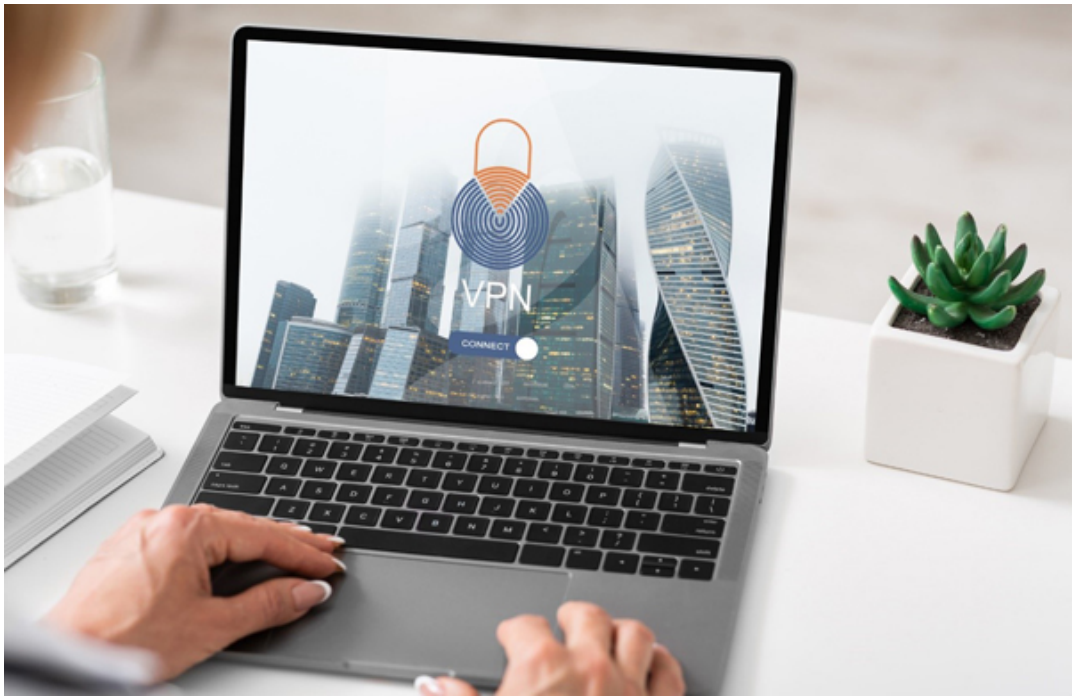
基本のキ。セキュリティ入門（第10回）

テレワークに利用されるVPNとは？仕組みについて

2021.03.15



近年、多くの企業でテレワークの導入が進められ、VPNについても耳にする機会が多くなってきているのではないでしょうか。テレワークを安全に実施するのに欠かせない存在であるVPNですが、その概要や仕組みについてよく分からない方も多いでしょう。

そこで今回は、VPNの概要や仕組みと併せて、VPNを利用する目的やメリット・デメリットなどについて解説します。

テレワークで導入されるVPNとは？

ここでは、VPNの概要や仕組みと併せて、テレワークについておさらいしましょう。

＜そもそもテレワークとは＞

テレワークは働く場所にとらわれない柔軟な働き方です。従来はオフィスで働くのが一般的でしたが、2019年に施行された働き方改革関連法や新型コロナウイルスの感染拡大によって従来型の働き方が見直されています。

テレワークは自宅やカフェなどで働けて、けがや妊娠・育児、家族の介護などの理由で従来通りの働き方が難しい人でも働き続けられます。さらに、オフィスコストの削減効果も期待でき、非常に注目されています。

＜VPNの概要と仕組み＞

そんなテレワークを安全に実施するために用いられる技術がVPNです。VPNはVirtual Private Networkの略称で、日本語で表すと仮想専用線となります。自宅やカフェなどから社内ネットワークに接続するには、インターネットを経由しなければなりません。しかし、インターネットは不特定多数の人が接続し、機密情報などをやり取りするのには不向きです。

そこで、VPNを使って仮想的な専用線を用意して安全な通信を実現します。VPNは「承認」「トンネリング」「暗号化」の3つの仕組みから成り立ちます。承認によって認められた人のみが利用できるようにし、トンネリングと暗号化によって拠点間の通信経路と安全性を確保しているのです。

さらに、VPNにはいくつか種類があります。「IPsec-VPN」と「SSL-VPN」は違いを覚えておくとよいでしょう。IPsec-VPNは本社と支店といった拠点をつなぐために用いられることの多いVPNで、高いセキュリティが特徴です。SSL-VPNは複雑な設定が不要でWebブラウザーから利用できるSSLを用いるVPNで、在宅勤務などにも対応しやすい点が特徴です。

テレワークにおいてVPNを導入する方法について

ここでは、VPNを導入する方法と併せて、それぞれのメリット・デメリットについて解説します。加えて、テレワークでVPNを導入する目的についても、もう少し詳しく見ていきましょう。

