



Amazon Web Services (AWS)における IPv6対応状況 2020

菊池 之裕 (kyukihi@amazon.co.jp)

Amazon Web Services Japan K.K.

Sr.Solution Architect, Network Specialist

2020.02.06

自己紹介

名前: 菊池 之裕(きくち ゆきひろ) @yukihirokikuchi

所属: アマゾン ウェブ サービス ジャパン株式会社
技術統括本部 レディネス&テックソリューション本部
シニアソリューションアーキテクト ネットワークスペシャリスト

ロール: Network系サービスについてのご支援

経歴: ISP, IXP, VPN運用、開発を経てネットワーク機器、仮想ルータ販売会社のプリセールス、プロダクトSEからAWSへ(2017~今日で3年)

好きな AWS サービス: AWS Transit Gateway,
AWS Direct Connect, AWS Marketplace



amazon.com®

amazon services

aws

コンシューマー ビジネス

- 2億を超えるアクティブなアカウント
- 14カ国で展開

セラー向け ビジネス

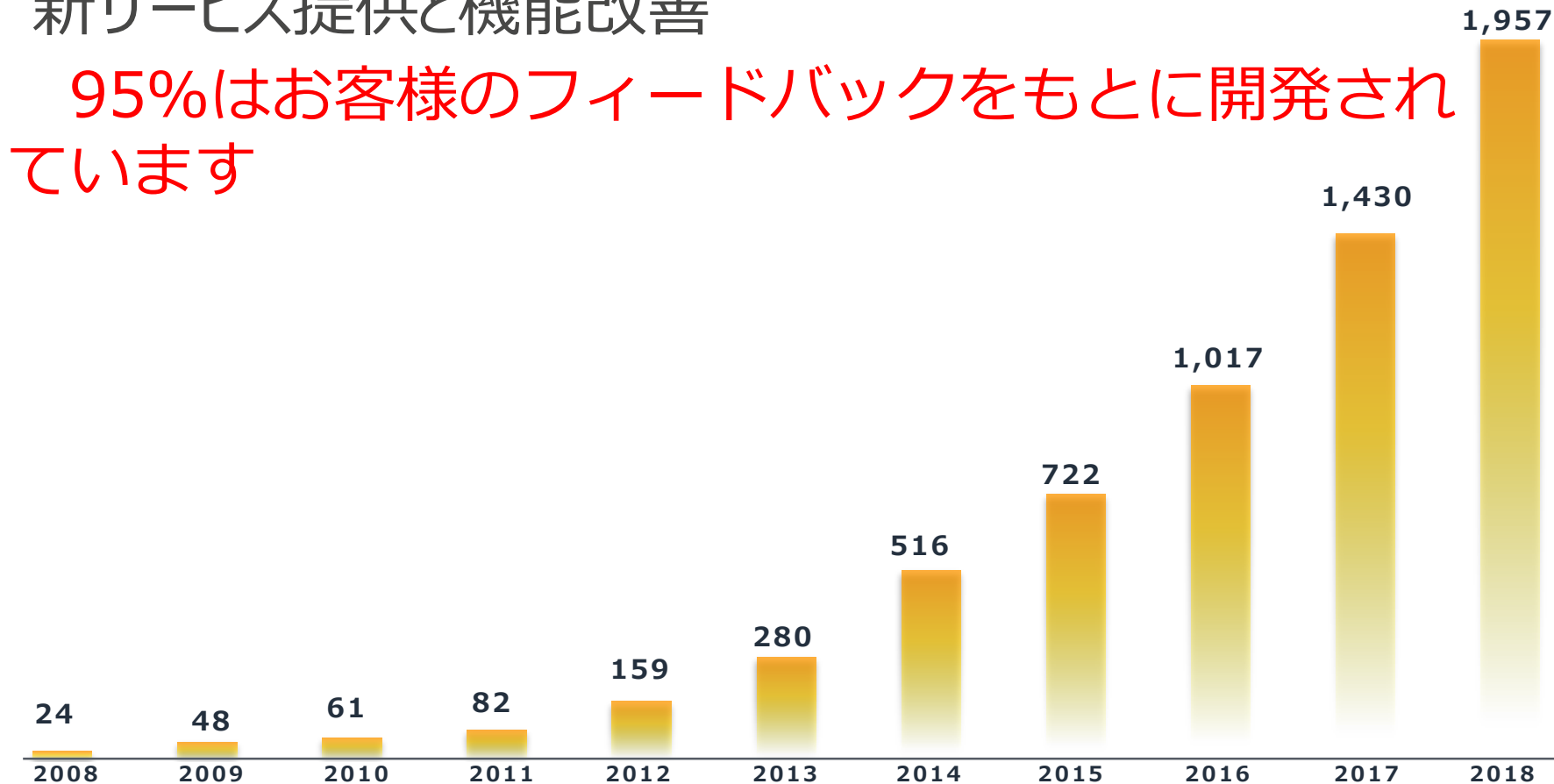
- アマゾンのウェブサイト上で販売
- アマゾンフルフィルメントセンターの活用

IT インフラ ビジネス

- ウェブスケールのクラウド基盤を提供
- 100万を超えるアクティブカスタマー

新サービス提供と機能改善

95%はお客様のフィードバックをもとに開発されています



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

補足：数値は累積ではなく、年度毎の新たな発表数です

アマゾン、AWSにおいてイノベーションをおこすためのメカニズムは？

低コスト

低価格

LOWER
COST
STRUCTURE

LOWER
PRICES

品揃え

Selection

顧客志向

GROWTH

成長

CUSTOMER
EXPERIENCE

顧客体験

SELLERS

売り手の数

TRAFFIC

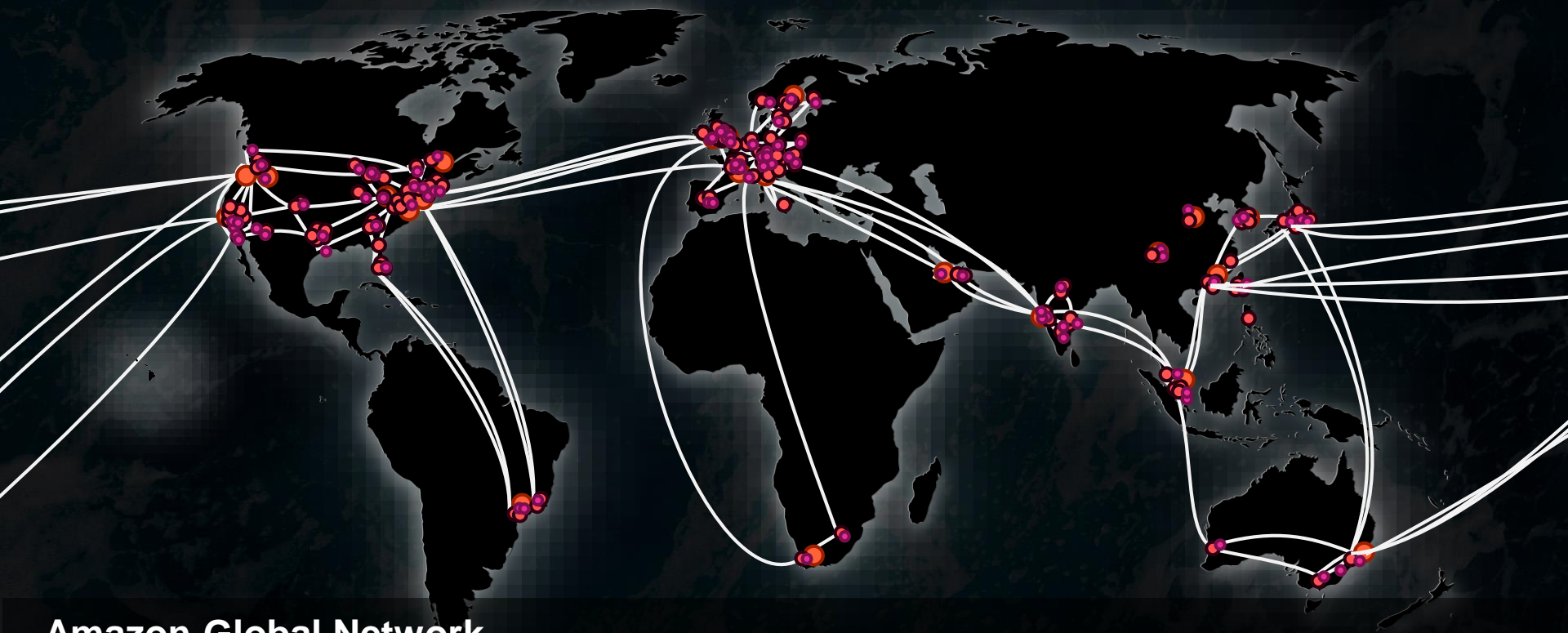
顧客数





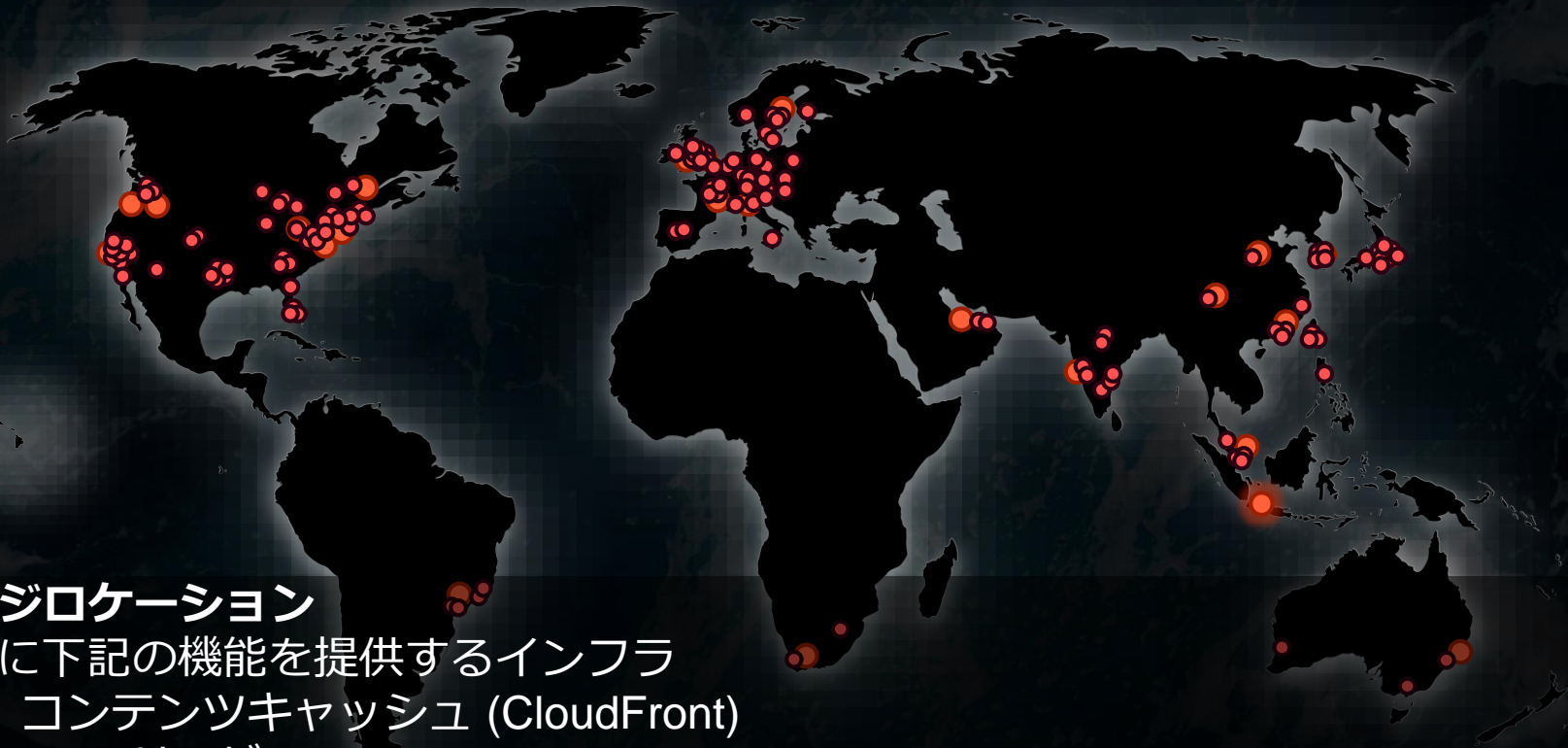
AWS グローバルインフラストラクチャ

- 69 AZs からなる 22 リージョンで構成
- +5 リージョンが近日公開予定



Amazon Global Network

- 冗長化された 100 GbE ネットワーク
- 中国を除く全てのリージョン間にプライベートキャパシティを提供



エッジロケーション

- 主に下記の機能を提供するインフラ
 - コンテンツキャッシュ (CloudFront)
 - DNS サービス (Route 53)
 - セキュリティ (AWS WAF, AWS Shield)
- グローバルで 200 箇所以上



Direct Connect ロケーション

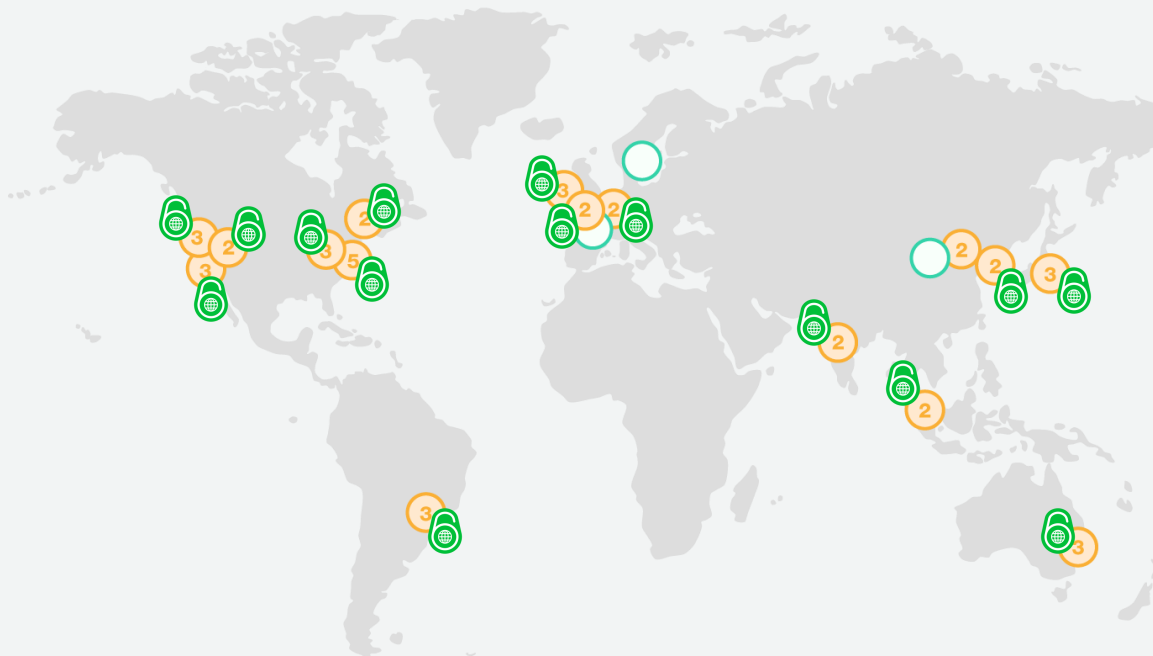
- お客様拠点と AWS リージョンを相互接続するポイント
- 日本には 3 箇所 (Equinix TY2, OS1, アット東京 CC1)

中国以外の各リージョンでIPv6対応のサービスを展開しています



IPv6 available in

