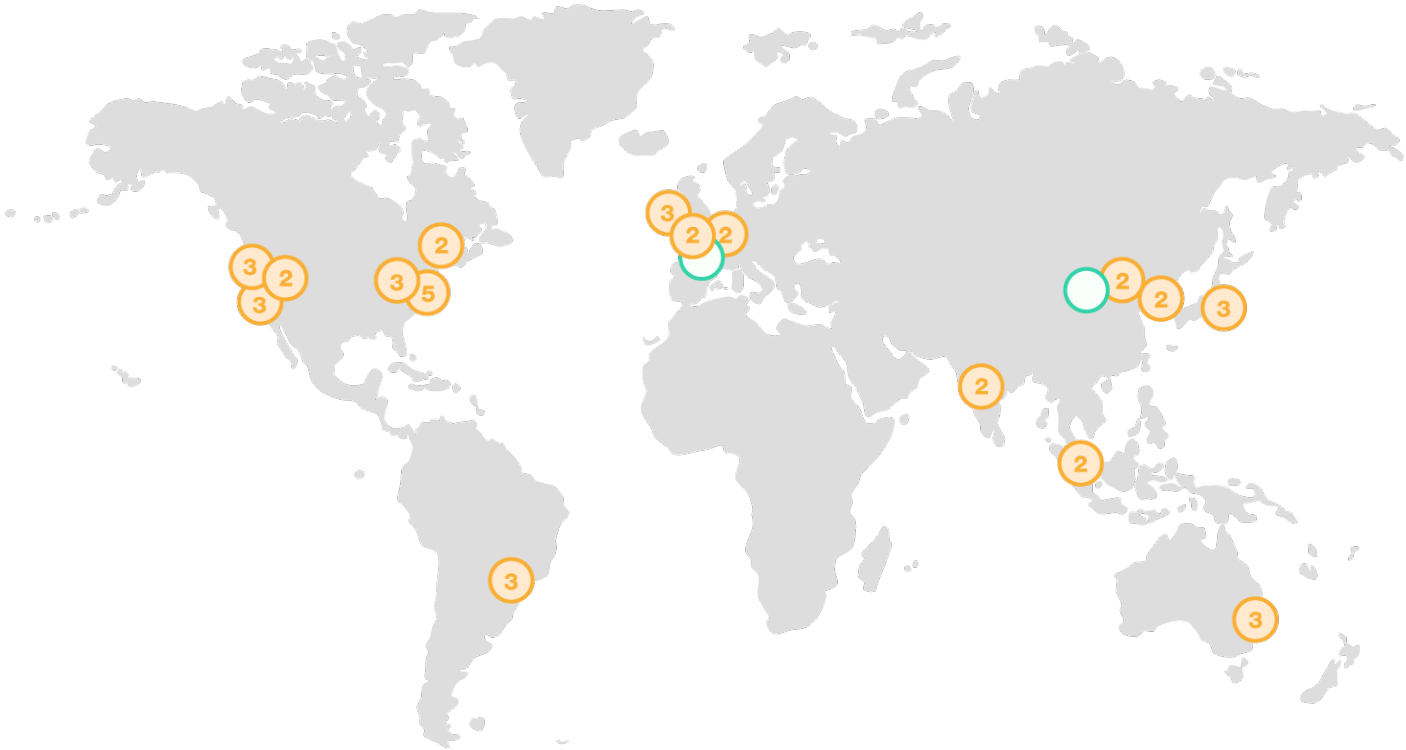
Amazon Web Services (AWS)における IPv6対応状況

2017.04.19

荒木靖宏 （yasuarak@amazon.co.jp）
Amazon Web Services
Principal Solutions Architect
Sr. Manager, Solutions Architecture

AWSの今日

16 Regions – 42 Availability Zones – 68 Edge Locations



Region & Number of Availability Zones

AWS GovCloud (2)

US West

Oregon (3)

Northern California (3)

US East

N. Virginia (5), Ohio (3)

Canada

Central (2)

South America

São Paulo (3)

EU

Ireland (3)

Frankfurt (2)

London (2)

Asia Pacific

Singapore (2)

Sydney (2), Tokyo (3),

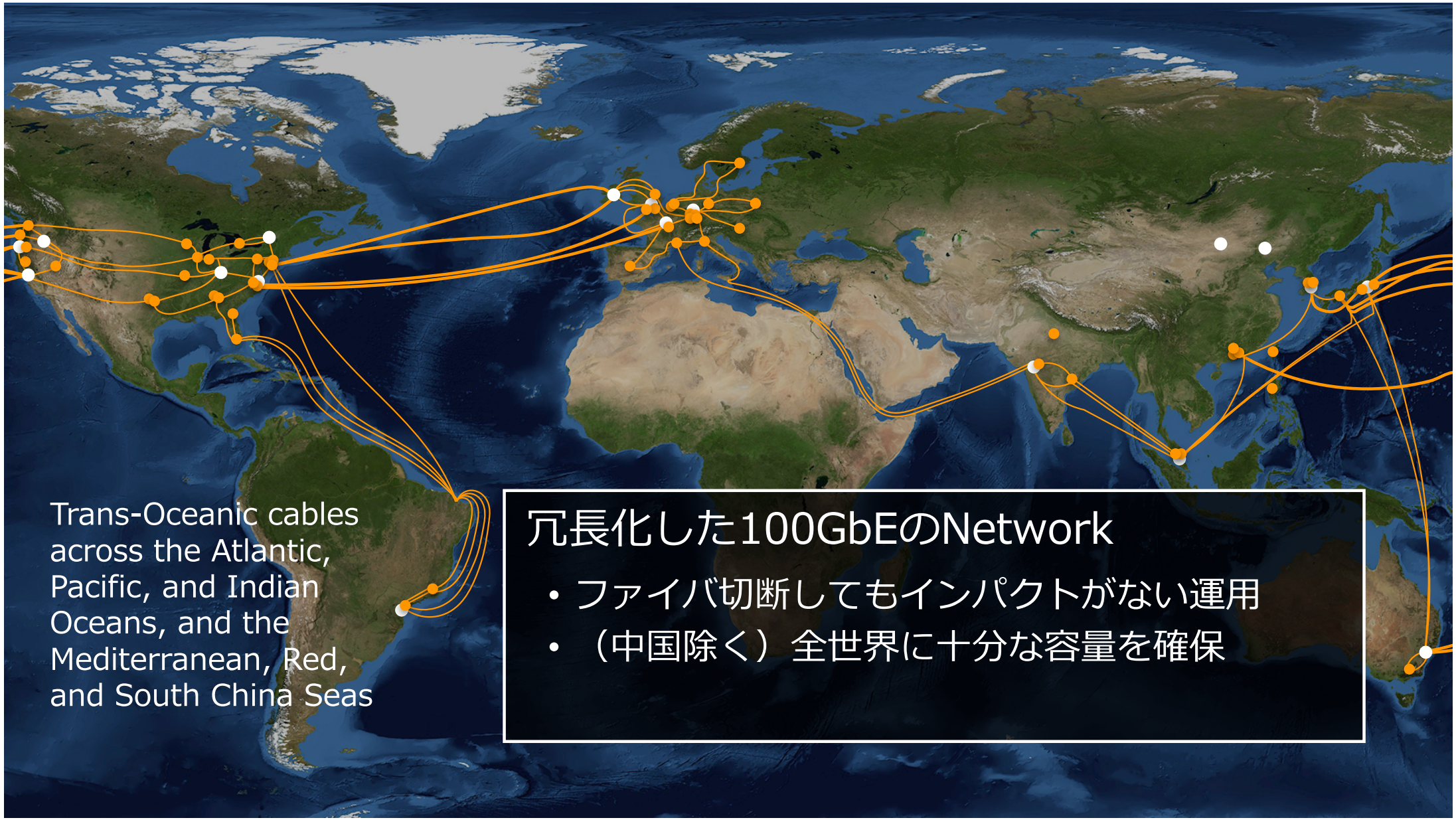
Seoul (2), Mumbai (2)

China

Beijing (2)

