資料３７－３

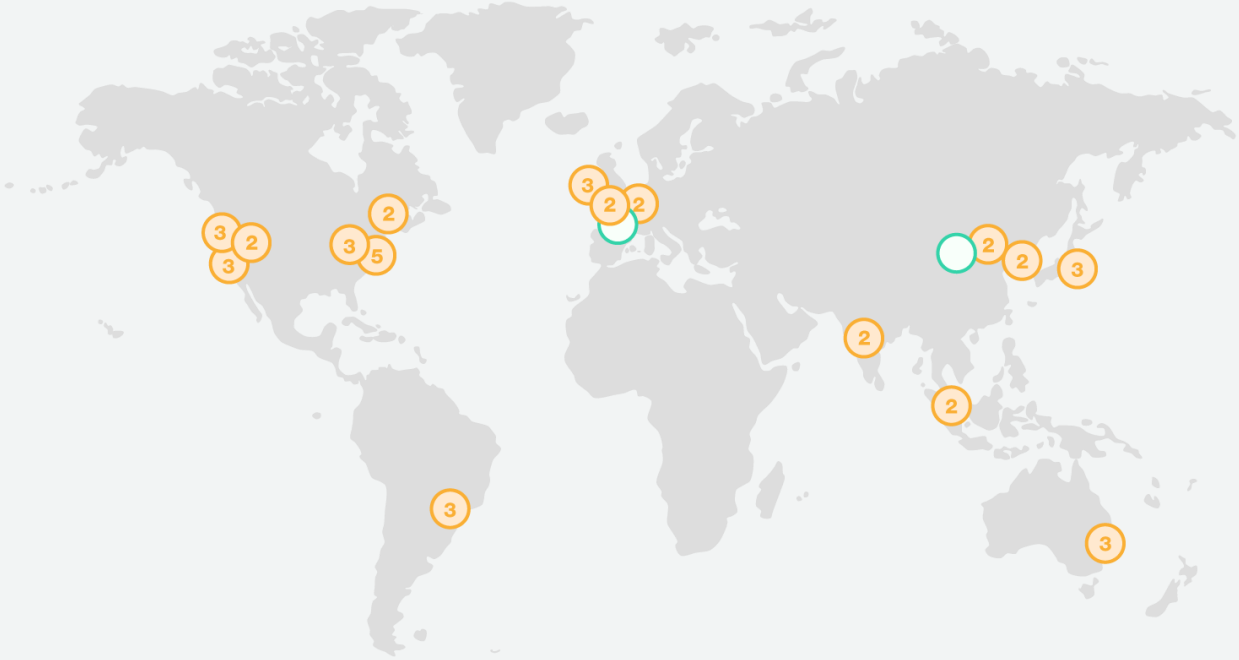
Amazon Web Services (AWS)における IPv6対応状況

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)

US West
Oregon (3)
Northern California (3)

US East
N. Virginia (6), Ohio (3)

Canada
Central (2)

South America
São Paulo (3)

EU
Ireland (3)
Frankfurt (2)
London (2)

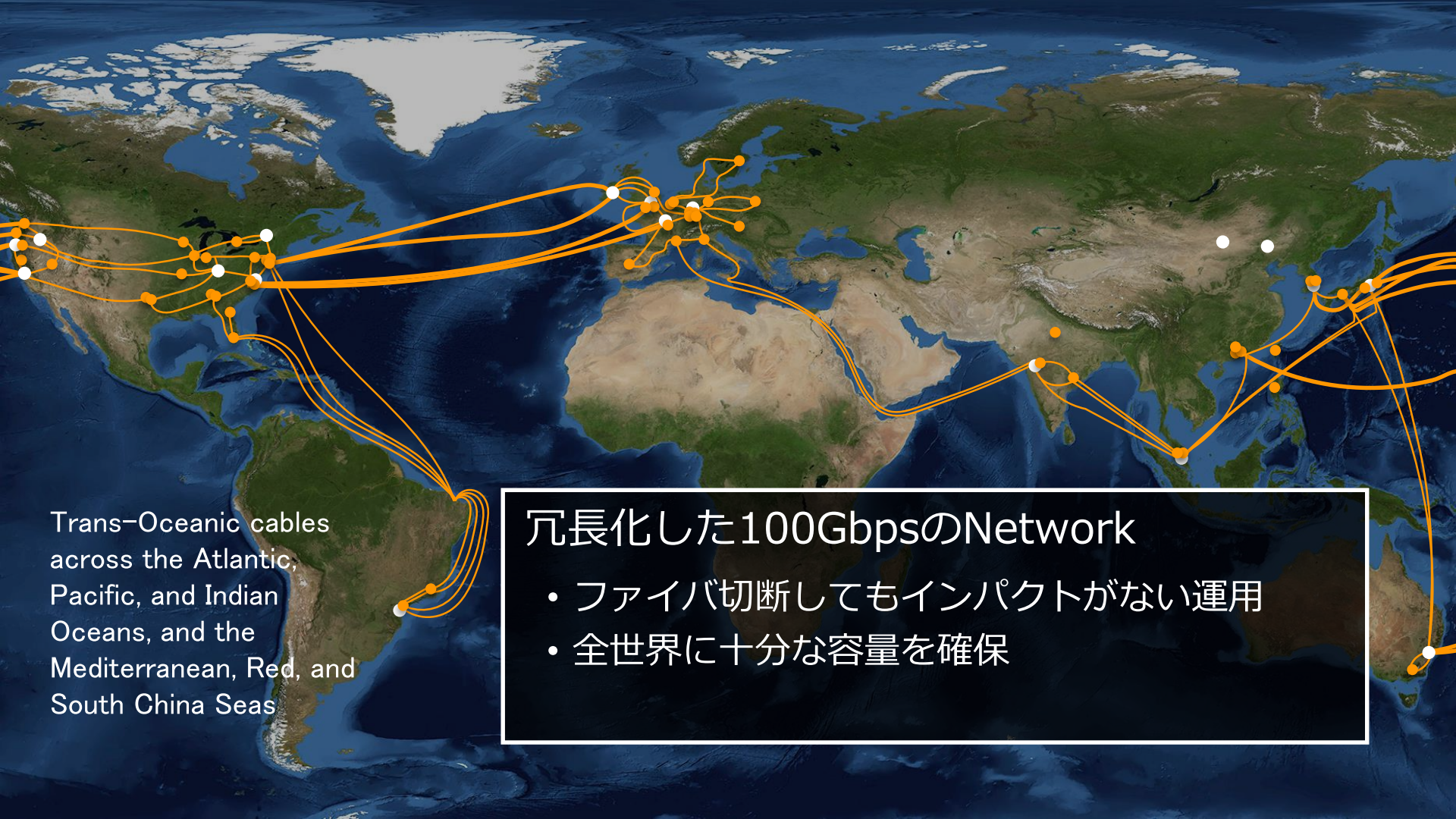
Asia Pacific
Singapore (2)
Sydney (2), Tokyo (3),
Seoul (2), Mumbai (2)

