



AWS  
**Black Belt**  
Online Seminar

# Amazon Elastic Compute Cloud (EC2)

AWS Black Belt Online Seminar 2017

アマゾン ウェブ サービス ジャパン株式会社

ソリューションアーキテクト 浅野 佑貴

2017.04.05



# Who are you?

名前：浅野 佑貴（あさの ゆうき）

所属：アマゾンウェブサービスジャパン  
ソリューションアーキテクト

ロール：製造業のお客様を中心に、技術的なご支援を担当

経歴：国内SIerにてクラウド関連ビジネスの立ち上げ・推進を担当

好きなAWSサービス： Consolidated Billing と AWS Organizations



# 内容についての注意点

- 本資料では2017年4月5日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A




# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A



# サービス開始

- 2006年8月26日
- m1.smallのみ
  - 1 vCPU
  - 1.7GHz Xeon プロセッサ
  - 1.75GB メモリ
  - 160GB インスタンスストア




Menu

## AWS Blog

### Amazon EC2 Beta

by Jeff Barr | on 25 AUG 2006 | In [Announcements](#) | [Permalink](#) | [Comments](#)

Innovation never takes a break, and neither do I. From the steaming hot beaches of Cabo San Lucas I would like to tell you about the Amazon Elastic Compute Cloud, or Amazon EC2, now open for limited beta testing, with more beta slots to open soon.



Amazon EC2 gives you access to a virtual computing environment. Your applications run on a "virtual CPU", the equivalent of a 1.7 GHz Xeon processor, 1.75 GB of RAM, 160 GB of local disk and 250 Mb/second of network bandwidth. You pay just 10 cents per clock hour (billed to your Amazon Web Services account), and you can get as many virtual CPUs as you need. You can learn more on the [EC2 Detail Page](#). We built Amazon EC2 using a virtual machine monitor by the name of [Xen](#).

Amazon EC2 works in terms of AMIs, or Amazon Machine Images. Each AMI is a pre-configured boot disk — just a packaged-up operating system stored as an [Amazon S3](#) object. There are web service calls to create images, and to assign them to virtual CPUs to run your application. If your application consists of the usual web server, business logic, and database tiers, you can build distinct AMIs for each tier, and then spawn one or more instances of each type based on the load.

## HYBRID ARCHITECTURE

Integrated Networking

Direct Connect

Identity Federation

Integrated App Deployments

Data Backups

VMware Integration

Integrated Resource Management

## MARKETPLACE

Business Apps

Business Intelligence

DevOps Tools

Security

Networking

Databases

Storage

## TECHNICAL & BUSINESS SUPPORT

Support

Professional Services

Optimization Guidance

Partner Ecosystem

Training & Certification

Solutions Architects

Account Management

Security & Billing Reports

### ANALYTICS

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

### APP SERVICES

Queuing & Notifications  
Workflow  
Search  
Email  
Transcoding

### MOBILE SERVICES

API Gateway  
Single Integrated Console  
Identity  
Sync  
Mobile Analytics  
Mobile App Testing  
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

### MIGRATION

Schema Conversion  
Petabyte-Scale Data Migration  
Application Migration  
Database Migration

## 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, Containers, Cloud functions

Storage  
Object, Blocks, File, Archivals, Import/Export

CDN

Databases  
Relational, NoSQL, Caching, Migration

Networking  
VPC, DX, DNS

## INFRASTRUCTURE

Regions

Availability Zones

Points of Presence

# リージョン: EC2を利用できるAWSの拠点



16のリージョン  
42のアベイラビリティゾーン(AZ)



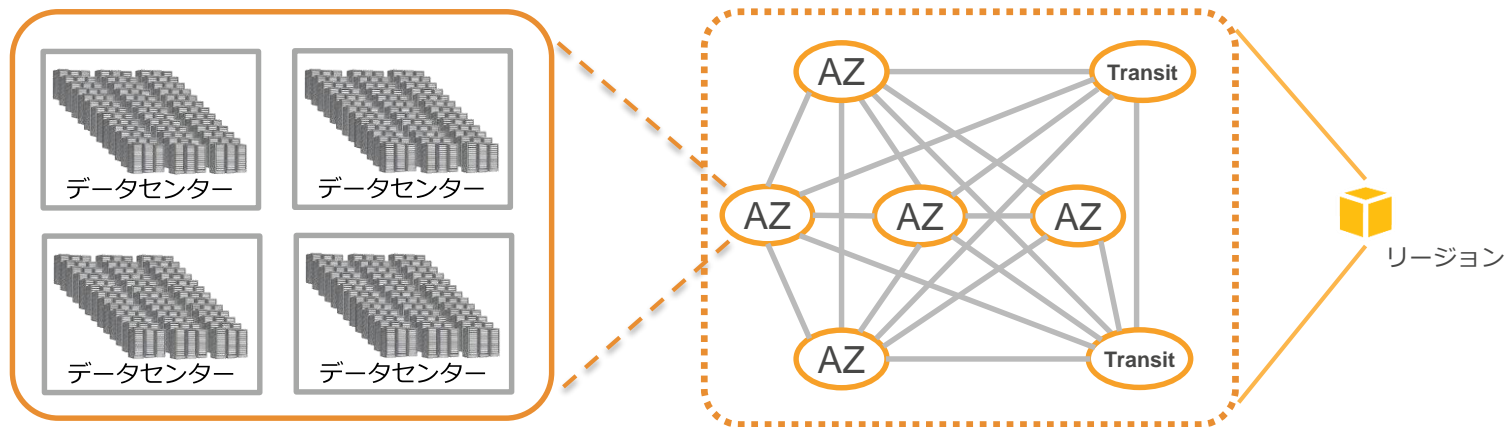
# AWSインフラストラクチャー

## リージョン

- 各リージョンは完全に独立
- リージョン間の通信はパブリックインターネット経由

## アベイラビリティゾーン(AZ)

- リージョンは2つ以上のアベイラビリティゾーン(AZ)から構成
- 各AZは、互いに影響を受けないように、地理的・電源的・ネットワーク的に独立
- AZ間は低遅延の高速専用線で接続
- 1つのAZは、最低1ヶ所以上のデータセンターで構成



# Amazon EC2(Elastic Compute Cloud)



- インスタンス:
  - 仮想コンピューティング環境
  - 数分で起動し、1時間ごとの従量課金で利用可能
  - 追加・削除、スペック変更が数分で可能
- 管理者権限(root / Administrator) で利用可能

# 既存のOS/アプリ/ミドルウェアが利用可能

フロントUI



×

開発言語



×

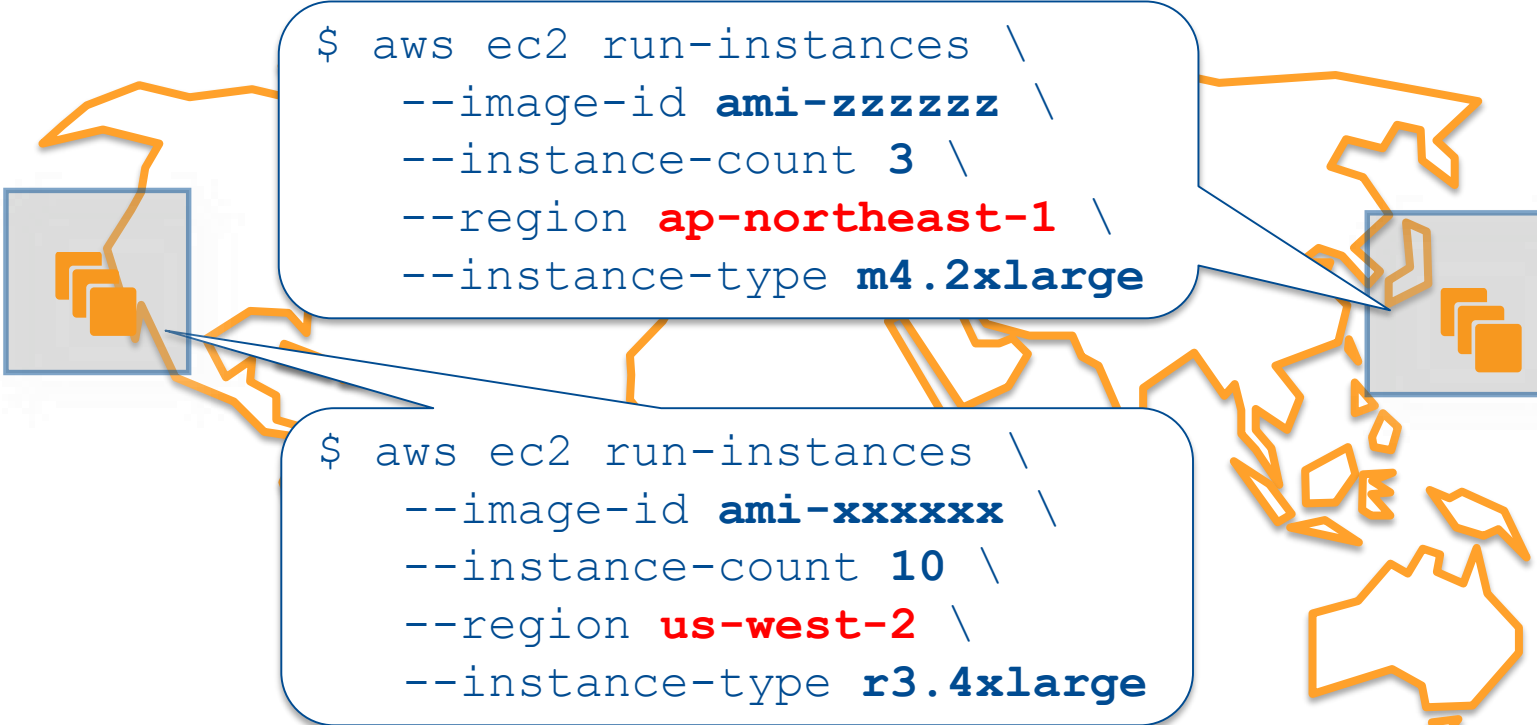
ミドルウェア



OS



# APIでインフラの自動化が可能

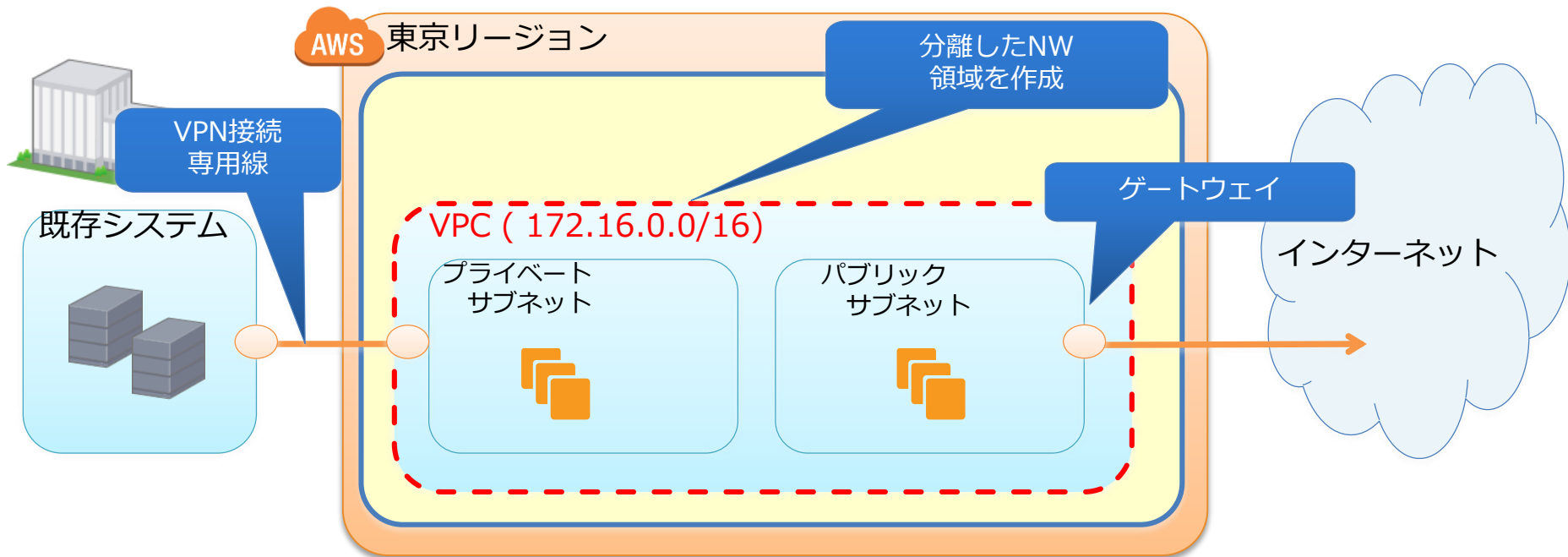


```
$ aws ec2 run-instances \  
  --image-id ami-zzzzzz \  
  --instance-count 3 \  
  --region ap-northeast-1 \  
  --instance-type m4.2xlarge
```

```
$ aws ec2 run-instances \  
  --image-id ami-xxxxxx \  
  --instance-count 10 \  
  --region us-west-2 \  
  --instance-type r3.4xlarge
```

