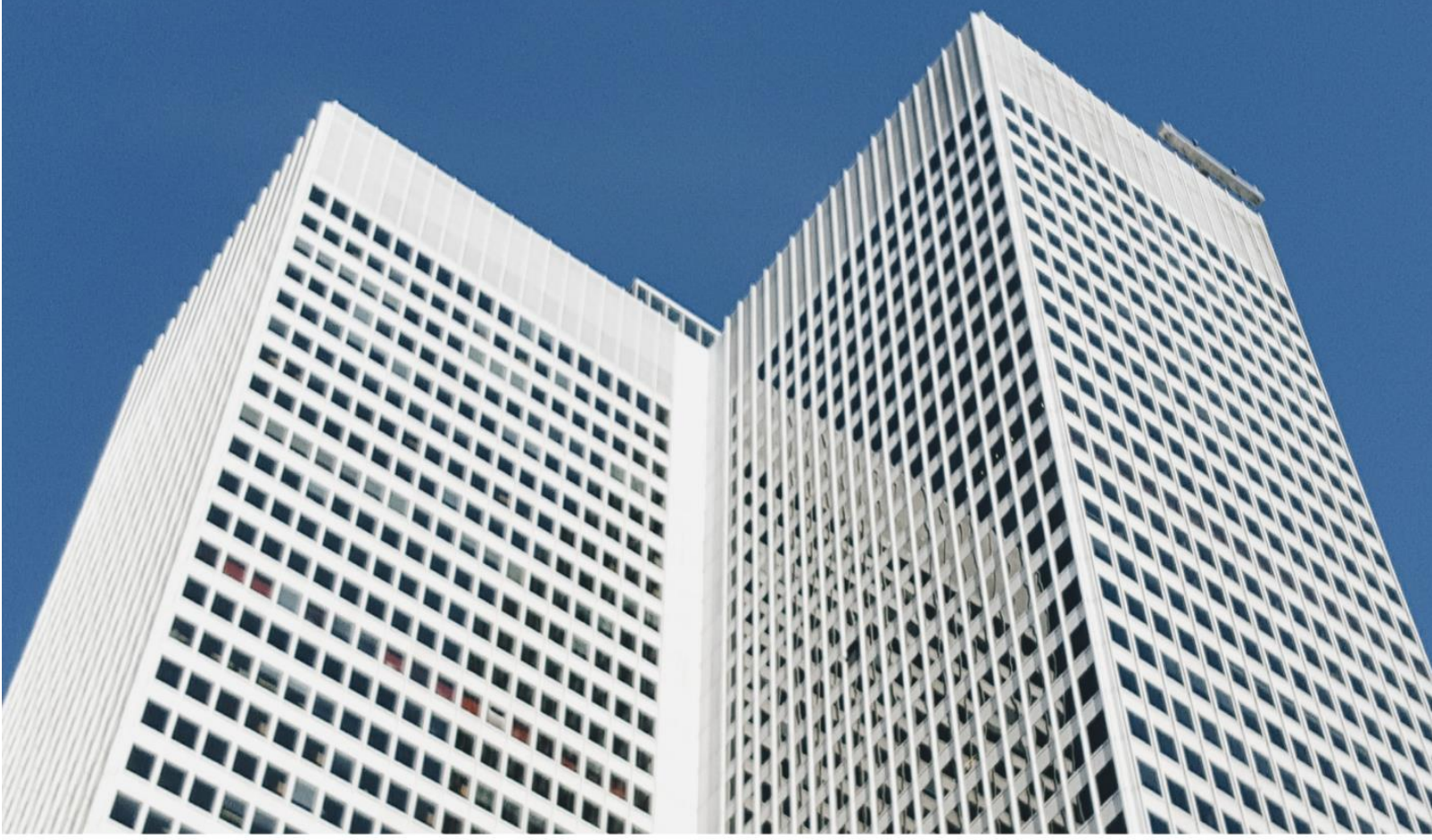
もう迷わない！

VPNの選び方

VPN接続の種類やプロトコル、
監視ソリューションを解説



ManageEngine　ゾーホージャパン株式会社

目次

はじめに

COVID-19 の影響により、多くの企業で業務をリモート環境に移すなどの対応を迫られています。

リモート環境への移行を成功させるには、リモートでも今までどおり業務を続けられるように、社内のオンプレミスのサービスにアクセスできることが重要です。**社内のサービスに社外からアクセスするには、適切な仮想プライベートネットワーク（VPN）を導入している必要があります。**ただし、VPN にはさまざまな種類があります。技術的な専門知識を持っていない限り、最適なものを選択することは容易ではありません。