China
Beijing (2)

Announced Regions

Paris, Ningxia, Sweden, Hong-Kong, Osaka

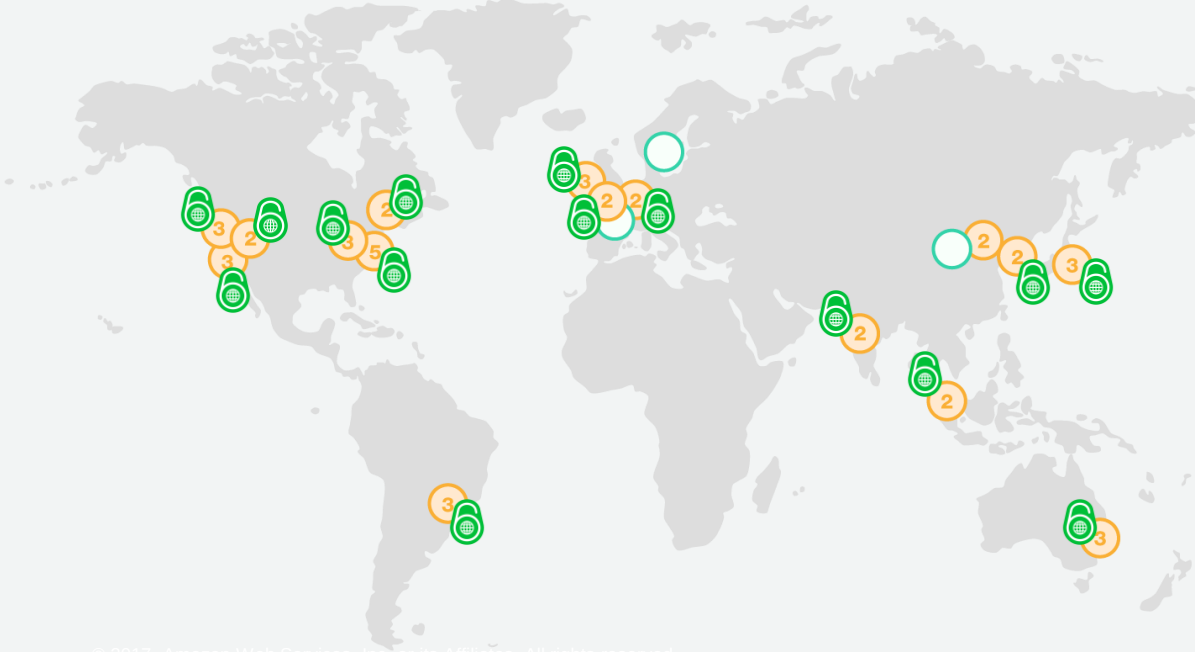
aws


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

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)

