AWSで実現するセキュリティと事例のご紹介
世界中に膨大なコンピュートリソースを提供するAWSとは？

2014年11月17日

アマゾン データサービス ジャパン株式会社
エコシステム ソリューション部 部長
松本 大樹

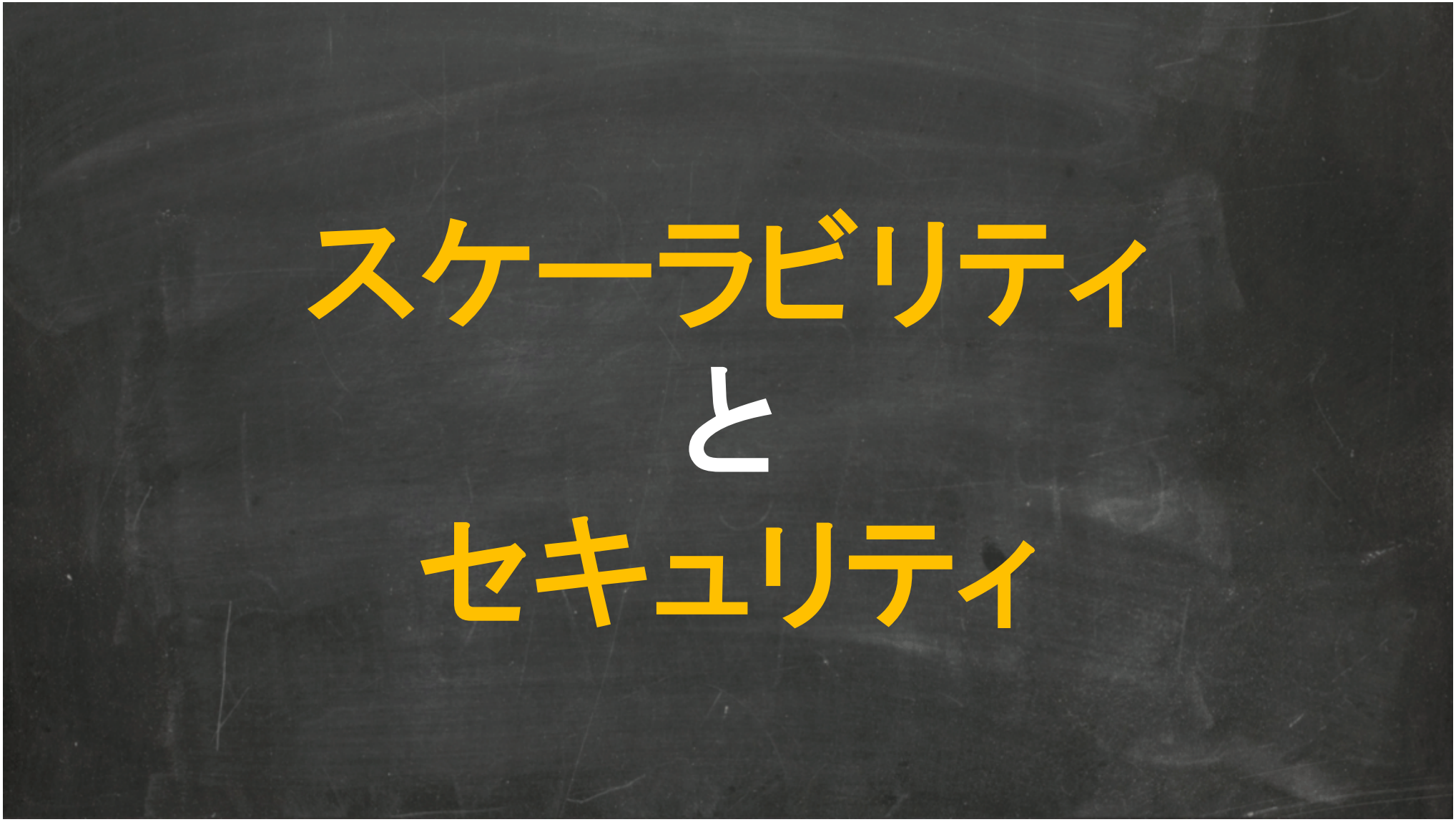
amazon web services

自己紹介

松本 大樹(まつもと ひろき)

