

これだけでOK!

AWS認定クラウドプラクティショナー

試験突破講座



はじめに



本講座のゴール

本講座だけでプラクティショナー試験に合格するための
知識と経験を獲得します！



本講座のコンセプト

理論と実践とテストを組合わせることで学習効果を最大化する



市販の書籍等との比較

書籍などと比較して網羅的に十分な学習範囲をカバー

市販の書籍

- 試験範囲が不足している。
- 試験問題が易しいため、実際の問題に対応できない。
- AWSの更新に対応できない。



本講座

- 試験範囲が網羅的である。
- 難易度が高めの問題にも対応できる内容を提供
- AWSの更新に応じてコンテンツを刷新



市販の書籍等との比較

書籍などと比較して網羅的に十分な学習範囲をカバー

コンピューティング	ストレージ	ネットワーキング	データベース	セキュリティ
<ul style="list-style-type: none">■ EC2■ Lambda■ Lightsail■ Amazon ECS	<ul style="list-style-type: none">■ S3■ EBS■ EFS■ Glacier	<ul style="list-style-type: none">■ VPC■ Route53■ CloudFront■ Direct Connect■ API Gateway■ AWS Storage Gateway	<ul style="list-style-type: none">■ RDS■ Aurora■ DynamoDB■ ElastiCache■ Redshift	<ul style="list-style-type: none">■ IAM■ GuardDuty■ Inspector■ KMS■ CloudHSM■ WAF■ Shield■ Artifact
マネジメント	アプリ統合	移行と移転	AWSコスト管理	その他
<ul style="list-style-type: none">■ CloudWatch■ CloudTrail■ Config■ Organizations■ AWS Personal Health Dashboard■ Service Catalog■ Well Architected tool■ AWS Systems Manager■ AWSサポート	<ul style="list-style-type: none">■ SNS■ SQS■ SNS	<ul style="list-style-type: none">■ AWS ADS■ AWS DMS■ AWS SMS■ AWS Snow ファミリー	<ul style="list-style-type: none">■ Cost Explorer■ AWSのコストと 使用状況レポート■ AWS Budgets■ 価格算定ツール■ Cost Categories■ Trusted Advisor	<ul style="list-style-type: none">■ CodeCommit■ CodeBuild■ CodeDeploy■ CodePipeline■ Elastic BeansStalk■ OpsWorks■ Kinesis■ CloudFormation



講座の内容

セクション	セクションで学ぶ内容
プラクティショナー試験を知る	実際にプラクティショナー試験問題を受けていただき、その試験範囲を確認します。
クラウドとAWSの概要	AWSクラウドとAWSの基本的な概念や仕組みを学習して、試験に出題されるAWSサービスの全体像を把握します。
AWSのコアサービス 1	AWSのメインのサービスであるEC2インスタンスとVPCとRoute53を学習し、クラウドサーバーによるWEBサイト構築を体験します。
AWSのコアサービス 2	AWSの設計原則を学習し、ELBとAutoScalingによる冗長構成を実際に構築します。
AWSのコアサービス 3	S3とRDSというデータ保存・処理を実行するサービスを学習して、実際に操作します。



講座の内容

セクション	セクションで学ぶ内容
AWSのコアサービス4	IAMとCloudTrailとCloudWatchといった運用管理に利用するサービスを学習します。
AWSコスト管理	AWSのコスト管理サービスの概要を理解した上で、様々なツールを操作していただきます。
試験範囲に出てくる その他のサービス	コアサービス以外で、そのサービス内容が出題される可能性があるAWSサービスを網羅的に学習します。
模擬試験問題	本番レベルの模擬試験問題を2回分実施して、実力を確認します。

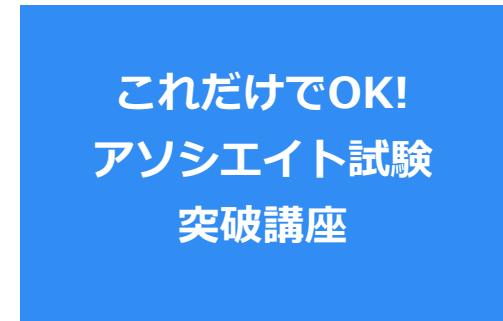


他の講座との関連

超初心者の基礎知識を固めたい方向け



さらに知識を深めたい方向け



もっと問題を解きたい人向け



AWSの利用料について

本講義のレクチャーを実施するとAWSの利用料金が発生しますが、極力最低コストになるように進めます。

無料枠の利用	<p>EC2・S3・VPCなどの基本機能は無料枠を利用してレクチャーを進めます。EC2とS3は長時間利用すると有料化しますが、適時削除して無料枠で利用します。</p>
最小コスト構成による 料金の最小化	<p>RDSは有料ですが、レクチャー直後に削除しますので極力課金を抑制します。（100円前後）</p>



次に本番レベルのプラクティショナー試験を体験して
合格レベルを確認しましょう！！

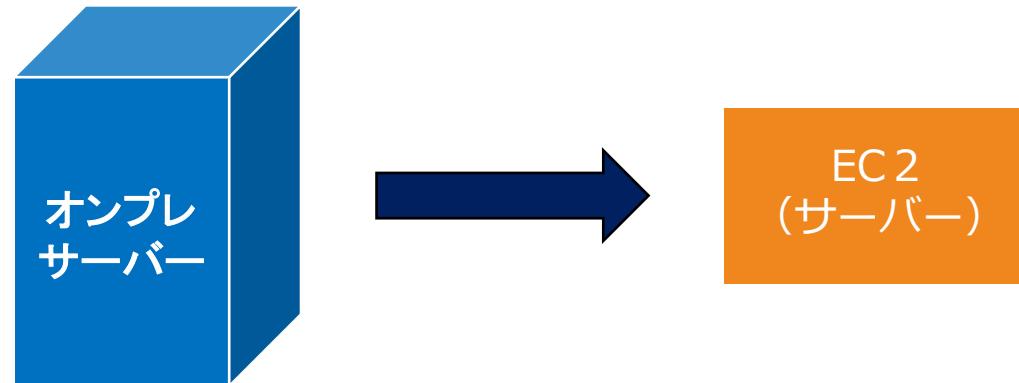


AWSとは何か？



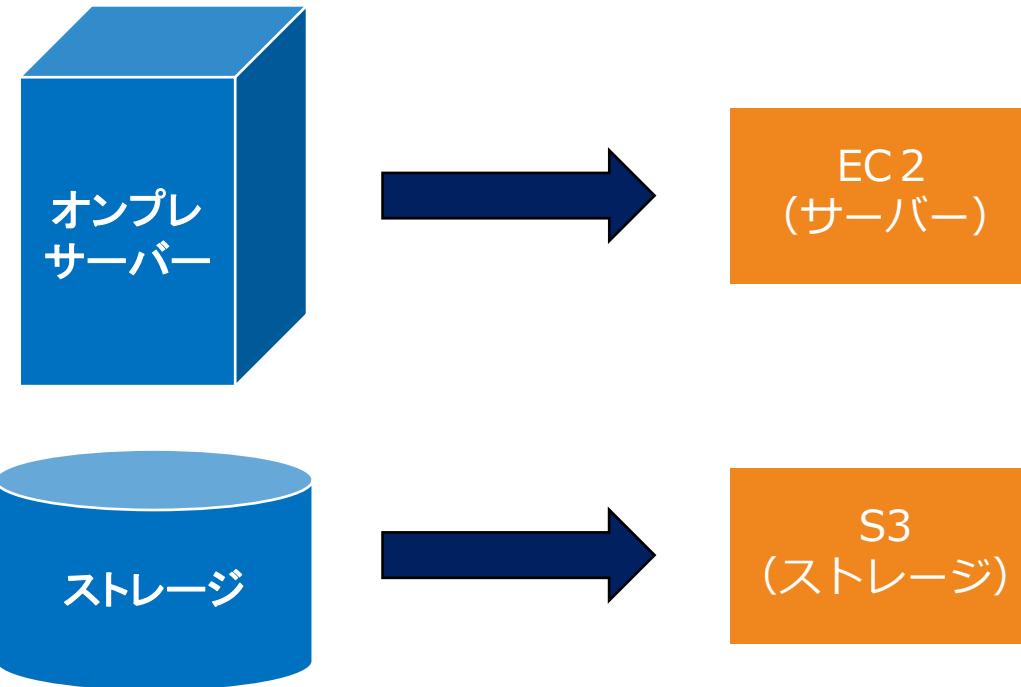
AWSとは

インフラやアプリ開発に必要な機能がいつでも、どこでも即時に利用できるサービス



AWSとは

AWSを利用すればサーバー、ストレージ、データベースなどのインフラを即時に利用することが可能

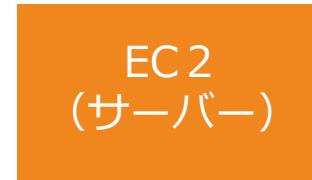


AWSとは

サーバーを立ち上げるのに数分で無料で今すぐ利用できることが大きな特徴



- ✓ 時間がかかる
- ✓ コストがかかる

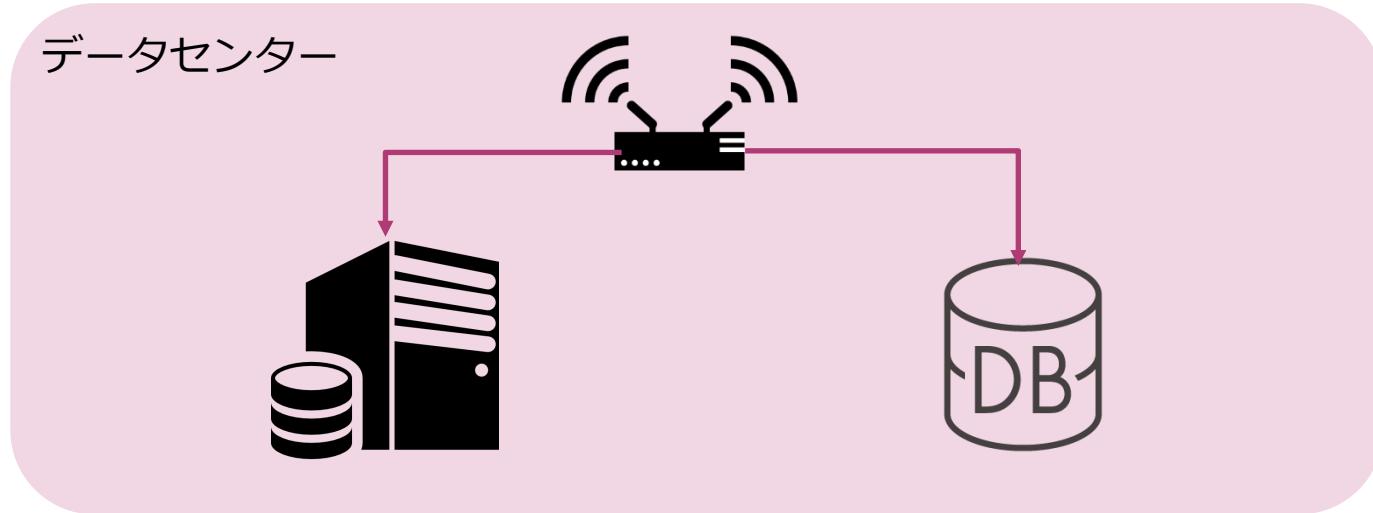


- ✓ 数分で立ち上がる
- ✓ 無料から利用可能



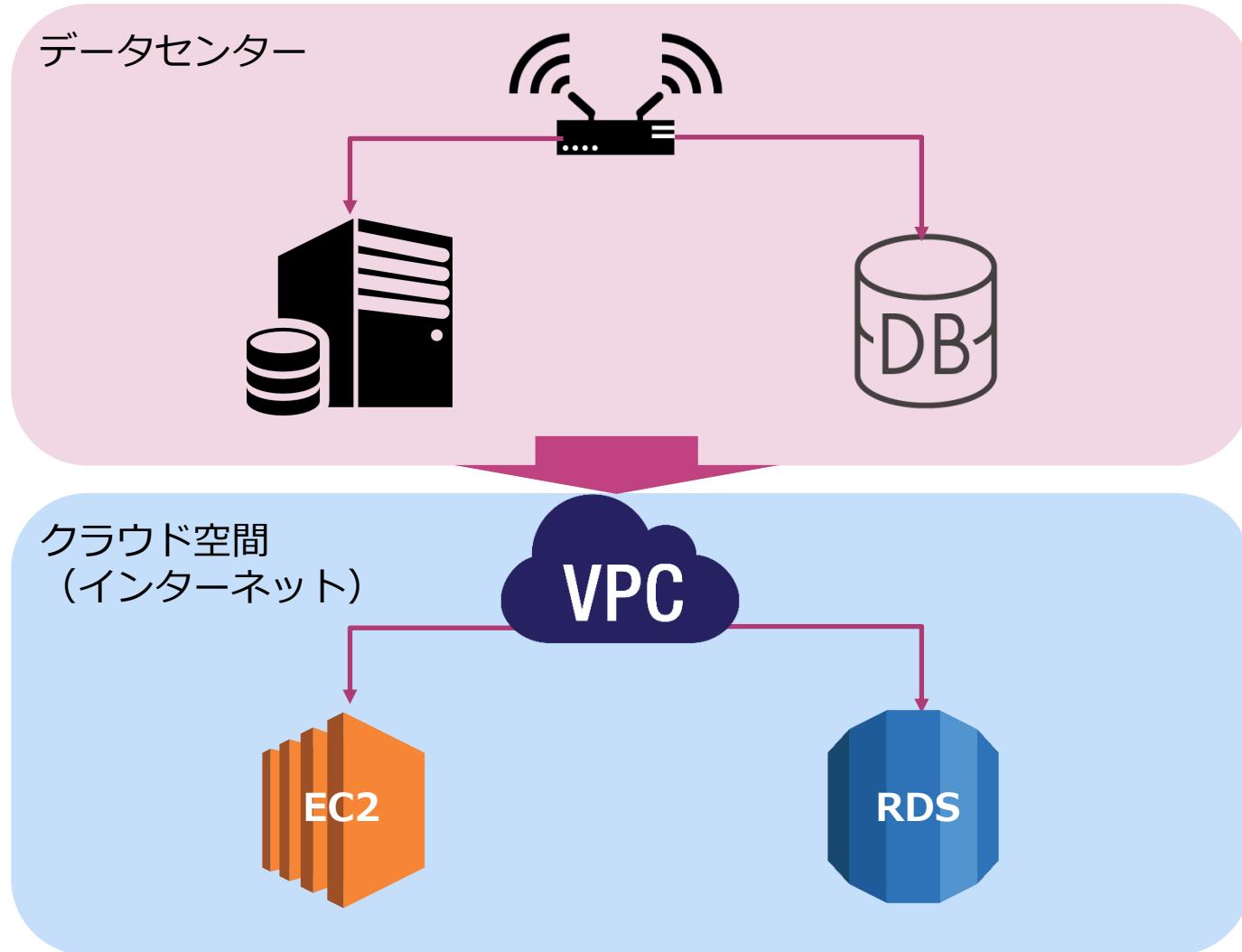
物理的な機器をネットサービスへ

システム運用に必要な物理機器をインターネット経由で借りて
くることで、効率的なシステム管理が可能になる。



物理的な機器をネットサービスへ

システム運用に必要な物理機器をインターネット経由で借りて
くることで、効率的なシステム管理が可能になる。



サービスが豊富

システム構築・運用に必要なサービスが一通りそろっており、185以上のサービスから容易に組み合わせて利用できる。

コンピューティング	ストレージ	ネットワーキング	データベース	セキュリティ
<ul style="list-style-type: none">■ EC2■ Lambda■ Lightsail■ Fargate	<ul style="list-style-type: none">■ S3■ EBS■ EFS■ Glacier■ Amazon FSx for windows■ Amazon FSx for Lustre	<ul style="list-style-type: none">■ VPC■ Route53■ CloudFront■ Direct Connect■ API Gateway■ AWS Storage Gateway	<ul style="list-style-type: none">■ RDS■ Aurora■ DynamoDB■ ElastiCache■ Redshift■ Neptune■ ElasticSearch■ CloudSearch	<ul style="list-style-type: none">■ IAM■ GuardDuty■ Inspector■ KMS■ CloudHSM■ WAF■ Shield■ Artifact
マネジメント	アプリ統合	移行と移転	AWSコスト管理	その他
<ul style="list-style-type: none">■ CloudWatch■ CloudTrail■ Config■ Organizations■ AWS Personal Health Dashboard■ Service Catalog■ Well Architected tool■ AWS Systems Manager■ AWSサポート	<ul style="list-style-type: none">■ SNS■ SQS■ SNS■ MQ	<ul style="list-style-type: none">■ AWS ADS■ AWS DMS■ AWS SMS■ AWS Snow ファミリー	<ul style="list-style-type: none">■ Cost Explorer■ AWSのコストと使用状況レポート■ AWS Budgets■ 価格算定ツール■ Cost Categories■ Trusted Advisor	<ul style="list-style-type: none">■ CodeCommit■ CodeBuild■ CodeDeploy■ CodePipeline■ ElasticBeansStalk■ OpsWorks■ Amazon ECS■ Kinesis■ CloudFormation

最先端の技術

AI・ブロックチェーン・量子コンピューター・AR・VRなどの最先端技術がクラウドで提供され、すぐに利用できる

IoT

AI

ロボット

人工衛星

ブロック
チェーン

量子
コンピューター

ゲームテック

メディア
サービス

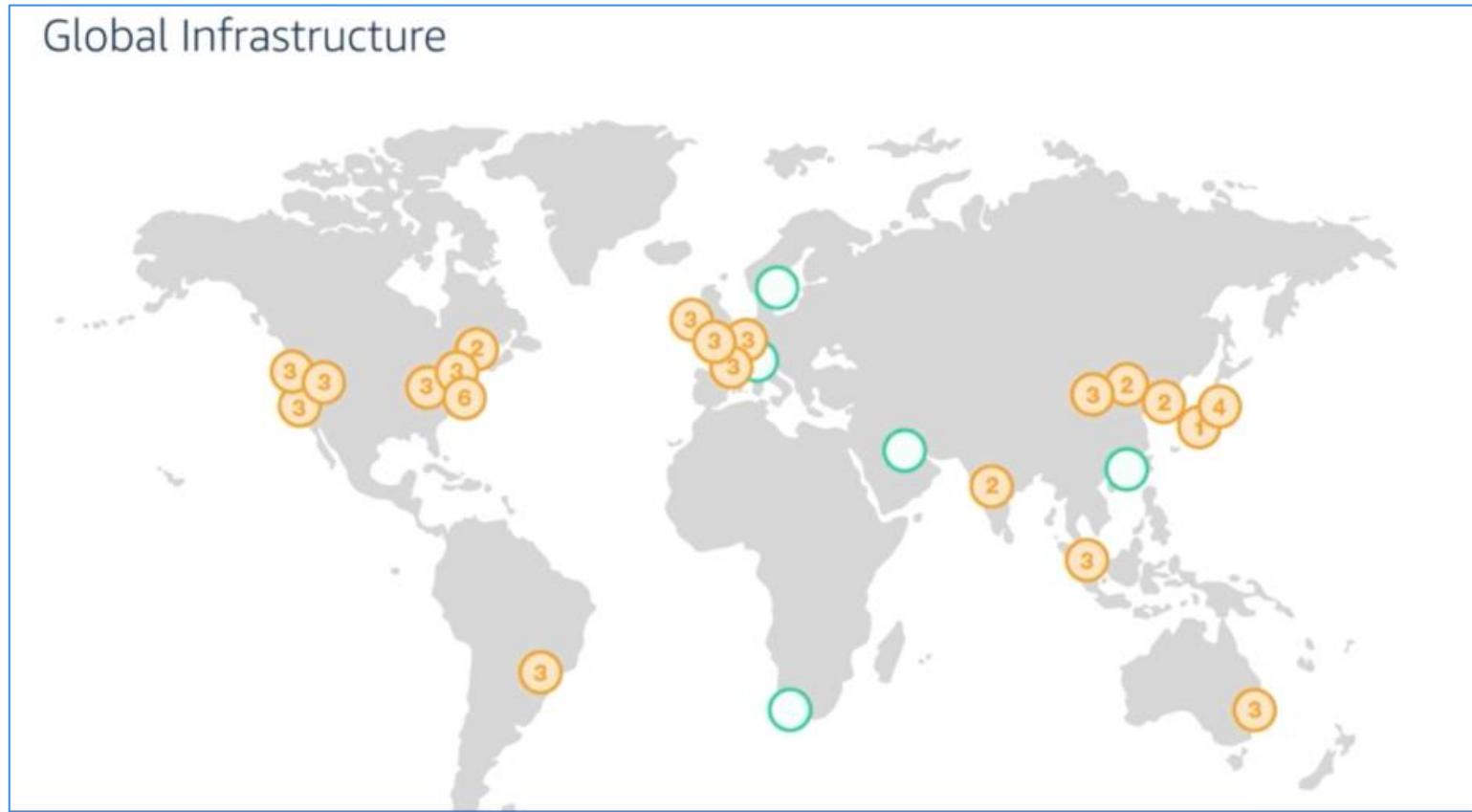
VR／AR

仮想
デスクトップ



グローバルに展開

グローバルにインフラを有しているため、日本にいながら世界中にインフラやシステムを構築できる。



AWSの資格体系



AWSの資格体系

AWS資格には基礎コース、アソシエイト、プロフェッショナル、専門知識の4つのカテゴリーがある。

Professional

Two years of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud



Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the exam guide



Foundational

Six months of fundamental AWS Cloud and industry knowledge

<https://aws.amazon.com/jp/blogs/big-data/upgrade-your-resume-with-the-aws-certified-big-data-specialty-certification/>



AWSの資格体系

AWS認定資格の取得レベルと理想的な取得順序

AWS認定ソリューション
アーキテクト
プロフェッショナル

AWS認定DevOps
エンジニア
プロフェッショナル

AWS認定SysOps
アドミニストレーター

AWS認定ソリューション
デベロッパー

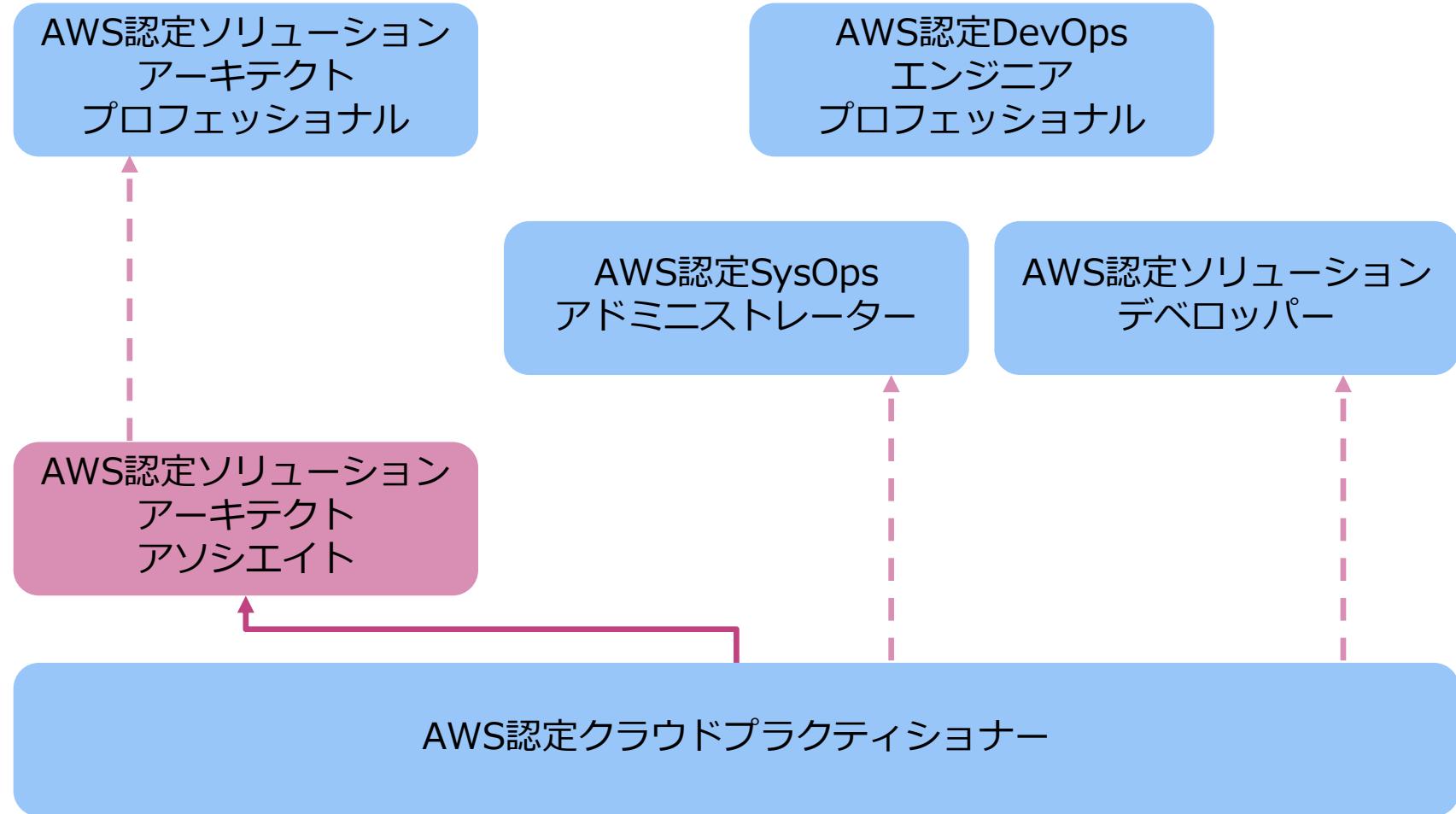
AWS認定ソリューション
アーキテクト
アソシエイト

AWS認定クラウドプラクティショナー



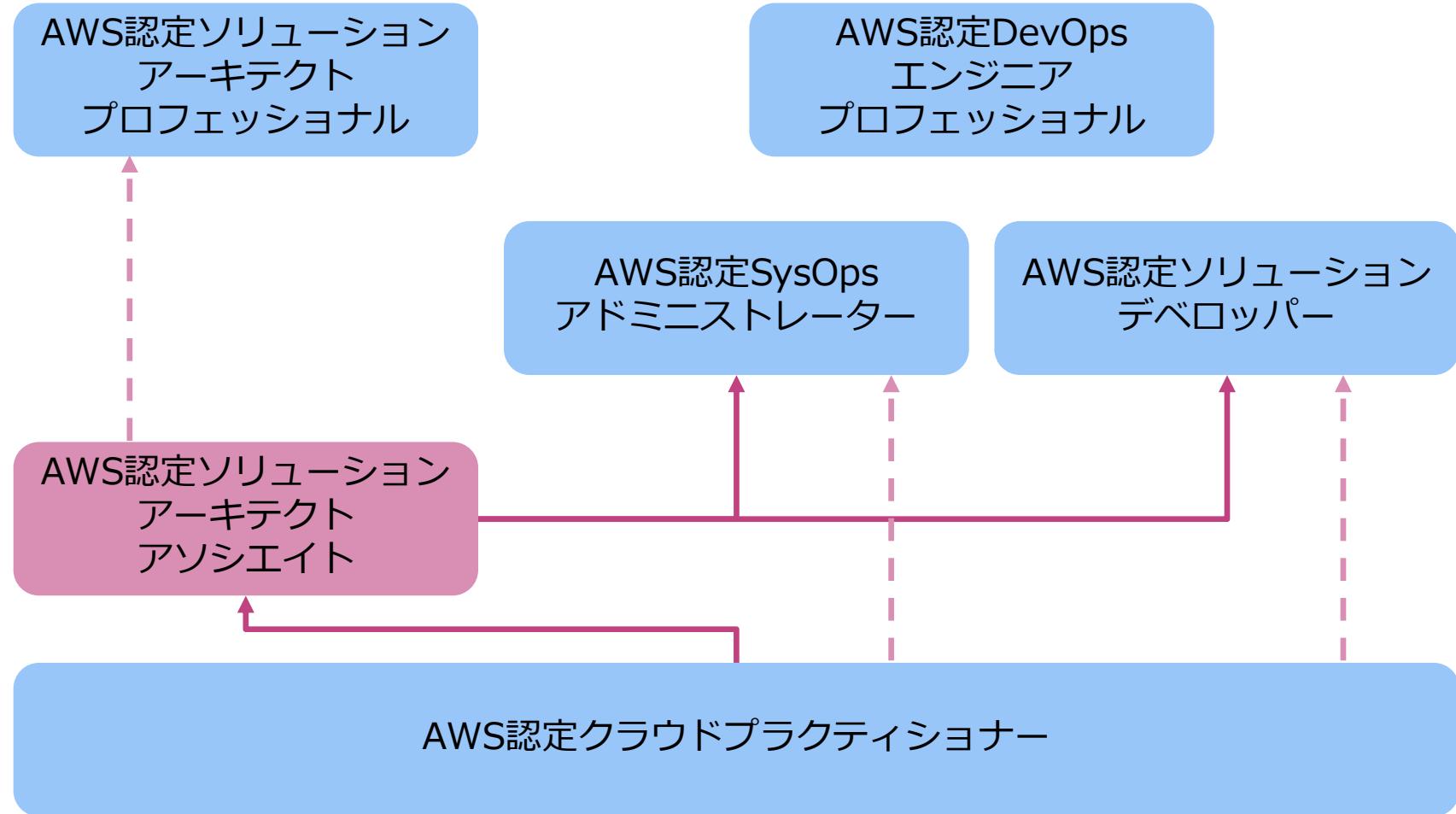
AWSの資格体系

AWS認定資格の取得レベルと理想的な取得順序



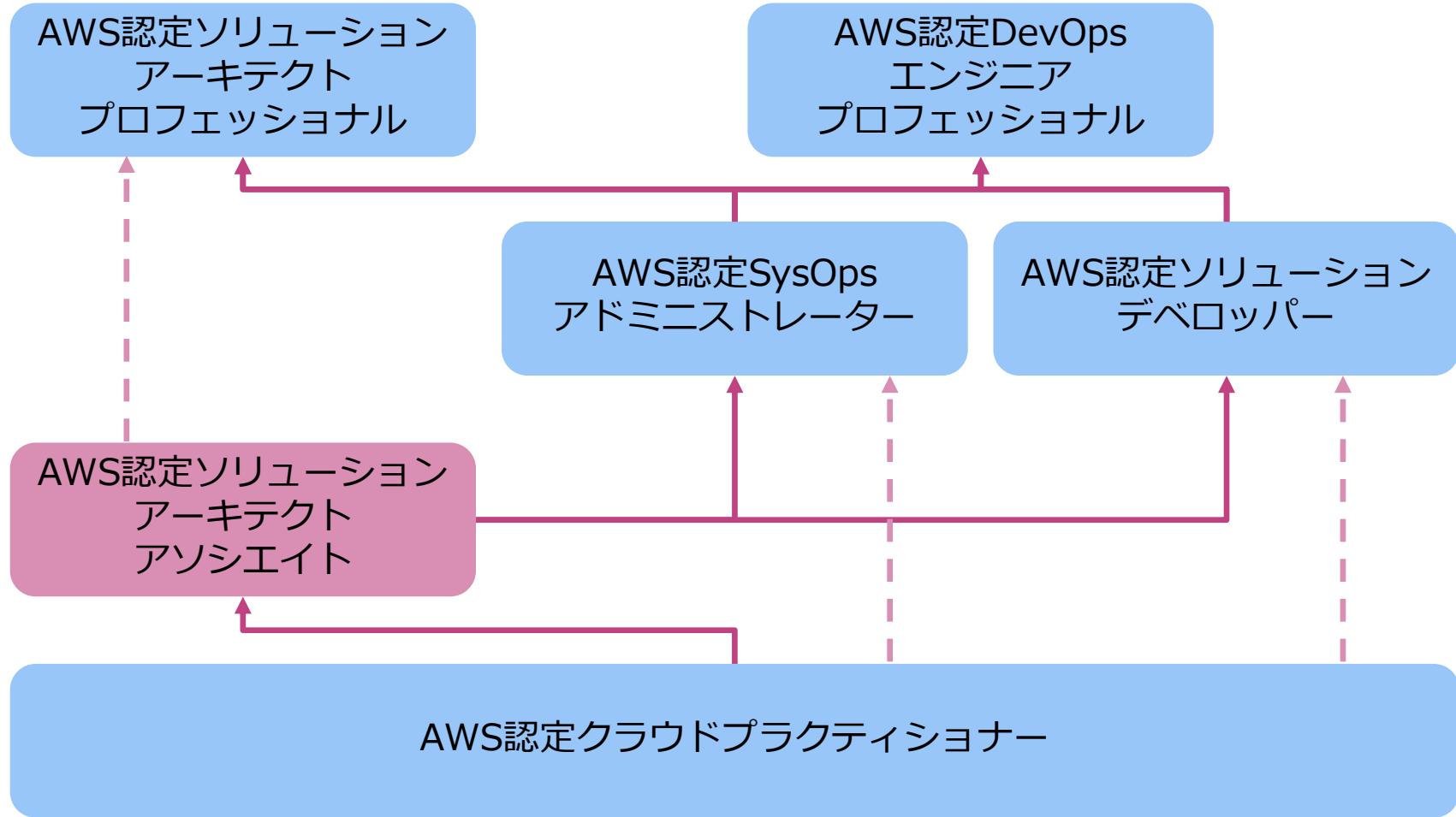
AWSの資格体系

AWS認定資格の取得レベルと理想的な取得順序



AWSの資格体系

AWS認定資格の取得レベルと理想的な取得順序



プラクティショナー 試験概要



プラクティショナーとは？

AWS クラウドの知識とスキルを身に付け、全体的な理解を効果的に説明できる個人向けのテスト

AWS 認定ソリューションアーキテクトなどのアソシエイト認定または専門知識認定を取得する前の基本知識の証明



試験内容

- 択一選択問題: 選択肢には 1つの正解と 3つの不正解
- 複数選択問題: 5つ以上の選択肢のうち、2つが正解



アソシエイト試験範囲 (SAA-C02)

試験分野	比率
分野 1 クラウドの概念	26%
分野 2 セキュリティ	25%
分野 3 テクノロジー	33%
分野 4 請求と料金	16%



分野1：クラウドの概念

- AWS クラウドの概念とその価値提案について説明する
- AWS クラウドエコノミクスの特徴を説明する
- 多種多様なクラウドアーキテクチャの設計原理を定義する



分野1：クラウドの概念

「AWS クラウドの概念とその価値提案について説明する」に関する問題

ユーザー側でオペレーティングシステムを管理する必要性を排除するクラウドコンピューティングモデルはどれですか？

- 1) PaaS
- 2) IaaS
- 3) SaaS
- 4) DaaS



分野1：クラウドの概念

ユーザー側でオペレーティングシステムを管理する必要性を排除するクラウドコンピューティングモデルはどれですか？

- 1) PaaS
- 2) IaaS
- 3) SaaS
- 4) DaaS

オプション1が正解となります。Platform as a Serviceにより、ユーザーは基盤となるインフラストラクチャ（通常はハードウェアとオペレーティングシステム）を管理する必要がなくなり、アプリケーションの展開と管理に集中できます。これにより、リソースの調達、キャパシティプランニング、ソフトウェアメンテナンス、パッチの適用、またはアプリケーションの実行に関する他の未分化の重い作業を心配する必要がなくなるため、より効率的になります。



分野 1：クラウドの概念

「AWS クラウドエコノミクスの特徴を説明する」に関する問題

コンピューティングワークロードが変動するアプリケーションにとって、AWS が従来型データセンターよりも経済的であるのはなぜですか。

- 1) Amazon EC2 の利用料金は毎月請求される。
- 2) ユーザーは常に、自分の Amazon EC2 インスタンスに対するフル管理アクセス権限を付与される。
- 3) Amazon EC2 インスタンスは、必要に応じて起動できる。
- 4) ユーザーは、ピーク時間帯のワークロードを処理するのに十分な数のインスタンスを常に実行できる。



分野1：クラウドの概念

コンピューティングワークロードが変動するアプリケーションにとって、AWS が従来型データセンターよりも経済的であるのはなぜですか。

- 1) Amazon EC2 の利用料金は毎月請求される。
- 2) ユーザーは常に、自分の Amazon EC2 インスタンスに対するフル管理アクセス権限を付与される。
- 3) **Amazon EC2インスタンスは、必要に応じて起動できる。**
- 4) ユーザーは、ピーク時間帯のワークロードを処理するのに十分な数のインスタンスを常に実行できる。

オプション3が正解となります。必要に応じてインスタンスを起動できるので、ユーザーは、ワークロードの変動に合わせてインスタンスを 起動および削除できます。この方法は、ピーク時間帯のワークロードを処理するのに十分な数のオンプレミスサーバーを購入する方法に比べ、より経済的です。