Announced Regions

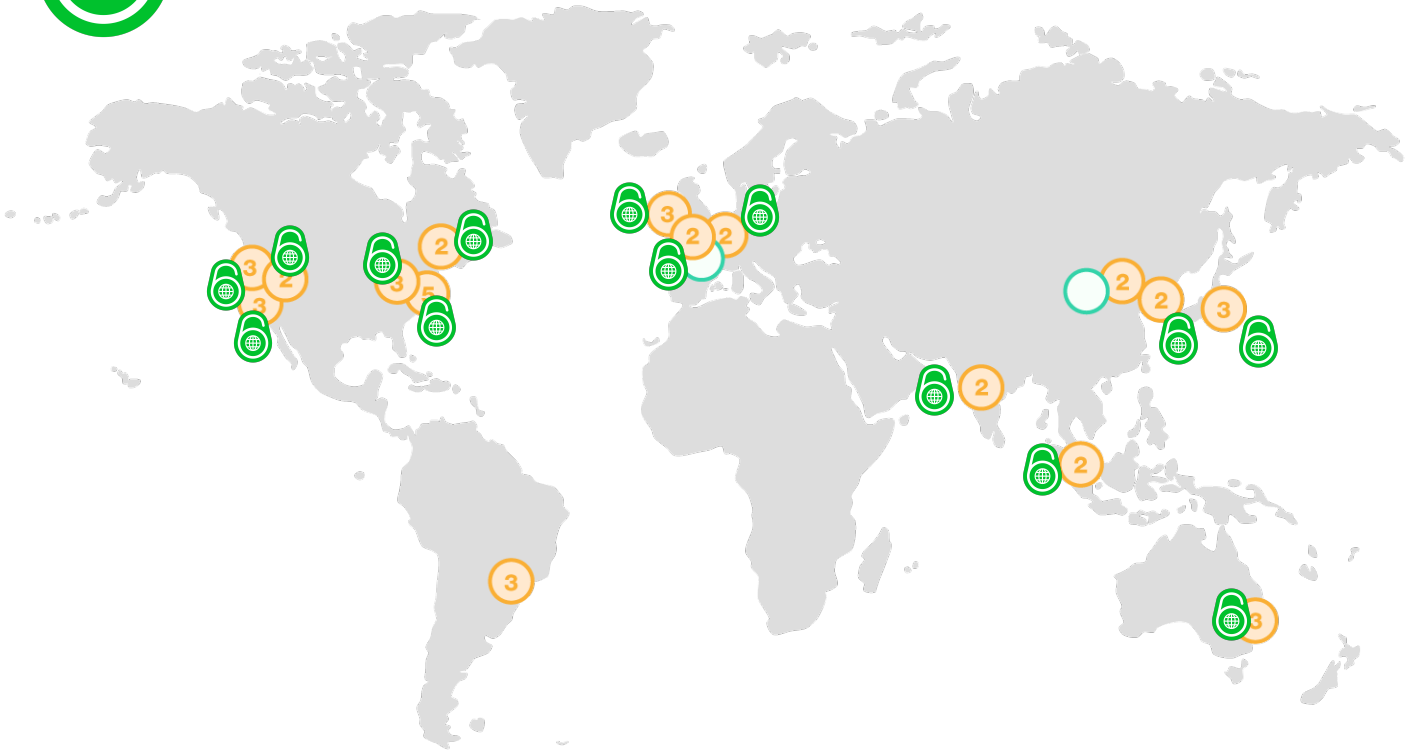
Paris, Ningxia


Trans-Oceanic cables across the Atlantic, Pacific, and Indian Oceans, and the Mediterranean, Red, and South China Seas
冗長化した100GbEのNetwork
• ファイバ切断してもインパクトがない運用
• （中国除く）全世界に十分な容量を確保

AWSのIPv6対応は中国以外の全てですすめられている

IPv6 available

Regions – 40 Availability Zones – 68 Edge Locations



Region & Number of Availability Zones

AWS GovCloud (2)

US West

Oregon (3)

Northern California (3)

US East

N. Virginia (5), Ohio (3)

Canada

Central (2)

South America

São Paulo (3)

EU

Ireland (3)

Frankfurt (2)

London (2)

Asia Pacific

Singapore (2)

Sydney (2), Tokyo (3),

Seoul (2), Mumbai (2)

China

Beijing (2)

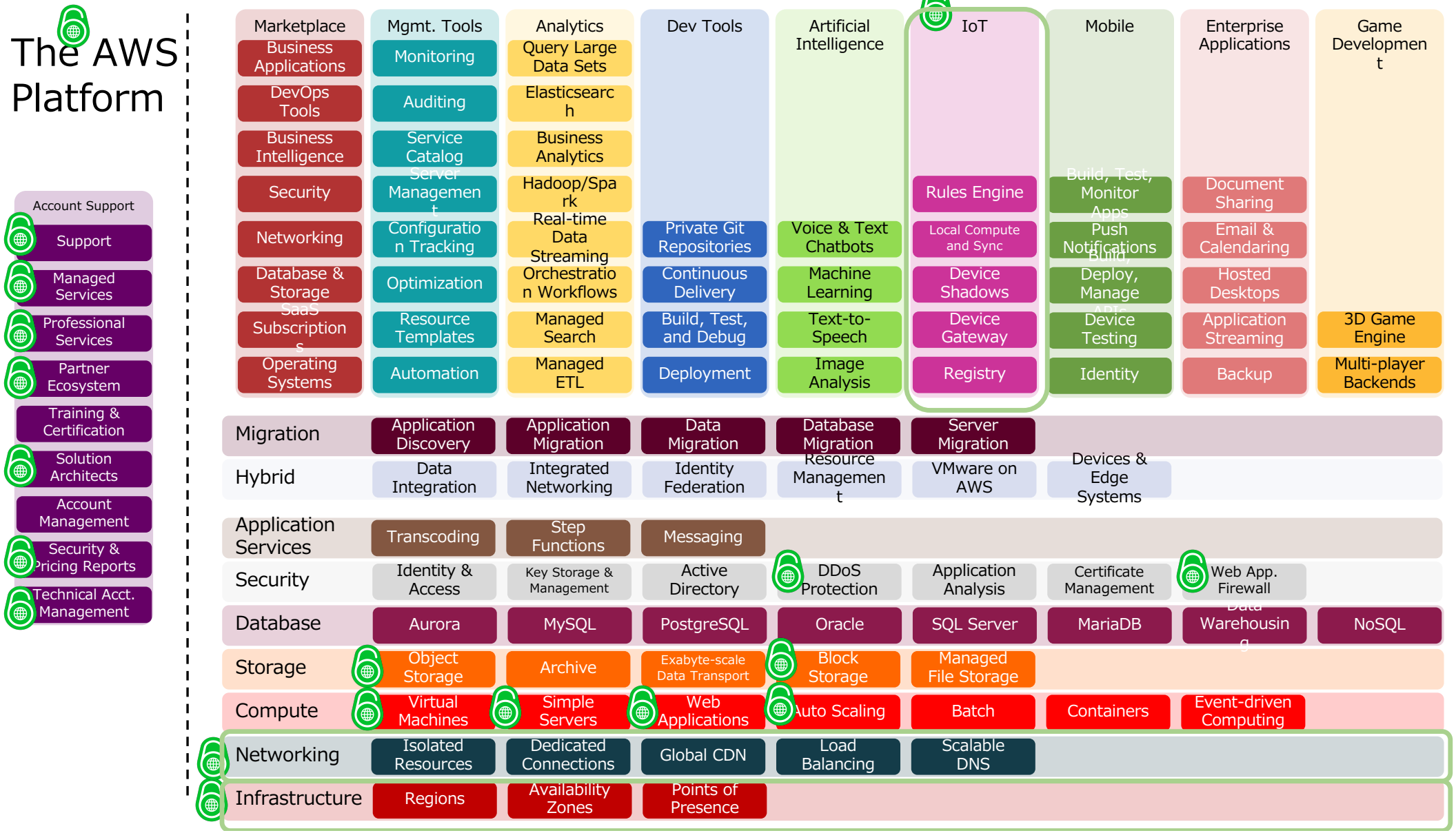
IPv4 Only

Announced Regions

Paris, Ningxia

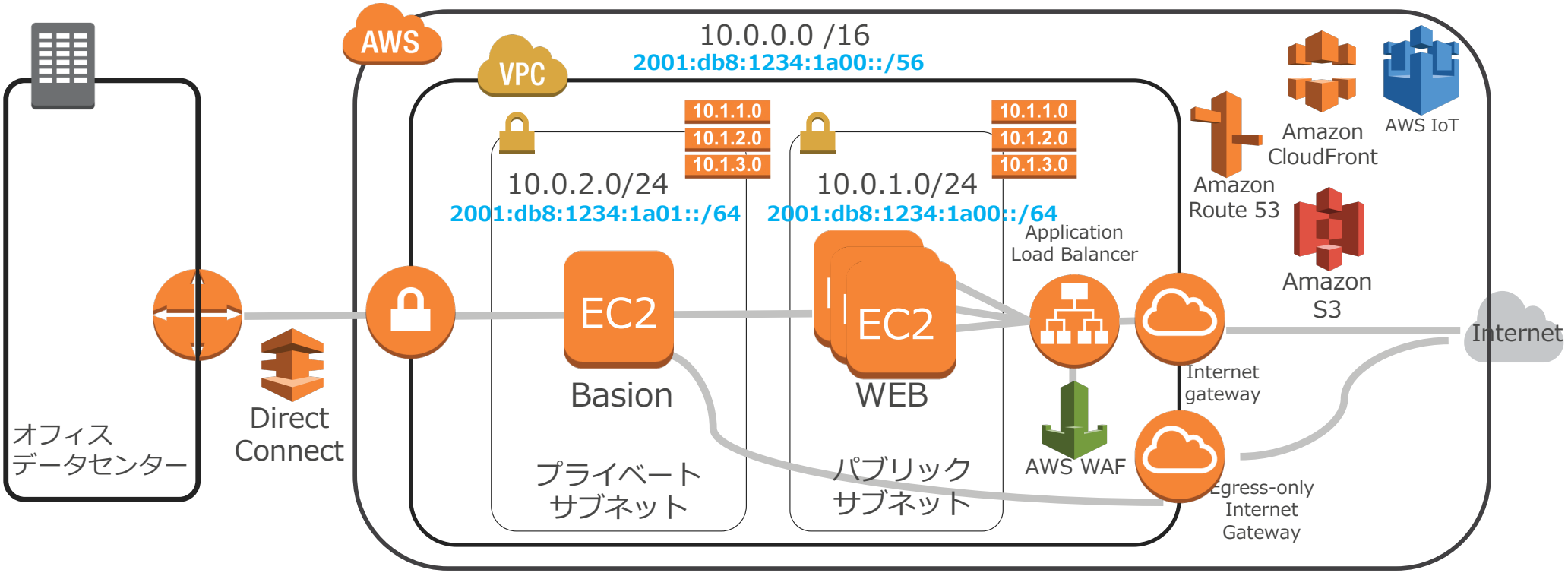
The AWS Platform

The AWS Platform



IPv6の対応

IoT、S3、CloudFront、WAF、Route53に続きVPC、ALBがIPv6対応



Egress-only Gateway(EGW) を利用して
IPv6においてもプライベート利用が可能

上記のような構成をIPv4/IPv6デュアルスタックで構築可能

https://aws.amazon.com/jp/blogs/news/new-ipv6-support-for-ec2-instances-in-virtual-private-clouds/