# Amazon VPCによるハイブリッド構成

- クラウド内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**を実現可能



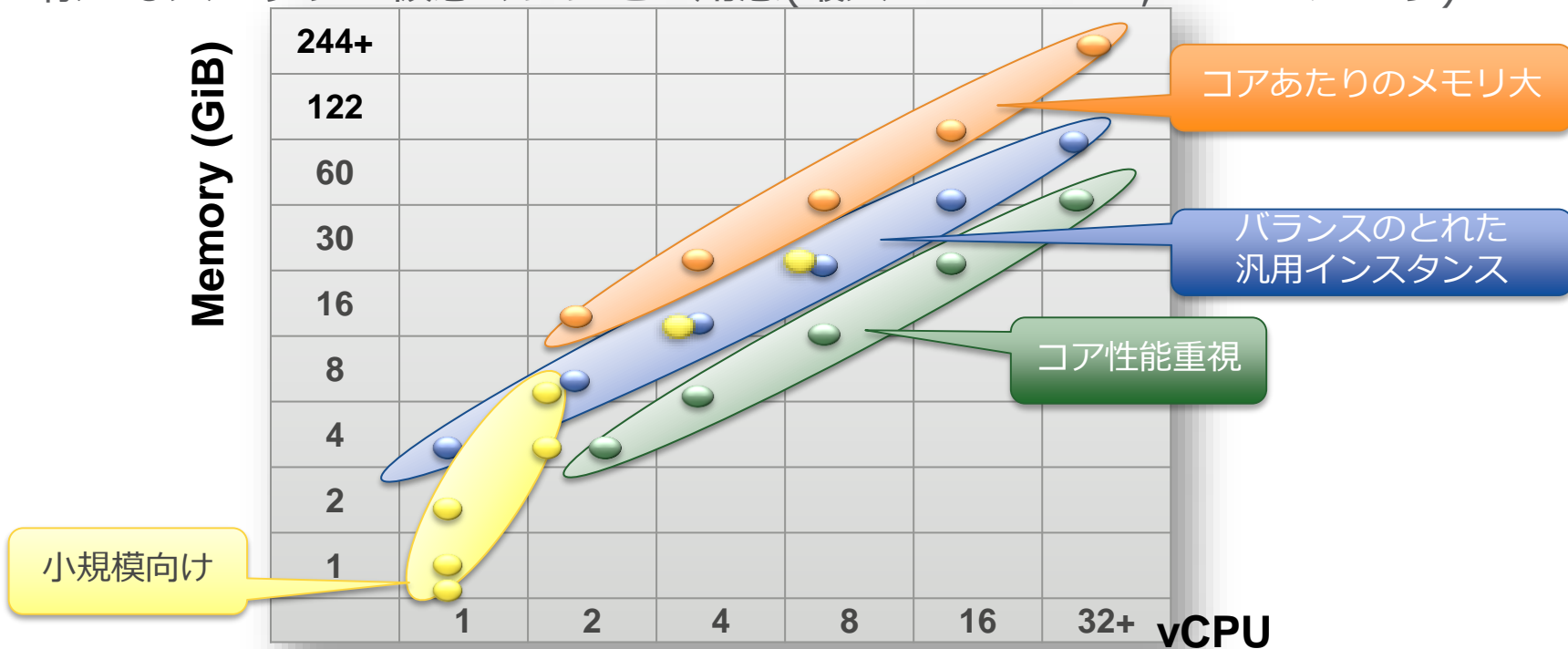
# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A



# EC2インスタンスタイプ

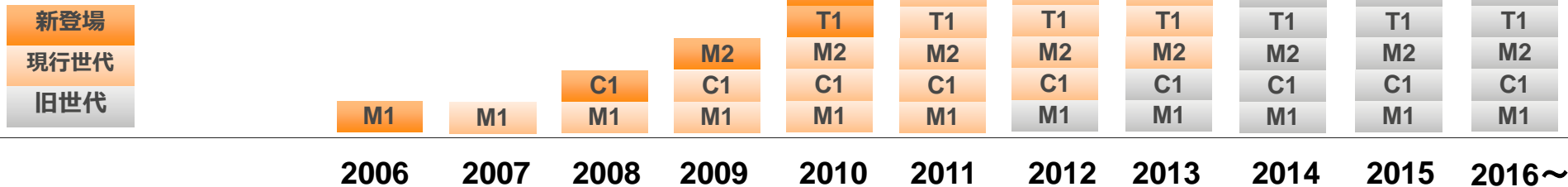
- 様々なスペックの仮想マシンをご用意(最大 128vCPU 1,952GiBメモリ)



# インスタンスタイプの変遷

- AWSを開始した2006年より、様々な用途に応じた インスタンスタイプを随時追加
- インスタンスタイプを切り替えることで、即座に新しいインスタンスを利用可能
- 新しいCPUを搭載した新世代タイプも増加

[http://aws.typepad.com/aws\\_japan/2015/05/ec2-instance-history.html](http://aws.typepad.com/aws_japan/2015/05/ec2-instance-history.html)





# インスタンスファミリー

汎用

コンピューティング最適化

ストレージ・IO最適化

メモリ最適化

GPU/FPGA



T2



M4



M3



C5



C4



C3

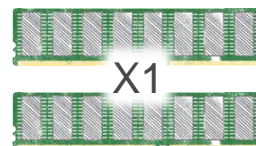


I3

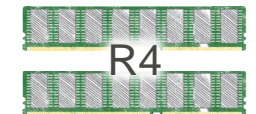
I2



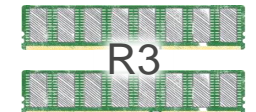
D2



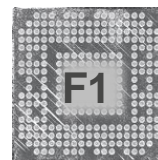
X1



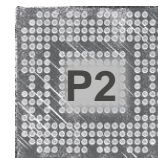
R4



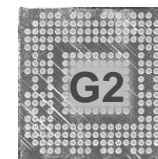
R3



F1

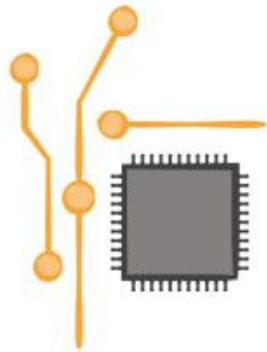


P2



G2

# 常に最新のインテルアーキテクチャを採用



**Intel AES-NI** -パフォーマンスを犠牲にすることなく暗号化が可能

**Intel AVX** -HPC ワークロードの高並列処理で、パフォーマンスが飛躍的に向上

**Intel Turbo Boost Technology** - コンピューティング速度のクロックレートを引き上げ



# インスタンスタイプの整理と選択

インスタンスファミリー



世代



インスタンスサイズ

C 3 . 8xlarge



インスタンス  
ファミリー

世代

サイズ

用途に応じて、インスタンスファミリーと世代を決めた後に、必要なサイズを選択

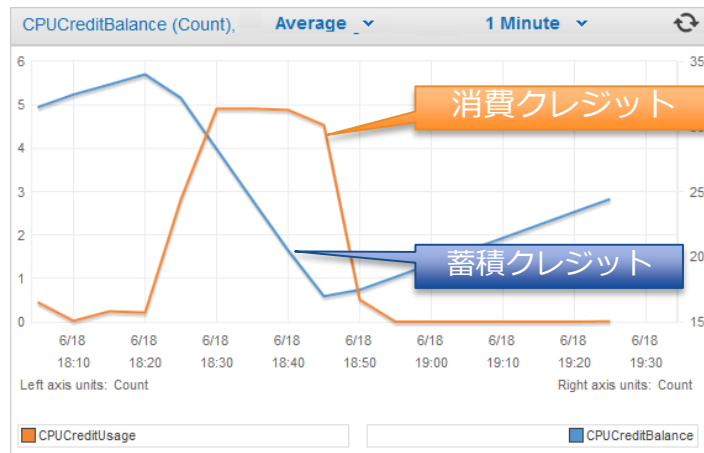
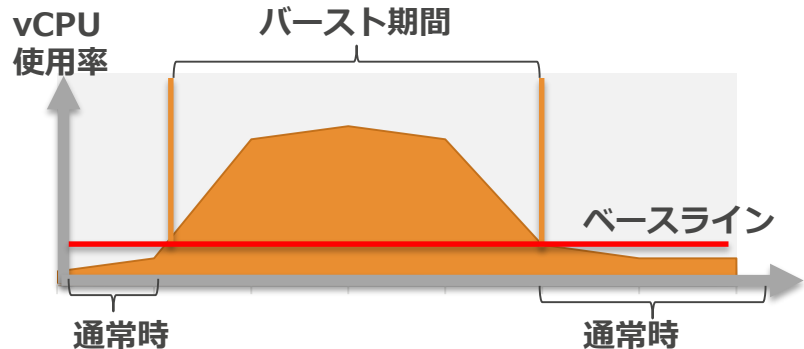
C3インスタンスの例

モデル	vCPU	メモリ (GiB)	SSD ストレージ (GB)
c3.large	2	3.75	2 x 16
c3.xlarge	4	7.5	2 x 40
c3.2xlarge	8	15	2 x 80
c3.4xlarge	16	30	2 x 160
c3.8xlarge	32	60	2 x 320

# T2: バースト可能パフォーマンスインスタンス



- バースト可能とは
  - 通常は低負荷、まれに高負荷になるシステム向け
  - コストパフォーマンスを重視
- 想定用途
  - トラフィックの少ないウェブサイト
  - 開発環境(テスト、ビルドサーバ等)
  - サンプルコードリポジトリ
- CPUクレジットによる性能管理
  - ベースライン性能以下の利用時にクレジット蓄積
  - バースト時に貯めたクレジットを消費する
  - CPUクレジットはCloudWatchで監視可能
    - CPUCreditBalance, CPUCreditUsage



# T2: CPUクレジットの考え方

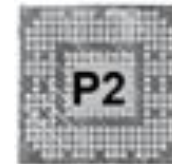
- 1CPUクレジット = 1分間バースト可能
- バースト=ベースライン性能以上のCPU利用率時
- 蓄積したクレジットを使い切ると、ベースライン性能まで低下

