



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

菊池 之裕

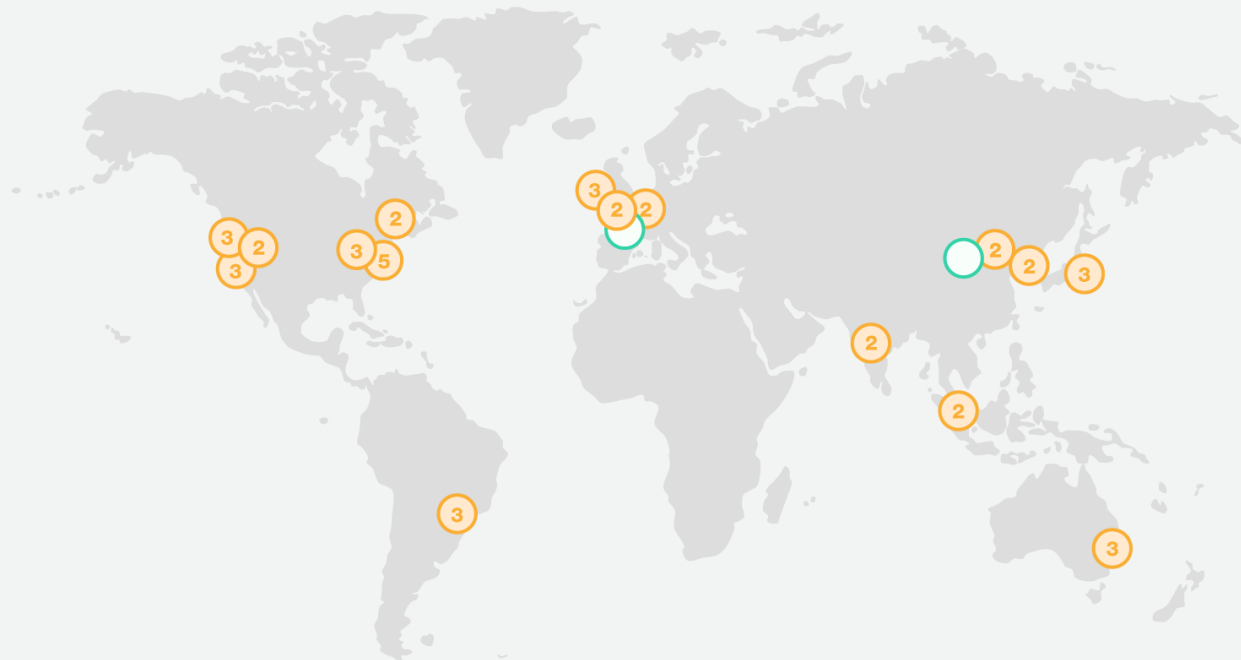
Amazon Web Services

Solution Architect, Network Specialist

2017.12.12

AWSの今日

16 Regions – 44 Availability Zones – 107 Edge Locations

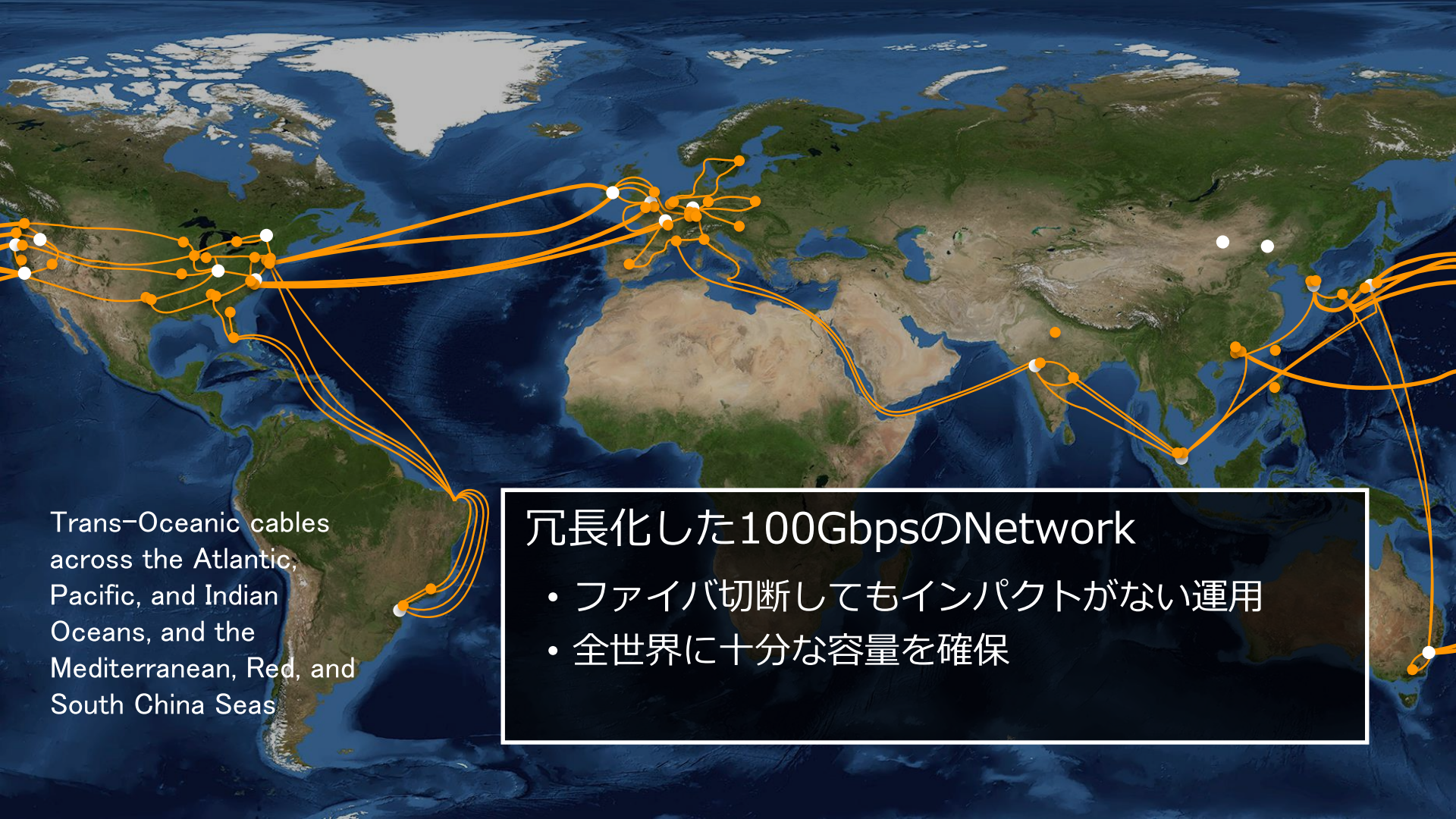


Region & Number of Availability Zones

AWS GovCloud (2)	EU
	Ireland (3)
US West	Frankfurt (2)
Oregon (3)	London (2)
Northern California (3)	
	Asia Pacific
US East	Singapore (2)
N. Virginia (6), Ohio (3)	Sydney (2), Tokyo (3), Seoul (2), Mumbai (2)
Canada	
Central (2)	China
	Beijing (2)
South America	
São Paulo (3)	

Announced Regions

Paris, Ningxia, Sweden, Hong-Kong, Osaka



Trans-Oceanic cables
across the Atlantic,
Pacific, and Indian
Oceans, and the
Mediterranean, Red, and
South China Seas

冗長化した100GbpsのNetwork

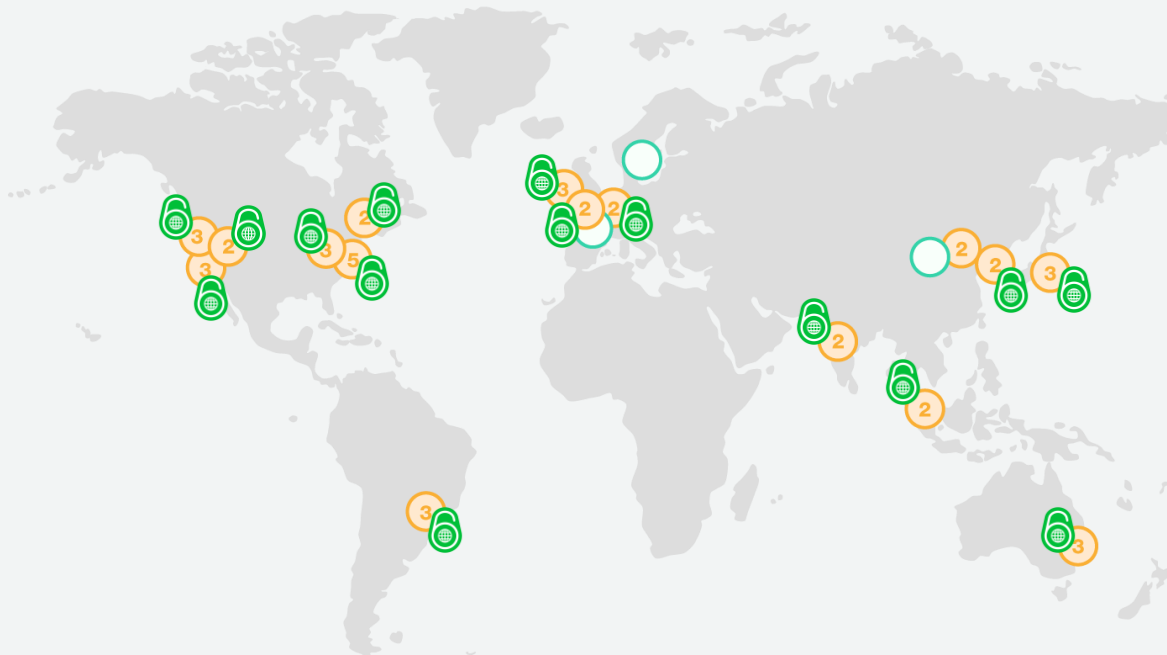
- ファイバ切断してもインパクトがない運用
- 全世界に十分な容量を確保

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

15 Regions – 42 Availability Zones – 107 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)

Announced Regions

Paris, Ningxia(寧夏), Stockholm, Osaka

Europe

Ireland (3)

Frankfurt (2)

London (2)

Asia Pacific

Singapore (2)

Sydney (2), Tokyo (3),

Seoul (2), Mumbai (2)

China

Beijing (2)









AWSサービスポートフォリオ

TECHNICAL & BUSINESS SUPPORT

-  Support
-  Professional Services
-  Partner Ecosystem
-  Training & Certification
-  Solutions Architects
-  Account Management
-  Security & Pricing Reports








HYBRID ARCHITECTURE

-  Integrated Networking
-  Direct Connect
-  Identity Federation
-  Integrated App Deployments
-  Data Backups
-  Integrated Resource Management






MARKETPLACE

-  Business Apps
-  Business Intelligence
-  DevOps Tools
-  Security
-  Networking
-  Databases
-  Storage