19 Regions – 61 Availability Zones – 205 Edge Locations



Region & Number of Availability Zones

AWS GovCloud (2)

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)

Europe

Ireland (3)

Frankfurt (2)

London (2)

Paris(2)

Stockholm(3)

Asia Pacific

Singapore (2)

Sydney (2), Tokyo (3),

Seoul (2), Mumbai (2)

HongKong(3), Osaka(1)

China

Beijing (2)

Ningxia(寧夏)(3)

幅広い機能：175以上のサービスを提供(※2020年2月時点)

コンピューート



Amazon EC2 AWS Elastic Beanstalk AWS Lambda Amazon ECS ELB

ネットワーク



Amazon VPC AWS Direct Connect Amazon Route 53

アナリティクス



Amazon Athena Amazon EMR AWS Data Pipeline Amazon Kinesis Amazon QuickSight Amazon Elasticsearch Amazon Redshift AWS Glue

ゲーム



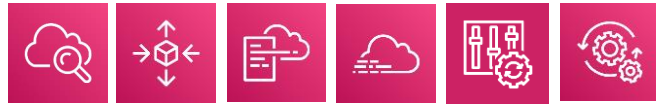
Amazon GameLift

開発ツール



AWS CodeBuild AWS CodeCommit AWS CodeDeploy AWS CodePipeline

管理ツール



Amazon CloudWatch AWS Auto Scaling AWS CloudFormation AWS CloudTrail AWS Config AWS Managed Services

セキュリティ



Amazon Cognito Amazon GuardDuty Amazon Inspector AWS KMS AWS Organizations AWS IAM

ストレージ & 配信



Amazon S3 Amazon EBS Amazon FSx Amazon EFS AWS Storage Gateway AWS Snowball

アプリケーションインテグレーション



AWS Step Functions Amazon SNS Amazon SQS Amazon MQ AWS AppSync

機械学習



Amazon Polly Amazon Rekognition Amazon SageMaker Amazon Translate Amazon Forecast

モバイルサービス



Amazon API Gateway AWS Amplify AWS Device Farm AWS AppSync

データベース



Amazon RDS Amazon Aurora Amazon DynamoDB Amazon ElastiCache Amazon Redshift AWS DMS

IoT



AWS IoT Core Amazon FreeRTOS AWS IoT Greengrass AWS IoT Analytics AWS IoT Device Defender

