AWSのルートテーブルとは？その概念から設定方法まで詳しく解説！

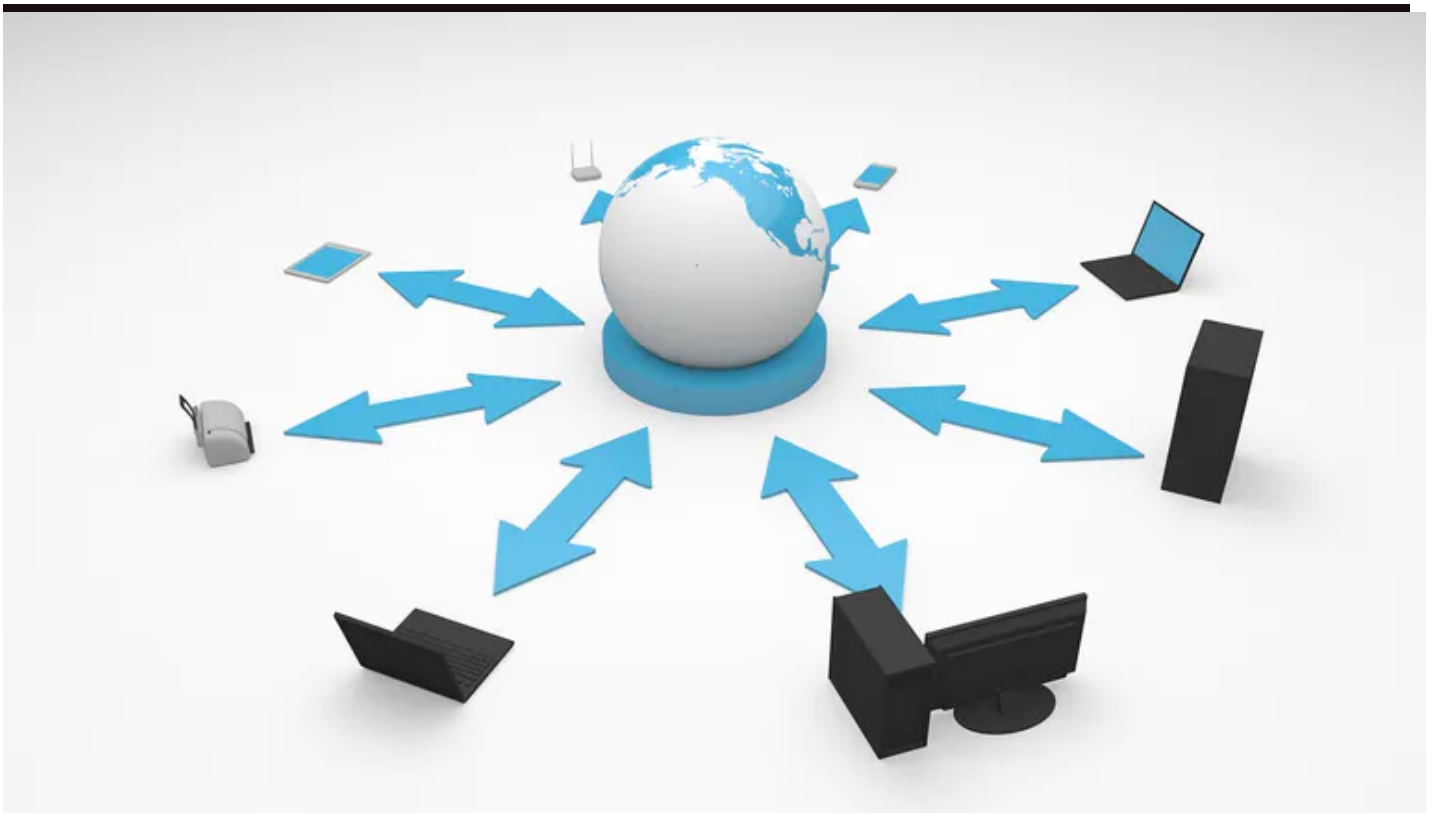
開発ツール

アンドエンジニア編集部 2021.07.20

この記事でわかること

- ✓ Amazon VPCとは仮想ネットワークを構築し、プライベートネットワークで安全に運用するためのサービスを指します
- ✓ ルートテーブルとは、Amazon VPCでインターネットと仮想ネットワークのアクセスを実現するための経路設定テーブルです
- ✓ ルートテーブルは利用ゲートウェイごとに関連付けすることで、必要なアクセス経路を提供します