分野 1：クラウドの概念

「多種多様なクラウドアーキテクチャの設計原理を定義する」に関する問題

EC2インスタンスの障害対応力や負荷分散を実現するための冗長構成にするためには、ELBを利用して、どのアーキテクチャ設計を実現するべきでしょうか？

- 1) マルチAZ構成
- 2) マルチVPC構成
- 3) マルチリージョン構成
- 4) エッジロケーション分散構成



分野1：クラウドの概念

EC2インスタンスの障害耐性や負荷分散を実現するための冗長構成にするためには、ELBを利用して、どのアーキテクチャ設計を実現するべきでしょうか？

- 1) マルチAZ構成
- 2) マルチVPC構成
- 3) マルチリージョン構成
- 4) エッジロケーション分散構成

オプション1が正解となります。AWSのアベイラビリティゾーン (AZ) はリージョン内の単一または複数のデータセンターの塊です。複数のAZに跨ってサーバーを冗長構成とすることで、データセンター障害に強い負荷分散と障害耐性を実現することができます。



分野2：セキュリティ

- AWSの責任共有モデルについて理解する
- AWSクラウドのセキュリティとコンプライアンスに関するコンセプトを理解する
- AWSのアクセス管理機能を特定する
- セキュリティサポートのリソースを特定する



分野2：セキュリティ

「AWSの責任共有モデルについて理解する」に関する問題

AWS 責任共有モデルにおいて、AWS 側の責任である作業はどれですか。

- 1) サードパーティ製アプリケーションを構成する。
- 2) 物理ハードウェアを保守する。
- 3) アプリケーションアクセスとデータをセキュア化する。
- 4) ゲストオペレーティングシステムを管理する。



分野2：セキュリティ

AWS責任共有モデルにおいて、AWS 側の責任である作業はどれですか。

- 1) サードパーティ製アプリケーションを構成する。
- 2) **物理ハードウェアを保守する。**
- 3) アプリケーションアクセスとデータをセキュア化する。
- 4) ゲストオペレーティングシステムを管理する。

オプション2が正解となります。AWS責任共有モデルにおいて、物理ハードウェア保守作業は AWS側の責任です。



分野2：セキュリティ

「AWSクラウドのセキュリティとコンプライアンスに関するコンセプトを理解する」に関する問題

AWSクラウドのコンプライアンス情報を取得するためのリソースとして無関係なものはどれでしょうか？

- 1) AWS コンプライアンスページ
- 2) ホワイトペーパー
- 3) コンプライアンス関連のトレーニングプログラム
- 4) AWS Guard Duty
- 5) IAMポリシー



分野2：セキュリティ

AWS クラウドのコンプライアンス情報を取得するためのリソースとして無関係なものはどれでしょうか？

- 1) AWS コンプライアンスページ
- 2) ホワイトペーパー
- 3) コンプライアンス関連のトレーニングプログラム
- 4) AWS Guard Duty
- 5) IAMポリシー

オプション5が正解となります。 AWS Identity and Access Management (IAM) では、AWS のサービスやリソースへのアクセスを安全に管理できます。コンプライアンスに関する情報を取得するサービスではありません。



分野2：セキュリティ

「AWSのアクセス管理機能を特定する」に関する問題

システム管理者がユーザーの AWS Management Console にログインセキュリティレイヤーを追加するには、どうすればよいですか。

- 1) Amazon Cloud Directory を使用する。
- 2) AWS Identity and Access Management (IAM) ロールを監査する。
- 3) Multi-Factor Authentication (MFA) を有効化する。
- 4) AWS CloudTrail を有効化する。



分野2：セキュリティ

システム管理者がユーザーの AWS Management Console にログインセキュリティレイヤーを追加するには、どうすればよいですか。

- 1) Amazon Cloud Directory を使用する。
- 2) AWS Identity and Access Management (IAM) ロールを監査する。
- 3) **Multi-Factor Authentication (MFA) を有効化する。**
- 4) AWS CloudTrail を有効化する。

オプション 3 が正解となります。 Multi-Factor Authentication (MFA) は、ユーザー名/パスワードに加え、さらに保護レイヤーを追加するための、シンプルなベストプラクティスです。 MFA を有効化した場合、ユーザーは AWS Management Console にサインインする際に、ユーザー名とパスワード (1 番目の要素: ユーザーが知っている情報) と、ユーザーの MFA デバイスの認証コード (2 番目の要素: ユーザーが保有している情報) の入力を求められます。つまり、これら複数の要素によって、AWS アカウント設定と AWS リソースのセキュリティが強化されます。



分野2：セキュリティ

「セキュリティサポートのリソースを特定する」に関する問題

AWSインフラストラクチャ上で禁止されているアクションに関する情報は、どこで見つけることができますか。

- 1) AWS Trusted Advisor
- 2) AWS Identity and Access Management (IAM)
- 3) AWS Billing Console
- 4) AWS Acceptable Use Policy



分野2：セキュリティ

AWSインフラストラクチャ上で禁止されているアクションに関する情報は、どこで見つけることができますか。

- 1) AWS Trusted Advisor
- 2) AWS Identity and Access Management (IAM)
- 3) AWS Billing Console
- 4) AWS Acceptable Use Policy

オプション4が正解となります。AWS Acceptable Use Policy を読めば、AWS インフラストラクチャ上で禁止されているアクションに関する情報がわかります。



分野3：テクノロジー

- AWS クラウドにおけるデプロイと運用の方法を理解する
- AWS のグローバルインフラストラクチャについて理解する
- AWS の主要なサービスを識別する
- テクノロジーサポートのリソースを特定する



分野3：テクノロジー

「AWS クラウドにおけるデプロイと運用の方法を理解する」に関する問題

Amazon CloudWatch アラームに基づいてアラートを送信するには、どのサービスを使用すればよいですか。

- 1) Amazon Simple Notification Service (Amazon SNS)
- 2) AWS CloudTrail
- 3) AWS Trusted Advisor
- 4) Amazon Route 53



分野3：テクノロジー

Amazon CloudWatch アラームに基づいてアラートを送信するには、どのサービスを使用すればよいですか。

- 1) Amazon Simple Notification Service (Amazon SNS)
- 2) AWS CloudTrail
- 3) AWS Trusted Advisor
- 4) Amazon Route 53

オプション1が正解となります。Amazon SNSとAmazon CloudWatchは統合されています。ユーザーはCloudWatchを利用してAWSリソースのメトリクスを収集、表示、および分析できます。Amazon SNSをCloudWatchを設定して、Amazon SNSトピック、プッシュ通知、およびSMS配信を実施することが可能となります。

分野3：テクノロジー

「AWS のグローバルインフラストラクチャについて理解する」に関する問題

Amazon CloudFrontにおいて低レイテンシー配信を実現するために使用される、AWS グローバルインフラストラクチャのコンポーネントはどれですか。

- 1) AWS リージョン
- 2) エッジロケーション
- 3) アベイラビリティゾーン
- 4) VPC



分野3：テクノロジー

Amazon CloudFrontにおいて低レイテンシー配信を実現するために使用される、AWS グローバルインフラストラクチャのコンポーネントはどれですか。

- 1) AWS リージョン
- 2) エッジロケーション**
- 3) アベイラビリティゾーン
- 4) VPC

オプション 2 が正解となります。Amazon CloudFrontでは、コンテンツをユーザーに配信する際のレイテンシーを低くするため、全世界でグローバルネットワークポイントオブプレゼンス（エッジロケーションおよびリージョン別エッジキャッシュ）を使用しています。



分野3：テクノロジー

「AWS の主要なサービスを識別する」に関する問題

ソフトウェアソリューションを探して購入し、AWS 環境ですぐに使い始めるには、どのAWS サービスを使用すればよいですか。

- 1) AWS Config
- 2) AWS OpsWorks
- 3) AWS SDK
- 4) AWS Marketplace



分野3：テクノロジー

ソフトウェアソリューションを探して購入し、AWS 環境ですぐに使い始めるには、どのAWS サービスを使用すればよいですか。

- 1) AWS Config
- 2) AWS OpsWorks
- 3) AWS SDK
- 4) AWS Marketplace

オプション4が正解となります。AWS Marketplace は、独立系ソフトウェアベンダー製の数千種類のソフトウェアが登録されている、デジタルカタログです。AWS Marketplaceを使用すれば、AWS 上で動作するソフトウェアを簡単に探して購入し、デプロイすることができます。



分野3：テクノロジー

「テクノロジーサポートのリソースを特定する」に関する問題

AWSの最適なアーキテクチャ設計原則に沿うために参照するべきツールはどれでしょうか？

- 1) ホワイトペーパー
- 2) AWS Trusted Advisor
- 3) ブラックベルト
- 4) AWS Well-Architected Framework tool



分野3：テクノロジー

AWSの最適なアーキテクチャ設計原則に沿うために参考するべきツールはどれでしょうか？

- 1) ホワイトペーパー
- 2) AWS Trusted Advisor
- 3) ブラックベルト
- 4) AWS Well-Architected Framework tool

オプション4が正解となります。 AWS Well-Architected Toolを利用すると、ワークロードの状態をレビューし、最新の AWS アーキテクチャのベストプラクティスと比較することができます。このツールは、AWS Well-Architectedフレームワークをベースとし、クラウドアーキテクトがアプリケーション向けに実装可能な、安全で高いパフォーマンス、障害耐性を備えた、効率的なインフラストラクチャの構築をサポートする目的で開発されています。



分野4：請求と料金

- AWS のさまざまな料金モデルを比較対照する
- AWS 請求と料金に関連した多様なアカウント構造を認識する
- 請求サポートに利用できるリソースを特定する



分野4：請求と料金

「AWS のさまざまな料金モデルを比較対照する」に関する問題

1年間継続利用が決まっているアプリケーション開発向けにEC2インスタンスを購入するときに選択すべき購入オプションはどれでしょうか？

- 1) リザーブドインスタンス
- 2) オンデマンドインスタンス
- 3) スケジュールドリザーブドインスタンス
- 4) スポットインスタンス



分野4：請求と料金

1年間継続利用が決まっているアプリケーション開発向けにEC2インスタンスを購入するときに選択するべき購入オプションはどれでしょうか？

- 1) リザーブドインスタンス
- 2) オンデマンドインスタンス
- 3) スケジュールドリザーブドインスタンス
- 4) スポットインスタンス

オプション1が正解となります。Amazon EC2 リザーブドインスタンス (RI) とは、通常のオンデマンド料金に比べて大幅な割引価格 (最大 72%) が適用され、特定のアベイラビリティーゾーンで使用するキャパシティーを予約できる仕組みです。1年または3年の期間利用を継続することを事前に予約することで割引が適用されます。



分野4：請求と料金

「請求サポートに利用できるリソースを特定する」に関する問題

現在のAWS利用状況がコスト最適化されているかどうかを確認するために利用できるサービスを選択してください。（2つ選択してください。）

- 1) AWS Trusted Advisor
- 2) AWS Systems Managers
- 3) 請求アラーム
- 4) 請求ダッシュボード
- 5) AWS Cost Explore



分野4：請求と料金

現在のAWS利用状況がコスト最適化されているかどうかを確認するために利用できるサービスを選択してください。（2つ選択してください。）

- 1) AWS Trusted Advisor
- 2) AWS Systems Managers
- 3) 請求アラーム
- 4) 請求ダッシュボード
- 5) AWS Cost Explore

オプション1が正解となります。 AWS Trusted Advisor では、コストの削減、可用性とパフォーマンスの向上、セキュリティの改善に役立つ一連のベストプラクティスチェックと推奨事項を提供しています。

オプション5が正解となります。 Cost Explorer の適切なサイズ設定に関する推奨事項の機能を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) でインスタンスを縮小または終了してコストを削減する機会を特定できます。適切なサイズ設定に関する推奨事項では、Amazon EC2 のリソースと使用状況を分析し、支出を削減する方法を示します。リンクされたアカウント全体で十分に活用されていない Amazon EC2 インスタンスが単一のビューに表示されるため、削減できる量をすぐに確認できます。



試験時間と合格

- 試験時間：90分
- 問題数：65問
- 得点100～1000 点の範囲で難易度が平均化されて表示
- 合格点：700（およそ7割以上）



検証される能力

- AWS クラウドとは何かということ、およびベーシックなグローバルインフラストラクチャについて定義できる
- AWS クラウドのベーシックなアーキテクチャ原理を説明できる
- AWS クラウドの価値提案について説明できる
- AWS プラットフォームの主なサービスと一般的なユースケース (例: コンピューティング、分析など) について説明できる
- AWS プラットフォームのセキュリティとコンプライアンスのベーシックな側面、および共有セキュリティモデルについて説明できる
- 請求、アカウントマネジメント、料金モデルを明確に理解している
- ドキュメントや技術サポートのソースを特定できる (例: ホワイトペーパー、サポートチケットなど)
- AWS クラウドにおけるデプロイと運用のベーシックで重要な特徴を説明できる



必要な知識と経験

- テクノロジー、マネジメント、販売、購買、またはファイナンスの分野で最低 6 か月の AWS クラウド使用経験がある
- IT サービスのベーシックな知識と、AWS クラウドプラットフォームにおけるそれらのサービスの使用に関する知識がある



受験者に求められる能力

【知識系】

クラウドの概念から
AWSサービスと役割の
包括的な理解

【実践系】

6ヶ月という最低限の実践経験



受験者に求められる能力

【知識系】

クラウドの概念から
AWSサービスと役割の
包括的な理解

【実践系】

6ヶ月という最低限の実践経験



【本講座の対応】

全くの初学者の状態からクラウドの基礎知識から網羅的にAWSサービスとコンセプトを学習します。



受験者に求められる能力

【知識系】

クラウドの概念から
AWSサービスと役割の
包括的な理解

【実践系】

6ヶ月という最低限の実践経験



【本講座の対応】

全くの初学者の状態からクラウ
ドの基礎知識から網羅的に
AWSサービスとコンセプトを
学習します。

【本講座の対応】

AWSサービスの利用方法と、
サポート対応などへのアクセス
などプラクティショナーとして
必要な実践力を確保



クラウドとAWSの概要

レクチャー	レクチャーで学ぶ内容
仮想化を理解する	クラウドのベースとなっている仮想化技術について学習します。
クラウドの基礎	クラウドの技術的な背景とその特徴について基本知識を獲得します。
AWSの意義	なぜAWSを利用するべきか？という基本的な質問に対する回答となる、AWSの意義を理解します。
AWSのグローバルインフラ構成	AWSのグローバルインフラ構成を確認して、その基本的な仕組みを理解します。
AWSサービスの全体像	AWSサービスにおいて、試験範囲になる主要なサービスを確認します。



セクションの内容

レクチャー	レクチャーで学ぶ内容
AWSの活用メリット	AWSの活用する意義をユースケースから確認します。
オンプレミスとAWSクラウドの良し悪し	オンプレミス環境とクラウドを比較して、メリットとデメリットを確認します。
AWSの操作方法	AWSサービスを操作するツールなど、その操作方法を確認します。



仮想化を理解する

クラウドと仮想化

クラウドは仮想化技術によって成り立っているサービス

```
graph TD; A[クラウド] --> B[仮想化されたインフラ]
```

クラウド

仮想化されたインフラ

仮想化とは

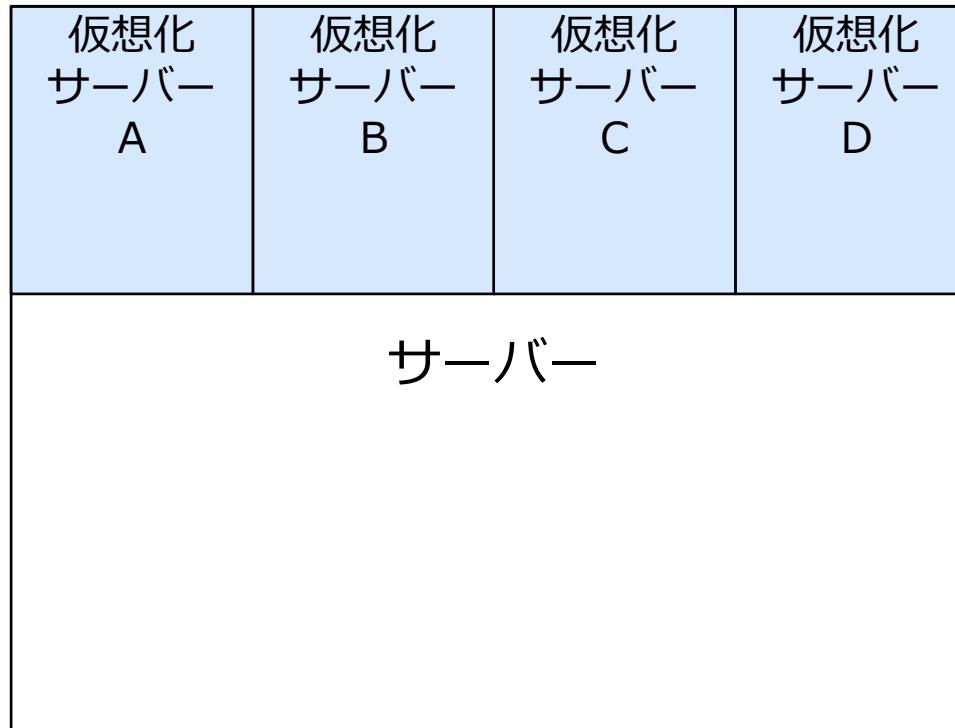
物理的なインフラの構成を隠して、仮想化された単位に分けたり、統合したりして利用させる技術



サーバー

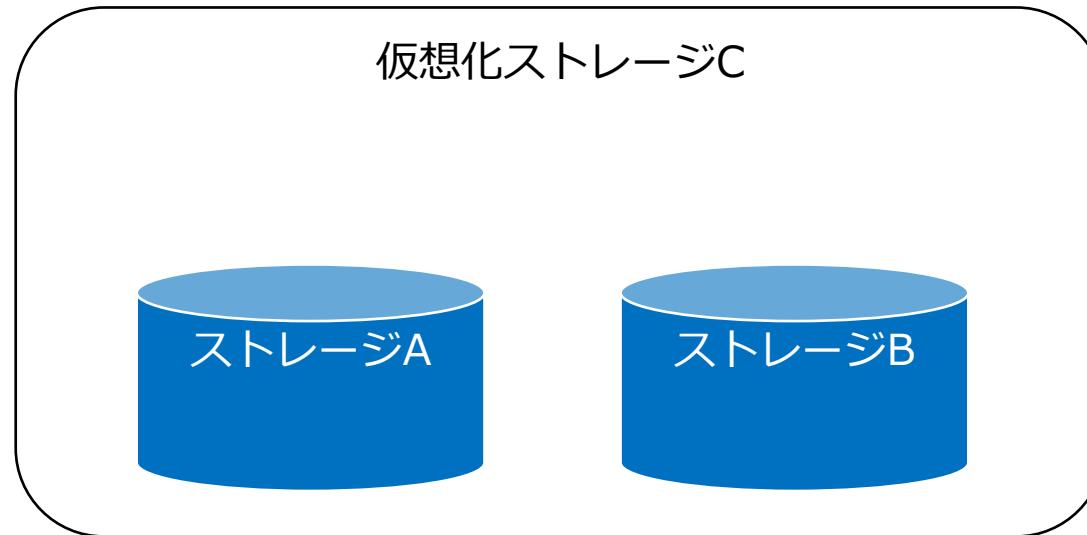
仮想化とは

物理的なインフラの構成を隠して、仮想化された単位に分けたり、統合したりして利用させる技術



仮想化とは

物理的なインフラの構成を隠して、仮想化された単位に分けたり、統合したりして利用させる技術



仮想化の仕組み

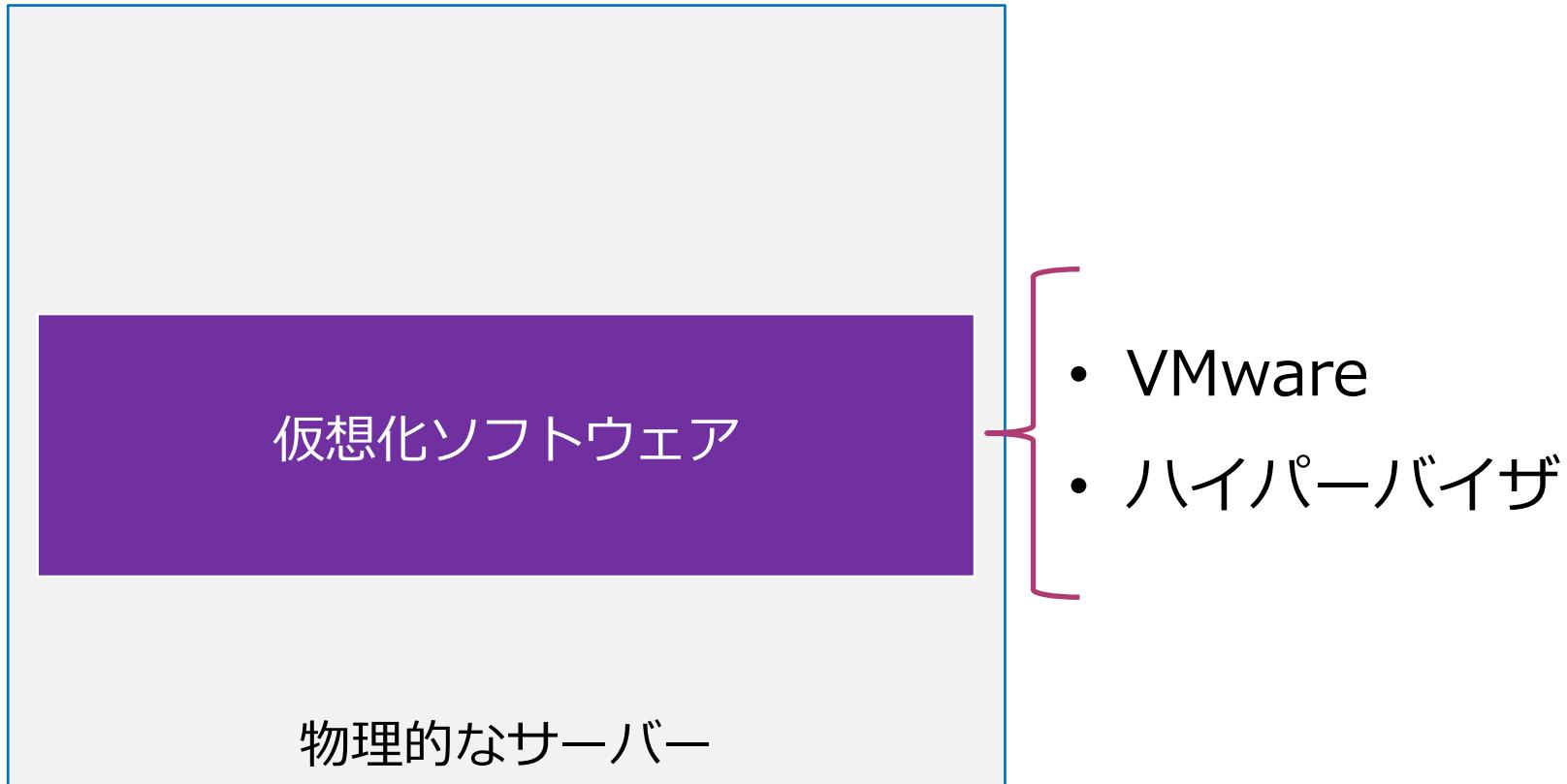
物理的なインフラに仮想化ソフトウェアを設定して、実質的な機能をユーザーに切り分けて提供する

物理的なサーバー

1つの物理的なサーバーを
買ってきていたけど、容量が大き
すぎて1つのシステムでは利
用しきれなくて、もったいな
い。

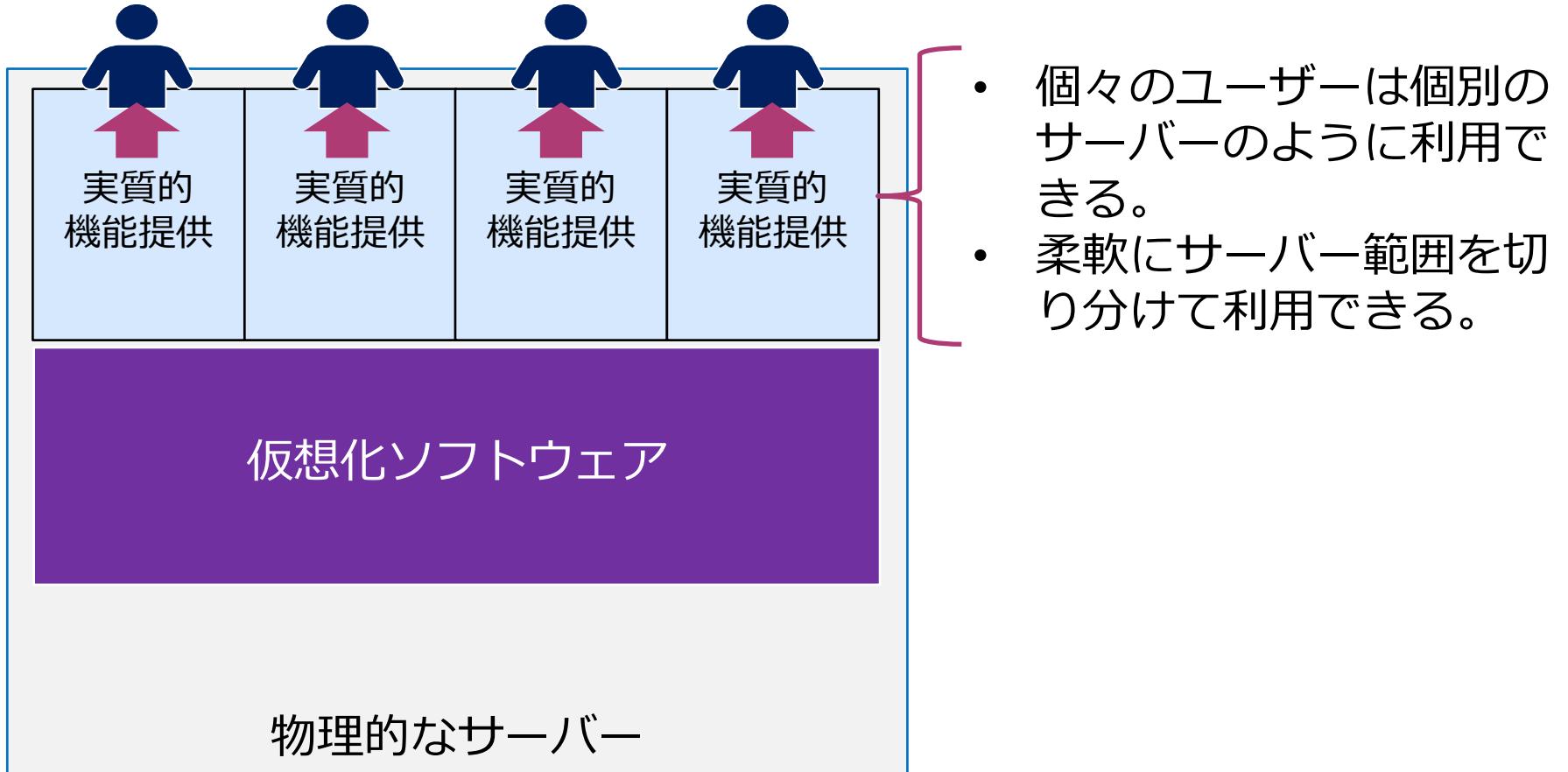
仮想化の仕組み

物理的なインフラに仮想化ソフトウェアを設定して、実質的な機能をユーザーに切り分けて提供する



仮想化の仕組み

物理的なインフラに仮想化ソフトウェアを設定して、実質的な機能をユーザーに切り分けて提供する



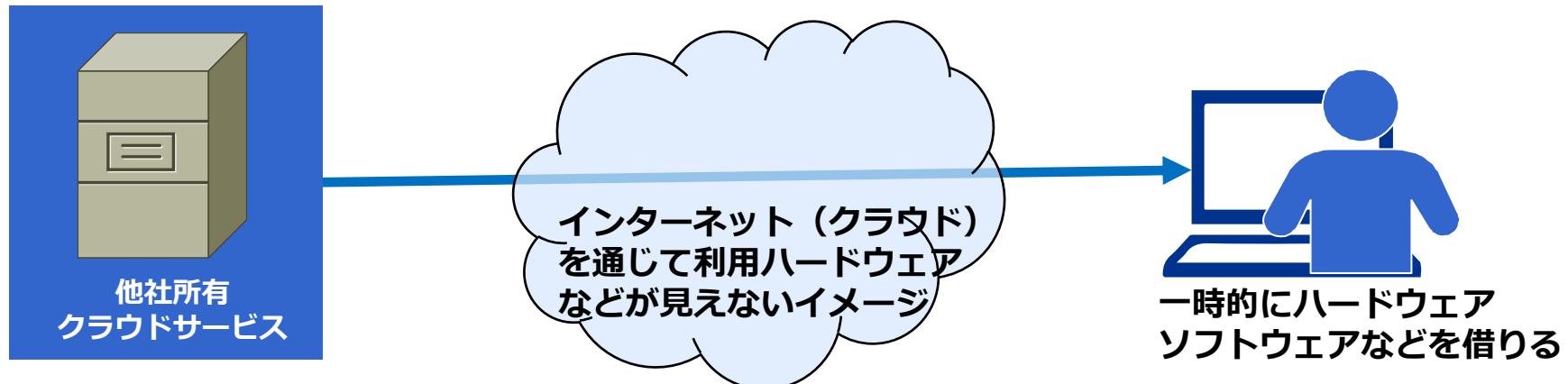
クラウドの基礎

クラウドとは

必要に応じて他社所有のハードウェア・ソフトウェア等をネットワークを介して利用するシステム利用形態

こんな時はクラウドに・・・

- ✓ 短期的なキャンペーン用に一時的にサーバーがほしい。
- ✓ 需要増に応じサーバーを増強し、需要減には削減したい。
- ✓ 今すぐデータベースが必要だけど調達している時間がない。



クラウドとは

インフラを仮想化することで、ソフトウェア化されたサービスとして提供されているのがクラウド型のインフラサービス



クラウドとは

インフラを仮想化することで、ソフトウェア化されたサービスとして提供されているのがクラウド型のインフラサービス



クラウドとは

インフラを仮想化することで、ソフトウェア化されたサービスとして提供されているのがクラウド型のインフラサービス



クラウド構成要素

クラウドで提供されるシステム構成要素はインフラ、ミドルウェア、アプリケーションの3層

システムアーキテクチャ

アプリケーション	アプリケーション (プログラミングソフトウェア)		フレームワーク	・プログラミング開発したアプリケーション ・業務機能が実装されたパッケージソフトウェア
ミドルウェア ／OS	システム連携	セキュリティ	運用管理	・ミドルウェアとは共通利用される機能をまとめたソフトウェア ・Windowsなどの基本ソフト(OS:オペレーティングシステム)
インフラ	サーバー機器	クライアント端末	ネットワーク機器	・物理的な機器(ハードウェア) ・ネットワーク回線

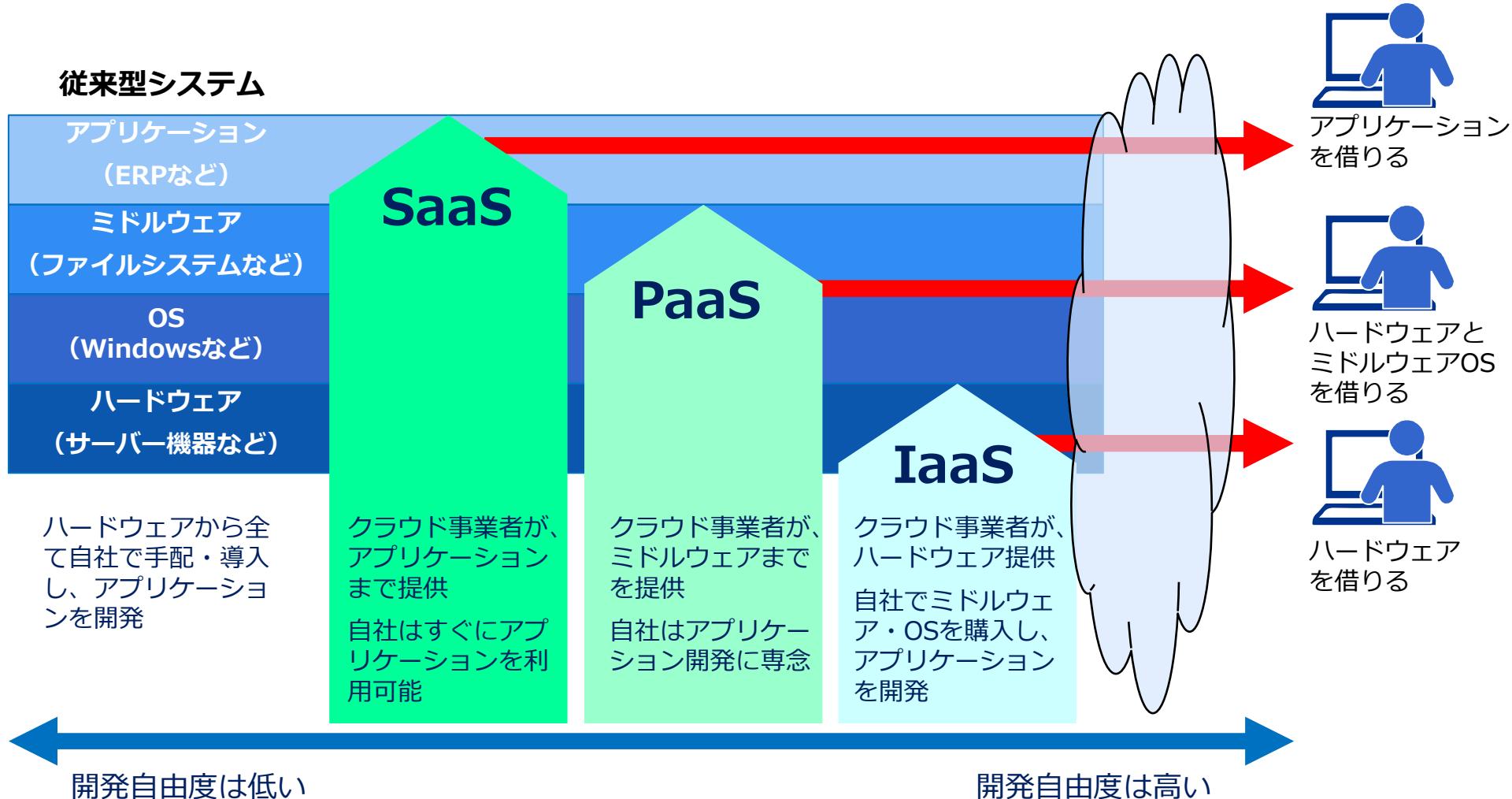
クラウドの5つの基本特性

クラウドの特徴は「5つの基本特性」「3つのサービス」「3つの提供形態」

5つの基本特性	概要
オンデマンド・セルフサービス	✓ 利用者は人を介さず、必要に応じてサーバー、ネットワーク、ストレージを設置・拡張・設定が可能
幅広いネットワークアクセス	✓ ネットワークを通してPC、スマホ、タブレットなど各種デバイスから利用可能
リソースの共有	✓ ハードウェアの使用容量などのリソースは複数利用者により共有し、利用者の需要に応じて動的に割り当てる。物理的配置は考慮不要
迅速な拡張性	✓ ハードウェア等の資源は必要に応じて自動または主導で増やしたり、減らしたりできる
サービスは計測可能	✓ 稼働状況が常に計測されており、利用状況をコントロール・最適化できる。 ✓ 計測結果に応じて従量課金が可能