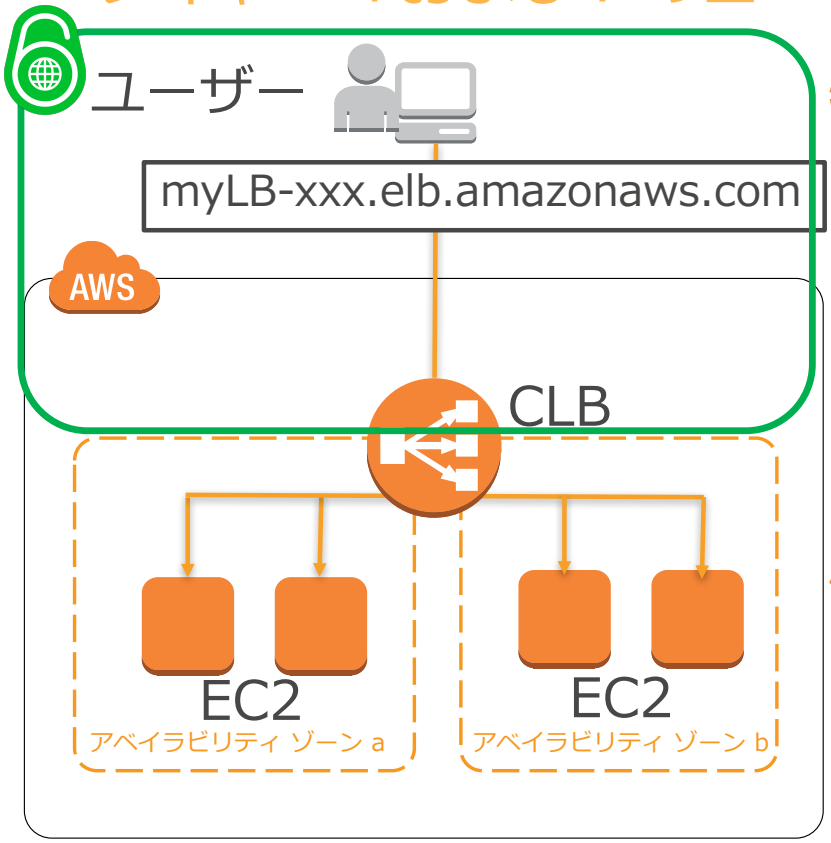
- Working Backwards

すべてはお客様から逆に考える

"We work backwards from the customer, rather than starting with an idea for a product and trying to bolt customers onto it."

Classic Load Balancer (CLB)

レイヤー４および７のロードバランサー



特徴 (https://aws.amazon.com/jp/elasticloadbalancing/classicloadbalancer/)

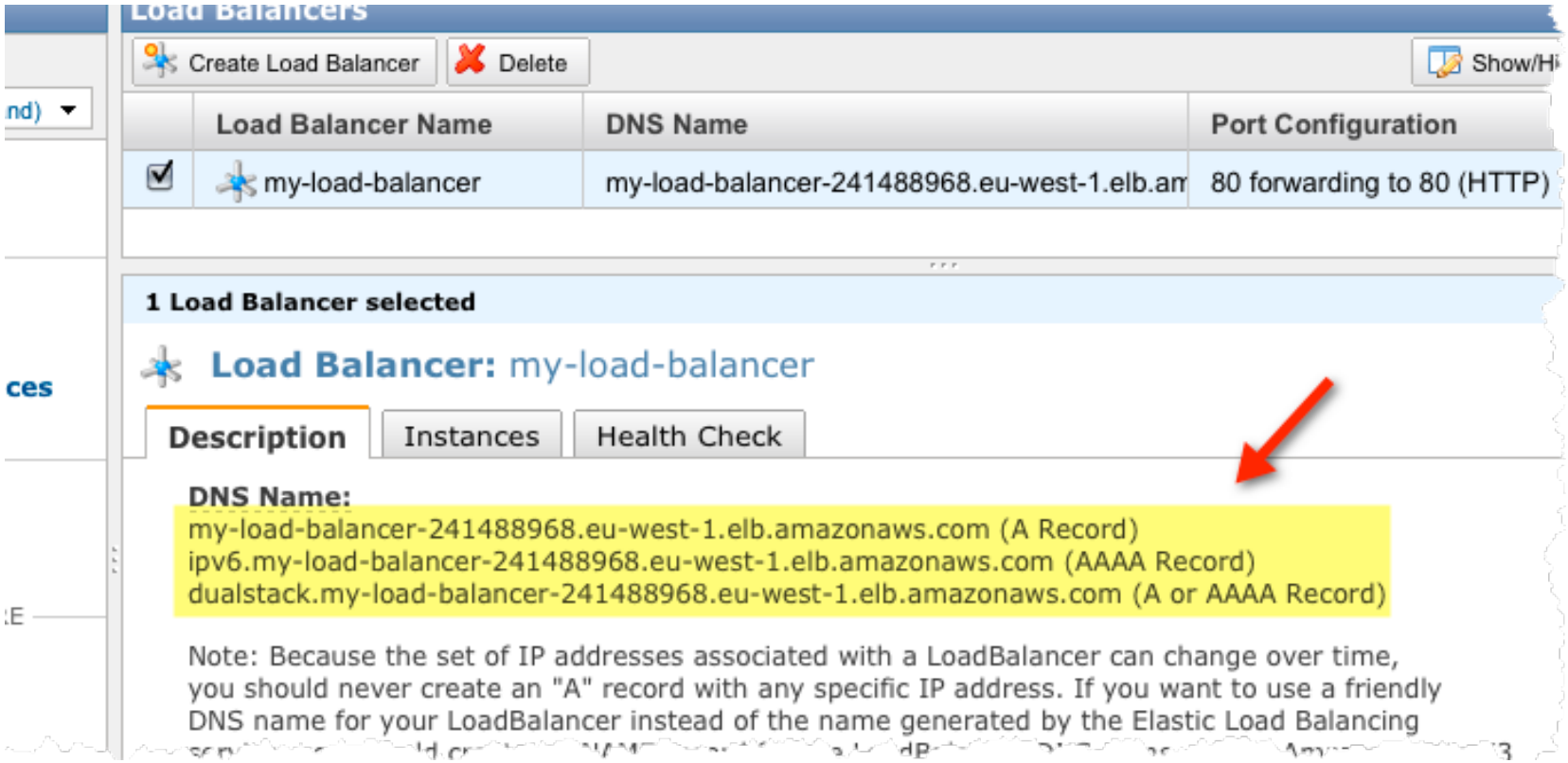
- 複数のAmazon EC2インスタンスに負荷分散
- 複数のアベイラビリティゾーンに跨って、高レベルの耐障害性を実現
- CLB自体が自動的にキャパシティを増減
- IPv4動作のバックエンドホストの前面でIP v 6を変換(EC2-Classicネットワーク向け)

価格体系

(https://aws.amazon.com/jp/elasticloadbalancing/classicloadbalancer/pricing/)

- CLBの起動時間
- CLBのデータ転送量

ELBにおけるIPv6はオプトイン



Web向けIPv６サポートは2011年５月から

AWS Blog

Elastic Load Balancing – IPv6, Zone Apex Support, Additional Security

by Jeff Barr | on 24 MAY 2011 | in Amazon Elastic Load Balancer | Permalink | Comments

We've added three new features to EC2's Elastic Load Balancing feature:

- **IPv6 Support** – All Elastic Load Balancers in the US East (Northern Virginia) and EU (Ireland) regions now have publicly routable IPv6 addresses in addition to their existing IPv4 addresses.
- **Zone Apex Support** – You can now point the root or apex of your Route 53 hosted zone to your Elastic Load Balancer.
- **EC2 Security Group Support** – You can now configure an EC2 Security Group for your application instances such that they accept traffic only from an Elastic Load Balancer.

