

サービス基盤を支える AWSのアーキテクチャ

Amazon Web Services Japan

エコシステムソリューション部
パートナーソリューションアーキテクト 小梁川

自己紹介

小梁川 貴史(こやながわ たかし)



- パートナーソリューションアーキテクト
 - APNさまへの技術支援
 - アーキテクチャの検討支援やレビューなど
- 経歴
 - ソフトハウスにて、開発とSI業務を経験
 - 電機メーカーにて、自社Webサービスの設計から運用まで経験
 - AWSのユーザとして4年半、1000台を超えるインスタンス環境での開発・運用
- 好きなサービス
 - Cloudwatch events
 - AWS IoT

アマゾンのビジネス

Eコマース
(物販&デジタル)
amazon.co.jp[®]

アドバタイジング
amazon
media group

マーケットプレイス
ロジスティックス
amazon services
japan

クラウド

 **amazon**
web services

Since 1995...

「規模の経済」×「ITの活用」で「薄利多売」の
ビジネスモデルを実現

低コスト化 → 値下げ
顧客満足度の向上
利用量の増加
スケールメリット
テクノロジーカンパニー



初期投資不要



完全従量課金



柔軟なキャパシティ



市場投入スピード



セキュア



グローバル展開

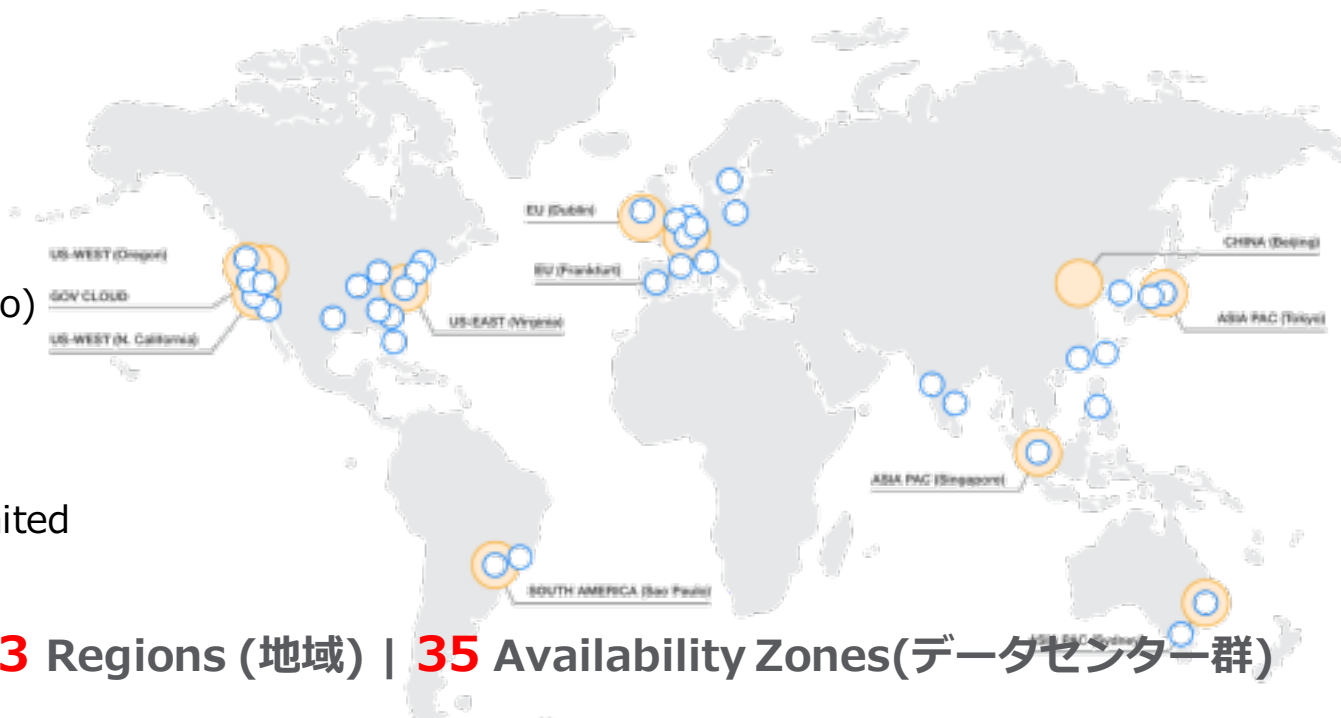
柔軟なインフラリソースを、
いつでも、誰でも、安く、手に入れることができる

13のリージョン

1. US EAST (Virginia)
2. US WEST (N. California)
3. US WEST 2 (Oregon)
4. EU WEST (Ireland)
5. **JAPAN (Tokyo)**
6. South America (Sao Paulo)
7. ASP 1 (Singapore)
8. ASP 2 (Sydney)
9. GovCloud
10. BJS 1 (Beijing China) limited
11. **EU (Frankfurt)**
12. **Seoul(korea)**
13. **Mumbai(India)**