Instance type	初期クレジット	クレジット蓄積/時	ベースライン性能	最大蓄積クレジット	vCPU(※)	メモリ
t2.nano	30	3	5%	72	1	0.5GiB
t2.micro	30	6	10%	144	1	1GiB
t2.small	30	12	20%	288	1	2GiB
t2.medium	60	24	40%	576	2	4GiB
t2.large	60	36	60%	864	2	8GiB
t2.xlarge	120	54	90%	1296	4	16GiB
t2.2xlarge	240	81	135%	1944	8	32GiB

New  
New

※2.5GHz(ターボ最大3.3GHz)のXeonプロセッサ

# P2 インスタンス



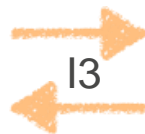
## 高性能GPUインスタンスタイプ

- NVIDIA K80を最大16GPU搭載
- 最大64 vCPUのIntel Broadwell プロセッサと、最大 732GiB RAM
- Elastic Network Adaptor (ENA)による20Gbps ネットワーク
- 多くのISVやOSSに対応

Instance Size	GPUs	GPU Peer to Peer	vCPUs	Memory (GiB)	Network Bandwidth*
p2.xlarge	1	-	4	61	1.25Gbps
p2.8xlarge	8	Y	32	488	10Gbps
p2.16xlarge	16	Y	64	732	20Gbps

\*In a placement group

# I3 インスタンス



- 最新世代のストレージ最適化ハイ I/O インスタンス
  - Non-Volatile Memory Express (NVMe) ベースの SSD を利用可能
  - Elastic Network Adaptor (ENA)により最大20Gbps
  - 負荷の高いリレーショナルデータベースや、NoSQLデータベースに最適

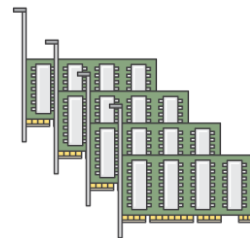
Instance Size	vCPU	Memory (GiB)	Storage	Read IOPS	Write IOPS
i3.large	2	15.25	1 x 475 NVMe SSD	100,125	9,375
i3.xlarge	4	30.5	1 x 950 NVMe SSD	206,250	18,750
i3.2xlarge	8	61	1 x 1,900 NVMe SSD	412,500	37,500
i3.4xlarge	16	122	2 x 1,900 NVMe SSD	825,000	75,000
i3.8xlarge	32	244	4 x 1,900 NVMe SSD	1,650,000	150,000
i3.16xlarge	64	488	8 x 1,900 NVMe SSD	3,300,000	300,000

<https://aws.amazon.com/jp/about-aws/whats-new/2017/02/now-available-amazon-ec2-i3-instances-next-generation-storage-optimized-high-i-o-instances/>

# Amazon EC2 Instance 最新情報

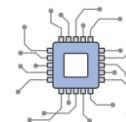
## Preview

- F1: FPGA搭載し高性能計算用途に最適なインスタンス
  - Intel Xeon E5-2686v4(2.3GHz, Turbo mode対応)
  - 最大8個のFPGA(Xilinx UltraScale+ VU9P)
  - FPGA Developer AMIを提供。FPGA向けアプリケーションはVHDLまたはVerilogを利用して開発する
  - バージニアリージョンにてデベロッパープレビューを実施中。



## Announced

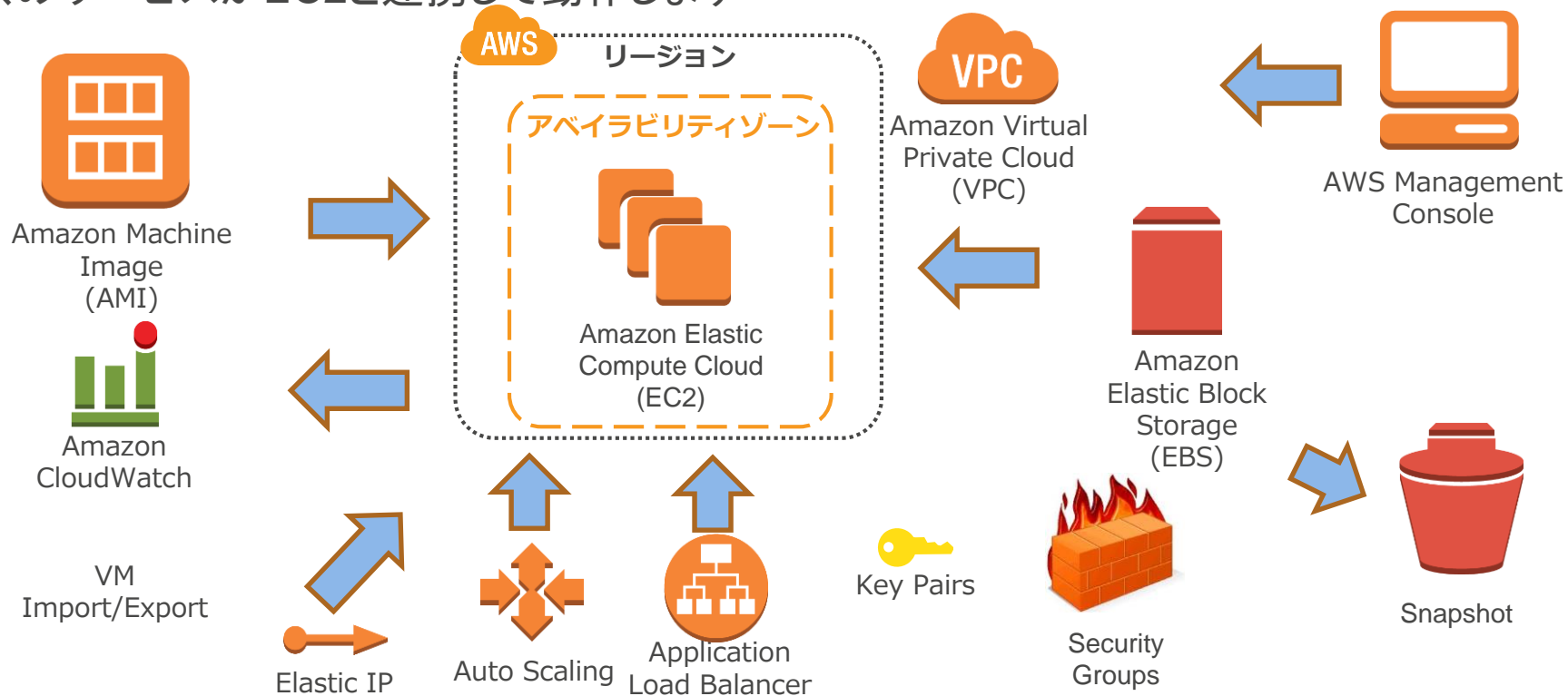
- C5: C4インスタンスの後継インスタンスファミリー
  - Intel Xeon Skylakeを搭載予定
  - 最大72vCPU, 144GiB搭載予定
  - 機械学習、マルチメディア処理、科学計算、金融業務などに最適
  - 2017年リリース予定





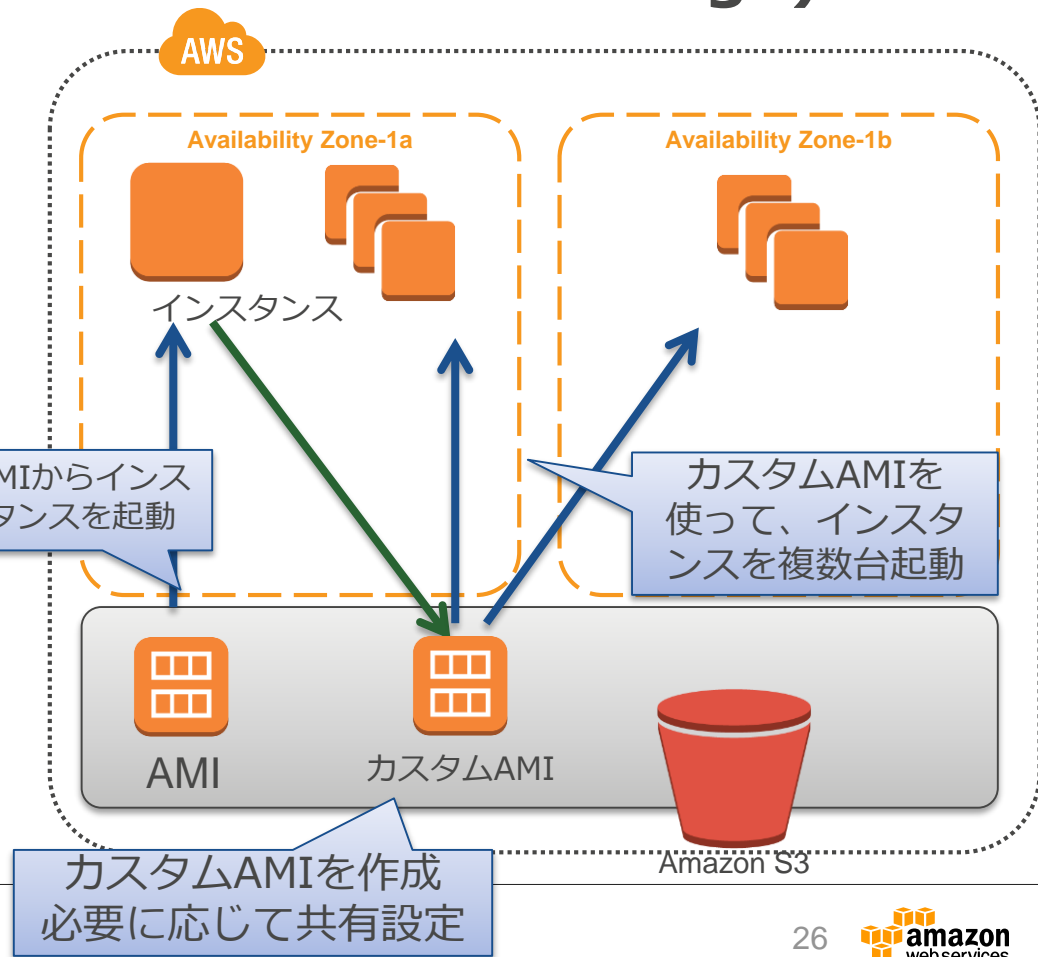
# EC2に関連する主要コンポーネント

多くのサービスがEC2と連携して動作します



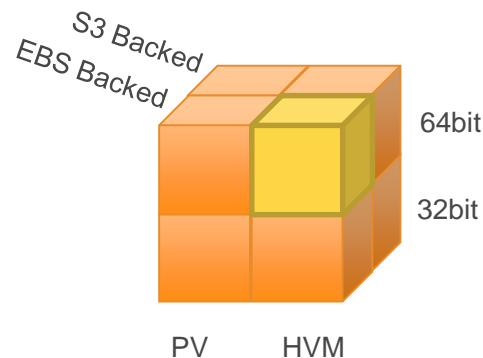
# インスタンスとAMI (Amazon Machine Image)

- AMIはインスタンス起動に必要なOSイメージ
  - イメージはS3に保存
- AWS以外にサードパーティもAMIを提供
- 自由に自前のカスタムAMIを作成可能
  - 作成したAMIは別アカウントと共有可能
  - カスタムAMIから何台でもEC2インスタンスを起動可能
  - 別リージョンへのコピーも可能



# AMIの分類

- ビット数
  - 32bit と64bit
- 仮想化方式
  - 準仮想化 ( Paravirtual, PV)
  - 完全仮想化 (Hardware-assisted VM, HVM)
- ブートストレージ
  - EBS Backed
  - Instance Store-Backed (S3 Backed)



同じOSでも、上記種類で複数のパターンが存在  
一般的な推奨は 64bit HVM EBS-Backed

例: Amazon Linux <http://aws.amazon.com/jp/amazon-linux-ami/instance-type-matrix/>