Here's the scoop:

IPv6 Support

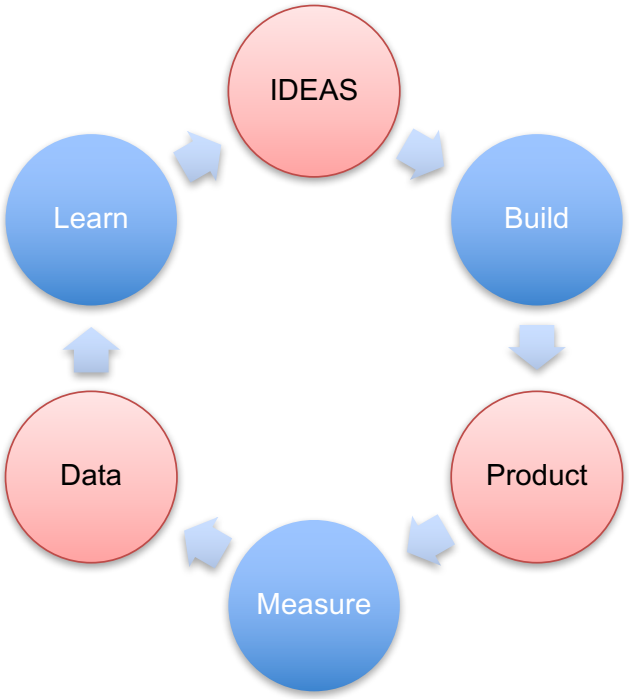
You've probably read some panic-inducing articles about the fa r to support the continued growth in the number of devices connected to the Int n of the IP protocol, commonly known as IPv6. This version of the protocol n incredible 2^{128}, and also lays the groundwork for other capabilities in the future.

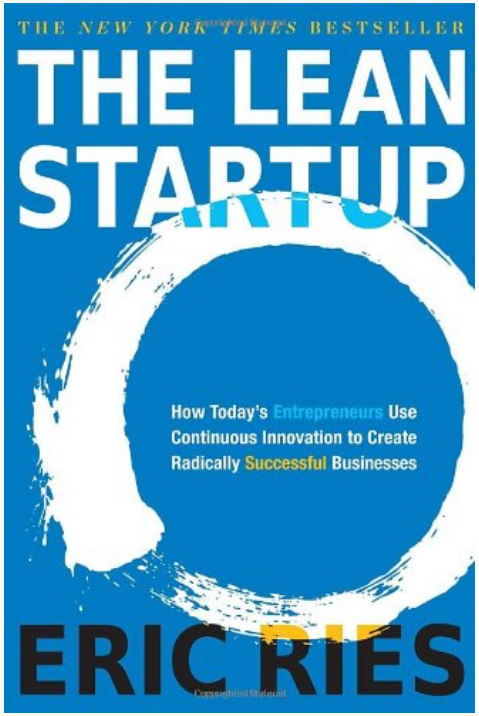
The migration from IPv4 to IPv6 is now underway across the globe. This migration creates many technical and challenges for all

2011.June.8のWorld IPv6 dayでは、実際に多くのAWS顧客がこの機能を使用して対応

ユーザのフィードバックに早く対応するのが成功の鍵

- スタートアップのバイブル”リーンスタートアップ”で提唱された考え方
- MVP(Minimum Viable Product：実現最小限の機能）を定義
- ユーザのフィードバックをベースに進化させる

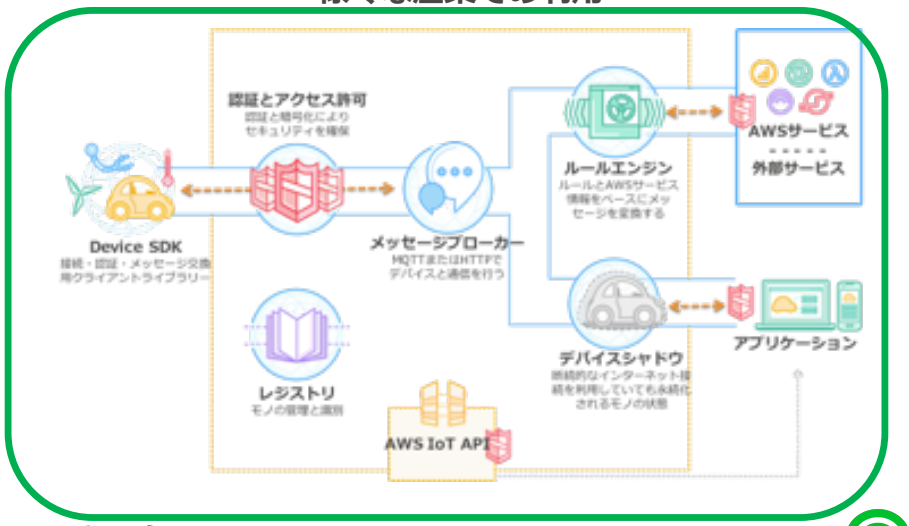




AWS IoT

簡単で安全なクラウドへのデバイス接続サービス

様々な産業での利用



アーキテクチャ図

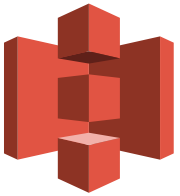
特徴 (https://aws.amazon.com/jp/iot/)

- デバイスとクラウドの双方向コミュニケーション
- HTTP、MQTT、Websocketに対応
- SQLベースのルールとアクション定義
- AWSサービスとのシームレスな連携
- デバイス向けのSDK

価格体系 (https://aws.amazon.com/jp/iot/pricing/)

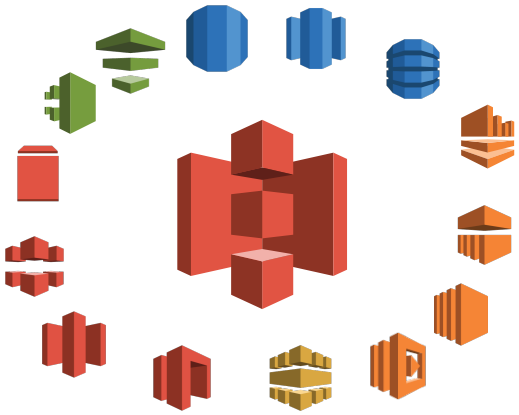
- 100万メッセージあたり$8(日本リージョン)
- 無料利用枠利用は25万メッセージ/月を(1年間)

Amazon Simple Storage Service (S3)



マネージドオンラインストレージサービス

Amazon S3



特徴 (http://aws.amazon.com/jp/s3/)

- 高い堅牢性 99.999999999%
- 格納容量無制限。利用した分のみ課金
- 様々なAWSサービスと連携するセンターストレージ
- APIおよびRESTのWebサーバ機能を持つ

価格体系 (http://aws.amazon.com/jp/s3/pricing/)

- データ格納容量
- データ転送量(OUT)
- APIリクエスト数

Amazon CloudFront

マネージドCDN(Contents Delivery Network)サービス

特徴 (http://aws.amazon.com/jp/cloudfront/)

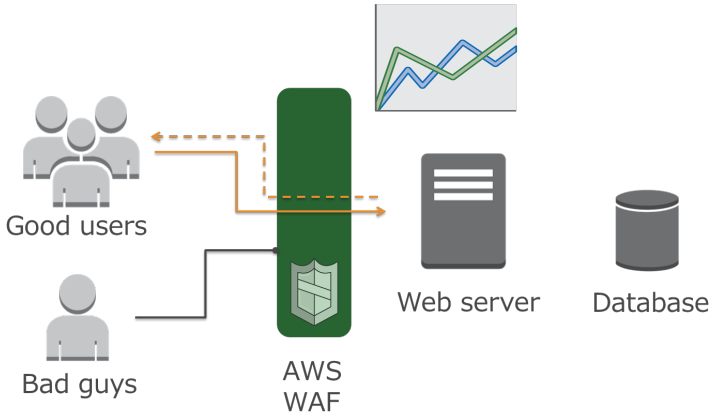
- 簡単にサイトの高速化が実現できると共に、サーバの負荷も軽減
- 様々な規模のアクセスを処理することが可能
- 世界70箇所のエッジロケーション

価格体系 (http://aws.amazon.com/jp/cloudfront/pricing/)

- データ転送量(OUT)
- HTTP/HTTPSリクエスト数
- (利用する場合)SSL独自証明書 など

AWS WAF(Web Application Firewall)

AWSが提供するウェブアプリケーションファイアウォール



特徴 (https://aws.amazon.com/jp/waf/)

- カスタムルールによるアクセス制御を実現
- SQLインジェクションやXSS攻撃などへの対応が可能。APIを利用した動的なルールの変更もサポート

CloudFrontとALB(Application Load Balancer)で利用できる

価格体系 (https://aws.amazon.com/jp/waf/pricing/)

- ウェブACLの数とルール数
- リクエスト数

Amazon Route53

高い可用性と豊富な機能を提供するフルマネージドな権威DNS

Route53の特徴的な機能

- 各ネームサーバは冗長化され世界中に分散配置。
- IP Anycast
- ヘルスチェック/DNSフェイルオーバー
- 重み付けラウンドロビン
- レイテンシーベースルーティング
- ジオルーティング
- ドメイン取得と管理
- AAAA, Query in IPv6

特徴 (http://aws.amazon.com/jp/route53/)