The AWS Platform

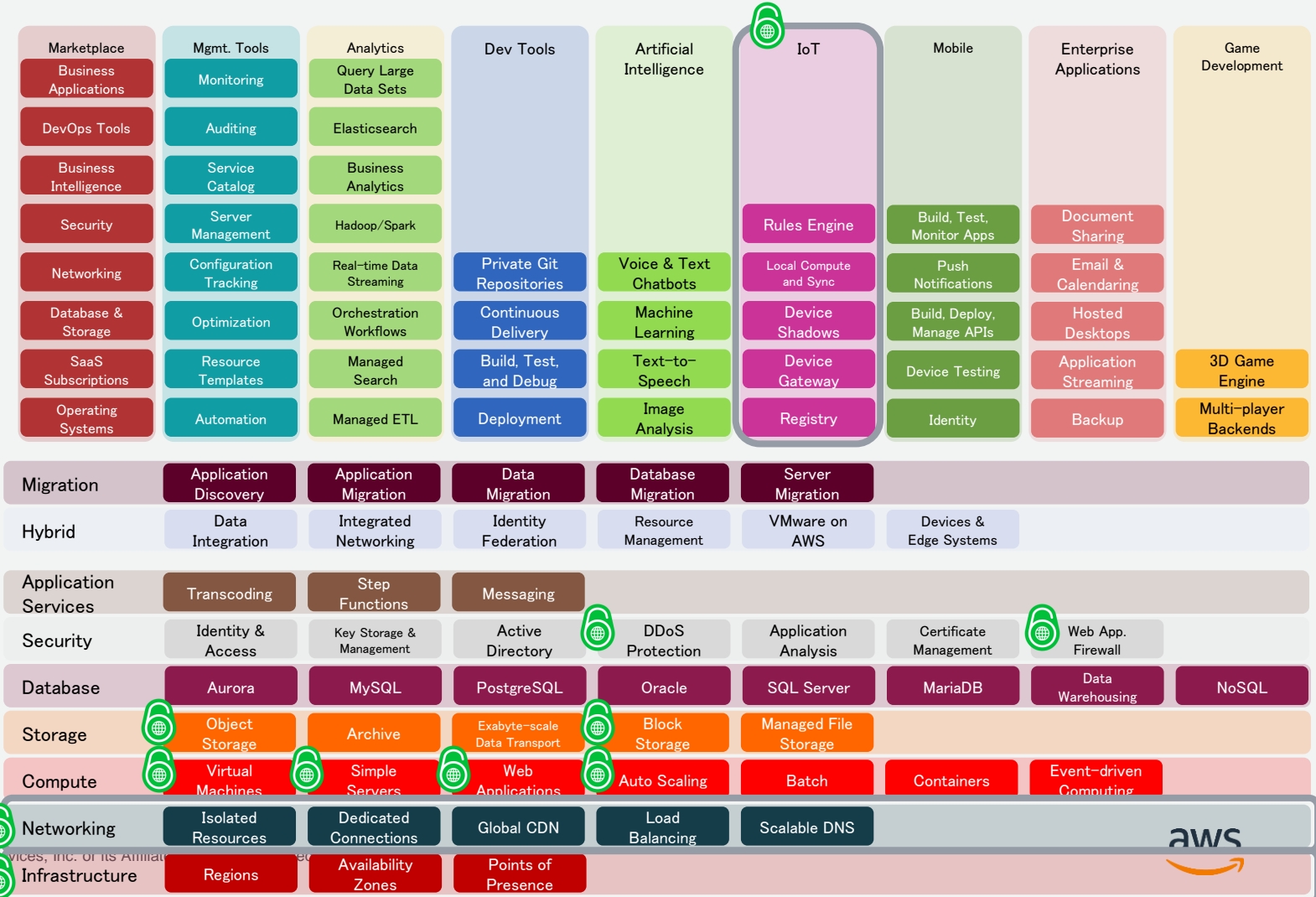
- Account Support
- Support
- Managed Services
- Professional Services
- Partner Ecosystem
- Training & Certification
- Solution Architects
- Account Management
- Security & Pricing Reports
- Technical Acct. Management

Marketplace	Mgmt. Tools	Analytics	Dev Tools	Artificial Intelligence	IoT	Mobile	Enterprise Applications	Game Development
Business Applications	Monitoring	Query Large Data Sets						
DevOps Tools	Auditing	Elasticsearch						
Business Intelligence	Service Catalog	Business Analytics						
Security	Server Management	Hadoop/Spark			Rules Engine	Build, Test, Monitor Apps	Document Sharing	
Networking	Configuration Tracking	Real-time Data Streaming	Private Git Repositories	Voice & Text Chatbots	Local Compute and Sync	Push Notifications	Email & Calendaring	
Database & Storage	Optimization	Orchestration Workflows	Continuous Delivery	Machine Learning	Device Shadows	Build, Deploy, Manage APIs	Hosted Desktops	
SaaS Subscriptions	Resource Templates	Managed Search	Build, Test, and Debug	Text-to-Speech	Device Gateway	Device Testing	Application Streaming	3D Game Engine
Operating Systems	Automation	Managed ETL	Deployment	Image Analysis	Registry	Identity	Backup	Multi-player Backends
Migration	Application Discovery	Application Migration	Data Migration	Database Migration	Server Migration			
Hybrid	Data Integration	Integrated Networking	Identity Federation	Resource Management	VMware on AWS	Devices & Edge Systems		
Application Services	Transcoding	Step Functions	Messaging					
Security	Identity & Access	Key Storage & Management	Active Directory	DDoS Protection	Application Analysis	Certificate Management	Web App. Firewall	
Database	Aurora	MySQL	PostgreSQL	Oracle	SQL Server	MariaDB	Data Warehousing	NoSQL
Storage	Object Storage	Archive	Exabyte-scale Data Transport	Block Storage	Managed File Storage			
Compute	Virtual Machines	Simple Servers	Web Applications	Auto Scaling	Batch	Containers	Event-driven Computing	
Networking	Isolated Resources	Dedicated Connections	Global CDN	Load Balancing	Scalable DNS			
Infrastructure	Regions	Availability Zones	Points of Presence					



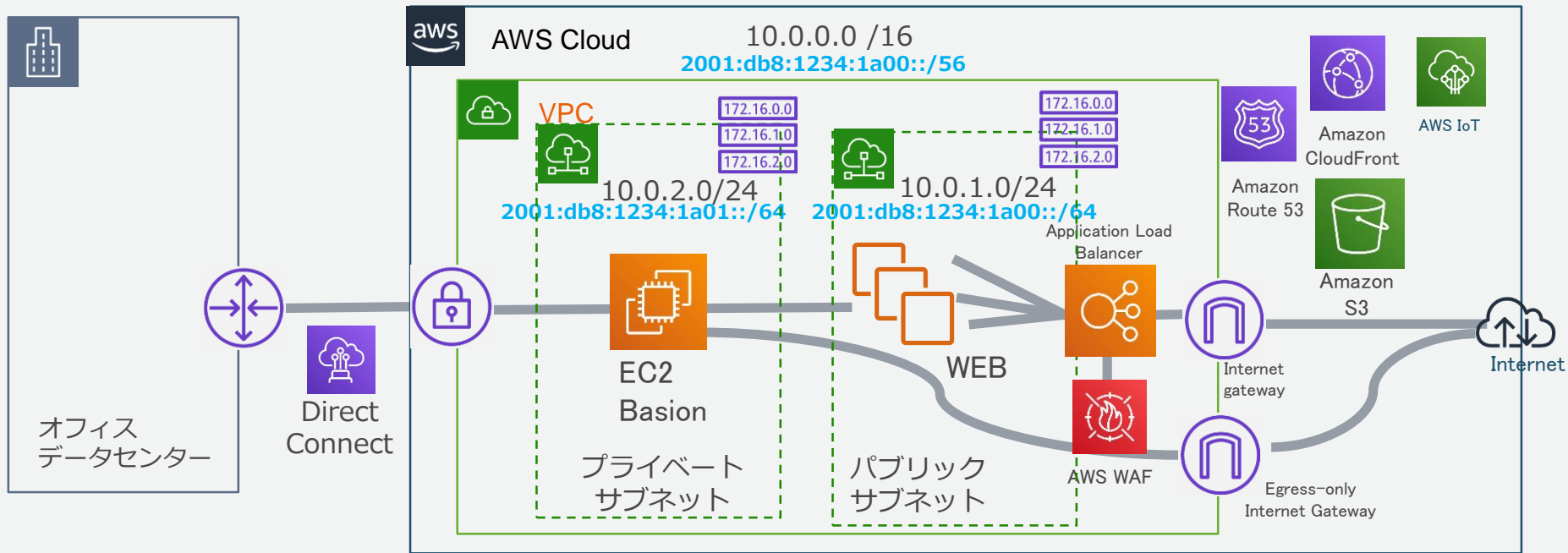
The AWS Platform

- Account Support
- Support
- Managed Services
- Professional Services
- Partner Ecosystem
- Training & Certification
- Solution Architects
- Account Management
- Security & Pricing Reports
- Technical Acct. Management