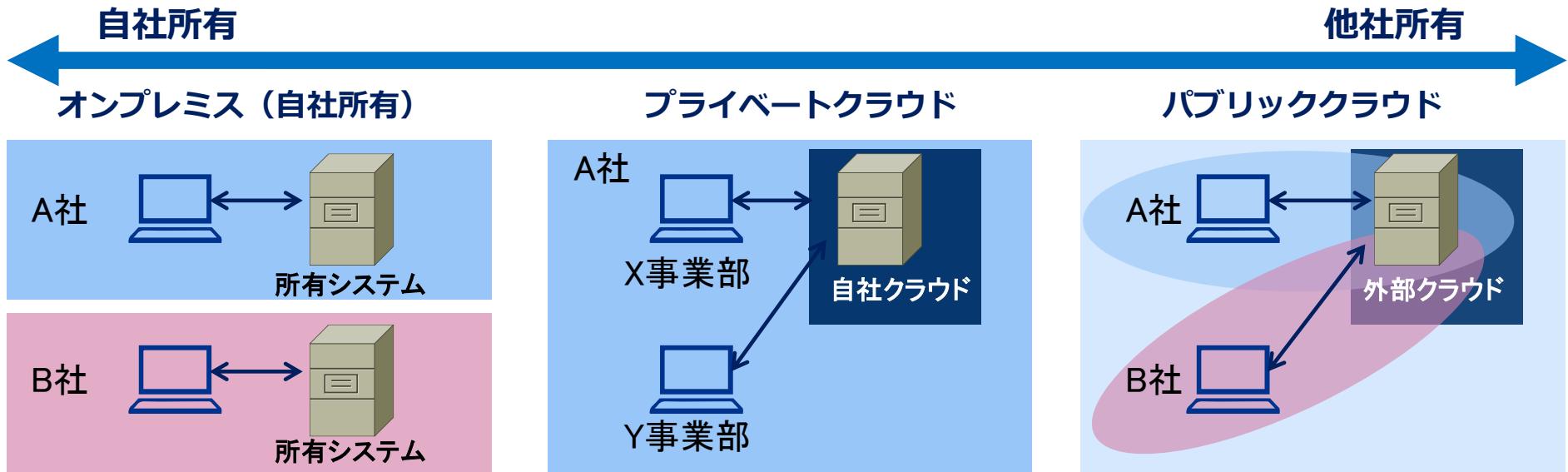
クラウドの3つのサービス形態

主にSaaS、PaaS、IaaSの3つのサービスが存在



クラウドの3つの提供形態

クラウド提供形態はプライベートとパブリックが主流。加えて両方を併用するハイブリッド型の提供形態がある



【所有形態】

自社所有

【特徴】

ハードウェア／ソフトウェアを購入し、
自社にシステムを構築

メリット：自社でハードウェアを自由に
コントロール可能

デメリット：調達・構築に時間を要す。
運用管理に人材・コストを要す

【所有形態】

自社所有

【特徴】

自社内にクラウド基盤を構築し、ハード
ウェア・ソフトウェアを事業部や子会社
間で共同利用

メリット：自社資産の効率化。パブリック
と比較しコントロールが自由

デメリット：クラウド運用管理が難しく、
クラウドのメリットが低下

【所有形態】

他社所有

【特徴】

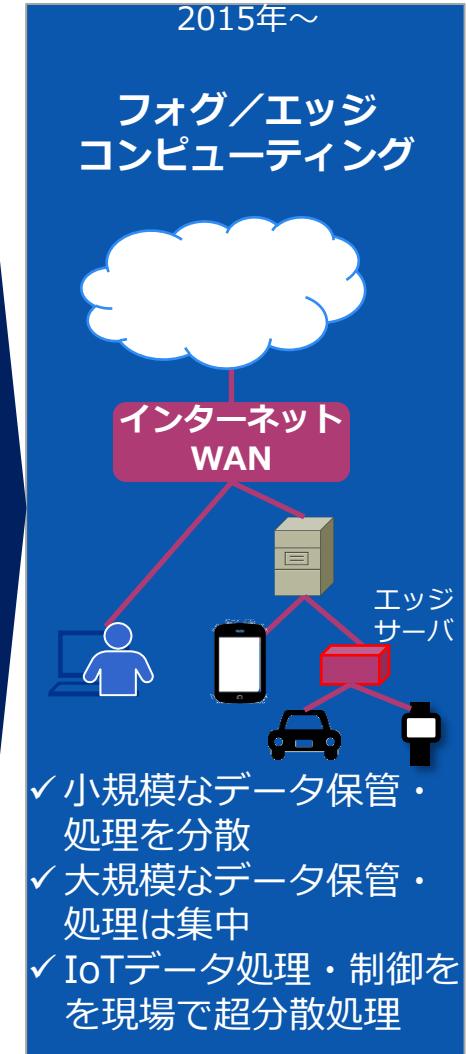
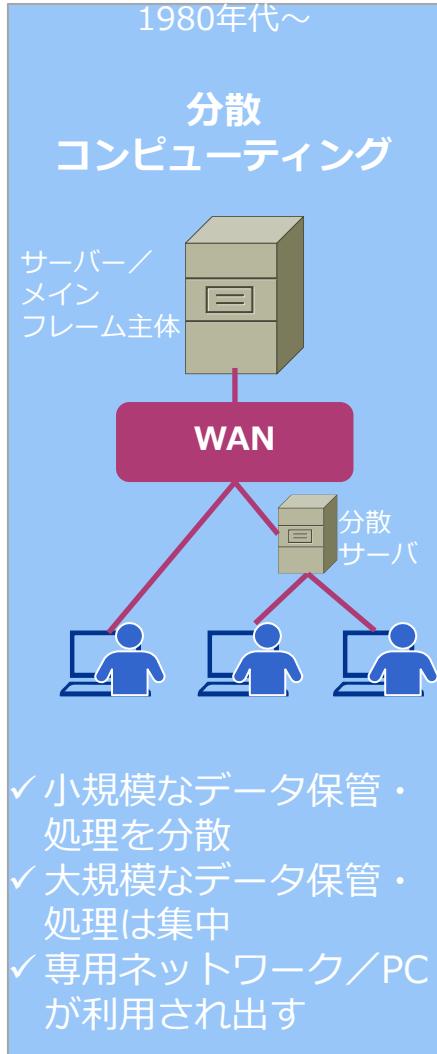
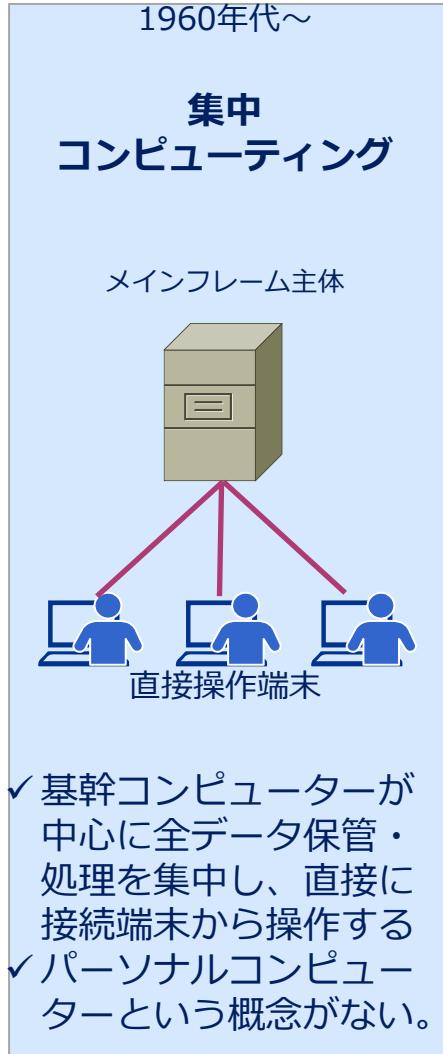
ハードウェア・ソフトウェアを他社と共
同利用し、柔軟に構築・解除が可能

メリット：運用管理を他社に委任可能。
システム調達・構築の自由度が高い

デメリット：自社コントロールの範囲が
制限

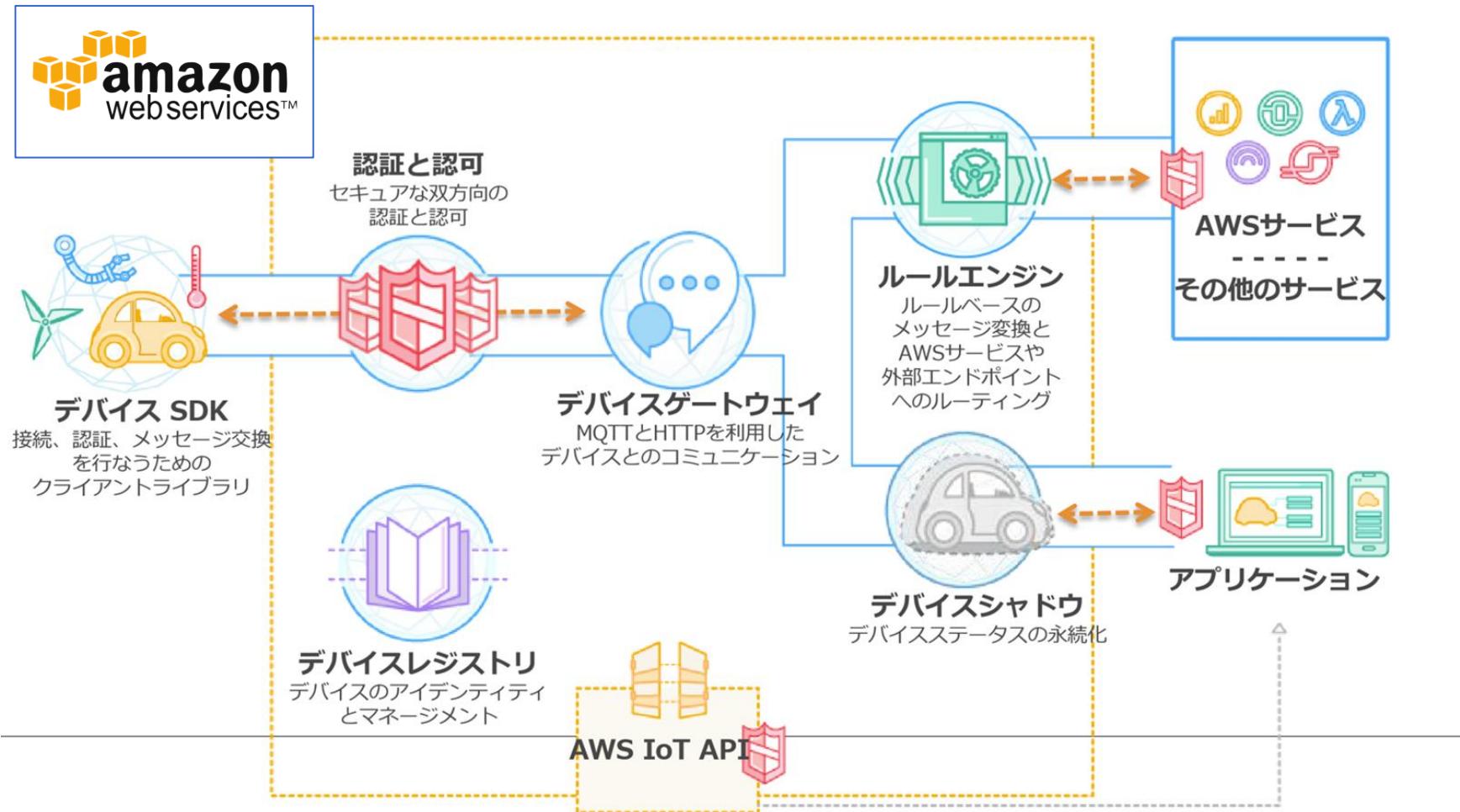
クラウドへの進化

クラウドから超分散コンピューティング型のクラウドへと発展



クラウドIoT

AWSは他のプラットフォームよりも機能が豊富で、グローバルシェアも高い



クラウドAI

完成したAI機能をクラウドを通じて即座に利用することも可能

クラウドAIサービス

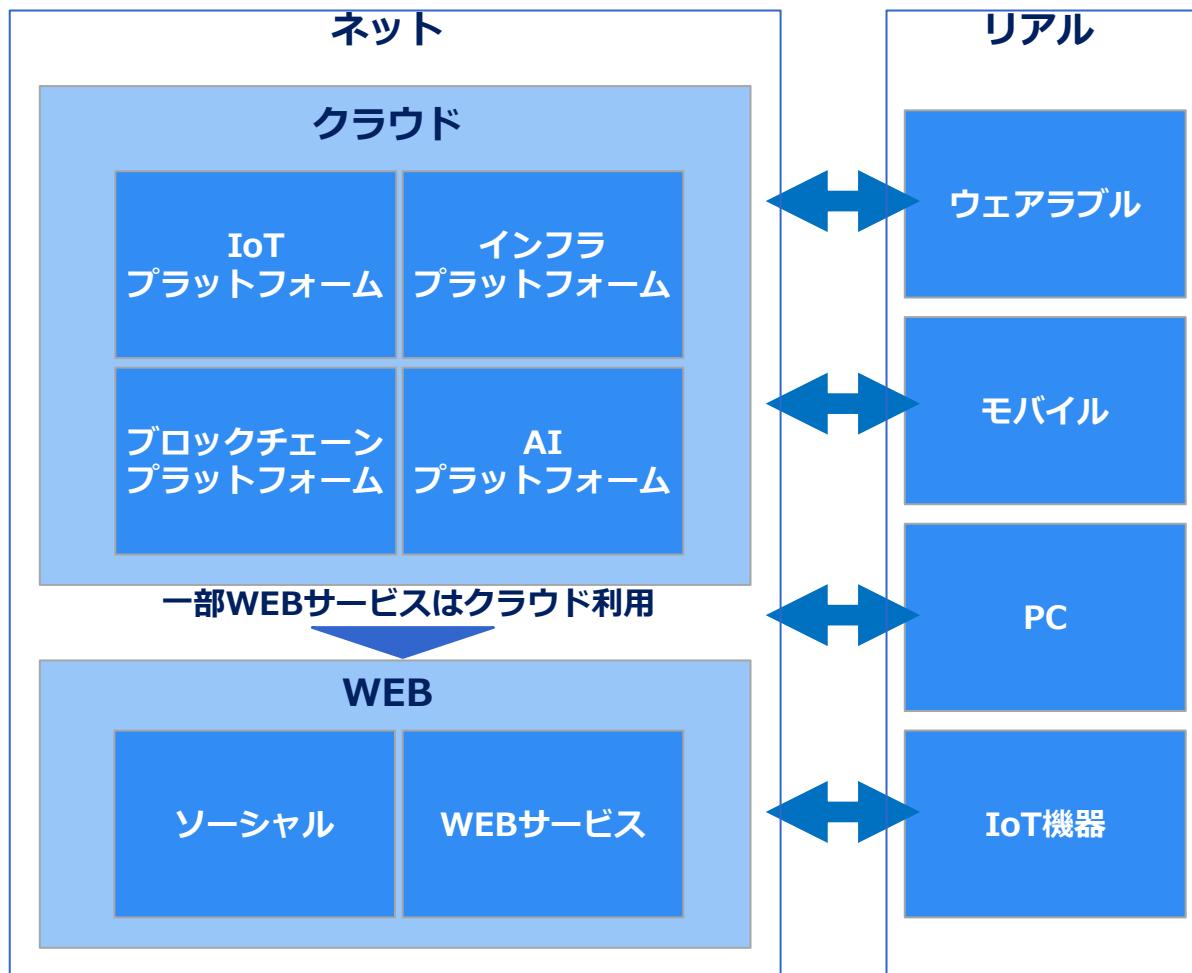
	Amazon ML Amazon API Amazon Alexa
	Azure ML Azure API
	Watson ML Watson API
	Google ML Tensorflow Google API

概要

- ✓ 機械学習環境を提供するPaaSサービス
- ✓ 画像識別などのAI機能を提供するAPIサービス
- ✓ 音声コンシェルジュ開発向けのPaaSサービス
- ✓ ワークフローでコーディングなしでも開発可能な機械学習環境を提供するPaaSサービス
- ✓ 画像識別などのAI機能を提供するAPIサービス
- ✓ もともとWatson機能になかった機械学習環境を提供するPaaSサービス
- ✓ 言語識別などのAI機能を提供するAPIサービス
- ✓ 機械学習環境を提供するPaaSサービス。Cloud MLの実行基盤と自社開発のTensorflowが特徴
- ✓ 画像識別などのAI機能を提供するAPIサービス

クラウドファーストの時代へ

クラウドを中心核に「ネットとリアルの融合」「ITとビジネスの融合」が促進される



クラウドがもたらす変化

- クラウドを媒体に私たちの生活が変化
 - Amazon/G-mail/DropBox等様々なサービスはクラウドサービス
 - 私たちは既に様々なサービスをクラウドから利用している
⇒様々なデバイスからクラウドにアクセスする生活スタイルに変化
- クラウドでネットとリアルが融合
 - IoT／ウェアラブル／モバイルにより、リアル世界の行動データや機器データがクラウドに集約
 - クラウドから各種デバイスを操作
- クラウドを媒体にビジネスが変化
 - クラウドによりシステム構築が高速化し、柔軟性が高まる
 - AI／IoT／ブロックチェーンの多くがクラウドで提供
⇒クラウドベースでビジネスを検討することが当たり前に

クラウドファーストの時代へ

「テクノロジーの進化」と「ビジネス変化のスピード」に対応するため、柔軟で素早いシステム開発が求められる

テクノロジー×ビジネス スピードへの対応

- ① テクノロジー進化のスピードが加速
- ② テクノロジーを活用したビジネスの展開スピードが加速
- ③ これまでより短期に開発可能かつ変更に強いシステムの必要性



多様な顧客ニーズへの対応

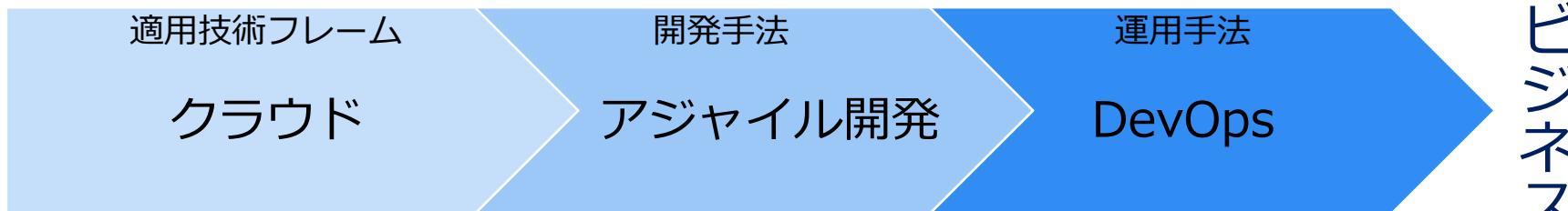
- ① 多様な顧客ニーズに柔軟にかつスピーディに対応する必要性
- ① デザイン思考／リーンスタートアップなどの顧客中心手法の導入
- ① 本当に使うシステムだけを開発・運用する必要性



ビジネス変化に即応できる開発手法・技術の導入

クラウドファーストの時代へ

今後のテクノロジー×ビジネスに柔軟に対応するためには、クラウドファーストが必要不可欠



■ IaaS

- インフラのクラウド提供による環境構築を迅速化

■ PaaS

- 開発環境のクラウド提供による開発迅速化

■ SaaS

- アプリサービスのクラウド提供によるサービス利用の迅速化

開発手法

アジャイル開発

■ アジャイル手法の活用拡大

- アプリケーション開発・変更への迅速な対応
- 顧客要件確認の柔軟化

運用手法

DevOps

■ 運用と開発の一体化

- 運用チームと開発チームの継続的連携による運用
- 運用チームと開発チームのコミュニケーション齟齬や組織文化の一体化

■ CI/CDソフトウェア・サービスの活用

- アジャイルとDevOpsはContinuous Integration（継続的開発）とContinuous Delivery（継続的導入）の利用が基本
- 開発・テスト・導入を迅速にする自動化ツールを活用

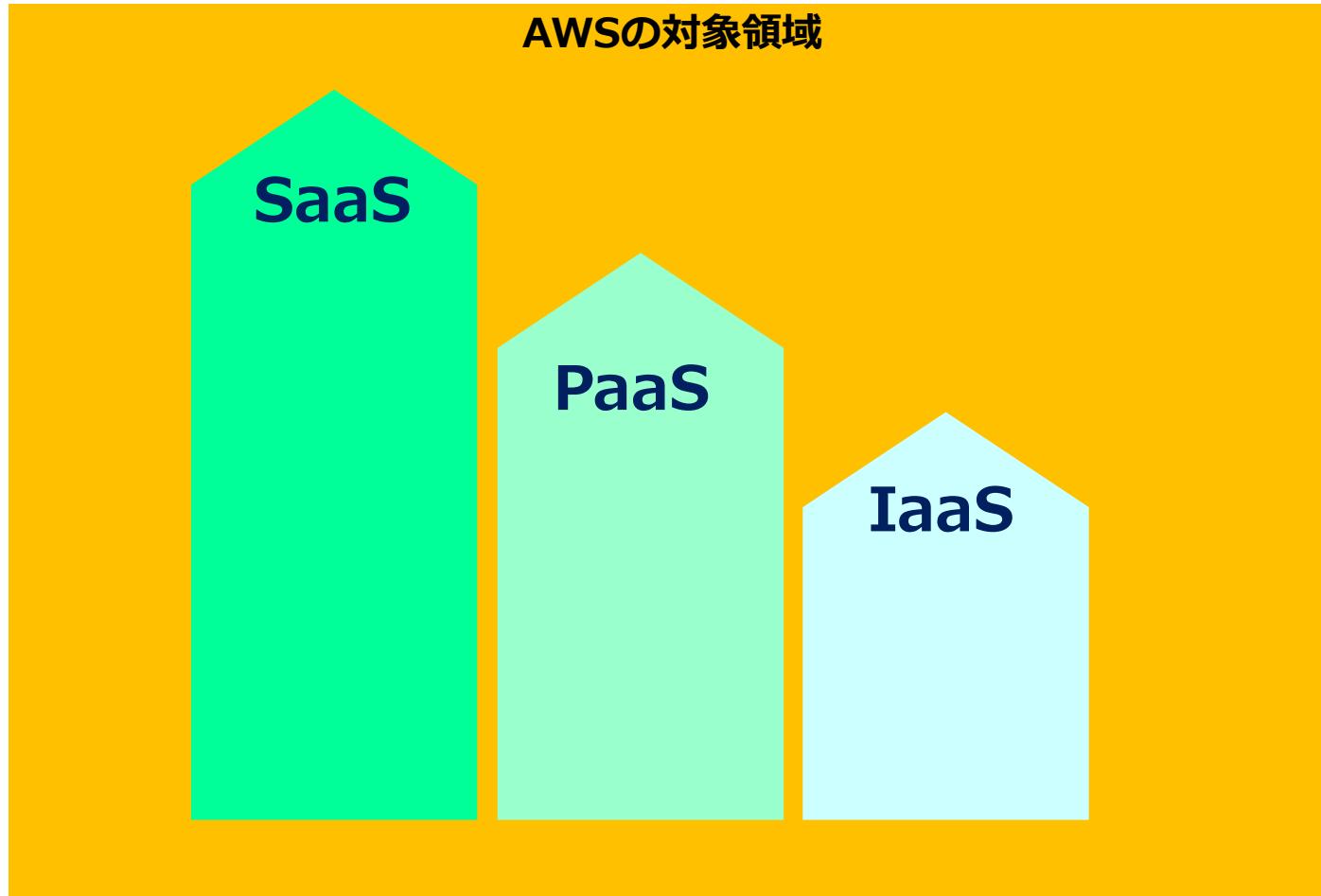
ビジネススピードへの対応

AWSの意義



AWSとは

AWSはAmazonが提供する総合クラウドサービスで、あらゆる領域のクラウドサービスを網羅的に提供しています。

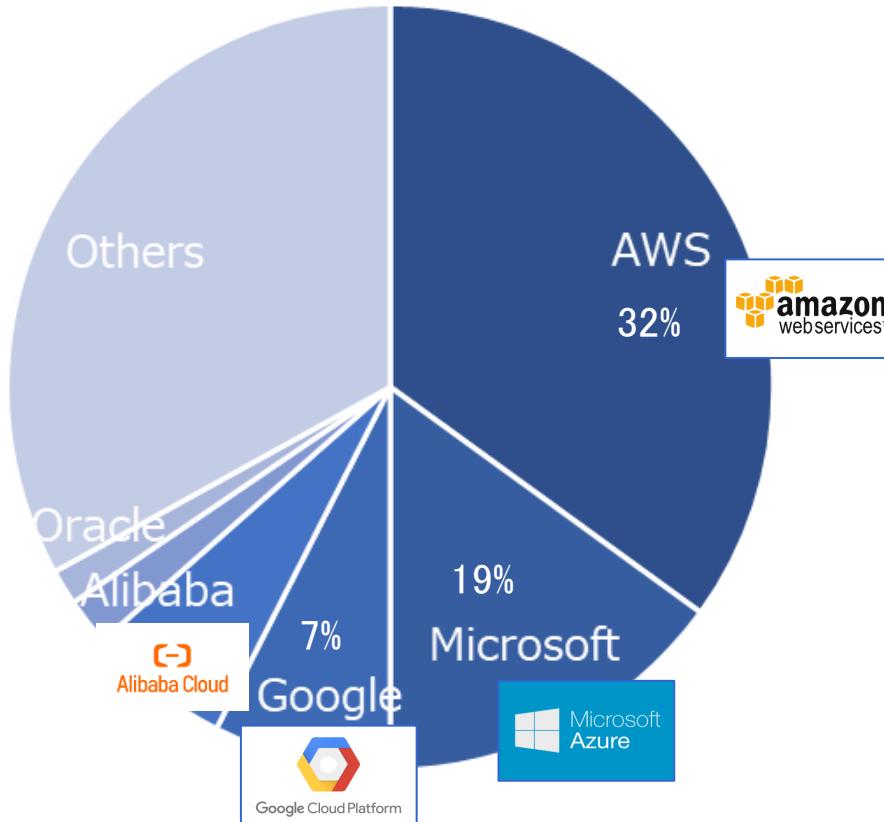


なぜAWSか？

圧倒的なトップリーダーの地位

グローバルシェア

Amazonは長年クラウドシェアで3割以上のシェアをキップしており圧倒的な存在である（2021年四半期シェア）



参照：グローバルのクラウドにおけるシェア、AWSが32%、Azureが19%、Google Cloudが7%。上位3社で全体の6割近くを獲得。2021年第1四半期、Canalysが発表 — Publickey (publickey1.jp)

グローバルシェア

Gartnerの調査においてもクラウドのトップリーダーとして位置づけられている。



参照 : <https://japan.zdnet.com/article/35140211/>

クラウドベンダー（日系）

国内シェアもAWSとMicrosoft Azureが二分しており、大きなシェアを占めている

Public Cloud Leadership – APAC Region

Rank	Total APAC Region	China	Japan	Rest of Region
Leader	Amazon	Alibaba	Amazon	Amazon
#2	Alibaba	Tencent	Microsoft	Microsoft
#3	Microsoft	Baidu	Fujitsu	Google
#4	Google	Sinnet-AWS	Google	Alibaba
#5	Tencent	China Telecom	NTT	IBM
#6	Baidu	China Unicom	Softbank	Naver

Based on public IaaS and PaaS revenues in Q4 2019

Source: Synergy Research Group

なぜAWSがトップなのか

圧倒的な投資額でクラウドをリード

データ活用の軍拡競争

【2020年世界研究開発費ランキング】

- 1位 Amazon \$427.4億ドル (約4.8兆円)
- 2位 アルファベット (グーグル) \$ 275.7億ドル
- 3位 Huawei \$220.4億ドル
- 4位 Microsoft \$192.7億ドル
- 5位 Apple \$187.5億ドル
- 6位 サムスン \$187.5億ドル
- 7位 Facebook \$184.5億ドル
- ⋮

データ活用の軍拡競争

圧倒的投資によりAIを含めた最新サービスが続々とリリースされ、後発企業が単体で追いつくことはもはや不可能

巨額のテクノロジー投資の実施



- AWSは「re:Invent 201○」
 - Microsoftは「Microsoft Build 201○」
 - Googleは「Google I/O 201○」
 - IBMは「Inter Connect 201○」
- ⇒テクノロジートレンドを確認するためには、各ベンダーイベントの追跡が必須

アマゾンはre:Inventにおいて数十にも及ぶ最新機能やサービスをリリース

⇒後発企業がクラウドサービスの充実度で追いつくことはもはや不可能

AWSファースト

ITインフラ構築検討の際には
AWSファーストにならざるを得ない

AWSファースト

IT関連の全てのビジネスマンはAWSの知識が必須となっている

インフラ
エンジニアは
もちろん

プログラマーも

SEも

ITコンサル
タントも



全てのIT従事者にAWSスキルは必須

AWSのグローバル インフラ構成



AWSのグローバルインフラ構成

リージョンとアベイラビリティゾーン (AZ) とエッジロケーションを中心に世界中にDCを展開している。

リージョン
(26+8)

AZ
(84)

エッジロケーション
(300以上)

ローカルゾーン
(14+33)

Wavelength
Zone
(20)

Direct Connect
ロケーション
(108)



AWSのグローバルインフラ構成

リージョンとアベイラビリティゾーン (AZ) とエッジロケーションを中心に世界中にDCを展開している。

26 リージョンがローンチ済み

各リージョンに複数のアベイラビリティゾーン (AZ) を展開

84 アベイラビリティゾーン

**14 ローカルゾーン
20 Wavelength Zones**

超低レイテンシーアプリケーション向け

8 リージョンのローンチ発表

33 ローカルゾーンのローンチ発表

2 倍のリージョン数

複数AZのものを次に規模の大きいクラウドプロバイダーと比べて

245 の国と地域でサービスを提供

108 の Direct Connect ポート

310 以上の POP (Point Of Presence)

300 以上のエッジロケーションと 13 のリージョン別エッジキャッシュ

参照：<https://aws.amazon.com/jp/about-aws/global-infrastructure/>



リージョン

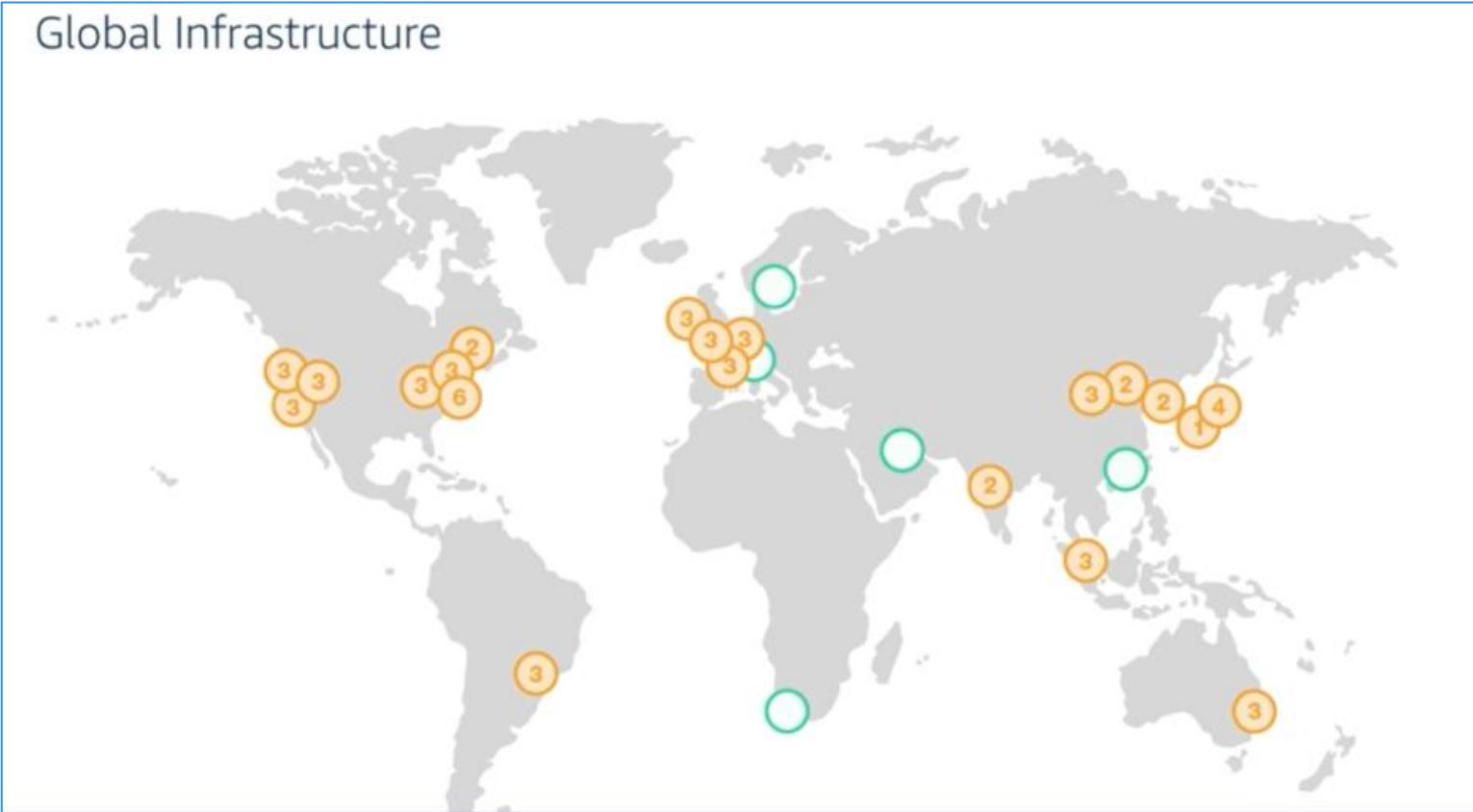
リージョンはデータセンターが集積された地理的なロケーションのこと

- ✓ データセンターが集積されている世界中の物理的ロケーションのこと。
- ✓ AWS では、北米、南米、欧州、中国、アジアパシフィック、南アフリカ、中東などのリージョンを含む、複数の地理的なリージョンを整備している。
- ✓ リージョンに応じて価格と利用可能なサービスが少し異なる。
- ✓ 各AWS リージョンは、1 つの地理的エリアにある、隔離され物理的にも分離された 複数のAZ によって構成される。
- ✓ 1 つのリージョンにはユーザーが利用可能なAZが2つ以上で構成される。その中でユーザーが選択できないAZもあり、3つ以上のAZが存在する。



リージョン

リージョンは国や地域における地理的に隔離されたAWS拠点



リージョン

日本には東京と大阪の2つのリージョンが設置されている

東京リージョン

大阪ローカル
リージョン



リージョン

リージョンとリージョンは物理的に独立したインフラ拠点



東京リージョン

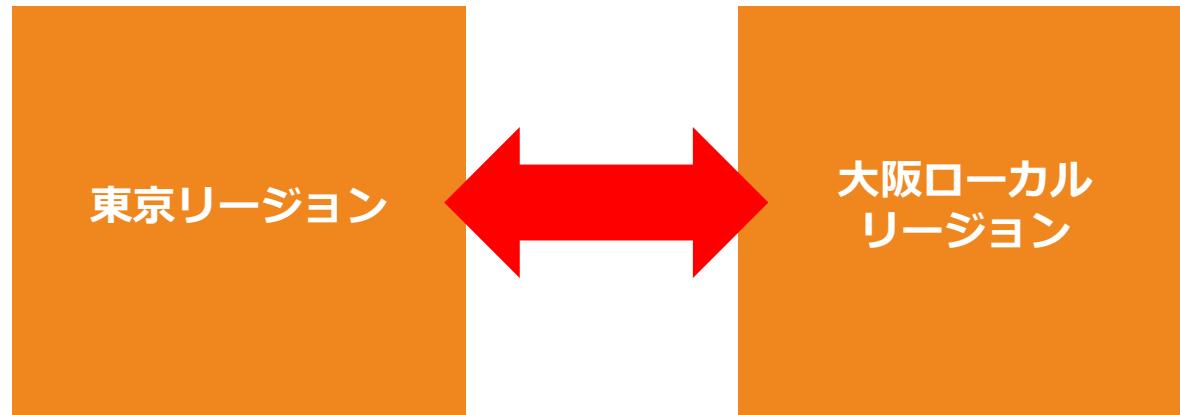


大阪ローカル
リージョン



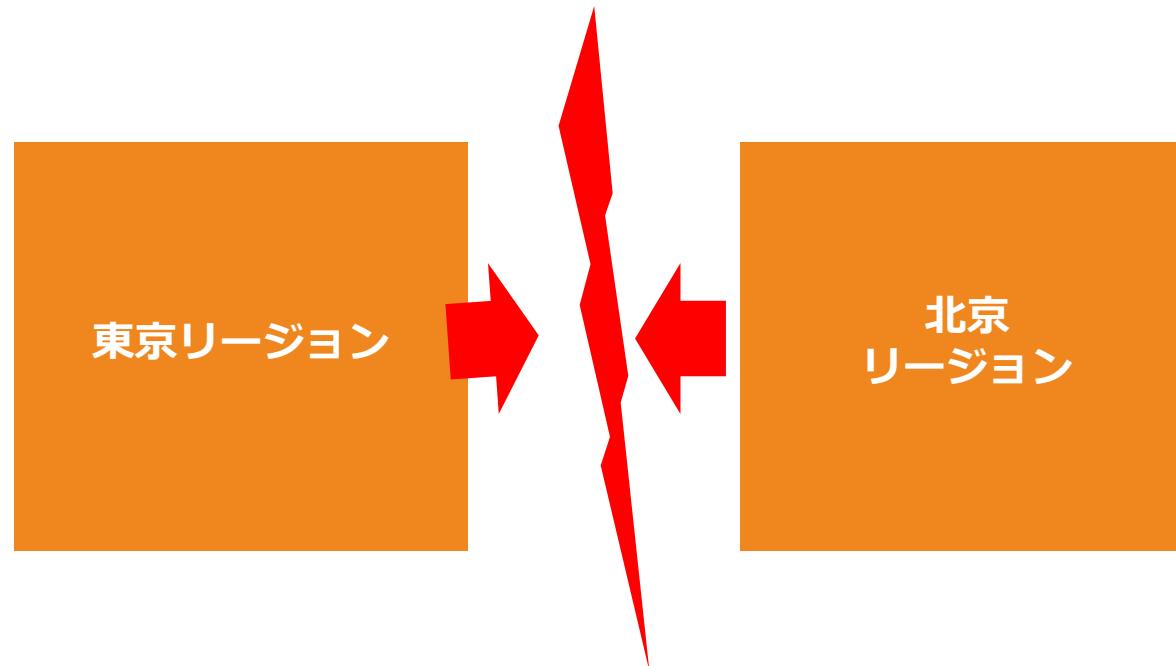
リージョン

ただし、隣接リージョン間は広帯域の専用ネットワークで接続されている



北京リージョン

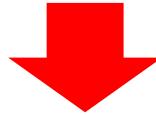
中国国内のリージョンは政治的な理由で他のAWSリージョンとは完全に断絶している



リージョン

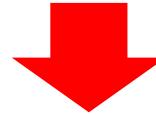
リージョンに応じてAWSサービスの利用可否と値段が異なる

東京リージョン



最新機能が使えない

米国東部
(バージニア北部)