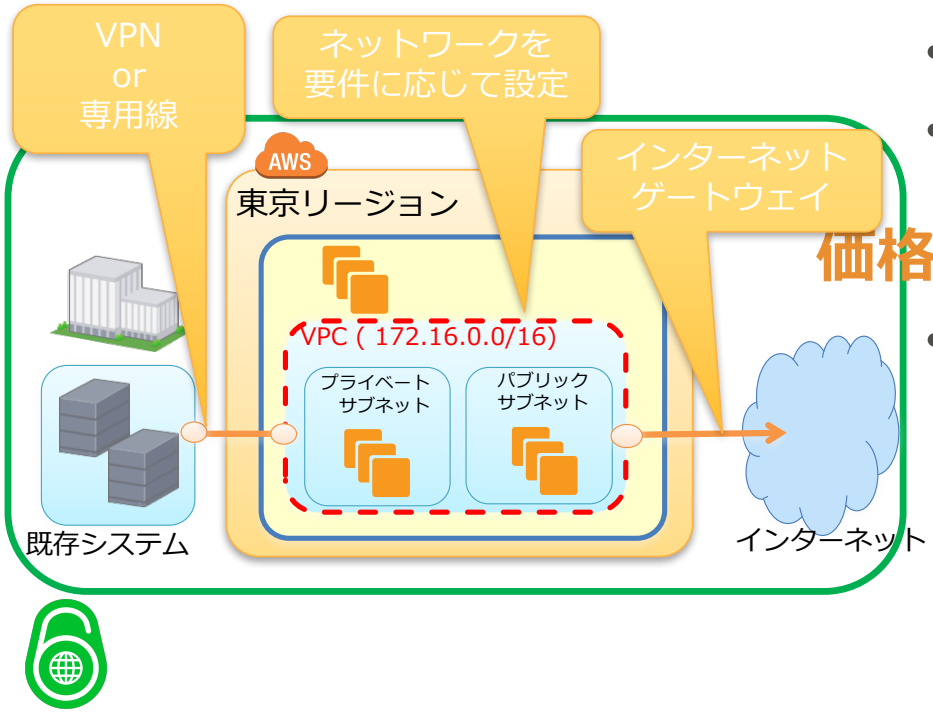
- 高い可用性：Amazon Route53は世界中に配置されたサーバーによって、非常に高い可用性を提供。
- 多様な機能：管理ホストに対するヘルスチェックや様々なアルゴリズムによるラウンドロビンなど、柔軟なアプリケーションの運用を助ける機能が豊富。
- アプリケーションの内部DNSをとしても利用可能。

価格体系 (http://aws.amazon.com/jp/route53/pricing/)

- 非常に低価格なのが特徴。
- ホストするゾーンあたり 0.5USD/月
- 標準クエリ：１０億クエリあたり0.4USD

Amazon Virtual Private Cloud (VPC)

仮想プライベートクラウドサービス



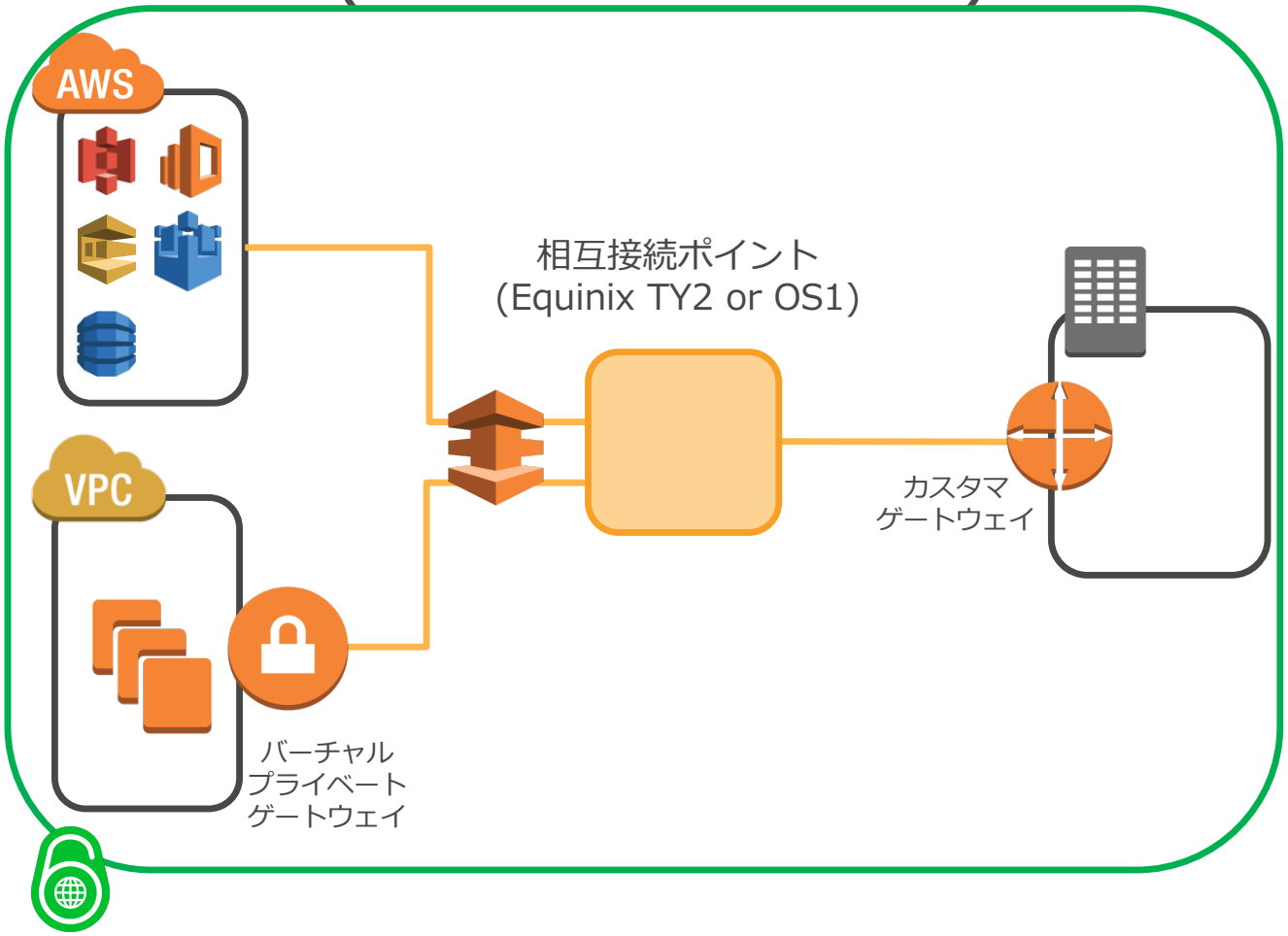
特徴 (http://aws.amazon.com/jp/vpc/)

- AWS上にプライベートネットワークを構築
- AWSと既存環境のハイブリッド構成を実現
- きめ細かいネットワーク設定が可能

価格体系 (http://aws.amazon.com/jp/vpc/pricing/)

- VPCの利用は無料

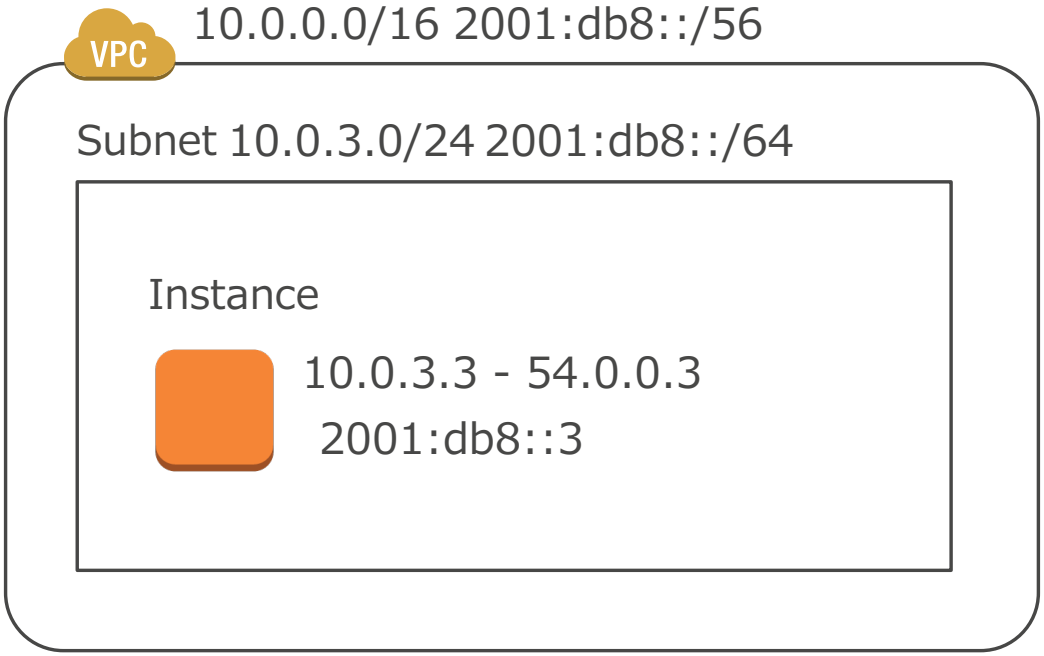
専用線(Direct Connect)接続構成



- AWSとお客様設備を専用線でネットワーク接続
- 相互接続ポイントへ専用線を敷設し、AWSのルータと相互接続
- 日本の相互接続ポイントは
  - 東京(Equinix TY2)
  - 大阪(Equinix OS1)
- ルーティングはBGPのみ
- 接続先は以下の２つ
  - VPC(プライベート接続)
  - AWSクラウド(パブリック接続)
- VPNよりも一貫性がある
- 帯域のパフォーマンスも向上
- ネットワークコストも削減

