

# Amazon Web Services ネットワーク入門

---

sizu

スライド雑なのは  
許して.....

# Chapter 1 の前に ...

# AWS アカウントの作成

- <https://aws.amazon.com/jp/register-flow/>
- セキュリティ管理 (IAM) / 多要素認証 (MFA) / 仮想デバイスの有効化などは各自設定
  - Identity and Access Management ドキュメント
    - <https://aws.amazon.com/jp/documentation/iam/AWS>
  - MFA 仮想デバイスの有効化
    - [http://docs.aws.amazon.com/ja\\_jp/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_enable\\_virtual.html](http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html)
- 無料サービスの範囲 / 料金体系などの確認
  - 無料利用枠について
    - <http://aws.amazon.com/jp/free>
  - 無料利用枠の使用
    - [http://docs.aws.amazon.com/ja\\_jp/awsaccountbilling/latest/aboutv2/billing-free-tier.html](http://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/billing-free-tier.html)
  - etc ...

# はじめに (まだ Chapter 1 じゃない)

- クラウドは必要不可欠なインフラに成長
  - 登場当初は信頼性 / セキュリティを疑問視
- **AWS のメリット: 手軽なネットワーク構成**
  - 使用時にすぐにネットワーク / サーバを用意
  - 規模 / 構成の変更が容易
  - 管理の手間が不要
  - 負荷分散 / 冗長性の担保 / 安全対策の考慮
- 様々な機能の提供によるサービスの複雑化
- **基本的な構成であるネットワークとサーバを説明**
  - ネットワーク: **VPC**
  - サーバ: **EC2 インスタンス**