AWSとは？



AWSとはAmazon Web Serviceの略で、最大のクラウドサービス事業者です。AWSはクラウドコンピューティングのサービス全般を事業としており、豊富なサービス提供を特徴としています。AWSは全世界を25の地域から成るリージョンに分割し、均一なサービスを提供しています。

Amazon VPCとは？

Amazon VPCとは、Amazon Virtual Private Cloudの略です。Amazon VPCにより仮想ネットワークを構築し、IPアドレスおよびサブネットの管理・ルーティング・ゲートウェイの設定等一連の仮想ネットワークの制御を簡単に実現することができます。

参考：Amazon Virtual Private Cloud

Amazon VPCのルートテーブルとは？

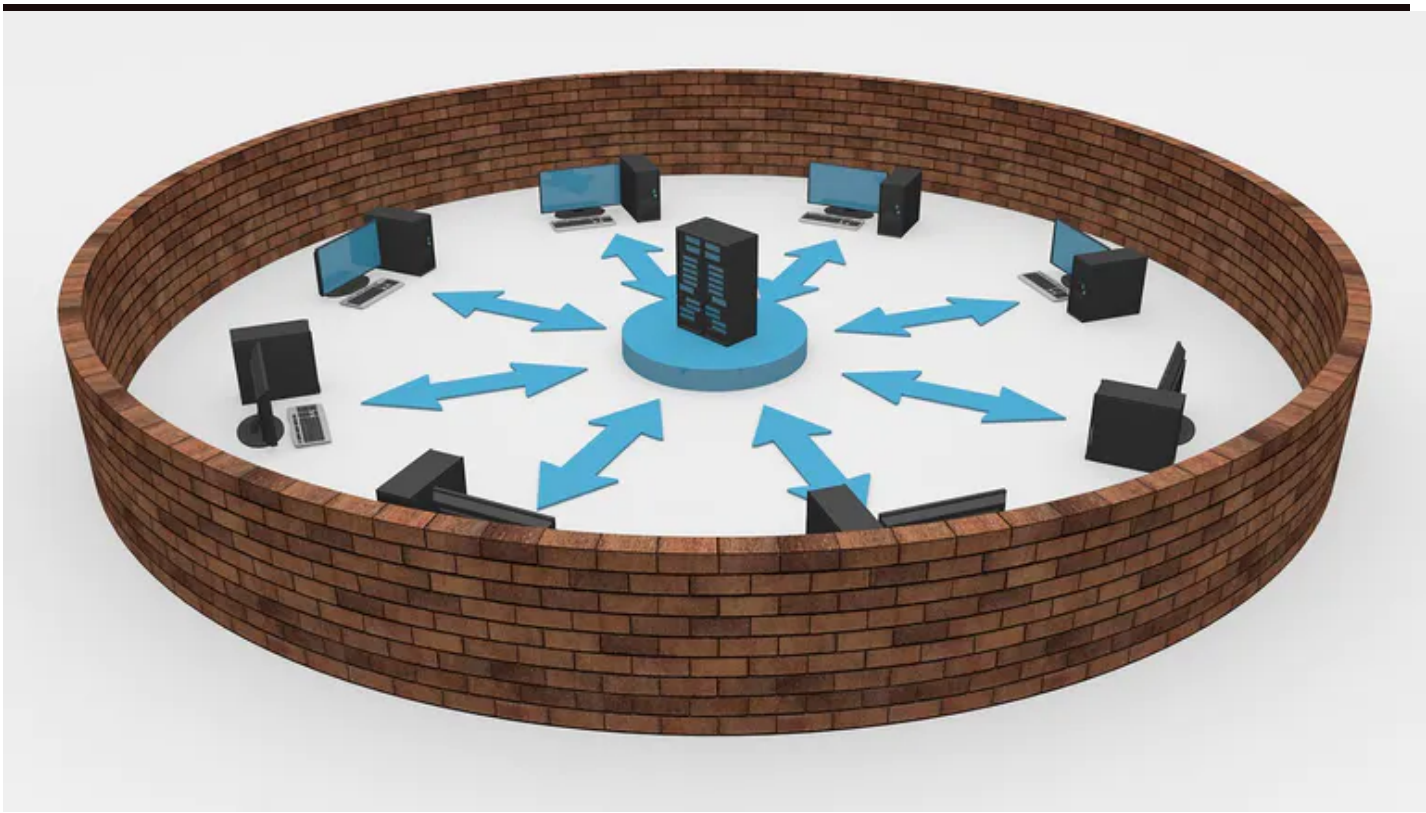
VPCを利用する場合は一連のルールに従い、ルートと呼ばれるネットワーク経路を選択します。そのルールの記載されたテーブルを、ルートテーブルと言います。ルートテーブルには、ゲートウェイからのネットワークトラフィックをトラフィックに応じて経路設定します。そのため、VPCのルートテーブル

