VPCとの接続

VPCとのオンプレミス接続

VPN接続

専用線接続
（Direct connect）

Direct Connect

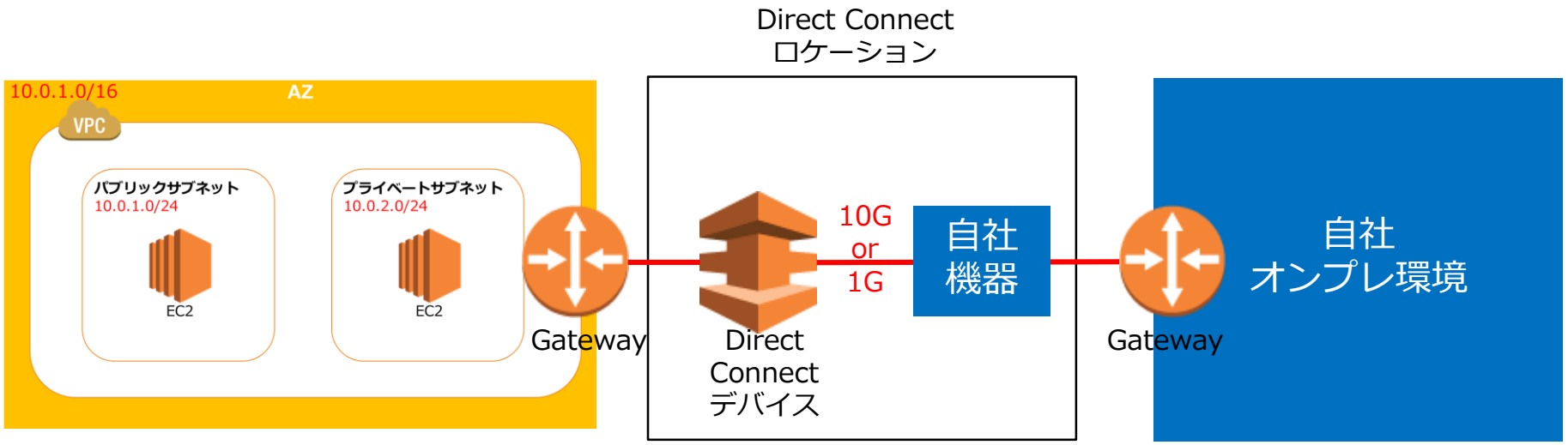
お客様のデータセンターやオフィスを専用線などを介してAWSへプライベートに接続するサービス