ANALYTICS

-  Data Warehousing
-  Business Intelligence
-  Hadoop/Spark
-  Streaming Data Analysis
-  Streaming Data Collection
-  Machine Learning
-  Elastic Search







APP SERVICES

-  Queuing & Notifications
-  Workflow
-  Search
-  Email
-  Transcoding






MOBILE SERVICES

-  API Gateway
-  Identity
-  Sync
-  Mobile Analytics
-  Single Integrated Console
-  Push Notifications





DEVELOPMENT & OPERATIONS

-  One-click App Deployment
-  DevOps Resource Management
-  Application Lifecycle Management
-  Containers
-  Triggers
-  Resource Templates

IoT

-  Rules Engine
-  Device Shadows
-  Device SDKs
-  Device Gateway
-  Registry

ENTERPRISE APPS

-  Virtual Desktops
-  Sharing & Collaboration
-  Corporate Email
-  Backup

SECURITY & COMPLIANCE

-  Identity Management
-  Access Control
-  Key Management & Storage
-  Monitoring & Logs
-  Configuration Compliance
-  Web application firewall
-  Assessment and reporting
-  Resource & Usage Auditing

CORE SERVICES

-  Compute VMs, Auto-scaling, & Load Balancing
-  Storage Object, Blocks, Archival, Import/Export
-  CDN
-  Databases Relational, NoSQL, Caching, Migration
-  Networking VPC, DX, DNS

INFRASTRUCTURE

-  Regions
-  Availability Zones
-  Points of Presence

The AWS Platform

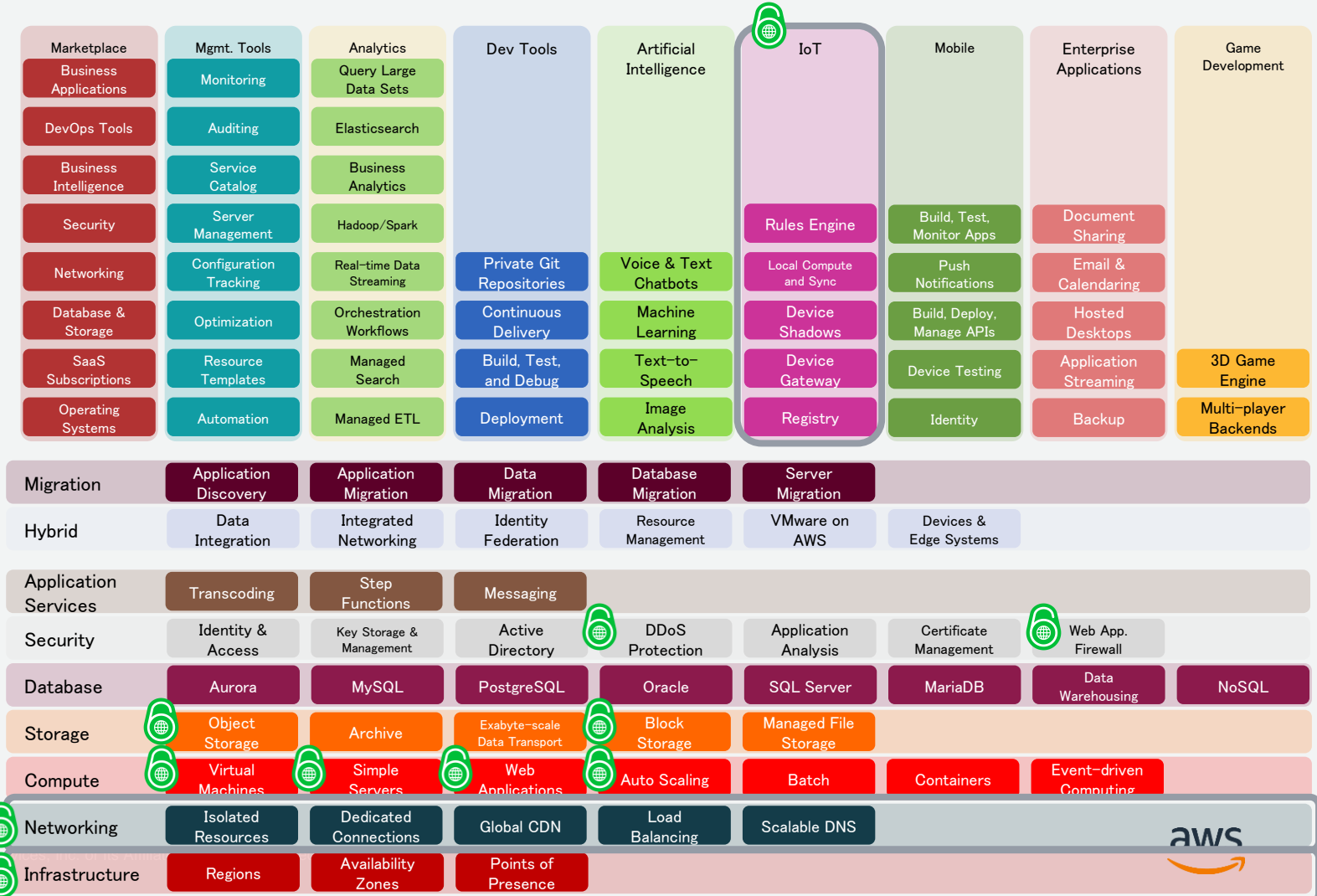
- Account Support
- Support
- Managed Services
- Professional Services
- Partner Ecosystem
- Training & Certification
- Solution Architects
- Account Management
- Security & Pricing Reports
- Technical Acct. Management