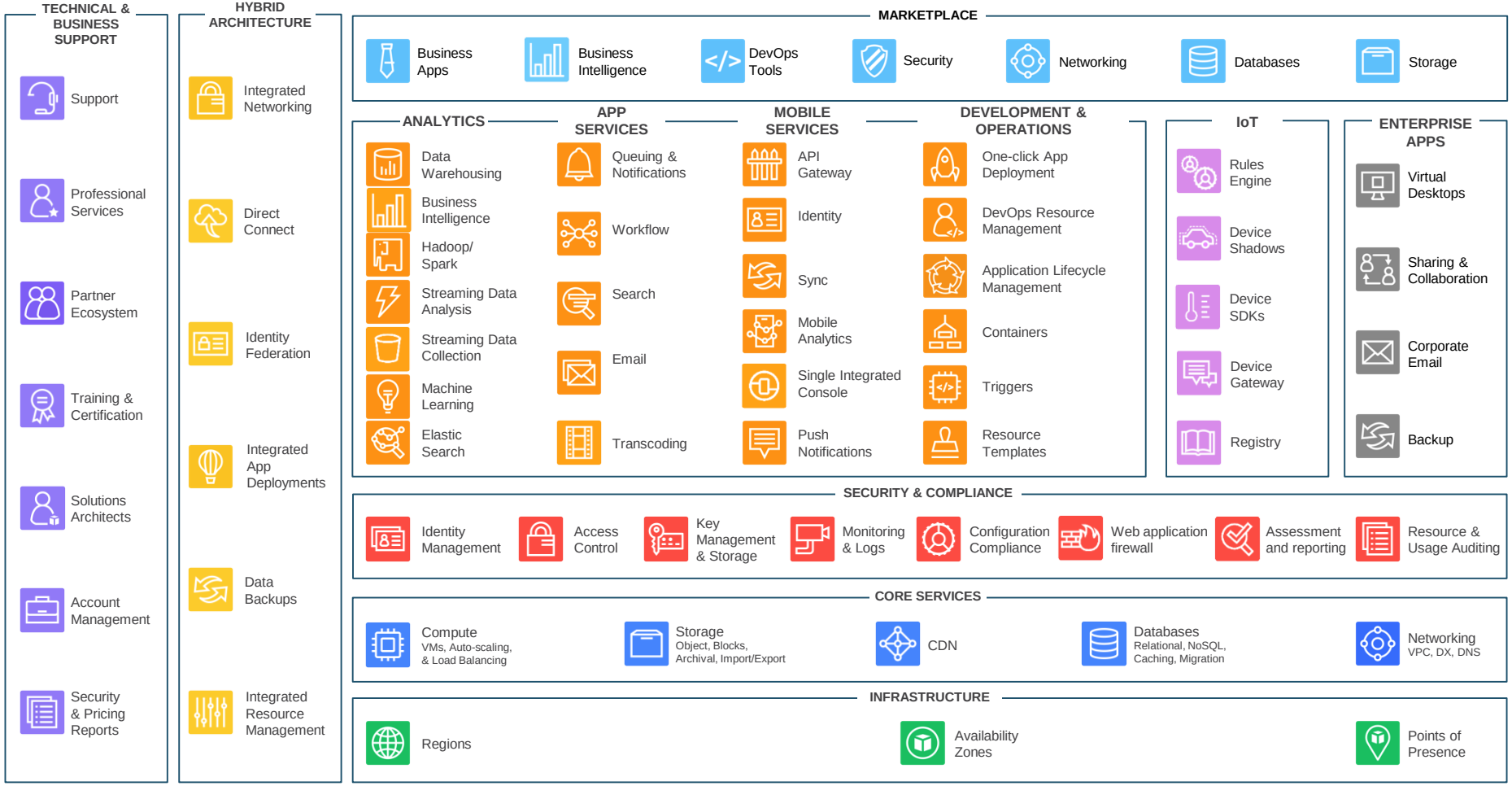
Asia Pacific
Singapore (2)
Sydney (2), Tokyo (3),
Seoul (2), Mumbai (2)

China
Beijing (2)

Announced Regions

Paris, Ningxia(寧夏), Stockholm, Osaka

AWSサービスポートフォリオ



The AWS Platform

The AWS Platform

Account Support

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

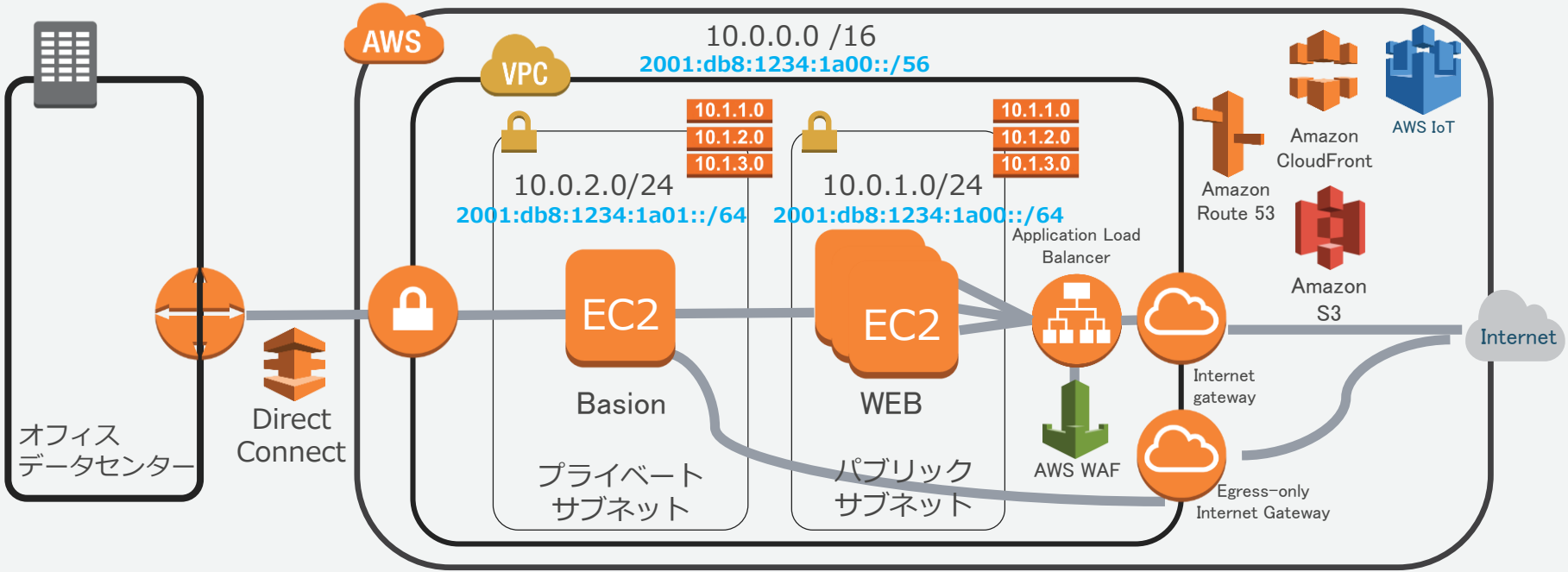
Marketplace	Mgmt. Tools	Analytics	Dev Tools	Artificial Intelligence	IoT	Mobile	Enterprise Applications	Game Development
Business Applications	Monitoring	Query Large Data Sets						
DevOps Tools	Auditing	Elasticsearch						
Business Intelligence	Service Catalog	Business Analytics						
Security	Server 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					

