自宅で在宅勤務したりサテライトオフィスで働いたりする際は、社内システムにもアクセスしたい。従業員の自宅やサテライトオフィスと、社内システムを接続する通信環境のセキュリティが脆弱だと、攻撃者から不正アクセスを受ければひとたまりもない。データが盗まれたり、盗聴・改ざんの被害に遭ったりする。

こうしたリスクを減らす方法の1つが、自宅やサテライトオフィスと社内システムとの間でやり取りするデータの暗号化だ。通信時の安全性を確保したネットワークを構築する方法は、少し前までは“専用線”を用意して、他者からのアクセスを遮断していた。しかし、それには多額の費用がかかる。今、一般的なのがVPN（Virtual Private Network：仮想閉域網）の活用だ。

VPNとは、インターネットや通信事業者の通信網に仮想の専用線を設定し、他者からのアクセスを遮断するネットワークだ。通信事業者などが、顧客企業ごとにVPNが構築できるIP-VPNサービスを提供している。こうしたサービスを活用するには、サービスを提供する通信事業者との契約と、本社・拠点や在宅勤務を行う従業員の自宅やサテライトオフィスをIP-VPNサービスにつなぐアクセス回線（フレッツ網など）が必要になる。だが、費用は専用線よりも格段に安い。

IP-VPNを導入した場合、もう1つメリットがある。本社と支社といった拠点間においては、通信事業者のアクセス回線を収容する回線終端装置と企業側のルーターを接続することで、インターネットを介さずに閉域のIP網で各拠点を接続できる。セキュアな通信が可能になるわけだ。

手軽に導入できるIP-VPNサービス… 続きを読む