13 Regions (地域) | **35** Availability Zones(データセンター群)

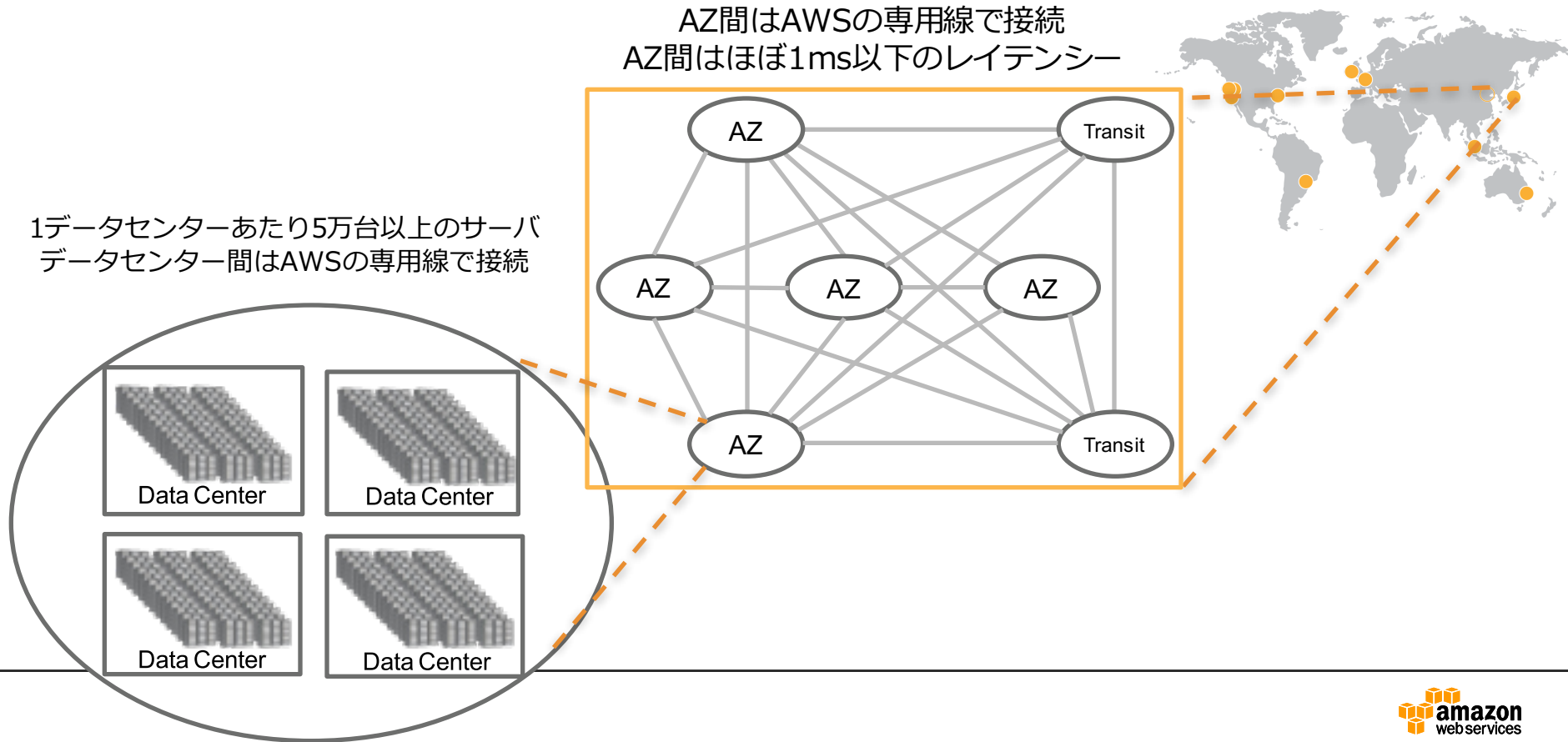
54か所のエッジロケーション



世界中に広がるAWSの拠点

AZ間はAWSの専用線で接続
AZ間はほぼ1ms以下のレイテンシー

1データセンターあたり5万台以上のサーバ
データセンター間はAWSの専用線で接続



世界中に広がるAWSの拠点

収集されるデータのロケーションはお客様が選択

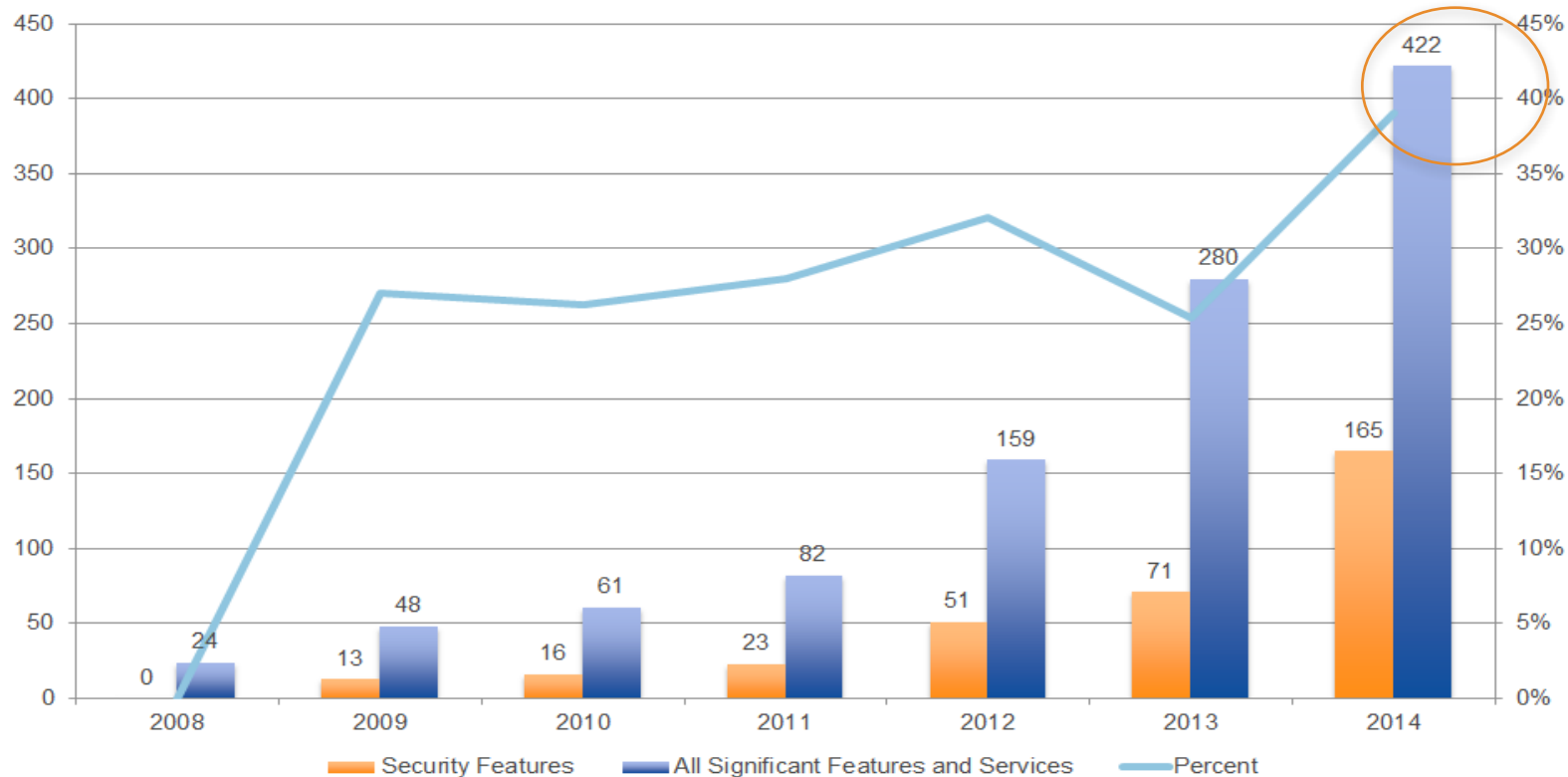
**データは配置されたリージョンから許可なく他
リージョンへコピーされない**

**むしろ、DR目的であえて自動でコピーする設定を
行うことも可能**

AWSのセキュリティに対する取り組み

リリースとセキュリティの関係

40%以上がセキュリティに関するアップデートorリリース



共有責任モデル ～AWSのセキュリティに関する考え方



お客様のアプリケーションとコンテンツ

プラットフォーム、アプリケーション、アイデンティティ
& アクセス管理

オペレーティングシステム、ネットワーク、ファイア
ウォール構成

クライアント側で
のデータ暗号化

サーバー側での
データ暗号化

ネットワークトラ
フィックの保護

顧客はクラウ
ド内のセキュ
リティに責任
を持ちます。



AWS の基盤サービス

コンピュ
ーティング

ストレージ

データベース

ネットワー
キング

AWS グローバ
ルインフラスト
ラクチャ

アベイラビ
ティーゾーン

リージョン

エッジロケー
ション

AWS はクラウド
のセキュリティに
責任を持ちます。

専門家の監査: 透明性と正確性

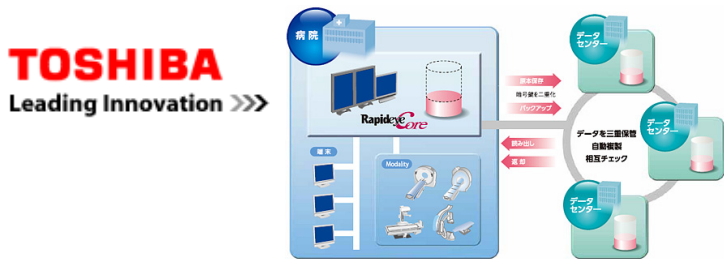
- ❏ 専門の監査人は、コンプライアンスに関して偏見のない見解を提供します
- ❏ プロセスが終わることはなく、常に尽力し続けています
- ❏ これまでにご覧になったことがないようなモニタリングを継続しています