<そもそもVPNを導入する目的とは>

テレワークにおいてVPNを導入する目的は、「社内ネットワークへの通信経路を確保する」と「通信経路の安全を確保する」という2つの目的が挙げられます。

私たちが一般的に利用するネットワークとしては、インターネット・自宅のネットワーク・社内ネットワークの3つが挙げられるでしょう。自宅や社内ネットワークからインターネットに接続するのは可能ですが、自宅から社内ネットワークに接続することは原則できません。

なぜなら、それぞれが異なるネットワークで、セキュリティ対策として外部から社内ネットワークへの接続は禁止されていることがほとんどだからです。そのため、VPNを利用して仮想的な専用線を設け、自宅やカフェなどにいながら社内ネットワークに接続できるようにすることが目的の1つとなります。

加えてVPNは通信内容が暗号化され、インターネットの公共網に構築してもその内容を盗み見られにくくします。VPNを利用することで安全な通信経路を確保できるのです。

このような目的から、VPNはオフィス外から企業のサーバーへアクセスしたり、個人の端末と社内ネットワークをつなげたり、本社と支社とのデータのやり取りで利用されたりします。

<VPNの導入方法>

VPNを利用してテレワークを実現する比較的実現しやすい3つの方法を紹介します。

・持ち帰り方式
社内で利用するノートパソコンなどのモバイル端末を自宅に持ち帰ってVPNを利用する方法です。新規に端末を用意する

コストが削減できる点や、既存の環境をそのまま活用できる点がメリットとなります。その半面、データが端末に残ってしまうため情報漏えいのリスクが残る点がデメリットです。

・リモートデスクトップ方式
自宅のパソコンなどから会社のパソコンにリモートデスクトップで接続して利用する方式です。持ち帰り方式と同じように新規に端末を用意するコストが不要であり、既存の環境をそのまま活用できる点がメリットです。しかし、接続先の会社パソコンを常時起動させておく必要があり、自宅パソコンにデータが保存できる設定のまま利用すると情報漏えいのリスクが残る点がデメリットとして挙げられるでしょう。

・シンクライアント方式
端末にHDDなどの外部記憶媒体を持たないシンクライアント端末を利用する方式です。リモートデスクトップや仮想デスクトップに接続して利用するため、社外にデータを持ち出さずに業務が行えることから情報漏えい対策ができる点がメリットです。デメリットとしてシンクライアント端末の導入コストがかかる点が挙げられます。

テレワークにおけるVPN利用のメリットとデメリット

最後に、テレワークにおけるVPN利用のメリットとデメリットをまとめましたので、それぞれ見ていきましょう。VPN利用の際にはメリットだけでなくデメリットも十分に理解しておくことが重要です。

<VPN利用のメリット>
VPNを利用するメリットとしては、次の3点が挙げられます。

・安全な通信が可能
・遠隔地からでも操作できる
・モバイル端末からもアクセス可能

VPNは通信内容が暗号化され、遠隔地からでも安全に社内ネットワークに接続できます。加えて、VPNはあくまでも通信経路を安全に確保する技術なのでデバイスは問わず、モバイル端末でも利用可能です。

<VPN利用のデメリット>
反対にVPNを利用するデメリットとしては、次の3点が挙げられます。

・セキュリティリスク
・コストがかさむ場合がある
・通信速度の低下

VPNは安全に通信するための技術ですが、テレワークにおいてVPNさえ利用していれば完全に安全なわけではありません。2020年8月にはVPNを利用する日本企業38社が不正アクセスを受けた事例も報告されています。

この事例では特定のVPN装置の脆弱性が狙われ、VPN装置の管理がしっかりとできていなかったのが原因です。新たにVPNを導入する際は、セキュリティ管理すべき対象も増えセキュリティリスクが増加する点はデメリットといえるでしょう。

加えて、VPNの導入にかかるコストやVPN装置の管理コストがかさむことも考えられ、全体的な導入・維持コストが高くなりがちな点もデメリットです。

VPNの仕組み上、接続に関する手間が増えるためどうしても通信速度は通常の接続よりも遅くなります。この点もデメリットとして挙げられます。

テレワーク化のお困りには！NTT西日本の「フレッツ・SDx」

テレワーク導入の際には、VPNは欠かせない存在です。VPNは自宅と社内ネットワークなどの異なるネットワーク間を接続するのに必要な技術であり、安全な通信経路を確保できます。

このようなメリットがある半面、VPNだけでは対応できないセキュリティリスクの存在やコストがかさむ可能性がある点がデメリットです。

加えて、VPNはその性質上どうしても通常の通信よりも速度が低下してしまいがちです。そのため、こんなお悩みをお持ちの方もい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

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です。高セキュリティかつ、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。

また、コントローラーを通じて各拠点の機器を遠隔・自動設定可能で、ネットワーク管理も効率的に行えます。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方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