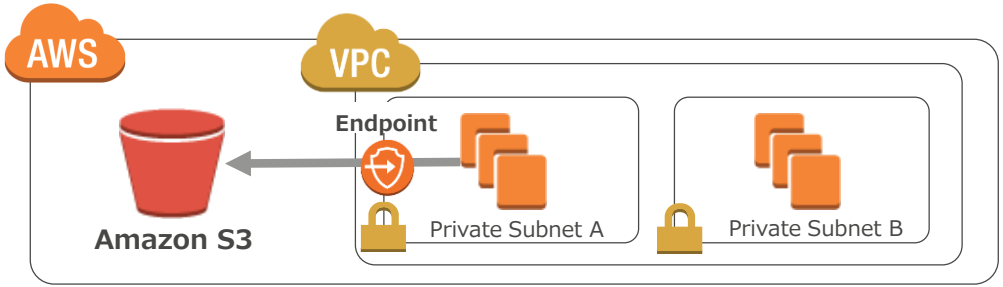
VPC Endpoint

(*) 2015.5月より

VPC内の**Private Subnet**上で稼働するサービスから、NAT GatewayやNATインスタンスを経由せずに直接S3とセキュアに通信させることが可能

- 通信可能なのは**同一リージョン**のS3のみ
- VPC管理画面のEndpointで作成し、S3と通信したいSubnetの**ルートテーブル**に追加
- Endpoint作成時にアクセスポリシーを定義し、通信可能なBucketや通信元のVPCの指定が可能 (バケットポリシーやIAMポリシーを利用したSource IPやVPC CIDRによる制限は利用不可)
- 別のVPCやSubnetを跨いだ直接のEndpointの利用は不可



http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-endpoints.html
http://aws.typepad.com/aws_japan/2015/05/vpcendpointfors3.html

amazon web services