aws

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

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."

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:

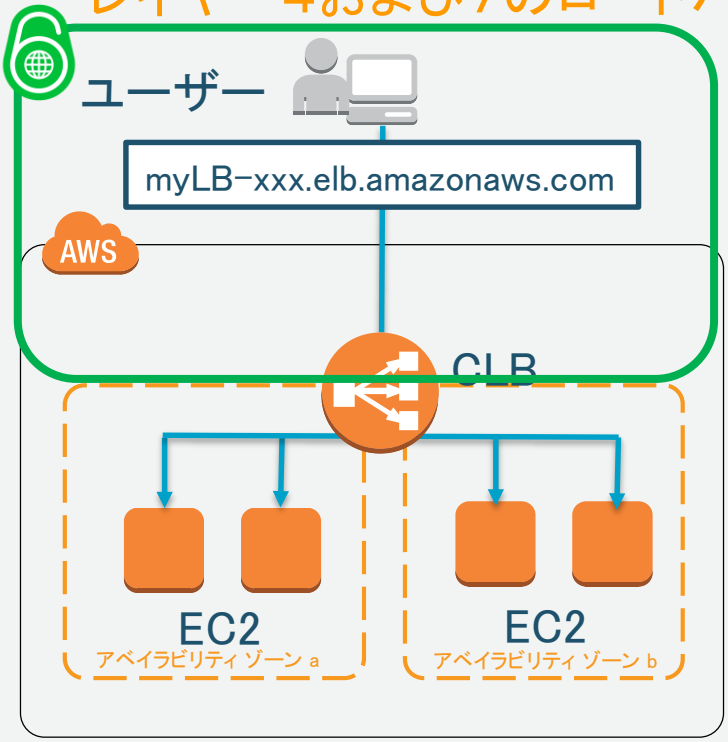
IPv6 Support

You've probably read some panic-inducing articles about the fa
continued growth in the number of devices connected to the In
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



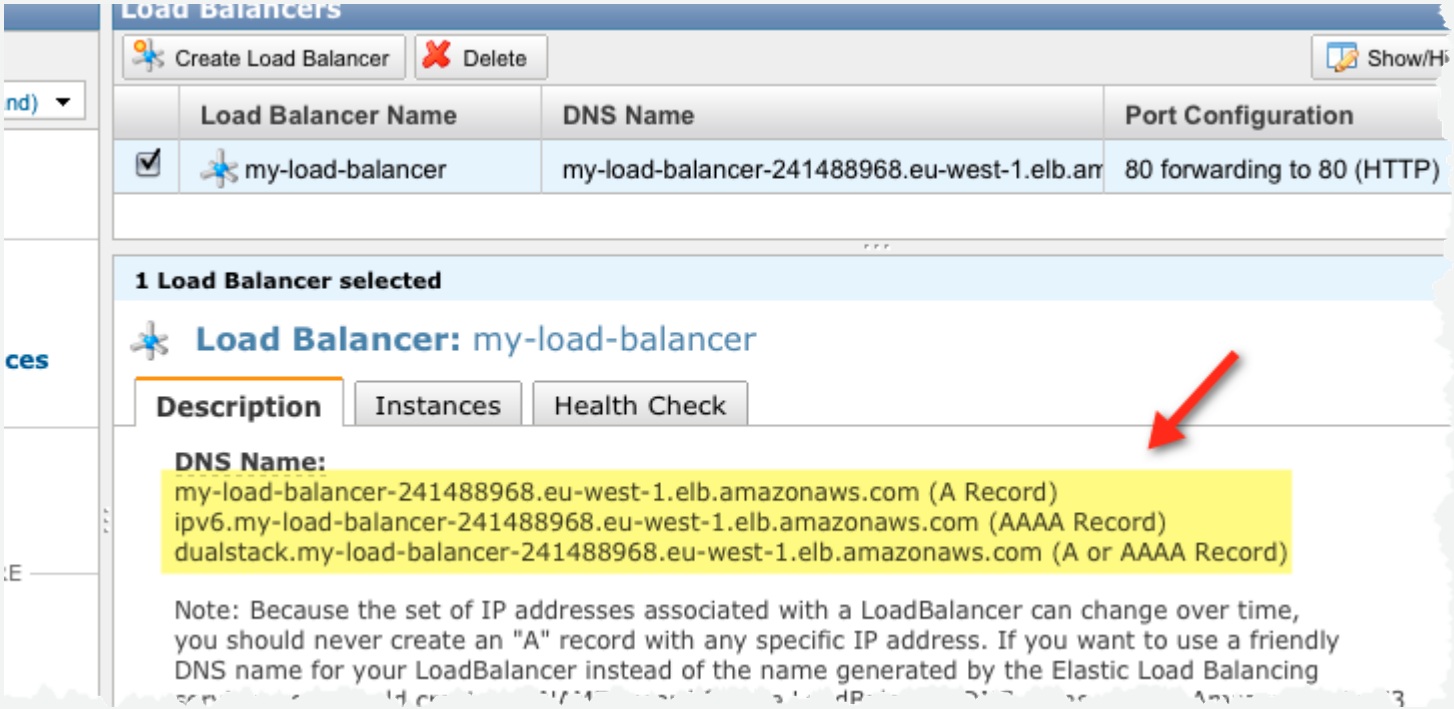
特徴 (https://aws.amazon.com/jp/elasticloadbalancing/classicloadbalancer/)

