仮想ネットワーク

- Amazon VPC -

Amazon VPCとは

- *Virtual Private Cloud* (VPC) は、AWS アカウント専用の仮想ネットワークです。(AWS ドキュメント)
- VPC領域とは「利用するIPアドレス範囲の枠組み」
- そのIPアドレス範囲をサブネットを作って切り分ける
  - EC2インスタンスなどはサブネットに配置する

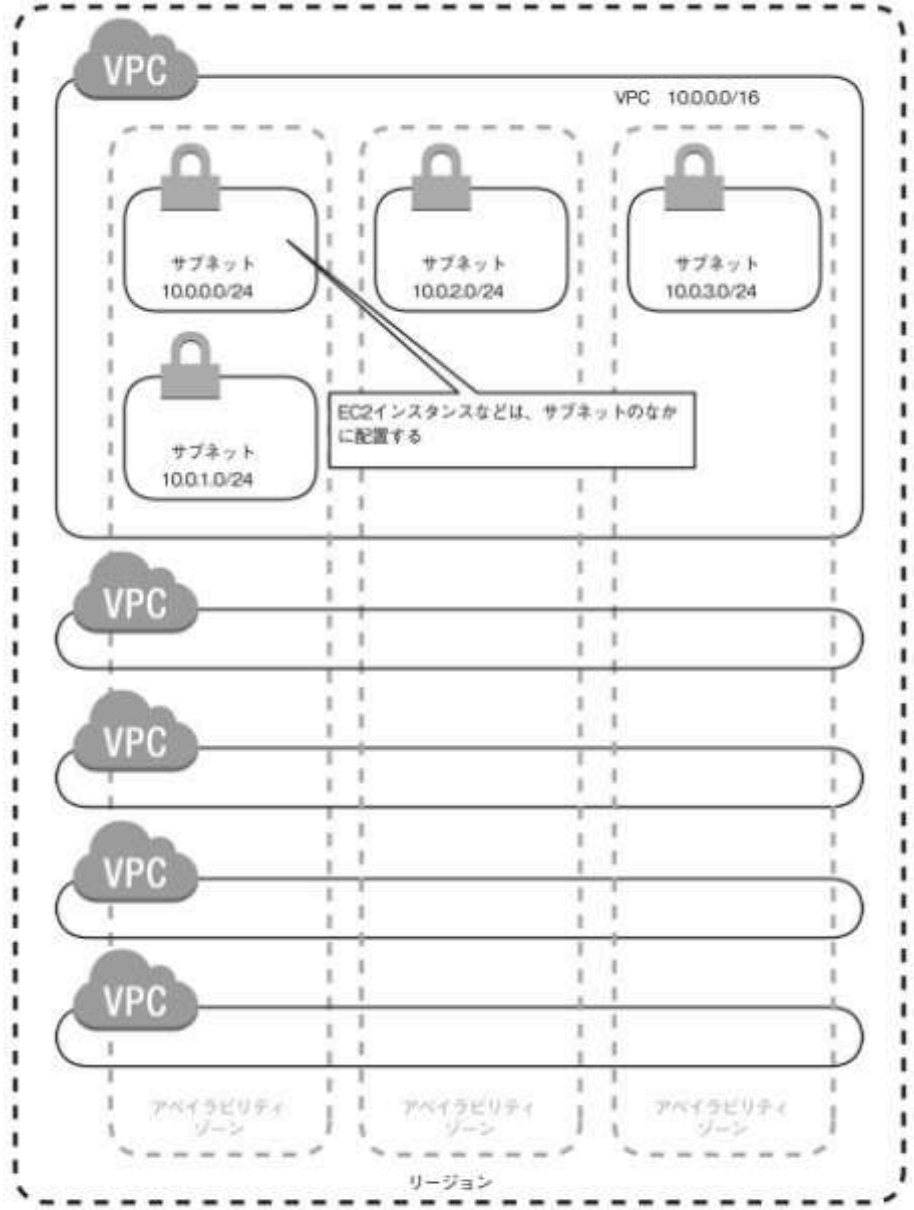

図 2-1　VPC 領域とサブネットの関係

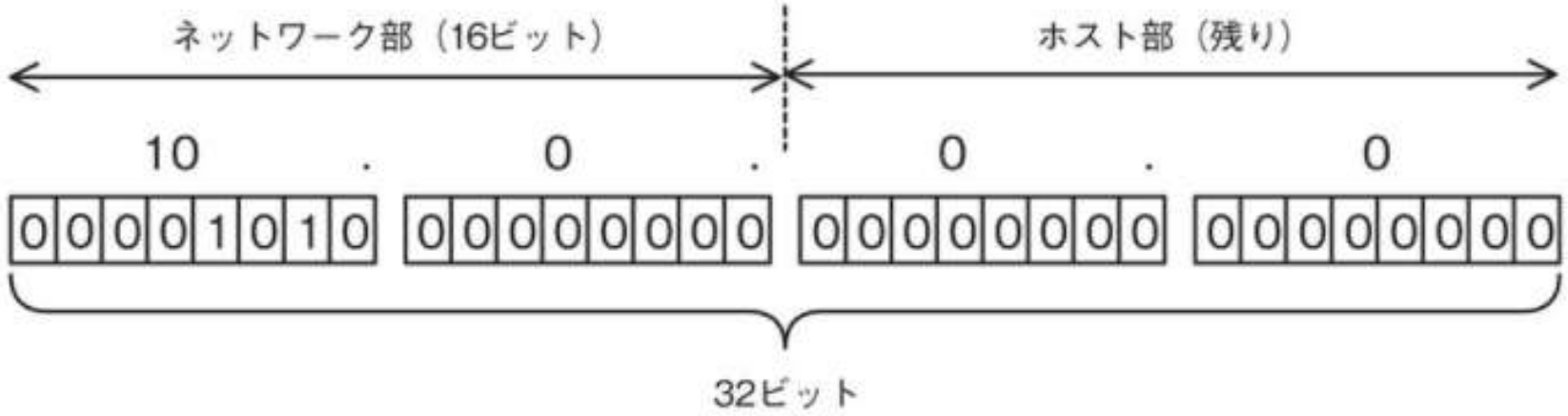

図 2-2　ネットワーク部とホスト部

CIDR表記

- IPアドレスは32ビット長のうち一部の上位ビットをネットワーク部, 下位ビットをホスト部とする
- CIDR表記では「10.0.0.0/16」のように"/"のあとにネットワーク部のビット数を示す
- 先頭と末尾はそれぞれネットワークアドレス, ブロードキャストアドレスのため使用できない
  - 10.0.0.0/16なら先頭は10.0.0.0, 末尾は10.0.255.255

VPC領域と他のネットワークとの接続

- AWSによって5つの接続ポイントが用意されている
  - インターネットとの接続
    - インターネットゲートウェイを用いることで可能
  - 拠点との専用線での接続