	Marketplace Business Applications	Mgmt. Tools Monitoring	Analytics Query Large Data Sets	Dev Tools	Artificial Intelligence	IoT	Mobile	Enterprise Applications	Game Development
	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						



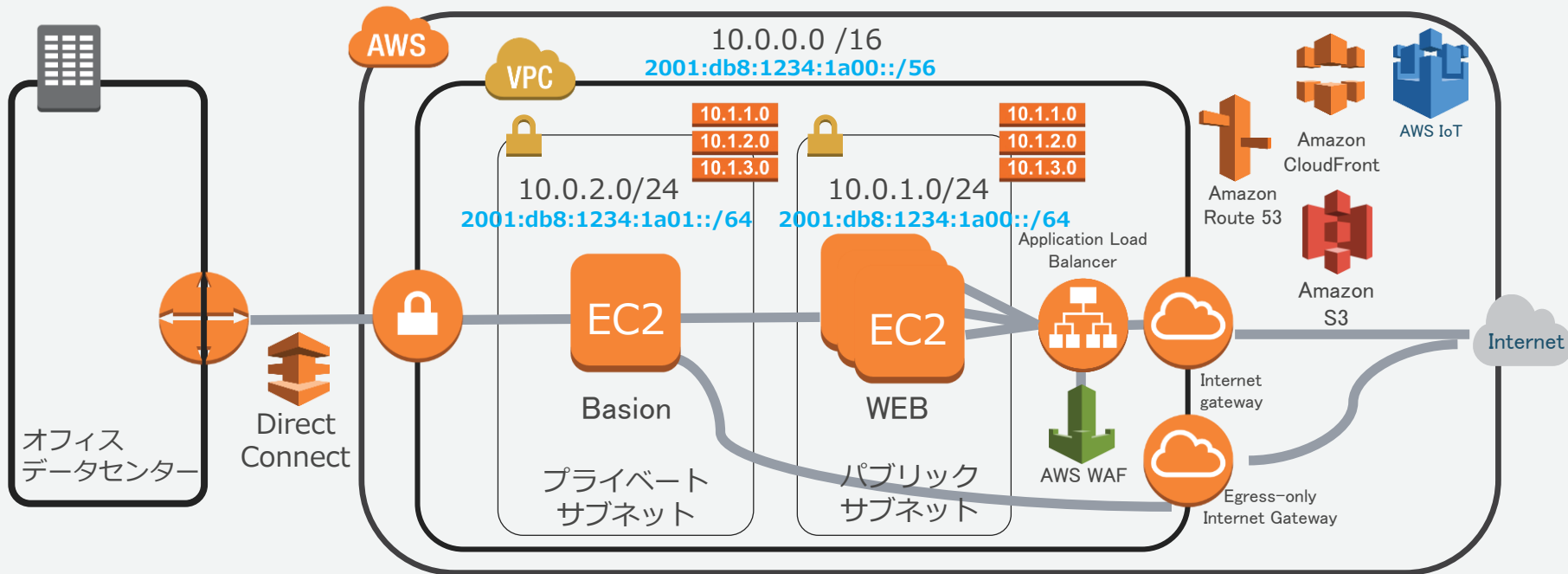
The AWS Platform

- 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

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."



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

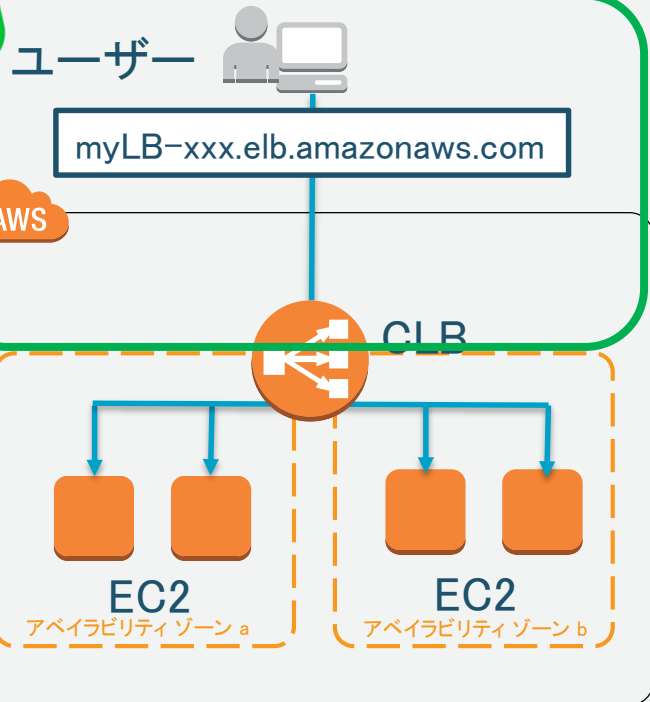
You've probably read some panic-inducing articles about the fact that the number of devices connected to the Internet is continuing to grow at a rapid rate. This growth is driven by the continued growth in the number of devices connected to the Internet using the Internet Protocol (IP) version 6 (IPv6) 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 [\(https://aws.amazon.com/jp/elasticloadbalancing/classicloadbalancer/\)](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-Classicalネットワーク向け)

価格体系 [\(https://aws.amazon.com/jp/elasticloadbalancing/classicloadbalancer/pricing/\)](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. At the top, there are buttons for 'Create Load Balancer' and 'Delete'. Below this is a table listing the load balancer:

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)

Below the table, the console shows '1 Load Balancer selected' and details for 'Load Balancer: my-load-balancer'. There are tabs for 'Description', 'Instances', and 'Health Check'. The 'Description' tab is active, and the 'DNS Name' section is highlighted in yellow. It lists three DNS record options:

- 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)

A red arrow points to the 'dualstack' record. Below the DNS names is a note: '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 DNS Name. Any...