は通常のルーティングテーブルと同じ仕組みと考えて良いでしょう。
参考：AWS Amazon VPC ユーザーガイド VPC のルートテーブル

ルートテーブルの関連用語は？

VPCのルートテーブルを説明するにあたり、必要とされるネットワーク用語を解説していきます。
・サブネット
サブネットとは、IPネットワークを細分化することを指します。記述方法はCIDR（サイダー）表記で、IPアドレスのプレフィックスとしてネットワークアドレスの後にスラッシュ（/）の後とネットワークアドレスビット数を記載します。使用例は、”10.0.0.0/16”等が挙げられます。
AWSのサブネットは、VPCで設定するネットワークアドレス単位を指します。ここでいうサブネットとは、一般的にネットワーク環境で用いるサブネットと同等の考え方となります。
参考：Amazon VPC ユーザーガイド VPC とサブネット
・CIDR（サイダー）
CIDRは、Classless Inter-Domain Routingの略です。IPネットワークのクラスを部分的に割り当ててIPアドレスの使用量を削減します。従来IPアドレスはプレフィックスとホストアドレスに分かれており、32ビットのIPアドレスはプレフィックスとして8ビット・16ビット・24ビットのいずれかを割当していました。
そのため、ホストアドレスはクラスCで8ビット分クラスBで16ビット分しか割当できず、ホストアドレスをルーティング処理するため多くのオーバーヘッドが発生していました。したがって、クラスフルに用いたクラスA・クラスB・クラスCの管理体系ではIPアドレス管理上の無駄が生じてしまいます。
CIDRでは、可変長サブネットマスクVLSM（Variable Length Subnet Masking）を用いるため、IPアドレスの浪費を抑えてルーティング効率を向上します。このことから、クラスレスとして必要なアドレス個数に合わせてネットワークアドレスとホストアドレスの境界を任意に決定する方式として考案され、現在広く利用されています。
・CIDRブロック
CIDRブロックとは、CIDRのプレフィックスに基づいてIPアドレスを解釈するアドレスのグループを指します。つまり、CIDRプレフィックスで記載したIPアドレスの範囲をCIDRブロックとしてネットワーク割当や設定の対象アドレスとして指定することができます。

Amazon VPCルートテーブルの種別は？



VPCでは以下のテーブル種別に基づきルートテーブルを設定します。

・メインルートテーブル
VPCに自動割り当てされるルートテーブル
・カスタムルートテーブル
VPC用に各自設定するルートテーブル
・サブネットルートテーブル
サブネットに関連付けられるルートテーブル
・ゲートウェイルートテーブル
インターネットゲートウェイまたは仮想プライベートゲートウェイに関連付けられるルートテーブル
・ローカルゲートウェイルートテーブル
Outposts ローカルゲートウェイに関連付けられるルートテーブル

Amazon VPCルートテーブルの仕組みは？

VPCルートテーブルの仕組みは、一般に用いられているネットワークルーティングテーブルと同等の考え方に基づきます。
VPCでは、デフォルト設定されたメインルートテーブルとカスタムルートテーブルを用いてルーティングを行います。同様に、サブネットに関してはサブネットルートテーブルを使用します。また、VPCへのインバウンドトラフィックについては、ゲートウェイルートテーブルを用います。
VPCでは設定リソースに上限値があり、クォータと呼びます。そのため、作成できるルートテーブル数やルートテーブルに追加可能なルート数はクォータが設定されています。
参考：AWS Amazon VPC ユーザーガイド Amazon VPC クォータ