エコシステム ソリューション部 部長
パートナー ソリューション アーキテクト

- 十数年、某ハードウェアベンダーにてエンジニアを経験
- クラウドに興味を示し、数年前にAWSにジョイン。
- 世の中を便利にすべく、クラウドの啓蒙活動中。

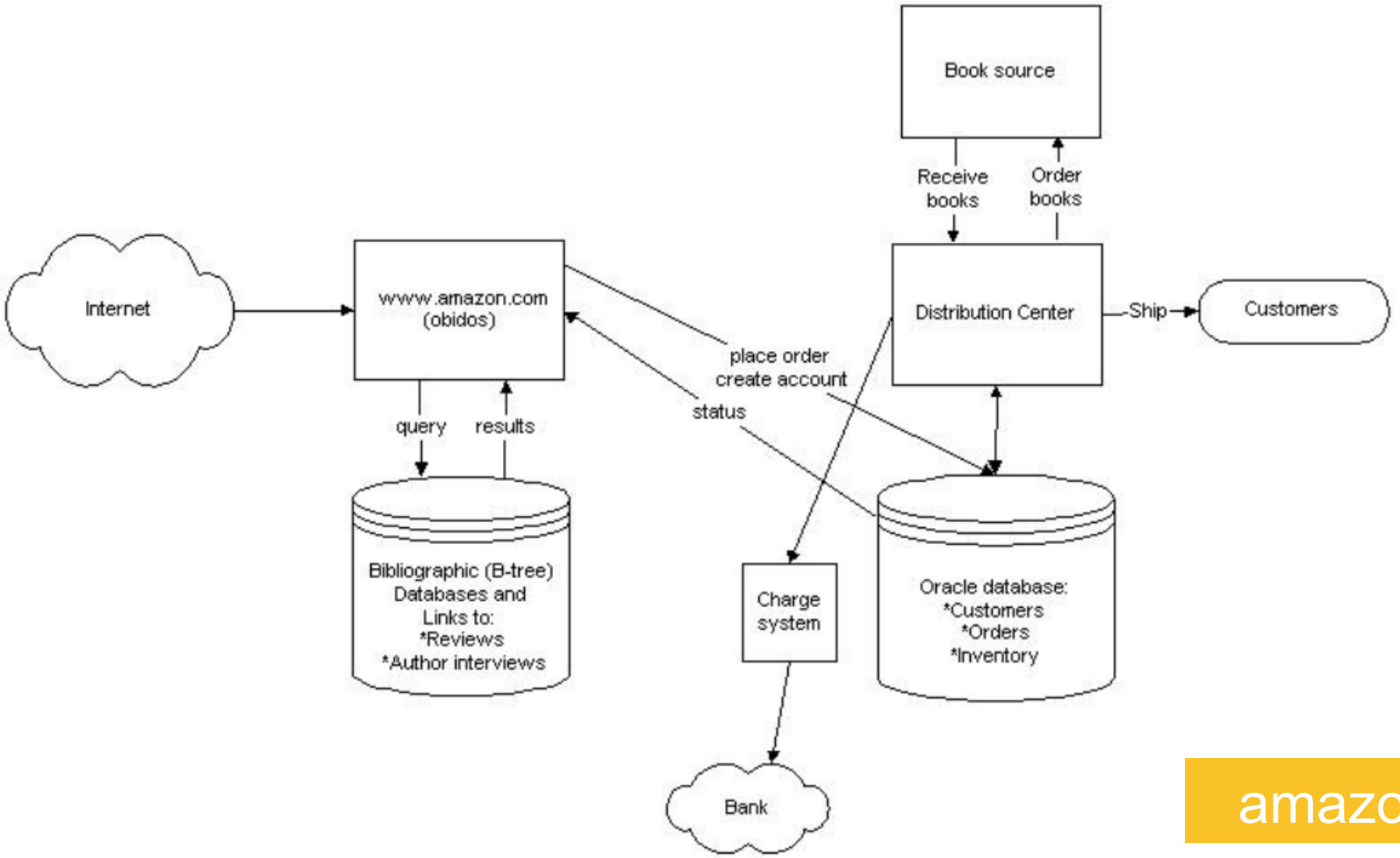

スケーラビリティ
と
セキュリティ

Amazon?
amazon
web services

What is Amazon?

- 創業：1995年7月16日
- 創設者＆CEO:
  ジェフ・ベゾス
- 2億人超アクティブカスタマ
  （2014年3月時点）
- 611億ドルの総売上高
  （2014年度）

amazon.com, 1995

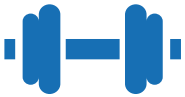


amazon.com, **1996**

初期Amazon.comの課題

amazon.com

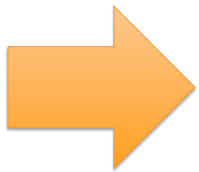
- システムがスケールしない
  - システム間の依存性が高い単一なアーキテクチャ
- 自社またはデータセンター会社の増設が追いつかない
- 高いハードウェア・ソフトウェア購入費用
- サービスの追加や改善がインフラ要件で遅延



amazon.com, 1999

amazon web services

AWSクラウドの起源は、
アマゾン社内の
ビジネス課題を解決するために
生まれた



Amazonのビジネスの基幹システムを支える技術
= “Amazon Web Services”

AWS (Amazon Web Services)とは？

AWS(Amazon Web Services)の歴史

2006年	米国で、クラウドストレージ＝Amazon S3 クラウド仮想サーバ＝Amazon EC2のサービスを開始
2009年	仮想プライベートクラウドサービス＝Amazon VPC RDBMSサービス＝Amazon RDSを開始
2011年3月	世界で５番目のリージョンとして、 日本に東京リージョン(データセンタ群)を開設
現在	世界10か所のデータセンター群と、 50拠点を超えるエッジロケーション網で、 30を超えるサービスを提供中

amazon web services

AWSのグローバルインフラストラクチャー

GovCloud	US West		US East	South America	EU	Asia Pacific		
US ITAR Region	N. California	Oregon	N. Virginia	Sao Paulo	Ireland	Sydney	Tokyo	Singapore