PCI DSS: Payment Card
Industry Data Security
Standard

クレジットカード情報および
取引情報を取り扱うための
セキュリティ基準

AWSのセキュリティ実証例



Eコマースでも

クラウド上で、顧客情報、
クレジット決済を管理



医情情報でも

クラウドに医療情報を分散格納し、
情報漏えいや災害時の情報消失防止に対処



金融サービスでも

PCI DSSを取得して
金融決済サービスを提供

日本で20,000以上のお客様



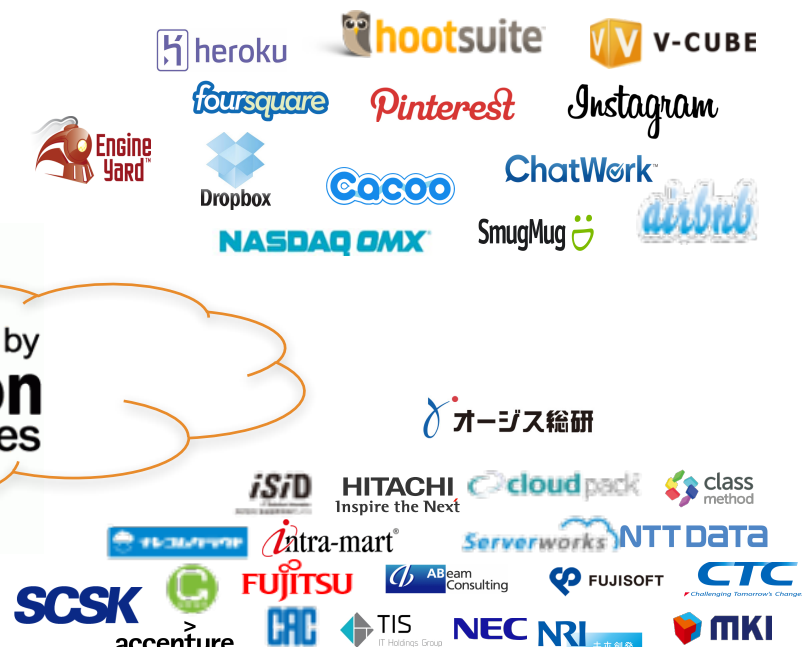
エコシステムで課題解決！

AWSクラウド上で構築



アプライアンス、ネットワーク
ベンダーのクラウド対応

クラウドサービス提供



システムインテグレーション

すべての IT を on AWSで

Marubeni

LAWSON



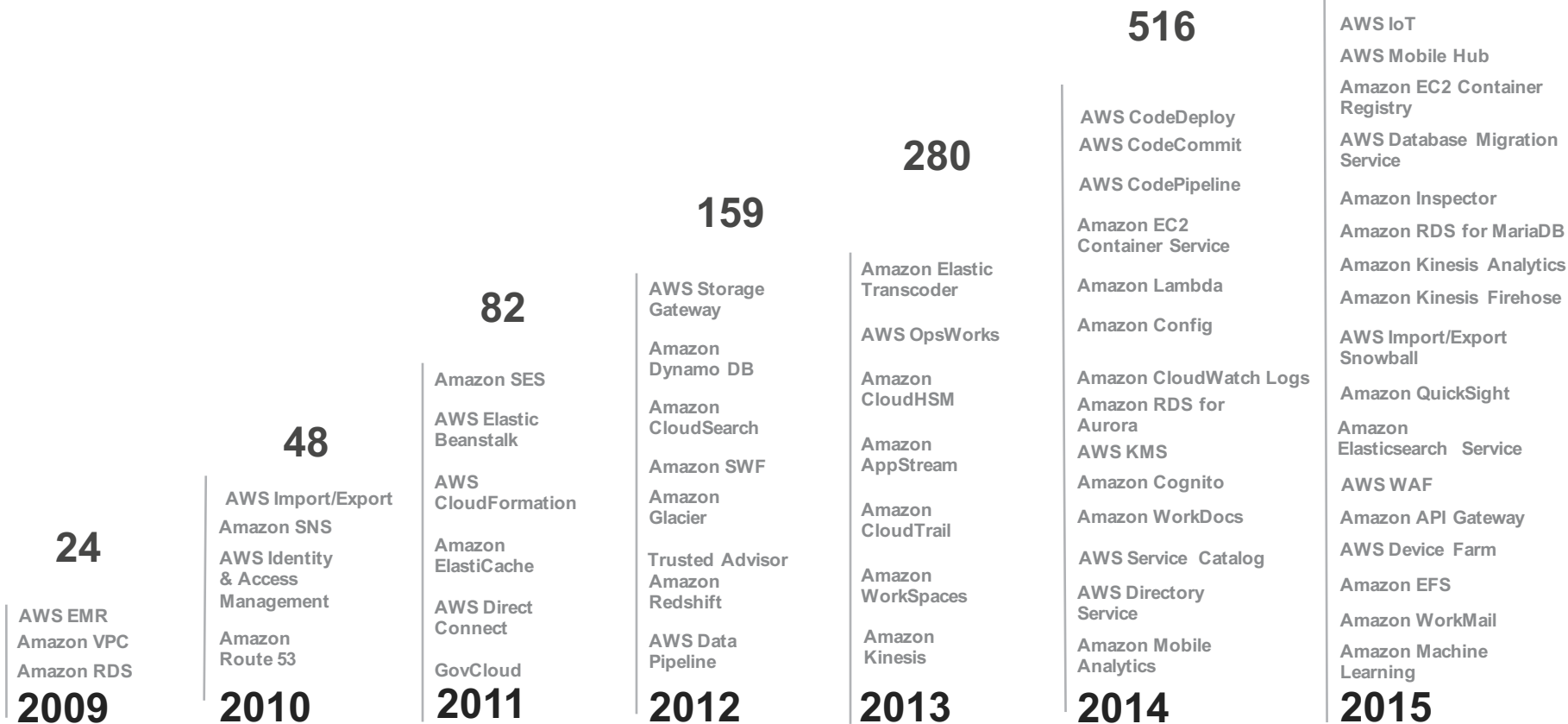
500台規模のプライベートクラウドを丸ごとAWSへ
業務システムの全インフラを
数年かけてAWSに移行

基幹システムをAWSに移行
その他の業務システムも
順次AWSに移行

1000台以上のサーバーを
ほぼ全てをクラウドへ移行
5年間で40%のコスト削減

AWS自体にて継続的なイノベーションを加速

722



数字で見るAWSクラウド

- 世界に先駆け**2006年**より、クラウドサービスを提供
- 世界に**13か所**のデータセンター群
- 世界で190か国の**100万を超えるお客様**が利用
- 年間で合計**700を超える(15年度実績)**、イノベーション機能拡張/改善
- 世界に**10,000**を超えるパートナー・エコシステム
- 累計で**51回**以上値下げをして利益をお客様へ還元