IPv6の対応

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

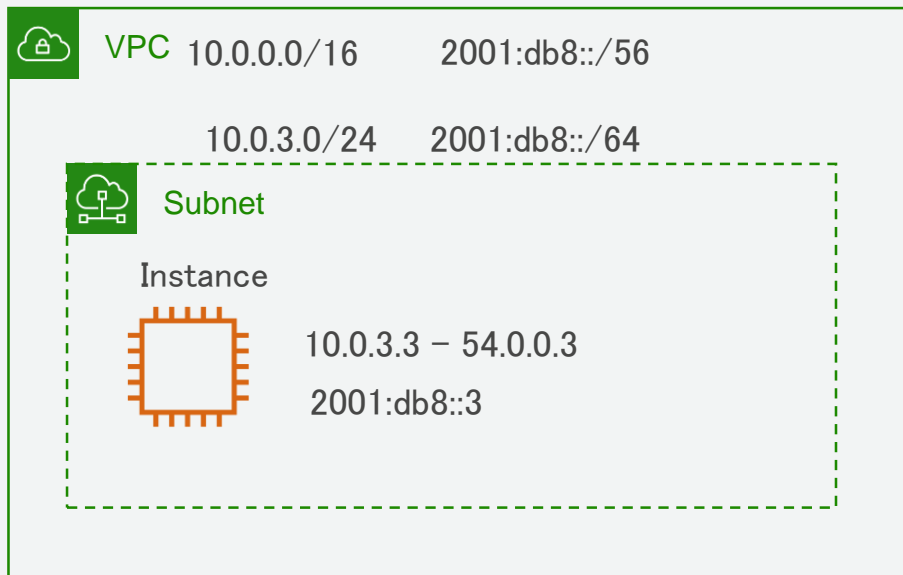


Egress-only Gateway(EGW) を利用して IPv6においてもプライベート利用が可能

上記のような構成をIPv4/IPv6デュアルスタックで構築可能

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 はオプティン

My VPCs




<input type="checkbox"/>	Name ▲	IPv4 CIDR ▼	IPv6 CIDR ▼
<input checked="" type="checkbox"/>	My Default VPC	172.31.0.0/16	
<input type="checkbox"/>	IPv6 Demo	10.100.0.0/16	2600:1f16:266:fa00::/56

My Subnets

<input type="checkbox"/>	Name ▲	IPv4 CIDR ▼	IPv6 CIDR ▼
<input type="checkbox"/>	Dual-stack Subnet	172.31.32.0/20	2600:1f16:342:d700::/64
<input checked="" type="checkbox"/>	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

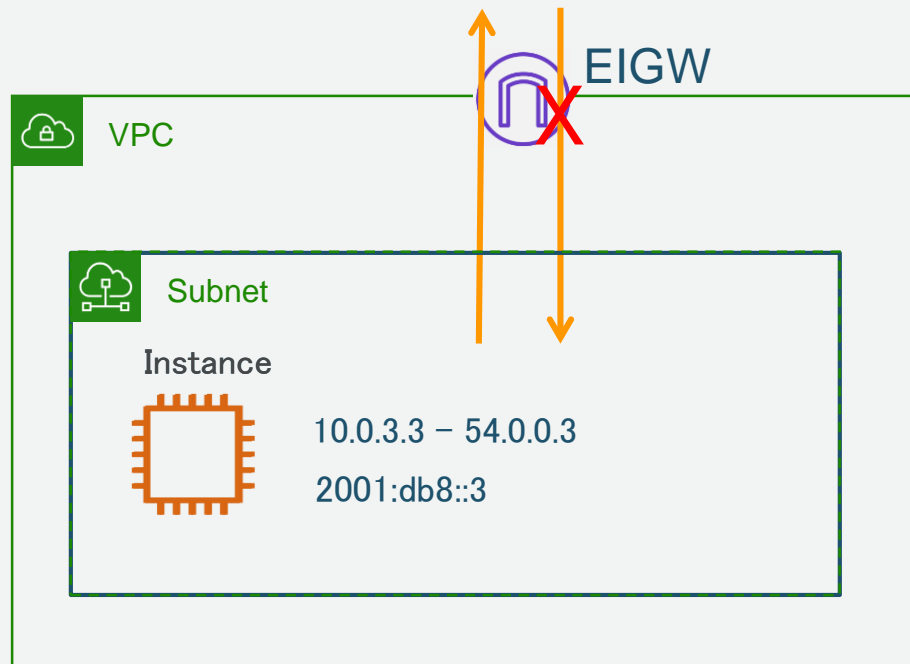
<input type="checkbox"/>	Name	Instance State	IPv4 Public IP	IPv6 IPs	Private IP Address
<input type="checkbox"/>	vpc-2	 running	52.15.170.128	-	172.16.0.176
<input type="checkbox"/>	demo-a	 running	52.15.142.67	2600:1f16:266:fa00:700:20cb:5f20:3dff	10.100.0.119
<input type="checkbox"/>	demo-c	 running	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ー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

Dual-stack

IPv4
Address

IPv6
Address

```
$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:ED:5E:CC  
          inet addr:10.61.82.96  Bcast:10.61.87.255  Mask:255.255.248.0  
          inet6 addr: 2001:db8:a:1ae::2/64  Scope:Global  
          inet6 addr: fe80::a00:27ff:feed:5ecc/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1500  
          RX packets:178686208  errors:19165  dropped:0  overruns:0  frame:0  
          TX packets:23844794  errors:0  dropped:0  overruns:0  carrier:0  
          collisions:0  txqueuelen:1000  
          RX bytes:47587268090 (44.3 GiB)  TX bytes:6872220198 (6.4 GiB)  
          Interrupt:193  Base address:0xd000
```

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

Working Backwards

全ては、お客様を起点に考え、お客様体験を徹底的に固める



① プレスリリースを書く



② FAQをつくる



③ お客様体験の定義と
マニュアル作成



BY USING VIDEO ANALYSIS
IN STORES

**JUST
WALK
OUT**

SHOPPING

amazon



AWS 誕生も Press Release, FAQから



AWS re:Invent

Andy Jassy
Chief Executive Officer
Amazon Web Services

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.

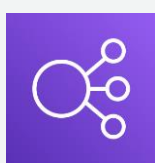
Here's the scoop:

IPv6 Support

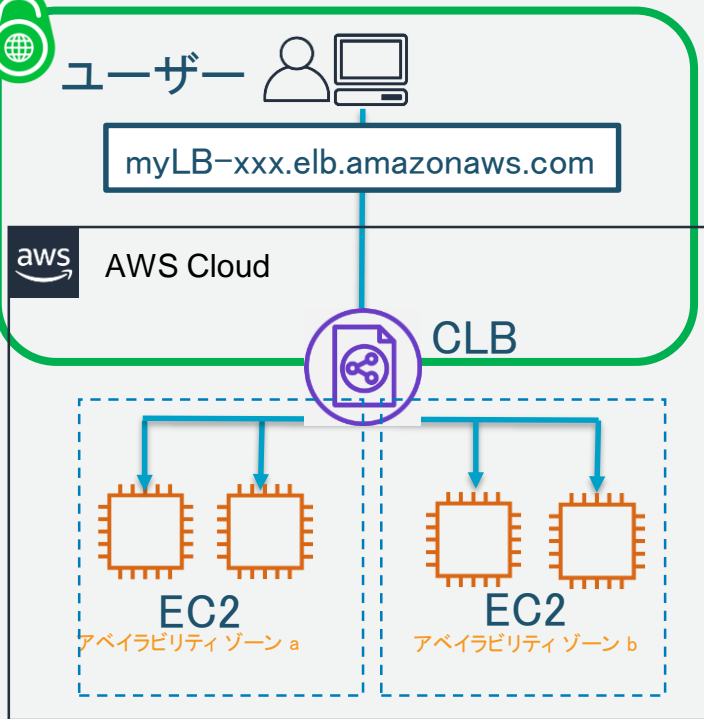
You've probably read some panic-inducing articles about the fact that the number of devices connected to the Internet is continuing to grow at an exponential rate. This growth is driven by the continued growth in the number of devices connected to the Internet using the Internet protocol, commonly known as IPv6. This version of the protocol raises the theoretical limit on the number of devices to an incredible 2^{128} , and also lays the groundwork for other capabilities in the future.

