安全なネットワーク接続を実現する「VPN」の仕組みとは

テレワークの急増で、自宅の通信環境のセキュリティ対策を行なう必要が出てきました。
通信内容を守る手段の１つであるVPNについて、その仕組みや導入方法を解説します。

株式会社ベロンパワークス
笠　木　渉　太

新型コロナウイルス感染症の流行にともない、テレワークを推進する企業が急速に増えています。テレワークの形式は複数ありますが、業務内容によっては自宅のPCから社内のサーバを操作するケースもあります。

しかし、多くの企業では情報漏洩のリスクを回避するため、社外のネットワークから社内のネットワークへアクセスできないような仕組みが取られています。そのため、会社のPCを持ち帰っただけではテレワークを行なえないケースもあるでしょう。

社外からのアクセスが認められたとしても、インターネットや公共のWi-Fiを通じて社内のネットワークへアクセスするのはセキュリティ上安全とはいえません。

インターネットは不特定多数のユーザーが利用しているため、悪意ある第三者にやりとりの内容を盗み見られる危険性があります。顧客データなど機密性の高い情報が漏洩してしまった場合、その損害は計り知れません。

生活様式が変わりつつある昨今、テレワークにおけるセキュリティ対策は急務といえます。

そこで注目されているのが、本稿で解説するVPNです。

ネットワーク同士を安全に繋ぐVPN

(1) 専用線と公衆回線の利点を併せ持つVPN

VPNは、「Virtual Private Network」の略称で、日本語では「仮想専用線」と言います。

専用線とは、２つの拠点間を１本に結んだように扱う専用の回線です。

接続された拠点同士の通信にのみ使用されるため、情報漏洩などのリスクは低くなります。一方で、敷設に時間がかかる、拠点間の距離に応じてコストが増すといった欠点がありました。

専用線に対し、インターネットのように多くのユーザーが共用する通信回線のことを、公衆回線と言います。

拠点間の通信でインターネットを利用すれば、専用線を敷設するよりもはるかにコストを抑えられます。しかし、前述のようにインターネットで情報をやりとりすると第三者によって内容を盗み取られる可能性が高くなります。

セキュリティ面を考えると、機

密情報をやりとりする業務には適切ではありません。

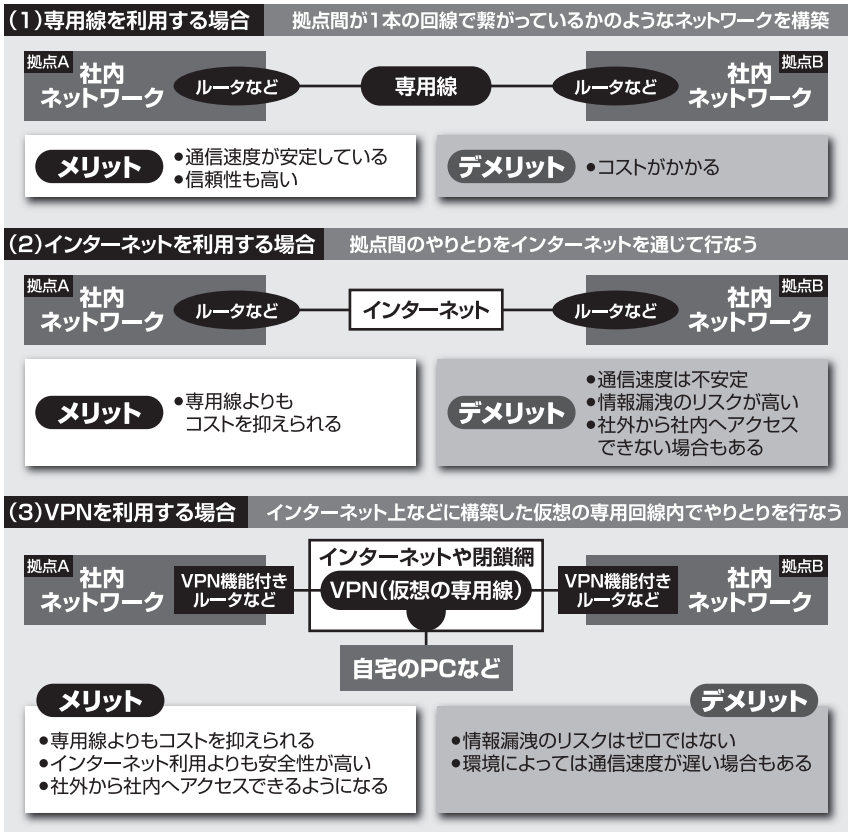
ＶＰＮは前述の専用線の安全性と、公衆回線のコストの低さを兼ね備えた仕組みといえます。

ＶＰＮでは暗号技術を利用し、インターネット上などに拠点間を結ぶ専用のネットワークを構築します。

これにより、離れた拠点同士があたかも１つのネットワークであるかのように扱われるため、部外者のアクセスを禁止しているネットワークにも社外からアクセスできるようになります。