コンセプト：IPv6 in Amazon VPC

- IPｖ６を有効にした場合には、デュアルスタックとなる



コンセプト：IPv6 in Amazon VPC

- IPv4がデフォルト。 IPv6 はオプトイン

My VPCs

Name	IPv4 CIDR	IPv6 CIDR
My Default VPC	172.31.0.0/16	
IPv6 Demo	10.100.0.0/16	2600:1f16:266:fa00::/56

My Subnets

Name	IPv4 CIDR	IPv6 CIDR
Dual-stack Subnet	172.31.32.0/20	2600:1f16:342:d700::/64
IPv4-only Subnet	172.31.16.0/20	

コンセプト：IPv6 in Amazon VPC

インスタンス情報

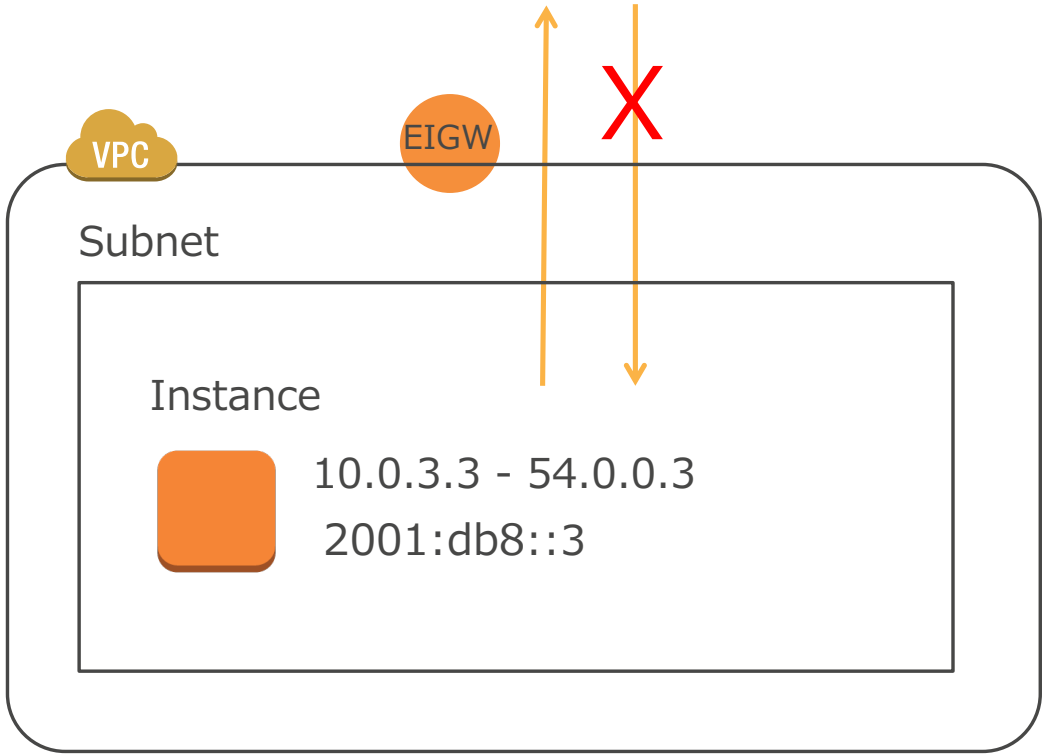
Name	Instance State	IPv4 Public IP	IPv6 IPs	Private IP Address
vpc-2	running	52.15.170.128	-	172.16.0.176
demo-a	running	52.15.142.67	2600:1f16:266:fa00:700:20cb:5f20:3dff	10.100.0.119
demo-c	running	52.15.95.116	2600:1f16:266:fa02:ddd7:f6cb:9496:bbef	10.100.2.222

コンセプト：IPv6グローバルユニキャストアドレス

- IPv6を有効にしたVPCではグローバルユニキャストアドレス(GUA)を使う
- それぞれのインスタンスはGUAが付与される
- １：１のNATは存在しない
- GUAの使用はセキュリティやプライバシ問題発生を意味しない。ルートテーブル、セキュリティグループ、ゲートウェイは別途設定する。

Egress-only Internet Gateway

- IPv6インターネットアクセスのための仮想デバイスを導入
- コスト負担なし
- パフォーマンスや可用性の制限はない



コンセプト：
セキュリティグループ、ルートテーブル、NACL

- IPv6もIPv4も同様に設定、動作する

Example Security Group Rules

Type	Protocol	Port Range	Source
ALL UDP	UDP (17)	ALL	sg-84b760ed
ALL Traffic	ALL	ALL	0.0.0.0/0
ALL Traffic	ALL	ALL	::/0

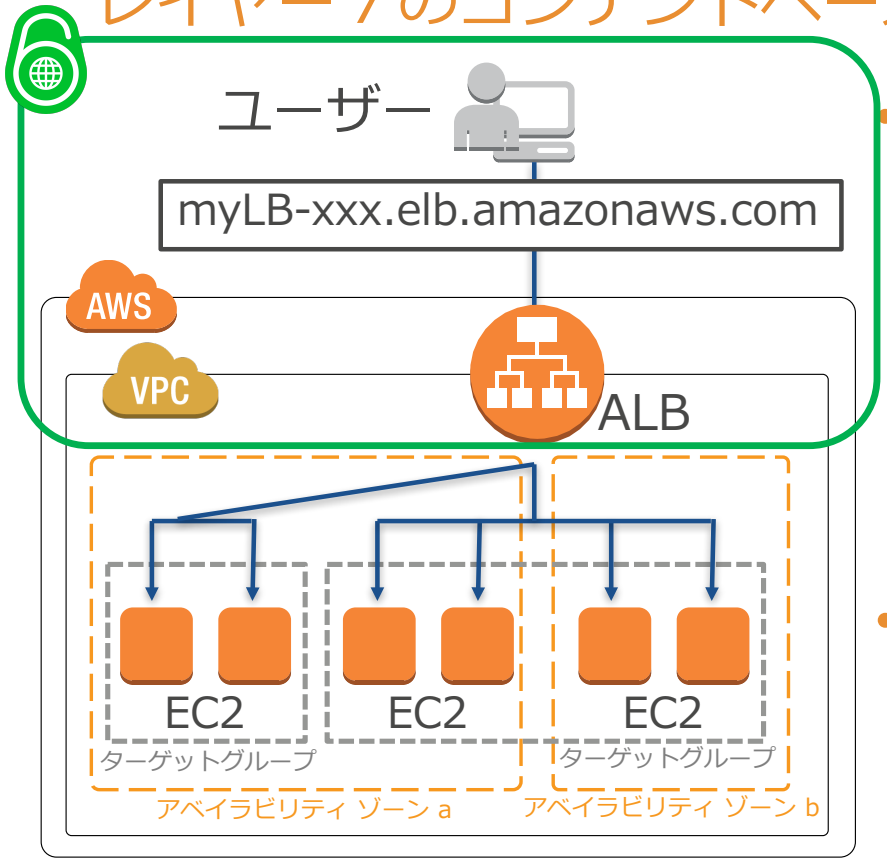
VPCにおけるIPv4とIPv6の特徴と制限

	IPv4	IPv6
アドレス体系	32bit	128bit
VPCでの利用	デフォルトで適用	オプトイン （自動適用ではなく任意）
CIDRブロックサイズ	16～28bitで選択 自分で任意のアドレスを設定可能	56bit固定 Amazon保有のprefixから自動で56bit CIDRがアサインされる（選べない）
サブネット ブロックサイズ	16～28bitで選択	64bit固定
パブリックIP/ プライベートIP	それぞれ存在 （NATを介してパブリックIPをプライマリプライベートIPにMAP）	パブリックのみ （プライベートにするにはEgress-only Internet Gatewayを利用）
インスタンスタイプ	全てのインスタンスタイプ	M3、G2を除く全ての現行世代のインスタンスタイプでサポート
アマゾン提供DNS	プライベートIP、Elastic IPに対するそれぞれのDNSホスト名を受信	提供されるDNSホスト名はなし
閉域接続	VPN、DirectConnect	DirectConnectのみ