お客様のアプリケーション

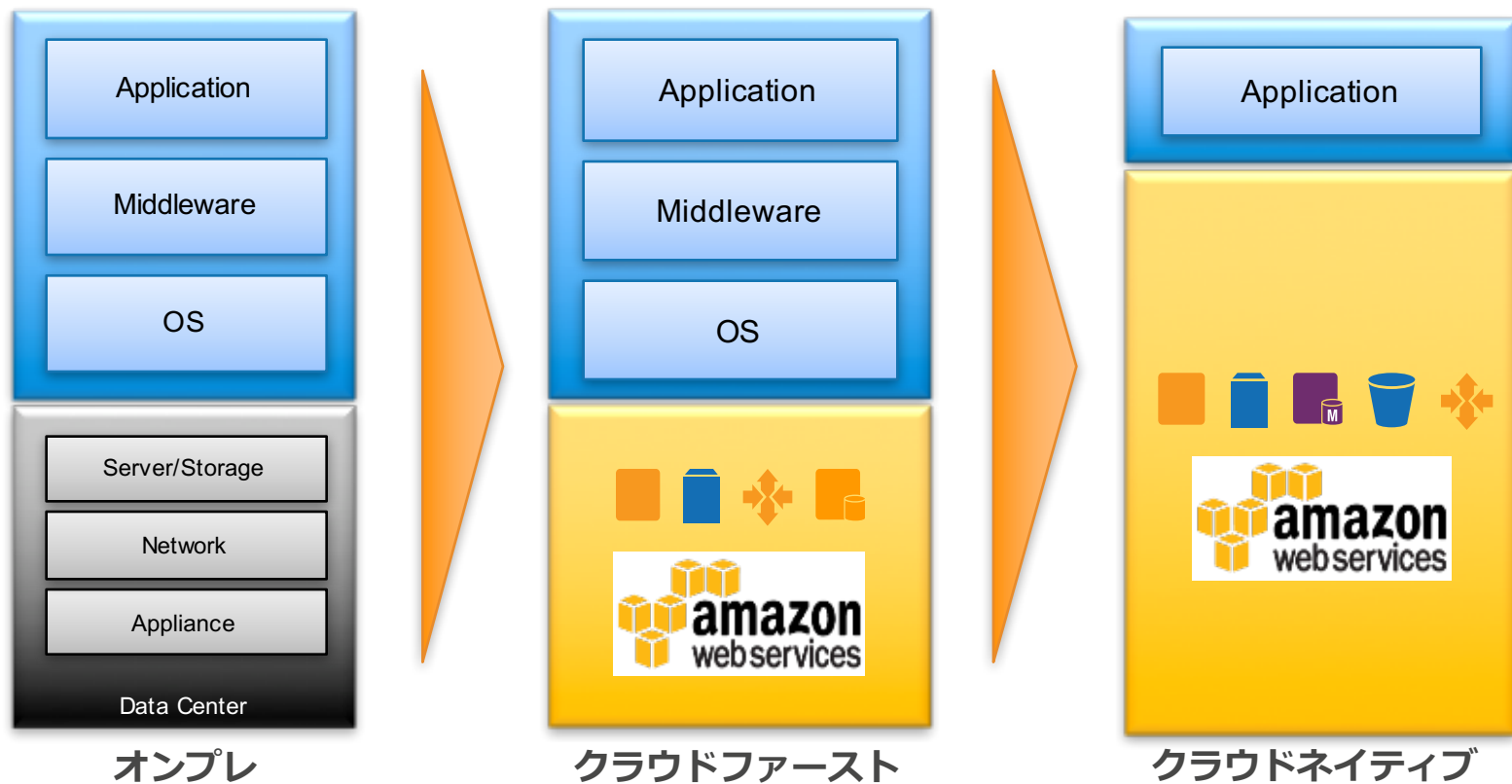
 ライブラリ & SDKs Java, PHP, .NET, Python, Ruby	 管理インターフェイス Management Console, CLI	 認証とログ IAM, Cloud Trail, Cloud HSM, Config	 ディレクトリ Directory Service	 モニタリング Cloud Watch, Trusted Advisor	 コード管理 CodeDeploy, CodeCommit, CodePipeline	 デプロイと自動化 Elastic Beanstalk, Cloud Formation, OpsWorks
--	--	---	--	---	--	---

**エンタープライズアプリケーション**
WorkSpaces, WorkDocs, WorkMail**モバイルサービス**
Mobile Analytics, Cognito, SNS

サーバー、ストレージ、DBから、アプリケーションまで
70を超えるクラウドサービスを提供

**EC2, Auto Scaling, Lambda**
Elastic Load Balancing, EC2 Container Service**EBS, S3, Glacier, Storage Gateway****コンテンツ配信**
CloudFront**ネットワーク**
VPC, Route 53, Direct Connect**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

クラウドネイティブ化による本業集中への変遷イメージ



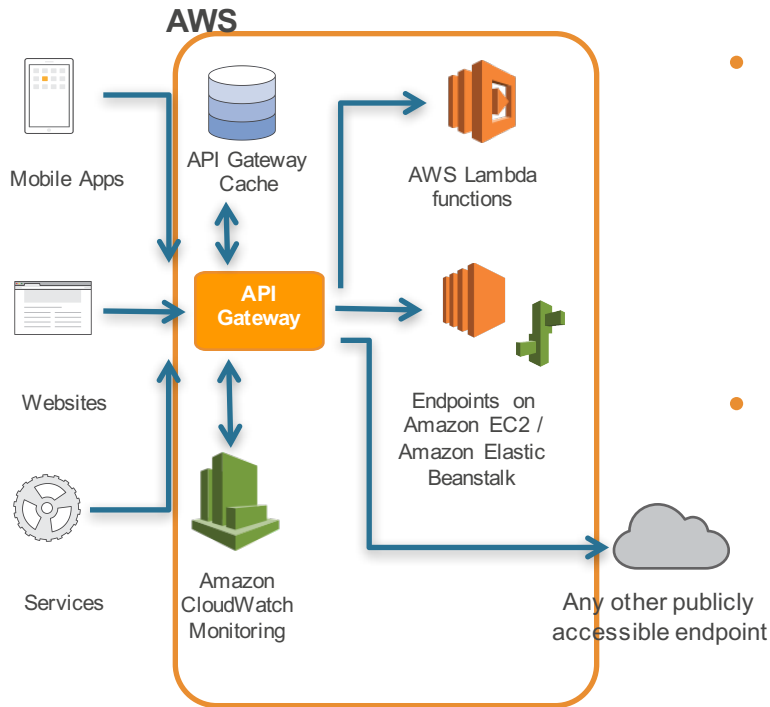
A close-up photograph of a child's hand, wearing a white sleeve, placing a blue LEGO brick onto a structure. The structure is composed of various colored bricks: red, yellow, green, and grey. The background is a light-colored, textured surface.

AWSサービスの本質はビルディングブロック。
サービスを組み合わせることで、
素早くアプリケーション構築が可能

Amazon API Gateway



Web APIの作成・保護・運用と公開を簡単に



- **特徴** (<http://aws.amazon.com/jp/lambda/>)
 - OS、キャパシティ等インフラの管理不要
 - バックエンドとしてLambda、既存Webシステムを利用可能
 - スロットリング/キャッシュ
- **価格体系** (<http://aws.amazon.com/jp/lambda/pricing/>)
 - 呼び出し回数とキャッシュ容量
 - 100万回の呼び出しにつき\$3.5
 - キャッシュ容量に応じて\$0.02/時～\$3.8/時

Amazon API Gateway



提供するAPIのバージョン管理



API利用状況のモニタ、管理とマネタイズ



APIに対する認証とアクセス権の管理



トラフィック管理とAPIエンドポイントの攻撃からの保護



インフラのセットアップおよび管理とメンテナンス

スロットリング

- メソッド単位でのスロットリングを提供
 - ステージ単位で全体的に同一設定にすることも、個々のメソッドに対して個別に設定することも可能
 - スロットリングによりバックエンドのパフォーマンスと可用性を維持
 - 許容するリクエスト/秒を指定
 - バーストを許容する設定も可能
 - トークンバケットアルゴリズムによる実装
- リミットを超えたリクエストがスロットリングされる
 - HTTPステータス429(Too many request)をレスポンス
 - 生成したSDKを使う場合、自動でリトライする