AWS IoT



簡単で安全なクラウドへのデバイス接続サービス

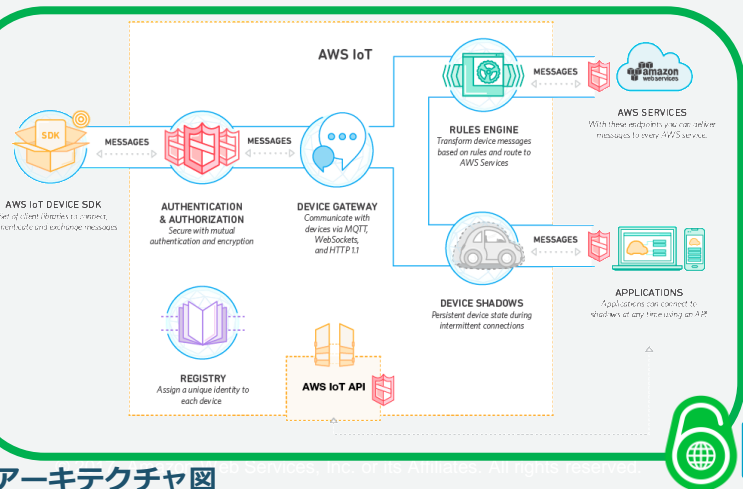


特徴 [\(https://aws.amazon.com/jp/iot/\)](https://aws.amazon.com/jp/iot/)

- 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)



正式サービス開始当初からIPv6をサポート

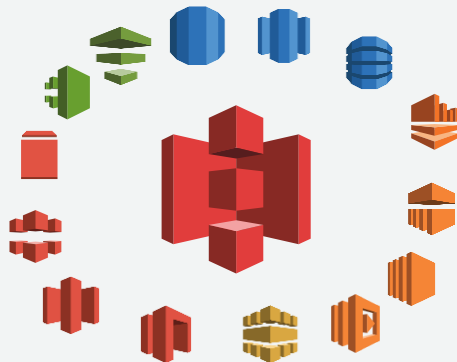
Amazon Simple Storage Service (S3)



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



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

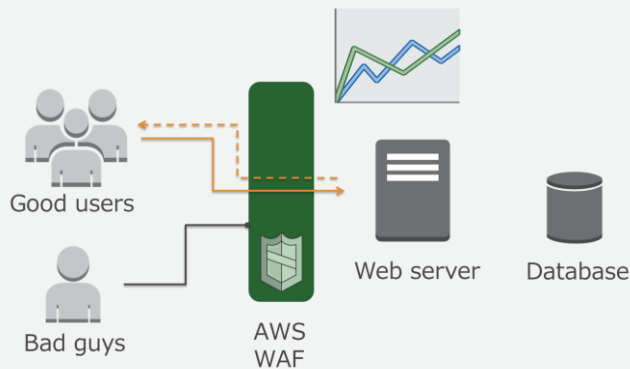
(<http://aws.amazon.com/jp/cloudfront/pricing/>)

- 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)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。

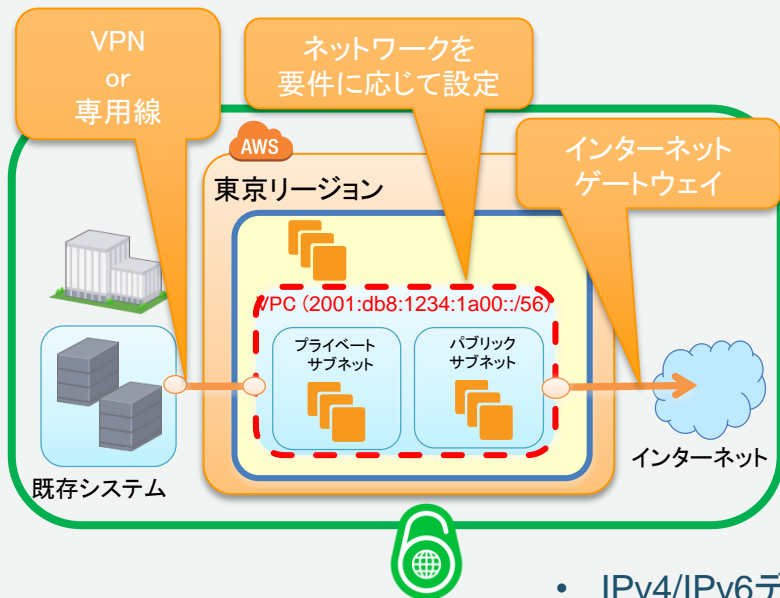
価格体系 (<http://aws.amazon.com/jp/route53/pricing/>)

- 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 [\(http://aws.amazon.com/jp/vpc/\)](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