2011-06-08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

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/>)

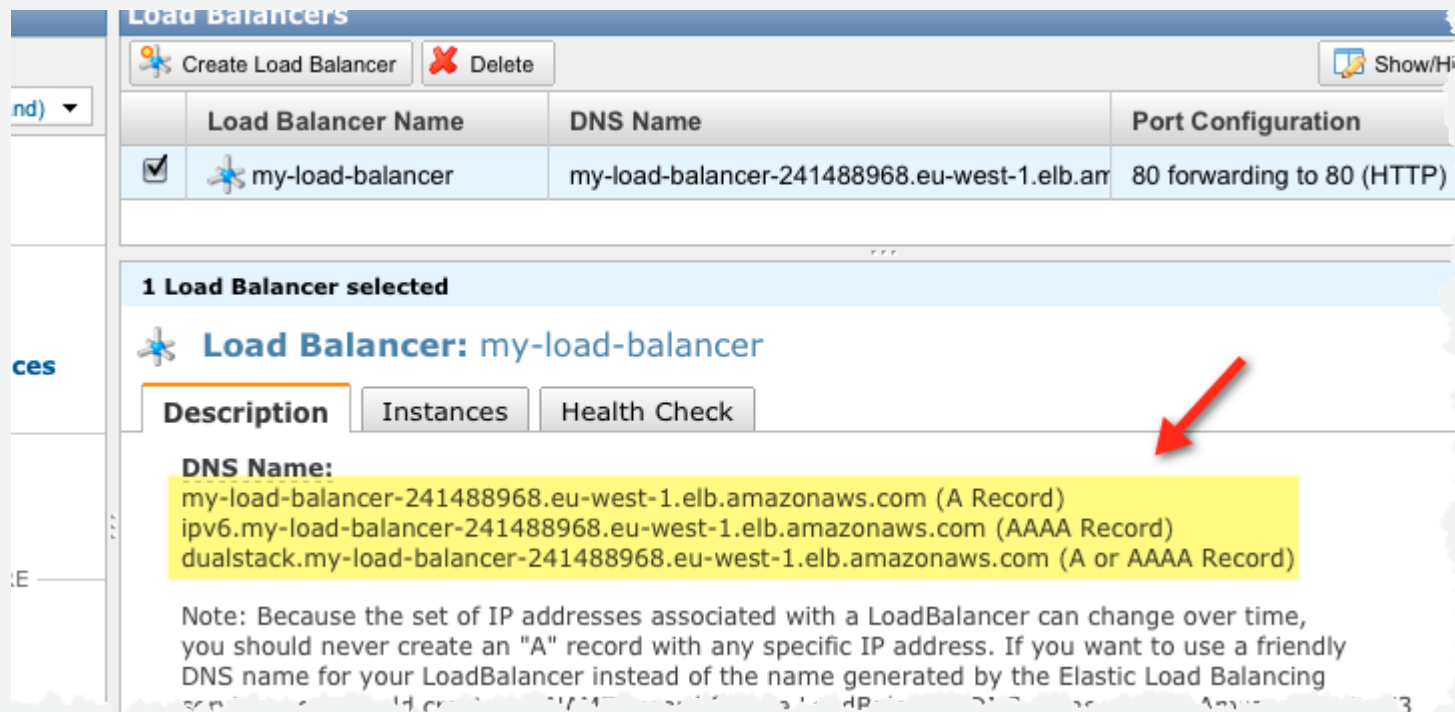
- 複数のAmazon EC2インスタンスに負荷分散
- 複数のアベイラビリティゾーンに跨って、高レベルの耐障害性を実現
- CLB自体が自動的にキャパシティを増減
- IPv4動作のバックエンドホストの前面でIPv6を変換 (EC2-Classicネットワーク向け)

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(当時)におけるIPv6はオプトイン



The screenshot displays the AWS Management Console interface for configuring an Elastic Load Balancing (ELB) instance. The 'Load Balancers' section is active, showing a table with one entry: 'my-load-balancer'. Below the table, the 'Description' tab is selected, and the 'DNS Name' field is highlighted in yellow. The DNS Name field contains three records: 'my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (A Record)', 'ipv6.my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (AAAA Record)', and 'dualstack.my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (A or AAAA Record)'. A red arrow points to the dualstack record. Below the DNS Name field, a note states: 'Note: Because the set of IP addresses associated with a LoadBalancer can change over time, you should never create an "A" record with any specific IP address. If you want to use a friendly DNS name for your LoadBalancer instead of the name generated by the Elastic Load Balancing service, you should create an "AAAA" record for the LoadBalancer. Do not create an "A" record for the LoadBalancer.' The page number '3' is visible at the bottom right of the console output.

Load Balancer Name	DNS Name	Port Configuration
<input checked="" type="checkbox"/> my-load-balancer	my-load-balancer-241488968.eu-west-1.elb.am...	80 forwarding to 80 (HTTP)

1 Load Balancer selected

Load Balancer: my-load-balancer

Description | Instances | Health Check

DNS Name:
my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (A Record)
ipv6.my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (AAAA Record)
dualstack.my-load-balancer-241488968.eu-west-1.elb.amazonaws.com (A or AAAA Record)

Note: Because the set of IP addresses associated with a LoadBalancer can change over time, you should never create an "A" record with any specific IP address. If you want to use a friendly DNS name for your LoadBalancer instead of the name generated by the Elastic Load Balancing service, you should create an "AAAA" record for the LoadBalancer. Do not create an "A" record for the LoadBalancer.

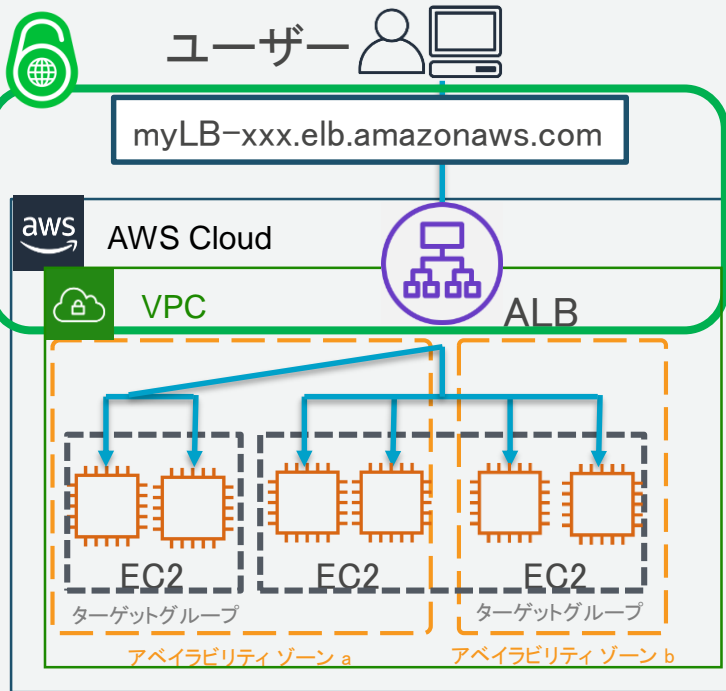
3

Network

Application Load Balancer (ALB)



レイヤー7のコンテンツ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のコンテンツベースで、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

AWS IoT



簡単で安全なクラウドへのデバイス接続サービス

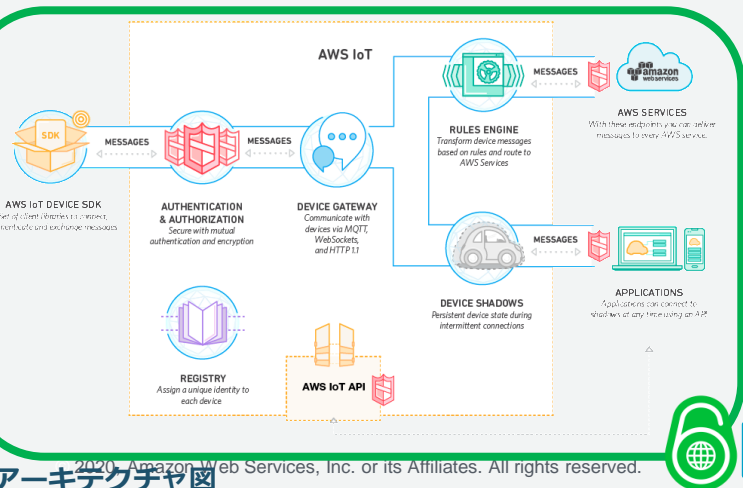


特徴 [\(https://aws.amazon.com/jp/iot/\)](https://aws.amazon.com/jp/iot/)

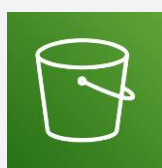
- デバイスとクラウドの双方向コミュニケーション
- HTTP、MQTT、Websocketに対応
- SQLベースのルールとアクション定義
- AWSサービスとのシームレスな連携
- デバイス向けのSDK

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

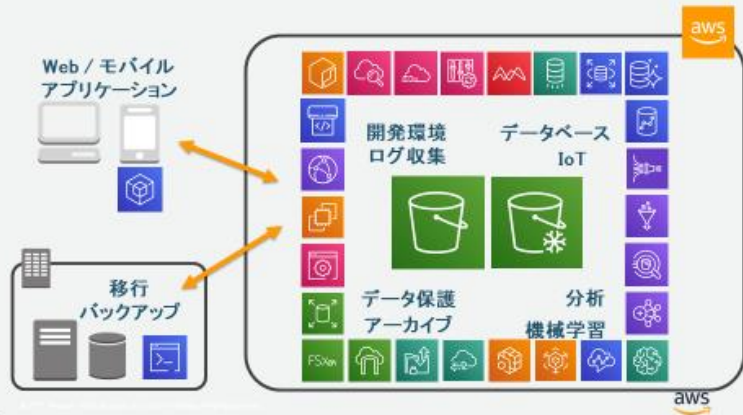
- 100万メッセージあたり\$8(日本リージョン)
- 無料利用枠利用は25万メッセージ/月を(1年間)