最新機能が使える



アベイラビリティゾーン

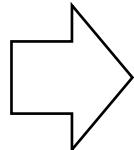
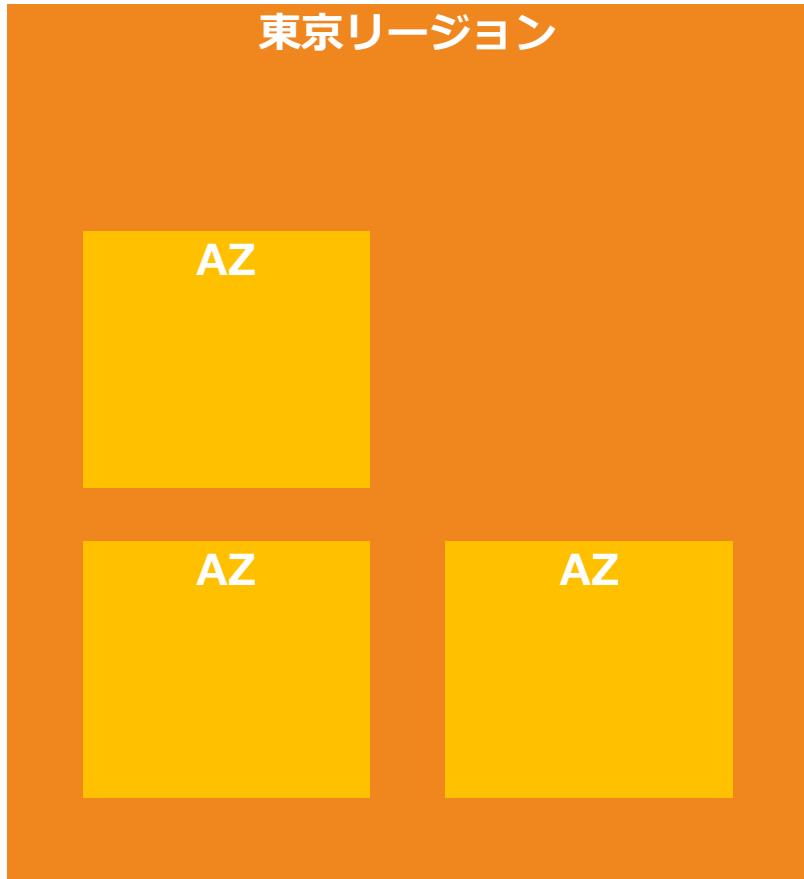
アベイラビリティゾーンは1つ以上のデータセンターで構成された論理的なデータセンターのグループ

- ✓ 1つの AWS リージョン内でそれぞれ切り離され、冗長的な電力源、ネットワーク、そして接続機能を備えている 1 つ以上のデータセンターであり、論理的データセンターのグループ
- ✓ AZは1つ以上のデータセンターで構成されており、AWSリソースを提供するサーバーが設置されている。
- ✓ AZによって、単一のデータセンターでは実現できない高い可用性、耐障害性、および拡張性を備えた本番用システムの運用が可能になる。
- ✓ 各AZには個別の電力源、冷却システム、物理的セキュリティが備わっており、AZ間は冗長で低レイテンシーなネットワークを介し接続されている。
- ✓ アプリケーションがAZ間で分割されている場合は停電、落雷、竜巻、地震などの問題からより安全に隔離され保護される。
- ✓ 同じリージョンにある各AZはそれぞれ他のAZから物理的に意味のある距離（数キロメートル）があるものの、互いは 100 km (60 マイル) 以内に配置されている。



アベイラビリティゾーン (AZ)

リージョンの中に複数の独立したインフラ拠点が存在し、それをアベイラビリティゾーンと呼ぶ



1つのリージョンには
複数のAZが存在



アベイラビリティゾーン (AZ)

リージョンの中に複数の独立したインフラ拠点が存在し、それをアベイラビリティゾーンと呼ぶ

展開されるAZ

中国本土 (北京) リージョン

アベイラビリティゾーン: 3

詳細については www.amazonaws.cn をご覧ください

アジアパシフィック (シンガポール) リージョン

アベイラビリティゾーン: 3

2010 年ローンチ

アジアパシフィック (シドニー) リージョン

アベイラビリティゾーン: 3

2012 年ローンチ

アジアパシフィック (ムンバイ) リージョン

アベイラビリティゾーン: 3

2016 年ローンチ

アジアパシフィック (大阪) リージョン

アベイラビリティゾーン: 3

2021 年ローンチ

中国本土 (寧夏) リージョン

アベイラビリティゾーン: 3

詳細については www.amazonaws.cn をご覧ください

アジアパシフィック (東京) リージョン

アベイラビリティゾーン: 4

2011 年ローンチ

アジアパシフィック (ソウル) リージョン

アベイラビリティゾーン: 4

2016 年ローンチ

アジアパシフィック (香港) リージョン

アベイラビリティゾーン: 3

2019 年ローンチ

アジアパシフィック (ジャカルタ) リージョン

アベイラビリティゾーン: 3

2021 年ローンチ

利用できるAZ

アベイラビリティゾーン 情報

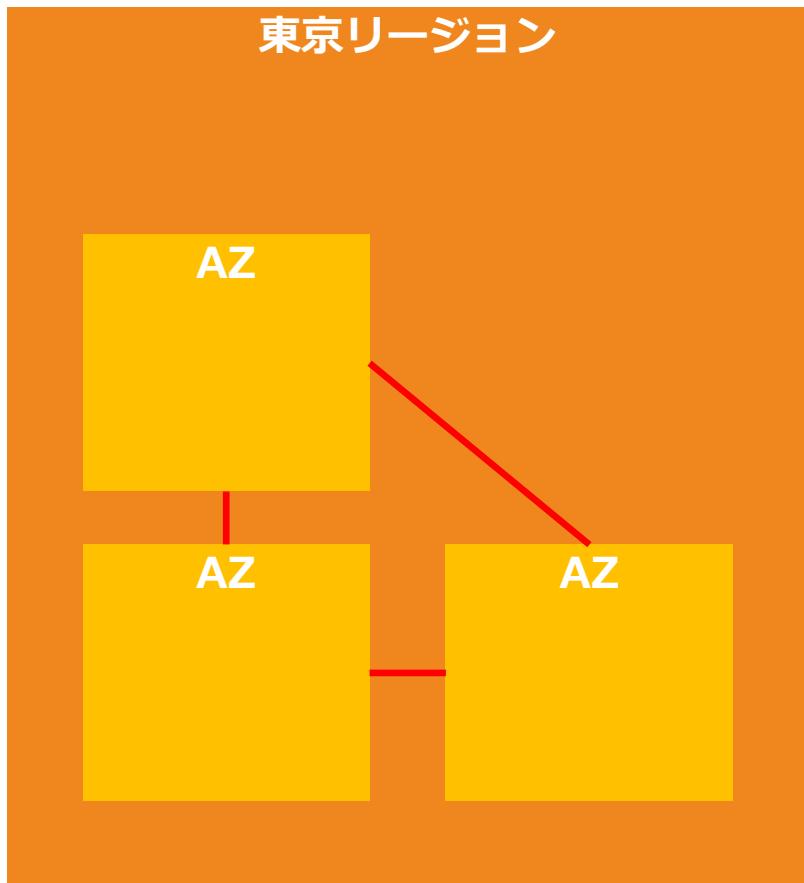
サブネットが存在するゾーンを選択するか、Amazon が選択するゾーンを受け入れます。

指定なし	▲
<input type="text"/>	
指定なし	
アジアパシフィック (東京) / ap-northeast-1a ID: apne1-az4 ネットワークボーダーグループ: ap-northeast-1	ap-northeast-1
アジアパシフィック (東京) / ap-northeast-1c ID: apne1-az1 ネットワークボーダーグループ: ap-northeast-1	ap-northeast-1
アジアパシフィック (東京) / ap-northeast-1d ID: apne1-az2 ネットワークボーダーグループ: ap-northeast-1	ap-northeast-1



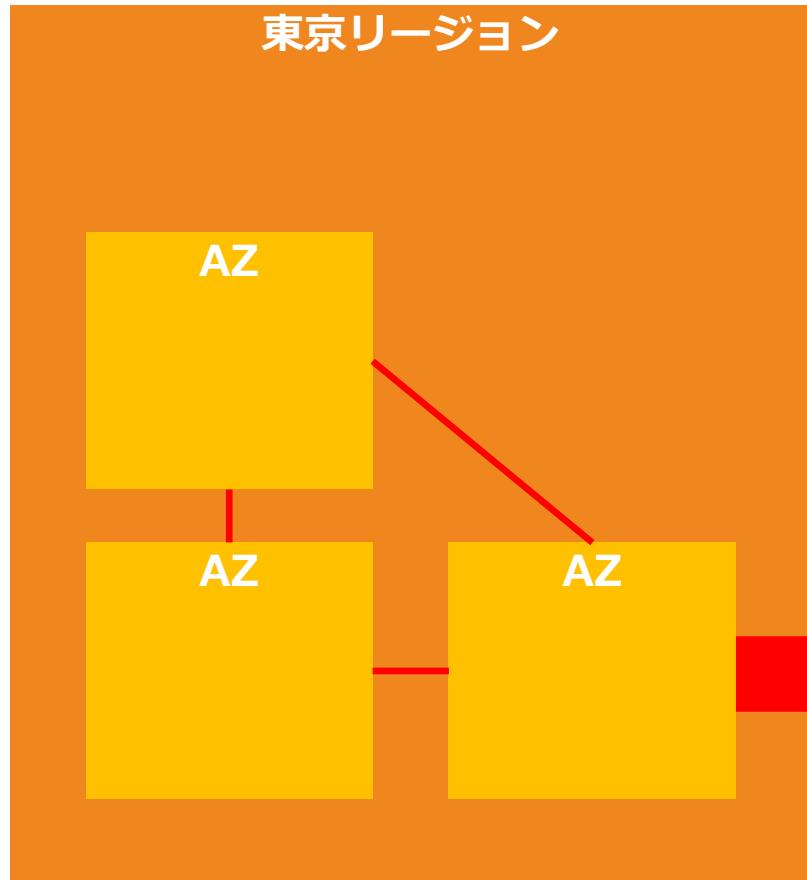
アベイラビリティゾーン (AZ)

同リージョン内のAZ同士は低レイテンシーのリンクで接続されている

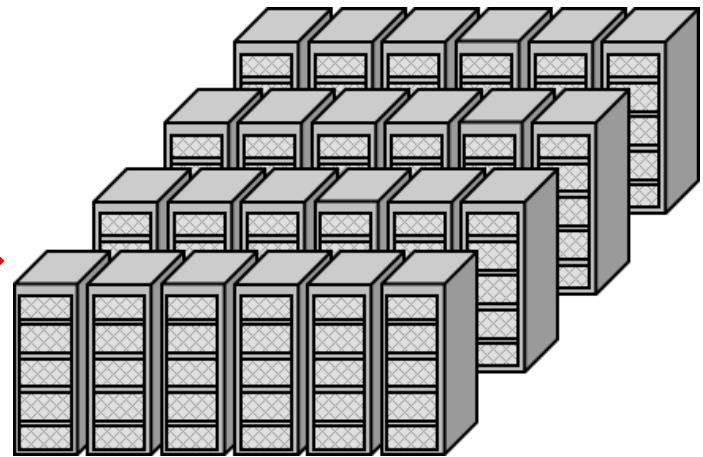


アベイラビリティゾーン (AZ)

AZは1つの複数の物理的なデータセンターで構成されている

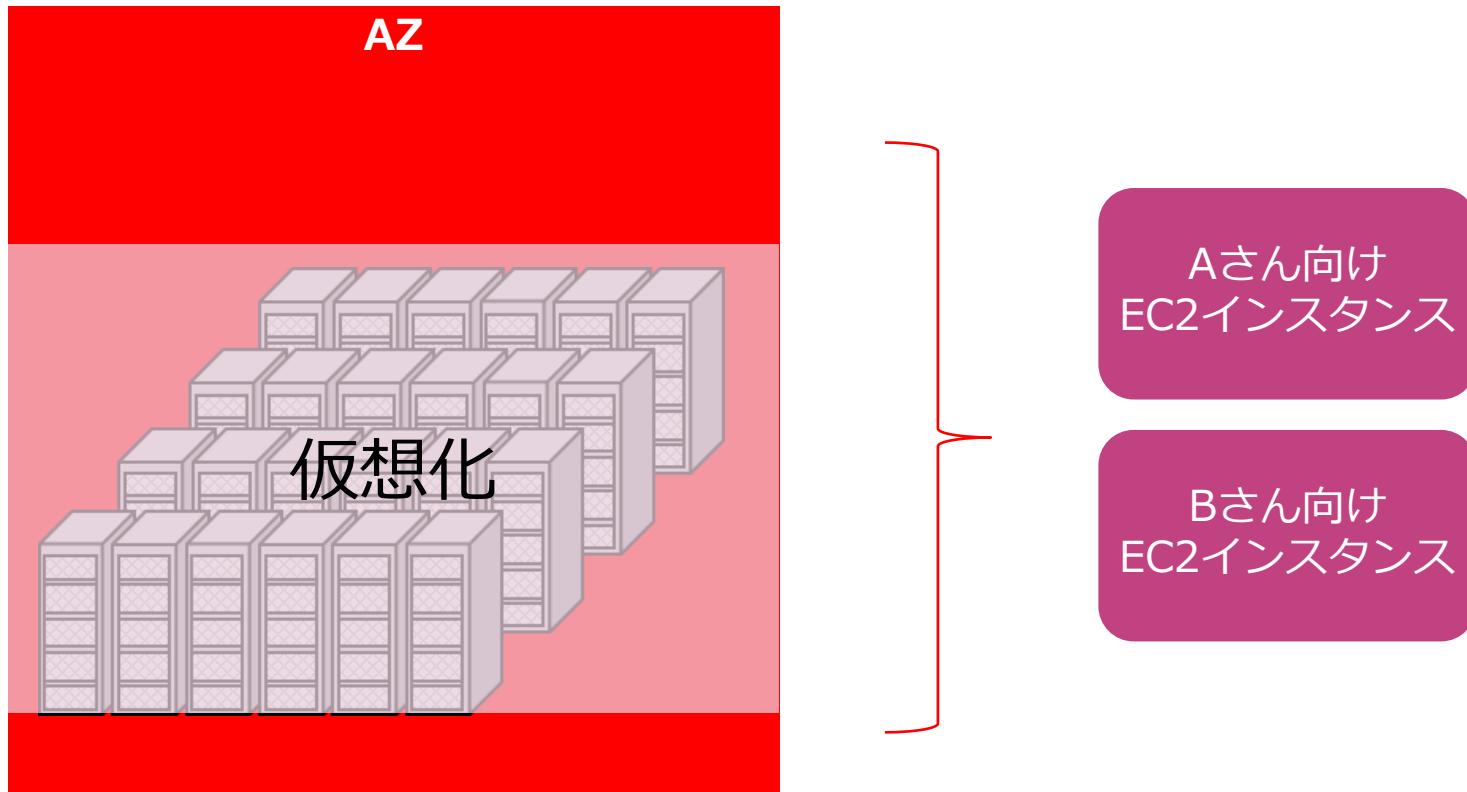


- ✓ AZは1つ以上のデータセンターで構成されている。
- ✓ データセンターにある多数のサーバーがAWSサービスを提供している



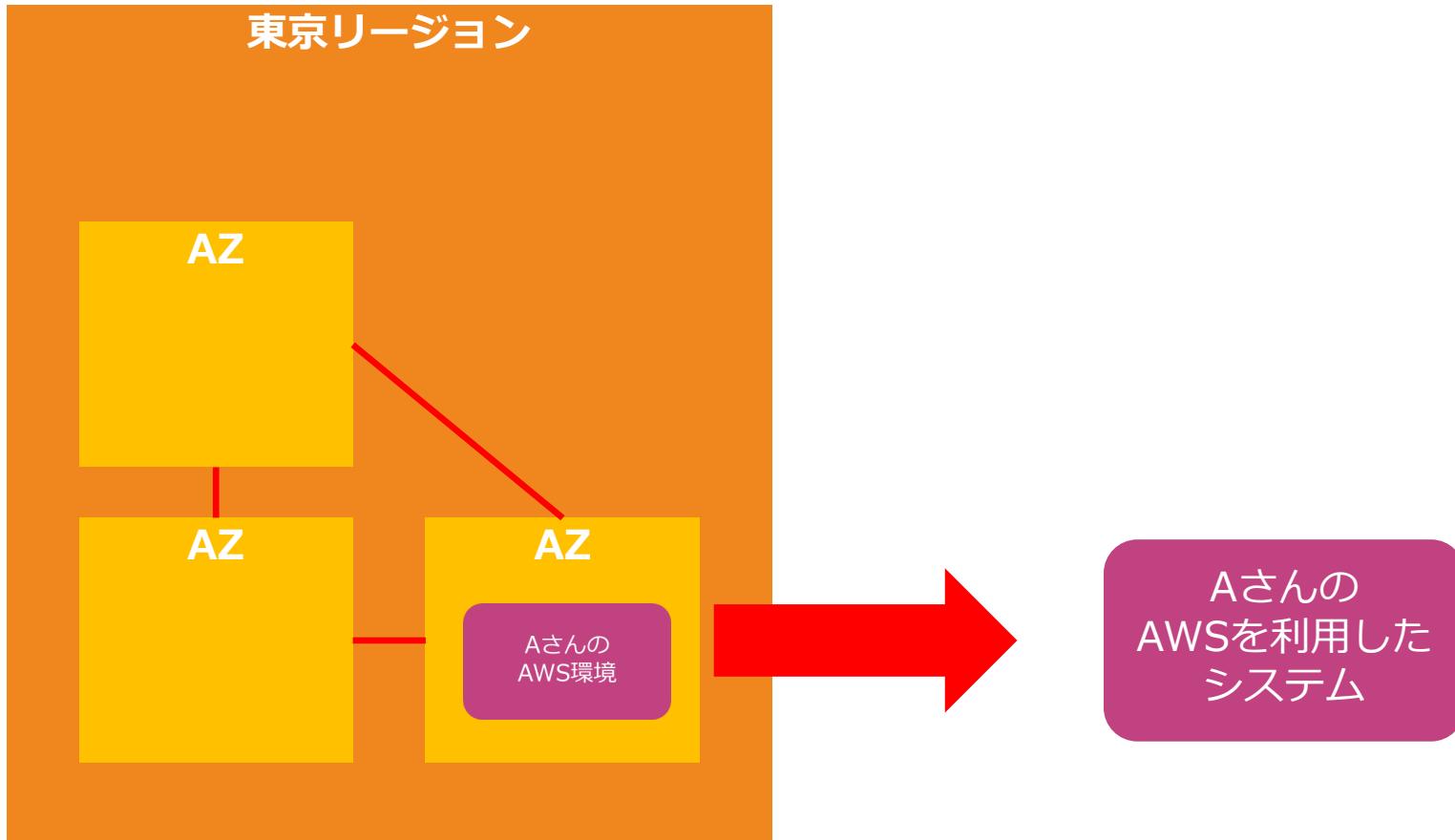
アベイラビリティゾーン (AZ)

AZにある物理インフラを仮想化してユーザーにインフラ機能をサービスとして提供している



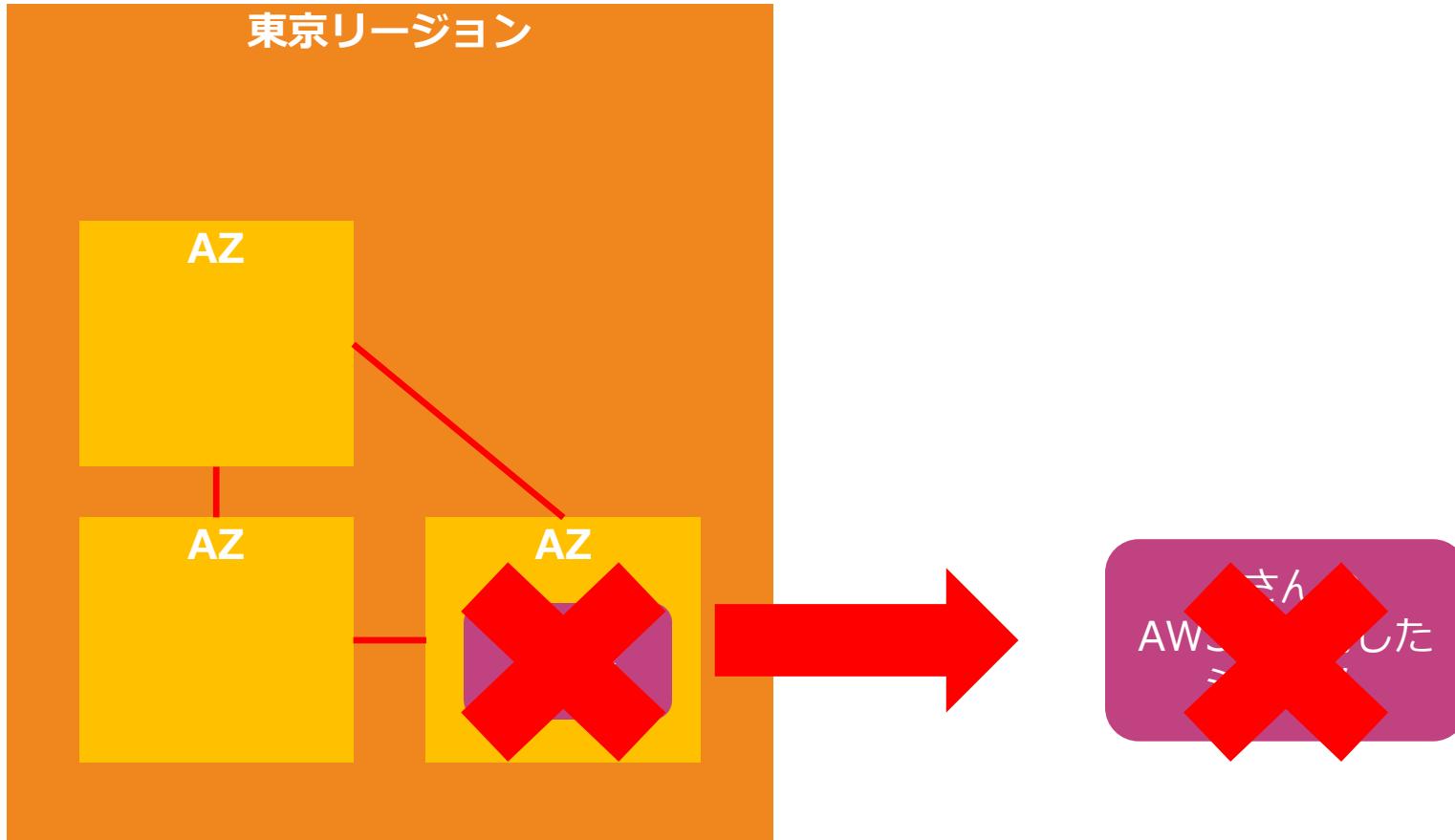
アベイラビリティゾーン (AZ)

よって、1つのAZ内のみでAWSサービスを利用しているとデータセンターの停止によるサービス停止の可能性がある



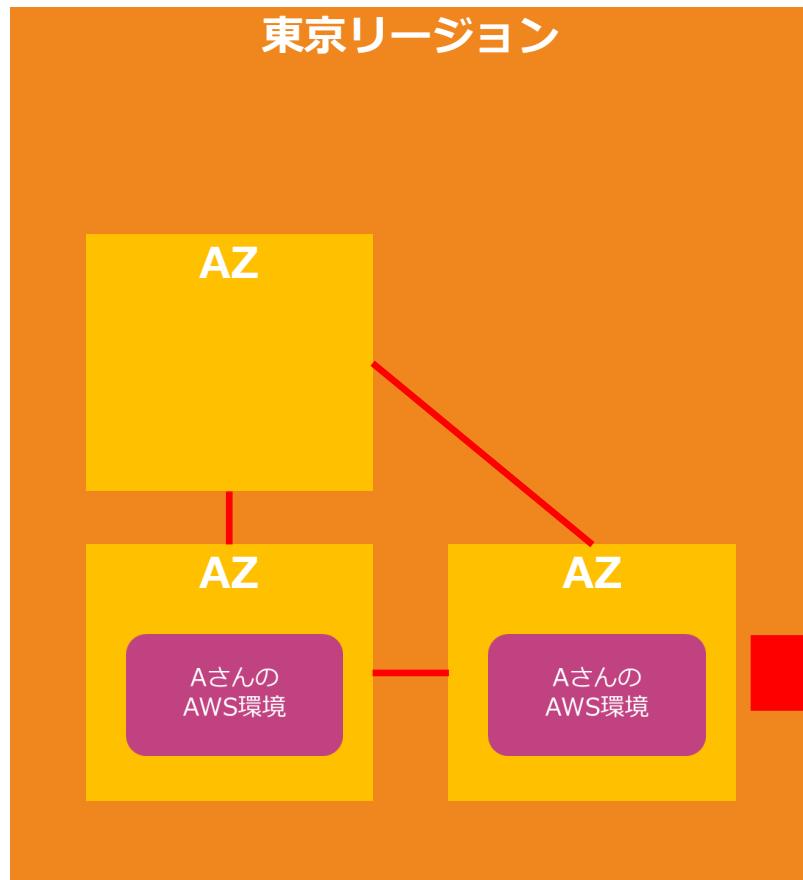
アベイラビリティゾーン (AZ)

よって、1つのAZ内のみでAWSサービスを利用しているとデータセンターの停止によるサービス停止の可能性がある



アベイラビリティゾーン (AZ)

複数AZで分けて信頼性の高いシステム構成にするのが基本的なAWSアーキテクチャとなる



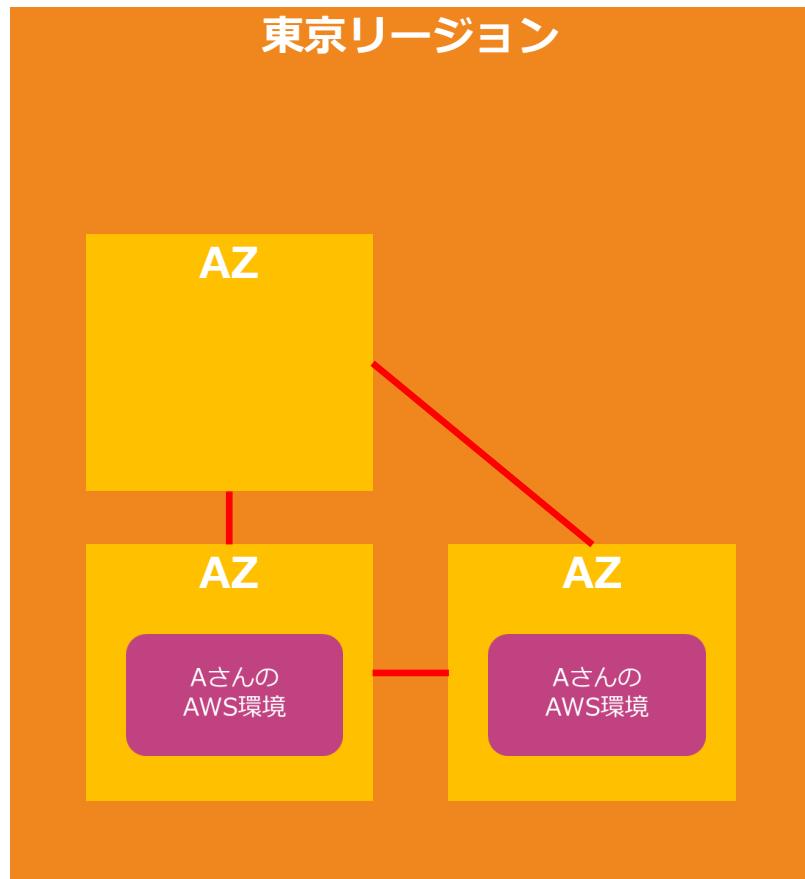
【推奨】
1つのリージョンに2つのAZから始める

Aさんの
AWSを利用した
システム



アベイラビリティゾーン (AZ)

複数AZを跨ぐと物理的な耐久性などが向上するが、システム間の連携や共有が制限される

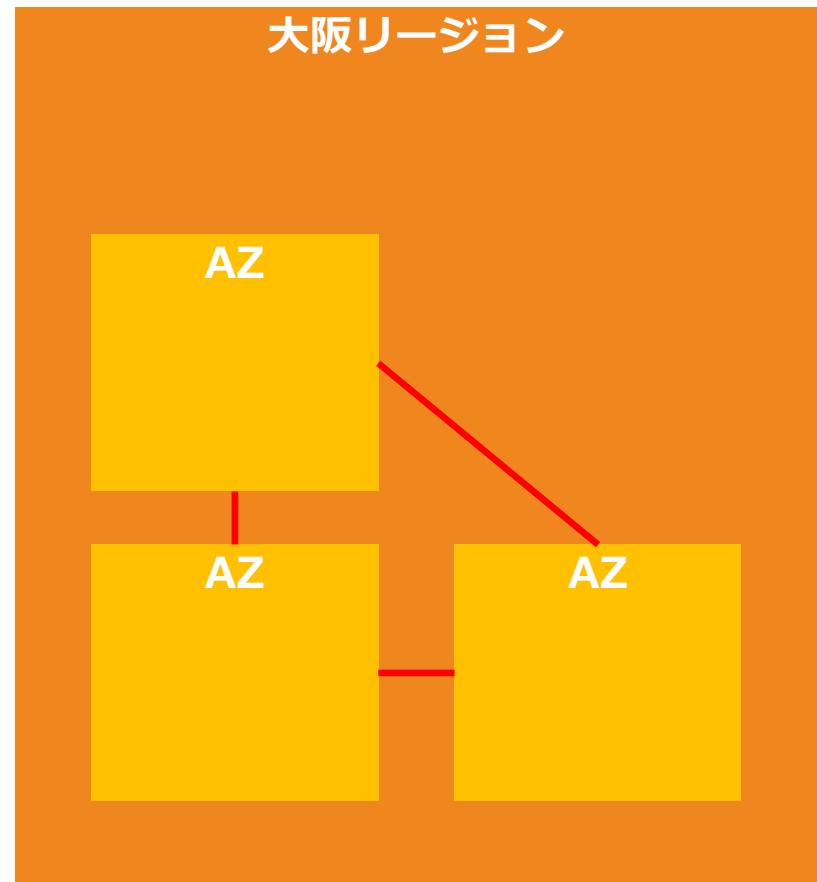
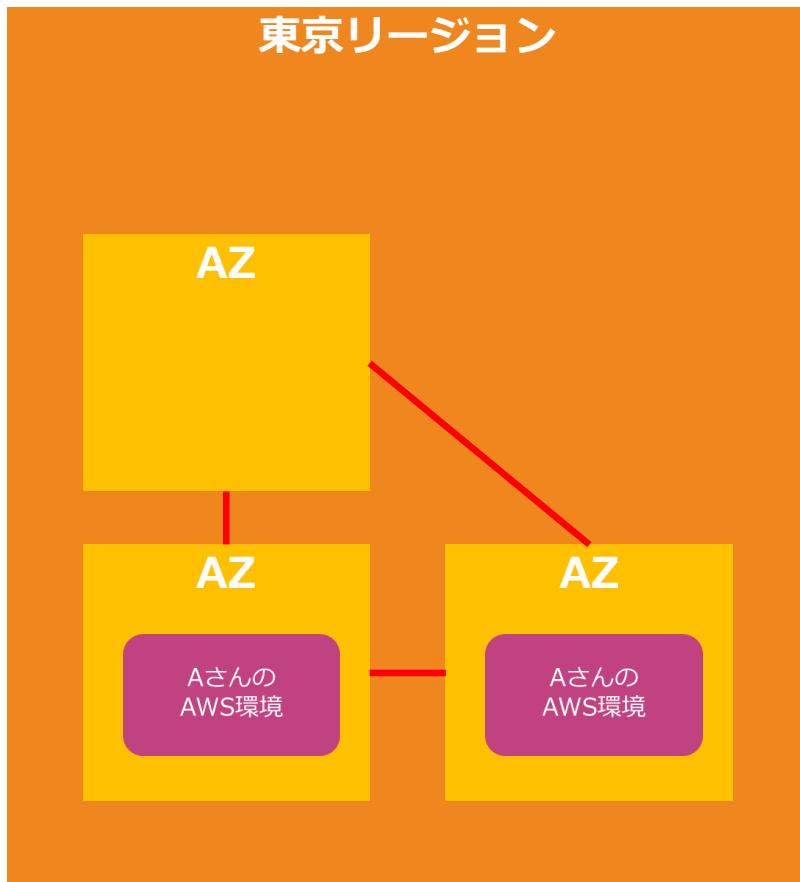