レスポンスのキャッシング

- レイテンシ減とバックエンドへのトラフィック軽減
 - キャッシュがあった場合、バックエンドを呼び出すことなくレスポンス
- ステージ単位のキャッシュプロビジョニング
 - 0.5GBから最大237GBの間でプロビジョニング
- 細やかな設定
 - メソッド単位で暗号化とTTLを設定
 - クエリパラメータ、ヘッダ、パスパラメータ単位でキャッシュ有無を設定
- キャッシュアルゴリズムはLRU (Least Recently Used)



AWS Lambda

イベントをトリガーにコードを実行するコンピュータサービス

1

インフラ管理不要



ビジネスロジックにフォーカスできる
コードをアップロードするだけで、あ
とはAWS Lambdaが以下をハンドリ
ング

2

高いパフォーマンス



イベントのレートに合う
ようにLambdaが自動で
スケール

3

細やかな料金

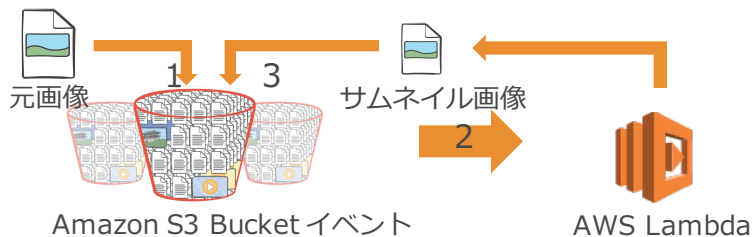


100ミリ秒単位でのコンピュー
ト時間に対する価格設定

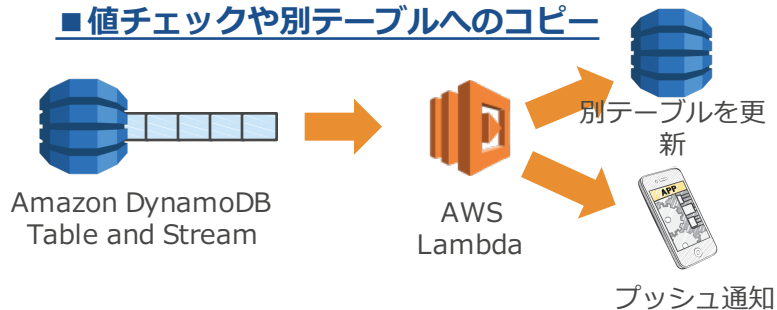
AWS Lambda

サービスの組み合わせ

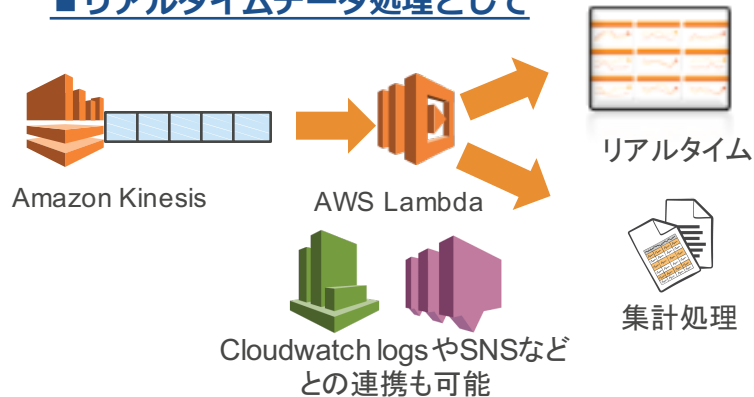
■ イメージのリサイズやサムネイルの作成



■ 値チェックや別テーブルへのコピー



■ リアルタイムデータ処理として



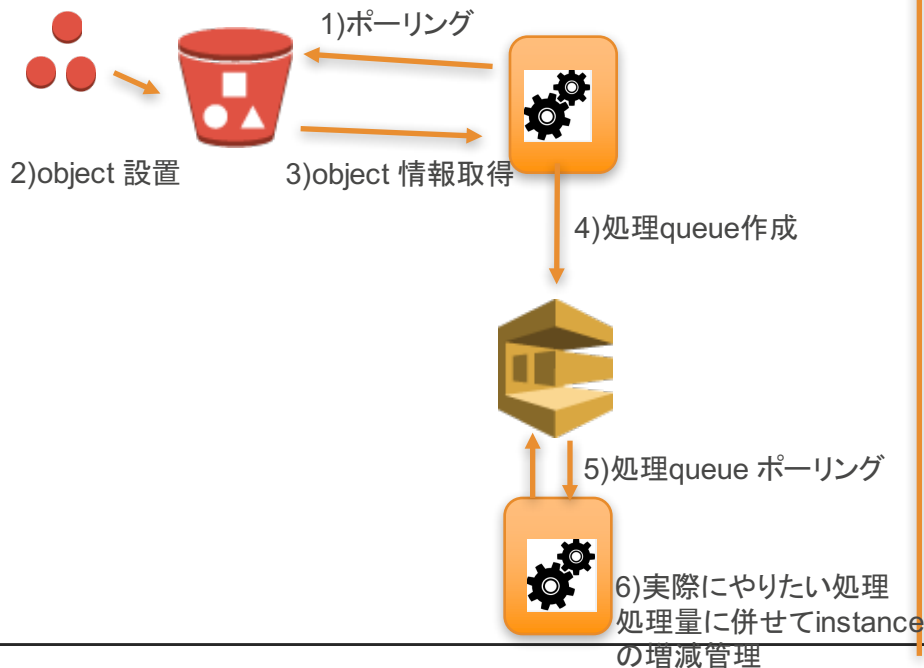
■ SWF Workerとして (バッチジョブフローのタスクとして)



従来型アーキテクチャとAWS Lambdaの比較

S3へファイルアップロードされたら解析するようなユースケース

従来型アーキテクチャ



AWS Lambda



EC2インスタンス不要

- ・EC2 コスト

- ・監視

- ・リアルタイム性の向上

従来型アーキテクチャの6)のコードのみ

- ・コード圧縮可能

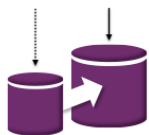
Amazon Relational Database Service (RDS)



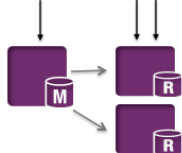
フルマネージドRDBMSサービス

	可用性	スループット増	レイテンシ
スケールアップ		✓	
Multi AZ	✓		
リードレプリカ		✓	
プロビジョンドIOPS		✓	✓

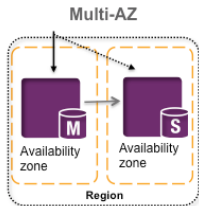
スケールアップ



リードレプリカ



プロビジョンド IOPS



特徴 [\(http://aws.amazon.com/jp/rds/\)](http://aws.amazon.com/jp/rds/)

- MySQL / PostgreSQL / Oracle DB / SQL Serverに対応
- 数クリックで構築可能で、バックアップやパッチの適用、フェイルオーバーは自動で行われる
- Oracle DB / SQL Serverのライセンスを従量課金モデルで利用可能 (Oracle DB: Standard Edition One / SQL Server: Express、Web、Standard Edition), Enterprise Editionなど他のエディションをBYOL可能
- Multi-AZ配置(SQL ServerはVirginia, Oregon, Irelandリージョン)により2つのAZにMasterを配置可能(Hot-Standby構成) / リージョン間でスナップショット自動転送も可能

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

- インスタンスタイプに応じて
- Oracle / SQL Serverはライセンスの時間課金
- ストレージ / バックアップストレージは利用量に応じて。Multi-AZ配置を利用の場合料金表記載の料金