Amazon Simple Storage Service (S3)



マネージドオンラインストレージサービス



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

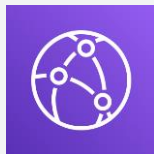


- APIおよびRESTのWebサーバ機能を持つ

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



Amazon
CloudFront



レスポンス向上

負荷軽減

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87箇所のエッジロケーション

価格体系

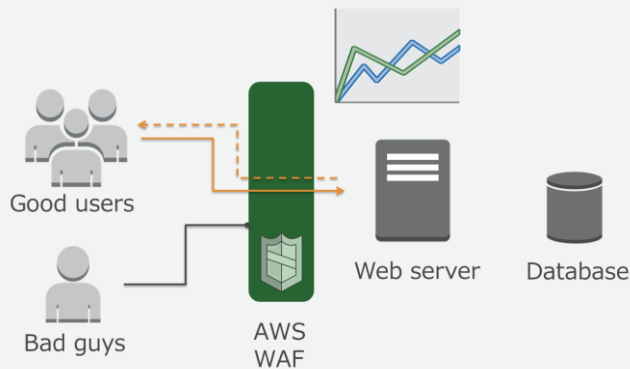
(<http://aws.amazon.com/jp/cloudfront/pricing/>)

- 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



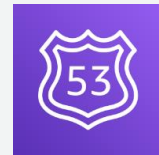
CloudFrontとALB(Application Load Balancer)、APIGWで利用できる

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

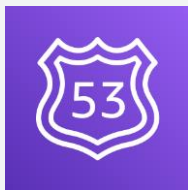
- ウェブACLの数とルール数
- リクエスト数

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
- ジオルーターティング
- ドメイン取得と管理
- AAAA, Query in IPv6

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

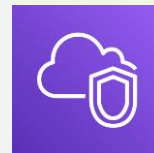
特徴 (<http://aws.amazon.com/jp/route53/>)

- 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

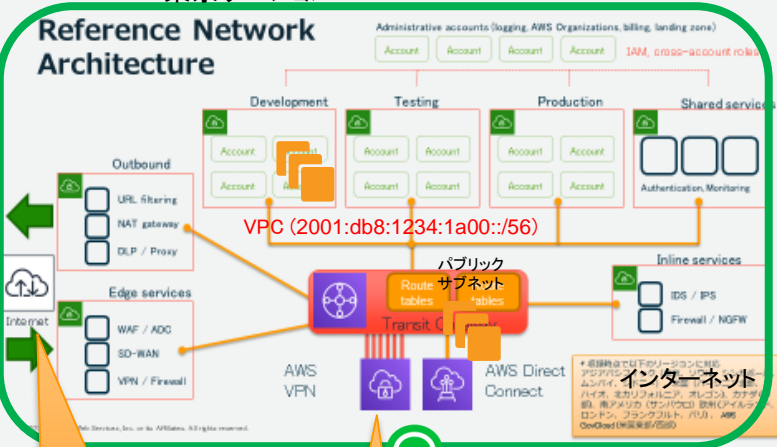
価格体系

(<http://aws.amazon.com/jp/vpc/pricing/>)

- VPCの利用は無料

東京リージョン

Reference Network Architecture

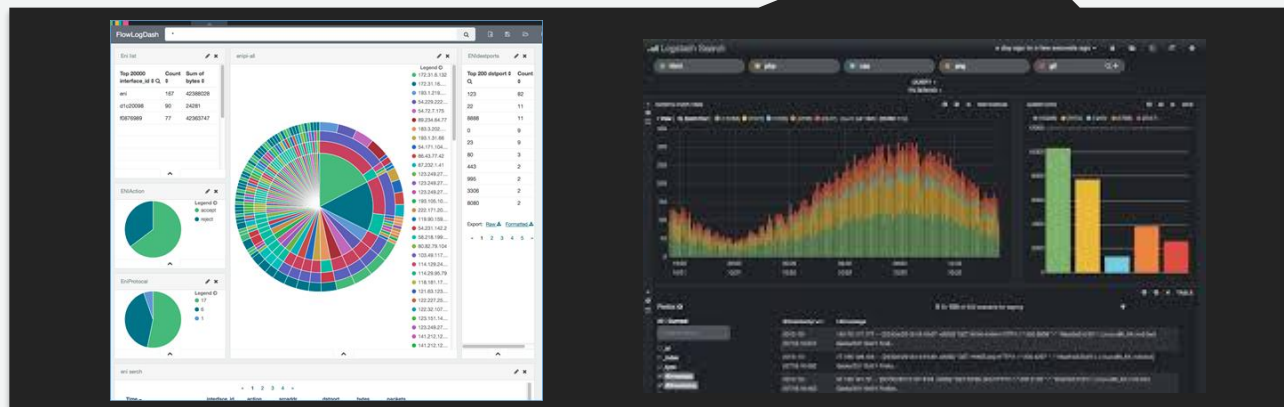
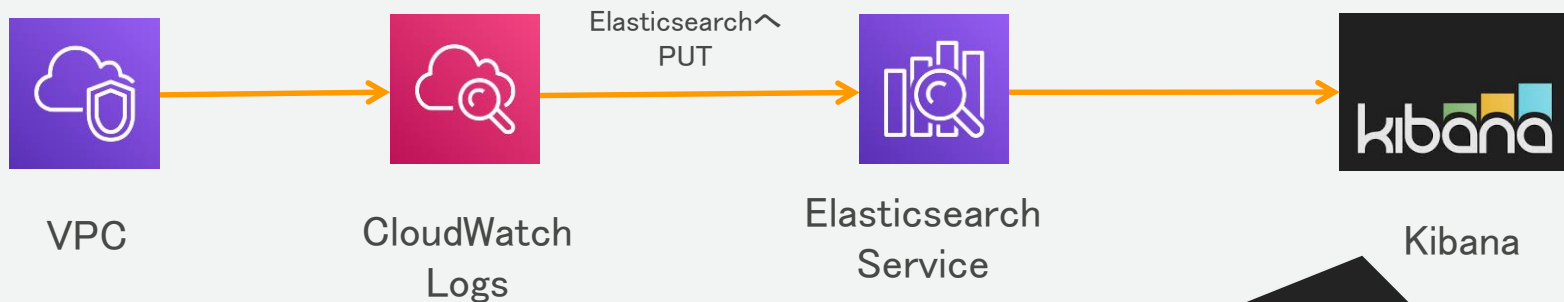