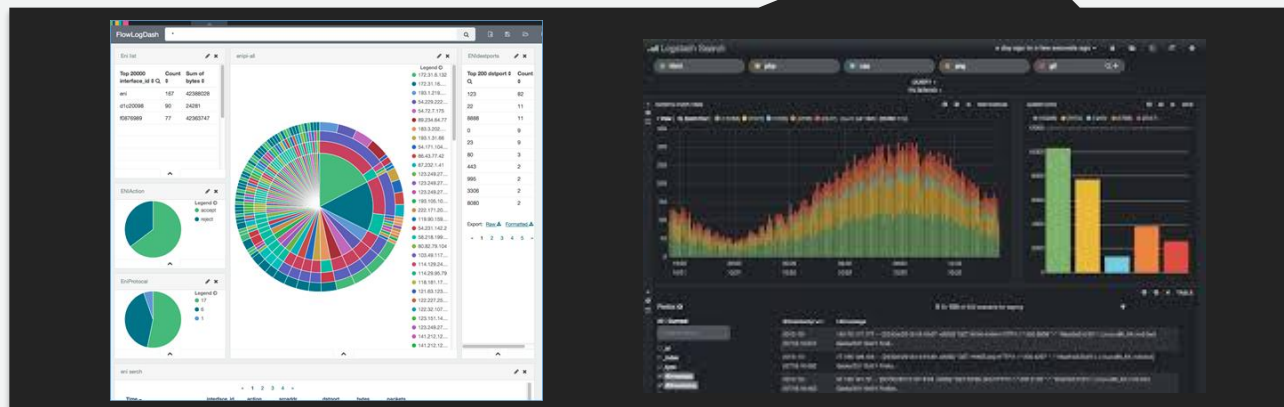
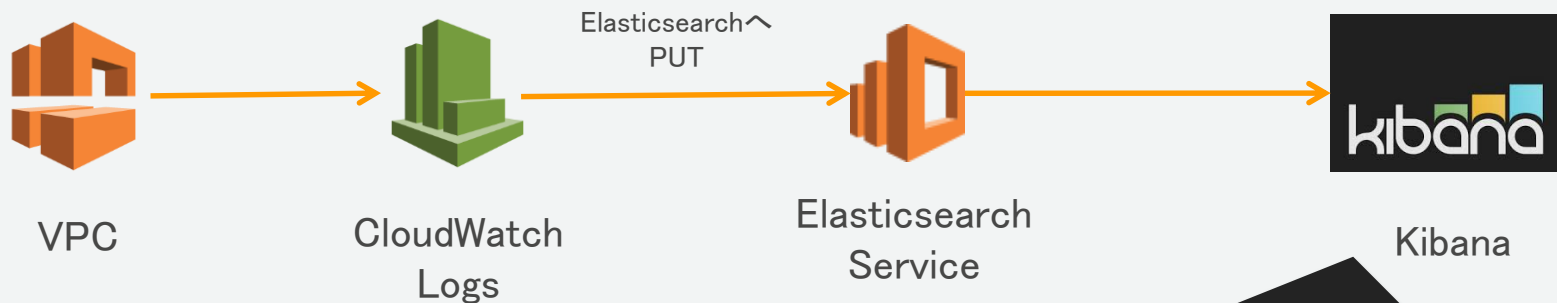
価格体系 [\(http://aws.amazon.com/jp/vpc/pricing/\)](http://aws.amazon.com/jp/vpc/pricing/)