# AMIと仮想化方式

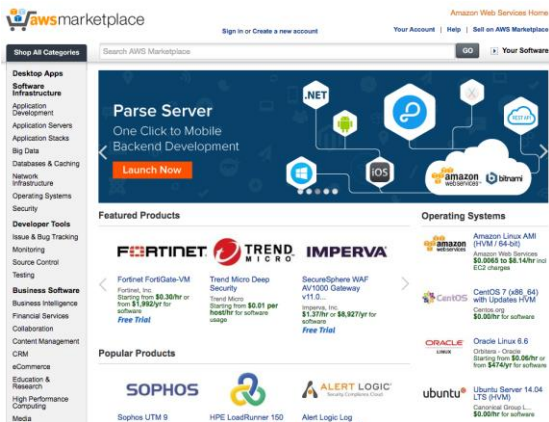
- 仮想化方式
  - 準仮想化 ( Paravirtual, PV)
  - 完全仮想化 (Hardware-assisted VM, HVM)
- 一般的に
  - EC2開始当時はLinux PV AMIのみ (Windows AMIは全てHVM)
  - LinuxでもHVM AMIで性能向上が見込める場合が多い
  - 現行世代のインスタンスファミリーは、全てHVM AMIが動作可能
    - HVMしかサポートしないインスタンスファミリーも
- Tips
  - VM Import/Exportは HVMのみ対応
  - 一部のCPU拡張命令(AVX等)はHVMのみ対応
  - PV・HVM間の変換機能は提供していない

# AMIを探す

- コミュニティAMI
  - コンソールでEC2起動時に検索
  - CLI/APIで `describe-images` を利用
- AWS Marketplace
  - AWS上で実行されるソフトウェアやサービスを見つけて購入しすぐに使用開始できるオンラインソフトウェアストア
  - 多くのソフトウェアベンダー製品やOSSのソフトウェアがインストール済みOSイメージを公開中
  - 有償ソフトウェアを従量課金で利用可能

## ステップ 1: Amazon マシンイメージ (AMI)

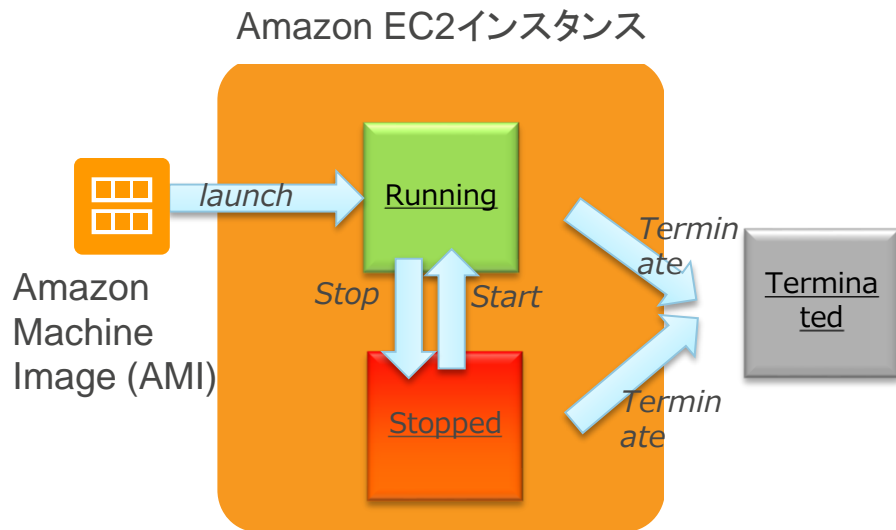
AMIは、インスタンスの作成に必要なソフトウェア構成 (OS、アプリケーションサーバー、アプリケーション) を含むテンプレートです。AMIは、AWS が別の、または AWS Marketplace に掲載されているものを選択できます。独自の AMI のいずれかを選択することもできます。



# インスタンスのライフサイクル

起動したインスタンスは状態を持つ

- Running
  - 実行中。課金される
  - Stop操作でStoppedへ、Terminate操作でTerminatedに遷移
- Stopped
  - 停止中。課金されない
  - Start操作で再度Running状態に遷移
- Terminated
  - 終了済み。Stop/Startはできない



EBS-Backed AMIは Stopped状態の遷移が可能  
S3-Backedは Stop不可

# 物理ホストの専有

- 2つの方法
  - ハードウェア専有インスタンス (Dedicated Instance) (2011/3～)
  - Amazon EC2 Dedicated Host (2015/11～)
- 共通の機能
  - お客様専用の物理サーバにインスタンスを起動可能
    - 別のお客様のインスタンスは起動しない
  - コンプライアンスやライセンス対応で、物理サーバ専有が必要なお客様向け
  - クラウドのメリットはそのまま確保
    - オンデマンドとリザーブドの課金体系
    - 瞬時に調達
- Dedicated Hostsの特徴
  - 物理ホストへのインスタンス配置が、制御・確認可能
  - 物理ホスト単位のソフトウェアライセンスを持ち込み(BYOL)可能
  - 物理ホスト単位での課金
  - AWS が提供、または AWS Marketplace で提供される RHEL、SUSE Linux、および Windows AMI を専有ホストで使用することは出来ないので注意すること

# ハードウェア専有インスタンスとDedicated Hostsの比較

特徴	ハードウェア専有インスタンス	Dedicated Hosts
物理サーバを専有する	○	○
インスタンスあたりの課金	○	
ホストあたりの課金		○
ソケット、コア、ホストIDの可視性		○
ホストとインスタンス間のアフィニティ		○
対象インスタンスの配置		○
自動インスタンスの配置	○	○
割りリクエストでのキャパシティ追加		○

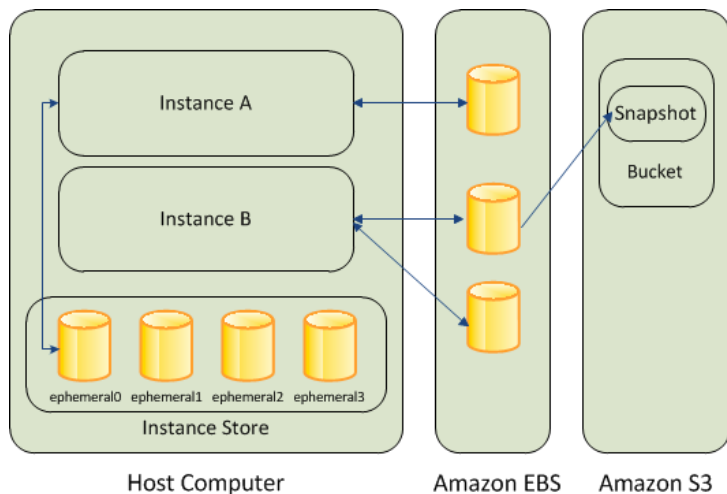


# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A



# EC2のストレージ



## Amazon EC2 インスタンスストア

- ホストコンピュータに内蔵されたディスク
- EC2と不可分
- EC2をStop/Terminateするとクリアされる
- 性能・容量はインスタンスタイプごとに規定
- 追加費用なし(無料)

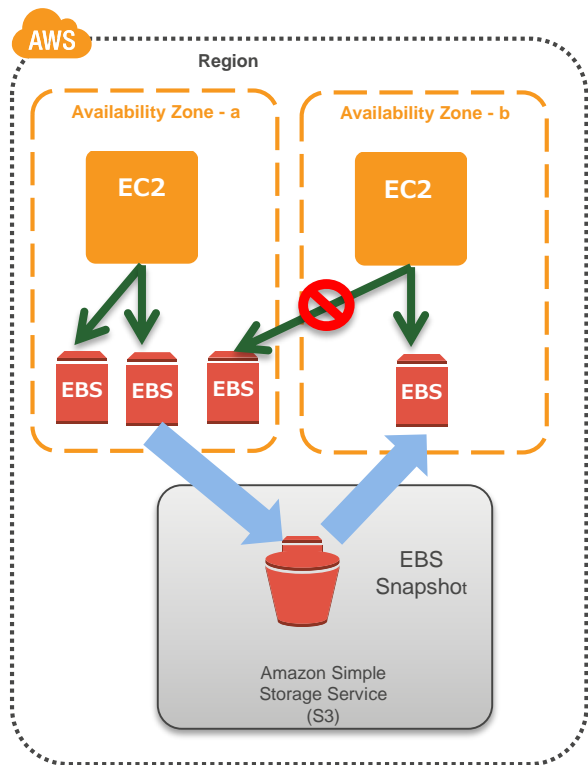
## Amazon Elastic Block Store (EBS)

- ネットワークで接続
- EC2とは独立管理
- EC2をTerminateしてもEBSは保持可能
- Volumeごとに性能・容量を定義可能
- EBSの費用が別途発生
- Snapshotを取得しS3に保存可能

# インスタンスストア

- ブロックレベルの一時ストレージ
  - 頻繁に更新される情報(バッファ、キャッシュ)やインスタンスのフリート全体でレプリケートされるデータの保存に最適
- インスタンスタイプごとに仕様が決められている
  - サイズの変更はできない
  - 搭載していないインスタンスタイプも。(T2,M4,C4,R4,P2)
- 高速I/O用途
  - I3インスタンスはSSDストレージを搭載し、低コストで高いランダムI/O (IOPS)に最適化し、TRIMもサポート
  - 最大 8 x 1,900 GB のNVMe SSDを搭載( i3.16xlarge)
- 大容量
  - D2インスタンスはストレージ密度が極めて高く、インスタンスあたりのシーケンシャルRead/Write性能が高い
  - 最大2TB x 24 のHDDを搭載( d2.8xlarge)

# Amazon Elastic Block Storeについて



EC2にアタッチされる  
ブロックレベルのストレージサービス

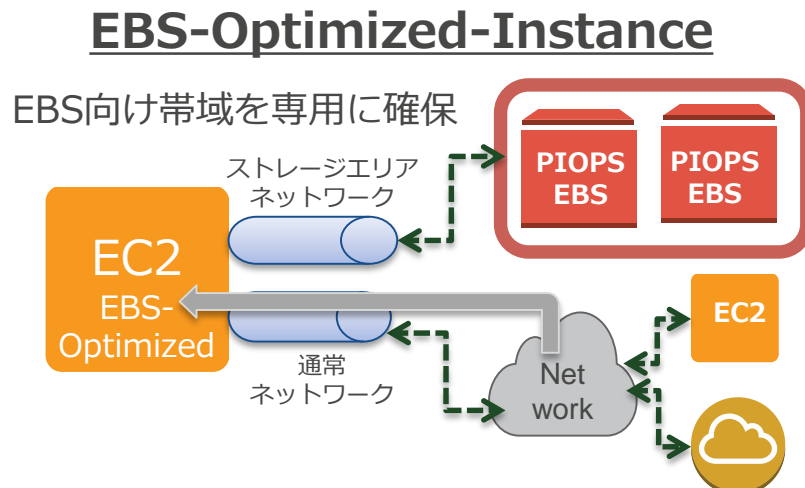
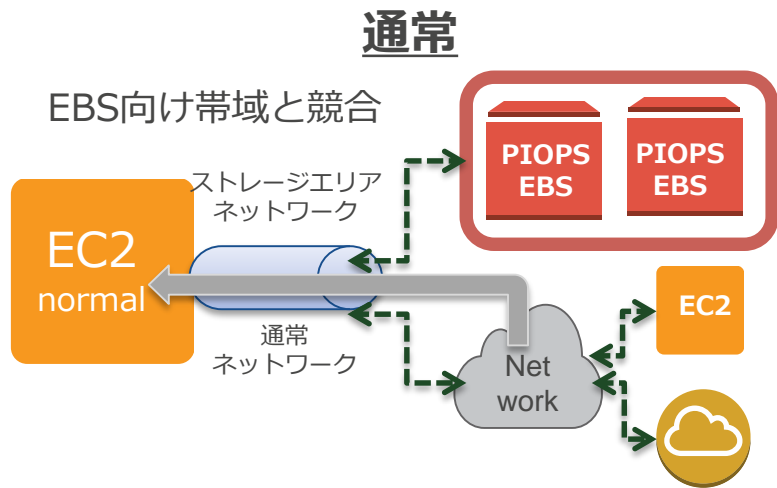
- サイズは1GB単位で1GB～16TBまで
- サイズ/期間で課金される(MagneticはIO課金あり)