さらにＶＰＮでは第三者から内容が見えないような処理を行なうため、セキュリティリスクも抑えられます。もちろん、安全性は専用線には劣りますが、圧倒的にコストを抑えたネットワークを構築できます（**図表１**）。

図表１　拠点間の通信の種類



(2) 拠点間ＶＰＮとリモートアクセスＶＰＮ

ＶＰＮを利用するには、拠点と拠点、あるいはユーザーと拠点それぞれにＶＰＮ対応の装置や端末が必要となります。拠点には、ＶＰＮ機能を持ったルータを設置するのが一般的です。ルータなどで拠点同士を接続するＶＰＮを、拠点間ＶＰＮと呼びます。

一方、ユーザーと拠点を接続するＶＰＮはリモートアクセスＶＰＮと呼びます。こちらの場合、装置を設置するのは拠点側だけになります。

ユーザー側は自分のＰＣやスマホに専用のソフトウェアをインストールしたり、環境を設定したりすることで拠点とＶＰＮ接続が行なえるようになります。

装置を設置する必要がなく手軽に導入できるため、テレワークではこちらの手法を採用している場合が多いようです。

(3) インターネットＶＰＮとＩＰ－ＶＰＮ

さらに、ＶＰＮはどのような環境で仮想専用線を構築するかによっても２つに分けられます。

１つめはインターネットＶＰＮです。これは、その名のとおりインターネット上に仮想専用線を構築するＶＰＮです。

前述したリモートアクセスＶＰＮはインターネットＶＰＮの一種といえます。インターネットＶＰＮでは、「トンネリング」「暗号化」「認証」といった３つの仕組みを用いて安全に情報をやりとりします。具体的には次のような処理が行なわれています。

トンネリングでは「カプセル化」という仕組みで自宅とオフィスなど、２つのネットワーク間を閉じられた仮想の回線で結びます。

あるネットワークから異なるネットワークへは、そのままの状態だとデータを送れないため、データを一旦カプセルのようなもので包みます。これがカプセル化です。

カプセル化により、２つの拠点はトンネルで繋がっているかのように扱われるため、前述したように自宅からでも、社内のサーバなどにアクセスできるようになるのです。

また、カプセル化を行なう際、第三者に情報を盗まれても内容が

わからないようにする暗号化や、別の人がデータを受け取ってしまわないようにする認証という処理も行なわれます。

インターネットVPNは、インターネットを利用しているのでコストを抑えることができますが、一方で通信が不安定になりやすいというデメリットがあります。

また、次に解説するIP-VPNと比較して、セキュリティリスクが高い点にも注意が必要です。

2つめのIP-VPNは、閉鎖網と呼ばれる、大手通信業者が用意した独自の回線上で仮想専用線を構築します。

閉鎖網は通信会社と契約しているユーザーのみが利用できるため、インターネットVPNよりも安全に、かつ安定した通信を行なうことが可能です。ただし、インターネットVPNと比べるとコストは高くなります。

VPNの導入方法

ここからは、実際にリモートアクセスVPNを利用して、テレワークを行なうための手順について見ていきます。

(1) VPN装置を用意する

社内にVPN装置がない場合は新たに用意が必要です。その際、機器の用意や設定を自社内で行なうのか、業者に依頼するのかを考慮する必要があります。

これらを自社内で行なう場合、ユーザー認証など複雑な作業を行なわなければなりません。

また、初期設定を誤ってしまうと安全性が保てなかったり、業務に支障が出たりする可能性もあります。

社内に専門知識を持った人材がいなければ、業者に依頼するのが無難でしょう。業者に構築を依頼した場合は、機器のレンタルや保守・運用の代行が可能になるといったメリットがあります。

実際にルータを購入、あるいは業者を選ぶ際は次の4つがポイントとなります。

① VPN対応ルータ

ルータのなかには、VPN機能が搭載されていないモデルも存在します。自社でルータを用意する際は、VPN機能が搭載されているかをチェックしましょう。

② VPNの方式

後述しますが、VPNの通信方式にはいくつかの種類がありますので、目的に合ったVPNが使用可能か確認しましょう。

③ QoS機能

ネットワーク上のサービスを安定して使えるようにするために、通信を調整する技術をQoS（Quality of Service）と言います。ルータにQoSが実装されていないと、アクセスが集中した際に通信が不安定になる可能性も考えられます。

多くのユーザーが同時にVPNルータを利用したり、大容量のデータを送受信したりする可能性がある場合は、QoSが搭載されていて十分な通信速度が保証されているかを確認しておきましょう。

④ セキュリティ機能

VPNルータは、いわばインターネットと社内ネットワークの関所です。通信内容は基本的にVPNによって保護されていますが、セキュリティホールを狙ったサイバー攻撃や情報漏洩のリスクはゼロではありません。