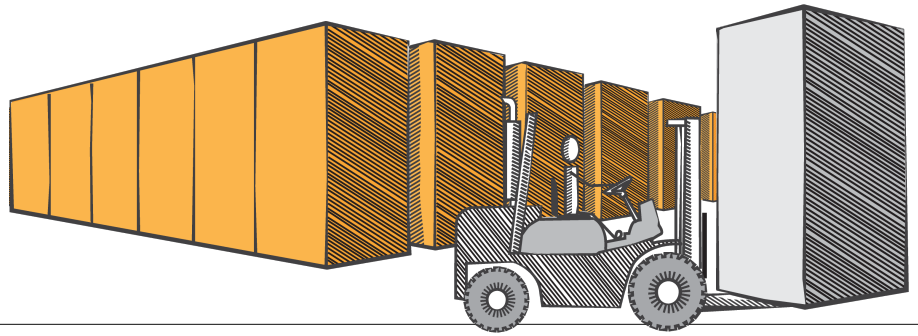
10 Regions

25 Availability Zones

55 Edge Locations

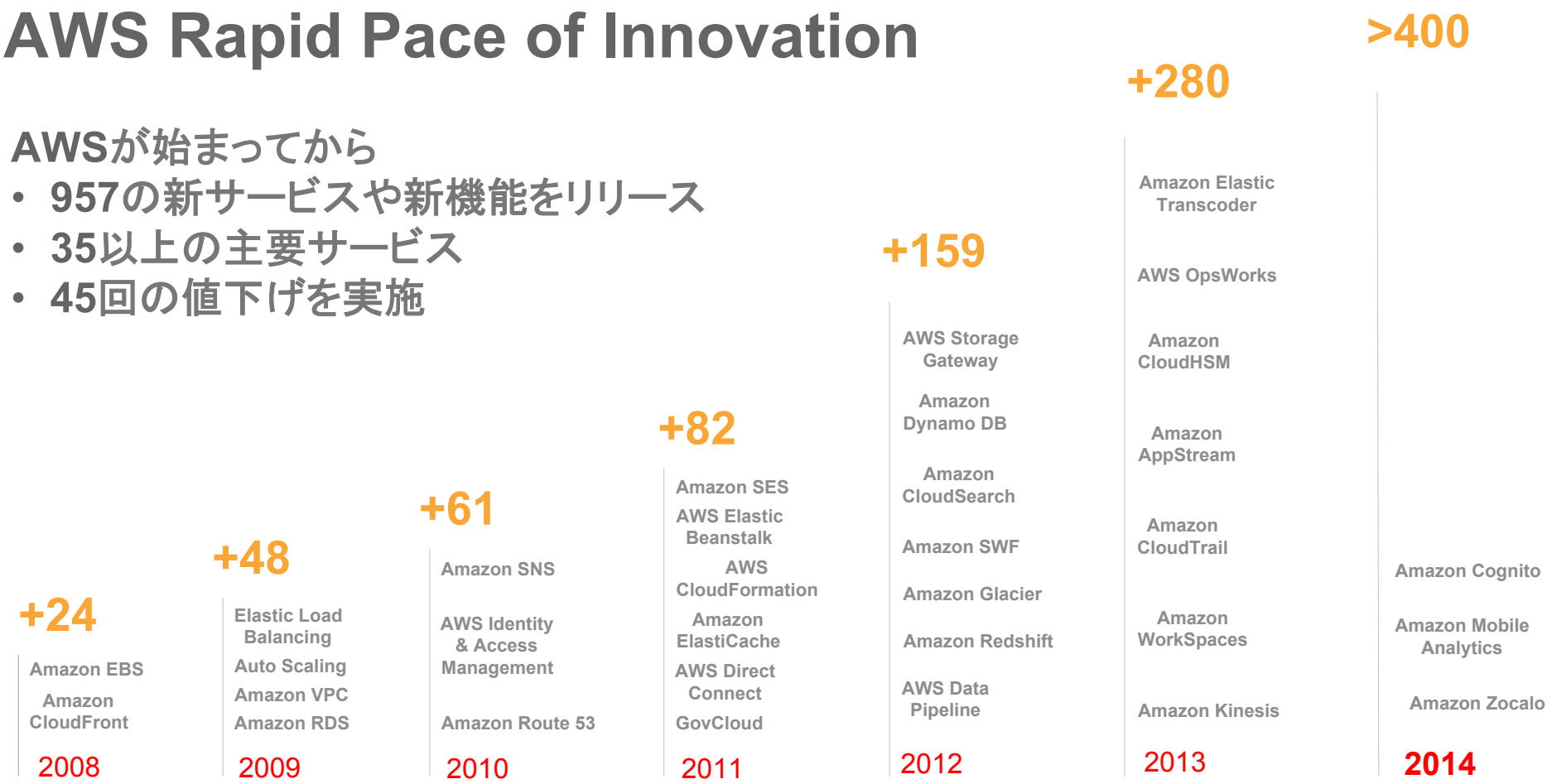
AWSクラウドの規模

アマゾンが**年商 70 億ドル**のビジネス規模だった時に必要なコンピューターリソースを、AWSでは**毎日追加**しています



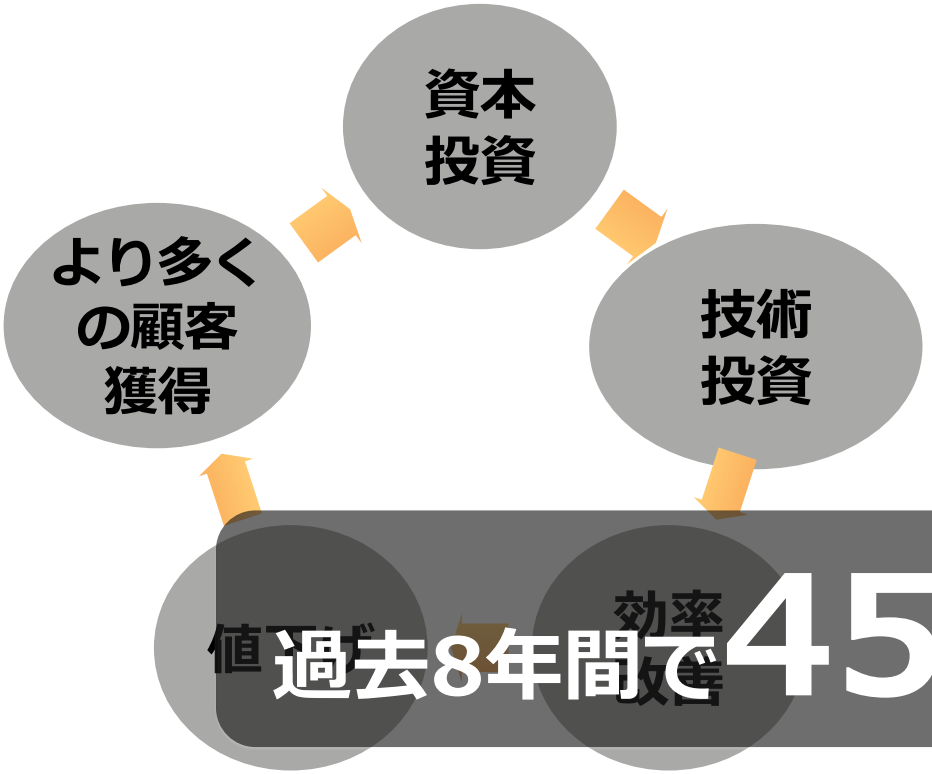
AWS Rapid Pace of Innovation

AWSが始まってから
- 957の新サービスや新機能をリリース
- 35以上の主要サービス
- 45回の値下げを実施



amazon web services
© 2014 Amazon.com, Inc. and its affiliates. All rights reserved.