- 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

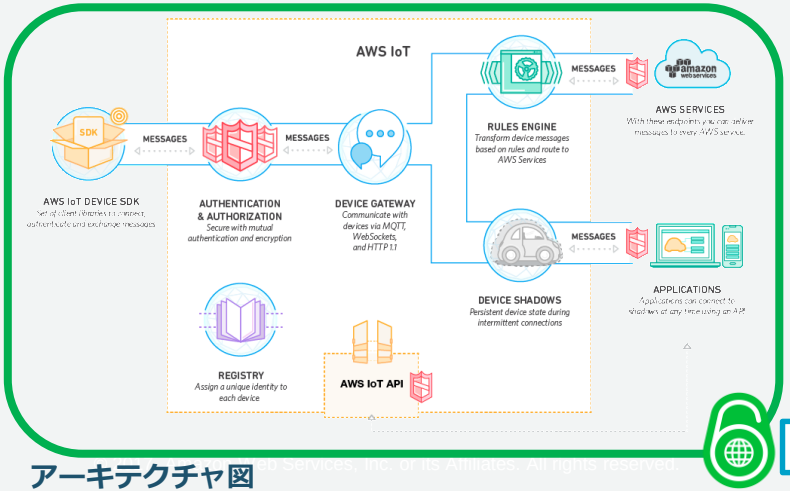
ELB(当時)におけるIPv6はオプトイン



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/)

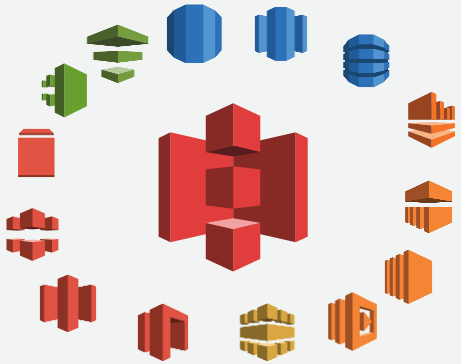
- 100万メッセージあたり$8(日本リージョン)
- 無料利用枠利用は25万メッセージ/月を(1年間)

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

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

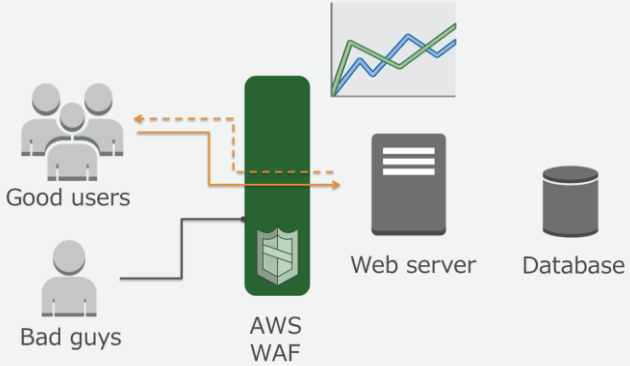
- 簡単にサイトの高速化が実現できると共に、サーバの負荷も軽減
- 様々な規模のアクセスを処理することが可能
- 世界87箇所のエッジロケーション

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。

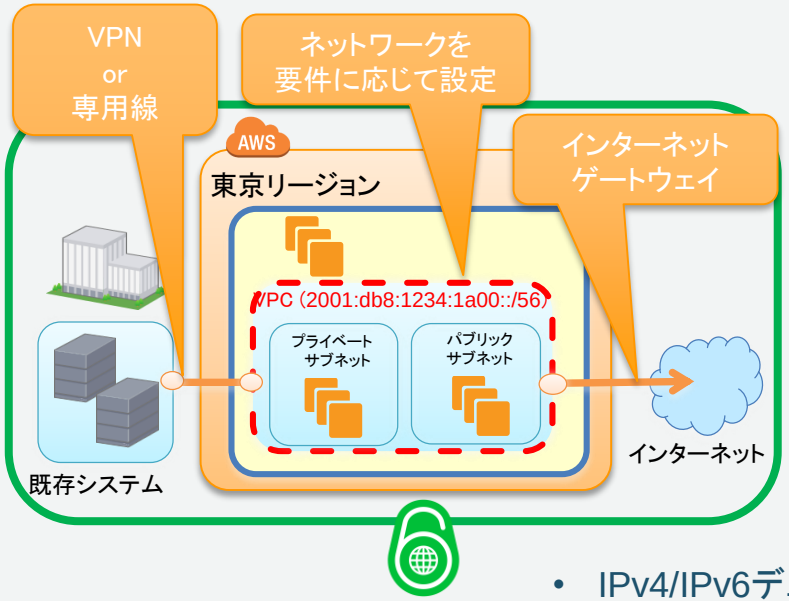
価格体系 (http://aws.amazon.com/jp/route53/pricing/)