## 特徴

- EC2インスタンスから独立している  
(他のEC2インスタンスに付け替え可能)
- データは永続的に保存される
- 任意のアベイラビリティゾーン(AZ)に作成可能
- Snapshotバックアップから、EBSボリュームを作成可能  
(他のAZに作成できる)

# EBS最適化インスタンス

- 通常のネットワークとは別にEBS専用帯域を確保するオプション
  - 起動時に有効/無効を選択可能
  - インスタンスサイズによって帯域が異なる
  - インスタンスタイプによってはデフォルトで有効(C4,M4,D2,I3,P2,R4,X1)



# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A



# AWSのセキュリティの考え方「責任共有モデル」

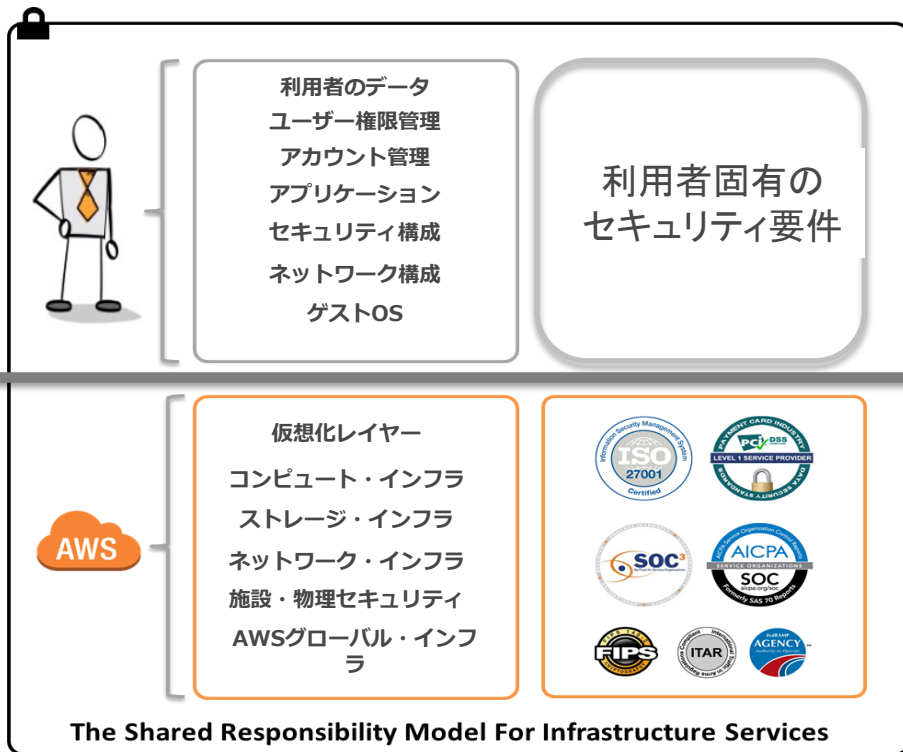
**利用者の統制**  
ユーザが責任をもって管理する



**共有の責任**

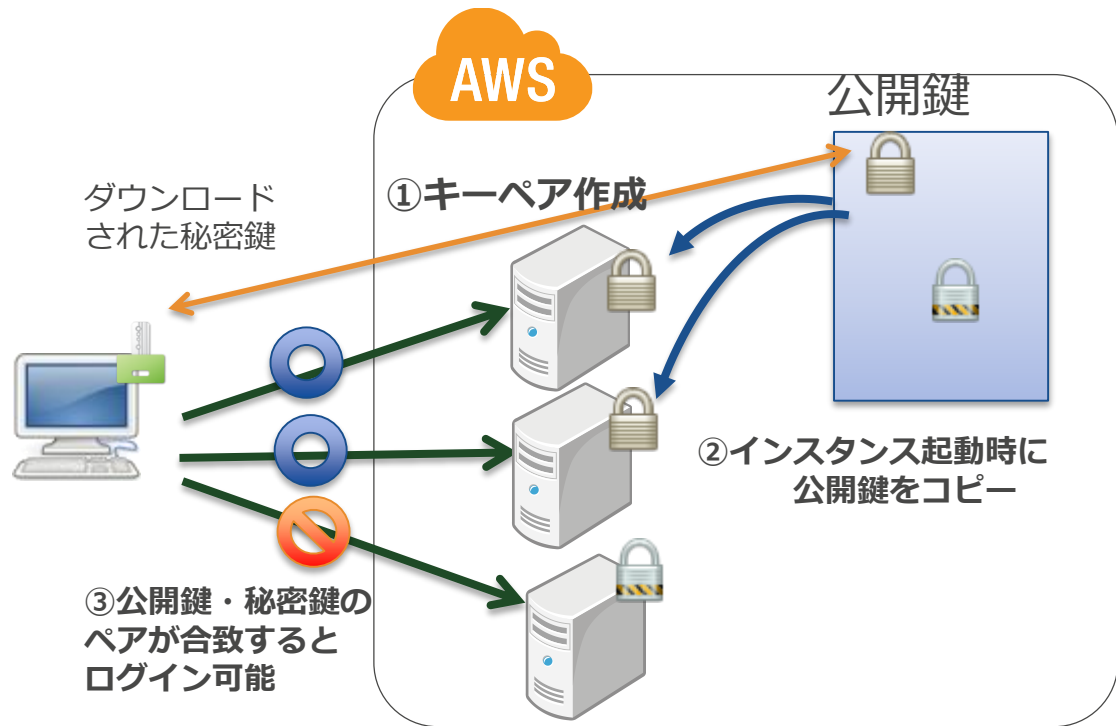


**AWSの統制**  
AWSが責任をもって管理する



# Key Pairとは

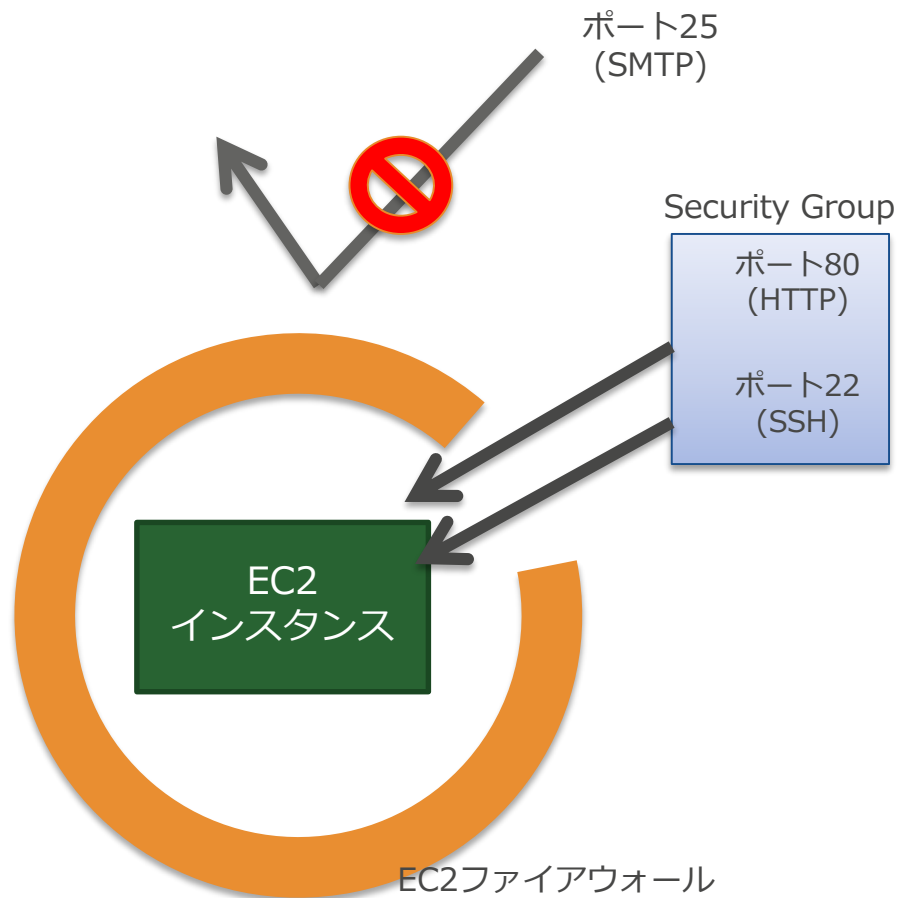
- 鍵認証は、ユーザ名・パスワードの認証よりも安全な認証方式
- AWSでは公開鍵のみ保持し、起動時に公開鍵をコピーする
- 秘密鍵は、ユーザにて適切に管理・保管する



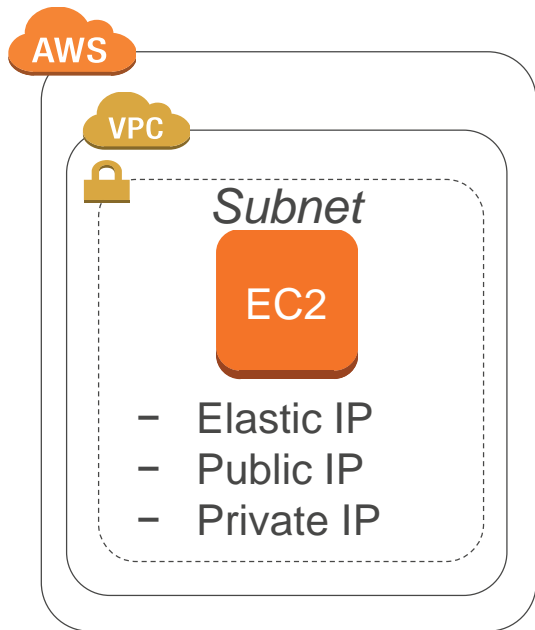


# Security Groupとは

- インスタンスへのトラフィックを制限する**ファイアウォール機能**
- デフォルトで全トラフィック閉
- 必要な受信アクセスに対してアクセスルールを定義する
  - プロトコル( TCP/UDP)
  - 宛先ポート
  - アクセス元IP / Security Group
- ルールをひとまとめにしたテンプレートをSecurity Groupと呼ぶ



# AWS上でのIPの種類



- Elastic IP (EIP)
  - 明示的にIPを割り当てる
  - Stop/Startしてもアサインされたまま(VPCのみ)
  - 利用していない場合は課金発生
- Public IP
  - ランダムに割り当てられるPublic IP
  - Stop/Startすると別のIPが割り当てられる
  - 割当ての有無を変更することも可能(VPCのみ)
- Private IP
  - 必ず割り当てられるIPアドレス。
  - EC2作成時にIPを指定可能(VPCのみ)
  - Stop/StartしてもIPは変わらず固定(VPCのみ)