- ✓ 単一AZ内でしか共有されない設定などが多い
- ✓ 多くはAZ間で連携するための設定が必要



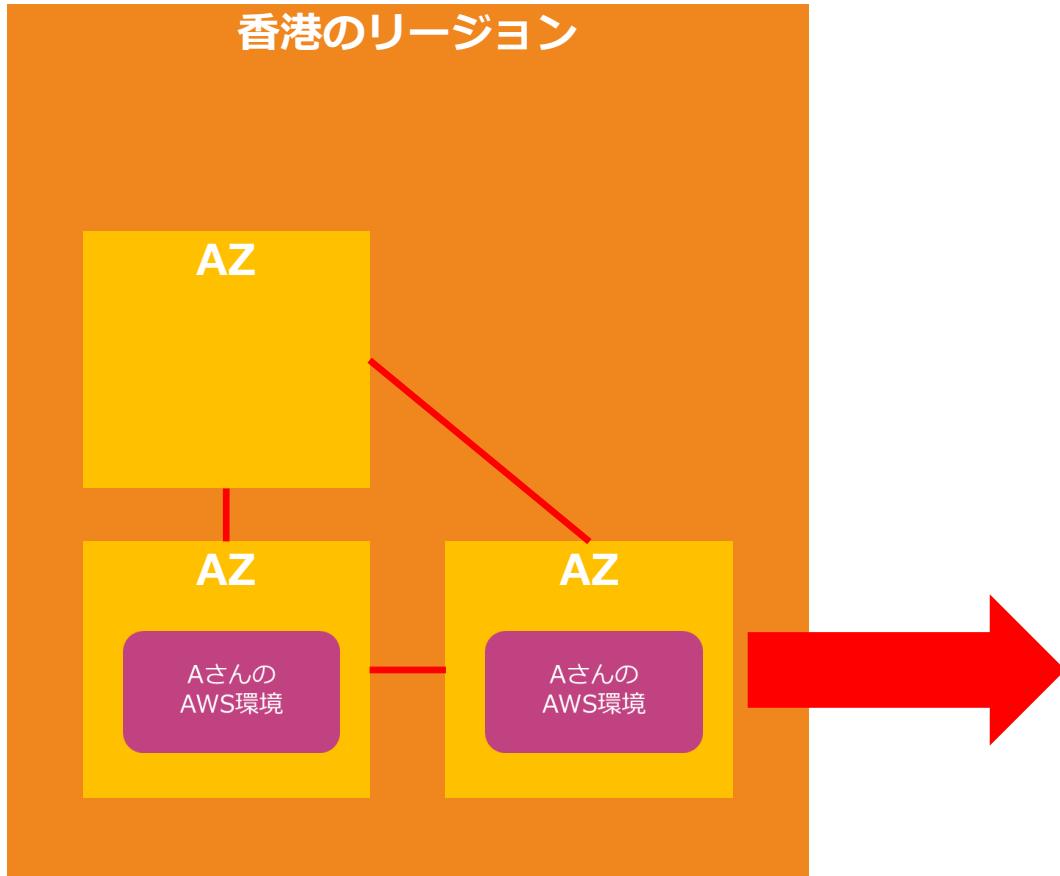
リージョンの選択

データやシステムに係る法律や社内規定を考慮し、基本的には自身の身近なリージョンを選択してAWSシステムを構築する



リージョンの選択

リージョンのある国の法律に影響される可能性も考慮する

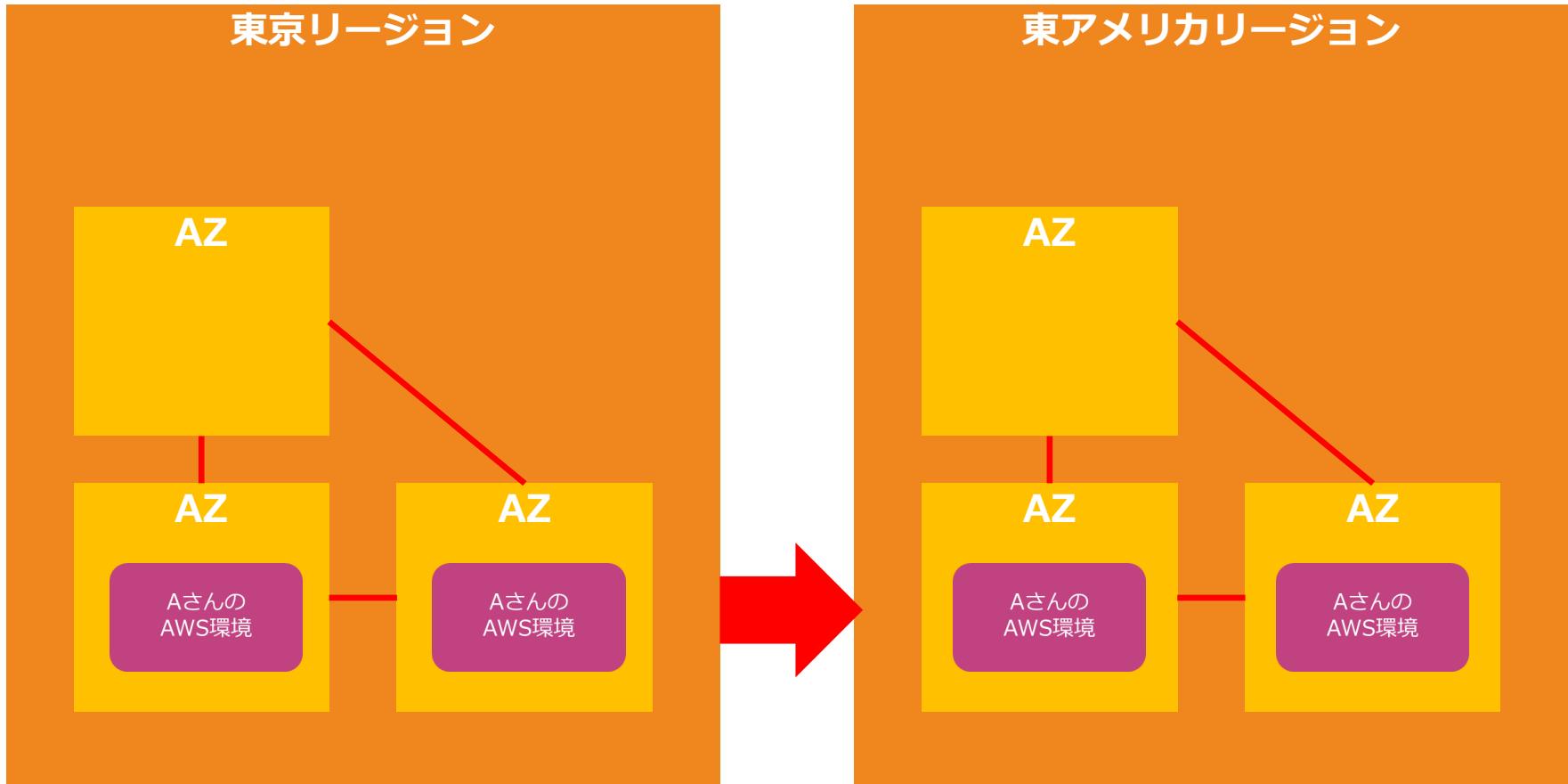


- ✓ 中国政府の要請に従いAWS中国はデータを提示する義務が生じる
- ✓ 中国内のデータの持ち出し制限がある



リージョンの選択

事業継続性計画（BCP）などの対策のためデータや予備システムとして別リージョンを利用する



エッジロケーション

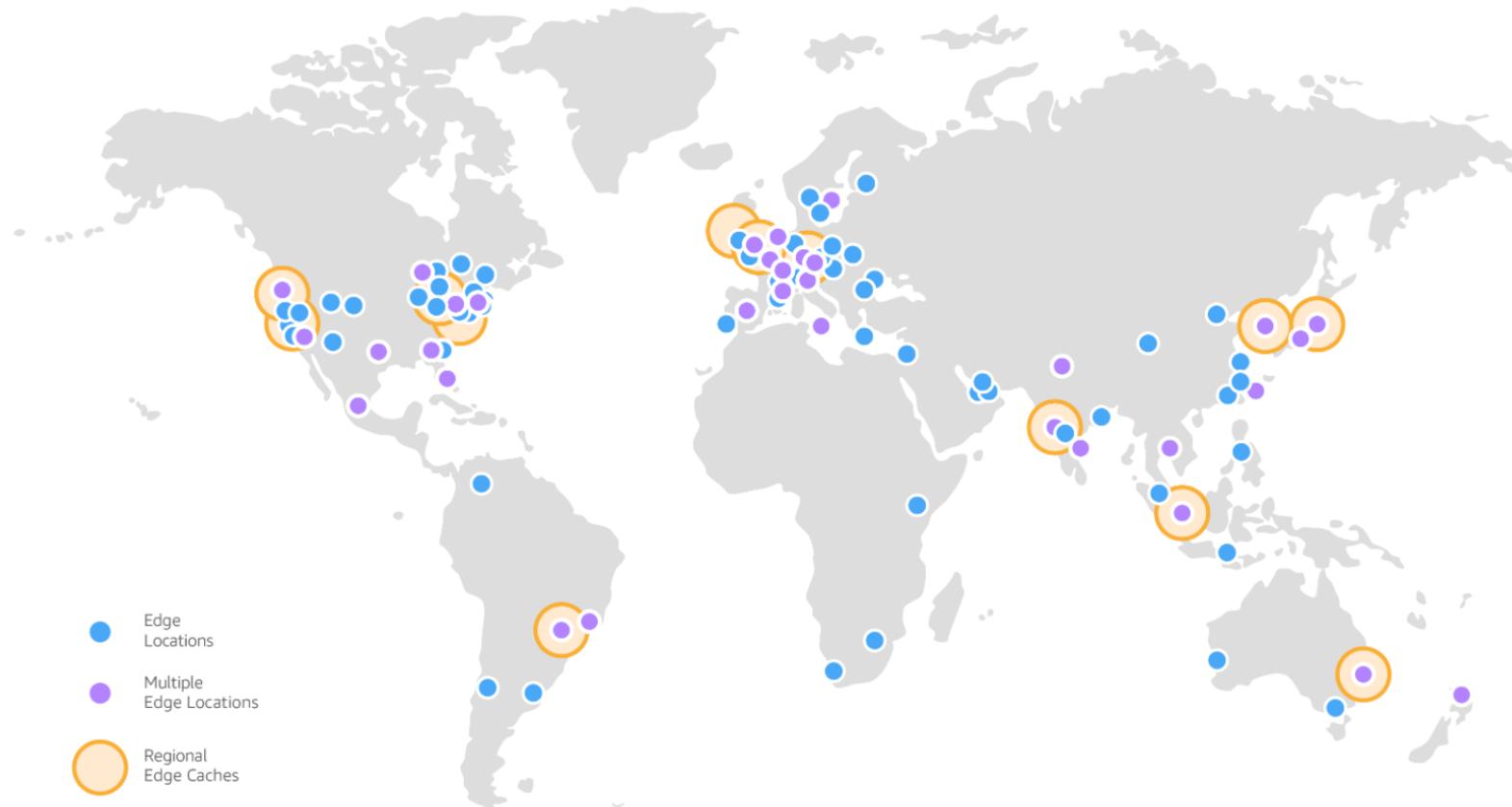
グローバルにコンテンツ配信に利用されるロケーションのこと

- ✓ AWSのAZを構成するデータセンターとは別にコンテンツ配信を実行する高速・広帯域なネットワークロケーションのこと
- ✓ 47か国 90以上の都市にある 310以上のPOP (Point Of Presence) (300以上のエッジロケーションと 13のリージョン別エッジキャッシュ) で構成される。
- ✓ リージョン別エッジキャッシュのキャッシュは個別のPOPよりも大きいため、オブジェクトは最も近いリージョン別エッジキャッシュロケーションでより長くキャッシュを残せる。



エッジロケーション

グローバルにコンテンツ配信に利用されるロケーションのこと

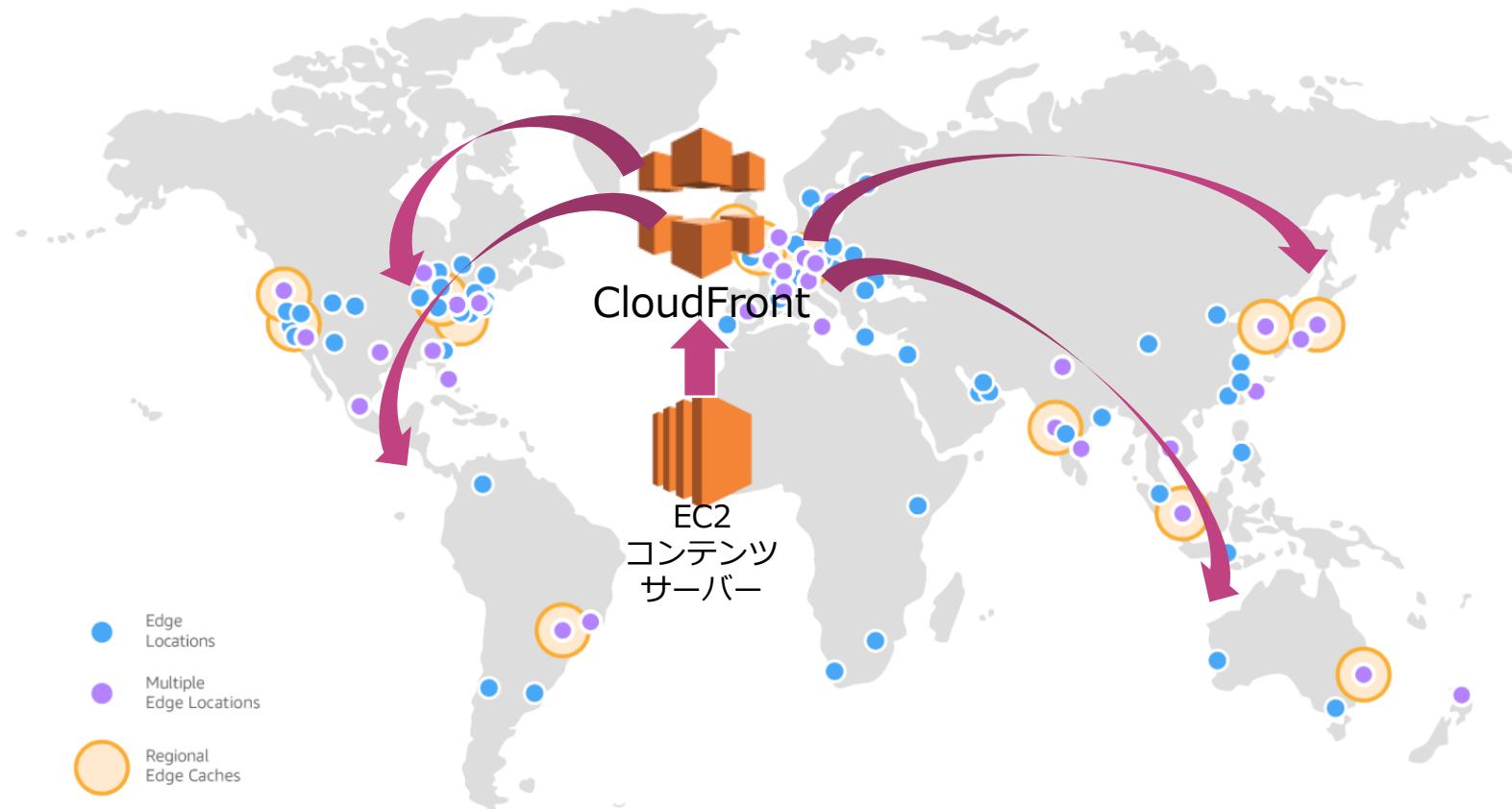


参照: <https://aws.amazon.com/jp/cloudfront/features/?whats-new-cloudfront.sort-by=item.additionalFields.postDateTime&whats-new-cloudfront.sort-order=desc>



エッジロケーション

グローバルにコンテンツ配信に利用されるロケーションのこと

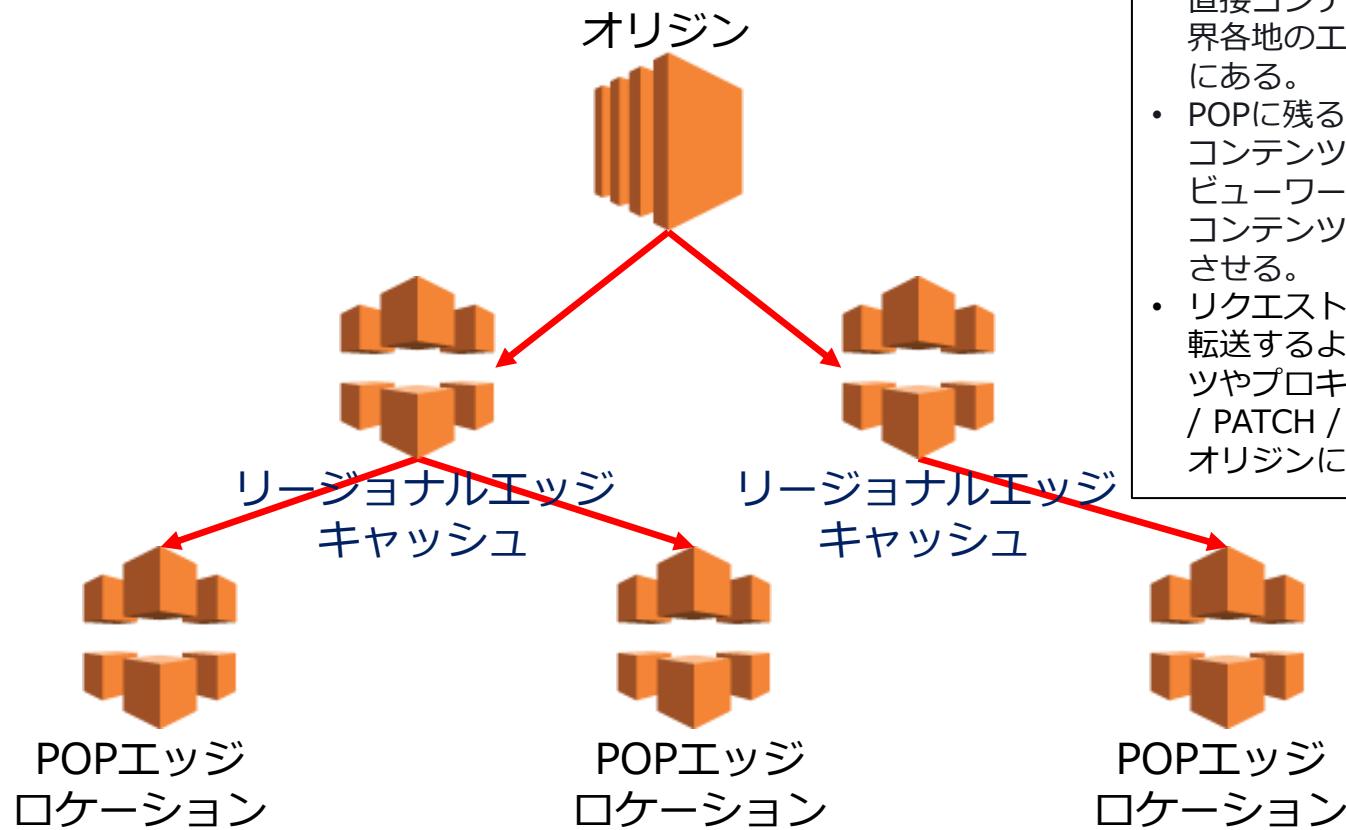


参照: <https://aws.amazon.com/jp/cloudfront/features/?whats-new-cloudfront.sort-by=item.additionalFields.postDateTime&whats-new-cloudfront.sort-order=desc>



エッジロケーション

リージョナルエッジキャッシュが追加されより効率的な配信処理が可能になった



- リージョナルエッジキャッシュは、オリジンサーバーと、ビューワーに直接コンテンツを提供するPOP（世界各地のエッジロケーション）の間にある。
- POPに残るような人気が十分にないコンテンツでも、中間地点としてビューワーの近くに配置して、そのコンテンツのパフォーマンスを向上させる。
- リクエスト時にすべてのヘッダーを転送するように構成されたコンテンツやプロキシメソッドPUT / POST / PATCH / OPTIONS / DELETEはオリジンに直接移動する。

CloudFront ポイントオブプレゼンス (POP) は、人気のあるコンテンツをなるべくユーザーの近くに配置されたエッジロケーション



AWSローカルゾーン

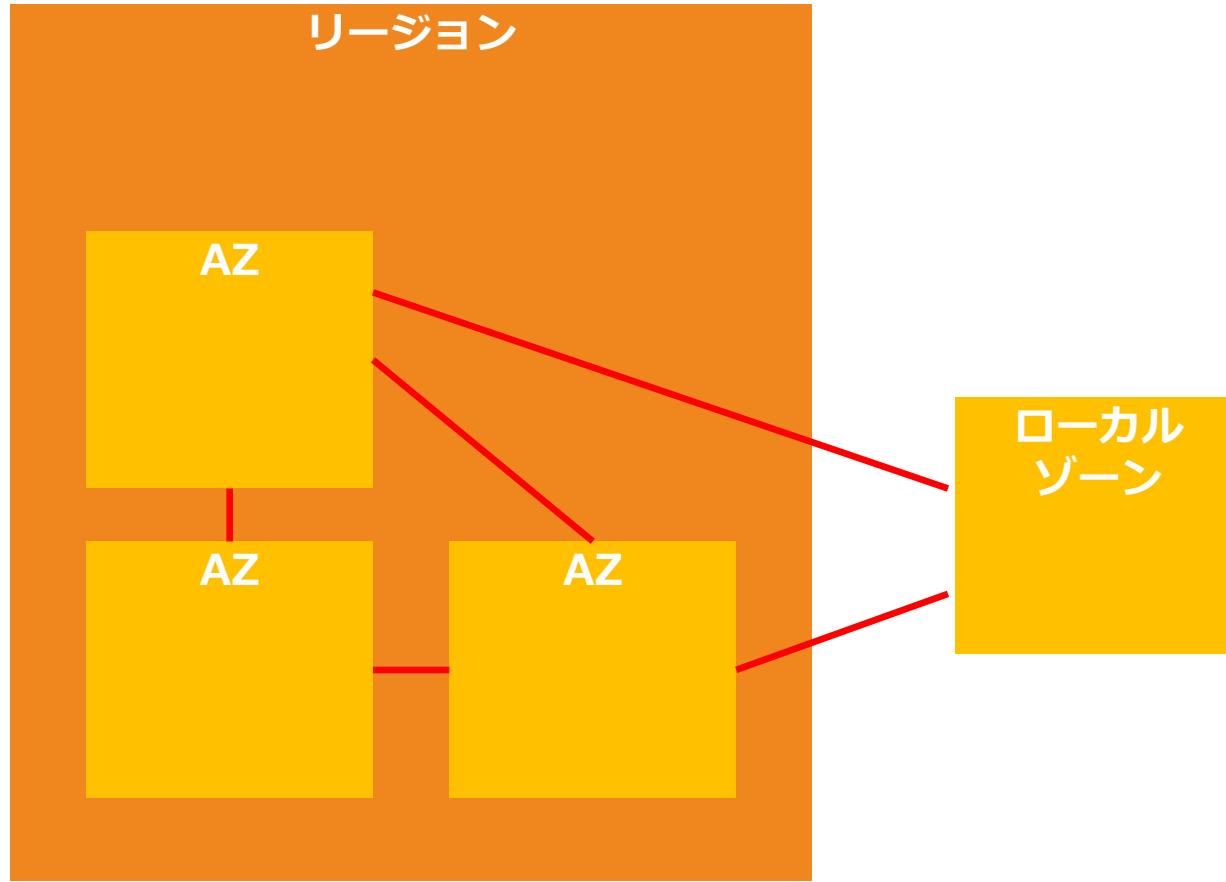
レイテンシーの影響を受けやすいアプリケーションをエンドユーザーにより近い場所で実行するためのロケーション

- ✓ 1 桁ミリ秒単位のレイテンシーを要求する革新的なアプリケーションを、エンドユーザーとオンプレミスインストールにより近い場所で提供
- ✓ リージョンから距離がある大都市（人口の多い場所や産業の中心地）の近くで高速アプリケーションを展開するための特別なロケーション
- ✓ コンピューティング、ストレージ、データベース、およびその他の選択された AWS のサービスをエンドユーザーに近い場所に配置する
- ✓ ローカルとAWSリージョンでそれぞれ実行中のワーカーロード間で高帯域幅かつ安全な接続が利用できる。



ローカルゾーン

リージョンから離れたユーザーに近い場所にサービスを提供するロケーションのこと。



Wavelength Zone

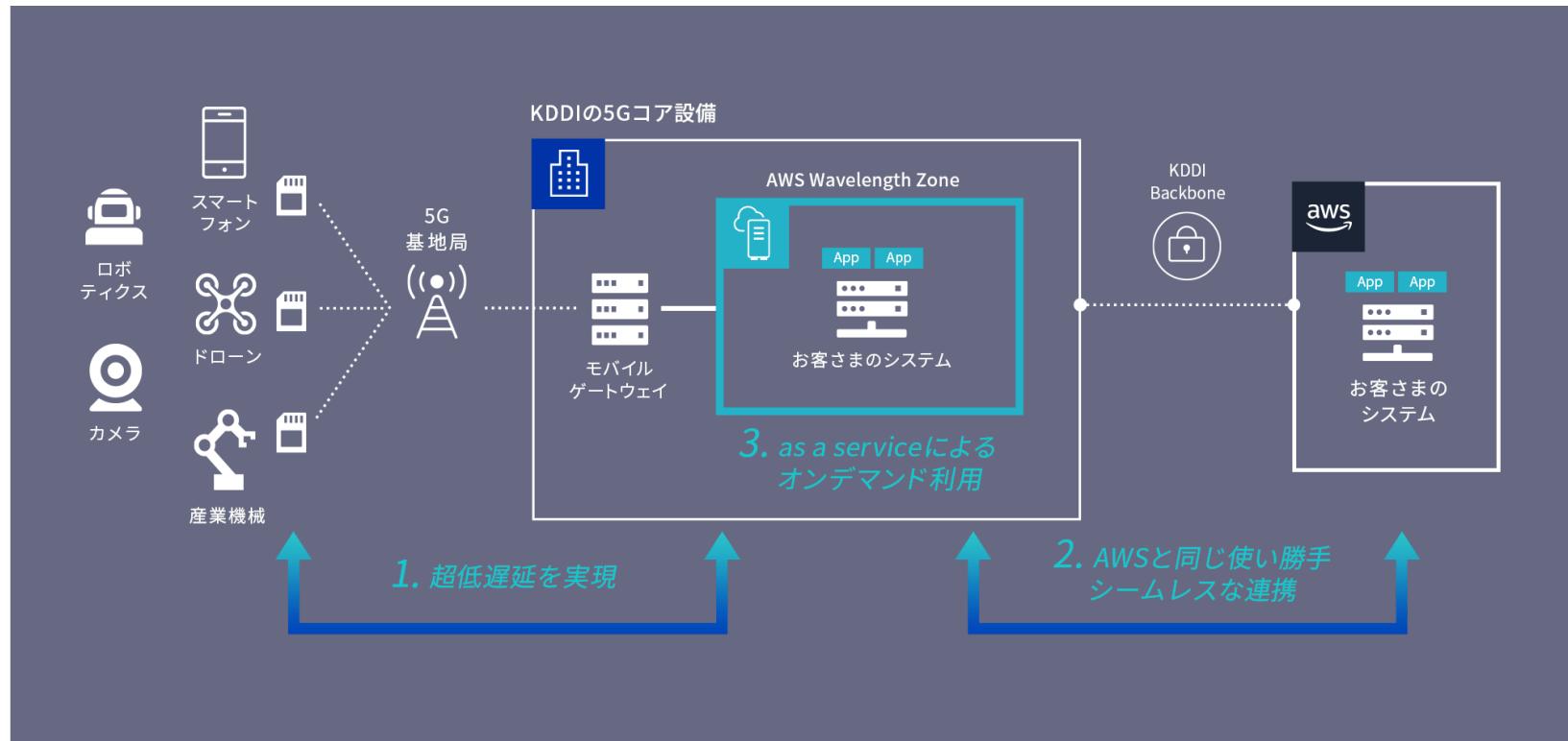
5Gネットワークを利用した高速アプリケーションを開発できる
□ケーションこと

- ✓ 5Gネットワークのエッジにある通信プロバイダーのデータセンターに、AWS のコンピューティングおよびストレージサービスを組み込んだ AWS インフラストラクチャのデプロイ可能な□ケーション
- ✓ モバイルデバイスおよびエンドユーザーに対して 10 ミリ秒未満のレイテンシーを実現するアプリケーションを構築できる
- ✓ ゲーム、ライブ動画ストリーミング、エッジでの機械学習推論、拡張現実やバーチャルリアリティ (AR/VR) など、10 ミリ秒未満のレイテンシーが必要なアプリケーションを実現



Wavelength Zone

5Gネットワークを利用した高速アプリケーションを開発できる
□ケーションこと



参照: https://biz.kddi.com/5g/aws_wavelength/



AWSサービスの全体像



AWSの仕組み

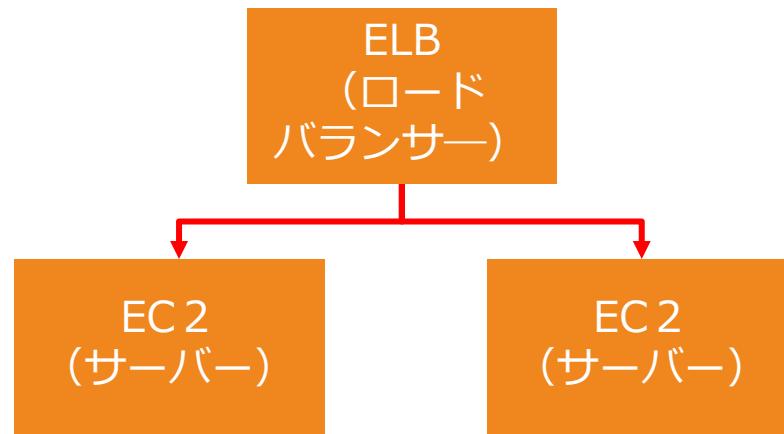
インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み

EC2
(サーバー)



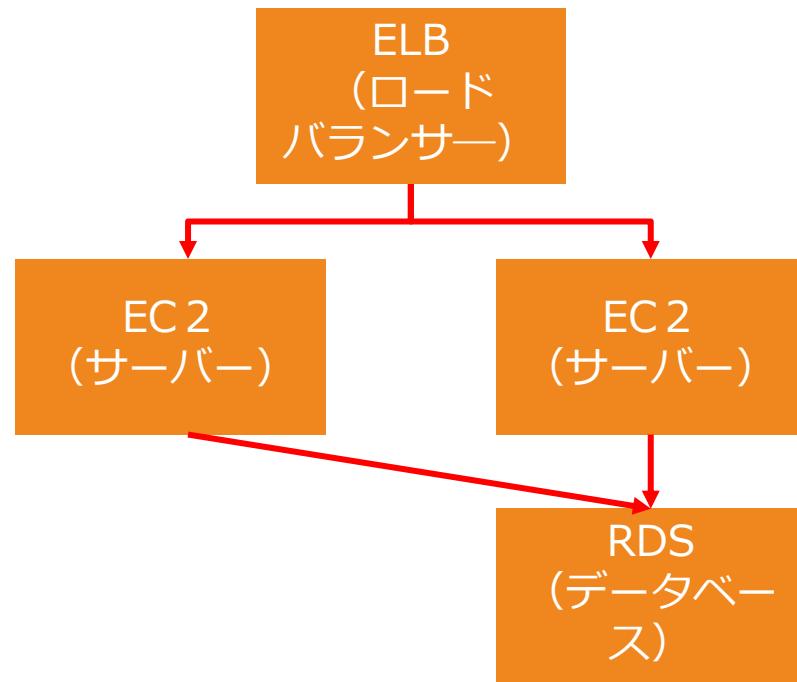
AWSの仕組み

インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み



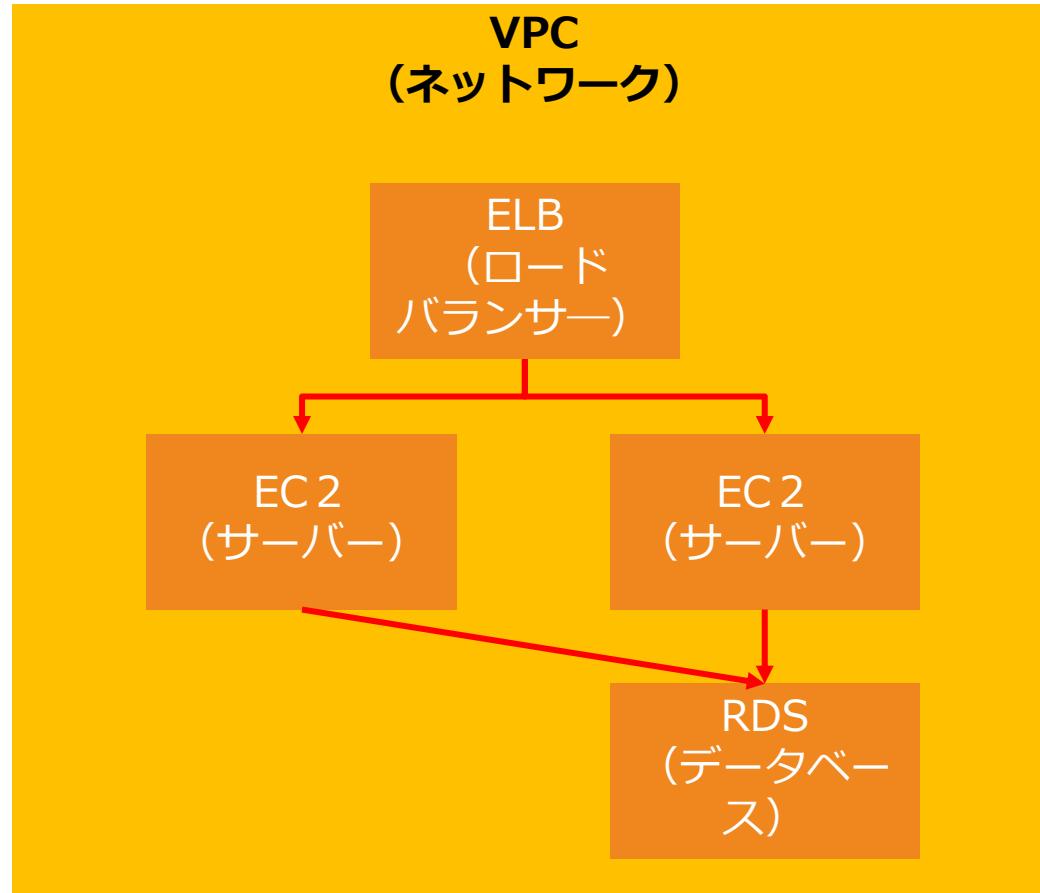
AWSの仕組み

インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み



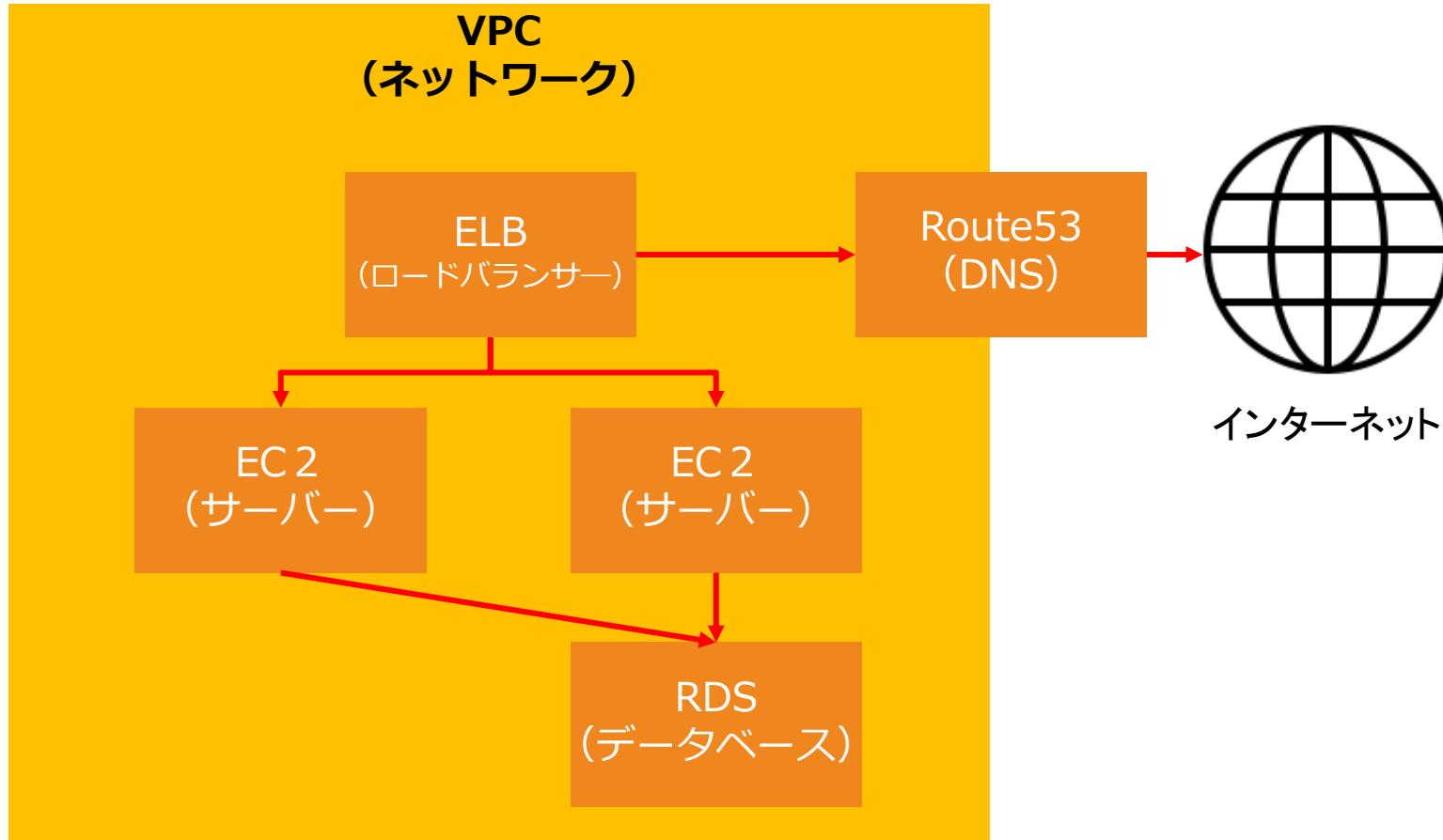
AWSの仕組み

インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み



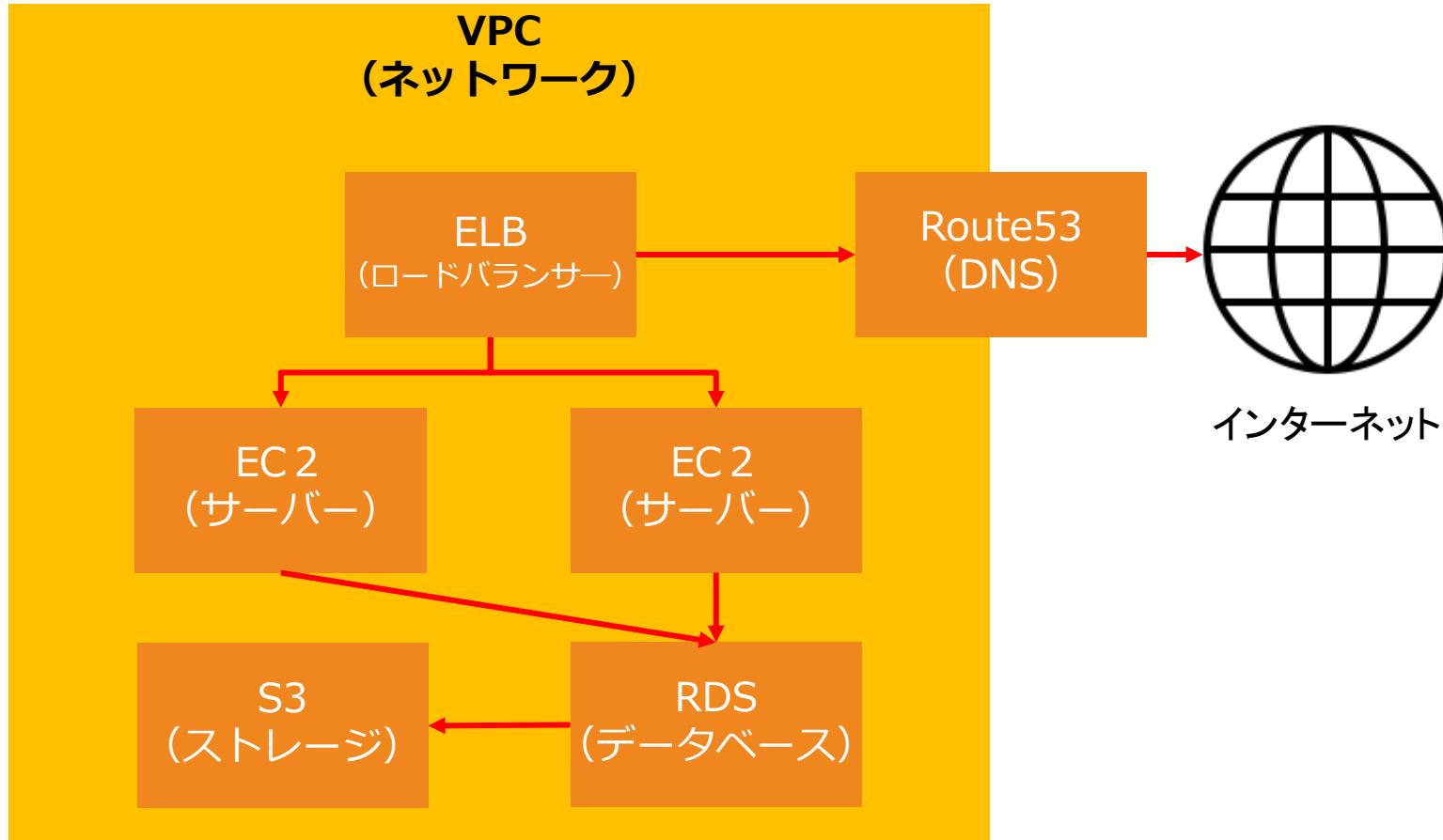
AWSの仕組み

インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み



AWSの仕組み

インフラ／システム機能をブロックパーツのようにオンライン上に組合わせて自分の好きな構成を実現する仕組み



コンピューティング

アプリケーションを構築する際に利用するサーバーなどのコンピューティングを提供するサービス

コンピューティング
(サーバー)