http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html

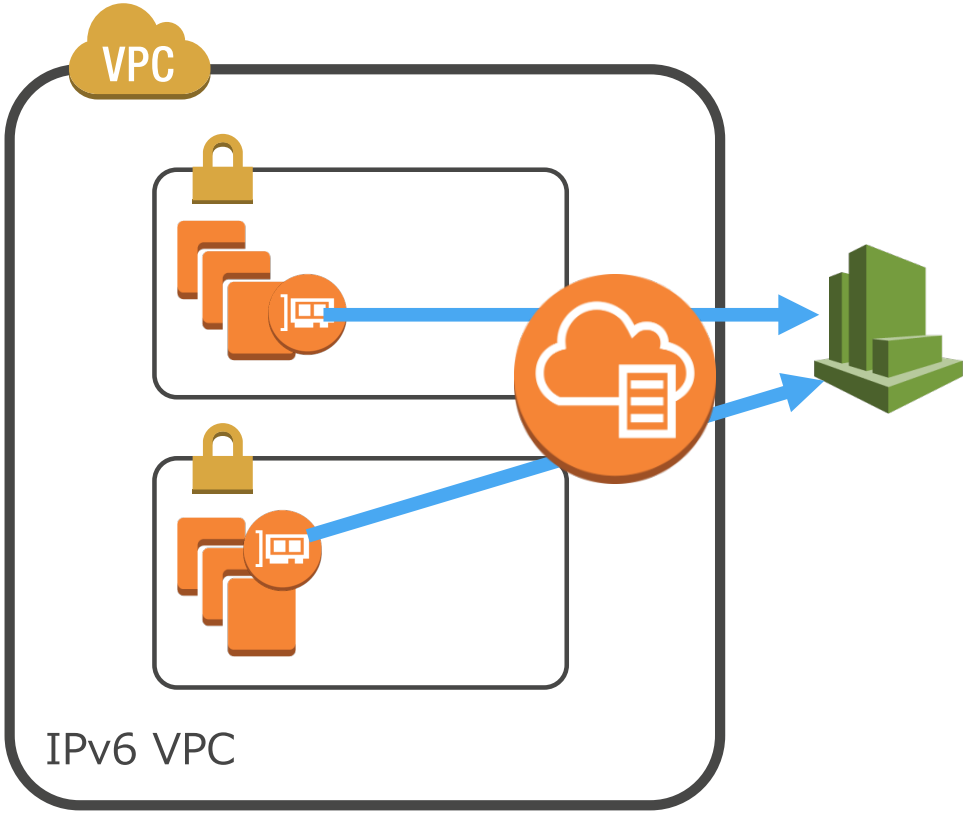
Application Load Balancer (ALB)

レイヤー７のコンテントベースのロードバランサー



- **特徴** (https://aws.amazon.com/elasticloadbalancing/applicationloadbalancer/)
  - レイヤー7のコンテントベースで、ターゲットグループに対してルーティング
  - コンテナベースのアプリケーションのサポート
  - WebSocket, HTTP/2, IPv6, AWS WAF をサポート
  - 複数のアベイラビリティゾーンに跨って、高レベルの耐障害性を実現
  - ALB自体が自動的にキャパシティを増減
- **価格体系**
  (https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/)
  - ALBの起動時間
  - Load Balancer Capacity Units (LCU)の使用量

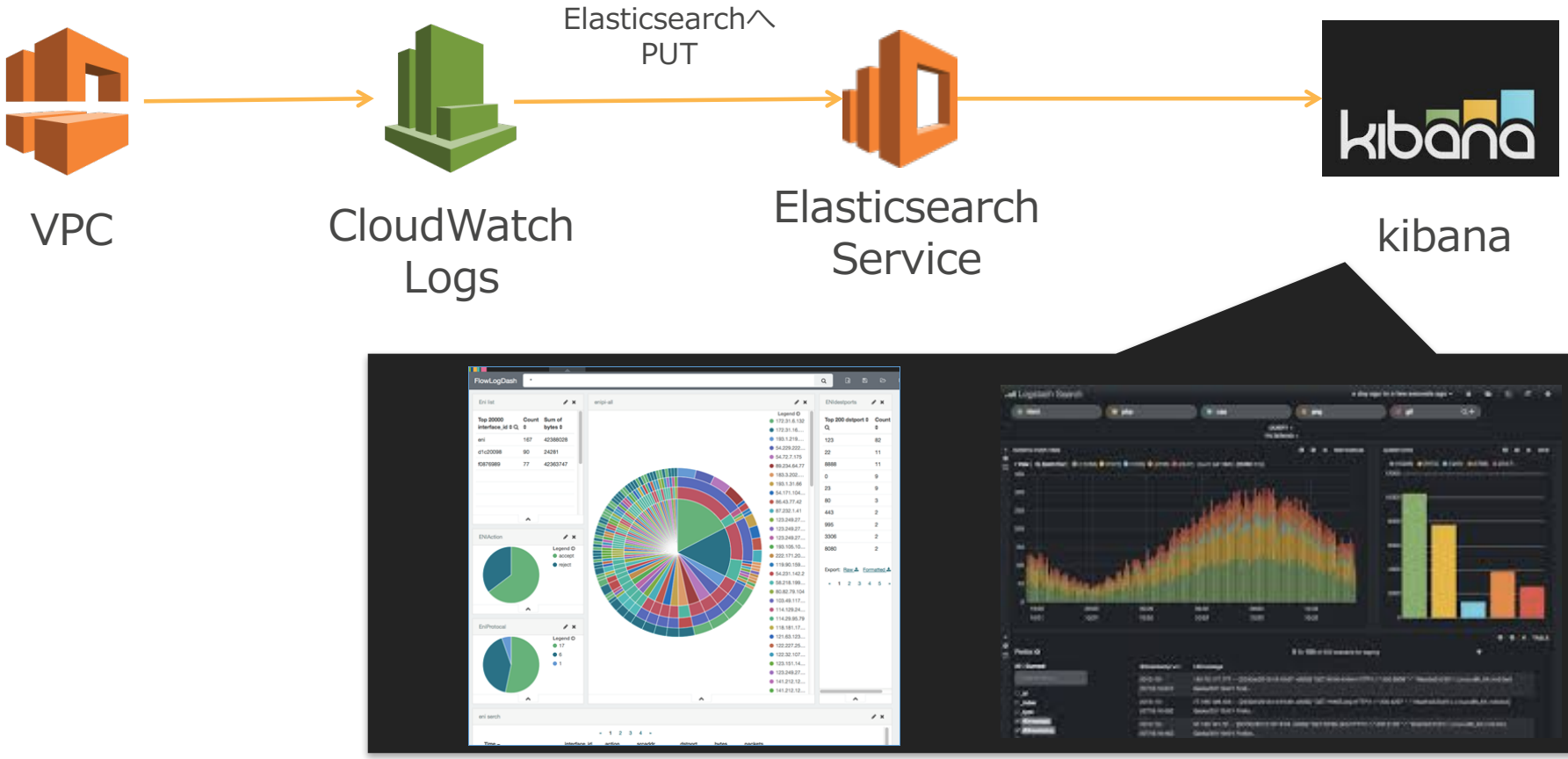
VPC Flow Logsとは



- ネットワークトラフィックをキャプチャし、CloudWatch LogsへPublish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
- 追加料金はなし(CloudWatch Logsの標準料金は課金)

amazon web services

利用例：Elasticsearch Service + kibanaによる可視化



https://blogs.aws.amazon.com/security/post/Tx246GOZNFIW79N/How-to-Optimize-and-Visualize-Your-Security-Groups

