企業のネットワーク管理（第7回）

ネットワークの要となるルーターの運用をおまかせ

2021.03.08

テレワークでは、従業員は自宅の端末からインターネットを介して社内ネットワークに接続し業務を行う。インターネットは手軽に利用できるものの、悪意のある第三者からデータを盗聴されたり、不正アクセスされたりする危険が付きまとう。データを暗号化せずに送受信するのは非常に危険だ。では、どうすれば安全に通信ができるのか。その解決策の1つに、VPN（仮想閉域網）の利用という方法がある。

安全にデータ通信できるVPNの利用が拡大

安全に通信を行う方法の1つとして知られる専用線サービス。これは専用の回線使用により、高いセキュリティや安定した通信を可能にするものだ。だが、大容量データをやり取りするには通信コストが割高になる場合がある。

一方VPNは、インターネット上に仮想的な閉域網（閉じたネットワーク）を設け、あたかも企業専用ネットワークのように安全に通信ができるというものだ。回線の混雑時には通信速度が低下する場合があるものの、インターネットや通信事業者のIPネットワークなどを利用するため、低コストで大容量のデータをやり取りできる利点がある（VPNには、インターネットを利用する「インターネットVPN」と、通信事業者が提供する「IP-VPN」サービスなどがある）。

テレワークにおいても安全かつ手軽に利用できるインターネットVPNは、認証やデータ暗号化技術を用いてデータ送受信を行う。自宅から会社のネットワークに通信する手段として導入が進んでいる。

テレワーク時にインターネットVPNを利用するには、従業員のパソコンにインストールするVPNクライアントソフトが必要になる。VPNクライアントソフトは、Windows 10が標準機能として搭載するほか、ルーター機器メーカーも独自のクライアントソフトウエアを提供する。VPNの同時接続数は、VPNルーターのタイプによって異なる。従業員数や使用度合いに応じて選択するといいだろう。

他方、通信事業者が提供するIP-VPNサービスは、インターネットを介さず閉域のIPネットワーク上で、特定の拠点間のみ安全に接続できる。本社と支社・営業所などの各拠点にVPNルーターを設置。各拠点の従業員は本社のファイルサーバーや業務システムにアクセスしたり、本社のVPNルーターを経由してインターネット上のクラウドサービスを利用したりできる。本社側のルーターは各拠点の通信が集中することから、各拠点のVPNルーターより高性能な機器が必要となる場合もある。

「ルーターおまかせプラン」でルーターの障害をサポート… 続きを読む