小売りのDNA：更なる低価格へのこだわり



過去8年間で45回以上の値下げを実施

Gartner Magic Quadrant for Cloud Infrastructure as a Service

2013

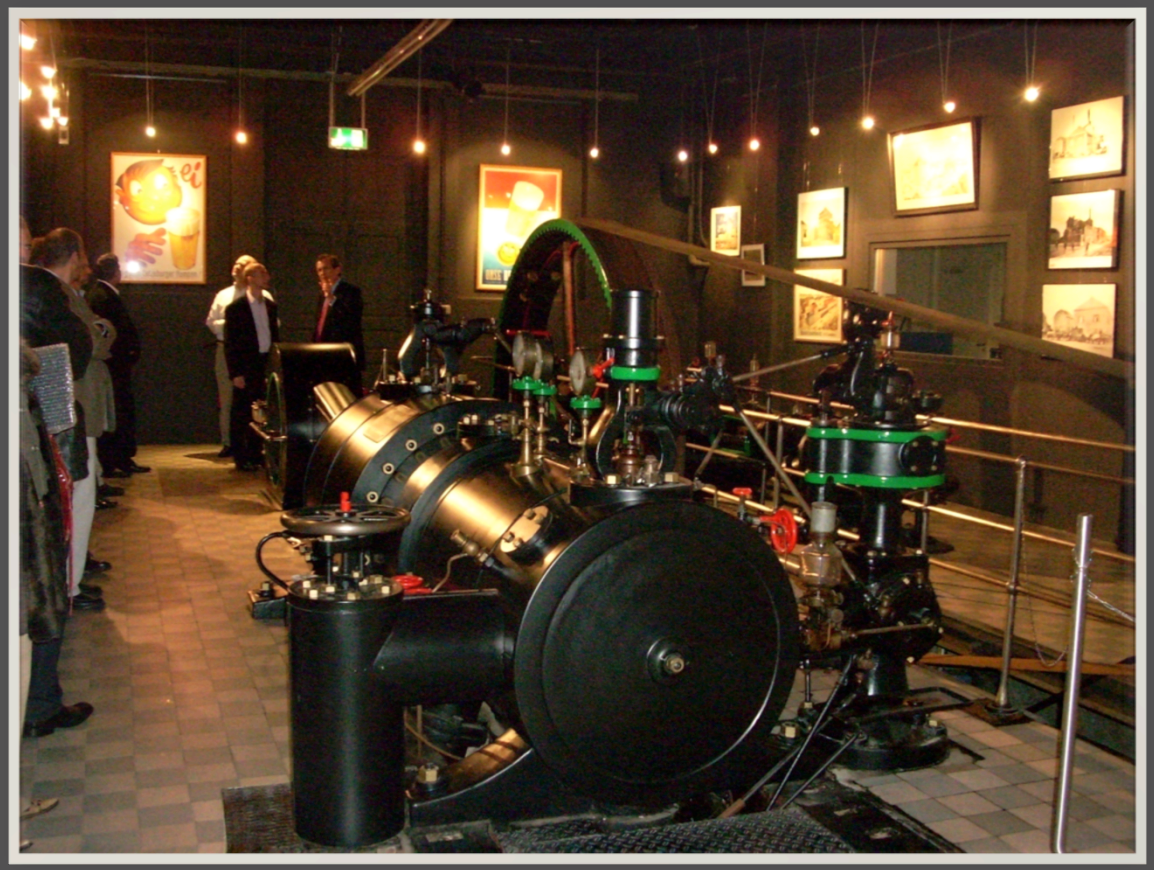
2014

Source: Gartner (May 2014)

Gartner "Magic Quadrant for Cloud Infrastructure as a Service," Lydia Leong, Douglas Toombs, Bob Gill, Gregor Petri, Tiny Haynes, May 28, 2014. This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available at http://aws.amazon.com/resources/analyst-reports/. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

amazon web services

クラウドのインパクトを
歴史上の出来事に例えると・・・



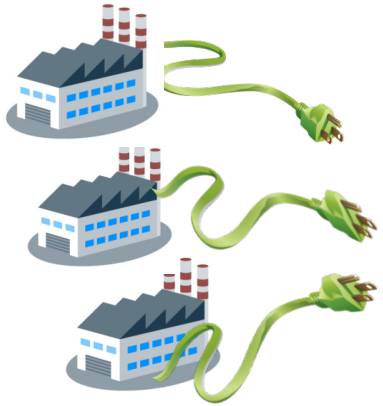
発電機所有が差別化要因だった時代の終焉

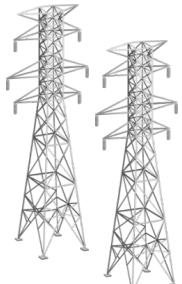
中央発電所＋
送電網の出現が
パラダイムシフトに

いつでも、必要なだけ、安価に

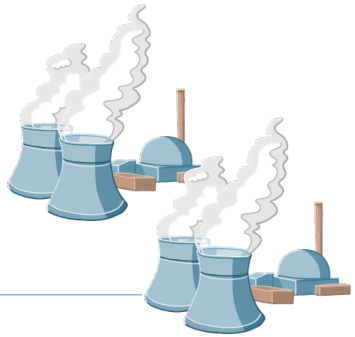
電気

工場





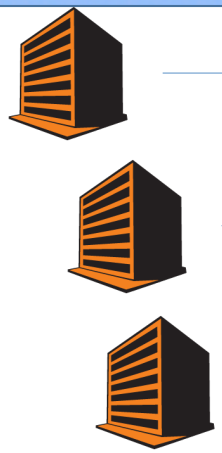
送電線



発電所

コンピュータ

IT部門



インターネット

データセンター

お客様のアプリケーション

ライブラリ & SDKs
Java, PHP, .NET, Python, Ruby

コマンドライン インターフェース
CLI

Web管理画面
Management Console

認証とログ
IAM, CloudTrail, CloudHSM

監視
Cloud Watch

デプロイと自動化
Elastic Beanstalk, Cloud Formation, OpsWorks

アプリケーション
Workspaces, Zocalo

モバイル
Mobile Analytics, Cognito, SNS

アプリケーションサービス
AppStream, Cloud Search, SWF, SQS, SES, Elastic Transcoder

データベース
RDS, DynamoDB, Redshift, ElastiCache

分析
Elastic MapReduce, Kinesis, Data Pipeline

ストレージ
EBS, S3, Glacier, Storage Gateway

コンテンツ配信
CloudFront

コンピュート処理
EC2, Auto Scaling, Elastic Load Balancing,

ネットワーク
VPC, Route 53, Direct Connect

AWS Region AWS AZ

グローバルインフラ
リージョン、アベイラビリティゾーン、エッジロケーション

amazon web services

EC2

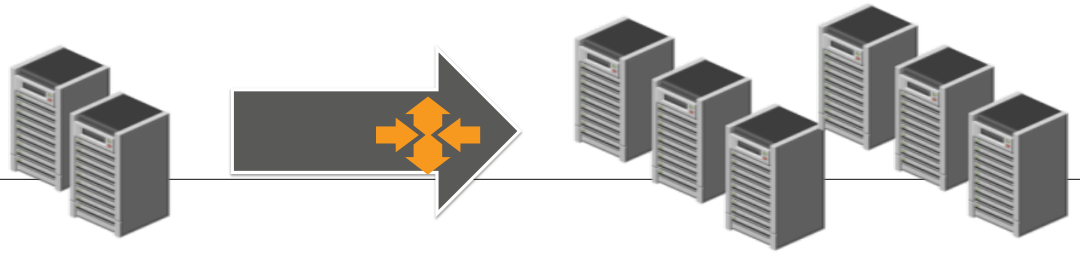
Amazon EC2(Elastic Compute Cloud)