【Direct connectのメリット】

- 安価なアウトバウンドトラフィック料金
- ネットワーク信頼性の向上
- ネットワーク帯域幅の向上

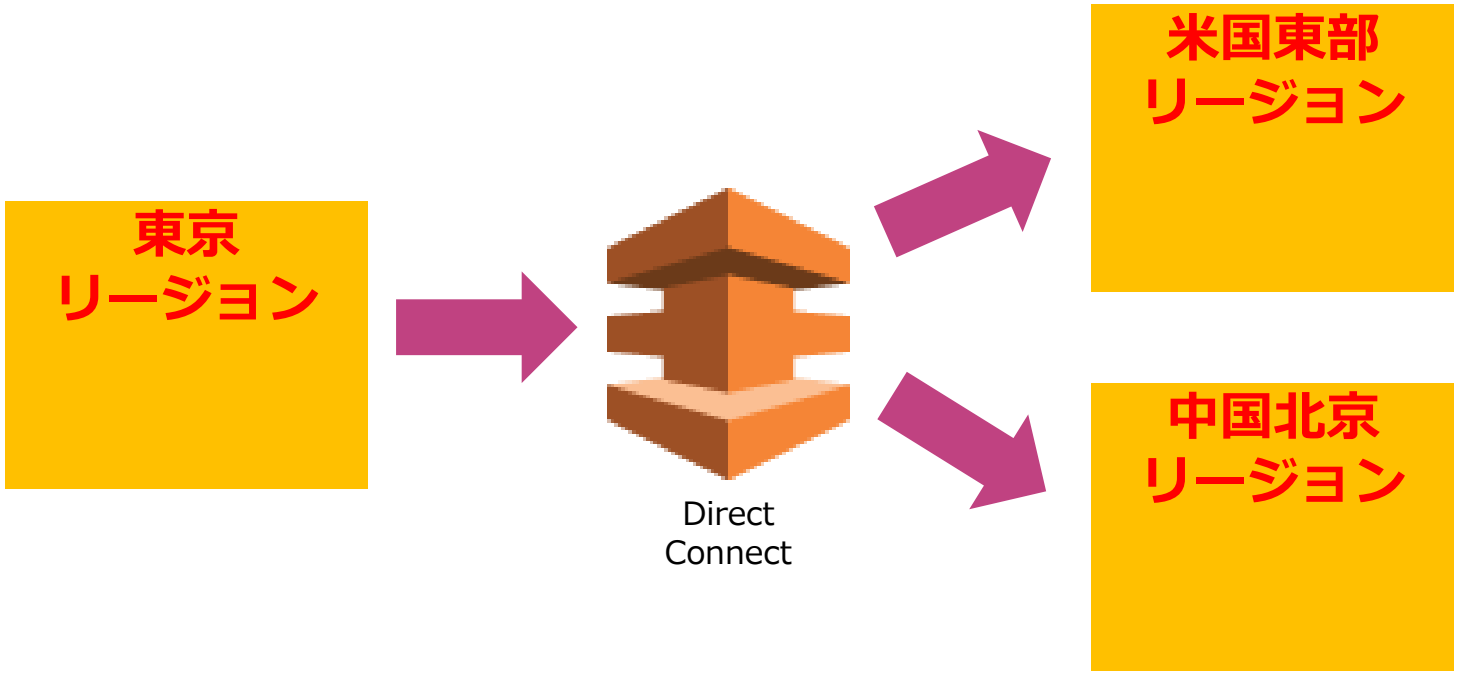
Direct Connect

Direct Connectロケーションに物理的に自社オンプレ環境を接続することでAWS環境との専用線接続を実現する



Direct Connect gateway

Direct Connect gatewayにより、同一アカウントに所属する複数リージョンの複数AZから複数リージョンの複数VPCに接続



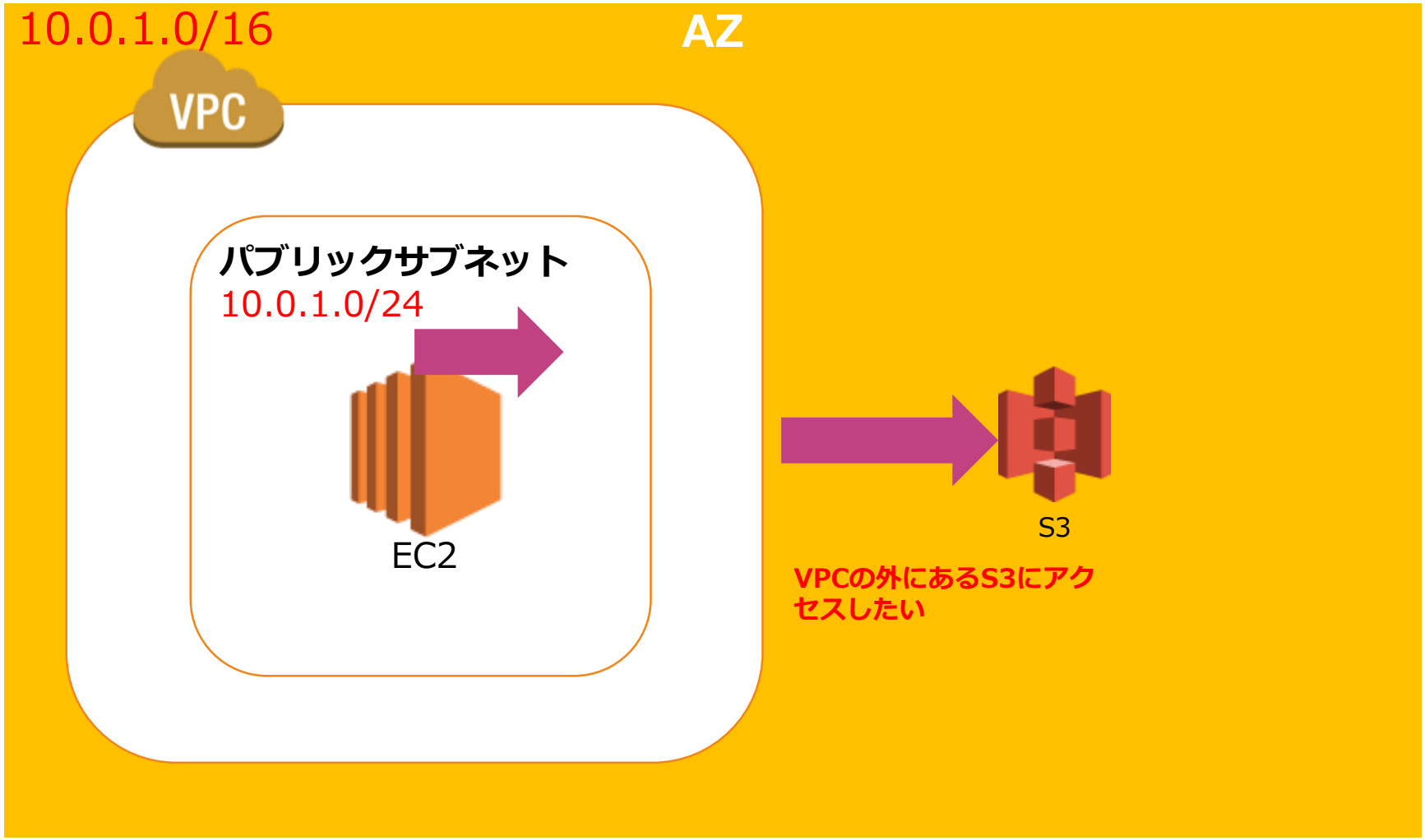
VPNとのDirect Connect

VPNの方が安く素早く利用できるが、信頼性や品質は専用線が勝る

	VPN	専用線
コスト	✓ 安価なベストエフォート回線が利用可能	✓ キャリアの専用線サービス契約が必要となりVPNより割高
リードタイム	✓ クラウド上での接続設定で可能なため即時	✓ 物理対応が必要なため数週間
帯域幅	✓ 暗号化のオーバーヘッドにより制限がある	✓ ポートあたり1G/10Gbps
品質	✓ インターネット経由のためネットワーク状態の影響を受ける	✓ キャリアにより高い品質が保証される
障害切り分け	✓ インターネットベースのため自社で保持している範囲以外の確認は難しい	✓ 物理的に経路が確保されているため比較的容易