サーバ 1 台 / DB (DataBase) サーバ 1 台で構成される  
システムの構築を目指す

# Chapter 1: AWS でのシステム構築

---

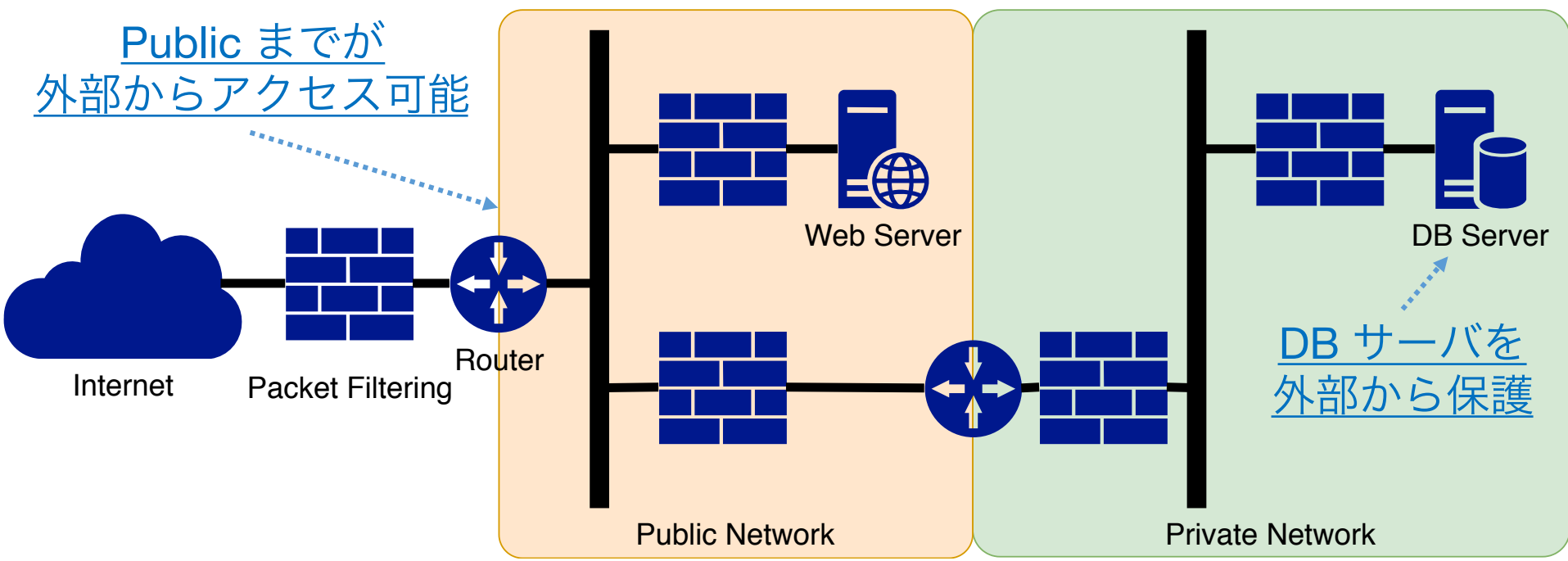
sizu

# 企業 IT インフラを AWS へ

- **AWS (Amazon Web Service)**
  - 2006 年からサービス開始
  - 現在では多様なサービスを提供
    - e.g., 仮想サーバ / DB サーバ / ビッグデータ処理 / 機械学習
- 企業におけるクラウドサービスの適用領域の拡大
  - クラウドサービスのメリットを活用
    - コストダウン / スケーラブル / オンデマンド / マネージド
  - AWS を利用して斬新なサービスを提供する企業の登場
  - 高額 / 大規模なシステムを AWS で安価に実現
- **オンプレミス環境を徐々に AWS へ移行**
  - 最初はオンプレミスのシステム構造をそのまま移行
  - 徐々にマネージドサービスを利用
  - パブリッククラウド環境へ最適化

# オンプレミスネットワーク

- オンプレミスネットワークは様々な要素から構成
  - e.g., ルータ / スイッチングハブ / Internet への接続口
- DB / Web サーバのオンプレミス環境を考慮
  - Web サイトの構築を想定
  - 本来, 障害対応に冗長構成 / ロードバランスなどを考慮
    - 今回は簡単の為に省略





# Public / Private Network

- パブリックネットワーク

- 外部から接続可能なネットワーク
- **パブリック IP アドレス** を付与する必要
  - インターネットにおいて唯一のアドレス
  - グローバル IP アドレスと同じ意味
  - AWS においてはパブリック IP アドレスと呼称

- プライベートネットワーク

- 外部から接続できないネットワーク
- **プライベート IP アドレス** を付与する必要
  - インターネットにおいて使用されることがないアドレス
  - 組織内で自由に使用することが可能

Chapter 2 で出てくるので  
今分からなくても  
焦らないで！！！！

クラス	IP addr の範囲
クラス A	10.0.0.0 ~ 10.255.255.255 (10.0.0.0/8)
クラス B	172.16.0.0 ~ 172.31.255.255 (172.16.0.0/12)
クラス C	192.168.0.0 ~ 192.168.255.255 (192.168.0.0/16)

# Firewall (FW)

- 外部からの攻撃を防ぐファイアウォールを設置
- よく使用される手法: パケットフィルタリング
  - TCP/IP ヘッダの IP addr / プロトコル / ポート番号でフィルタリング
- 設定例
  - Web サーバの設定
    - HTTP / HTTPS を許可するために 80 / 443 ポートを許可
    - 社内ネットワークからの SSH を許可するために 22 ポートを許可
    - 上記以外ドロップ
  - DB サーバの設定
    - Web サーバとの通信のみ許可
    - 上記以外ドロップ

サーバを管理するため



# AWS 移行で考慮すべき点

- ネットワーク全体

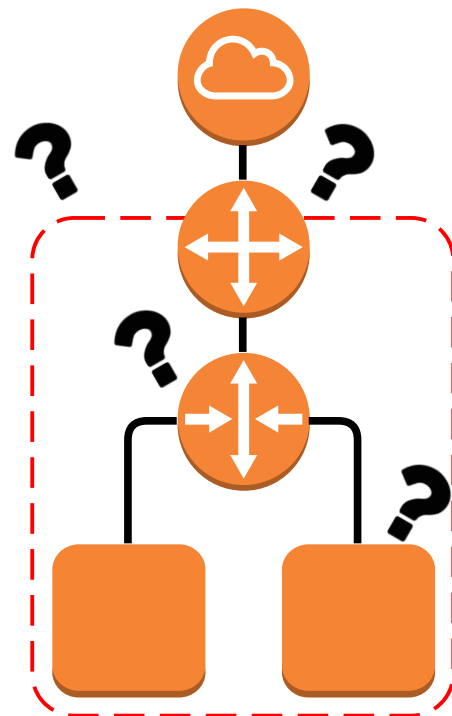
- AWS 上に構築するネットワークの構成
  - サブネットの作成
  - IP アドレスの割り当て
  - インターネットへの接続

- サーバ

- AWS 上に構築するサーバの構成
  - CPU (Central Processing Unit) 数
  - メモリ容量
  - ストレージの種類 / 容量
  - OS (Operation System)