# EC2のPublic IPレンジ

- EC2(を含むAWS)が利用するIPアドレスレンジを公開
  - JSONフォーマットで公開
    - [http://docs.aws.amazon.com/ja\\_jp/general/latest/gr/aws-ip-ranges.html](http://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-ip-ranges.html)
  - 変更時にSNSで通知
    - 指定されたトピックをサブスクライブすることで受信可能

```
javascript
1  {
2    "syncToken": "1416523628",
3    "createDate": "2014-11-20-22-51-01",
4    "prefixes": [
5      {
6        "ip_prefix": "50.19.0.0/16",
7        "region": "us-east-1",
8        "service": "AMAZON"
9      },
10     {
11       "ip_prefix": "54.239.98.0/24",
12       "region": "us-east-1",
13       "service": "AMAZON"
14     },
```

arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged

# EIPの利用

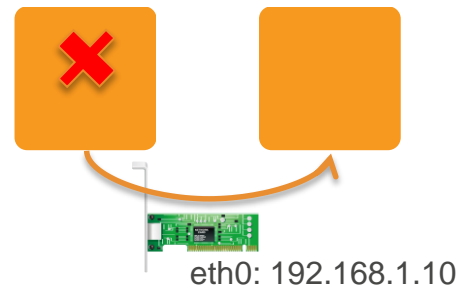
- 固定IPアドレスが必要な時にEIPを使う
  - 通常のケース(内部から外部へのアクセス)では Public IPで十分
- 固定IPが必要なケース
  - メールサーバ、監視サーバ等
  - 外部システムとの通信でアクセス元IPを固定する必要がある場合
- 注意点
  - EIPをインスタンスにアタッチしていない場合は利用料金が発生

# Elastic Network Interfaces (ENI)

- VPC上で実現する仮想ネットワークインタフェース
- 以下をENIに紐づけて維持可能
  - Private IP
  - Elastic IP
  - MACアドレス
  - セキュリティグループ
- インスタンスによって割り当て可能な数が異なる。

利用例1:

インスタンス障害時に待機インスタンスにNICを付け替え



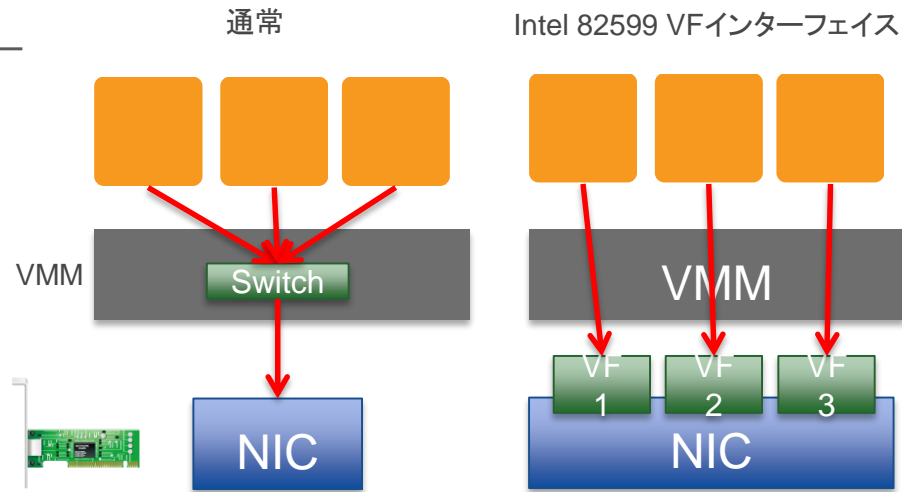
利用例2:

1インスタンスに複数NIC



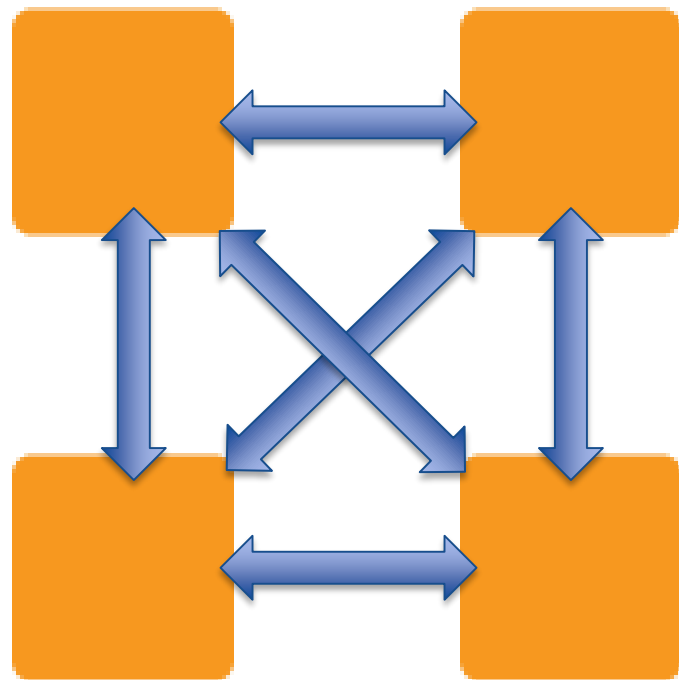
# 拡張ネットワーキング (Enhanced Networking)

- 拡張ネットワーキング
  - パケット毎秒(PPS)が非常に大きく、ネットワークレイテンシが低くなるオプション。
  - SR-IOVに対応
- ネットワーキングのタイプ
  - Intel 82599 VFインターフェイス
    - M4(m4.16xlarge以外), C3, C4, R3, I2, D2
  - New* - Elastic Network Adapter(ENA)
    - I3,P2,R4,X1,およびm4.16xlarge
    - 最大20Gbps
- 適応条件
  - VPC内でHVM AMIで起動
  - 対応ドライバがインストールされていること。
  - ENAはLinux kernel 3.2以降が必要



# Placement Groups

- インスタンス間通信を最適化
  - 広帯域 (最大20Gbps Full Bisection)
  - 低レイテンシ
  - 高PPS (packets per seconds)
- 用途
  - HPC、Hadoop、MPP、DWHなど、ノード間通信が大量に発生するクラスタに最適
  - 拡張ネットワーキングとの併用を推奨
- 制限
  - 単一アベイラビリティゾーンに閉じる
  - 利用可能なインスタンスタイプに制限あり。



Full bisection bandwidth

# 各種申請

- ペネトレーションテスト
  - 適正利用規約により、侵入テストやリソースのスキャンは禁止されてる
  - AWS 脆弱性/侵入テストリクエストフォームでテスト内容の申請が必要
    - <http://aws.amazon.com/jp/security/penetration-testing/>
- SMTP送信
  - EC2からSMTP送信するトラフィックは制限されている
  - 申請フォームによる申請が必要。
    - <http://www.slideshare.net/AmazonWebServicesJapan/aws-42885668>



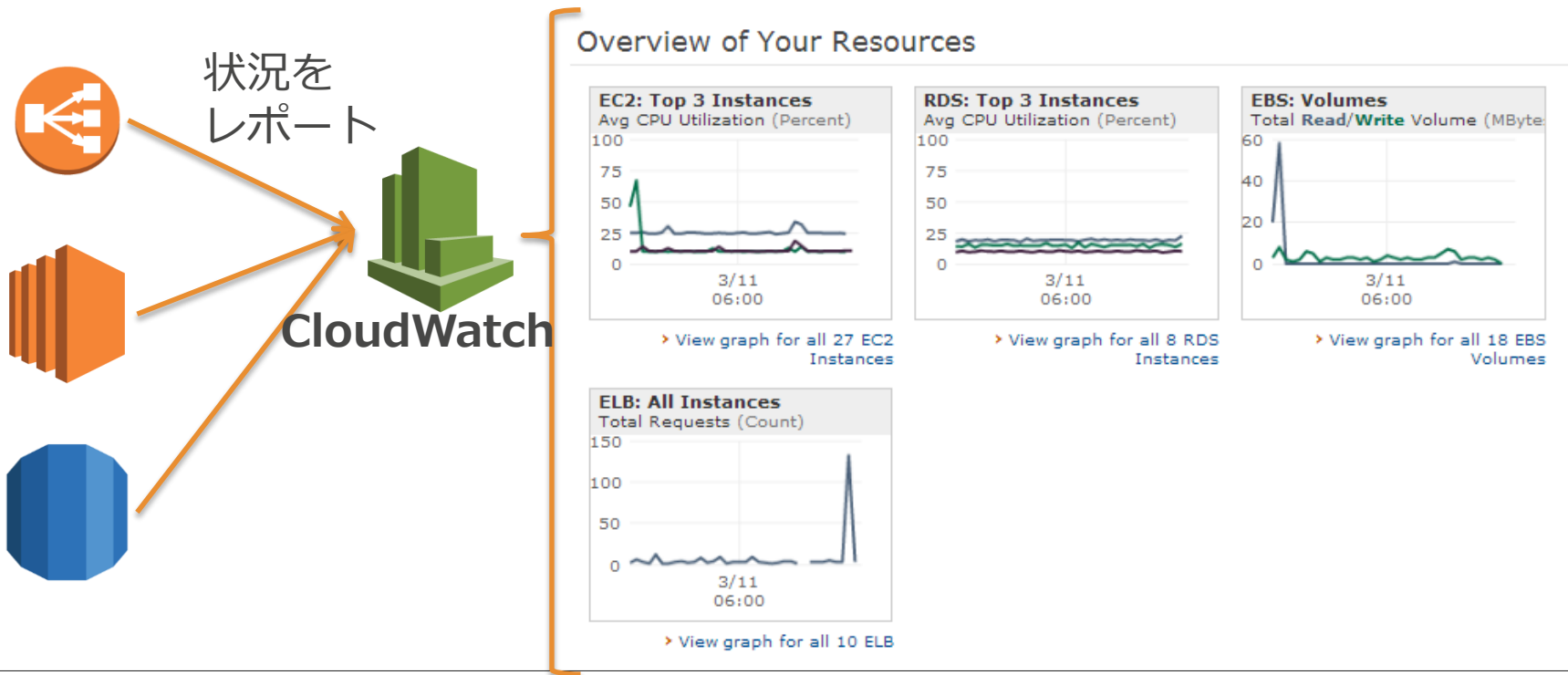
# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- 料金
- Q&A



# Amazon CloudWatchとは？

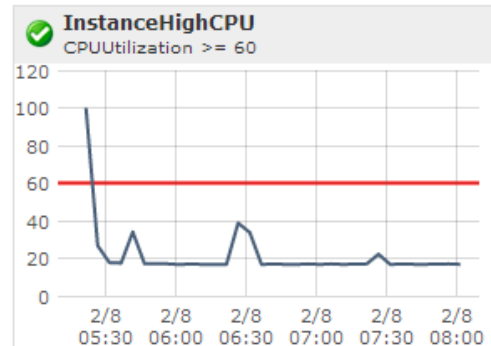
AWSの各種リソースをモニタリングするためのWebサービス



# CloudWatchができること

- 各AWSサービスのメトリックス監視

- メトリックス = 監視項目 (例: CPU使用率)
- メトリックスはあらかじめ定義され、構成済み
  - サービス開始時から監視開始
  - EC2ではハイパーバイザーから監視できる項目
- メトリックスを追加定義も可能
  - カスタムメトリックス
- メトリックス値を時系列にグラフ表示



- 各メトリックスに対して**アラーム**を作成可能

- しきい値を設定 (例: CPU使用率60%以上)
- メトリックス値がしきい値を越えたら起こすアクションを定義 (例: メールで通知)

- EC2上の**ログ監視** . . . Amazon CloudWatch Logs

- メトリックスとアラームも作成可能

# スケジュールイベント

- リタイヤ
  - インスタンスをホストしているハードウェアで回復不可能な障害が検出された場合、インスタンスリタイヤが予定される
  - スケジュールされたインスタンスには、時計マークが表示される
  - EC2のEventsメニューで一覧表示
  - DescribeInstanceStatus APIで取得可能
- 対策
  - リタイア日までにstop→start を実行

## Scheduled Events

US East (N. Virginia):

1 instances have scheduled events

The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, and a red arrow points to the 'Events' menu item under the 'EC2 Dashboard' section. The main content area displays the 'Scheduled Events' page for a specific instance. The page includes a table with the following columns: Resource Name, Resource Type, Resource ID, Availability Zone, Event Type, Event Status, and Event Description. The table contains one row of data for a scheduled event. Below the table, there is a section for 'Event:' with details for the selected event.