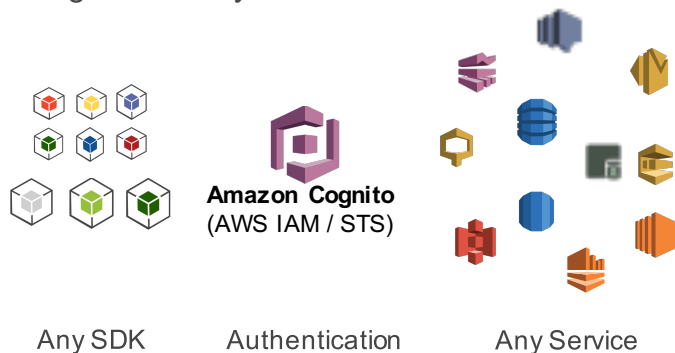


Amazon Cognito



アイデンティティの管理とクロスプラットフォームなデータ同期

■ Cognito Identity : AWSサービスへのゲートウェイ



■ Cognito Sync : クロスデバイスなデータ同期



特徴

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

- 複数のIDプロバイダや独自認証基盤との連携したユニークなアイデンティティの作成・管理
- クロスプラットフォーム、クロスデバイスでのデータ同期
- セキュリティのベストプラクティス実装を実現

価格体系

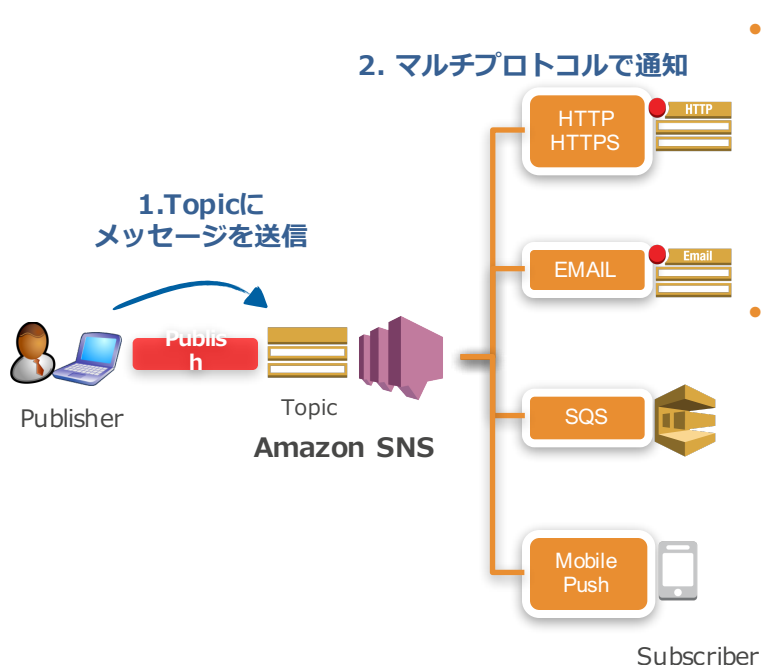
(<http://aws.amazon.com/jp/cognito/pricing/>)

- 無料利用枠
 - ・ 月あたり100万回の同期オペレーション
 - ・ 月あたり10GBのデータストア
 - ・ 最初の12ヶ月のみ
- それ以降
 - ・ 10000回の同期オペレーションあたり\$0.15
 - ・ 同期用データストアの容量：\$0.15/GB

Amazon Simple Notification Service (SNS)



マルチプロトコルに対応したフルマネージド通知サービス



特徴

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

- 個々のメッセージ送信や、多数の受信者にメッセージをファンアウトすることが可能
- AWSの様々なサービスと連携して通知可能
- フルマネージドなので高速かつスケーラブルで管理不要で非常に安価

価格体系

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

- 無料枠:
 - Email/Email-JSON: 1,000件
 - HTTP/HTTPS: 100,000件
 - Simple Queue Service (SQS) : 無料
- リクエスト単価(64KBのチャック毎に1リクエストとして課金)
 - Email/Email-JSON: 100,000件あたり2 USD
 - HTTP/HTTPS: 100万件あたり0.6 USD
 - Simple Queue Service (SQS) : 無料