- ファイアウォールとセキュリティ

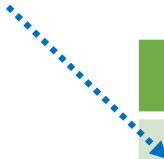
- サーバ毎のファイアウォール
- ネットワーク全体のファイアウォール



# Region

- AWS は全世界各地に存在する拠点で運営
  - 拠点: リージョン (Region)
  - 都市名が付与
    - 別にその都市にあるわけではない
  - リージョンが提供するサービスには多少の差異が存在
- 手元からリージョンまで遠ければ遅延も増大
- リージョン同士は独立
  - リージョン間で通信する際はインターネットを経由

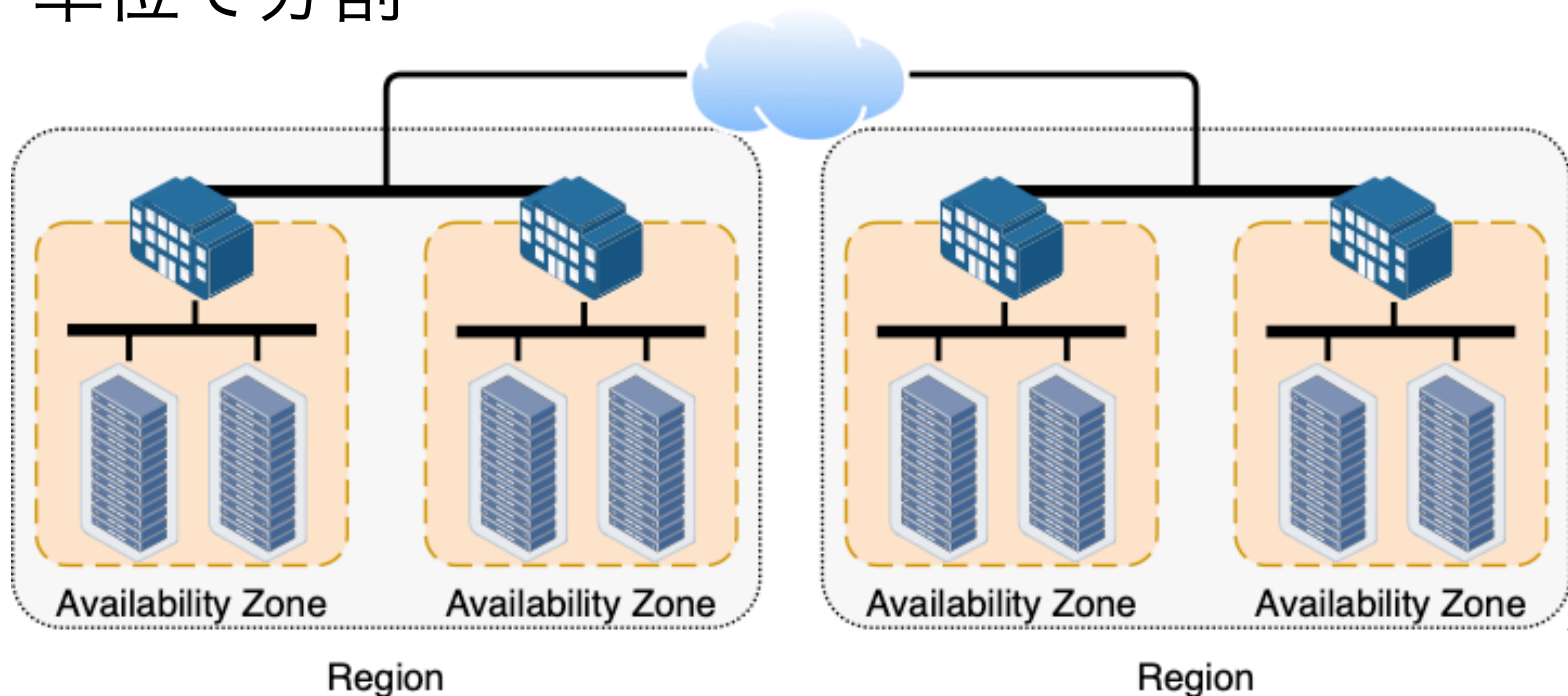
全てのAWSサービスが利用可能



名称	英語表記	略称
北バージニア	US East (N. Virginia)	us-east-1
オレゴン	US West (Oregon)	us-west-2
東京	Asia Pacific (Tokyo)	ap-northeast-1