Resource Name	Resource Type	Resource ID	Availability Zone	Event Type	Event Status	Event Description
Precise	Instance	us-east-1a	us-east-1a	system-reboot	Scheduled	Scheduled reboot

Event: ...

Availability Zone: us-east-1a  
Event type: system-reboot  
Event status: Scheduled  
Description: Scheduled reboot  
Start time: September 28, 2014 8:00:00 AM UTC+2  
End time: September 28, 2014 2:00:00 PM UTC+2

*Find out more about instances scheduled for reboot.*

# Auto recovery

- インスタンスの異常を検知し復旧

- インスタンスの異常を2つに分けて検知
  - StatusCheckFailed\_System : インスタンスをホストしているハードウェア側の障害
  - StatusCheckFailed\_Instance : EC2インスタンス内部で障害が発生している場合
- CloudWatch アラームにて 「Recover this Instance」 アクションを設定
- アラーム発生時に、自動的にインスタンス再起動を行う。インスタンスID、IPアドレスなどは維持される

- 条件

- 特定のインスタンスタイプのみ対応(C3,C4,M3,M4,R3,R4,T2,X1)
- VPC内のEBS-Backed インスタンスのみ対応

Availability Zone	Instance State	Status Checks	Alarm Status
theast-1b	● running	✓ 2/2 checks passed	✓ OK
theast-1b	● running	✓ 2/2 checks passed	None

# EC2のSLA

- EC2の可用性は99.95%
- 上記に満たない場合はServiceクレジットを返還する
- 詳細は
  - <http://aws.amazon.com/ec2-sla/>

# 自動化ツールと機能

インフラを自動化・プログラム化することが可能

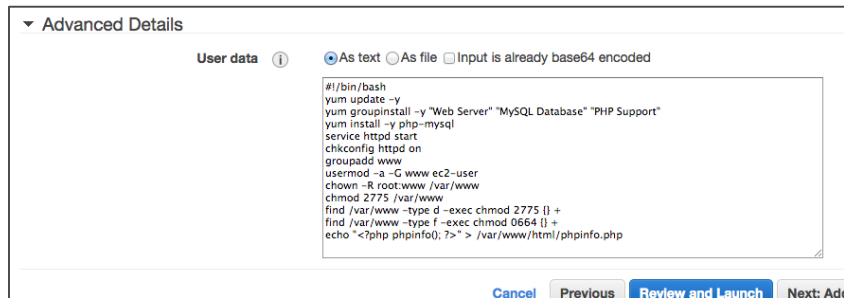
- User-Data
- Instance Meta Data
- AWS CLI
- AWS SDK
- Amazon EC2 Systems Manager
- AWS CloudFormation
- AWS Elastic Beanstalk
- AWS OpsWorks
- その他サードパーティ製品



各BlackBeltの資料を参照ください

# ユーザーデータ

- 起動時にスクリプト実行を行う機能
- 2種類の形式でインスタンスに渡す
  - シェルスクリプト
  - Cloud-initディレクティブ
- 利用用途
  - AMIでカバーできない起動時の設定変更
  - 起動時に実行するスクリプトやchef, puppetへ、外部からパラメータとして値を渡す
- 応用
  - 複数台の自動構成などは CloudFormation, OpsWorksも組み合わせて利用する



```
#!/bin/bash
yum update -y
yum groupinstall -y "Web Server" "MySQL Database" "PHP Support"
yum install -y php-mysql
service httpd start
chkconfig httpd on
groupadd www
usermod -a -G www ec2-user
chown -R root:www /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} +
find /var/www -type f -exec chmod 0664 {} +
echo "<?php phpinfo();?>" > /var/www/html/phpinfo.php
```



# インスタンスメタデータ

- 自インスタンスに関するデータを取得するための方法
- User-dataも取得可能
- 利用例
  - インスタンスタイプに応じて、設定ファイルのメモリ量などを調整
  - リージョンに応じて、タイムゾーンを自動設定
  - ネットワーク情報を取得して、DNSへ動的登録

```
curl http://169.254.169.254/latest/meta-data
```

ami-id	local-hostname
ami-launch-index	local-ipv4
ami-manifest-path	mac
block-device-mapping/ hostname	network/ placement/ profile
instance-action	public-hostname
instance-id	public-ipv4
Instance-type	public-keys/ reservation-id
kernel-id	

# 上限と制限緩和

- EC2は、誤って大量に起動しないよう、アカウント開設当初はリージョンごとに20インスタンスまでしか起動できないように設定されている
  - [http://docs.aws.amazon.com/ja\\_jp/general/latest/gr/aws\\_service\\_limits.html](http://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_service_limits.html)
- 各種上限は Trusted Advisorで確認可能(Service Limits)
  - EC2管理画面の「Limits」メニューでも確認可能
- 上限緩和申請はAWSサイト最下のメニューから
  - EC2管理画面の「Limits」メニューからも申請可能

The screenshot shows the AWS Management Console navigation menu on the left with '制限' (Limits) highlighted in a red box. The main content area is titled 'EC2 サービスの制限' (EC2 Service Limits) and contains the text: 'Amazon EC2 には、利用可能なさまざまなごとにこれらのリソースに対して制限が設けられています。' (Amazon EC2 has limits for these resources for various types of usage that you can use.) Below this is a section for 'インスタンスの制限' (Instance Limits) with a table header '名前' (Name). At the bottom of the console, there are four columns of links: '知識' (Knowledge), '開発者用リソース' (Developer Resources), 'アカウントの管理' (Account Management), and 'AWS について' (About AWS). The 'アカウントの管理' column has '各サービスの上限緩和申請' (Request to increase service limits) highlighted in a red box. The footer contains social media icons and a promotional banner for 'AWSキャリア採用イベント開催' (AWS Career Event).

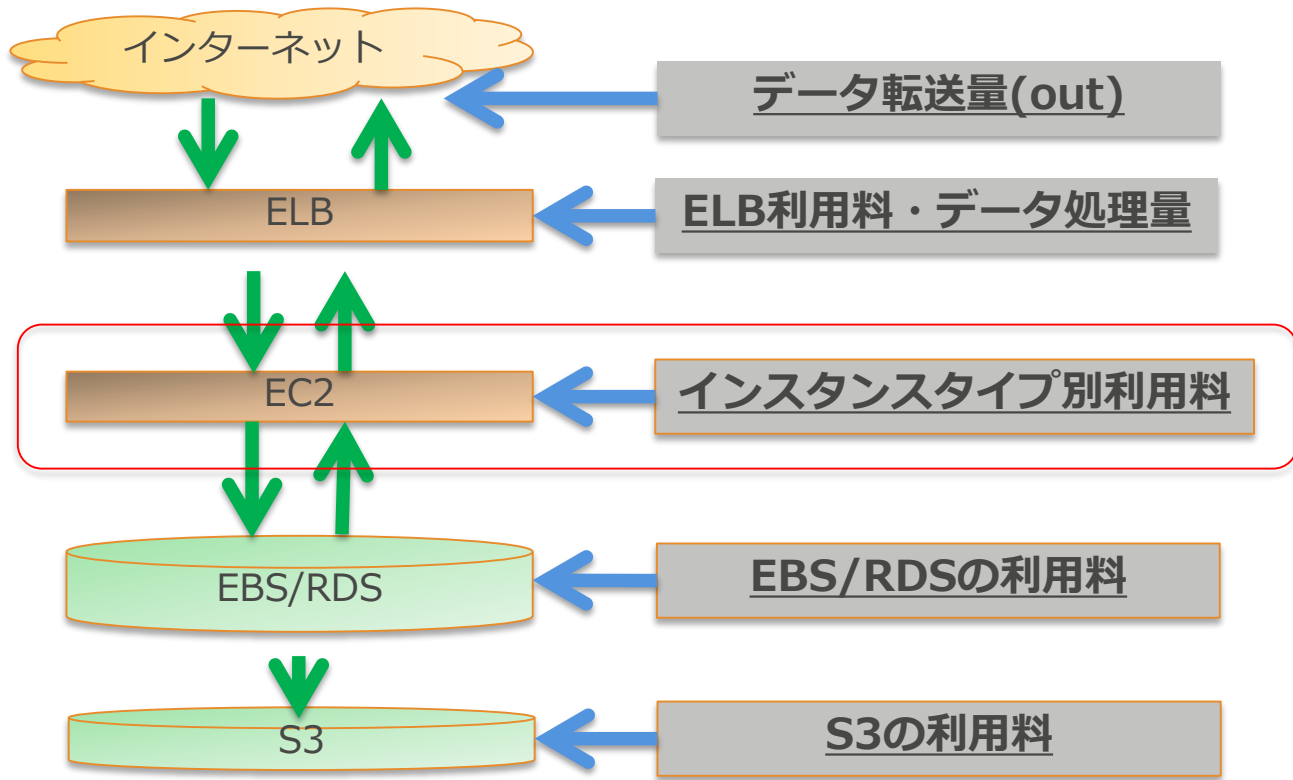
# Agenda

- EC2の基本
- インスタンスタイプ
- ストレージ
- ネットワーク・セキュリティ
- 運用・監視
- **料金**
- Q&A



# 一般的な構成の課金の内訳

EC2の費用が大半を占める！



# EC2の購入オプション

- オンデマンドインスタンス
  - 初期費用無し、従量課金
- リザーブドインスタンス
  - 1年間または3年間、常に利用可能なキャパシティ予約により、最大75%の割引
  - スケジュールされたリザーブドインスタンス
    - 1年間、日次・週次・月次で、指定した時間帯のみのキャパシティ予約により、5%-10%の割引
- スポットインスタンス
  - 未使用キャパシティに入札し、スポット価格よりも高い限り、大幅な割引で利用可能
  - 複数の入札方法を用意
- 専用ホスト(Dedicated Hosts)
  - インスタンス実行用物理ホストの単位で支払い。
- ハードウェア専用インスタンス( Dedicated Instance)
  - シングルテナント

# それぞれの想定ご利用シーン

## オンデマンド インスタンス (デフォルト)

- ・ピーク対応で増減するサーバ
- ・一時利用のキャンペーンサイト
- ・昼にしか使わない開発サーバ



## リザーブド インスタンス (オプション)

- ・常時稼働しているサーバ
  - DB, キャッシュサーバ
  - (最低限必要の) Web/Appサーバ



## スポット インスタンス (オプション)

- ・分散処理のタスクノード
- ・クローラ
- ・メディアプロセッシング等



# OS・ソフトウェアの料金

- 無料OS AMI
  - インスタンス費用のみ
    - Amazon Linux, CentOS, FreeBSD, Ubuntu, etc.
- 商用OS AMI
  - 従量課金: インスタンス費用+ソフトウェア費用(\$/h)
    - Windows Server (Windows + SQLServer)
    - Red Hat Enterprise Linux
    - SuSE Linux Enterprise
  - 構成によってはライセンス持ち込みも可能
- AWS Marketplace
  - 完全従量課金: インスタンス費用(\$/h)+ソフトウェア費用(\$/h)
  - ソフトウェアライセンス持ち込み(BYOL): インスタンス費用(\$/h)