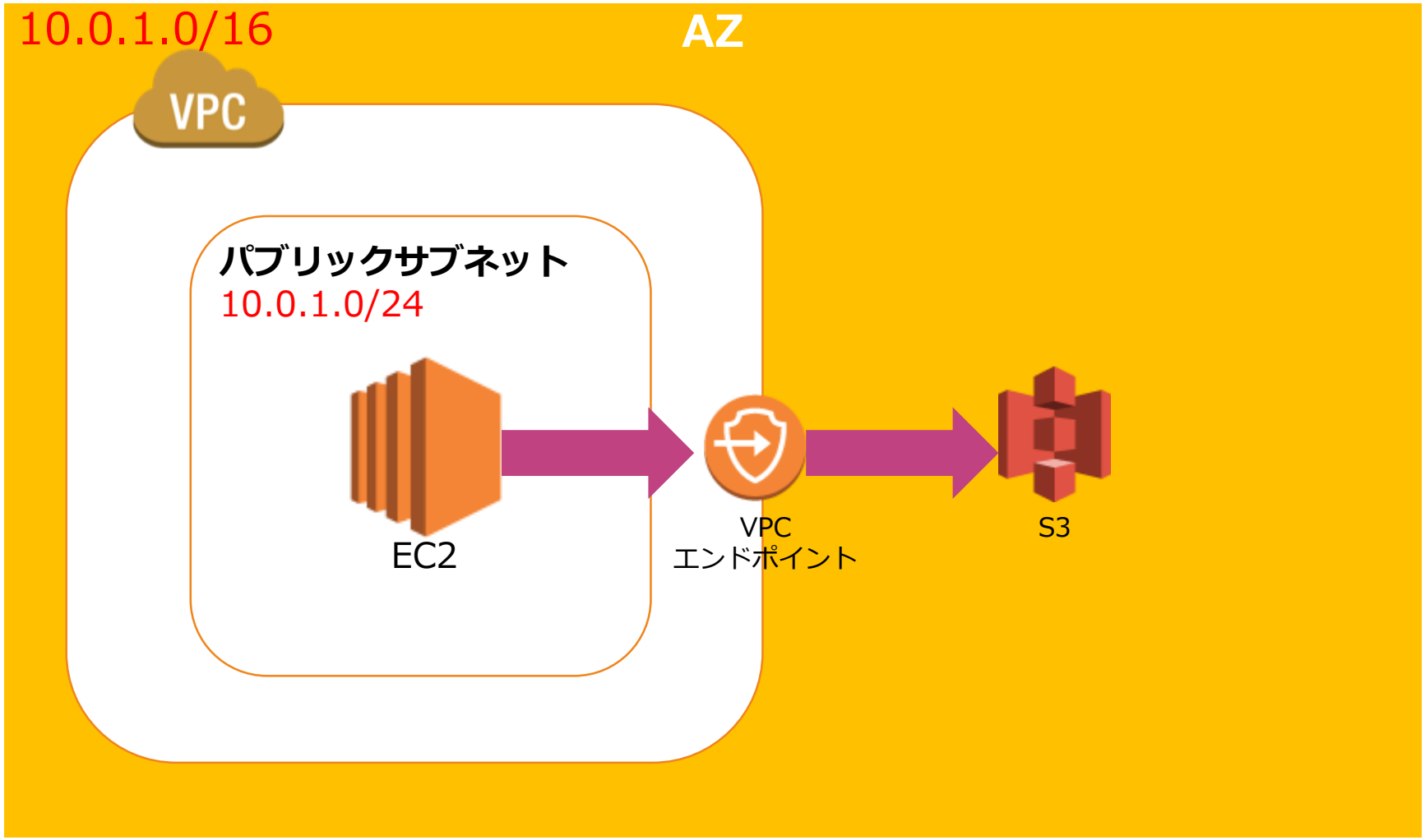
VPCエンドポイント

VPCエンドポイントはグローバルIPを持つAWSサービスに対して、VPC内から直接アクセスするための出口



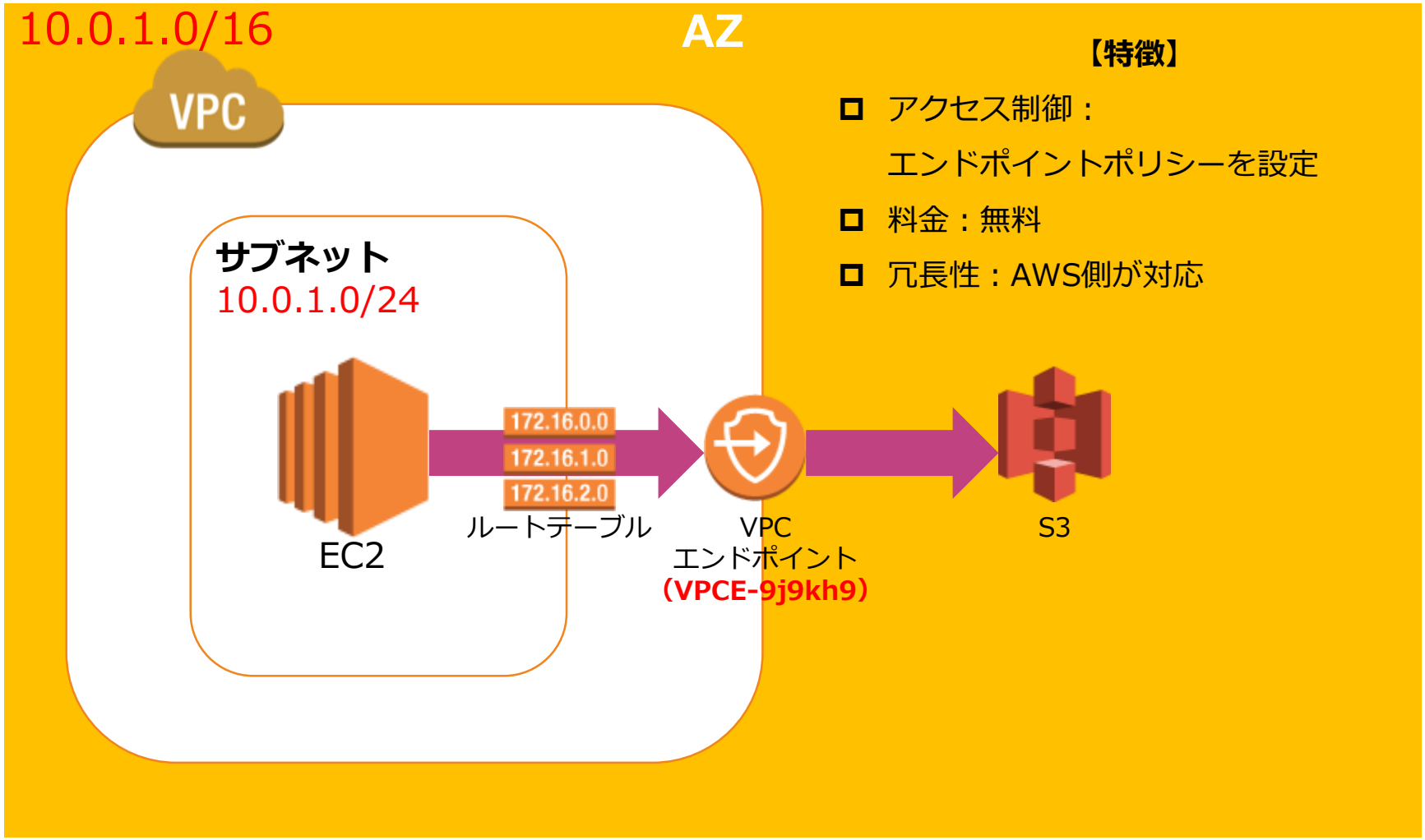
VPCエンドポイント

VPCエンドポイントはグローバルIPを持つAWSサービスに対して、VPC内から直接アクセスするための出口



