基本のキ。セキュリティ入門（第5回）

テレワークで導入されるVPNとは？

2020.12.22

猛威を振るう新型コロナウイルスの影響を受け、多くの企業がテレワークの導入に迫られています。テレワークは、2019年に施行された働き方改革関連法により、新しい働き方を実現するための手段として積極的な導入が推奨され、社会的にも広がりを見せている勤務形態といえるでしょう。

そんなテレワークを実現するための手段の1つとして、VPNが注目されています。

そもそもVPNがどのようなものか分からないという方も多いのではないでしょうか。そこで今回は、テレワークの実現のために導入されるVPNの概要や仕組み、メリット・デメリットについて解説します。

テレワークで導入されるVPNとは？

はじめに、テレワークの概要と併せて、VPNについて詳しく見ていきます。

＜テレワークの概要＞
テレワークは、ICT（Information and Communication Technology ・情報通信技術）の利用により、時間や空間を有効に活用する多様な就労・作業形態をいいます。つまり、遠隔地から社内ネットワークに接続して仕事をすることです。

総務省の「テレワークセキュリティガイドライン 第4版」によると、テレワークには次の3つの形態が示されています。

・在宅勤務
自宅を就業場所として働く形態

・モバイルワーク

施設に依存せず、いつでも、どこでも仕事が可能な形態

・施設利用型勤務
サテライトオフィスなどの会社以外のオフィススペースを就業場所とする形態

これらの3つの作業形態を総称したものがテレワークです。

＜テレワークにおけるセキュリティの問題＞
テレワークは社外で仕事を行うため、従来よりもしっかりとしたセキュリティ対策が必要となります。社内だけで仕事をする場合と異なり、インターネットを介した社外からの通信が必要になるのをはじめ、従業員以外の第三者が立ち入る場所で作業を行うケースも考えられます。

十分なセキュリティ対策がなされていない場合には、社外から社内ネットワークへ不正アクセスされる、テレワークで利用する端末を盗み見られ情報漏えいする、といった可能性もあります。

テレワークにおけるセキュリティ確保には、システム的なセキュリティ対策だけでなく、ルールを策定して従業員一人ひとりのセキュリティ意識を高めてルールを順守してもらうことが重要になります。

＜VPNとは＞
テレワークを実現するための手段の1つであるVPNは、社外から社内ネットワークへの安全な経路を用意するための技術です。VPNは「Virtual Private Network」の略称で、日本語では「仮想専用線」になります。

VPNにはいくつか種類がありますが、多くの企業は、インターネット経由で社内ネットワークに接続する「インターネットVPN」を利用しています。

インターネットVPNではインターネット上に仮想的な専用線を作り出し、通信内容を暗号化しながら利用することが可能です。

イメージとしては、自宅から会社へインターネットを通じて仮想的なトンネルが構築され、そのトンネル内を通って社内パソコンや社内システムにアクセスできると考えるとよいでしょう。

通常は社外から社内ネットワークへ接続できませんが、VPNによる仮想的な専用線を作ることで社内ネットワークへの接続が可能になり、遠方にいても社内パソコンと同じように操作できます。

＜テレワークとVPNの関係性＞
ノートパソコンなどの端末を社外から利用し、社内ネットワークに接続して利用する際、安全な接続を確保するために利用される接続方式がVPNです。

テレワークを構築する代表的な方式としては、主に次の3つが考えられます。

・会社パソコン持ち帰り方式
オフィスの端末を持ち帰り、テレワーク端末として利用する方式

・リモートデスクトップ方式
オフィスにある端末を遠隔操作する方式

・シンクライアント方式
テレワーク端末上に電子データを保存しないで済むように運用する方式（リモートデスクトップ方式、仮想デスクトップ方式、クラウド型アプリ方式、セキュアブラウザ方式などを利用した場合）