# 課金管理の方法

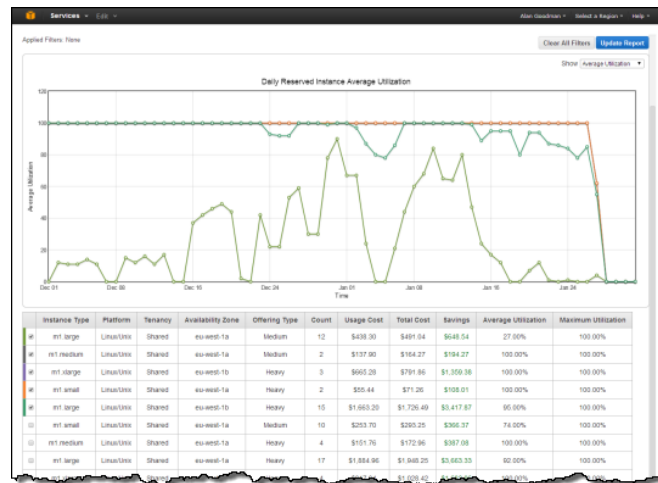
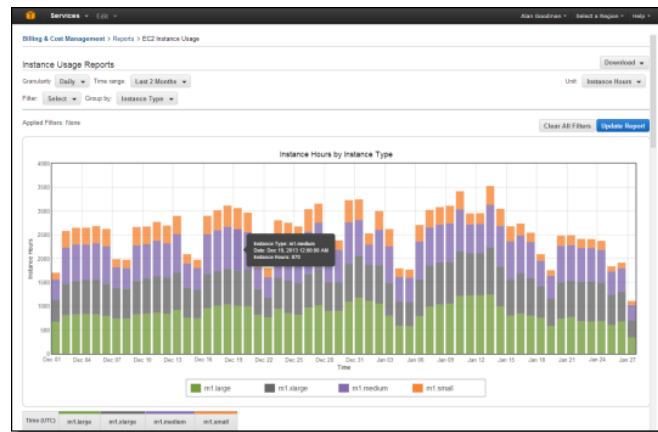
タスク		対応するAWSサービス
コスト管理	配布	<ul style="list-style-type: none"><li>請求書</li><li>Detailed Billing Report</li><li>Cost Explorer</li></ul>
利用管理	傾向分析	<ul style="list-style-type: none"><li>Cost Explorer</li><li>EC2使用状況レポート</li></ul>
	過剰利用対策 コスト最適化	<ul style="list-style-type: none"><li>予算</li><li>Trusted Advisor</li></ul>



# EC2使用状況レポート

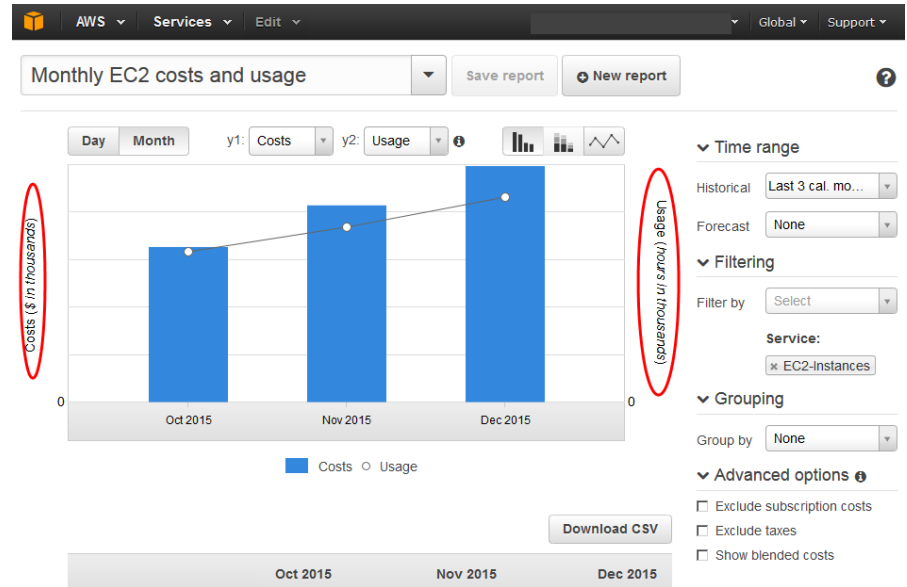
## 2種類のレポートを閲覧可能

- インスタンスの使用状況レポート
  - インスタンスタイプ、リージョン、等でどのくらい利用されているか表示
  - タグなどでグループ化、フィルタリング可能
- リザーブドインスタンスレポート
  - 購入したリザーブドインスタンスの使用量を表示
  - オンデマンド価格との比較による節約額を表示



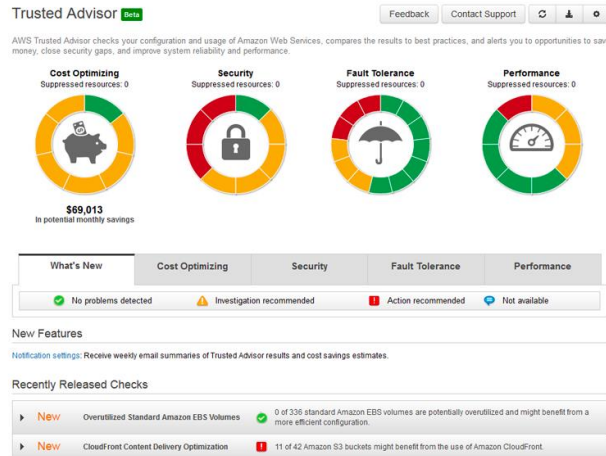
# Cost Explorer

- AWSリソースの使用量を時系列でグラフ化するツール
- コストの把握に役立つ傾向を分析
- 追加料金無し
- Viewのカスタマイズが可能



# AWS Trusted Advisor

- AWS Trusted Advisor
  - コスト最適化、セキュリティ、耐障害性、パフォーマンスをチェックし推奨事項をお知らせするサービス
- AWS Trusted Advisorによるコスト最適化
  - 不要リソースやアイドル状態のリソースを検出
  - リザーブドインスタンスの利用状況を可視化
- チェック項目の例
  - CPU利用率10%および N/W通信が 4日以上 5MB以下のインスタンス
  - リザーブドインスタンス最適化
  - 未活用のEBSボリューム
  - 未使用のEIP



# 概算見積もり

- Web上に費用試算ツールをご用意しています
  - [http://calculator.s3.amazonaws.com/index.html?lng=ja\\_JP](http://calculator.s3.amazonaws.com/index.html?lng=ja_JP)
- 詳しい使い方はこちら
  - <http://www.slideshare.net/AmazonWebServicesJapan/aws-simple-monthly-calculator-20130910>

Amazon Web Services Simple Monthly Calculator - Windows Internet Explorer

http://calculator.s3.amazonaws.com/calc5.html?lng=ja\_JP&key=calc-F9975B8D-71D1-4244-9E6D-01560A5FDB32

Amazon Web Services **SIMPLE MONTHLY CALCULATOR**

NEW! - Effective July 1st 2011. Free Inbound Data Transfer, Lower Outbound Data Transfer and New Tiers and Amazon EC2 running Red Hat Enterprise Linux

無料使用ティア: 新規顧客は12か月間、わたって無料使用ティアをご利用できます。

Services: あなたの毎月の請求書の見積もり (\$ 0.00)

リージョンの選択: US-East (Northern Virg) データ送信料は1か月間、リージョンあたり1GB無料です。

Amazon EC2 オンデマンドインスタンス:

インスタンス	参照名	OS	インスタンスタイプ	使用量	モニタリング
0		Linux/OpenSolaris	Micro	0 時間/月	<input type="checkbox"/>

Amazon EC2 リザーブドインスタンス:

インスタンス	説明	OS	タイプ	期間	使用量
0		Linux	Small	3年	0 時間/月

Amazon EBS ボリューム:

値段	説明	ストレージ量	平均IOPS	スナップショットストレージ*
0		0 GB-月	0	0 GB-月毎ストレージ

Elastic IP 数: 0

インターネット | 保護モード: 有効

# EC2価格データ

EC2の価格は、2種類の方法で取得できます。

- 価格ページ
  - <https://aws.amazon.com/jp/ec2/pricing/>
- Price List API
  - JSON/CSVフォーマットで取得可能
  - [http://docs.aws.amazon.com/ja\\_jp/awsaccountbilling/latest/aboutv2/price-changes.html](http://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/price-changes.html)
  - SNSで変更通知を受信可能

```
arn:aws:sns:us-east-1:278350005181:price-list-api
```

# AWS無料利用枠

- AWSサインアップ後12ヶ月間、AWSを無料で実際に利用可能。(自動的に設定済み)
- 無料枠対象サービスの無料利用条件の範囲内で無料。(超過した分は費用が発生)



## Amazon EC2

クラウド内でサイズ変更可能な計算処理機能。  
詳細はこちら >

**750 時間** 1 か月の Linux、RHEL、または SLES t2.micro インスタンス使用量

**750 時間** 1 か月の Windows t2.micro インスタンス使用量

一度に 1 インスタンスを実行するか、複数のインスタンスを同時に実行



## Amazon S3

高拡張性、高信頼性、低レイテンシーのデータストレージインフラストラクチャ。  
詳細はこちら >

**5 GB** 標準ストレージ

**20,000 件の Get リクエスト**

**2,000 件の Put リクエスト**



## Amazon DynamoDB

シームレスな拡張性を備えた、高速で柔軟な NoSQL データベースサービスです。  
詳細はこちら >

**25 GB** ストレージ

**25 ユニット** 書き込み容量

**25 ユニット** 読み込み容量

1 か月当たり最大 2 億リクエストの処理が十分に可能



## AWS Lambda

**新しい AWS 無料利用枠対象製品**

イベント発生時にお客様のコードを実行し、コンピューティングリソースを自動的に管理するコンピューティングサービス  
詳細はこちら >

**100 万回** 1 か月当たりの無料リクエスト数

**1 か月当たり最大 320 万秒** のコンピューティング時間

# 参考資料

- Amazon EC2
  - <http://aws.amazon.com/jp/ec2/>
- よくある質問
  - <https://aws.amazon.com/jp/ec2/faqs/>
- Amazon Elastic Compute Cloud ドキュメント
  - <http://aws.amazon.com/jp/documentation/ec2/>
- Amazon EC2開発者用リソース
  - <http://aws.amazon.com/jp/ec2/developer-resources/>
- EC2フォーラム
  - <https://forums.aws.amazon.com/forum.jspa?forumID=30>

# 参考資料

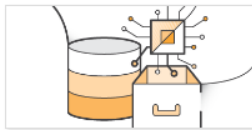
- AWS CLI
  - <http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-tech-2015-aws-cloudtrail-aws-sdk-for-powershell>
- AWS SDK
  - <http://www.slideshare.net/AmazonWebServicesJapan/20150318-aws-blackbeltsdk>
- Amazon EC2 Systems Manager
  - <https://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-online-seminar-2017-amazon-ec2-systems-manager>
- AWS CloudFormation
  - <http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-online-seminar-2016-aws-cloudformation>
- AWS Elastic Beanstalk
  - <http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-online-seminar-2017-aws-elastic-beanstalk>
- AWS OpsWorks
  - <http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt-online-seminar-2017-aws-opsworks>



# オンラインセミナー資料の配置場所

- AWS クラウドサービス活用資料集

- <http://a>



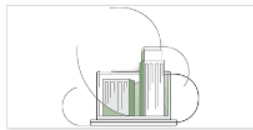
サービス別資料

無料オンラインセミナー「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。



ソリューション別資料

無料オンラインセミナー「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。



業種別資料

無料オンラインセミナー「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。



その他の資料

イベントに関する資料やアップデート情報などがご覧いただけます。

- AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています
  - <http://aws.typepad.com/sajp/>

# AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

<p>お問い合わせ</p> <p>日本担当チームへのお問い合わせ &gt;</p> <p>関連リンク フォーラム</p>	<h2>日本担当チームへのお問い合わせ</h2> <p>AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。</p> <p>※ご請求金額またはアカウントに関する質問は<a href="#">こちらからお問い合わせください</a>。 ※Amazon.com または Kindle のサポートに問い合わせは<a href="#">こちらからお問い合わせください</a>。</p> <p>アスタリスク (*) は必須情報となります。</p> <p>姓* <input type="text"/></p> <p>名* <input type="text"/></p>
--	---

※「AWS お問い合わせ」で検索してください