Amazon Mobile Analytics



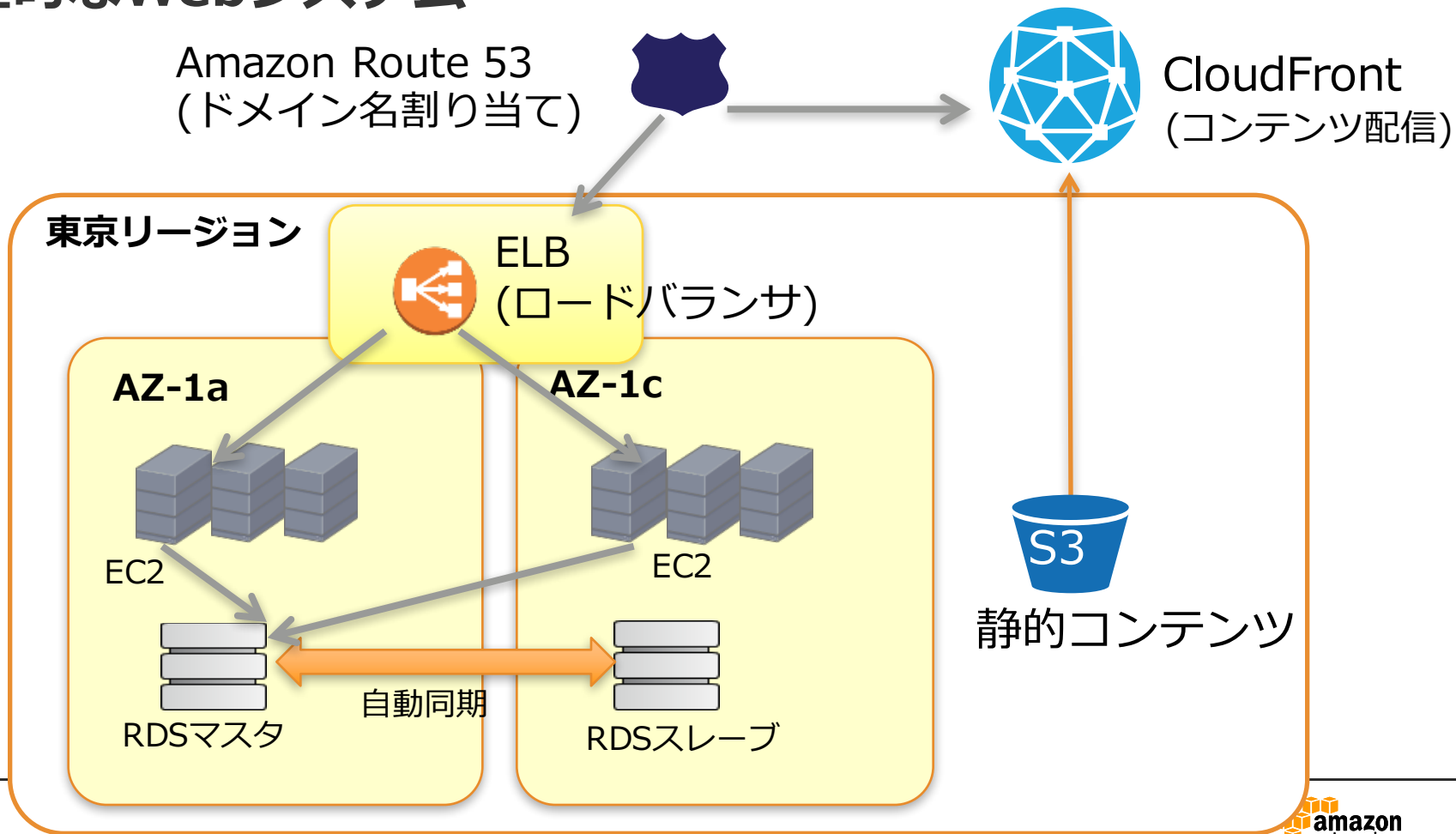
モバイルのためのスケーラブルなデータ収集と可視化



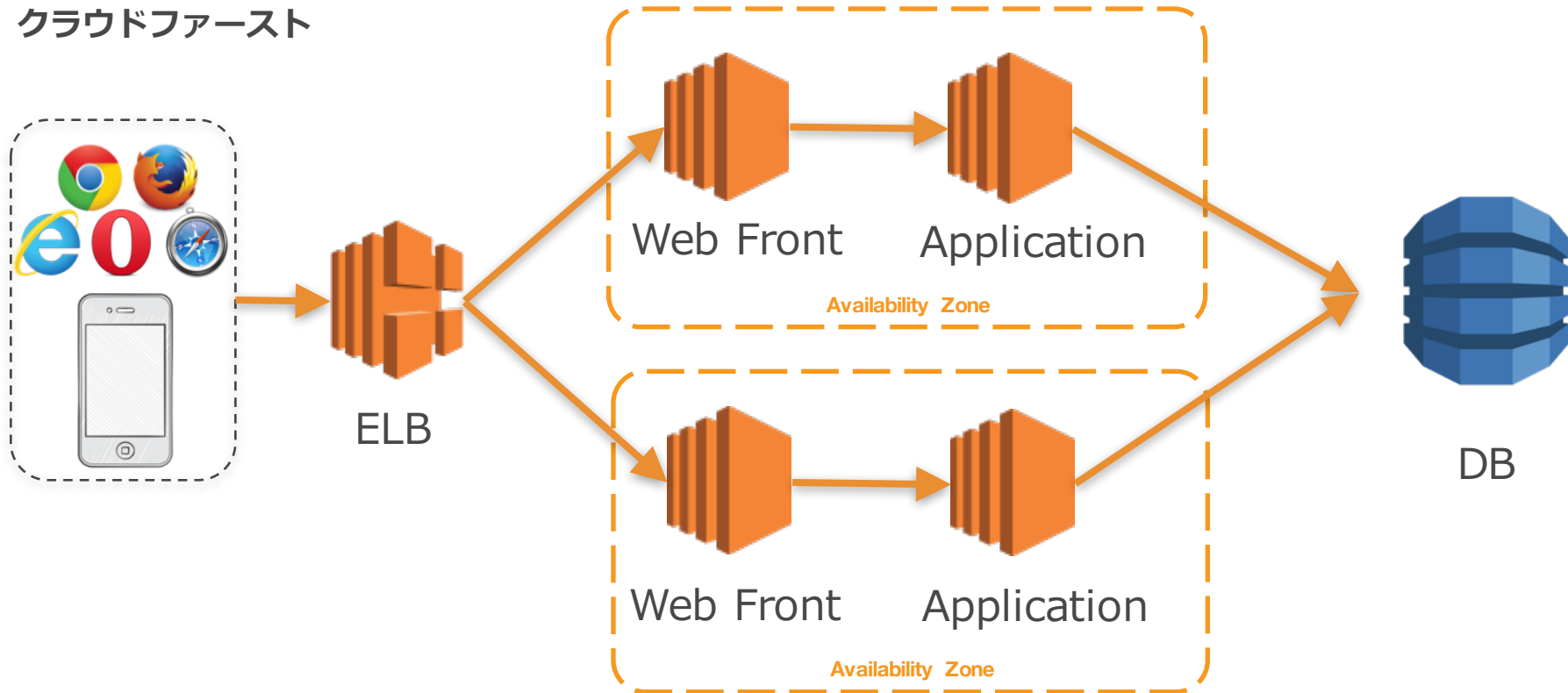
- **特徴** (<http://aws.amazon.com/jp/mobileanalytics/>)
 - モバイルアプリの利用状況データを大規模に収集、可視化して把握することが可能
 - 高速、スケーラブルでクロスプラットフォーム
 - S3、Redshiftへ生データを自動エクスポート
- **価格体系** (<http://aws.amazon.com/jp/mobileanalytics/pricing/>)
 - 収集するイベント数による課金
 - 無料枠
 - 月あたり1億イベントまで
 - それ以降
 - 月あたり100万イベントにつき\$1