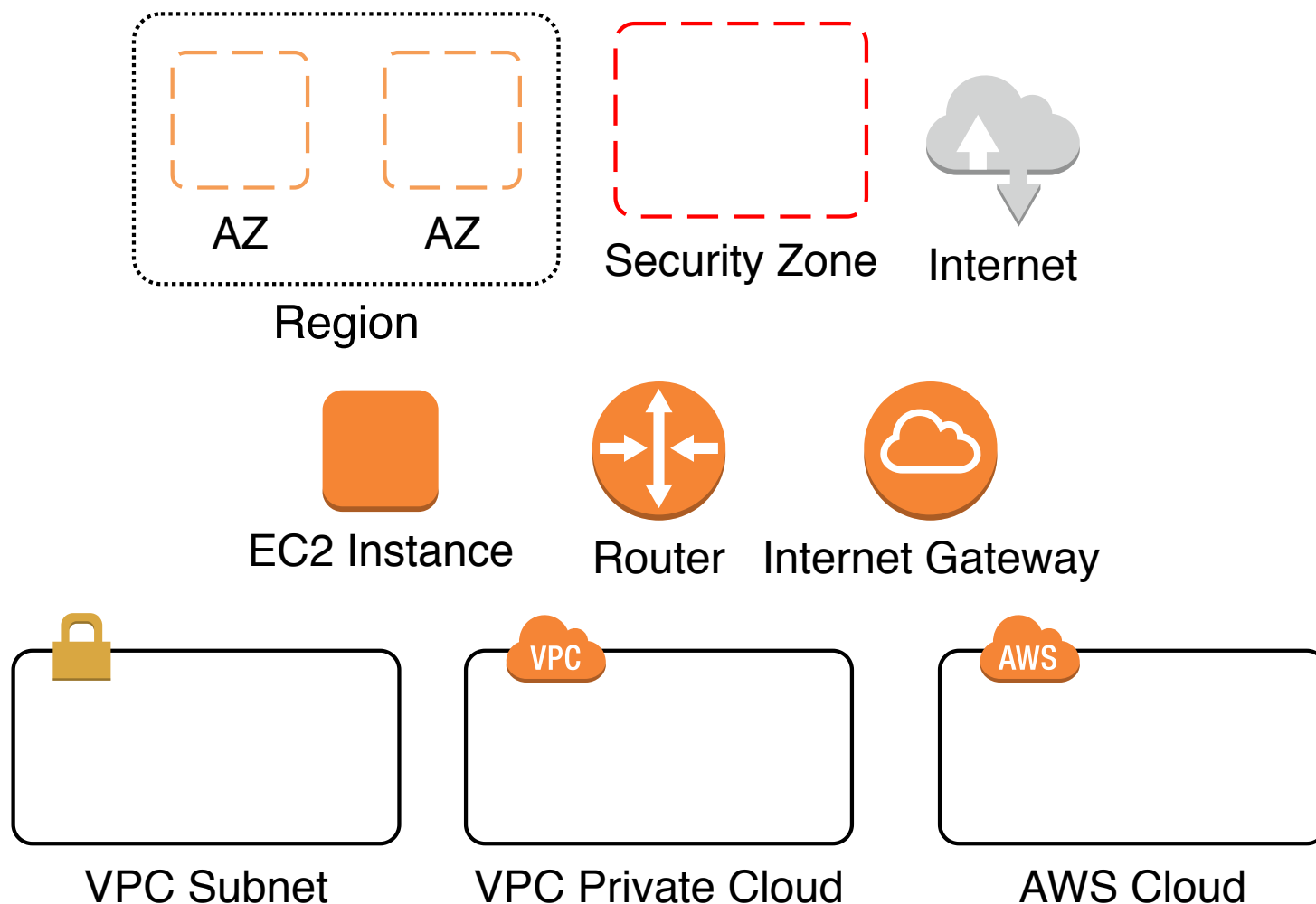
# Availability Zone (AZ)

- 各リージョンにおけるサービス拠点
  - いわゆるデータセンタ
- 1 リージョンに対して複数存在
  - 障害対策のため
- AWS ネットワークはアベイラビリティゾーン単位で分割



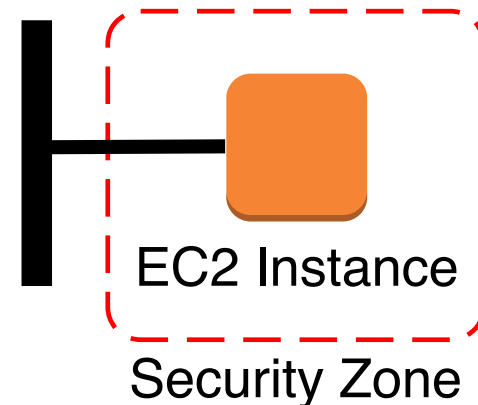
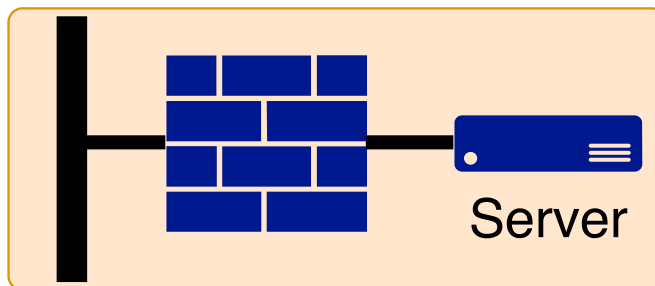
# AWS におけるシステム構成

