基本のキ。セキュリティ入門（第6回）

VPNのセキュリティ対策について徹底解説

2020.12.23

テレワークの普及が進む昨今、VPNを利用する企業も多くなってきました。VPN自体は昔からある技術ですが、テレワーク実現のために急きょVPNの利用を検討している方も多いのではないでしょうか。

「VPNは安全に通信できる」として多くの企業で利用されていますが、VPNにも情報セキュリティリスクは潜んでいます。適切な対策を講じなければ、セキュリティ事故につながる可能性も考えられます。

そこで今回は、VPNの情報セキュリティリスクについて解説し、安全に利用するための対策方法をご紹介します。

VPNとは？

はじめに、VPNの概要からその種類、仕組みを解説します。VPNに関する知識を付けて対策できるよう、1つずつ理解していきましょう。

＜VPNは仮想専用線＞

VPNはVirtual Private Networkの略称で、仮想専用線を意味します。セキュリティ上安全な経路を使ってデータのやり取りをしたい場合、専用のネットワークを仮想的に構築するので、物理的に専用線を用意するより低コストでの構築が可能です。

VPNは主に事業の拠点同士の接続や、遠隔地から社内ネットワークに安全に接続する目的で利用されます。最近ではテレワークを実現する手段として注目されています。

＜VPNの種類＞

VPNにはいくつか種類があります。ここでは大きく3つに分けて解説します。

・インターネットVPN
一般的な公衆回線を利用し、インターネット上に仮想専用線を設けるVPN。導入が容易で低コストですが、通信環境がインターネットの回線速度に依存します。

・IP-VPN（閉域網）
通信事業者が提供する閉域網を利用したVPN。インターネットは不特定多数が接続できますが、閉域網は限られた利用者のみが接続できる回線です。インターネットVPNよりも高セキュリティを実現でき、通信速度も安定しますがコストは高くなります。

・SSL-VPN
インターネットVPNの一種で、暗号化通信にSSLを利用します。SSLはWeb上の標準的な暗号化技術で、導入時のコストや環境構築の負担を最小限に抑えられます。テレワークでも設定しやすいVPNです。

＜VPNの仕組み＞
VPNの仕組みを簡単に説明すると、「トンネリング」「カプセル化」「認証」「暗号化」の4つの技術で構成されています。

トンネリングはVPNの根幹となる技術です。データの送信者と受信者の間に仮想的なトンネルを構築し、専用線に見せかけて外部からの侵入を防ぎます。

トンネル内を通るデータは、指定された受信者にのみ届くように“カプセル化”されます。カプセル化によって郵便物が荷造りされるように守られ、公衆回線を経由していても正しい宛先にデータを送信できます。

しかし、これだけではセキュリティ上安全とはいえません。VPNでは、なりすましやデータが盗まれるケースを想定して、認証というプロセスを設けています。身元証明のように、データの送信者と受信者が正規のアカウントであると確認することで、より安全な通信を実現しています。

さらに、VPNのトンネルに侵入された場合に備え、送受信しているデータに鍵をかけるのが暗号化です。通信内容を盗み見られたり、改ざんされたりするのを防ぎます。

このように、4つの技術を組み合わせることでVPNのセキュリティは保たれているのです。

VPNの情報セキュリティリスクについて解説

安全な通信を実現するVPNですが、情報セキュリティリスクがまったく存在しないわけではありません。VPNを利用するうえで注意すべき情報セキュリティリスクを解説します。

＜情報漏えいのリスク＞
VPNは安全な通信経路を構築するためのもので、通信経路外での情報セキュリティリスクに対しては安全性を保証できません。例えば、初期設定での誤操作や、テレワークで利用する端末上に社内データを保存したまま端末を紛失したり、盗まれたりしてしまうと、情報漏えいのリスクが高まります。

＜コスト重視による通信障害のリスク＞
VPNの中には無料や低価格のサービスが存在しますが、回線が混み合う時間帯に遅延が発生するなど、通信障害のリスクが高くなります。通信障害は業務の遂行に影響するため、企業にとって大きな損害になりかねません。企業でVPNを導入するなら、多少のコストがかかっても安定した通信環境を確保する必要があります。