- 数分で起動し、1時間ごとの従量課金で利用可能な仮想サーバ
- スケールアップ/ダウン、アウト/インが即座に可能
- OSのライセンス費用もEC2の料金に含まれるオプションも用意
- x86系のOSをサポートし、自由にソフトウェアインストール、セットアップが可能

redhat. Linux Windows

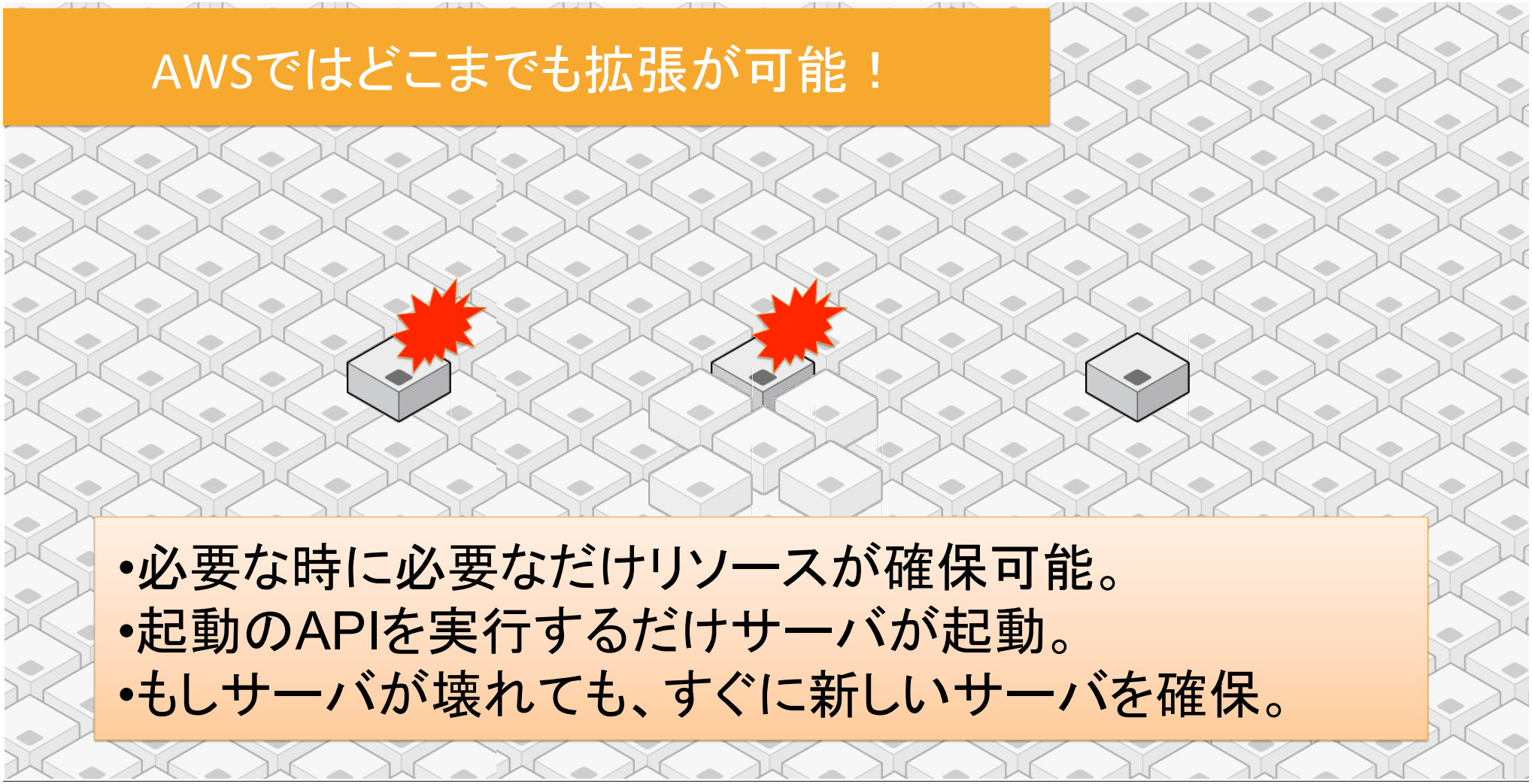
EC2のオートスケール機能

- 負荷に応じてEC2の台数を増やしたり減らしたりできる
- ピーク対応が楽になる！
  - CPU負荷が80%が5分間続いたらサーバを1台増やす
  - CPU負荷が30%が15分間続いたらサーバを1台減らす
  - 最小台数は2台で、最大台数は5台とする
- オートスケールする方法は、ポリシーまたは時刻
- 典型的なユースケース
  - 突発的なピークが来た場合
  - 予め来るとわかっているトラフィックでスケールさせたい場合
  - 障害のあったサーバがあっても自動リカバリして一定台数保ちたい場合