- 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

aws amazon web services

Amazon Virtual Private Cloud (VPC)

仮想プライベートクラウドサービス



※国内電気通信事業者と
協業して提供

特徴 (http://aws.amazon.com/jp/vpc/)

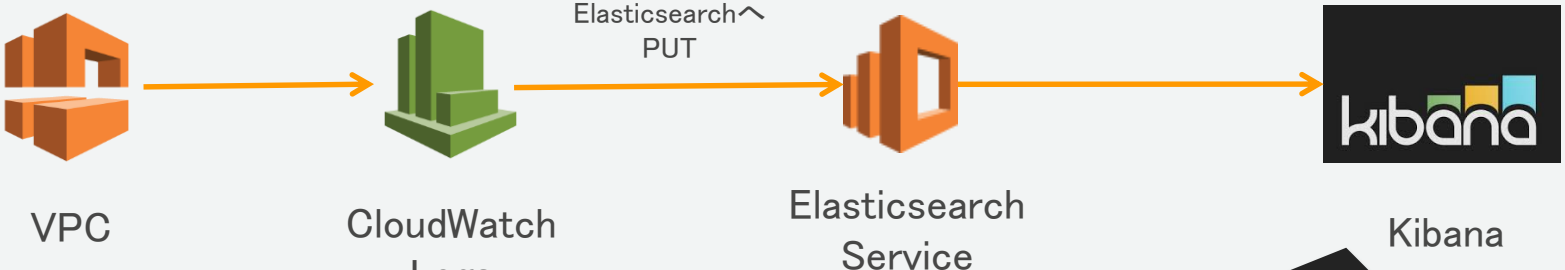
- AWS上にプライベートネットワークを構築
- AWSと既存環境のハイブリッド構成を実現
- きめ細かいネットワーク設定が可能

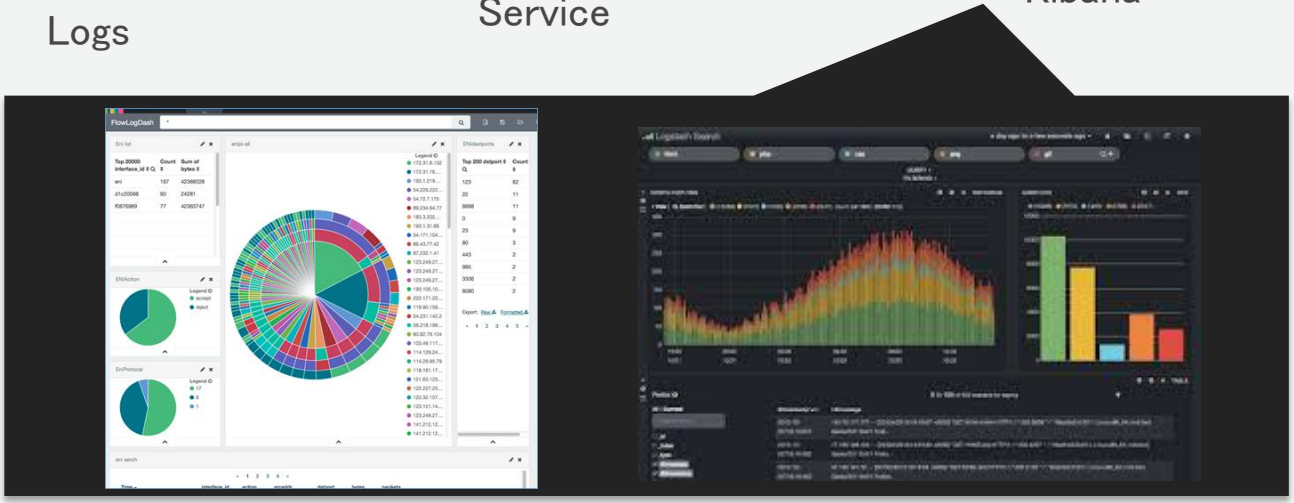
価格体系 (http://aws.amazon.com/jp/vpc/pricing/)