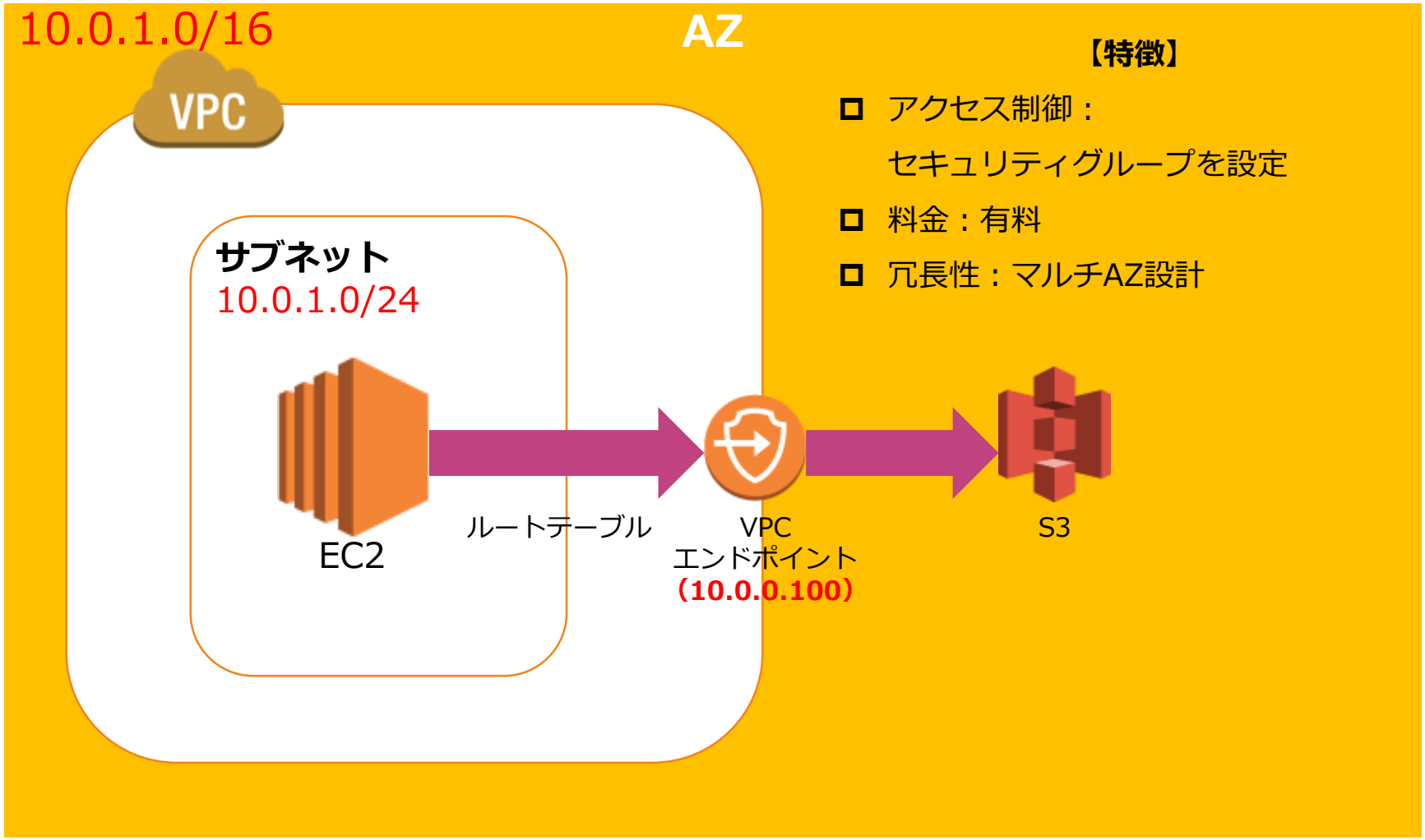
VPCエンドポイント

Gateway型はサブネットに特殊なルーティングを設定し、VPC内部から直接外のサービスと通信する



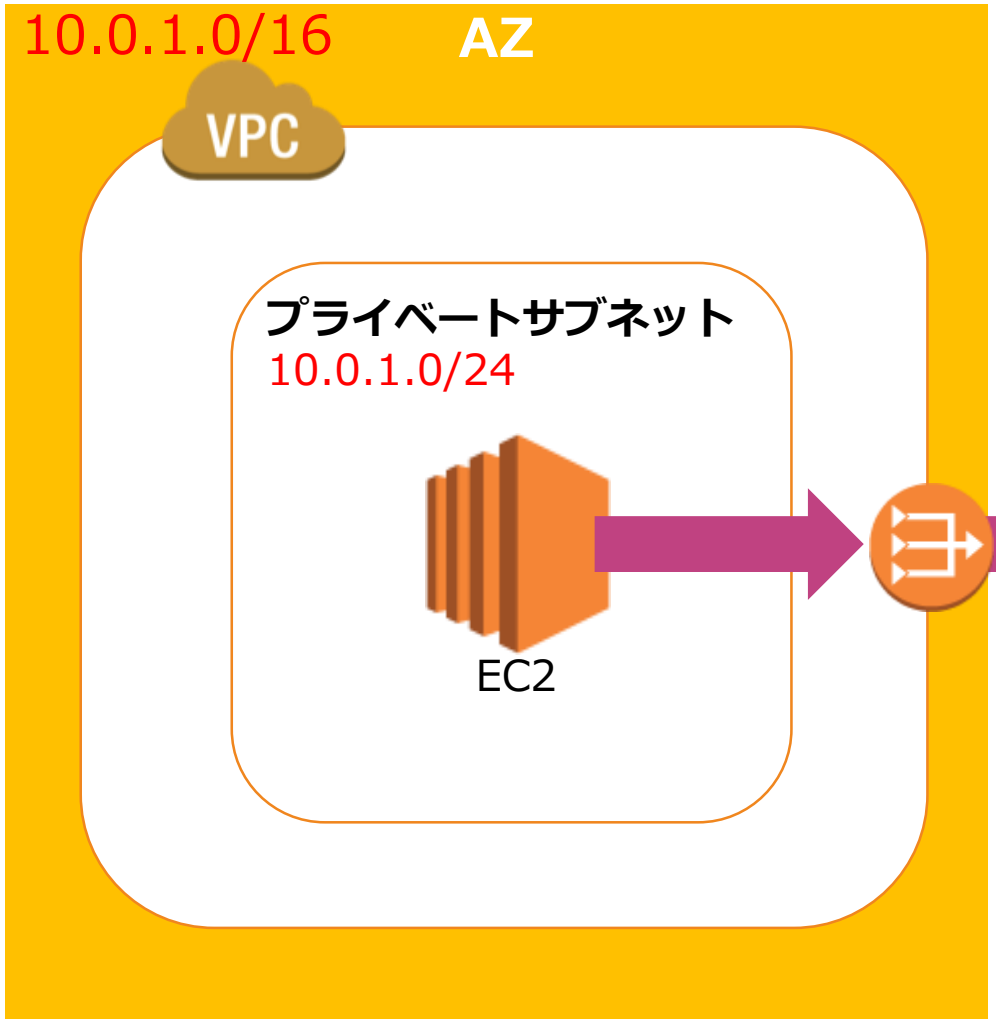
VPCエンドポイント

PrivateLink型はサブネットにエンドポイント用のプライベートIPアドレスを生成し、DNSが名前解決でルーティングする



NATゲートウェイ

NATゲートウェイによりプライベートサブネットのリソースがインターネットまたはAWSクラウドと通信が可能になる



【特徴】

- AWSによるマネージドNATサービス
- EIPの割り当て可能
- 最大10Gbpsの高パフォーマンス
- ビルトインで冗長化されている高可用性
- アベイラビリティゾーン毎に設置する