amazon web services

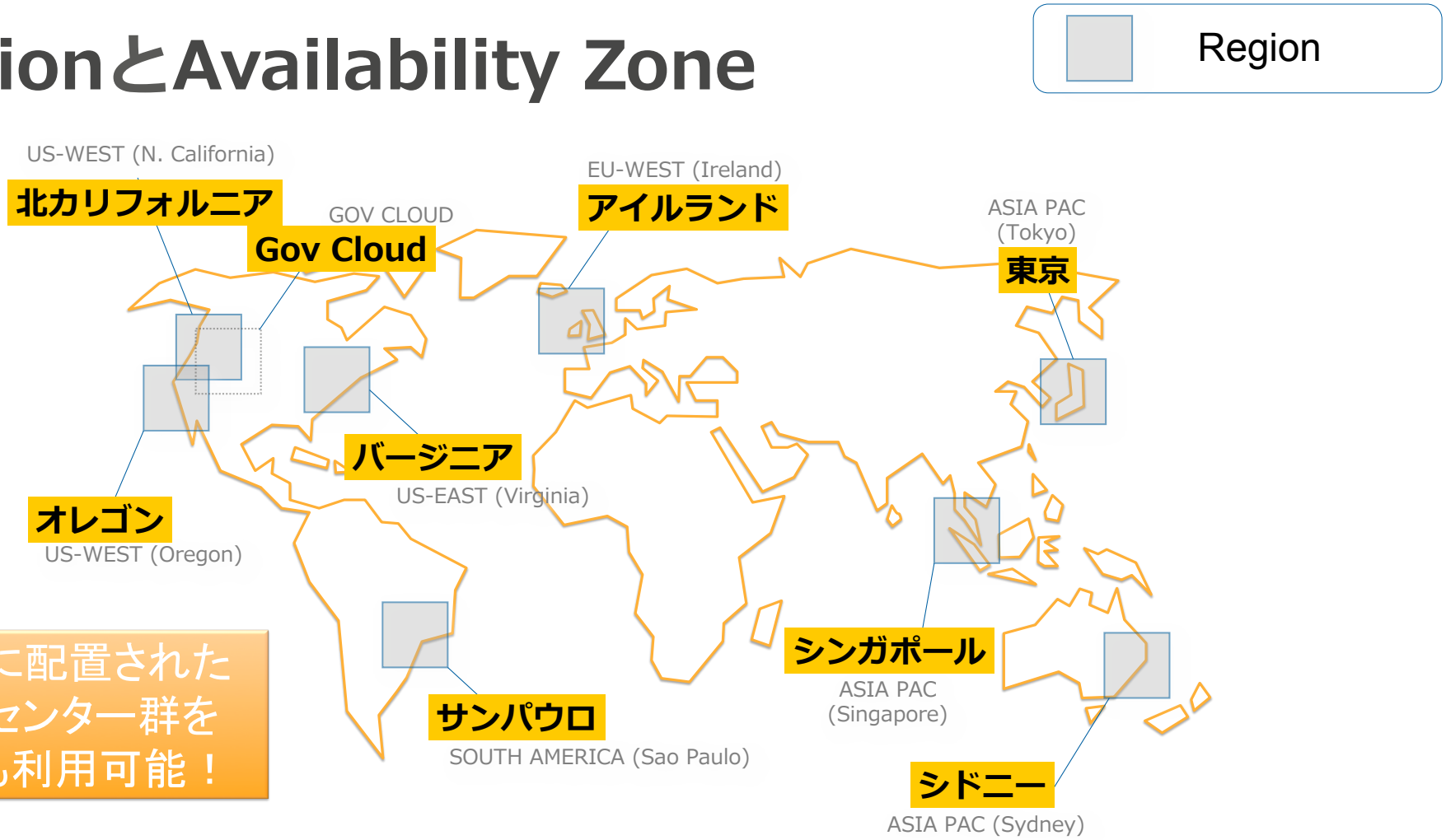
AWSではどこまでも拡張が可能！



- 必要な時に必要なだけリソースが確保可能。
- 起動のAPIを実行するだけサーバが起動。
- もしサーバが壊れても、すぐに新しいサーバを確保。

amazon web services

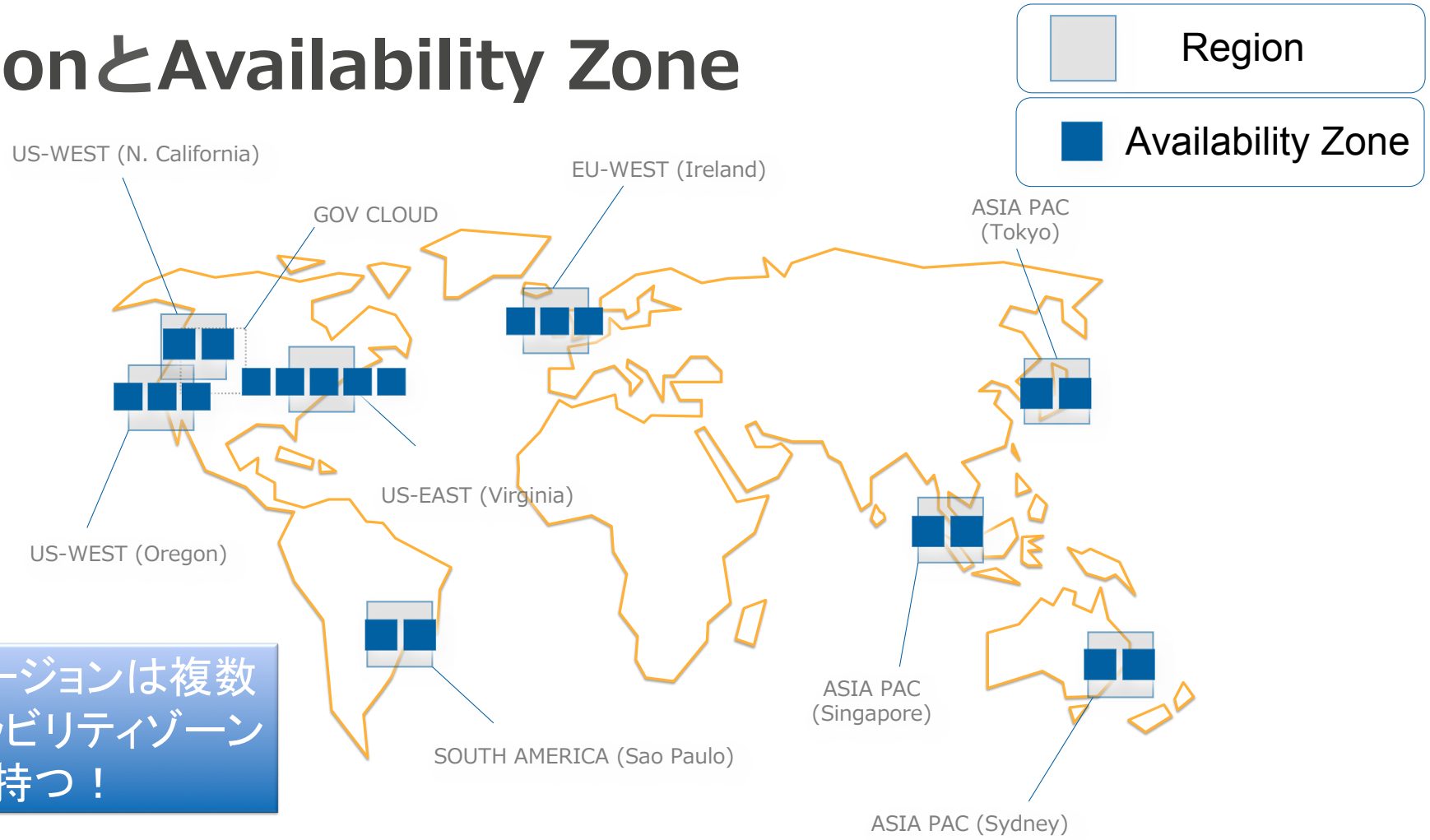
RegionとAvailability Zone



世界中に配置された
データセンター群を
いつでも利用可能！

amazon web services

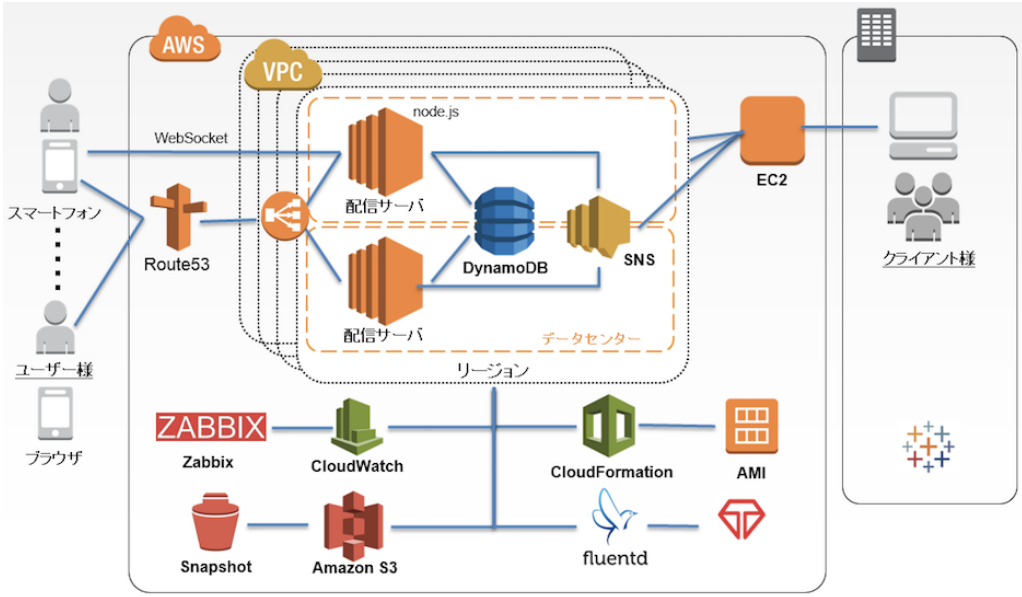
RegionとAvailability Zone



全てのリージョンは複数のアベイラビリティゾーンを持つ！

amazon web services

日本放送協会様事例
NHK紅白歌合戦



- 生放送と連動したミッションクリティカルなメッセージ配信プラットフォームを提供
- AWS上に数百台のサーバを複数リージョン、データセンターを利用して構築
- 1日のみ発生する毎秒数十万の同時接続という高負荷に耐えられる高可用性システムを実現

AWSのセキュリティ

AWSのセキュリティ方針

- AWSクラウドのセキュリティ
  - AWSにおいて最優先されるべき事項
  - セキュリティに対する継続的な投資
  - セキュリティ専門部隊の設置

- **共有責任モデルの採用**
  - AWSと利用者の2者でセキュリティを確保

AWS GovCloud (US)

米国政府、関連業者のみが利用可能