- VPCの利用は無料

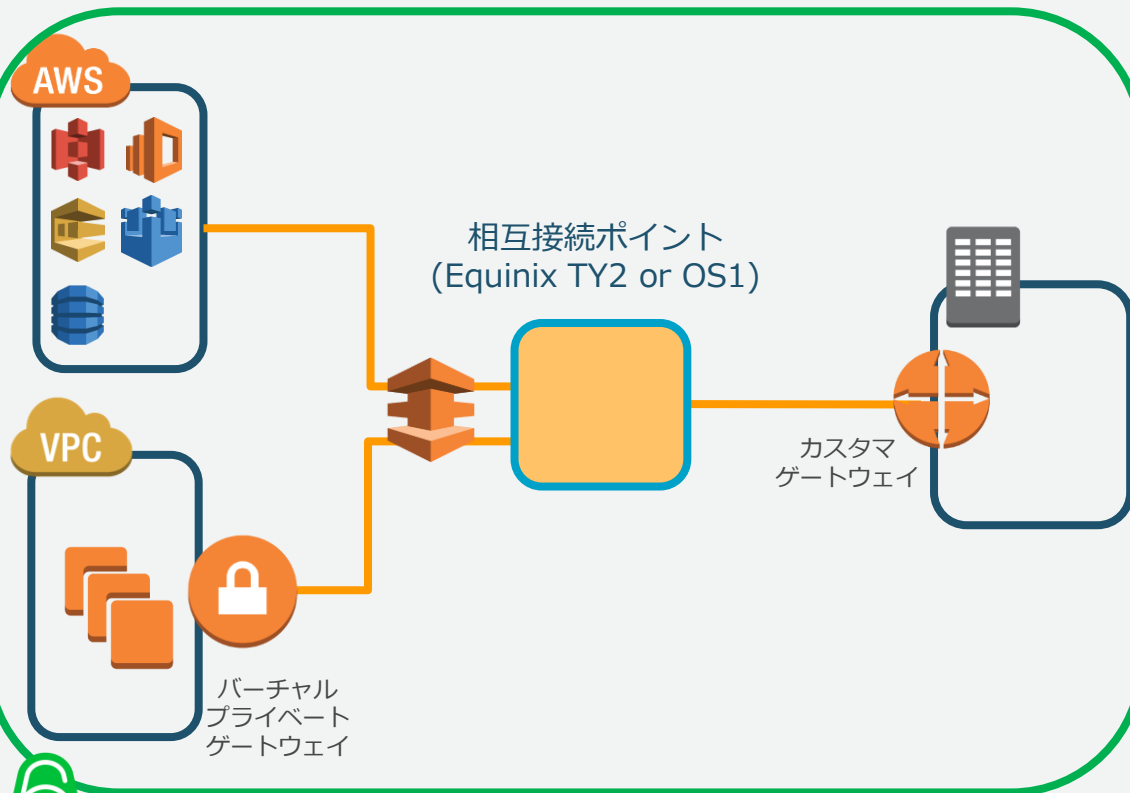
※国内電気通信事業者と
協業して提供

- 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

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



専用線(Direct Connect)接続構成



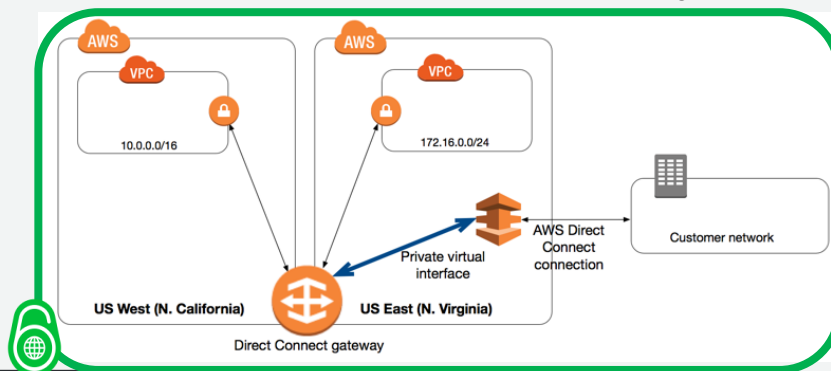
- ・AWSとお客様設備を専用線でネットワーク接続
- ・相互接続ポイントへ専用線を敷設し、AWSのルータと相互接続
- ・日本の相互接続ポイントは
東京(Equinix TY2/TY6/TY7/TY8)
大阪(Equinix OS1)
- ・ルーティングはBGPのみ
- ・接続先は以下の2つ
VPC(プライベート接続)
AWSクラウド(パブリック接続)
- ・VPNよりも一貫性がある
- ・帯域のパフォーマンスも向上
- ・ネットワークコストも削減

※国内電気通信事業者と協業して提供

Direct Connect Gateway



- Direct Connect GatewayがHubになり、同一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。

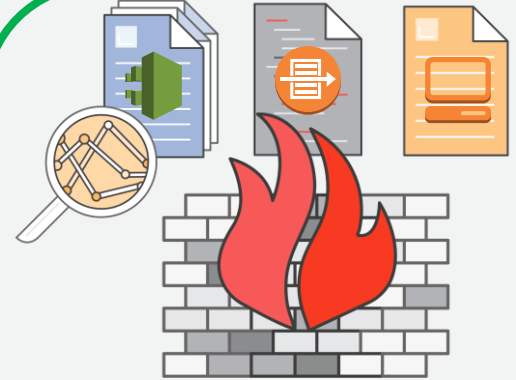


1つ以上のDirect Connect ロケーションに繋がれば
全世界の全リージョン(中国除く)に閉域網接続でき
同一リージョンまたは世界の複数リージョンをまたいで複数のVPCに接続できる機能

Amazon GuardDuty

NEW

- 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



Current findings Showing 59 of 59

Actions Save filters No saved filters

▼ Include and exclude filter options are available on certain finding attributes in the details

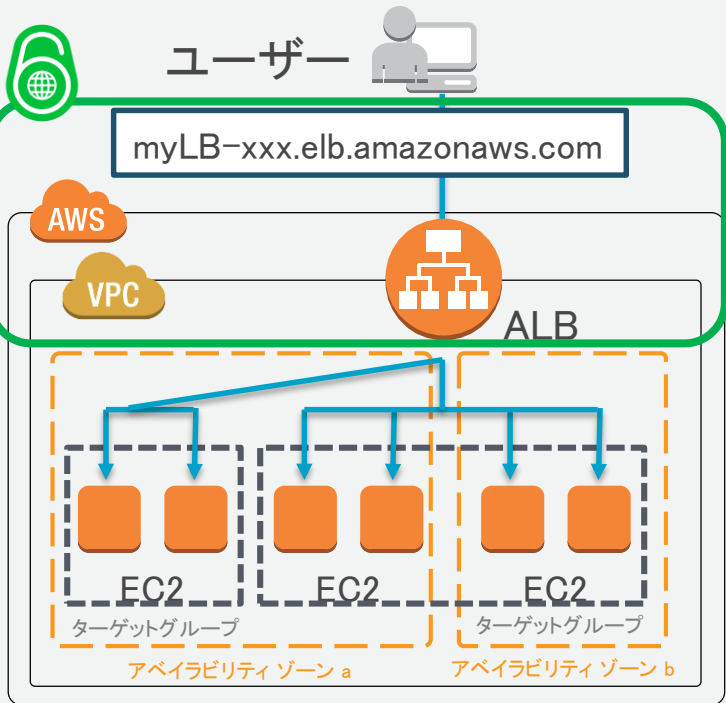
Finding	Last seen	Count
[SAMPLE] Bitcoin-related domain queries from EC2 instance i-999999...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] EC2 instance i-999999999 communicating with known XorD...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] Bitcoin-related domain name queried by EC2 instance i-99...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] IAM User GeneratedFindingUserName logged into the AW...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] API GeneratedFindingAPIName was invoked from a Kali L...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] Credentials for instance role GeneratedFindingUserName...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] EC2 instance involved in RDP brute force attacks	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] Reconnaissance API GeneratedFindingAPIName was invo...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] Blackholed domain name queried by EC2 instance i-999999...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] API GeneratedFindingAPIName was invoked from a know...	2017-11-09 16:00:04 (9 days ago)	1
[SAMPLE] Amazon EC2 instance i-999999999 type [sample]	2017-11-09 16:00:04 (9 days ago)	1



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 [\(https://aws.amazon.com/elasticloadbalancing/applicationloadbalancer/\)](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

[\(https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/\)](https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/)

- ALBの起動時間
- Load Balancer Capacity Units (LCU)の使用量

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



Amazon FreeRTOS Device Software

Amazon FreeRTOS is an operating system for microcontrollers that makes it easy to securely connect IoT devices locally or to the cloud. You can use a predefined configuration or create your own to get started.