- 以降では AWS シンプルアイコンを使用



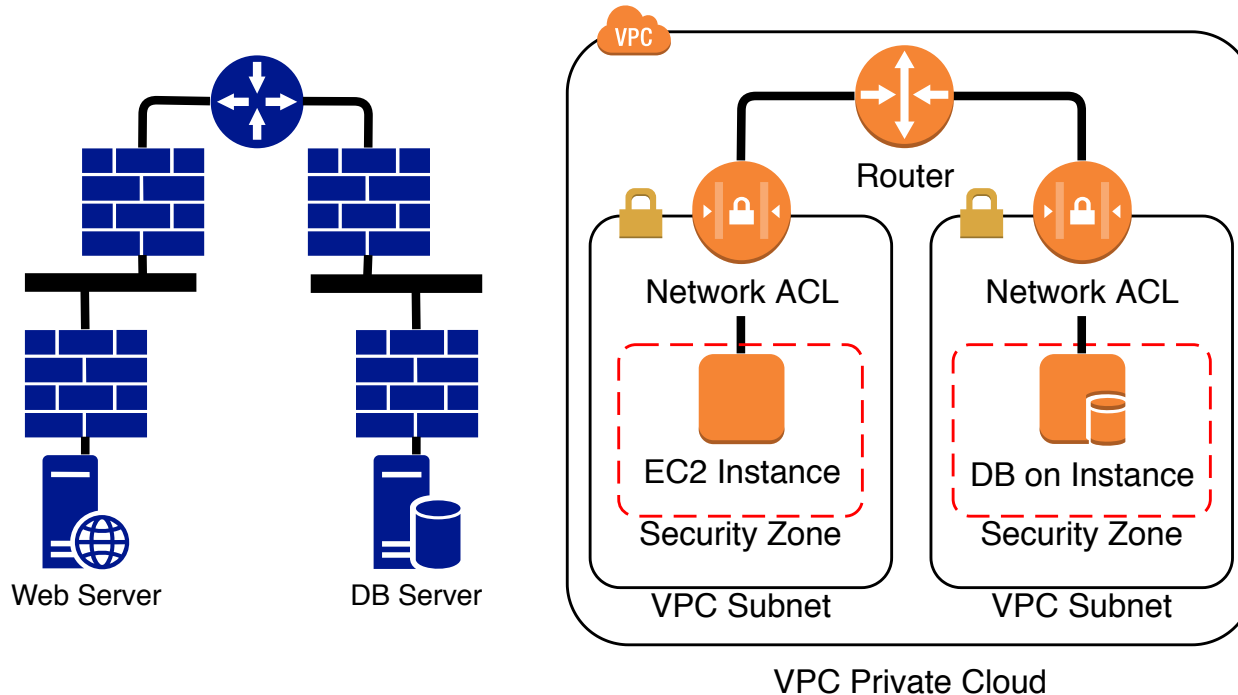
# Amazon EC2

- **Amazon EC2 (Amazon Elastic Compute Cloud)**
  - 仮想サーバの運用 / 構築が可能
    - 仮想サーバでは様々な OS が運用可能
- EC2 で起動した仮想サーバはインスタンス
- インスタンスの FW はセキュリティグループ
  - デフォルトではインバウンド方向を全てドロップ
    - インバウンド: ネットワークからインスタンス方向
  - 設定を変更しないと何処からもアクセス不可能



# Amazon VPC

- **Amazon VPC (Amazon Virtual Private Cloud)**
  - AWS においてネットワークを構成するサービス
  - VPC 領域, サブネットの順に作成
- **ネットワーク ACL (Access Control List)**
  - サブネットにおいてトラフィックの出入りを制御
    - セキュリティグループはインスタンスを対象





# Internet Gateway

- IGW (Internet Gateway)
  - VPC とインターネットを接続

ルータを省略しても  
VPC Subnet は暗黙的に接続されていると理解

Public Subnet には Public IP,  
Private Subnet には Private IP を  
割り当て