国際武器取引規制(ITAR)の要求に基づき
米国市民のみがアクセスできる環境を提供

利用者の統制

共有の責任

AWSの統制

利用者のデータ

ユーザー権限管理

アカウント管理

アプリケーション

セキュリティ構成

ネットワーク構成

ゲストOS

利用者固有の要件

AWS

仮想化レイヤー

コンピュート・インフラ

ストレージ・インフラ

ネットワーク・インフラ

施設・物理セキュリティ

AWSグローバル・インフラ

The Shared Responsibility Model For Infrastructure Services

AWSは以下のような第三者認証を取得済み

- SSAE 16/ISAE 3402基準、SOC1レポート（旧SAS70)
- SOC2レポート、SOC3レポート
- ISO 27001 Certification
- PCI DSS Level 1
- FISMA moderate
- Sarbanes-Oxley (SOX)
- FedRAMP
- DoD(国防総省暫定認証)

AWSにシステムをデプロイし、第三者認証を取得することも可能

- HIPAA (医療関係)
- Pマーク
- ASP・SaaS安全・信頼性に係る情報開示認定制度

利用者の統制

共有の責任

AWSの統制

利用者のデータ
ユーザー権限管理
アカウント管理
アプリケーション
セキュリティ構成
ネットワーク構成
ゲストOS

利用者固有の要件

AWS

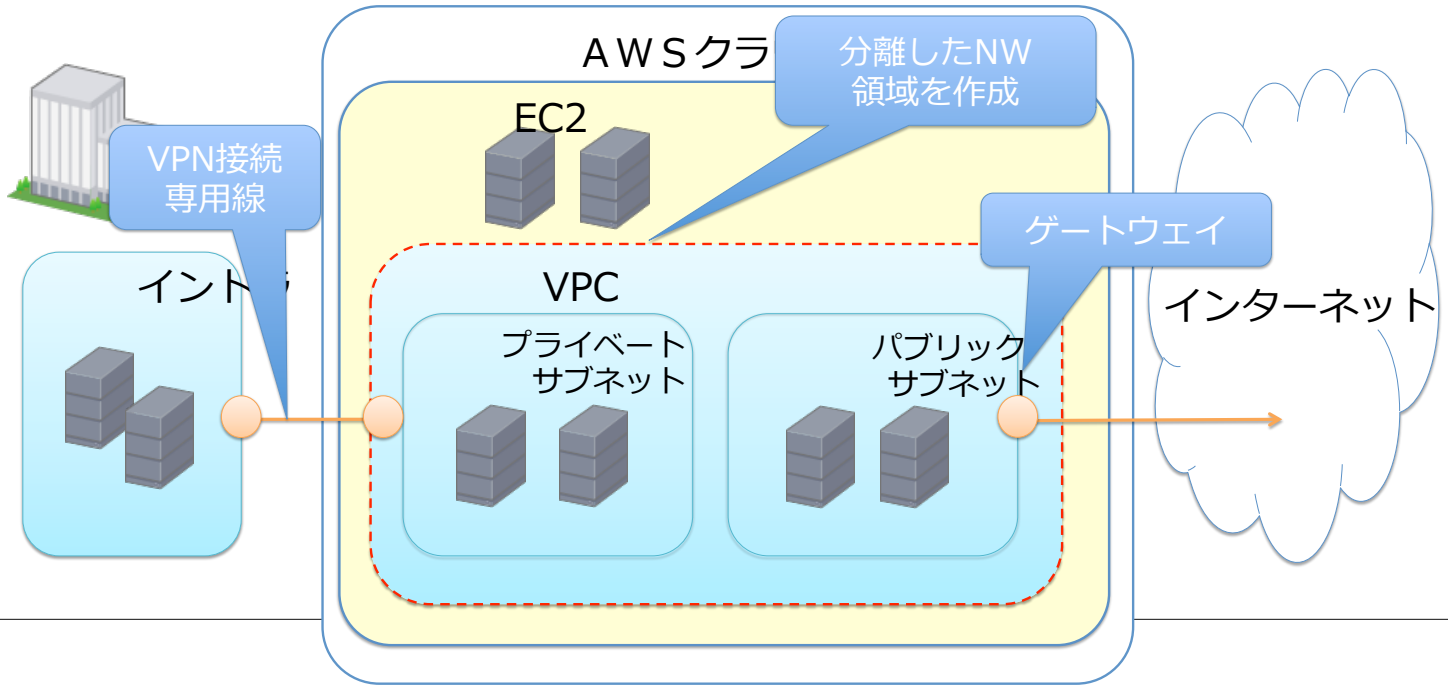
仮想化レイヤー
コンピュート・インフラ
ストレージ・インフラ
ネットワーク・インフラ
施設・物理セキュリティ
AWSグローバル・インフラ