インターネット
ゲートウェイ

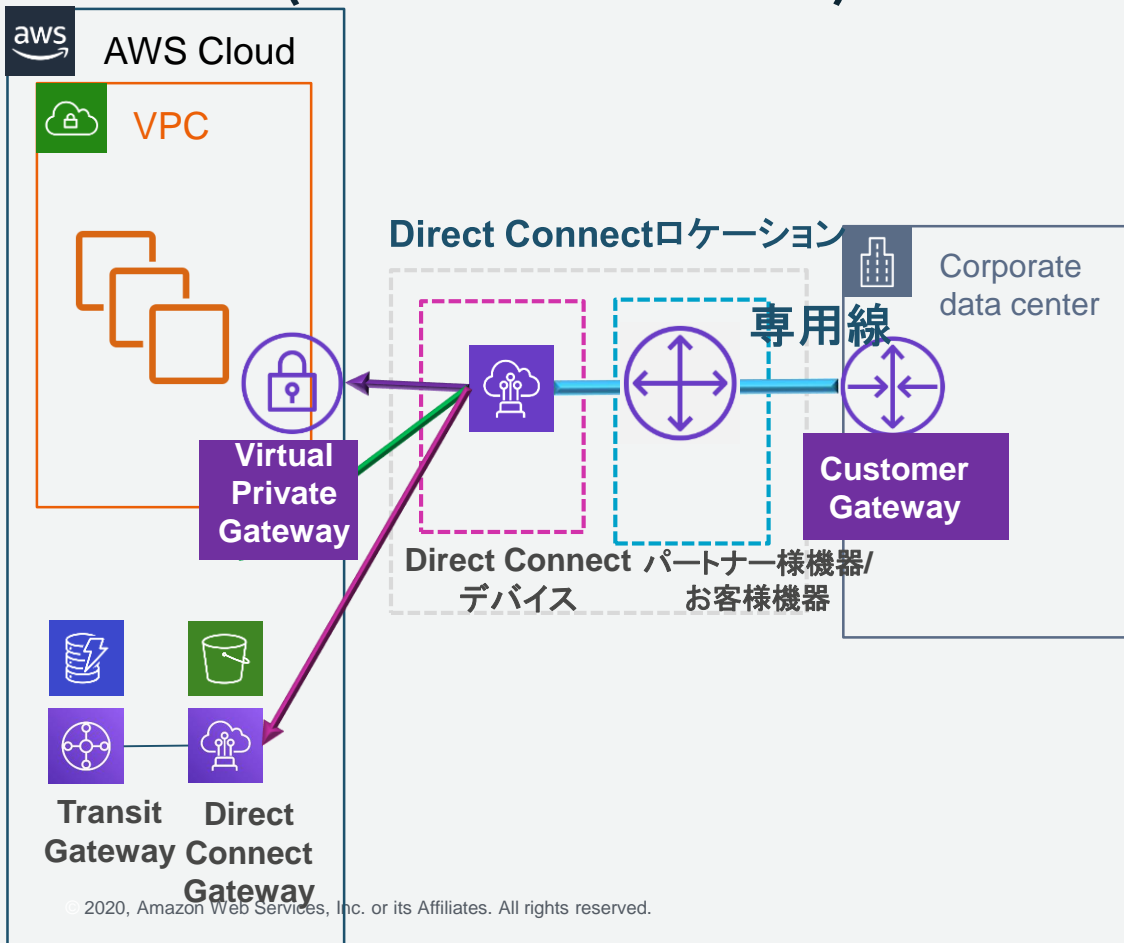
VPN
or
専用線

- IPv4/IPv6デュアルスタック
- EC2インスタンスにグローバルユニキャストアドレス (DHCPv6)
- Security Group/Network ACL標準対応
- Egress-Onlyインターネットゲートウェイ
- VPC Flow Logs, Transit Gateway

VPC Flow Logs+Elasticsearch Service+Kibanaによる可視化



専用線(Direct Connect)接続構成

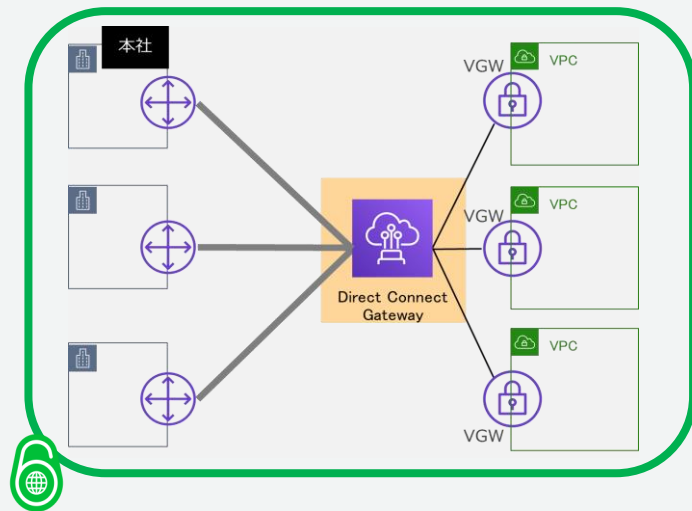


- ・AWSとお客様設備を専用線でネットワーク接続
- ・相互接続ポイントへ専用線を敷設し、AWSのルータと相互接続
- ・日本の相互接続ポイントは
東京(Equinix TY2/TY6/TY7/TY8 @Tokyo CC1)
大阪(Equinix OS1)
- ・ルーティングはBGPのみ
- ・接続先は以下の3つ
VPC(プライベート接続)
AWSクラウド(パブリック接続)
Transit Gateway(Transit接続)
- ・VPNよりも一貫性がある
- ・帯域のパフォーマンスも向上
- ・ネットワークコストも削減

Direct Connect Gateway



- Direct Connect GatewayがHubになり、複数アカウントに所属する複数のリージョンの複数のロケーションから複数リージョンの複数のVPCに接続できる機能。
 - Direct Connectから世界の全リージョン(中国除く)のVPCに接続することができる。
 - 1つのDirect Connectの仮想インターフェイスから複数のVPCに接続することができる。
 - 複数のDirect Connectの仮想インターフェイスをDirect Connect Gatewayに接続することができる。

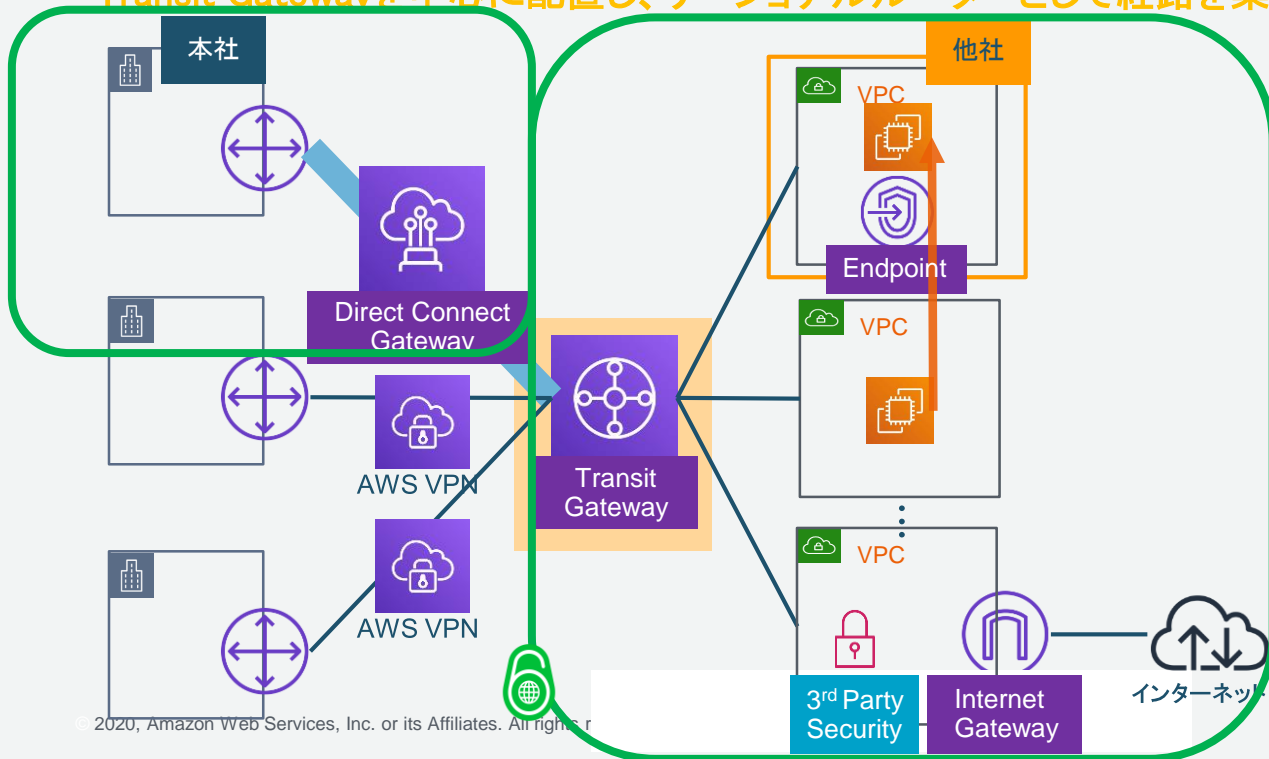


1つ以上のDirect Connect ロケーションに繋がれば
全世界の全リージョン(中国除く)に閉域網接続でき
同一リージョンまたは世界の複数リージョンをまたいで複数のVPCに接続できる機能

AWS Transit Gateway

管理・連携するVPCの数が増え、VPC Peeringのメッシュ化によりAWS上の構成が複雑化
多くのオンプレミス拠点がVPCへ接続

→ Transit Gatewayを中心に配置し、リージョナルルーターとして経路を集中管理



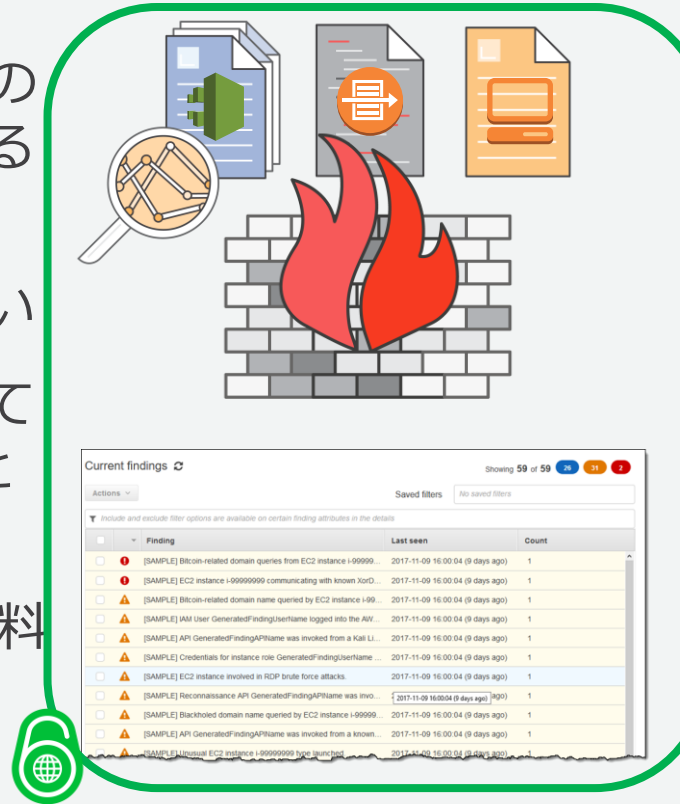
通信要件: オンプレミス、VPC間の
シームレスな連携、インターネット接
続環境をAWS上のセキュリティアプ
ライアンスに集約