VPC Flow logs

VPC Flow Logsはネットワークトラフィックを取得しCloudWatchでモニタリングできるようにする機能

- ネットワークインタフェースを送信元/ 送信先とするトラフィックが対象
- セキュリティグループとネットワークACLのルールでaccepted/rejectされたトラフィックログを取得
- キャプチャウインドウと言われる時間枠 (約10分間)で収集・プロセッシング・保存する
- RDS、Redshift、ElasticCache、WorkSpacesのネットワークインタフェーストラフィックも取得可能
- 追加料金はなし

VPCの設定上限

VPCの各種設定においては上限数があるため、大規模に利用する場合は考慮する必要がある

リソース	数
リージョン当たりのVPCの上限数	5
VPC当たりのサブネットの上限数	200
AWSアカウント当たりの１リージョン内のElasticIP数	5
ルートテーブル当たりのルート上限数	100
VPC当たりのセキュリティグループの上限数	500
セキュリティグループ当たりのルールの上限数	50

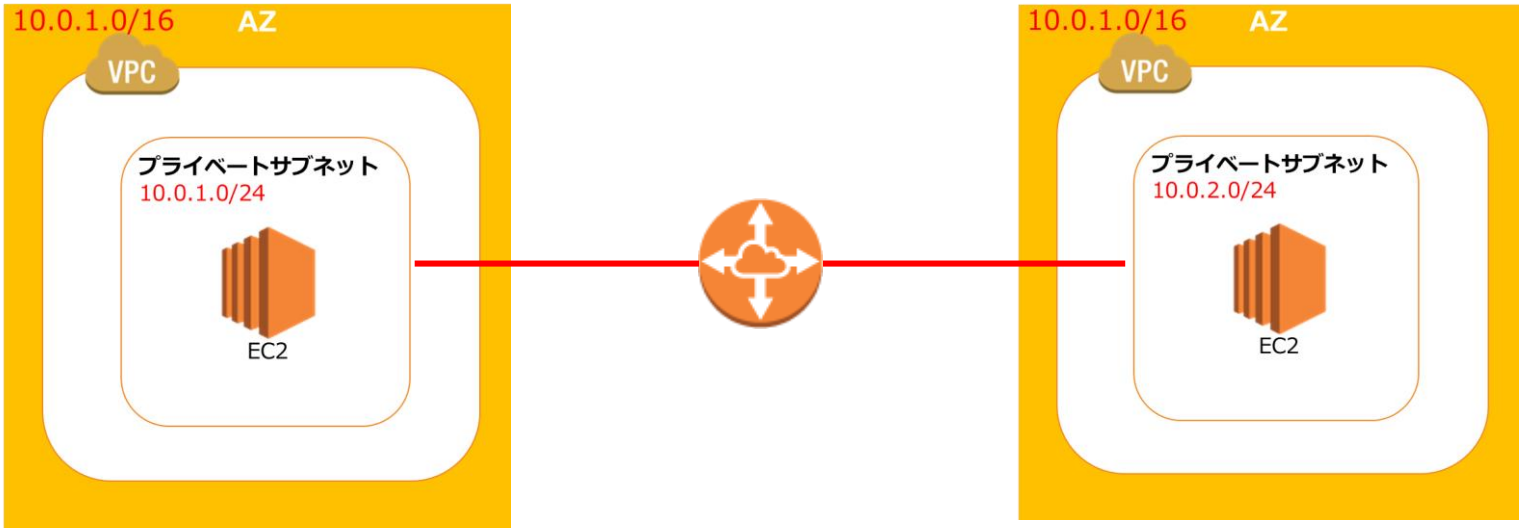
VPCを分割するケース

アプリサービスや組織構成などの用途に応じてVPCを分割する

- アプリケーションによる分割
- 監査のスコープによる分割
- リスクレベルによる分割
- 本番/検証/開発フェーズによる分割
- 部署による分割 共通サービスの切り出し

