Amazon VPNとは

AWS VPNの概要や接続方法の種類、閉域網であるAWS Direct Connectとの違いなどについて解説します。

VPNとは

VPN（Virtual Private Network）は、「仮想専用線」と訳されます。VPNを構築するとネットワーク上に仮想の専用回線を設けることができるので、重要なデータの盗み見や改ざんを防いで安全に通信するための手段として利用されています。具体例としては、企業の拠点間の通信やWi-Fi通信などにVPNの技術が使用されています。

VPNは、交通手段に例えるとイメージしやすくなります。一般的なインターネット通信は、ほかのユーザーと同じ経路を一緒に利用するという点で電車やバスなどの公共機関での移動です。VPN通信は、公共の道路を専用の交通手段で移動するという意味で、自家用車での移動になります。

AWS VPNの概要

AWS VPN はAWSの中で提供されているVPNを利用した通信の仕組みです。AWS VPNを利用した場合、AWSのグローバルネットワークに対して、自社のネットワークやPC、モバイルから仮想の専用通信網を使ってアクセスすることができます。

AWSネットワーク上の仮想専用スペースであるAmazon VPC（AWS仮想ネットワーク内にあるリソース）にVPN Gatewayを設置することでVPN接続することが可能になります。

AWSでのネットワーク設計はAWS VPNのほかにインターネット回線を使った接続や専用回線（AWS Direct Connect）を使った接続があるので、自社の用途や目的に報じたネットワーク設計をすることが重要です。

AWS VPNの接続方法

AWS VPNには以下の3通りの接続方法があります。また、以下のほかに、サードパーティー製ソフトウエア VPN アプライアンスを使ってVPN接続をすることも可能です。

AWS サイト間VPN

Amazon VPCとユーザーのPCやモバイルなどとの間のアクセスをVPN技術によって接続可能とするのがサイト間接続です。デフォルトの状態では、AWSの外にあるPCなどと接続することはできませんが、VPNを設定することにより接続できるようになります。1台のデバイスとリソースを個別に接続する方法です。

AWS Client VPN

仮想のVPNトンネルを使用してAWSリソースとオンプレミス環境を接続できるのがAWS Client VPNです。TLSによって暗号化されるため安全性が高いという特徴があります。オンプレミス環境をそのままAWSのリソースと接続することができます。AWS Client VPNを使用してどこからでも、あらゆるデバイス（Windows、Mac、iOS、Android、Linux）でAWSのリソースにアクセスすることができます。

AWS VPN CloudHub

複数のサイト間 VPN接続がある場合、CloudHubを使用することで相互に安全なサイト間接続ができるようになります。複数拠点のAWSインスタンスと既存のインターネット環境をひとつのネットワークで接続させるようなイメージです。

AWS Direct Connectとの違い

既存のインターネット環境でネットワークを構築する方法として、AWS VPNのほかにAWS Direct Connectがあります。両方ともセキュリティに優れた通信方法という点では共通していますが、最大の違いはAWS VPNがインターネット回線に仮想の環境を構築するのに対し、AWS Direct Connectは閉域網の専用回線を構築することです。

通信速度やセキュリティの面ではAWS Direct Connectが勝っていますが、構築方法や価格については、用途やネットワークの組み方によって一概にどちらが良いとは言い切れません。非常に専門性の高いネットワーク構築業務を含むため、設計方法や価格などの具体的な内容は設計業者と相談のうえ決定するとよいでしょう。

また、AWS Direct ConnectとAWS VPNを使い分けるだけではなく、連携させることも可能です。例えば、AWS Direct Connect接続をAWS サイト間接続と組み合わせると、暗号化された通信で専用回線を利用することができます。

AWS VPNのメリットとは

AWS VPNのメリットについて解説します。

セキュアな通信

VPNは一般のインターネット回線と異なり、仮想上の専用線を設けて暗号化された通信を行うので、情報の盗み見や改ざんのリスクが少ないセキュリティ面に優れた通信技術です。セキュアな通信はVPN接続の最も核となるメリットです。

高可用性

AWS VPN接続は、可用性の高さも大きなメリットです。サイト間接続の際には、2つの仮想トンネルを設け、万が一片方のトンネルにトラブルが生じても、あと一方のトンネルを使って中断せずに接続することが可能です。冗長性が確保されているので、確実にAmazon VPCへ配信することができます。

すべてのデバイスからアクセス可能

AWS VPN接続をすれば、すべてのデバイス（Windows、Mac、iOS、Android、Linux）からAWSのインスタンスにアクセスすることができます。

AWS VPNの料金体系と料金プラン

AWS VPNの料金体系とプランについて解説します。

AWS サイト間 VPNの料金

AWS東京リージョンやAWS大阪ローカルリージョンへのAWSサイト間接続の場合、1時間当たりサイト間VPN接続時間ごとに0.048USDとなっています。AWS VPNもほかの多くのAWSサービスと同様に従量課金の仕組みを取っているため、実際に通信した時間分のみを使用する料金体系となっています。

AWS Client VPNの料金

AWS Client VPNの場合は、アクティブになっているCient接続の数や関連付けられているサブネットの数に応じて料金が発生します。東京リージョンのAWS Client VPN 接続ごとの料金は、1時間当たり0.05USDです。また、ひとつのエンドポイント接続（Amazon VPCの関連付け）ごとに1時間当たり0.15USDかかります。

※料金はすべて2019年8月現在の設定です。
最新の料金につきましては、AWSの公式サイトをご覧ください。
https://aws.amazon.com/jp/vpn/pricing/

AWS VPNの課金単位と最低課金時間

AWS VPNの課金は1時間当たりの料金制度になっています。ただし、利用時間が1時間に満たないケースでも、1時間分の料金が課金される仕組みになっている点に注意が必要です。VPN接続の課金をストップするためには、AWSマネジメントコンソールやAWS CLIを使用して接続をストップする必要があります。

※料金はすべて2019年8月現在の設定です。
最新の料金につきましては、AWSの公式サイトをご覧ください。
https://aws.amazon.com/jp/vpn/pricing/

まとめ

AWSを活用するためには、ネットワークは不可欠です。そして、重要なデータをセキュアに扱うためには、AWS VPNやAWS Direct Connectなどの安全性の高い通信網の設定が必要です。コストや用途などによってはAWS VPNとAWS Direct Connectとの併用・使い分けの必要性も生じてくるでしょう。
今回の記事を参考に、コスト、安全性、速度などを踏まえ、最適のネットワーク環境を構築していくことが大切です。

まとめ

AWSマネジメントコンソールを利用すれば、さまざまなリソースやユーザーIDを視覚的に一元管理することができます。利用方法も非常にシンプルで、アプリを利用すればスマートフォンからのアクセスも可能です。
AWSの利便性を高め管理を容易にしてくれるサービスなので、ぜひ有効活用していきましょう。

AWS導入に向けて他に知っておくべきこと

AWSの各サービスは構築する情報システムによって利用適性が異なります。実際の構築にあたってはクラウド導入・運用支援事業者が提供している支援サービスを活用することで、自社の検討・構築・運用工数の削減が期待できます。