サービス: Transit Gateway、マー
ケットプレイスのパートナーアプ
ライアンス(セキュリティ関連)

Security

Amazon GuardDuty

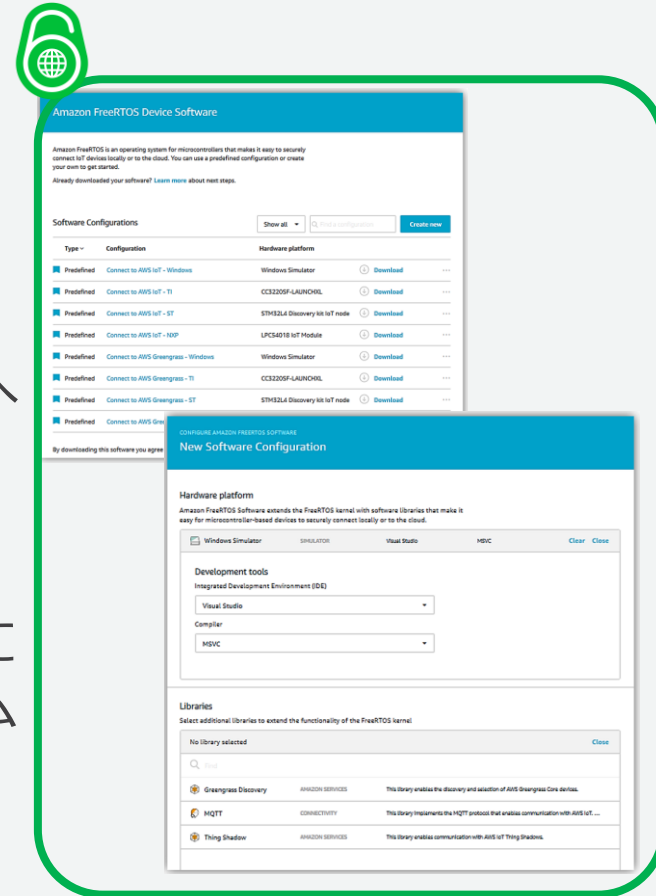
- CloudTrailやDNSのログ、VPC Flow Logs等のデータから疑わしいアクティビティを検知する
- GuardDutyはAWSが管理する基盤で動作し、エージェント等の導入は不要。性能影響もない
- サービスが検知したイベントは重要度に応じて3レベルにラベリングされ、推奨される対策とともに提示される
- 処理したログ量に応じた課金体系。30日の無料試用により実績量を測定できる
- 東京を含む各リージョンで利用可能に



IoT

Amazon FreeRTOS

- IoTデバイスの開発・保守・セキュリティをシンプルにするAmazon FreeRTOSを発表
- 一般的なリアルタイムOSであるFreeRTOSのカーネルを拡張し、ローカル環境とクラウドへの接続機能やセキュリティ機能を提供
- OTAアップデートを今後サポートする予定
- 各プラットフォームに向けた設定済みの環境に加え、必要なライブラリを絞り込んだカスタム環境を利用することもできる
- ハードウェア認定プログラムあり



その他

IP アドレス条件演算子(aws:SourceIp)

ip-ranges.json

```
"ipv6_prefixes": [  
  {  
    "ipv6_prefix": "2400:6500:0:7000::/56",  
    "region": "ap-southeast-1",  
    "service": "AMAZON"  
  },  
  {  
    "ipv6_prefix": "2400:6500:0:7100::/56",  
    "region": "ap-northeast-1",  
    "service": "AMAZON"  
  },  
  (...)  
]
```

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "someservice:*",  
    "Resource": "*",  
    "Condition": {  
      "IpAddress": {  
        "aws:SourceIp": [  
          "203.0.113.0/24",  
          "2001:DB8:1234:5678::/64"  
        ]  
      }  
    }  
  }  
}
```

IPv6の利用ドキュメントもご用意してあります

https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/get-started-ipv6.html

The screenshot shows the AWS documentation page for "Amazon VPC の IPv6 の使用開始". The page is in Japanese and includes a search bar, navigation tabs, and a table of contents. The main content area contains the following text:

Amazon VPC の IPv6 の使用開始

PDF

IPv6 アドレスをサポートする VPC を作成します。

この演習を完了するには、以下の作業を行います。

- IPv6 CIDR ブロックと 1 つのパブリックサブネットを持つデフォルトでない VPC を作成します。サブネットを使うと、インスタンスをセキュリティや運用上の必要に応じてグループ化することができます。パブリックサブネットとは、インターネットゲートウェイを通してインターネットにアクセスするサブネットです。
- 特定のポートのみからトラフィックを許可するセキュリティグループをインスタンスに作成します。
- サブネット内に Amazon EC2 インスタンスを起動し、起動時に IPv6 アドレスをインスタンスに関連付けます。IPv6 アドレスはグローバルに一意であり、インスタンスがインターネットと通信できるようにします。

IPv4 アドレスと IPv6 アドレスの詳細については、「[VPC の IP アドレス指定](#)」を参照してください。

初めて Amazon VPC を使用する際には、Amazon Web Services (AWS) にサインアップする必要があります。サインアップすると、Amazon VPC を含む AWS のすべてのサービスに対して AWS アカウントが自動的にサインアップされます。AWS アカウントをまだ作成していない場合は、https://aws.amazon.com/ja_jp/アカウント/ にアクセスし、「[まだ無料体験し始める](#)」を選択します。

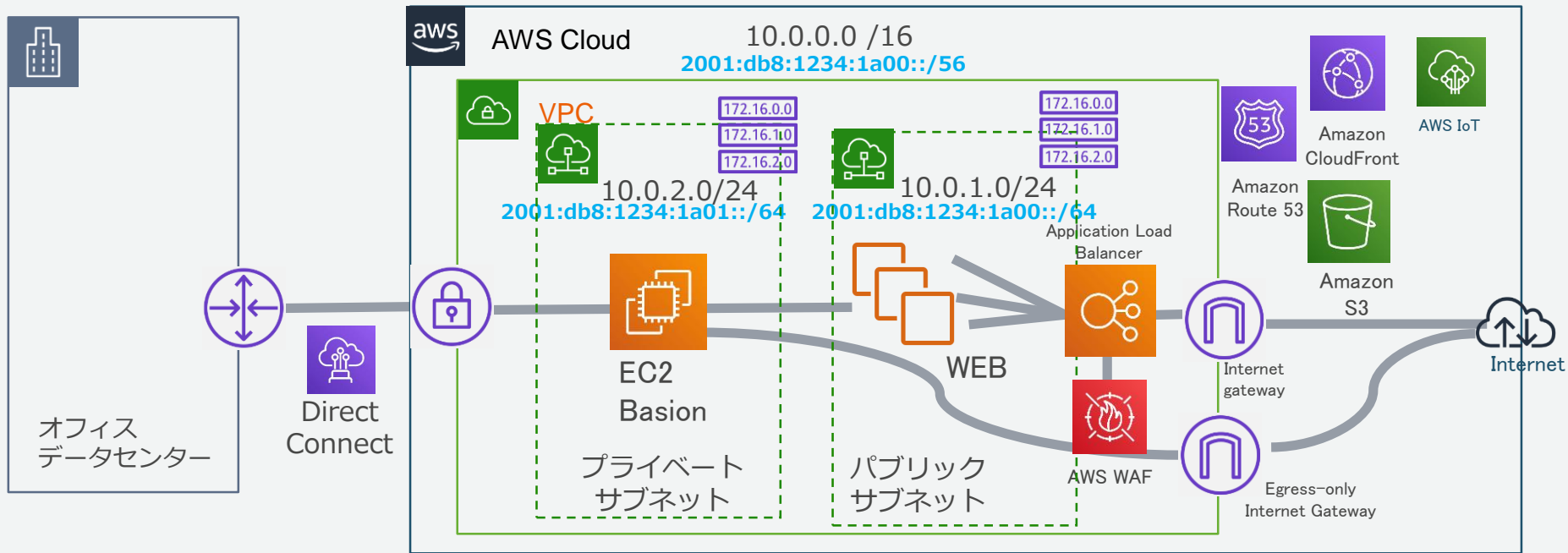
このページの内容

- ステップ 1: VPC を作成する
- ステップ 2: セキュリティグループを作成する
- ステップ 3: インスタンスを起動する

まとめ

IPv6の対応

IoT、S3、CloudFront、WAF、Route53、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

Working Backwards

AWSサービスのIPv6化

- IPv6でお客様がサービス提供をできるように
- IPv6でも同じように運用できるように
 - ログ、メトリクス、モニタリング、アクセスコントロール
- お客様がご利用を選択できる（有効化、無効化）

AWSサービスのIPv6対応のご要望がございましたら、是非お聞かせください