本 eBook では、VPN の選び方についてわかりやすく解説しています。また、VPN 選定後に行うべき監視についても紹介しています。

VPN 接続とは？主な種類について

VPN 接続とは、インターネット上に特定の人のみが利用できる**仮想的なネットワークを設けて、情報を安全にやり取りするためのもの**です。ひと口に「VPN」と言っても、いくつかの種類があります。

[1] 拠点間 VPN

拠点間 VPN は、VPN を実装したルーター同士の接続で構成されます。クライアントの PC に VPN ソフトをインストールする必要はありません。遠く離れた拠点間のネットワークを接続するのに役立ち、例えば、さまざまな国に支店を持つ大規模企業で使用されています。拠点間 VPN は、さらに以下の 2 つに分類されます。

- イントラネット型 VPN： 同じ企業の異なる支社間を接続
- エクストラネット型 VPN： ある企業が他の企業のネットワークと接続

[2] リモートアクセス VPN

リモートアクセス VPN は、サーバー側とクライアント側のソフトウェアで構成されています。ユーザーが企業のプライベートネットワークに接続し、そのサービスやリソースに遠隔でアクセスできるようにするもので、個人とビジネスの両方に適しています。地域限定のウェブサイトにアクセスするために使用したり、自宅でのリモートワークや外出時に社内ファイルにアクセスするために使用したりします。

リモートアクセス VPN を利用した通信のルーティングには、以下の 2 つの方法があります。

- フルトンネリング方式 ： すべての通信が VPN トンネルを経由してルーティングされます。安全性が高い反面、VPN を通して重要ではないサイトへのアクセスが大量にあると、限られた帯域幅を消耗し、ビジネスで重要なサービスの機能にまで支障をきたす可能性があります。

- スプリットトンネリング方式 ： トラフィックを分割するのに役立ちます。どの通信を、VPN トンネルを通過させるか、あるいはインターネット・サービス・プロバイダ（ISP）を通過させるかを選択できます。ビジネスで重要なデータは VPN トンネルを通過させ、重要でないサイトへのアクセスは ISP を経由する、といった活用ができます。通信の体感速度が早くなる反面、脆弱性の懸念もあります。

次の章では、VPN 選びで重要な VPN プロトコルについて解説します。

VPN プロトコルの基本をおさえよう

VPN プロトコルを理解しておくことで、より良い VPN 選定をすることができます。VPN プロトコルとは、**VPN クライアントとサーバー間の接続を設定する際に従うべきルール**です。プロトコルは、提供する機能や VPN トンネルのセキュリティレベルによって異なります。以下では、VPN で使用されている一般的な VPN プロトコルを紹介します。

[1] PPTP（Point-To-Point Tunneling Protocol）

Microsoft が開発した PPTP には、暗号化機能がありません。PPTP は設定が簡単で、個人と組織の両方に適しています。欠点としては、セキュリティが弱いこと、ファイアウォールにブロックされやすいことです。手軽に地域限定のウェブサイトにアクセスしたい場合には便利ですが、セキュリティやプライバシーを気にする企業では利用を避けるべきです。

[2] IPsec（Security Architecture for Internet Protocol）

IPsec は、VPN トンネルを強力に暗号化し、**他のプロトコルと組み合わせて利用することで性能を向上させます**。IPsec には 2 つのモードがあります。

- トランスポートモード ： パケット内の特定のデータ部のみを暗号化します。2 つのホスト間、またはホストと VPN ゲートウェイ間の通信に用います。
- トンネルモード ： IP ヘッダも含めたパケット全体を暗号化します。ルーター間の通信で広く使用されています。

IPsec プロトコルは高いセキュリティレベルを実現しますが、価格が比較的高めで、設定が難しいという欠点もあります。

[3] L2TP（Layer 2 Tunneling Protocol）

L2TP は、PPTP の強化版です。PPTP と同様に L2TP にも暗号化機能はありませんが、前述の IPsec と組み合わせて使用することで安全性を確保します。二重にデータをカプセル化する分、通信速度は遅くなります。設定は簡単で、個人向けとしても気軽に使用できます。L2TP/IPsec は、地域限定のウェブサイトに適度なセキュリティでアクセスする場合や、**VPN 接続の速度が落ちても問題ない場合には良い選択**かもしれません。

[4] OpenVPN

OpenVPN は**人気があり、広く使われているオープンソースの VPN プロトコル**です。強力な暗号化機能を持っており、簡単に設定でき、複数の OS で動作します。OpenVPN は 443 の HTTPS ポートを含む任意のポートでも動作し、HTTPS 通信に見せかけることができるのでブロックされるのを防止できます。速度、セキュリティを含めた多くの面で他の VPN プロトコルと遜色ないと言えます。