VPC Peering

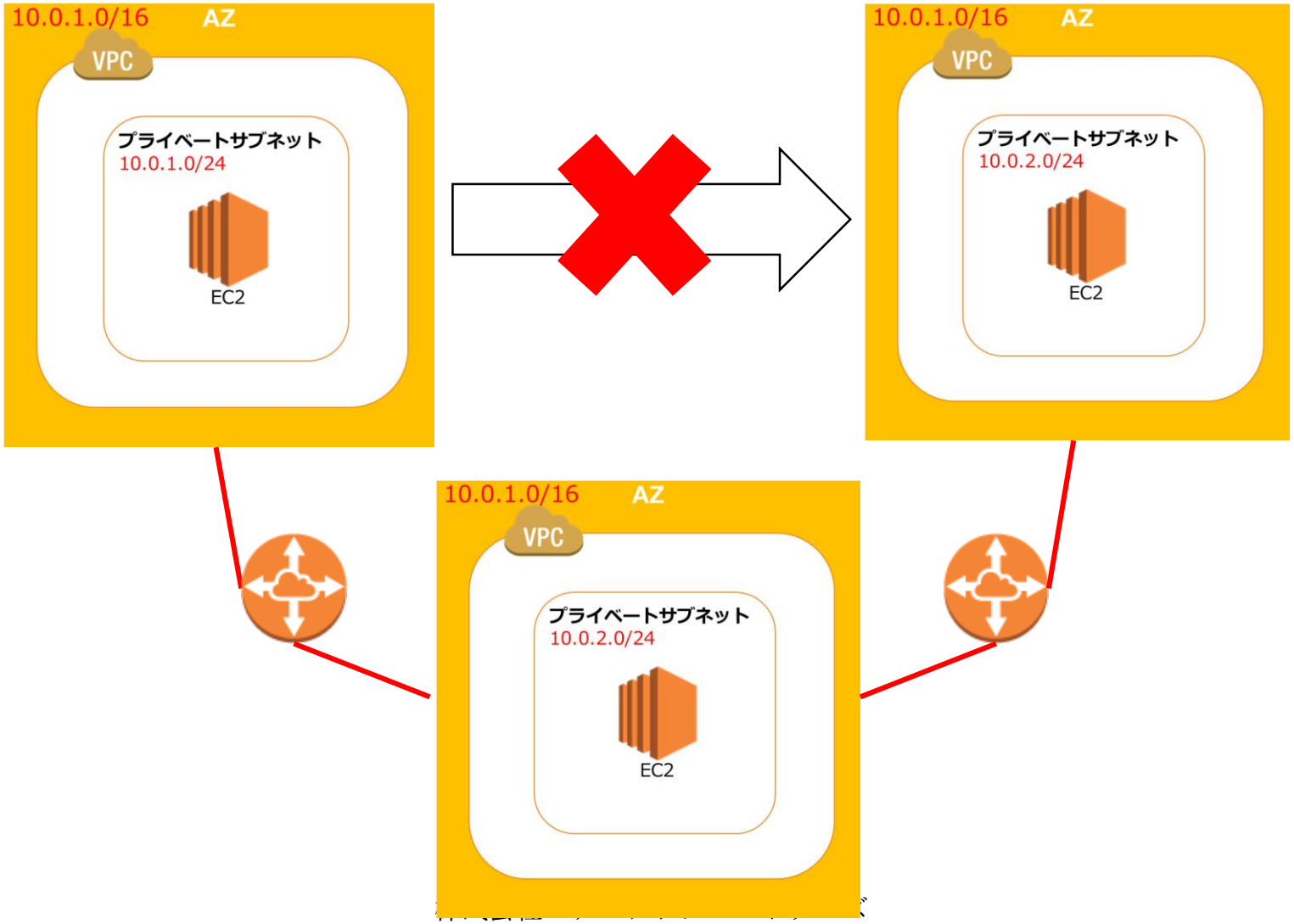
VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



- 異なるAWSアカウント間のVPC間をピア接続可能
- 一部のリージョン間の異なるVPC間のピア接続も可能
- 単一障害点や帯域幅のボトルネックは存在しない

VPC Peering

VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



VPC Peering

VPC peeringにより2つのVPC間でのトラフィックルーティングが可能