# ネットワーク

## 要件

## CIDR

VPC に割り当てるCIDRは以下の通り。

| 実行環境 | CIDR |
| --- | --- |
| 本番 | x.x.x.x/16 |
| 検証 | x.x.x.x/16 |

## VPC Flow Logs

VPC 内トラフィックをログとして保管する。  
VPC Flow Logs はアクセス傾向の把握、拒否された通信の監視などに使用する。

VPC Flow Logs 設定。

| 項目 | 設定値 |
| --- | --- |
| 対象 | VPC or サブネット or ネットワーク・インターフェース |
| 保管先 | S3 or CloudWatch Logs |
| 保管期間 | 60日 |

## サブネット設計

VPC 内は目的に応じて複数のサブネットを作成する。  
サブネットはルートテーブル(経路情報)を基準に作成する。

### 本番環境サブネット

| サブネット名 | ルートテーブル | CIDR |
| --- | --- | --- |
| プライベートサブネット | VPC 内部通信に限定 |  |
| パブリックサブネット | Internet Gateway への経路を持つ |  |
| プロテクテッドサブネット | NAT Gateway への経路を持つ |  |
| システム間連携サブネット | VPC ピアリングへの経路を持つ |  |

### 検証環境サブネット

| サブネット名 | ルートテーブル | CIDR |
| --- | --- | --- |
| プライベートサブネット | VPC 内部通信に限定 |  |
| パブリックサブネット | Internet Gateway への経路を持つ |  |
| プロテクテッドサブネット | NAT Gateway への経路を持つ |  |
| システム間連携サブネット | VPC ピアリングへの経路を持つ |  |

## Internet GateWay

インターネットアクセスが必要なリソースが存在するため、Internet Gateway を使用する。

## NAT Gateway

アウトバウンドのみのインターネットアクセスが必要なリソースが存在するため、NAT Gateway を使用する。  
NAT Gateway は可用性確保のため Availability Zone ごとに作成する。

## VPC エンドポイント

プライベートサブネット上のリソースから AWS サービスへのアクセスのために VPC エンドポイントを作成する。

VPC エンドポイントがサポートされている AWS サービスは AWS ドキュメントに記載がある。  
[VPC エンドポイント](https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpc-endpoints.html)

## DNSサーバー

### パブリック

外部向けの公開 DNS サーバーは Route 53 を使用する。

### プライベート

VPC 内サーバーの名前解決は Route 53 プライベートゾーンを使用する。

## 踏み台サーバー

開発/運用拠点からのリモートログイン用に踏み台サーバーを設置する。  
踏み台サーバーは Single-AZ 構成とし、使用していない時間帯はシャットダウンしておく。

## VPC ピアリング

VPC 間通信には VPC ピアリングを使用する。  
VPC ピアリングを使用する場合は双方で VPC CIDR の重複が無いように留意する。  
VPC ピアリングを大量に使用すると管理上の複雑性やパフォーマンスの問題が発生する可能性がある。  
その場合は Transit Gateway などの代替案を検討すること。