[5] SSTP（Secure Socket Tunneling Protocol）

SSTP は、Microsoft により開発されたプロトコルであり、セキュリティの面で PPTP よりも優れています。非常に安全なプロトコルと言えますが、**Windows プラットフォーム上のみで動作する**ため、人気は限定的です。

[6] **IKEv2**（Internet Key Exchange Version2）

IKEv2 は、Microsoft と Cisco により共同で開発されたものです。IPsec と組み合わせることで VPN プロトコルとなります。IKEv2 は通信速度が早く、OpenVPN の代替としても使用できます。最大の利点は安定性であり、接続中断が起こっても自動的に再接続を行うことができるため、**モバイル端末での VPN 通信に向いています。**

本章では、VPN 選定のポイントとなるプロトコルの違いについて解説してきました。しかし、**セキュリティやコストに関わるのは、VPN の選定だけではありません。**次の章では、VPN 監視の重要性について紹介しています。

▼ VPN 監視にも対応！概要資料は以下をクリック ▼

VPN 選定だけでない！監視も重要な理由

ここまで見てきたとおり、VPN にはさまざまな接続の種類やプロトコルが存在します。自社に最適な VPN を選ぶ上で、**企業の規模やコスト、通信速度、セキュリティや暗号化レベル**などが基準となります。

セキュリティレベルの高い VPN を選んだとしても、ネットワーク自体はセキュリティの脅威に対して脆弱である可能性があります。監視を行わなければ、VPN を含むネットワークは、サイバー攻撃やデータの不正利用につながる脅威の影響を受けやすくなります。

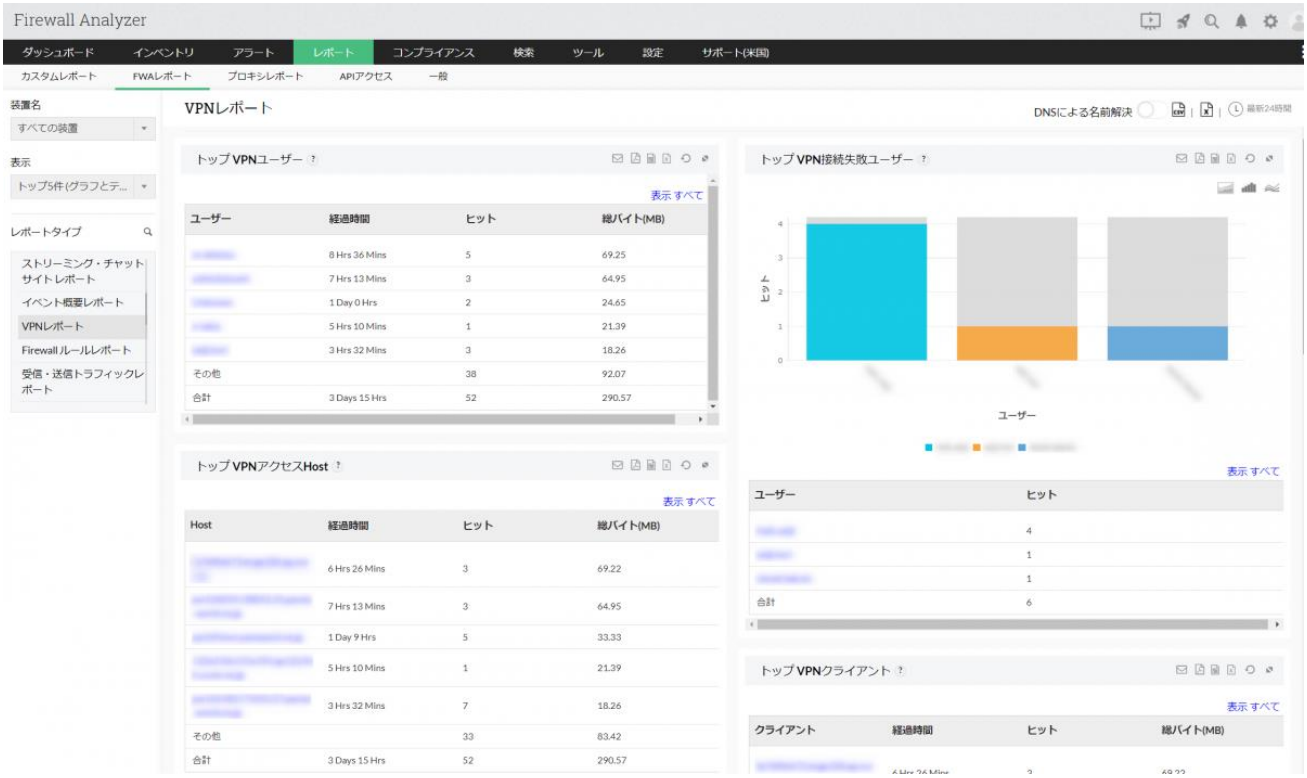
また、不適切な VPN 帯域幅の割り当ては、コストパフォーマンスや安定したサービスの維持の面でマイナスに働く可能性があります。そのため、**VPN 選びだけでなく VPN の監視も重要**です。