The Shared Responsibility Model For Infrastructure Services

amazon web services

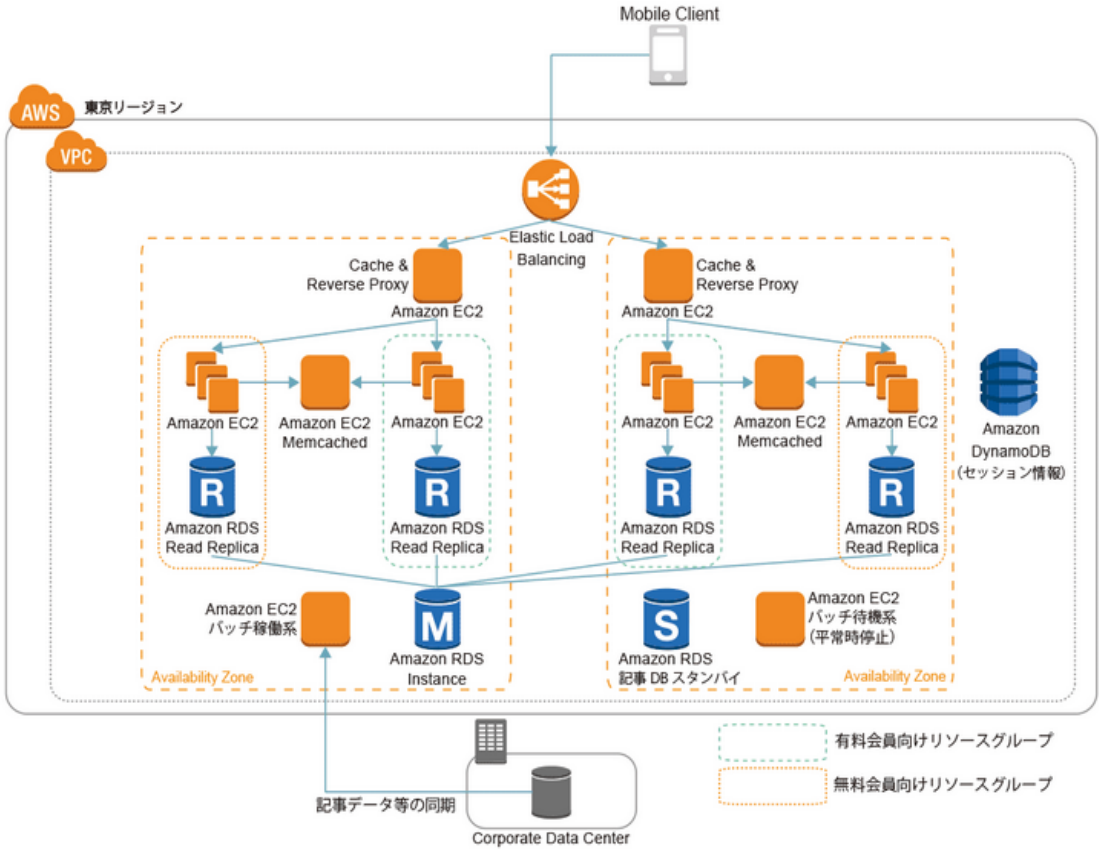
Amazon VPC(Virtual Private Cloud)

- クラウド内にプライベートネットワークを構築
- 既存データセンターの延長としてAWSを利用
- 認証の連携など、オンプレミスのシステムとの連携が容易



AWSの事例ご紹介

株式会社 日本経済新聞社様



- 日経電子版モバイルのサービスを開始する際の課題
  - タイトなスケジュール
  - 予測出来ないトラフィック
  - システム投資の削減
  - 規模に合わせた拡張性
- ELB, EC2, RDSをはじめElastiCacheやDynamoDBなど様々なサービスを利用

トヨタ自動車株式会社様

toyota.jp

www.toyota.co.jp

lexus.jp

11ドメインのサイトにてAWSを利用。
移行&5年間の運用コスト込みで大幅なコストを削減

花王株式会社様

自然と調和する こころ豊かな毎日をめざして

- 対外向けコーポレートウェブサイトおよび**CMS**を全て**AWS**に完全移行
- グローバルの花王グループのインフラを統合するために**AWS**を選定
- 従来のデータセンター利用時より年間コスト**80%**削減
- **AWS**利用正式決定後、システム構築から移行まで**4**ヶ月で完了
  機器設置が数日で完了する点が非常にメリット
- **Multi-AZ**構成により冗長構成化を行いシステム可用性を向上

“AWSは柔軟性が高いため常に最適なサーバーを利用することで性能を格段に上げられました。今後はハードウェアの陳腐化を気にすることなく運用することが可能となりました。”

花王株式会社 デジタルコミュニケーションセンター 田中 剛 様

amazon web services

クックパッド

- 月間1,400万人のユニークユーザをもつ日本最大規模のレシピサイト
- 突発的なアクセスへの対応と、サービス開発の迅速化が課題
- **サイトを完全にAWSに移行し、サービス提供スピードを改善**

“AWSに移行し、突発的なアクセスに対応でき、お客様のデータを安全かつ、容量を気にせず保管できる様になりました。新サービス開発スピードの向上も大きな利点です。”

クックパッド CTO　橋本　健太　様

190カ国数十万のお客様が利用
日本でも20,000以上のお客様がご利用中

本日の**AWSセッション**の
まとめ

本セッションのまとめ

- ✓ AWSは世の中のベンチャー企業からエンタープライズ企業のシステム基盤まで、**多くの様々ユーザー様**にご利用頂いています。
- ✓ ユーザー様は世界中にある**分散インフラストラクチャー**上で各種ソフトウェアを利用したシステムをいつでも素早く構築することが可能です！
- ✓ 既に多くのユーザー様はこれらの**新世代のインフラを活用**してビジネスを開始しております。

Webサイトも
アマゾンで！