テレワークで利用するVPNのメリットについて解説

テレワークでVPNを利用する際のメリットを大きく3つに分けて紹介します。

＜リモートで社内システムへアクセス可能＞
テレワークでは、インターネットを経由して社内ネットワークに接続する場合が多く、第三者から通信内容を盗み見られる可能性があります。VPNを利用すれば、情報の暗号化やトンネリング技術（※）によって、セキュリティ上、安全を確保しながらアクセスできます。
※トンネリング技術とは、拠点間で通信するために仮想的な通信路を作る技術

＜場所を問わずに社内ネットワークに接続できる＞
テレワークは多様な働き方を実現する手段であり、自宅やカフェなどの社外から仕事をできるようにするためのものです。例えば、出張先の海外から東京本社の社内ネットワークに接続したい場合などでも、VPNを利用すれば場所を問わずいつでも接続できます。

＜専用線に比べて導入コストが抑えられる＞
VPNは専用線に比べて、構築や維持にかかるコストを抑えられます。専用線は物理的な回線を用いて“1対1”の接続を行うため、大容量のデータを安全かつ安定的なやり取りができます。しかし、ネットワーク間の距離や接続数によってコストが変動し、接続する拠点との距離が長いほど、また、接続数が多いほどコストがかかります。

VPNはインターネットを活用した仮想的な専用線です。VPNは“多対1”の接続が可能であるうえ、専用線と同等の信頼性・安定性を保ったままの通信環境を構築できます。接続する拠点との距離や接続数によってコストも変動せず、専用線に比べてコストを抑えられます。

VPNのデメリットとは？テレワーク時に利用する際の注意点

テレワークを実現するために利用するVPNには、デメリットも存在します。VPNを導入する際に気をつけたい注意点と併せて、2つのデメリットを紹介します。

＜通信速度が低下する＞
VPNは、接続の際に暗号化やトンネリングなどの処理を行うため、通常の接続と比べて通信速度が低下する傾向があり、利用する回線速度によっても通信速度が遅くなる可能性があります。また、多くの人が同時に利用すると、VPN装置に負荷がかかり、通信速度が遅くなることもあります。実際に新型コロナウイルスの影響で急きょテレワークの実施に迫られた企業の中には、VPN装置への多大な負荷が原因で通信速度が低下して仕事ができない例もありました。

＜情報漏えいのリスクがある＞
VPNは通信経路上の安全を確保する技術ですが、完全なものではありません。インターネット環境を活用する以上、情報

漏えいのリスクは存在します。VPNの設定などに問題があった場合にも情報が漏えいするリスクがあります。テレワーク時にVPNを利用する際には、こうしたリスクがあることを注意しておきましょう。

テレワーク化のお困りには！NTT西日本の「フレッツ・SDx」

普及が進むテレワークを実現するための手段として、VPNを利用する企業は増えてきています。仮想的な専用線を構築するVPNは、社外から安全に社内ネットワークに接続するための通信経路を確保でき、テレワークの実現を後押しする技術です。

しかし、一方で通信速度の低下や情報漏えいのリスクがあり、利用する際にはしっかりとした環境の構築とセキュリティ対策が欠かせません。

実際にVPNを利用しており、次のような悩みを持つ方もいらっしゃるのではないでしょうか。

・拠点間の通信を遅延することなく、スムーズに実現したい
・機密情報などの大事な社内データをセキュアに確認したい
・人材不足の影響で拠点の通信ネットワークの管理、設定まで手が回らない
・OSのアップデート時期は通信が遅くなり、業務に支障が出る

そこでNTT西日本では、低遅延・高セキュリティなVPN通信を実現する「フレッツ・SDx」を提供しています。フレッツ・SDxはインターネットを介さない閉域網のIP-VPNであるため高セキュリティであり、フレッツ
光ネクストを利用した高速通信で映像データなどの大容量データも低遅延でリアルタイムに通信可能です。

加えて、コントローラーを通じて各拠点の機器を遠隔・自動設定可能。ネットワークの一括管理も行えます。働き方改革や新型コロナウイルスの影響によるテレワークの実現が迫られる今、テレワーク化にお困りの際にはお気軽にご相談ください。

※掲載している情報は、記事執筆時点のものです