弊社 ManageEnigne が提供している「Firewall Analyzer」は、**VPN 接続を含めたネットワーク全体を可視化**するのに役立ちます。主要なパフォーマンス指標を継続的に監視することで、VPN 接続の安全性を確保し、パフォーマンスを把握することができます。ファイアウォールのログ、アクティブなセッション数、VPN 帯域幅の使用率、使用されているプロトコル、VPN の使用傾向など、さまざまな項目を自動で監視できます。

お手軽な VPN 監視ソリューション

Firewall Analyzer はファイアウォール/UTM/プロキシサーバーなどのログ解析ツールであり、セキュリティ管理者がネットワーク上の脅威を検知し、回避するのに役立ちます。

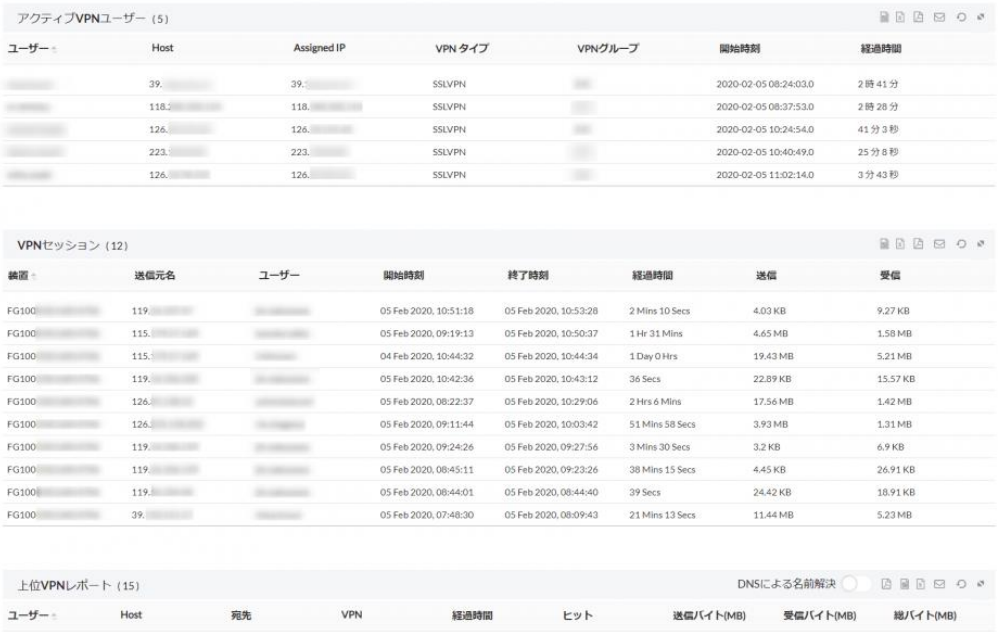
Firewall Analyzer の「**VPN 監視機能**」では、次のような課題の解決に寄与します。



ログをわかりやすく可視化！VPN レポート画面

＜帯域の状況把握＞

- 一定時間に、**通信量の多い VPN ユーザー**を特定したい
- VPN ユーザーの各セッションの開始/終了時刻を把握したい
- VPN セッションのリクエスト傾向を知りたい



「誰が」「いつ」「どのような」通信をしたかが丸わかり

＜セキュリティの向上＞

- **VPN 接続に失敗している、怪しいユーザー**を特定したい
- 業務時間外の VPN 通信が発生した際に、**アラート通知を受信**したい

VPN 監視の重要性は、これからもさらに増していくと考えられます。

社内ネットワークの**帯域把握**や**セキュリティ向上**でお悩みの方は、まずは無料の評価版でお試しください。Firewall Analyzer の特徴についてコンパクトにまとめた概要資料も、あわせてご参照ください。

VPN 監視にも対応！Firewall Analyzer

評価版インストール ｜ 概要資料ダウンロード