コンピューティング

アプリケーションを構築する際に利用するサーバーなどのコンピューティングを提供するサービス

Amazon EC2	AWSを利用して仮想サーバーを立ち上げるサービス
ELB	EC2インスタンスのトラフィック制御を実施するロードバランサーサービス
Auto Scaling	EC2インスタンスを自動で増やしたり、減らしたり調整してくれる（これをスケーリングと呼ぶ）サービス
AWS Lambda	サーバーなし（サーバレスと呼ぶ）でプログラミングコードだけを保存し、実行することができるサービス
Amazon Lightsail	仮想サーバー、ストレージ、データベース、およびネットワーキングのまとまった構成を低価格で提供するサービス
AWS Fargate	コンテナ向けサーバレスコンピューティング



コンピューティング（操作ツール）

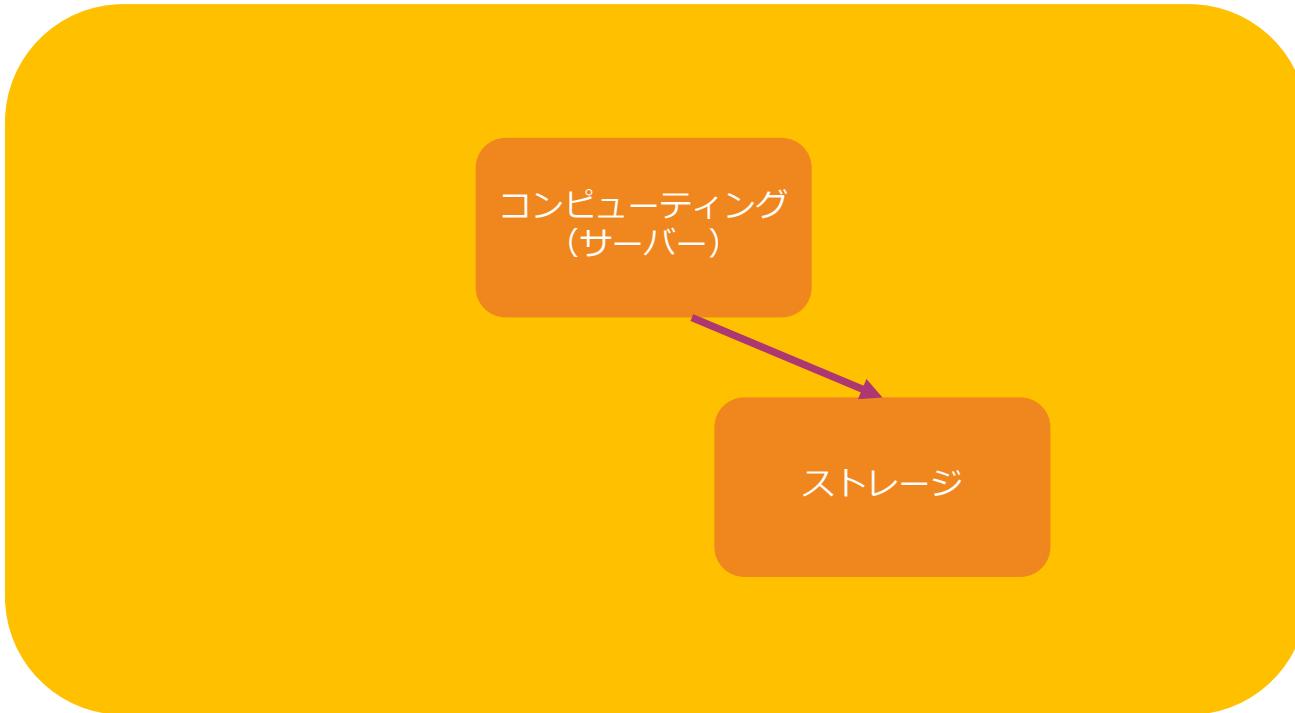
コンピューティングがAWSリソースを操作するツール

AWSマネジメント コンソール	WEBブラウザベースのAWSリソースを操作するGUIツール
AWS CLI	AWS操作を実行するコマンドラインツール
AWS CloudShell	AWS CLI、PowerShell、ECS CLI、SAM CLIが利用可能なブラウザベースのシェルツール。Node.jsやPythonのランタイムも利用可能
EC2 Instance Connect	EC2コンソール画面からSSHなどをを利用して、EC2インスタンスへのシンプルで安全な接続を提供
AWS Copilot	ECS向けのコマンドラインツール



ストレージ

データ保存やデータ処理に利用する多様なストレージが用意されている。



ストレージ

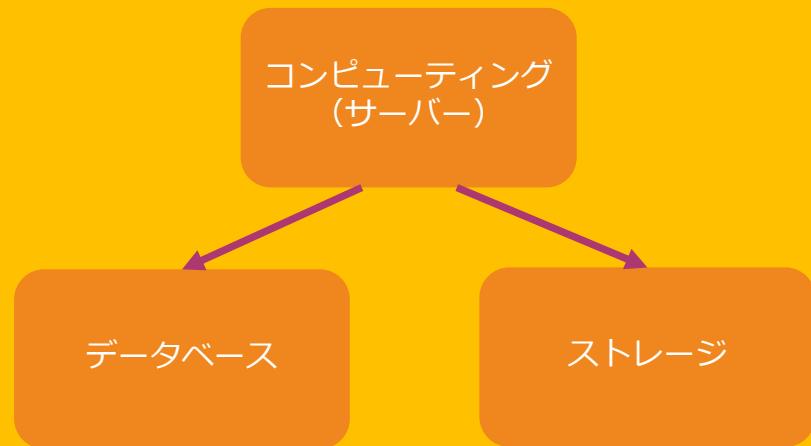
データ保存やデータ処理に利用する多様なストレージが用意されている。

Amazon Simple Storage Service (S3)	中長期に頻繁に利用するデータを大量に保存するためのオブジェクト型ストレージサービス
Amazon Elastic Block Store (EBS)	EC2にネットワークを介してアタッチして利用するEC2インスタンス専用のブロック型ストレージ
インスタンスストア	EC2に物理的に接続されているブロック型ストレージ データの一時保存用ストレージ
Amazon Elastic File System (EFS)	ディレクトリ構造でファイルデータを保存するのに向いている NFSファイルシステムを提供するサービス
Amazon S3 Glacier	S3と同じ可用性と耐久性を有しつつ、より価格の安いストレージサービス。データのアーカイブや長期バックアップに使用する
Amazon FSx	4タイプのファイルストレージを構成できるサービス。機能豊富で高性能なファイルシステムのクラウド上の起動、実行およびスケーリングを簡単かつコスト効率の高いものにする。
AWS Storage Gateway	オンプレミス環境のストレージをAmazon S3へと拡張するハイブリッドストレージサービス



データベース

AWSでは様々なタイプのデータベースがマネージド型サービスで提供されている



データベース（リレーションナル型）

AWSでは様々なタイプのデータベースがマネージド型サービスで提供されている

Amazon RDS	MySQL、PostgreSQL、Oracle、SQL Server、MariaDBと互換性のあるリレーションナルデータベースサービス
Amazon Aurora	MySQL および PostgreSQL と互換性のある分散・高速化された高性能リレーションナルデータベース
Amazon Redshift	AWS上で業務データ解析基盤を提供するデータウェアハウス
Amazon RDS Custom	基盤となるOSやDB環境へのアクセスが可能なマネージドデータベースサービス。SQL ServerとOracle版が対応可能
Amazon RDS on Outposts	RDSなどのフルマネージド型のデータベースインスタンスをオンプレミス環境にデプロイすることができる。



データベース（NoSQL型）

AWSでは様々なタイプのデータベースがマネージド型サービスで提供されている

Amazon DynamoDB	規模に関係なく数ミリ秒台のパフォーマンスを実現するキーバリュー型およびドキュメント型のNoSQLデータベース
Amazon ElastiCache	Redis または Memcachedと互換性のある完全マネージド型のインメモリデータストア
Amazon DocumentDB	ミッションクリティカルなMongoDB のワークロードを運用するための、スケーラブルかつ高い耐久性のフルマネージド型のNoSQL型データベース
Amazon Keyspaces	Apache Cassandra向けのフルマネージド型のNoSQL型データベースサービス
Amazon Neptune	ID グラフ、ナレッジグラフ、不正検出などのグラフのユースケースを強力にサポートする高速のグラフデータベース
Amazon Timestream (時系列DB)	IoT および運用アプリケーションに適した、高速かつスケーラブルなサーバーレス時系列データベースサービス



データベース（サーチ/分散台帳）

AWSでは様々なタイプのデータベースがマネージド型サービスで提供されている

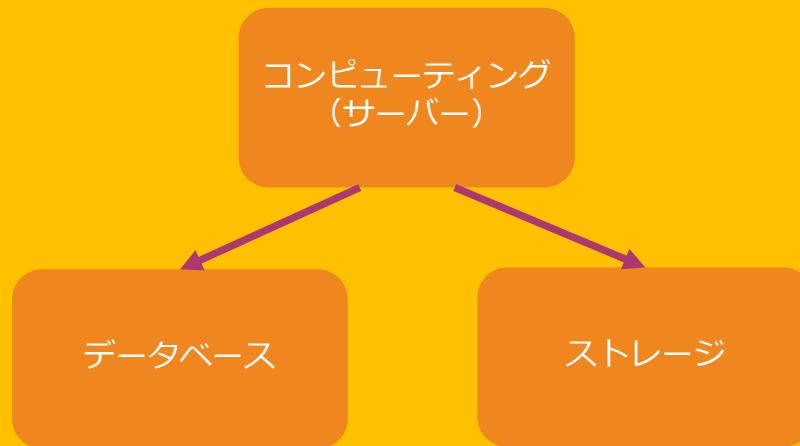
Amazon QLDB	フルマネージド型の台帳データベース。透過的かつイミュータブルで、暗号的に検証可能なトランザクションログの保存向き。データの全変更が追跡され、変更履歴が長期間維持される
Amazon OpenSearch Service	AWSでElasticsearchを実行する分散検索/分析エンジンで検索サービスを構築する。
Amazon CloudSearch	検索機能を手軽にWebサイトやアプリケーションに構築、実装できるクラウド型サービス



ネットワーキングとコンテンツ配信

ネットワーク構成やコンテンツ配信・AWS環境への接続設定に利用する多様なサービスが提供される。

ネットワーキングとコンテンツ配信



ネットワーク

オフィス



ネットワーキングとコンテンツ配信

ネットワーク構成やコンテンツ配信・AWS環境への接続設定に利用する多様なサービスが提供される。

Amazon VPC	IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイを設定することで、仮想ネットワーキング環境を構築するサービス
Amazon Route 53	ドメイン登録とルーティングを実施するDNSサーバーの機能を提供するサービス
Amazon CloudFront	エッジロケーションを利用して低レイテンシーの高速転送により世界中にコンテンツを配信するコンテンツ配信ネットワーク(CDN) サービス
AWS Global Accelerator	エッジロケーションを利用して、アプリケーションへのユーザーのトラフィックのパフォーマンスを最大 60% 向上させるネットワーキングサービス



ネットワーキングとコンテンツ配信

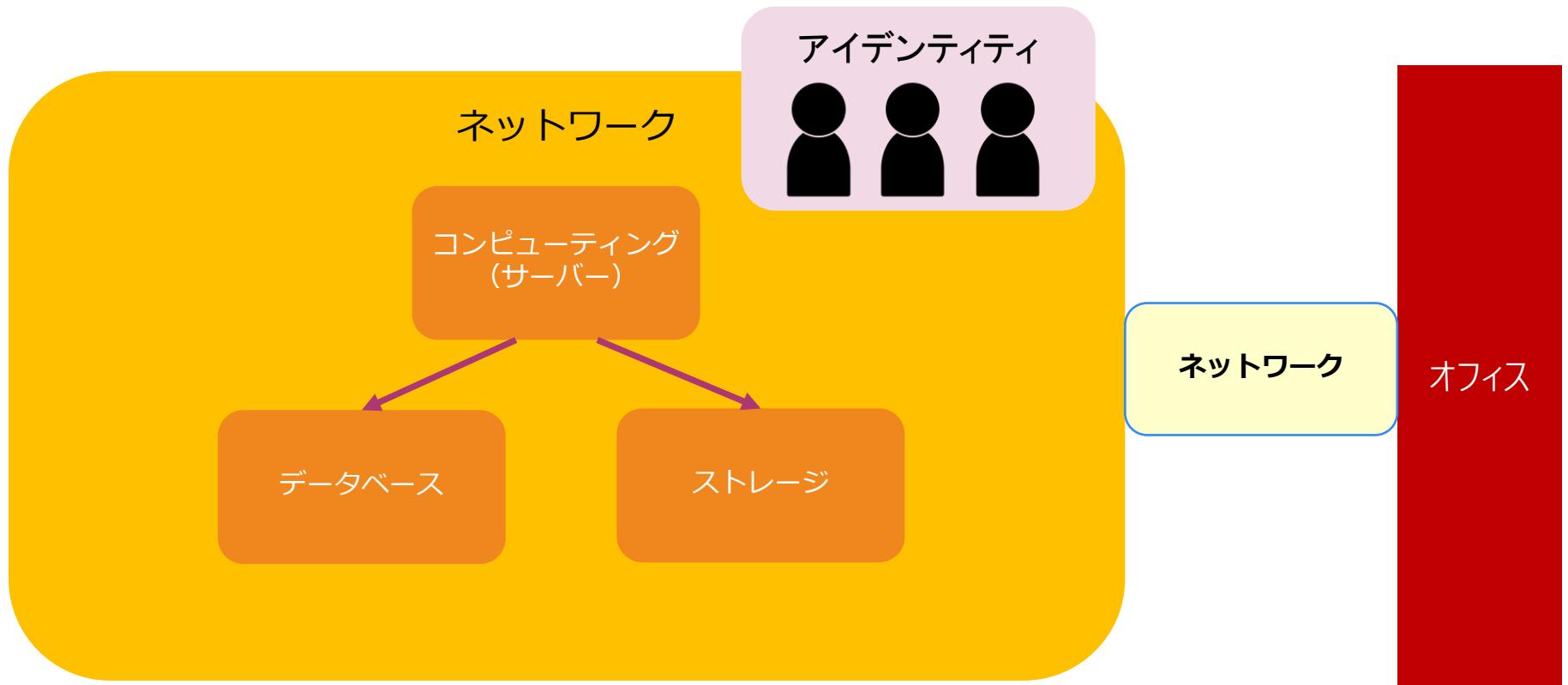
ネットワーク構成やコンテンツ配信・AWS環境への接続設定に利用する多様なサービスが提供される。

AWS Direct Connect	AWSとデータセンターやオフィスとの間にプライベート接続を確立する専用線サービス。AWS Direct Connect SiteLinkでオンプレミス拠点間のプライベートネットワーク接続を容易に実現
AWS Client VPN	ユーザー需要に合わせて自動的にスケールアップまたはスケールダウンする、フルマネージド型で伸縮自在な VPN サービス
AWSサイト間VPN	データセンターまたはオフィスと AWS間の安全な接続を実施。AWS Global Accelerator と連携することにより、サイト間 VPN の高速化オプションはさらに優れたパフォーマンスを提供
AWS Cloud WAN	クラウドとオンプレミス環境のリソース間で実行されるトラフィックを管理するWANサービス。AWSリージョン間のグローバルネットワークを自動的に作成
AWS Transit Gateway	VPC とオンプレミスネットワークを接続する中央ハブとなるクラウドルーター。複数VPCやオフィス間の接続に利用
AWS PrivateLink	データをインターネットに公開せずに、VPC と AWS でホストされているサービス、またはオンプレミス間でプライベート接続を確立する



アイデンティティ

AWSのユーザー管理や認証管理に利用されるサービス



アイデンティティ（ユーザー管理）

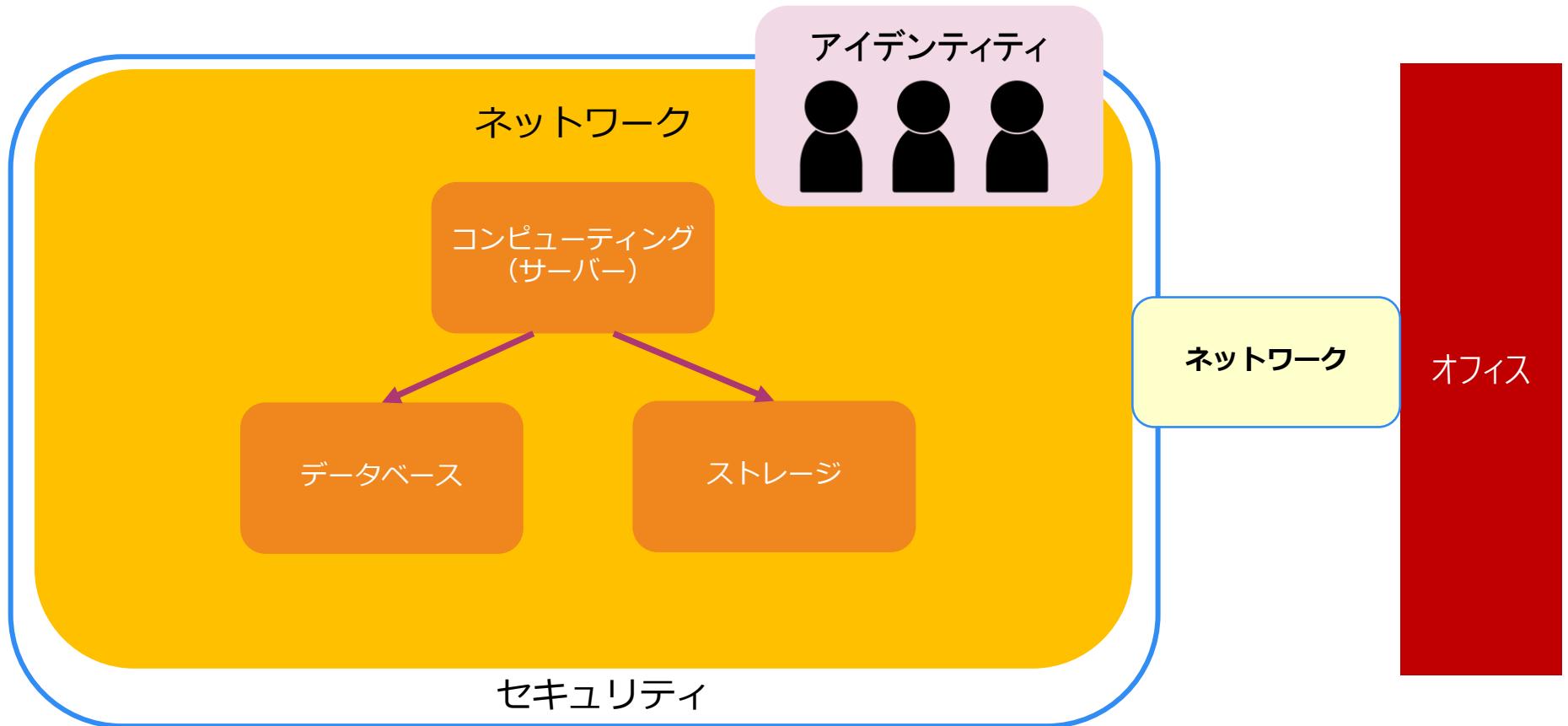
AWSのユーザー管理や認証管理に利用されるサービス

AWS Identity & Access Management (IAM)	AWSサービスを利用するユーザーを作成・管理するサービス
AWS Organizations	複数AWSアカウントを利用する際に、一括請求を実施したり、複数AWSアカウントの一元管理を実施するサービス
AWS Directory Service	オンプレミス環境の代表的な認証システムであるActive Directoryと連携した認証の仕組みを提供するサービス
AWS Single Sign-On (SSO)	オンプレミス環境とAWS環境とのシングルサインオンアクセスをユーザーに提供するAWS サービス
Amazon Cognito	AWS上に構築するWEBアプリケーションにユーザー認証機能を提供するサービス
AWS Security Token Service (STS)	AWS リソースへのアクセスをコントロールできる一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供
AWS Secrets Manager	データベース認証情報、APIキーなどのシークレット情報を管理できるサービス。自動的なパスワードのローテーションが可能



セキュリティ・コンプライアンス

AWSリソースに対するセキュリティやコンプライアンスに寄与するサービス



セキュリティ・コンプライアンス

AWSリソースに対するセキュリティやコンプライアンスに寄与するサービス

AWS WAF	一般的なウェブの脆弱性からウェブアプリケーションまたは API を保護するファイアウォールサービス
AWS Shield	分散サービス妨害 (DDoS) 攻撃からAWSリソースを保護するサービス
AWS Network Firewall	VPCに対して悪意のあるアクティビティの拡散を防ぐなど、ネットワークトラフィックを詳細まで制御できるファイアウォールルールを定義するサービス
AWS Firewall Manager	AWS Organizations にあるアカウントとアプリケーション全体で一元的にファイアウォールのルールを設定、管理できるようにするセキュリティ管理サービス
AWS Security Hub	セキュリティのベストプラクティスのチェックを行い、アラートを集約し、自動修復を可能にするクラウドセキュリティ体制管理サービス



セキュリティ・コンプライアンス（暗号化）

AWSリソースに対するセキュリティやコンプライアンスに寄与するサービス

AWS Key Management Service (KMS)

暗号化用のキーを作成・管理するサービス。幅広い AWS のサービスやアプリケーションの暗号化を制御することができる。

AWS Certificate Manager (ACM)

SSL/TLS証明書を作成・管理するサービス。CloudFrontやELBに証明書を設定して通信を暗号化する。

AWS CloudHSM

クラウドベースのハードウェアセキュリティモジュール (HSM) で、業界標準のFIPS 140-2 のレベル 3 認証済みの HSM を使用して、暗号化キーを管理する。



セキュリティ・コンプライアンス（自動検知）

AWSリソースに対するセキュリティやコンプライアンスに寄与するサービス

Amazon GuardDuty	悪意のある操作や不正なトラフィック通信を継続的にモニタリングする脅威検出サービス。機械学習を使った自動検出が可能。
Amazon Inspector	ソフトウェアの脆弱性や意図しないネットワークのエクスプローラーがないか継続的に AWS ワークロードをスキャンする自動脆弱性管理サービス
Amazon Macie	S3のデータを機械学習によって自動的に検出、分類、保護するサービス。不正アクセスやデータ漏洩などを監視する。
Amazon Detective	CloudTrailのログ、VPCフローログ、GuardDutyの結果を自動収集して、潜在的なセキュリティ案件を分析するサービス



セキュリティ・コンプライアンス（統制）

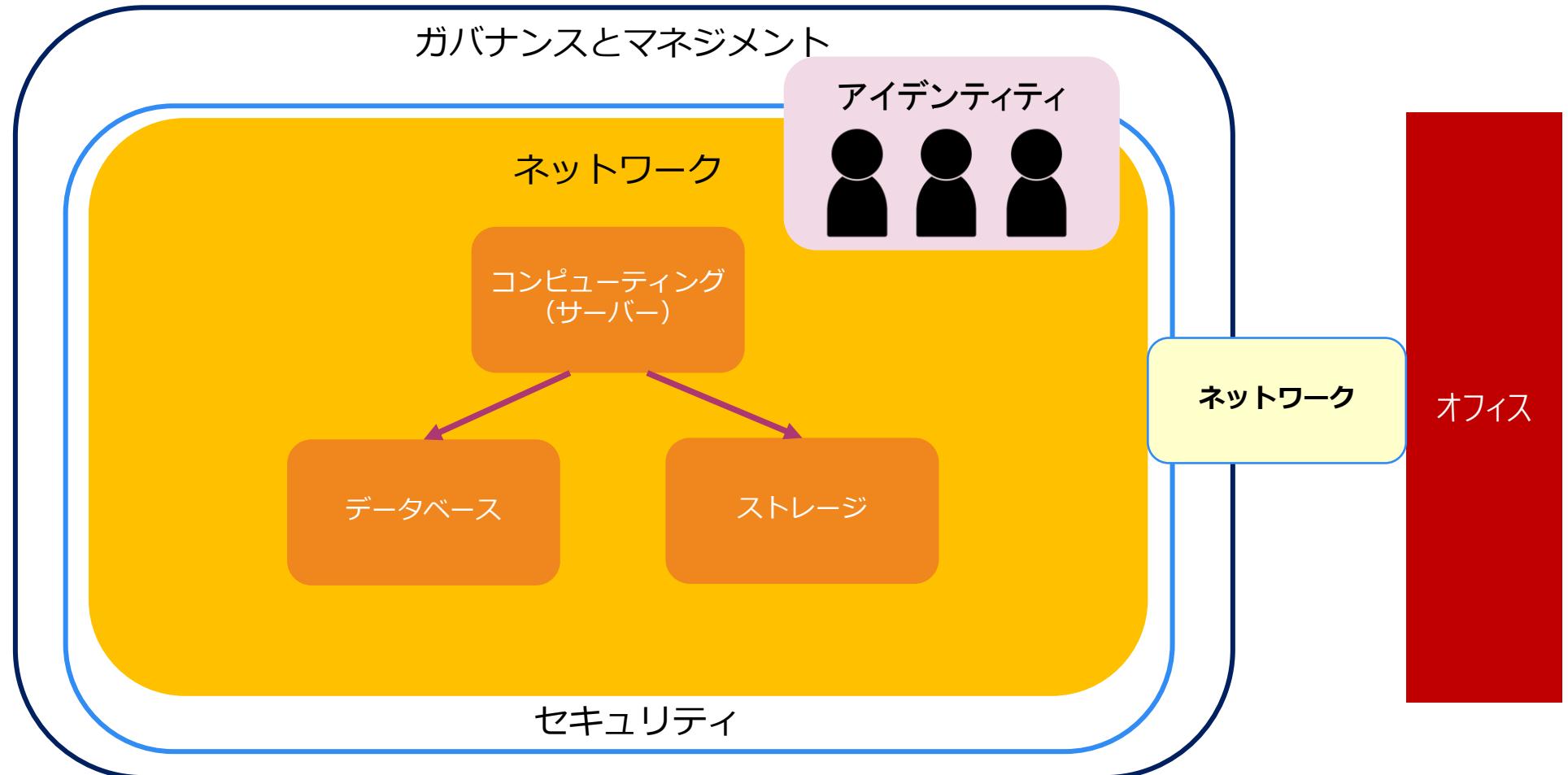
AWSリソースに対するセキュリティやコンプライアンスに寄与するサービス

AWS Control Tower	事前設定された安全なAWS環境であるランディングゾーン設定を自動化するサービス。継続的なポリシーの取得および統合ダッシュボードで、複数アカウントのセキュリティ設定を統制する
AWS Service Catalog	ポートフォリオに製品（複数リソースに基づくCloudFormationテンプレート）と制約、利用権限を登録することでユーザーが権限なしに製品を起動できるサービス
AWS License Manager	サーバーで利用されているソフトウェアのライセンスを管理するサービス。ライセンスルールを作成・適用することで、追跡、可視化、ライセンス違反の規制を可能にする。
AWS Audit Manager	フレームワークに基づきリソースの使用状況に関するエビデンスを継続的に自動収集し、評価、レポートするサービス。



マネジメントとガバナンス

運用保守やサポートに関する支援ツールやサービス



マネジメントとガバナンス（モニタリング）

運用保守やサポートに関する支援ツールやサービス

Amazon CloudWatch	ほとんどのAWSリソースに自動的に適用されるメトリクス値を取得してアラームなどを設定可能なモニタリングサービス RUMやEvidentlyでアプリケーションにも適用可能
AWS CloudTrail	ユーザー活動と API 使用状況を追跡するログを取得し、監視するサービス
AWS Systems Manager	AWSとオンプレミス環境のモニタリングデータを統合管理でき、運用タスクを自動化する運用支援サービス
AWS Config	AWSリソースの設定状況を評価して、AWSリソースの変更をモニタリングして、履歴管理する構成管理サービス
AWS Personal Health Dashboard	AWSサービスの異常・正常などのステータスをユーザーの利用状況に合わせて表示するモニタリングサービス



マネジメントとガバナンス（アプリ監視）

運用保守やサポートに関する支援ツールやサービス

AWS X-Ray	アプリケーションやその基盤となるサービスの実行状況を把握し、パフォーマンスの問題やエラーの根本原因を特定して、トラブルシューティングを行うツール
CloudWatch Real-User Monitoring(RUM)	ページの読み込み時間、クライアント側のエラー、およびユーザーの行動データなど実際のユーザーからみたWEBアプリケーションのパフォーマンスをモニタリングすることができる。
CloudWatch Application Insights	アプリケーションの異常やエラーを検出および関連付けしたり、アプリケーションで発生しているすべての問題を通知する。これらのテレメトリデータを継続的にモニタリングする。
CloudWatch ServiceLens	トレース、メトリクス、ログ、アラーム、および他のリソースヘルス情報を 1 か所に統合することで、サービスとアプリケーションの監視性を強化する。



マネジメントとガバナンス（評価）

運用保守やサポートに関する支援ツールやサービス

AWS Well-Architected Tool	AWSアーキテクチャの6つの設計原則に沿ってAWSリソースが利用されているかをチェックし、改善策を提示するツール
AWS Trusted Advisor	コストの最適化、セキュリティ、耐障害性、パフォーマンス、サービスの制限といった AWS のベストプラクティスに基づく 5 つのカテゴリにわたるチェックと推奨事項を提供します。



マネジメントとガバナンス（管理ツール）

運用保守やサポートに関する支援ツールやサービス

AWS Resource Groups	リージョン毎にリソースをグループ化して、インサイト表示やタスクを自動化するサービス
Tag Editor	様々なリソースに設定されたタグの編集を一括で実行できるサービス
AWS Resource Access Manager (RAM)	複数AWSアカウント間でAWSリソースを共有できるサービス。個別のアカウント間での共有とAWS Organizationsのアカウント間で共有することができる。



マネジメントとガバナンス（人的サポート）

運用保守やサポートに関する支援ツールやサービス

AWSサポート	AWSの人的サポートを受けることができるサービス。ベーシック、デベロッパー、ビジネス。エンタープライズ on Ramp、エンタープライズの5つのプランがある。
AWS TAM (Technical Account Manager)	AWSを導入している企業や個人に対して、効率良く運用するため技術的視点でサポートを行うAWSの専門家。 AWSサポートのエンタープライズプラン (on-Ramp含む) で利用可能
コンシェルジュサポートチーム	AWSサポートのエンタープライズプラン (on-Ramp含む) で利用可能なコンシェルジュ型サポートで、技術以外にもアカウントや請求などの全面的なサポートを実施する。



マネジメントとガバナンス（人的サポート）

運用保守やサポートに関する支援ツールやサービス

AWSパートナー ネットワーク	オファーリングの構築、マーケティング、およびお客様への販売のためのプログラムとリソースを活用するパートナーのグローバルコミュニティ。150 を超える国々から 100,000 パートナー
AWSコンサルティング パートナー	AWSパートナーネットワーク内でAWSのユーザーがAWS移行を実施する際のコンサルティングまたはマネージドサービスを提供するプロフェッショナル資格
AWSパートナーパス	AWS パートナーネットワーク (APN) 参加後に、パートナーとなった会社が登録するパス制度。ソフトウェア、ハードウェア、サービス、トレーニング、ディストリビューションの5つ
AWSプロフェッショナル サービス	AWSクラウドを使用して期待するビジネス上の成果を実現するようお客様をサポートする専門家からなるグローバルチーム。AWS専門家とパートナーネットワークによる支援チーム
AWS IQ	AWS認定サードパーティーエキスパートの利用を支援するサービス。最適なエキスパートを発見して、作業依頼や共同作業、統合された請求などを利用できる
AWS Managed Services	変更管理や障害管理など、ITILに準拠した既存のIT運用プロセスをAWS側が運用を自動化して対応してくれる。



マネジメントとガバナンス（ナレッジサポート）

運用保守やサポートに関する支援ツールやサービス

AWS re:Post	専門分野に基づいてコミュニティエキスパートと質問を共有して、理解を促進するコミュニティサービス
AWSナレッジセンター	AWSユーザーから頻繁に寄せられる質問と要望をまとめた参考サイト
AWSフォーラム	AWSのディスカッションフォーラムでフォーラムに質問とフィードバックを投稿できる。re:Postに移行された。
AWSホワイトペーパー	AWS と AWS コミュニティによって作成された、テクニカルホワイトペーパー、技術ガイド、参考資料
AWSドキュメント	ユーザーガイド、開発者ガイド、APIリファレンス、チュートリアルなどを検索できるドキュメントサイト