Amazon VPCルートテーブルの設定は？

VPCルートテーブルでは、ルートの送信先ならびにターゲットを関連付けします。
例えば、サブネットルートテーブルに「送信先 0.0.0.0/0」「ターゲット igw-XXXXXXXXX」を設定してみます。「送信先 0.0.0.0/0」は全てのIPv4アドレスを意味します。「ターゲット igw-XXXXXXXXX」はVPCに割当らえたインターネットゲートウェイを指します。
これにより、サブネットからインターネットゲートウェイ経由でインターネットアクセスが可能となります。
ここで言う送信先はCIDR表記で指定します。IPv4／IPv6が指定可能です。ターゲットはルーティング先に応じて設定します。

メインルートテーブルの作成は？

メインルートテーブルは、VPC作成時に自動的に割り当てられます。メインルートテーブルは、個別にルートテーブルで関連付けされていないサブネットのルーティングをデフォルト処理します。
作成時はローカルルートのみ設定されています。デフォルトVPC以外を設定する際に順次必要とされるルートが自動追加されます。メインルートテーブルは削除することはできません。

他のテーブルの作成は？

他のテーブルは必要に応じて作成します。コンソールで VPC ウィザードを使用してVPCを新たに作成すると、カスタムルートテーブルが作成されます。カスタムルートテーブルでは、ルートを追加・削除・変更することができます。カスタムルートテーブルは、関連付けがない場合に削除することが可能です。
VPCのサブネットは、カスタムルートテーブルかメインルートテーブルいずれかに関連付けを行います。
ゲートウェイルートテーブルはインターネットゲートウェイ、または仮想プライベートゲートウェイに関連付けを行います。ゲートウェイルートテーブルにより、VPCに入るトラフィックのルーティングパスを細かく制御可能です。

ルーティングの優先度は？

AWSのルーティングの優先度は、プレフィックス長の長い具体的なルートが選択されます。この選択方法は、ネットワークルーティングで用いるロンゲストマッチ（longest match、最長一致）と同一です。

次に、動的ルートと静的ルートが存在する場合は静的ルートが優先されます。この選択方法は、ネットワークルーティングで用いるアドミニストレーティブディスタンスと同一です。

その他ルーティングの指定方法？

ルーティングの指定は利用するゲートウェイに基づき関連付けを行います。具体的な指定方法は、以下の通りです。

・インターネットゲートウェイ
サブネットをパブリックサブネットとすることで、インターネットアクセスが可能です。
送信先をIPv4の場合は、0.0.0.0/0とします。
ターゲットをインターネットゲートウェイIDである、igw-XXXXXXXXXとします。

・NATデバイス
プライベートサブネットのインスタンスがインターネットに接続可能です。
送信先をIPv4の場合は、0.0.0.0/0とします。
ターゲットをNATゲートウェイIDである、nat-XXXXXXXXXとします。

・仮想プライベートゲートウェイ
VPCのインスタンスが独自のプライベートネットワークと通信可能です。
送信先をIPv4の場合は、例として10.0.0.0/16の様にします。
ターゲットを仮想プライベートゲートウェイIDである、vgw-XXXXXXXXXとします。

・AWS Outposts ローカルゲートウェイ
VPC内のサブネットに、ローカルゲートウェイが追加可能です。
送信先をIPv4の場合は、例として192.168.YY.ZZ/24の様にします。
ターゲットをローカルゲートウェイIDである、lgw-XXXXXXXXXとします。

・VPC ピアリング接続
プライベートIPv4アドレスを使用して、2つのVPC間でルーティングすることができます。
送信先をそれぞれのVPCのCIDRブロックとします。
ターゲットをlocalおよびVPCピアリング接続である、pcx-XXXXXXXXXとします。

・ゲートウェイVPCエンドポイント
VPCと他のAWSのサービスとをプライベートに接続可能です。
送信先はプレフィックスリストIDとして、pl-XXXXXXXXXが自動登録されます。
ターゲットはエンドポイントIDである、vpce-XXXXXXXXXが自動登録されます。

ここでは代表的なゲートウェイの指定方法を紹介しました。その他の指定方法詳細については、以下のリンクをご確認ください。

参考：Amazon VPC ユーザーガイド ルーティングオプションの例

AWSルートテーブルを活用してネットワークアクセスを最適化しましょう

AWSはVPCを用いることで、インターネットとプライベートネットワークを併用した仮想ネットワークを構築します。仮想ネットワークにより、トラフィック管理やセキュリティリスク低減が可能です。そのため、VPCは業務システムでの活用拡大が今後も期待でき、さらなる理解を深めることをおすすめします。