    - AWS Direct Connect というサービスがサポートしている
  - 拠点とのVPNでの接続
    - VPN Gatewayを構成する
  - VPCピア接続
  - AWSサービスとの接続

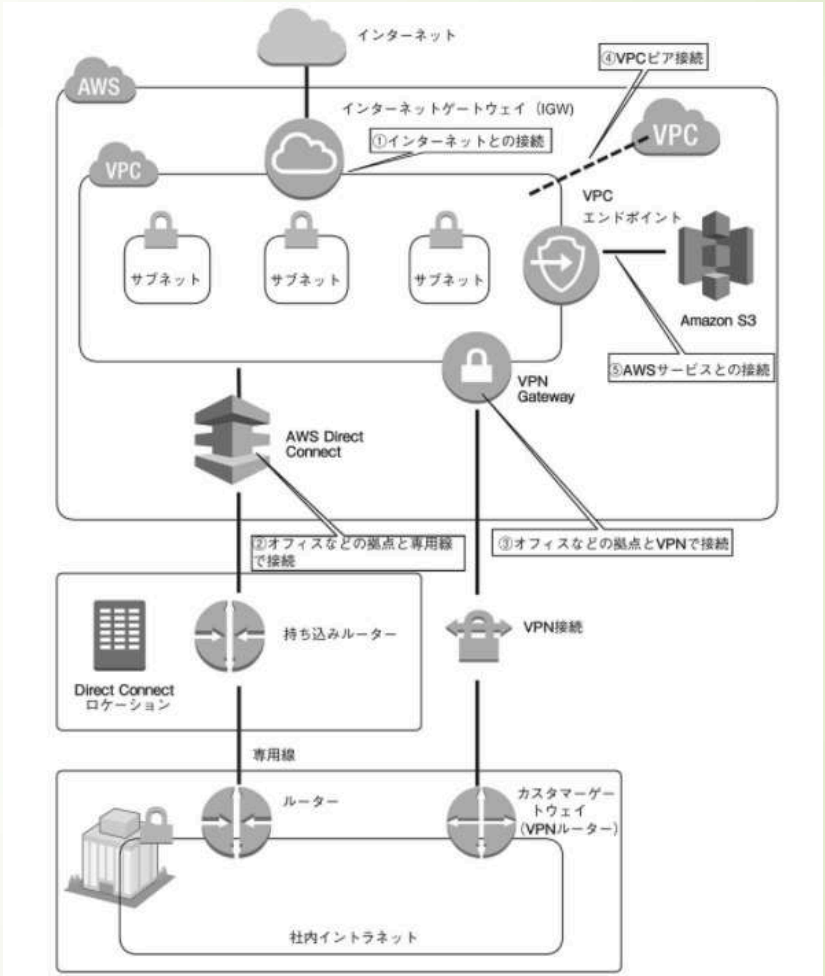

図 2-7　VPC 領域やサブネットを他のネットワークと接続する接続ポイント

VPCエンドポイント

- VPCエンドポイントを構成すると, インターネットに出ることなく, AWSが提供するマネージドサービスを利用できる
  - ゲートウェイエンドポイントでは, Amazon S3 に加え, DynamoDBへの接続がサポートされている
- コンソールや, AWS CLI を用いて作成することができる
  - どちらの場合でもエンドポイントを作成するVPCと接続先のサービスを指定, アクセス許可ポリシーを設定して作成する

デフォルトのVPC

- デフォルトのVPCとは，「標準で用意されたVPC」を指す
- デフォルトのVPCは「すぐに、インターネットに接続できるようにする」ことを目的に作られた特別なVPC領域
  - ユーザが自ら作成することはできない
- 構成は以下のようになっている：
  - IPアドレス範囲は「172.31.0.0/16」
  - サブネットは上のIPアドレス範囲のなかから「/20」のサイズで各アベイラビリティゾーンに配置される
  - インターネットゲートウェイが設定済み