＜ウイルス感染のリスク＞
VPNを利用すると、社外で利用する端末から社内ネットワークに接続できますが、端末のウイルス感染による社内ネットワークへの感染拡大は、リスクとして注意する必要があります。基本的にVPNにはウイルスを検出して排除する機能はなく、データの送信者と受信者それぞれでウイルスの感染対策が必要です。

＜通信履歴が漏れるリスク＞
VPNサービス事業者の中には、悪意を持った事業者が存在する可能性もあります。VPNの利用には事業者保有のVPNサーバーを経由しますが、一般的に事業者側はユーザーの通信履歴をログとして一切保持しません。ただし、悪意を持った事業者の場合は、通信履歴を取得し不正行為に利用する可能性があります。事業者の選定は慎重に行うことが重要です。

VPNを安全に利用するために情報セキュリティにおいてできること

VPNにも情報セキュリティリスクが潜んでいます。ここではVPNを安全に利用するための対策をご紹介します。

＜運用管理、保守方法をあらかじめ確認＞
VPNを安全に利用するための運用管理・保守方法は、事前にしっかりと計画することが重要です。例えば、VPNに接続する端末で利用可能なアプリケーションを制限したり、ウイルス対策ソフトを導入したりと、情報セキュリティリスクが発生しづらい環境を構築するとよいでしょう。他にも、リモート環境でVPNの設定がしやすい製品を選んだり、VPN装置の故障や問題が発生した際の対応手順をまとめたりするなど、導入前の準備がVPNを安全に利用するために重要となります。

＜社内のセキュリティ意識の向上＞
VPNは人が利用する以上、システム的な対策だけでなく人的な対策も必要です。VPNを利用すると遠隔地から社内ネットワークに接続するため、利用者を直接監視できません。VPNを安全に利用するには、利用者一人ひとりのセキュリティ意識の向上が不可欠です。VPNの導入・利用時には、利用者に対してセキュリティ教育を実施したり、利用時の安全マニュアルを作成して周知徹底したりするなどの対策を行いましょう。

＜エンドユーザーのパフォーマンスを確認＞
VPNを導入する際にコスト削減を重視し過ぎると、必要なパフォーマンスが発揮できない可能性があります。特に、通信速度が遅くなるとサービスの質を維持できず、エンドユーザーからのクレームにもつながります。あらかじめVPNの特性を理解したうえで適切な種類を選択し、動作の検証を行うなどの準備をしておきましょう。

＜端末の紛失・盗難時の対策＞
VPNに関わる情報漏えいで注意すべきなのは、利用端末の紛失・盗難時の対策です。効果的なのは、社内データや機密データを利用端末に保存できない仕組みの構築です。例えば、VPNで社内のパソコンを遠隔操作するリモートデスクトップの利用で、データを社外に持ち出さずに作業したり、必要最低限の機能だけを持つシンクライアント端末の利用で、端末にデータを残さないようにしたりするなどの対策が挙げられます。

テレワーク化のお困りには！NTT西日本の「フレッツ・SDx」

社外から社内ネットワークへの安全な通信を実現するVPNにも、情報セキュリティリスクは潜んでいます。VPNはトンネリング・カプセル化・認証・暗号化といった技術で構成され、通信経路上のセキュリティ対策は行えるものの、利用端末の紛失や

盗難による情報漏えい、ウイルス感染、通信履歴が漏れるリスクも考えられます。VPNを安全に利用するためには、運用管理・保守の計画や対策が欠かせません。

しかし、VPNのセキュリティ対策は管理者の負担や労力が大きく、適切な運用が難しいケースも少なくありません。こんな悩みをお持ちの方も多いのではないでしょうか。

・人材不足の影響で拠点の通信ネットワークの管理や設定まで手が回らない
・拠点間の通信でセキュリティを維持しつつ、遅延なくデータの受け渡しをしたい
・OSのアップデート時期は通信が一気に重くなるため業務に支障が出る

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のため、セキュアなネットワーク環境が構築でき、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通信可能です。

加えて、遠隔操作ができるコントローラーを通じて、各拠点の機器を自動設定でき、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