データの行き来を監視し、不正アクセスを未然に防ぐファイアウォールなどが搭載されたルータを選ぶと、よりセキュリティを高めることができます。

(2) 通信方法を決める

リモートアクセスVPNを利用する場合、暗号化方式を選ぶ必要があります。種類はいくつかありますが、ここでは代表的なIPsec-VPNとSSL-VPNについて紹介します（**図表2**）。

IPsec-VPNでは利用する端末に必ずIPsec-VPN用のソフトウェアをインストールする必要があります。ソフトウェアはアクセスするVPN機器と同製品でなくてはいけません。

また、端末によってはソフトウェアが対応していない場合もあります。端末ごとの環境設定も項目が多く、設定時のユーザーの負担は比較的大きいといえます。

一方のSSL-VPNはWEBブラウザを通じてVPNを行なうため、WEBに接続できる環境があれば基本的に専用ソフトウェアは必要ありません。

そのためユーザー側で行なう作業も少なく、スマホなど幅広い端末に対応しています。しかしIPsec-VPNよりも通信速度が遅く、セキュリティレベルも比較的低いという欠点があります。

業務上の注意点

VPNを利用したとしても、情報漏洩のリスクを完全になくすことは難しいでしょう。

たとえば、インターネットVPNでは暗号化によって通信内容を保護しますが、暗号化したデータそのものを取得される危険性があります。また、VPNの設定によってはセキュリティの穴が発生する場合も考えられます。

しかし、次のような注意点についてしっかり対策を取れば、セキュリティリスクをかなり抑えることができます。

■図表2　IPsec-VPNとSSL-VPNの特徴

IPsec-VPN	●ソフトウェアのインストールが必要 ●設定時のユーザーの負担が大きい ●通信速度が速い ●セキュリティレベルが高い
SSL-VPN	●専用のソフトウェアが不要 ●スマホなど幅広い端末に対応している ●通信速度が遅い ●セキュリティレベルが比較的低い

(1) 初期設定は慎重に

前述したようにVPN機器の初期設定に誤りがあると、外部からの不正な侵入を許したり社員がVPNにアクセスできなかったりする可能性があります。

社内でネットワークを設定する場合は脆弱性がないよう、慎重に行なわなければいけません。ネットワーク構築に詳しい人材が社内にいないのであれば、業者に設定を依頼しましょう。

(2) 業者の信頼性をチェックする

基本的に業者は利用者の通信ログなどについて「一切保持しない」と公表していますが、過去には業者から情報が流出した事例もありました。

業者が提供するIP-VPNやインターネットVPNサービスを利用する場合はその業者が本当に信頼できるかどうか、過去の実績などを元にチェックしましょう。

(3) PCのウイルス対策をする

テレワークを行なう場合は個人のPCのウイルス対策もしっかりしておきたいところです。

VPNをしっかり構築していても、使用するPCがウイルスに感染してしまったら重要な情報が第三者に筒抜けになってしまいます。テレワークなどで個人のPCを使用する際は、アンチウイルスソフトのインストールや信用できないサイトの閲覧禁止などを義務づける必要があります。

(4) 社員へのルールを徹底する

事前準備が不十分なまま、テレワークを導入した企業も少なくないでしょう。社員全体へVPNの使い方やルールの周知が徹底されていないケースもあるようです。

使い方がわからない社員は、誤ってVPN接続を行なわないまま機密情報をやりとりしてしまうかもしれません。マニュアルを作成する、勉強会を行なうなどの方法でVPNの使い方について共有しておくとよいでしょう。

(5) セキュリティプログラムは常に最新のものにする

VPNを導入している企業が増えたことにより、VPN機器の脆弱性を狙ったサイバー攻撃も増えています。

企業によってはVPNを利用して日が浅いこともあり、最新のセキュリティ更新プログラムを適用していないケースがあります。

セキュリティリスクを回避するためにも、メーカーから提供されるセキュリティプログラムは常に最新のバージョンに保っておくことが重要です。

(6) 通信が遅い場合もある

セキュリティの注意点ではありませんが、VPNは通信速度が遅い場合もあります。

とくにインターネットVPNは公衆回線を利用しているため、スピードが出ない、接続できないといったトラブルが発生する可能性もあるので注意しましょう。

(7) モバイル端末はバッテリー消費にも注意する

VPN利用中は暗号化を行なうため、通常よりも通信回数が増加します。

消費電力も増えるので、ノートPCなどで業務を行なっている場合はバッテリーの残量に気をつける必要があります。

テレワークは、自宅だけでなくカフェなどで業務をすることも考えられるので、電池切れに備えてモバイルバッテリーなどを用意しましょう。

かさぎ　しょうた　デジタルツール、マネー系メディアの編集・執筆業務を行なう株式会社ベロンパワークスで、フィンテックや資産運用、情報管理などを中心に、編集・ディレクター業務に携わる。