- VPCの利用は無料

- 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

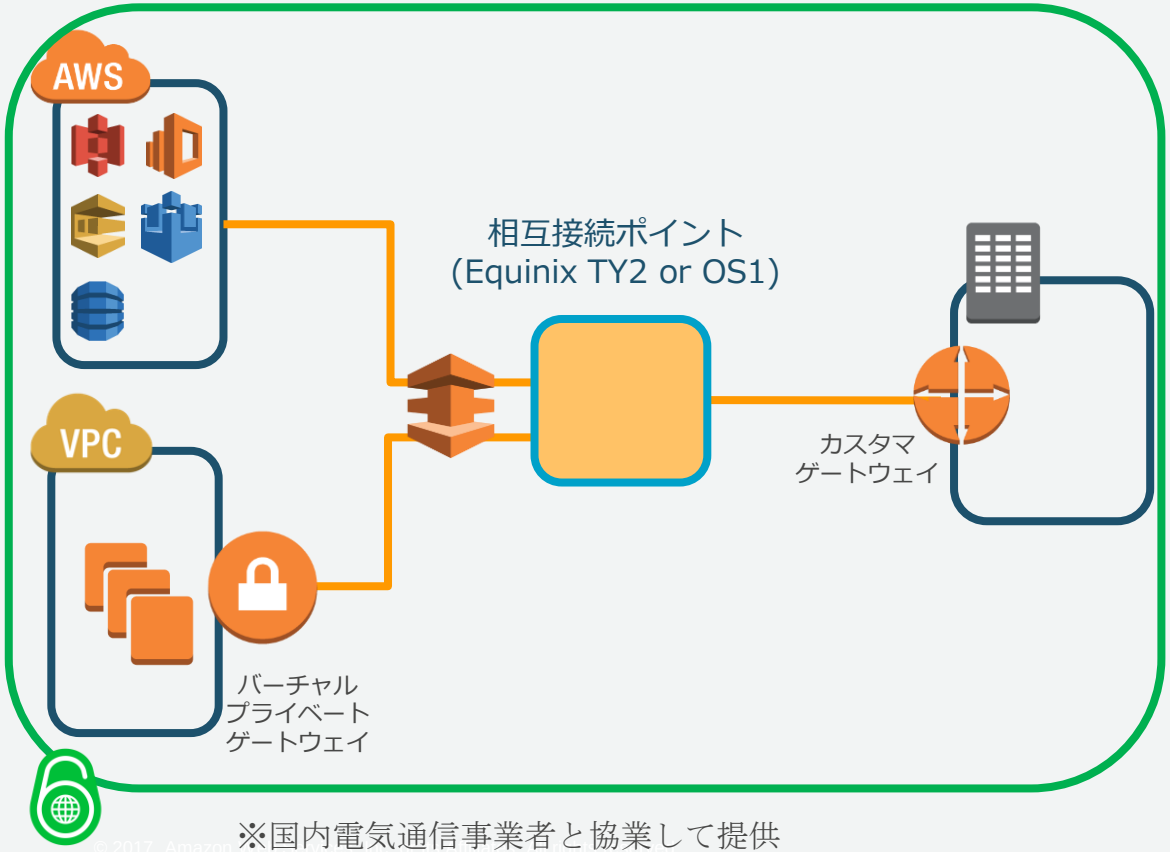
VPC Flow Logs+Elasticsearch Service+Kibanaによる可視化





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

専用線(Direct Connect)接続構成



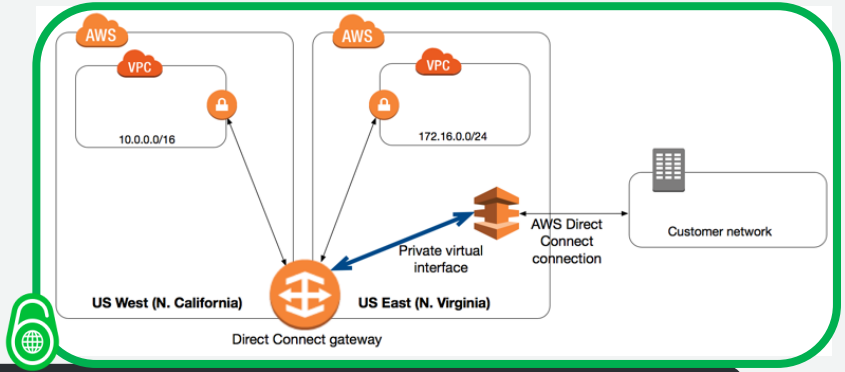
※国内電気通信事業者と協業して提供

- 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

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。

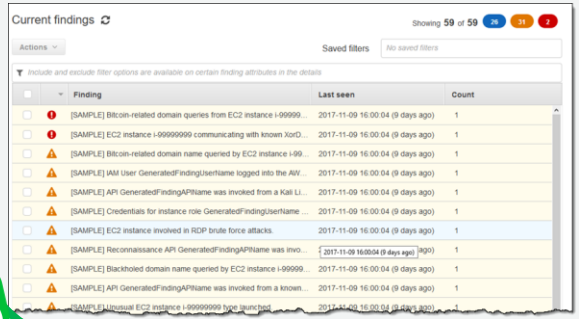


1つ以上のDirect Connect ロケーションに繋げば
全世界の全リージョン（中国除く）に閉域網接続でき
同一リージョンまたは世界の複数リージョンをまたいで複数のVPCに接続できる機能