従来型のサーバデザインと サーバレスアーキテクチャデザイン

典型的なWebシステム



クラウドファースト



認証・認可機能、スロットリング、コンテンツ配信、スケーリング、キャッシュ機構など



クラウドネイティブ

静的コンテンツ



認証機構



AIP定義
スロットリング設定
WebFront



ファンクション



DB
NoSQL DB



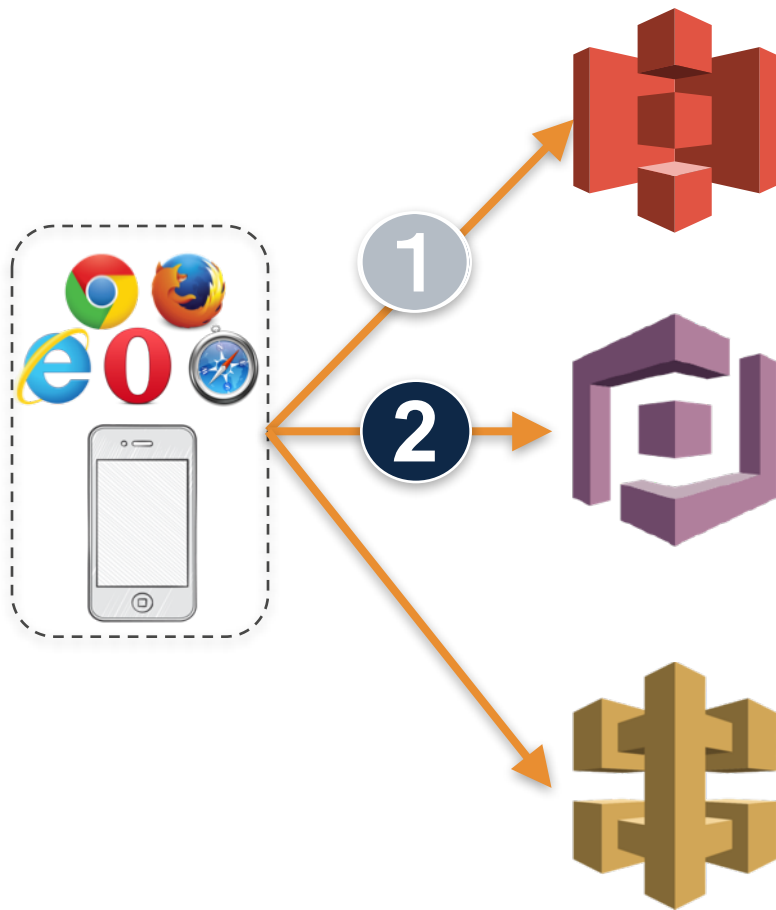


1



① S3のStaticWebsiteにアクセス

- S3の静的ウェブサイトホスティング機能でホストされたHTML, JS, CSSにアクセス。
以降は全てAjaxで処理する。

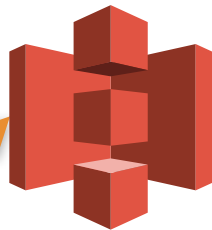


② Cognitoから認証情報取得

- AWSのリソースにアクセスするための一時的な認証情報をCognitoから取得。



1



2



3

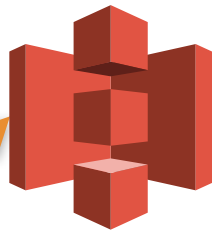


③ AjaxでAPI Gatewayを叩く

- Cognitoから取得した認証情報をを用いる。
- 新規コメント投稿や投稿内容の取得を行う。



1



2



3

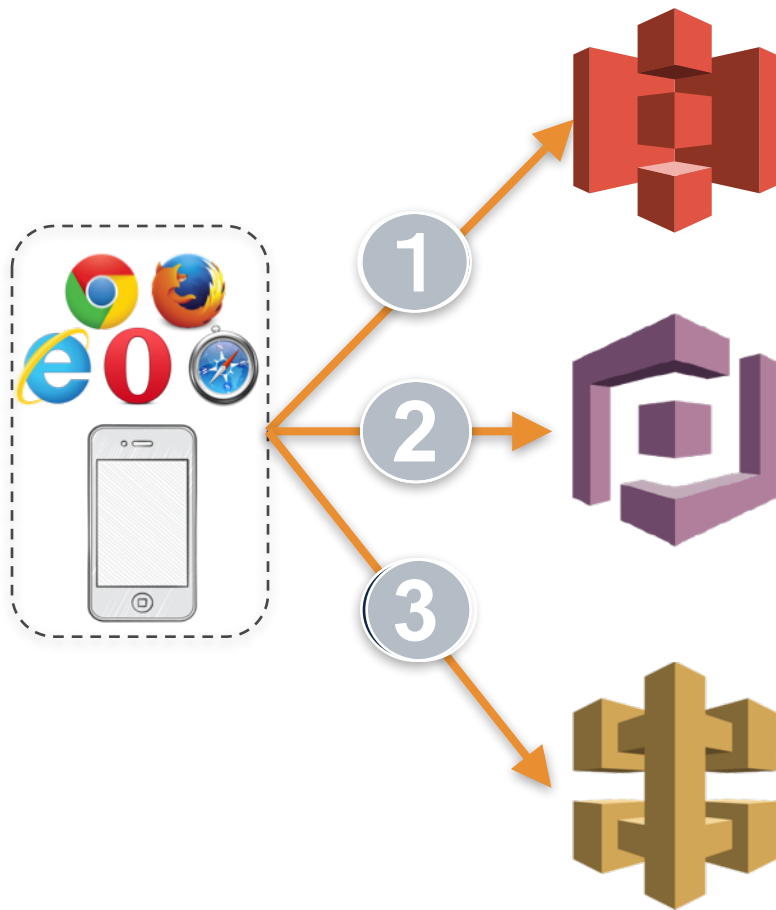


④ APIがLambdaをキック

- LambdaでDynamoDBにアクセスし、情報の登録/取得を行う。
- No servers.

4



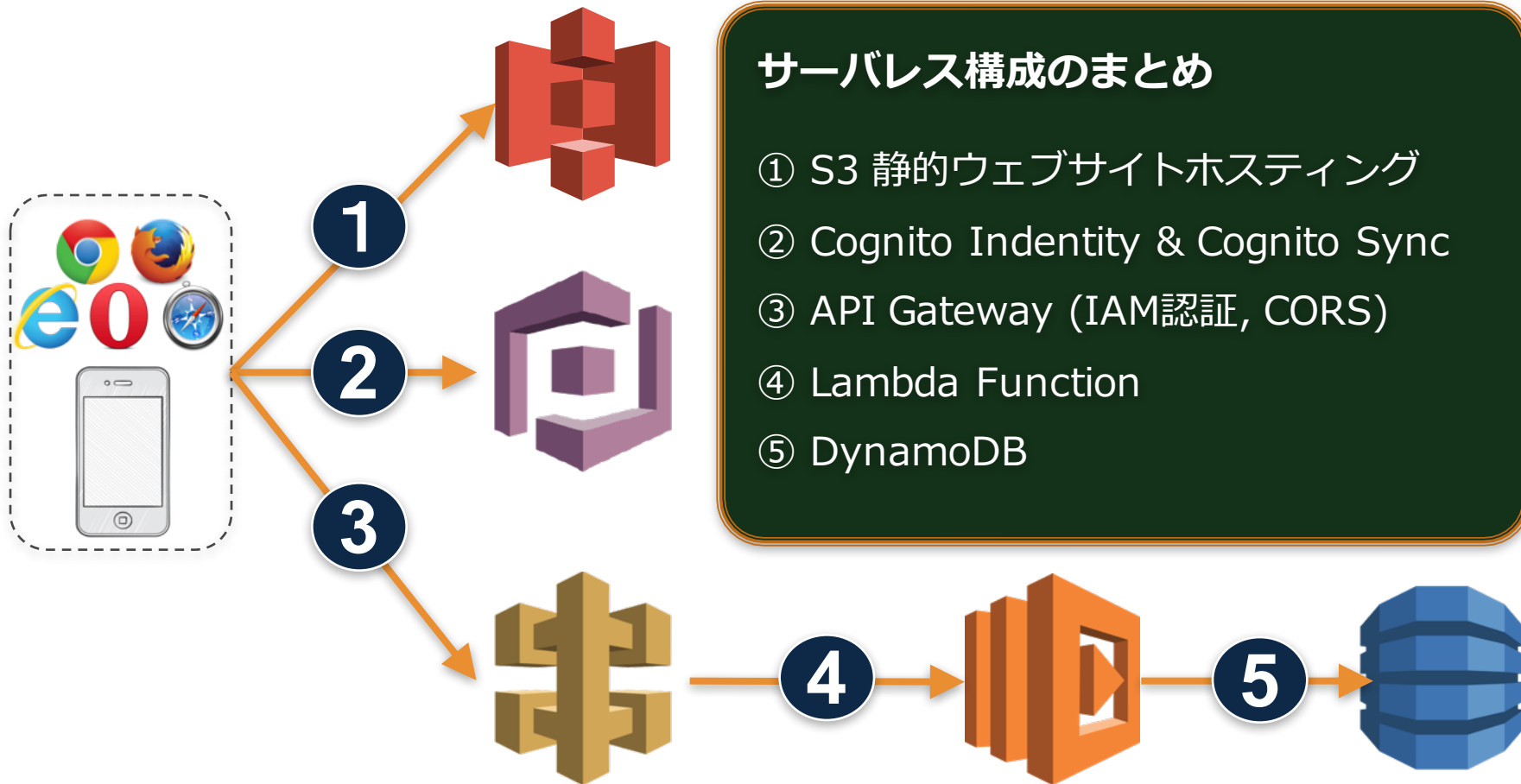


⑤ LambdaでDynamoDBを操作

- 情報の取得と更新を行う。

サーバレス構成のまとめ

- ① S3 静的ウェブサイトホスティング
- ② Cognito Identity & Cognito Sync
- ③ API Gateway (IAM認証, CORS)
- ④ Lambda Function
- ⑤ DynamoDB



まとめ

- サーバレスアーキテクチャ

- サーバがなくなるわけではなく、お客様自身がサーバ/インスタンスを管理する必要がなくなる
 - アプリケーション作成
 - API設計
に集中頂くことが可能
- 導入のポイント
 - REST API
 - ステートレス
 - 新しい技術に対する検討
 - 管理
 - テスト
など