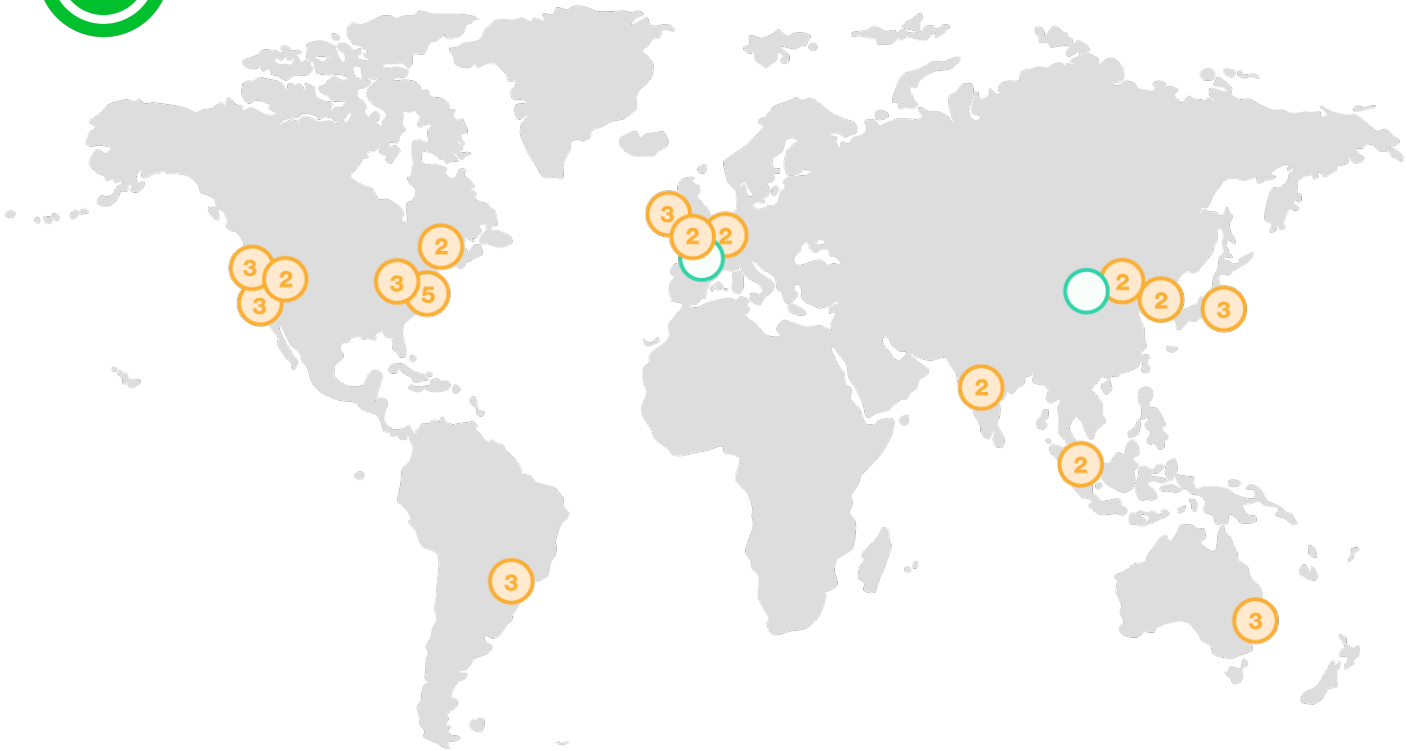
amazon web services

まとめ

AWSのIPv6対応は中国以外の全てですすめられている

IPv6 available

Regions – 40 Availability Zones – 68 Edge Locations



Region & Number of Availability Zones

AWS GovCloud (2)

US West

Oregon (3)

Northern California (3)

US East

N. Virginia (5), Ohio (3)

Canada

Central (2)

South America

São Paulo (3)

EU

Ireland (3)

Frankfurt (2)

London (2)

Asia Pacific

Singapore (2)

Sydney (2), Tokyo (3),

Seoul (2), Mumbai (2)

China

Beijing (2)

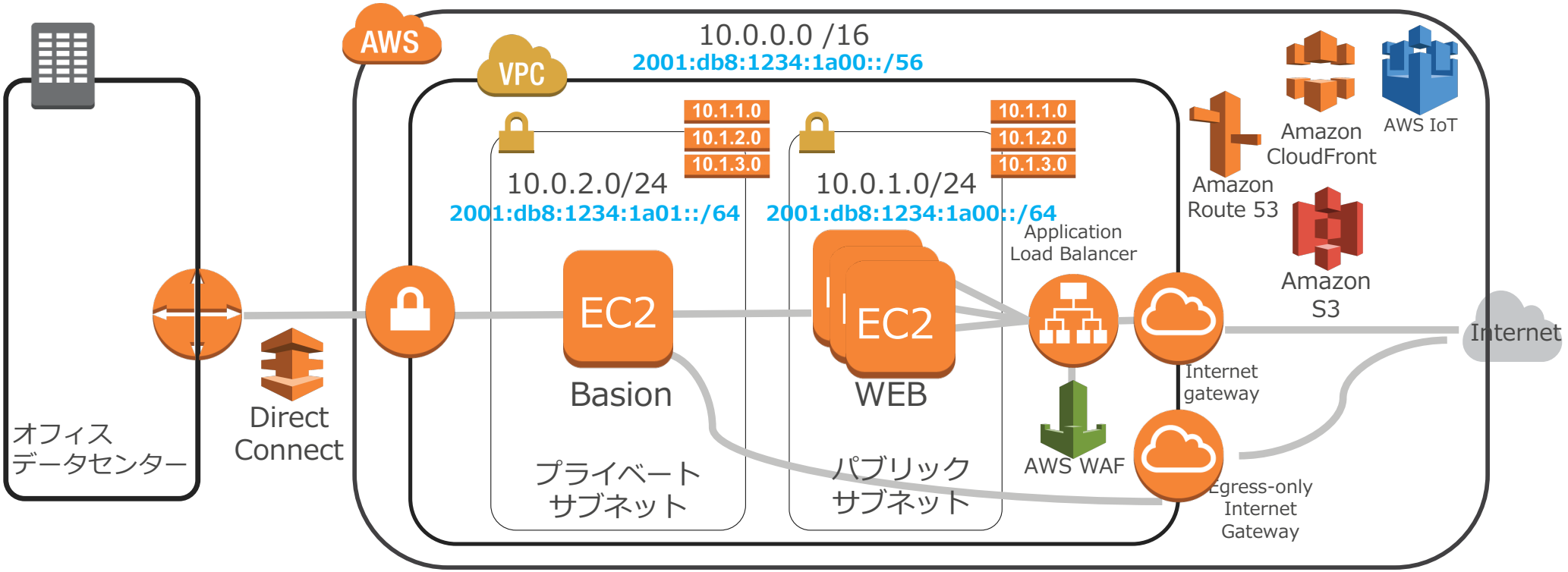
IPv4 Only

Announced Regions

Paris, Ningxia

IPv6の対応

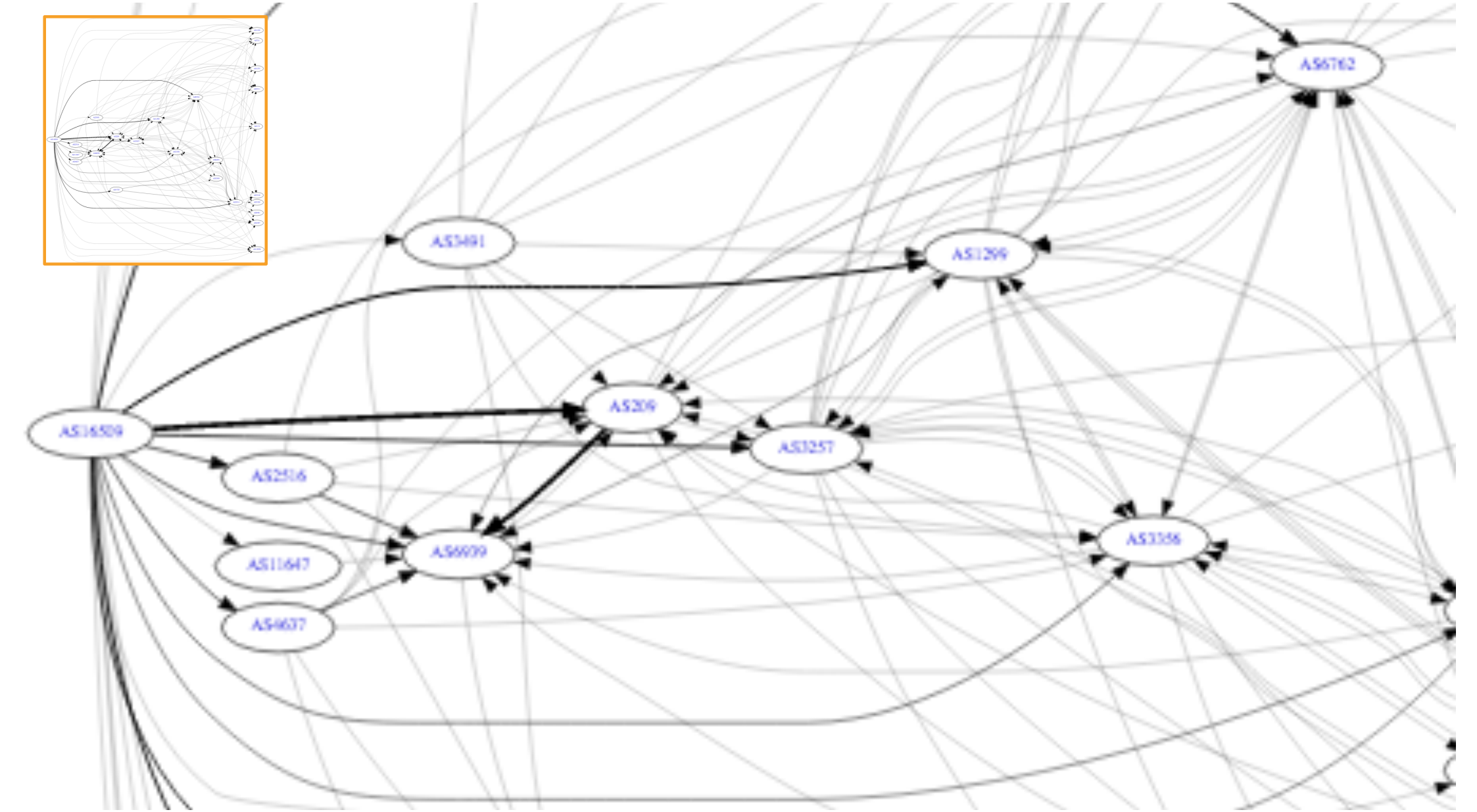
IoT、S3、CloudFront、WAF、Route53に続きVPC、ALBがIPv6対応



Egress-only Gateway(EGW) を利用して
IPv6においてもプライベート利用が可能

上記のような構成をIPv4/IPv6デュアルスタックで構築可能

https://aws.amazon.com/jp/blogs/news/new-ipv6-support-for-ec2-instances-in-virtual-private-clouds/


AS6762
AS3491
AS1299
AS209
AS16509
AS3257
AS2516
AS6939
AS3356
AS11647
AS4637