Amazon GuardDuty

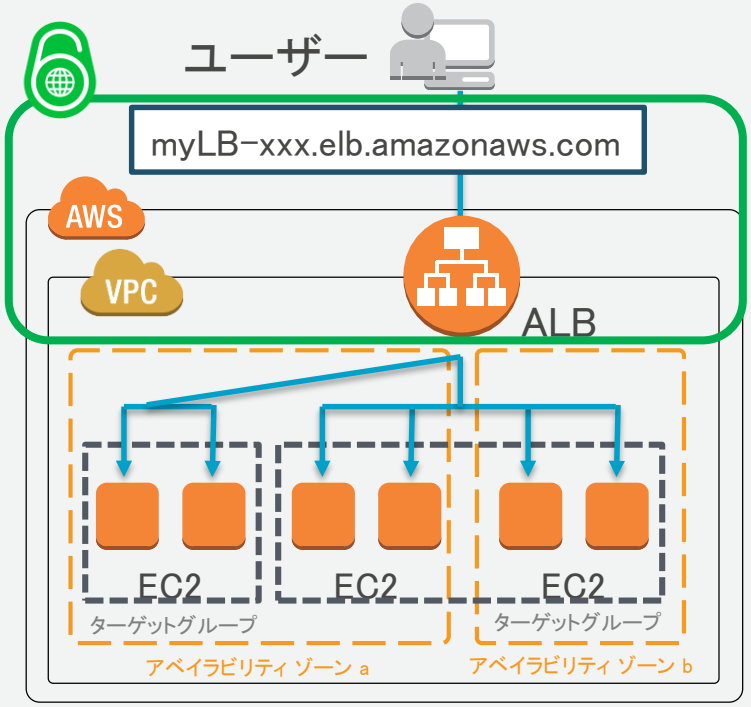
NEW

- 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



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

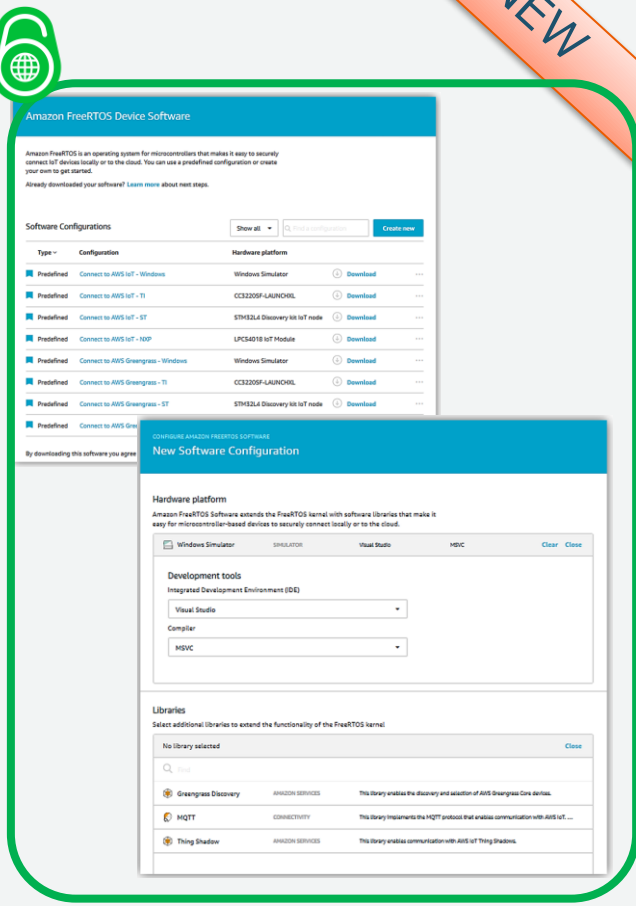
価格体系

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

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

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”
    },
    (…)
  ]
```

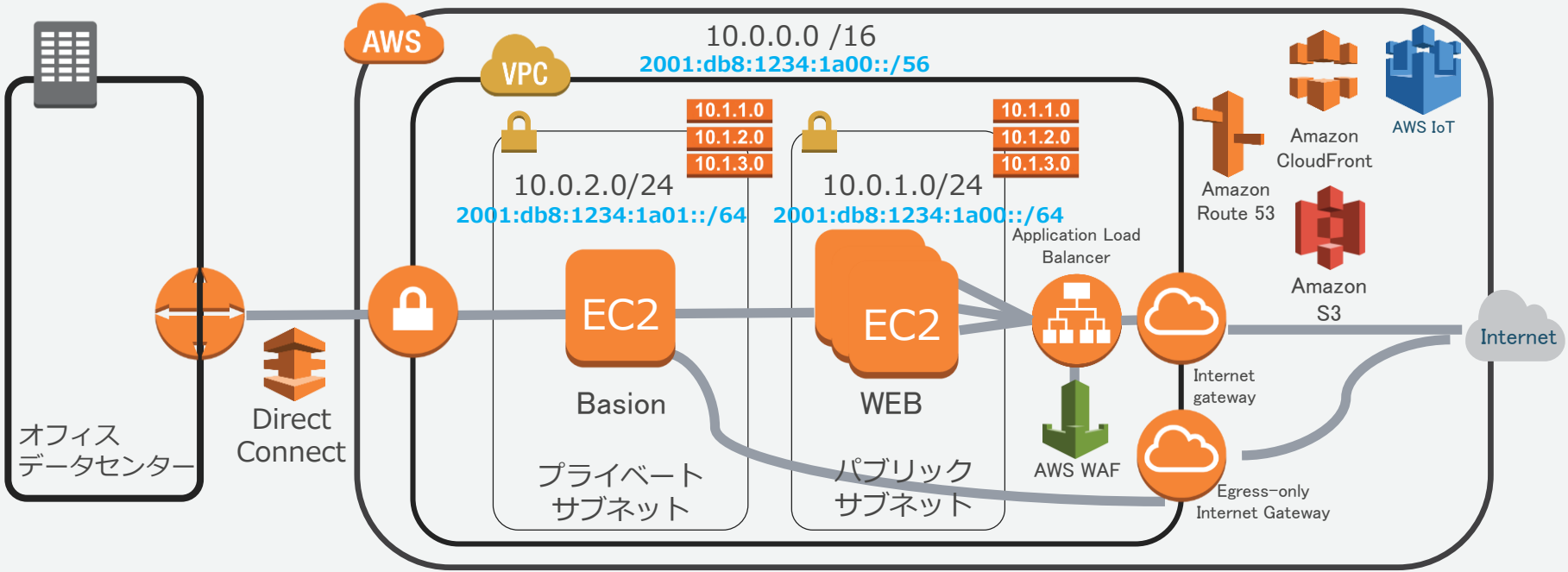
```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "someservice:*",
    "Resource": "*",
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "203.0.113.0/24",

"2001:DB8:1234:5678::/64”
        ]
      }
    }
  }
}
```

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

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

Working Backwards

AWSサービスのIPv6化

- IPv6でお客さま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
- お客さま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