マネジメントとガバナンス（その他のサポート）

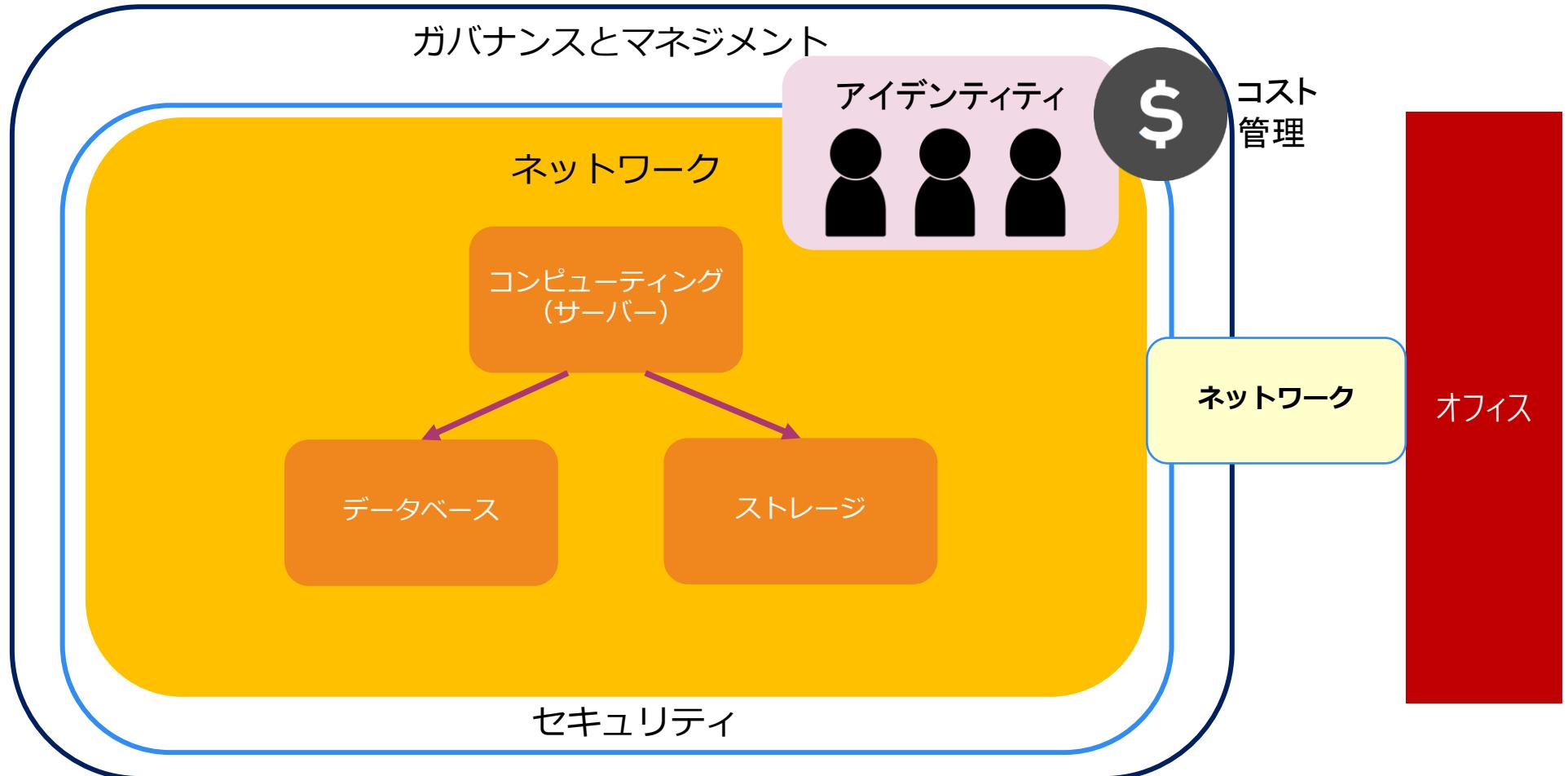
運用保守やサポートに関する支援ツールやサービス

AWS クイックスタート	ソリューションアーキテクトと AWS パートナーによって構築された自動参照デプロイメント。AWS のベストプラクティスに沿って、人気の高い技術を AWS にデプロイできる
Service Quotas	クォータをダッシュボードで一元的に確認し、上限緩和申請も可能となる AWS サービス制限の管理サービス
AWS Artifact	AWS のコンプライアンスレポートの提供やユーザーとの契約管理を実施するサービス
Amazon Mechanical Turk	Web または API から人的なタスクの依頼ができるクラウドソーシングサービス



AWSコスト管理

AWSを利用する際のコスト最適化を支援するツールやサービス



AWSコスト管理

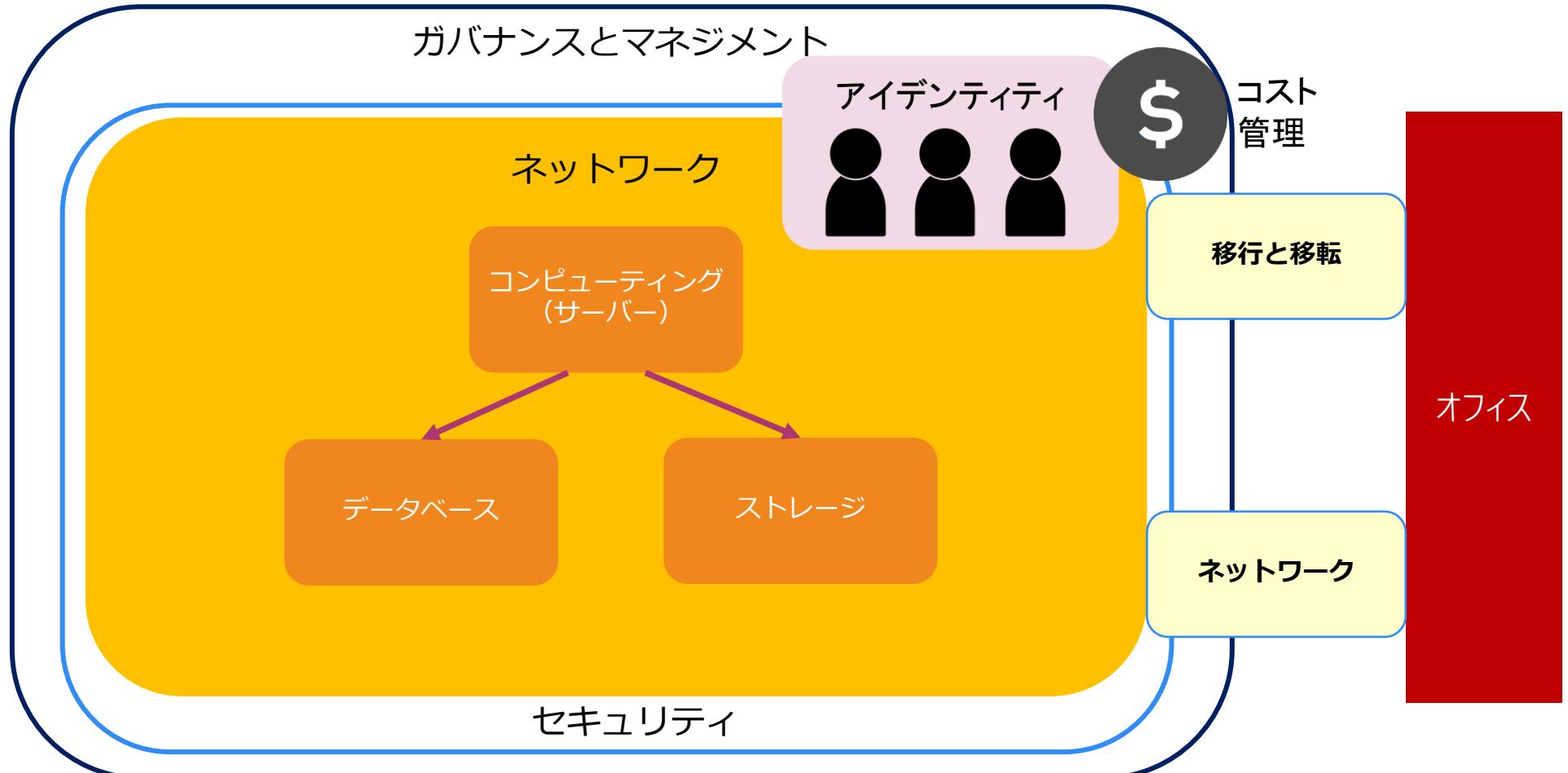
AWSを利用する際のコスト最適化を支援するツールやサービス

AWS Pricing Calculator	AWS のコスト計算を支援するツール
AWS Cost Explorer	AWSのコストと使用量や経済効率性を把握するために、AWSコスト分析を実施する可視化ツール
AWSのコストと 使用状況レポート	AWSのコストと使用状況の詳細を確認するためのレポート コストカテゴリーとコスト配分タグで項目を追加できる。
AWS Budgets	各AWSサービスに応じた予算のしきい値を超えたときにアラートを設定することができる予算監視ツール
AWS Compute Optimizer	使用率データに基づいて、EC2インスタンスタイプ、EBSボリュームおよびLambda 関数の最適な設定を選択できる。最大 25 %コスト削減を実施
AWS Cost Anomaly Detection	機械学習により異常な支出と根本原因を特定して、想定外のコストが発生する回数を減らし、コントロールを強化する。



移行と移転

AWSクラウドへのインフラ移行やデータ移行を支援するサービス



移行と移転

AWSクラウドへのインフラ移行やデータ移行を支援するサービス

AWS Application Discovery Service	オンプレミス環境のサーバーの設定データや使用状況データなどを収集して、サーバーの依存関係マッピングなどの移行に必要な情報を抽出することで移行計画の準備を支援するサービス
AWS Schema Conversion Tool	ソースデータベーススキーマやデータベースコードオブジェクトの大部分を自動的にターゲットデータベース互換フォーマットへと変換するツール
AWS Database Migration Service	データベースを短期間に安全にAWS に移行する際に利用するサービス。AWSのデータベース間の移行にも利用される。
AWS Server Migration Service	数千のオンプレミスワークロードを実行する仮想サーバー構成をAWSに移行可能な移行支援ツール
VM Import/Export	仮想マシンイメージを既存の環境から Amazon EC2 インスタンスにインポートすることや、元のオンプレミス環境にエクスポートを実行
CloudEndure	移行元サーバーに導入したエージェントを介してディスクイメージを転送し EC2に変換して移行するサービス。BCP向けにイメージ転送を継続する機能などが提供されている。



移行と移転

AWSクラウドへのインフラ移行やデータ移行を支援するサービス

AWS Migration Hub	各移行ツールの実行状況を追跡できるダッシュボードサービス
AWS Snow Family	オンプレミスに運んで直接移行データを取得して、AWSに運ぶことができるデータ移行デバイス。Snowball、Snowball edge、Snowmobileがある。
AWS DataSync	オンプレミスのストレージと、S3またはEFSとの間のデータ転送を自動化するサービス。オンプレミス環境側にDataSync Agentをデプロイしてデータを転送する。
AWS Transfer Family	SFTP、FTPおよびFTPSに対応したデータ転送サービス。S3を利用してアップロードファイルのアーカイブや処理に使用できる。
AWS Outposts	AWS インフラストラクチャとサービスを事实上すべてのオンプレミスまたはエッジロケーションに提供し、真に一貫したハイブリッドエクスペリエンスを実現



移行と移転 (Snow Family)

AWSクラウドへのインフラ移行やデータ移行を支援するサービス

AWS Snowball	Snowballは旧型アプライアンスで、現在はSnowball Edgeアプライアンスを提供
Snowball Edge Storage Optimized	ブロック/オブジェクトストレージと40個のvCPUを提供し、ローカルストレージや大規模データ転送を実施するデバイス。EC2とLambda関数に対応。容量は80TB
Snowball Edge Compute Optimized	高度な機械学習およびフルモーションビデオ分析などのユースケースのために、52個のvCPU、ブロックストレージとオブジェクトストレージ、オプションのGPUを提供。容量は40TB
AWS Snowmobile	エクサバイト規模のデータ転送サービス。セミトレーラートラックが牽引する長さ14mの丈夫な輸送コンテナで、Snowmobile 1台あたり100PBまで転送できる。
AWS Snowcone	エッジコンピューティング、ストレージ、データ転送用デバイス。重量2.1kgで8TBストレージと14TBのSSDを使用可能。緊急対応要員のバックパックの中、IoT、車載、ドローンなどに活用
AWS OpsHub	Snowballデバイス用のGUIツール。Snowballデバイスのセットアップと管理を容易にし、エッジコンピューティングワークフローを迅速にデプロイし、クラウドへのデータ移行を簡素化する。



移行と移転（災害対応）

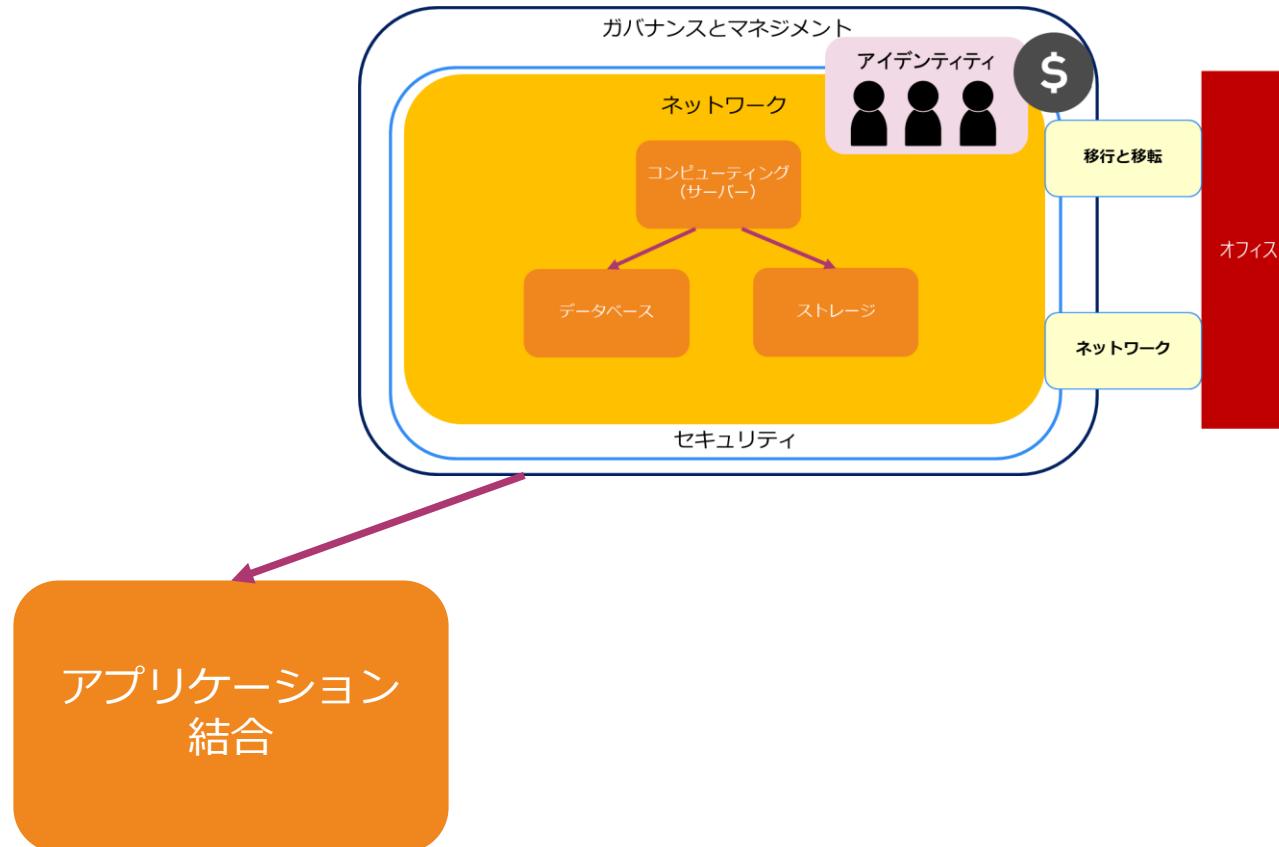
AWSクラウドへのインフラ移行やデータ移行を支援するサービス

CloudEndure Disaster Recovery	CloudEndureを利用したイメージ転送により既存の物理または仮想データセンター、プライベートクラウドなどからAWSに迅速かつ簡単に移行することが可能
AWS Elastic Disaster Recovery (AWS DRS)	手頃な料金のストレージ、最小限のコンピューティング、ポイントインタイムリカバリを使用して、アプリケーションを復旧してダウントIMEやデータ損失を最小限に抑えるサービス。



アプリケーション統合

アプリケーションやコンポーネント間の連携や通知に利用する
サービス



アプリケーション統合

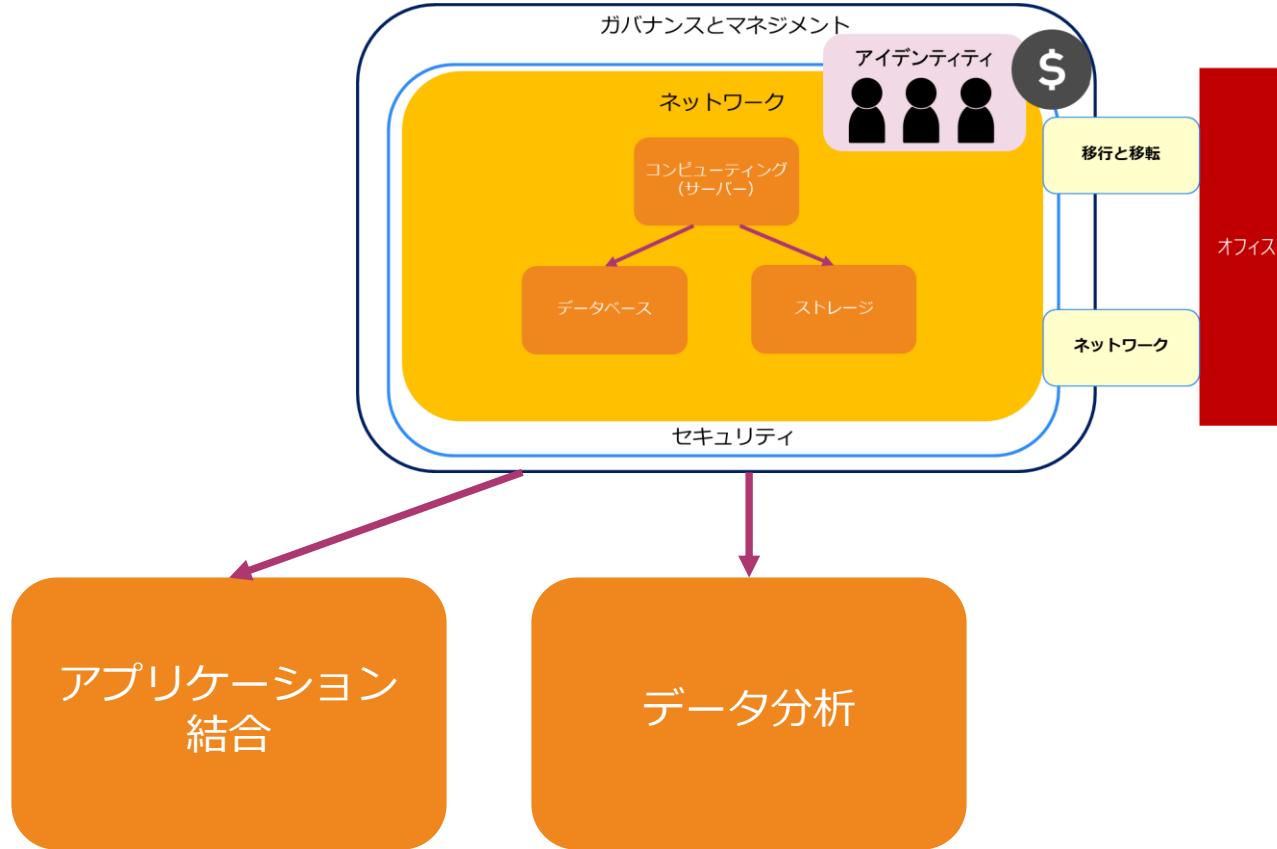
アプリケーションやコンポーネント間の連携や通知に利用するサービス

Amazon SNS	Pub/Sub型のメッセージングサービス。コンポーネント間のプッシュ型のメッセージ通知やアラート通知に利用する。
Amazon SQS	ポーリング型のメッセージキューイングサービス。プロセス処理の分散並列処理を可能にする。
Amazon SES	Eメールの送受信機能を提供するサービス。アプリケーション上のEメール通知機能を実装できる。
Amazon MQ	AWS でメッセージブローカーの設定や運用を簡単に行えるようしてくれる、Apache ActiveMQ および RabbitMQ 向けのマネージド型メッセージブローカーサービス
Amazon API Gateway	リアルタイム双方向通信アプリケーションを実現する RESTful API および WebSocket API を作成・管理するサービス



データ活用

データ処理やデータ解析に利用されるサービス



データ活用

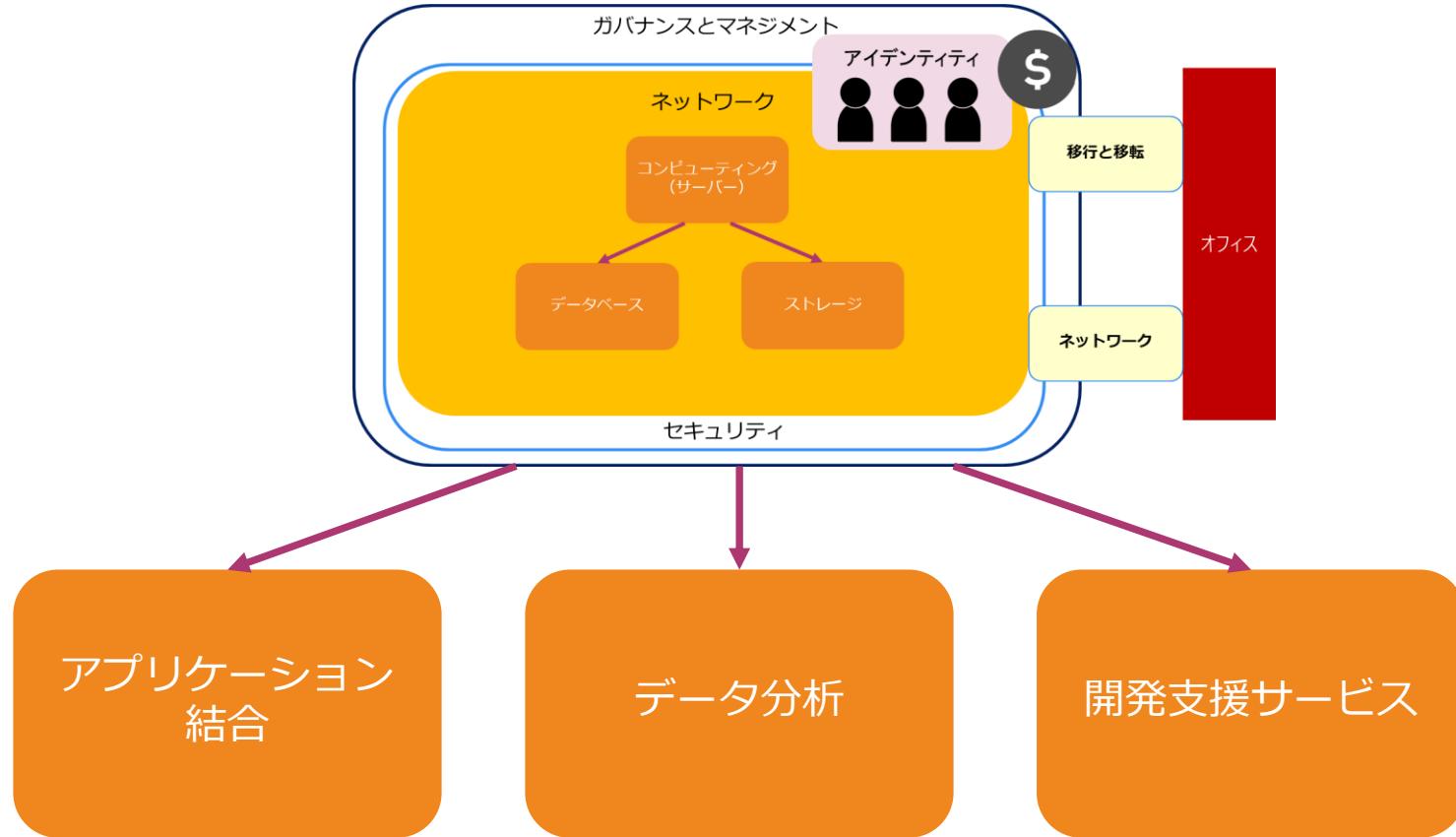
データ処理やデータ解析に利用されるサービス

Amazon Kinesis	ストリーミングデータをリアルタイムで収集、処理、分析するストリーミングデータ処理サービス。Data StreamsとVideo StreamsとData FirehoseとData Analyticsがある。
Amazon Athena	SQL型のデータ分析サービス。Amazon S3 内のデータを標準 SQL を使用して簡単に分析することができる。
Amazon EMR	Apache Sparkなどの分散データ処理ツールを使用して高速でペタバイト規模のビッグデータ処理を実行するサービス
AWS Glue	分析、機械学習、アプリケーション開発のためのデータの検出、準備、結合を簡単に行えるELTサービス。 AWS Glue DataBrew はノーコードでデータを視覚的にクリーンアップ・正規化する
Amazon QuickSight	簡単に分析環境を作ることができるBIサービス。データ分析時の可視化工ディタを提供
AWS Lake Formation	キュレートされた安全な一元的リポジトリである安全なデータレイクを数日で簡単にセットアップできるサービス
AWS Data Exchange	ユーザーが第三者へのデータ閲覧機能を提供できるサービス。クラウド内のサードパーティのデータを簡単に検索、サブスクリプション、および利用できるようになる。



開発支援サービス

AWS上でのアプリケーション開発を支援するサービス



開発支援サービス（環境自動化）

AWS上でのアプリケーション開発を支援するサービス

AWS CloudFormation	インフラ構成をテンプレート化して、AWSリソースのプロビジョニングを自動化するInfrastructure as Codeサービス
AWS Elastic BeanStalk	Java、.NET、PHP、Node.js、Python、Ruby、Go および Dockerを使用したWEBアプリケーションをAWSリソース環境にデプロイし、バージョン管理を自動化するサービス
AWS OpsWorks	Chef や Puppet のマネージド型インスタンスを利用できるようになる構成管理サービスです。Chef や Puppet は、コードを使用してサーバーの構成を自動化する。
AWS Serverless Application Model (AWS SAM)	AWS でサーバーレスアプリケーションを構築するために使用できるオープンソースのフレームワーク
AWS Launch Wizard	AWSのベストプラクティスに従ったSQL Server、SAP、Active Directoryを利用したアプリケーションを簡単にデプロイできるサービス
AWS Cloud Development Kit (AWS CDK)	TypeScriptやPythonなどの言語でAWSリソースの定義およびプロビジョニングするサービス。リソース定義はCloudFormation テンプレートに変換される。



開発支援サービス（環境自動化・コード作成）

AWS上でのアプリケーション開発を支援するサービス

AWS Cloud9	AWS上でコードを記述・管理するためのコーディングツール。GithubやCodeCommitと連携してコード管理を実施する。
AWS CodeBuild	ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを作成できる完全マネージド型のビルドサービス
AWS CodeCommit	プライベート Gitリポジトリをホストする安全で高度にスケーラブルなマネージド型のコードなどのソース管理サービス
AWS CodeDeploy	Amazon EC2、AWS Fargate、AWS Lambda、オンプレミスで実行されるサーバーなど、さまざまなコンピューティングサービスへのソフトウェアのデプロイを自動化
AWS CodePipeline	完全マネージド型の継続的デリバリーサービスで、素早く確実性のあるアプリケーションとインフラストラクチャのアップデートのため、パイプラインのリリースを自動化する。
AWS CodeStar	ソフトウェア開発プロジェクトを作成、管理、および操作するクラウドベースのサービス。AWS上でアプリケーションをすばやく開発、構築、およびデプロイする



開発支援サービス (Docker環境自動化)

AWS上でのアプリケーション開発を支援するサービス

Amazon ECS	Dockerコンテナーに基づいた開発環境の提供とアプリケーション開発・展開を支援するコンテナオーケストレーションサービス
Amazon EKS	AWS で Kubernetesを利用したDockerを簡単に実行できるようにするマネージド型サービス
Amazon ECR	Amazon Elastic Container Registry (ECR) は、フルマネージド Docker コンテナレジストリ。コンテナソフトウェアをどこにでも簡単に保存、共有、デプロイできる
AWS Fargate	ECSとEKS用のコンテナ向けサーバーレスコンピューティング
ECS / EKS Anywhere	オンプレミス環境でECSとEKSを実行する



開発支援サービス（プロセス作成）

AWS上でのアプリケーション開発を支援するサービス

AWS Step Functions	Lambda関数などの複数のAWSサービスをワークフロー上に連携させて実行プロセスを作成することができるワークフロー作成・管理サービス。サーバレスで実行できる。
Amazon Simple Workflow Service (Amazon SWF)	分散コンポーネント全体にわたって作業を調整するアプリケーションを構築する。ワーカーはEC2やオンプレミスで実行可能。Step Functionsと違いサーバーが必要で古いタイプのサービス
AWS Batch	フルマネージドサービス型でスケールのバッチコンピューティングワークロードを実行するサービス。コンピューティングリソースを自動的にプロビジョニングし、ワークロードを生成する。
Amazon EventBridge	AWSサービスやアプリケーションと連携して、イベント駆動型アーキテクチャを構築するサーバレスイベントバスサービス



開発支援サービス（開発支援）

AWS上でのアプリケーション開発を支援するサービス

AWS Software Developer Kit (AWS SDK)	プログラミング言語を使用してクラウドアプリケーションリソースを定義するためのオープンソースのソフトウェア開発フレームワーク。AWSリソースを開発に組み込むことができる。
AWS Mobile Hub	モバイルアプリ向けにCognito、Lambda、Device Farm、PinpointなどのAWSサービスと連携してアプリケーションの構築、テスト、モニタリングを実施する
AWS CodeArtifact	フルマネージド型のアーティファクトリポジトリサービスであり、あらゆる規模の組織がソフトウェア開発プロセスで使用されるソフトウェアパッケージを安全に保存、公開、および共有する
Amazon Location Service	地図、POI（Points Of Interest）、ジオコーディング、ルーティング、ジオフェンス、トラッキング機能を提供するデバイスの位置情報サービス
AWS Amplify	AWS Amplifyはクラウド向けWEB/モバイル開発向けのJavaScript/iOS/Androidライブラリ。AmplifyコンソールはWebアプリケーションのCI/CDおよびホスティングを実施
Amazon Honeycode	コード記述なしにモバイルおよびWebアプリケーションを構築できるサービス



開発支援サービス（品質・セキュリティ）

AWS上でのアプリケーション開発を支援するサービス

AWS暗号化SDK	クライアントサイド暗号化を実行する暗号化ライブラリ。この暗号化ライブラリを使用してクライアント暗号化の仕組みを実装
AWS Device Farm	様々なブラウザとモバイルデバイスのテストにより、ウェブアプリとモバイルアプリの品質を向上させるアプリケーションテストサービス
AWS Fault Injection Simulator	アプリケーションのフォールトインジェクション実験を実施し、パフォーマンス、オブザーバビリティ、および回復性を簡単に改善できるサービス
Amazon CodeGuru	機械学習を使用して、セキュリティの脆弱性を検出し、コードレビューを自動化するサービス
AWS Signer	LambdaとIoT coreに対応した署名プロファイルを作成し、信頼できる発行元のグループを表せるフルマネージドなコード署名サービス



開発支援サービス（データ連携）

AWS上でのアプリケーション開発を支援するサービス

Amazon AppFlow

コード記述なしに実行可能なS3およびRedshiftなどのAWSサービス間のデータ連携サービス

AWS AppSync

GraphQLを活用したオンライン・オフラインのリアルタイムデータ同期サービス（DynamoDB、Lambda、Elasticsearch Service、Aurora Serverless、HTTPエンドポイント対応）



開発支援サービス（ユーザー対応）

コンタクトセンター やイベント処理むけのサービス

Amazon Connect

顧客窓口を構築できるクラウド型コンタクトセンターサービス。
自動音声の作成、着電管理、ケース追跡などが可能

Amazon Pinpoint

ユーザー行動データを分析して、最適なタイミングでのメッセージ配信するユーザーエンゲージメントを改善するサービス



その他の最新テクノロジー

AI、量子コンピューター、VR/AR、ロボット、ブロックチェーンなどの最新技術を利用するサービスが提供されている。

IoT

AWS IoT Core
AWS IoT Analytics
AWS IoT Greengrass
AWS IoT Events

AI

Amazon SageMaker
Amazon Polly
Amazon Lex
Amazon rekognition

ロボット

AWS RoboMaker

人工衛星

AWS Ground Station

ブロック チェーン

Amazon Managed Blockchain
Amazon QLDB

量子コンピュータ

Amazon Braket

ゲームテック

Amazon GameLift
Amazon Lumberyard

メディア サービス

Elastic Transcoder
Elemental MediaConnect
Interactive Video Service
Elemental MediaLive

VR/AR

Amazon Sumerian

仕事環境

Amazon WorkSpaces
Amazon WorkLink
Amazon WorkDocs



仕事環境

仮想デスクトップなどの仕事環境を支援するサービス

Amazon WorkSpaces	様々なデバイスからリソースにアクセスできる Windows および Linux 向けのフルマネージドデスクトップ仮想化サービス
Amazon WorkLink	従業員がスマホから社内ウェブサイトやウェブアプリケーションに安全かつ簡単にアクセスできるようにするサービス
Amazon WorkDocs	AWS 内にコンテンツを一元管理して、コンテンツの作成、編集、共有を実現するサービス。他のユーザーとのコラボレーションが容易になる。
Amazon WAM	WorkSpacesへのアプリケーションの配布と管理を行うサービス。インストールやアップデートを制御でき、セキュリティやコンプライアンスを維持する。
Amazon WorkMail	企業向け E メールおよびカレンダーアプリケーションを提供。クライアントアプリケーションによりE メール、連絡先、およびカレンダーにシームレスにアクセスできる
Amazon Chime	ビデオ通話、テキストチャット、スクリーン共有などのオンライン会議環境を提供するサービス
Amazon AppStream 2.0	リモートから業務に必要なデスクトップやアプリケーションへのアクセスを安全に実施するサービス



IoT

IoT環境やアプリケーションを構築するためのサービス

AWS IoT Core	IoTデバイスが簡単かつ安全にクラウドやその他のデバイスと相互接続できるクラウドプラットフォーム。HTTP、MQTT、WebSocketプロトコルを使用しメッセージの送受信する
Amazon FreeRTOS	IoT向けのマイクロコントローラ向けリアルタイムOS
AWS IoT Analytics	IoT Coreなどからデータストアにメッセージを取り込み、SQLを使用して分析できるIoT分析サービス
AWS Greengrass	IoTデバイスにLambda関数を実行できるサービス
AWS IoT Device Management	IoTデバイスを数百万まで管理するサービス。オンボードのデバイス設定、インベントリの整理、監視、リモート管理が可能
AWS IoT Events	IoTセンサー上のイベントを検出できるサービス
AWS IoT Device Defender	デバイス設定の監査や異常動作を検出するフルマネージドなIoTセキュリティサービス



自然言語AI

自然言語系のAIを利用したサービス

Amazon Comprehend	自然言語処理を実施するAIサービス。テキストから場所や人物、キーフレーズ、感情を検出することができる。
Amazon Lex	音声やテキスト型のチャットボットを作成する対話型インターフェースの構築サービス
AWS Chatbot	チャットチャネルでの AWS ワークロードのモニタリング、運用、トラブルシューティングを簡単に行えるようにするインタラクティブなエージェント。Slack連携が可能
Amazon Kendra	自然言語の非構造化データを機械学習により検索するサービス
Amazon Translate	テキストベースのコンテンツを多言語へ翻訳するニューラル機械翻訳サービス。リアルタイム翻訳処理も可能

音声AI

音声系のAIを利用したサービス

Amazon Polly	テキストを自然な音声に変換するText to Speechのサービス。
Alexa for Business	組織でAlexaを使用するためのスキルやツールを提供するサービス。Alexaをオフィスの共有エリアにいるすべての人に共有して、会議室を管理するなども可能
Amazon Transcribe	音声をテキストに変換する文字起こしサービス
AWS DeepComposer	生成AIによるモデルを利用して音楽を作成しながら機械学習を学べるサービス



予測AI

予測系のAIを利用したサービス

Amazon Forecast	数値データを利用した時系列予測サービス。S3データから製品需要計画、財務計画などに対する予測モデルを作成する。
Amazon Personalize	ECサイトなどのパーソナライズおよびレコメンデーション生成できるサービス。AutoML機能によって適切なアルゴリズムの選択して、パーソナライズされた予測の生成が行える。
Amazon Fraud Detector	潜在的に不正なオンラインアクティビティを検出する不正検出モデルを作成できるフルマネージド型サービス