Already downloaded your software? [Learn more](#) about next steps.

Software Configurations

Type	Configuration	Hardware platform
Predefined	Connect to AWS IoT - Windows	Windows Simulator
Predefined	Connect to AWS IoT - TI	CC3200P-LAUNCHXL
Predefined	Connect to AWS IoT - ST	STM32L4 Discovery kit IoT node
Predefined	Connect to AWS IoT - 100P	LP34018 IoT Module
Predefined	Connect to AWS Greengrass - Windows	Windows Simulator
Predefined	Connect to AWS Greengrass - TI	CC3200P-LAUNCHXL
Predefined	Connect to AWS Greengrass - ST	STM32L4 Discovery kit IoT node
Predefined	Connect to AWS Greengrass - 100P	LP34018 IoT Module

By downloading this software you agree

Configure Amazon FreeRTOS Software

New Software Configuration

Hardware platform
Amazon FreeRTOS software extends the FreeRTOS kernel with software libraries that make it easy for microcontroller-based devices to securely connect locally or to the cloud.

Windows Simulator SIMULATOR Visual Studio MSVC [Clear](#) [Close](#)

Development tools
Integrated Development Environment (IDE)

Visual Studio

Compiler

MSVC

Libraries
Select additional libraries to extend the functionality of the FreeRTOS kernel:

No library selected [Close](#)

Search

- Greenpress Discovery AMAZON SERVICES This library enables the discovery and selection of AWS Greengrass Core devices.
- MQTT CONNECTIVITY This library implements the MQTT protocol that enables communication with AWS IoT ...
- Thing Shadow AMAZON SERVICES This library enables communication with AWS IoT Thing Shadow.

NEW

その他

IP アドレス条件演算子(aws:SourceIp)

ip-ranges.json

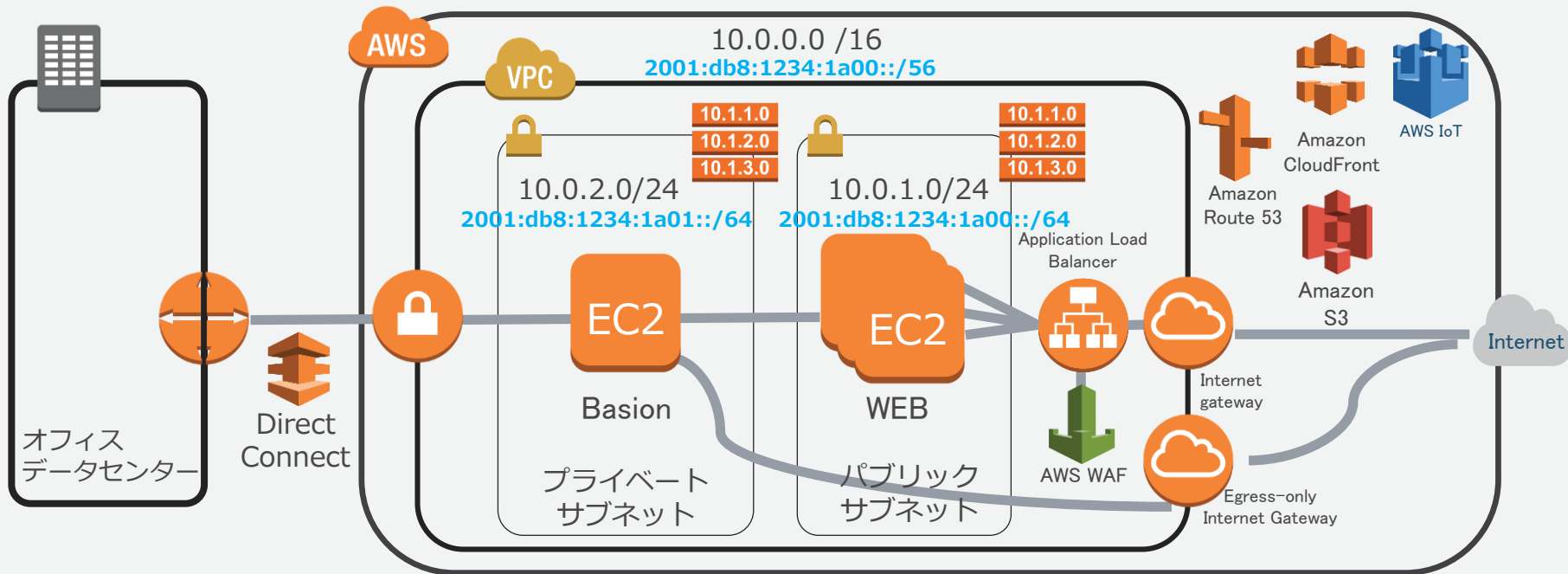
```
"ipv6_prefixes": [  
  {  
    "ipv6_prefix": "2400:6500:0:7000::/56",  
    "region": "ap-southeast-1",  
    "service": "AMAZON"  
  },  
  {  
    "ipv6_prefix": "2400:6500:0:7100::/56",  
    "region": "ap-northeast-1",  
    "service": "AMAZON"  
  },  
  (...)  
]
```

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

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