画像解析AI

画像解析系のAIを利用したサービス

Amazon Rekognition

画像と動画の解析を実行するサービス。画像と動画内の物体、シーン、テキスト、不適切なコンテンツの識別ができる。

Amazon Textract

電子ドキュメントからテキストデータを抽出するサービス。マルチカラムなどのレイアウト、テーブルやフォームの関連などを識別可能



AI開発系

ユーザーが機械学習モデルを生成するための支援サービス

Amazon Machine Learning	機械学習のモデルを構築し、予測を生成するサービス。モデルのデータソースとして、S3に保存されたデータセット、Redshift またはRDSのMySQLが使用できる。
Amazon SageMaker	データのクレンジングや前処理やモデル作成に利用可能なブラウザベースのIDEやJupiterノートブック環境などの機械学習モデルの開発構築が提供される。SageMaker Canvasはノーコード
Amazon Augmented AI	機械学習アプリケーションに対する人によるレビューが必要なワークフローを構築および管理するサービス



最新技術の活用

最新技術を活用するためのサービス

Amazon Sumerian	VR/ARおよび3Dアプリケーションの作成・ビルド・起動を提供するサービス。 PollyやLexと連携することで、3Dキャラクタを喋らせることも可能
AWS RoboMaker	ロボットデベロッパーがインフラストラクチャを管理することなく、シミュレーションの実行、スケール、自動化を可能にするクラウドベースのシミュレーションサービス
AWS Ground Station	衛星通信のコントロール、衛星データの処理、衛星運営のスケーリングを可能にする完全マネージド型サービス
Amazon Managed Blockchain	Hyperledger Fabric や Ethereum を使用して、パブリックネットワークへの参加や、スケーラブルなプライベートネットワークの作成と管理を
Amazon Braket	量子コンピューティングのための科学的研究とソフトウェア開発の高速化をサポートするために設計された、フルマネージド量子コンピューティングサービス



まとめ

- AWSは200以上のサービスが提供されており、IT関連で必要な機能はほぼ網羅されている。
- その中でもITインフラやアプリケーション開発に必要な主要サービスを理解することが重要となる。
- AI、ブロックチェーン、量子コンピューターなどの最新技術もクラウド経由で利用することができる。

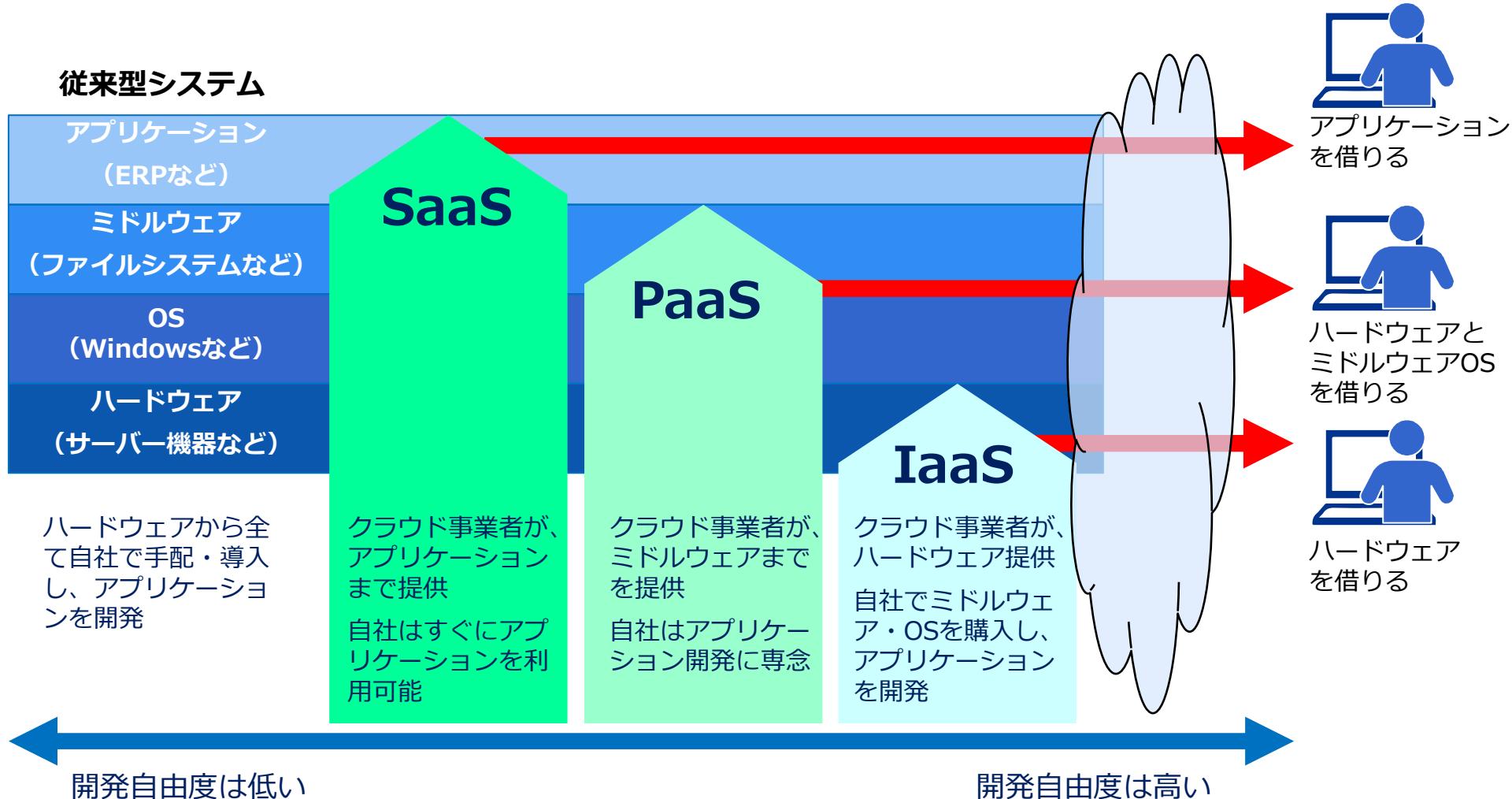


AWSの活用メリット



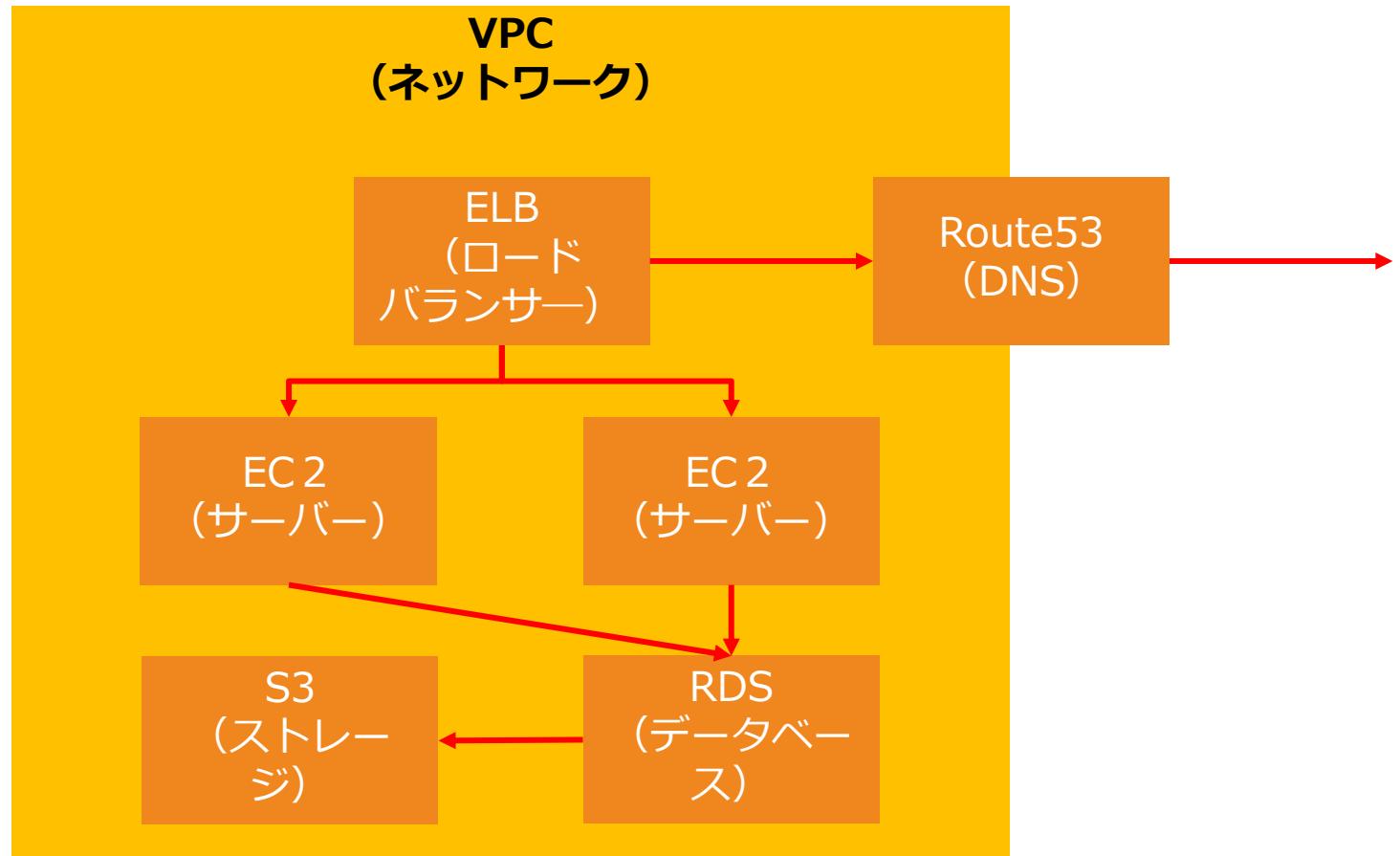
クラウドの3つのサービス形態

主にSaaS、PaaS、IaaSの3つのサービスが存在



IaaSとしてのAWS

AWSの基本サービスはIaaSであり、様々なインフラをインターネットを介してオンデマンドで利用可能なことが利点



AWS活用例

オイシックスは全てのインフラをAWSに移行し、自前の開発・運用体制を整備

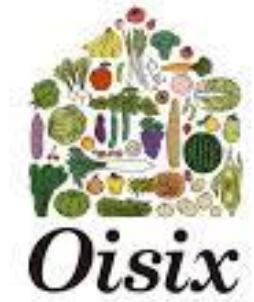
オンプレミス中心のインフラ体制



Oisix



全てのインフラ・アプリをAWSへ

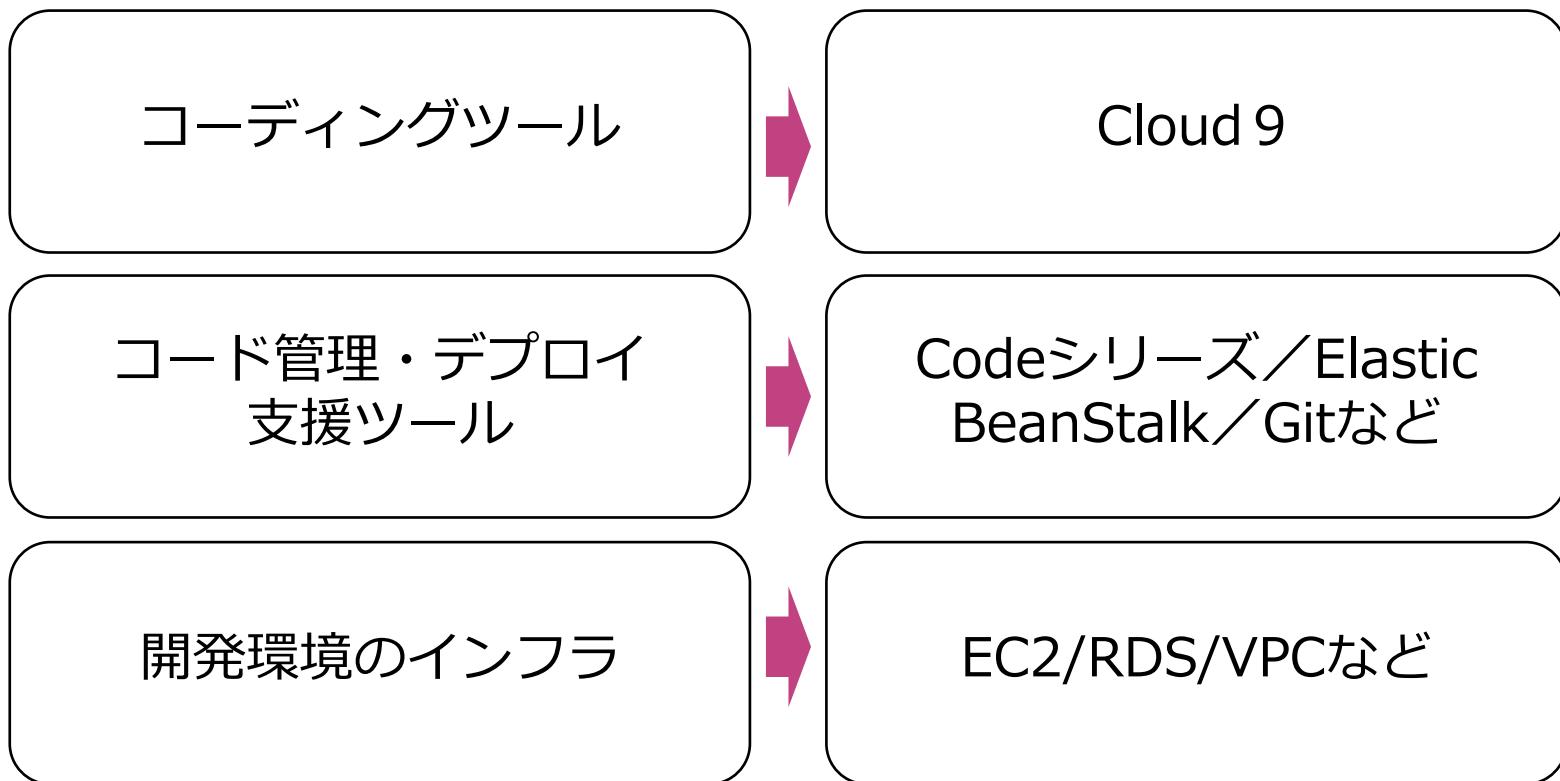


Oisix



PaaSとしてのAWS

AWSのIaaSに加え、アプリケーション開発ツール（PaaS）を利用して、アプリケーションを構築する



AWS活用例

新規アプリケーションをAWSインフラや豊富な開発機能や利用して素早く開発する



SaaSとしてのAWS

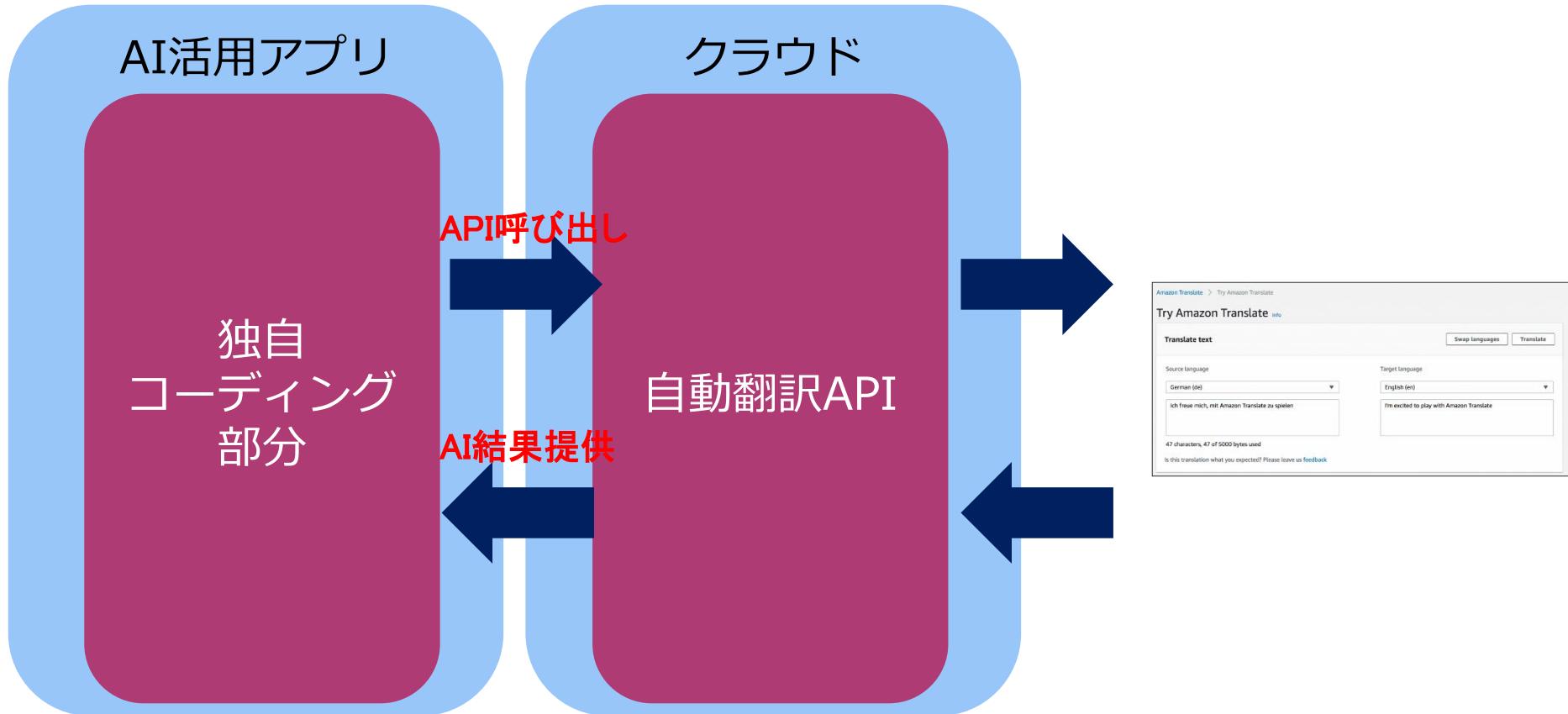
AI翻訳機能や文章解析AIなどのAWSによって既に完成されたサービスを利用するクラウド形態

The screenshot shows the 'Try Amazon Translate' interface. At the top, it says 'Amazon Translate > Try Amazon Translate'. Below that is the title 'Try Amazon Translate' with an 'Info' link. On the left, there's a 'Translate text' section. At the top right of this section are 'Swap languages' and 'Translate' buttons. Below this are two dropdown menus: 'Source language' set to 'German (de)' and 'Target language' set to 'English (en)'. Underneath each dropdown is a text input box. The German input box contains the text 'Ich freue mich, mit Amazon Translate zu spielen' and the English input box contains 'I'm excited to play with Amazon Translate'. Below the German input box, it says '47 characters, 47 of 5000 bytes used'. At the bottom, there's a feedback link: 'Is this translation what you expected? Please leave us [feedback](#)'.



AWS活用例

既にサービスとして出来上がったクラウドサービスをAPIから利用して組み込むことで、最先端の機能を利用できる



オンプレミスと
AWSクラウドの良し悪し



クラウドのメリット／デメリット

迅速に柔軟にリソースを活用できるクラウドのメリットに対して、ベンダーロックインという最大のデメリットがある。

クラウドのメリット

- オンデマンドでリソースを柔軟に迅速に活用することができる。

クラウドのデメリット

- クラウド業者のサービスに依存してしまうベンダーロックイン



ベンダーロックイン

オンプレミスのサーバーでシステム構築を自社内でしていれば、
サーバー変更やソフトウェア変更は“比較的”容易に可能

現行サーバー



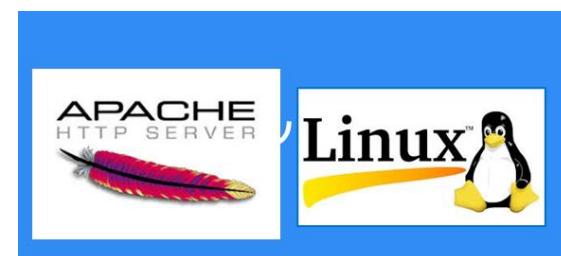
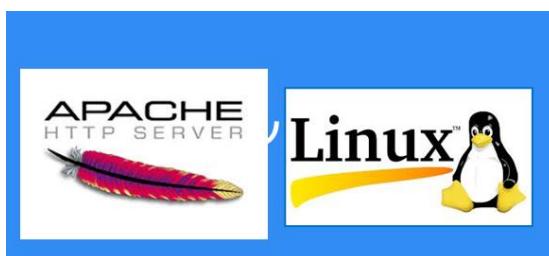
新しいサーバー
機器に移行



新サーバー



ソフトウェアを
入れ替える。



ベンダーロックイン

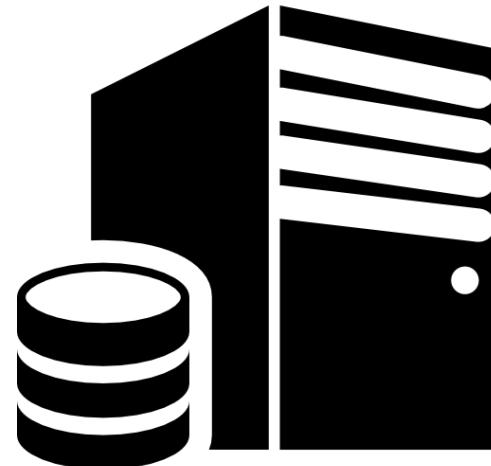
EC2インスタンスなどオンプレミスサーバーと類似の製品は移行が容易である



新しいサーバー
機器に移行



別サーバー



ソフトウェアを
入れ替える。



ベンダーロックイン

AWS独自のサーバレスの仕組みをアプリに組み込んで機能開発してしまうと、環境移行が困難になる。

AWS独自の仕組み

AWS Lambda

Amazon SQS

AWS API Gateway

他環境に移行



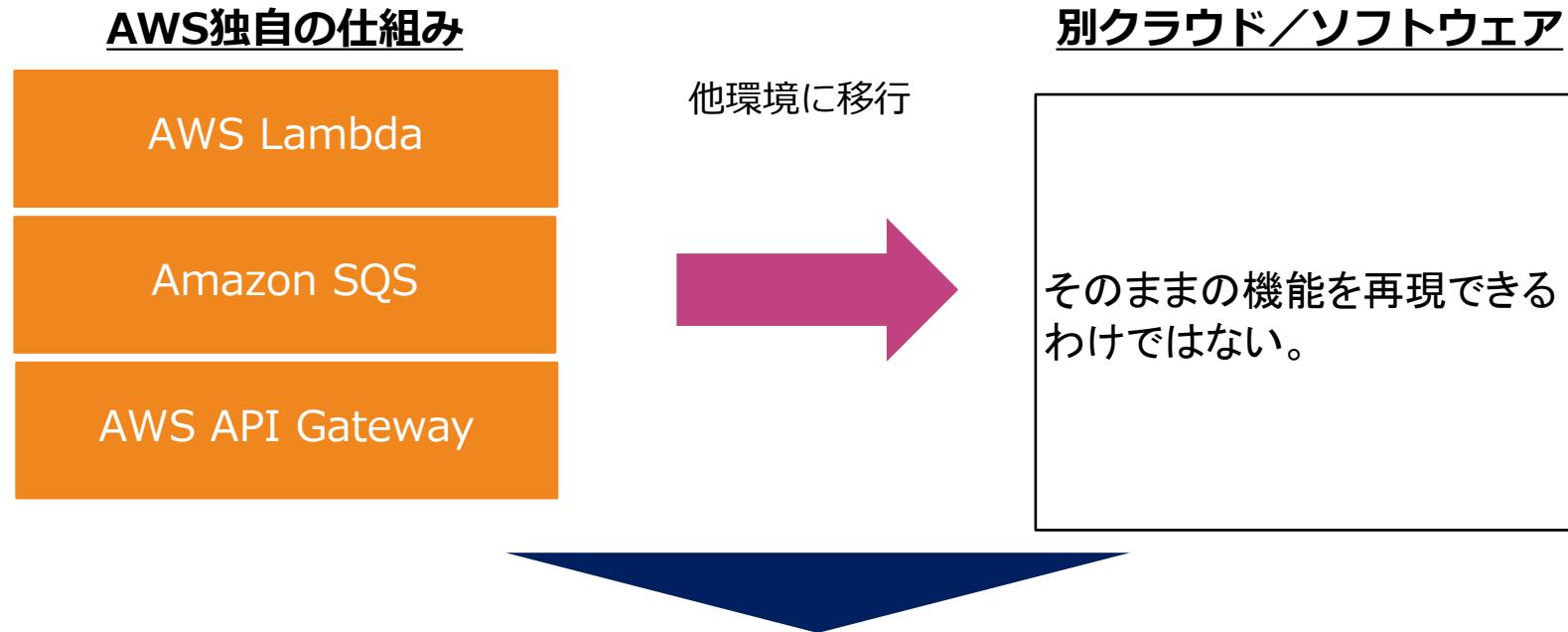
別クラウド／ソフトウェア

そのままの機能を再現できる
わけではない。



ベンダーロックイン

AWS独自のサーバレスの仕組みをアプリに組み込んで機能開発してしまうと、環境移行が困難になる。



どっぷりAWSに依存して環境設定や開発を進めてしまうと
AWS外への移行がどんどん困難になる



クラウドのメリット／デメリット

迅速に柔軟にリソースを活用できるクラウドのメリットに対して、ベンダーロックインという最大のデメリットがある。

クラウドのメリット

- オンデマンドでリソースを柔軟に迅速に活用することができる。

クラウドのデメリット

- クラウド業者のサービスに依存してしまうベンダーロックイン
- データ保存先や活用で社内での保管が義務付けられている等、クラウド環境が利用できない。



クラウドのメリット／デメリット

迅速に柔軟にリソースを活用できるクラウドのメリットに対して、ベンダーロックインという最大のデメリットがある。

クラウドのメリット

- オンデマンドでリソースを柔軟に迅速に活用することができる。
- オンプレミス環境とのハイブリッドやオンプレミス環境にAWSクラウドサービスを展開することも可能

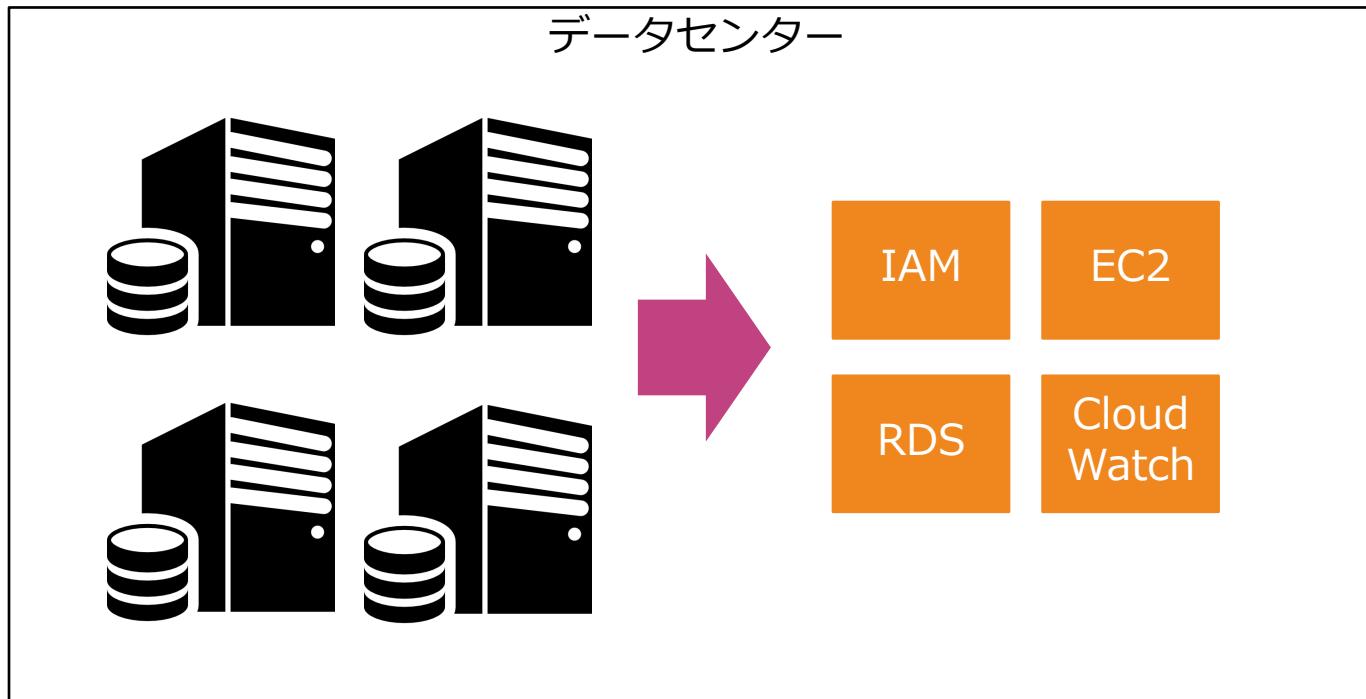
クラウドのデメリット

- クラウド業者のサービスに依存してしまうベンダーロックイン
- データ保存先や活用で社内での保管が義務付けられている等、クラウド環境が利用できない。



オンプレミス環境のAWS

AWS Outpostsはオンプレミス環境にAWSサービスをセットアップして独自に利用できるように構築できる



クラウドのメリット／デメリット

迅速に柔軟にリソースを活用できるクラウドのメリットに対して、ベンダーロックインという最大のデメリットがある。

クラウドのメリット

- オンデマンドでリソースを柔軟に迅速に活用することができる。
- オンプレミス環境とのハイブリッドやオンプレミス環境にAWSクラウドサービスを展開することも可能
- 下手に自社DC内でインフラを構成するよりも、AWSに依存した方がよっぽどセキュリティは高い

クラウドのデメリット

- クラウド業者のサービスに依存してしまうベンダーロックイン
- データ保存先や活用で社内での保管が義務付けられている等、クラウド環境が利用できない→回避策がある



クラウドのメリット／デメリット

迅速に柔軟にリソースを活用できるクラウドのメリットに対して、ベンダーロックインという最大のデメリットがある。

クラウドのメリット

- オンデマンドでリソースを柔軟に迅速に活用することができる。
- オンプレミス環境とのハイブリッドやオンプレミス環境にAWSクラウドサービスを展開することも可能
- 下手に自社DC内でインフラを構成するよりも、AWSに依存した方がよっぽどセキュリティは高い

クラウドのデメリット

- クラウド業者のサービスに依存してしまうベンダーロックイン
- データ保存先や活用で社内での保管が義務付けられている等、クラウド環境が利用できない→回避策がある



AWSの操作方法



AWSの操作

AWSの操作方法は3つ：

AWS
マネジメント
コンソール

インスタンス操作
(SSH等)

AWS
CLI操作

AWSマネジメントコンソール

AWSマネジメントコンソールはWEB画面からAWSを設定できるGUIツール

The screenshot shows the AWS Management Console with the EC2 dashboard selected. The main area displays the 'Step 1: Amazon Machine Image (AMI)' configuration page. The navigation bar at the top includes links for Services, Resource Groups, and Support, along with account information for EdutechPartners.

The left sidebar contains a navigation menu with the following categories and items:

- EC2 ダッシュボード**
 - イベント
 - タグ
 - レポート
 - 制限
- インスタンス**
 - インスタンス
 - Launch Templates
 - スポットリクエスト
 - リザードインスタンス
 - 専有ホスト
 - Capacity Reservations
- イメージ**
 - AMI
 - バンドルタスク
- ELASTIC BLOCK STORE**
 - ボリューム
 - スナップショット
 - Lifecycle Manager
- ネットワーク & セキュリティ**
 - セキュリティグループ
 - Elastic IP
 - 個のブレイスマントグループ
 - キーベア
 - ネットワークインターフェイス
- ロードバランシング**
 - ロードバランサー
 - ターゲットグループ
- AUTO SCALING**
 - 起動設定

The main content area shows the 'Step 1: Amazon Machine Image (AMI)' configuration. It includes a search bar and a table listing several AMI options:

AMI	Description	Architecture	Action
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-02e680c4540db351e (64ビットx86) / ami-0998858ab6ad47da8 (64ビットArm)	Amazon Linux 2には5年間のサポートが含まれます。Amazon EC2、systemd 219、GCC 7.3、Glibc 2.26、Binutils 2.29.1で最適なパフォーマンスを発揮できるように調整されたLinuxカーネル4.14、および、追加の最新のソフトウェアパッケージを提供します。	64ビット(x86) 64ビット(Arm)	選択
Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0cd3dfa4e37921605	Amazon Linux AMIは、AWSがサポートするEBS-backedイメージです。デフォルトのイメージには、AWSコマンドラインツール、Python、Ruby、Perl、およびJavaが含まれます。レポジトリには、Docker、PHP、MySQL、PostgreSQL、およびその他のパッケージが含まれます。	64ビット(x86)	選択
SUSE Linux Enterprise Server 15 (HVM), SSD Volume Type - ami-0eb9f58db22854f8f	SUSE Linux Enterprise Server 15 (HVM)、EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	64ビット(x86)	選択
Red Hat Enterprise Linux 7.6 (HVM), SSD Volume Type - ami-0b500ef59d8335eee (64ビットx86) / ami-0302c1ecc74930ba5 (64ビットArm)	Red Hat Enterprise Linux version 7.6 (HVM)、EBS General Purpose (SSD) Volume Type	64ビット(x86) 64ビット(Arm)	選択
Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0f65671a86f061fcf (64ビットx86) / ami-0f2057f28f0a44d06 (64ビットArm)	Ubuntu Server 18.04 LTS (HVM)、EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).	64ビット(x86) 64ビット(Arm)	選択
Amazon RDS	データベースインスタンスを起動中ですか。Amazon RDSをお試しください。	非表示	RDSを使いデータベースを起動

インスタンス接続

設置したインスタンス（サーバー）の操作はWindowsサーバーやLinuxサーバーなどの標準に準じたソフトウェアを利用

Windowsサーバー向け操作GUI



Linuxサーバー操作用SSHソフト

```
Connection to 52.17.142.65 closed by remote host.
Connection to 52.17.142.65 closed.
Ryans-iMac:Downloads ryanckroonenburg$ clear
Ryans-iMac:Downloads ryanckroonenburg$ ssh ec2-user@52.48.51.207 -i MyEC2Key.pem
The authenticity of host '52.48.51.207 (52.48.51.207)' can't be established.
ECDSA key fingerprint is SHA256:iDXGMyu3WriedahgRytDpNDSXptqbM9aPfyLFhul2Wo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.48.51.207' (ECDSA) to the list of known hosts.

--| --|- )
_-| ( / Amazon Linux AMI
---\---|_|
https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
20 package(s) needed for security, out of 39 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-36-83 ~]$
```

SSHソフトウェア

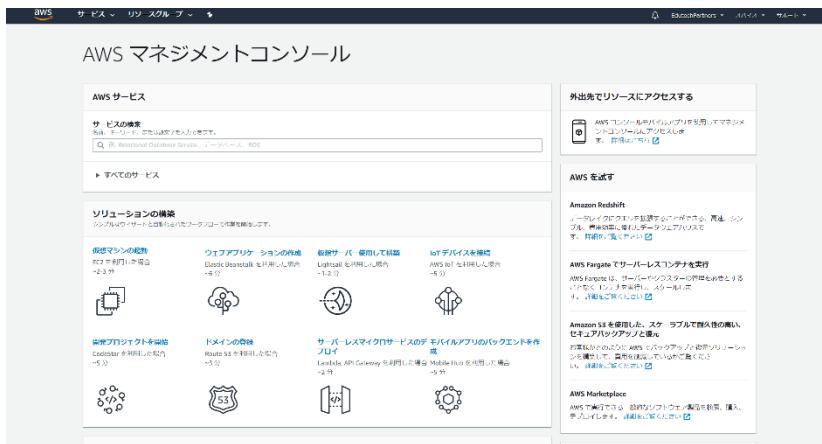
設置したサーバーなどにアクセスして内部設定やソフトウェア操作を実行する通信方式及びそのソフトウェア

```
Connection to 52.17.142.65 closed by remote host.  
Connection to 52.17.142.65 closed.  
Ryans-iMac:Downloads ryankroonenburg$ clear  
  
Ryans-iMac:Downloads ryankroonenburg$ ssh ec2-user@52.48.51.207 -i MyEC2Key.pem  
The authenticity of host '52.48.51.207 (52.48.51.207)' can't be established.  
ECDSA key fingerprint is SHA256:iDXGMyu3Wr1edahgRytDpNDSXptqbM9aPfyLFhuL2Wo.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '52.48.51.207' (ECDSA) to the list of known hosts.  
  
_ _ | _ _ | _ )  
_ | ( _ / Amazon Linux AMI  
_ _ \| _ _ | _ _ |  
  
https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/  
20 package(s) needed for security, out of 39 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-36-83 ~]$
```

基本操作

AWSの設定・操作はまずはマネジメントコンソールでインスタンスなどを設置し、SSHで接続して操作するのが基本

【AWSマネジメントコンソール】 AWS上にインスタンスなどを設置

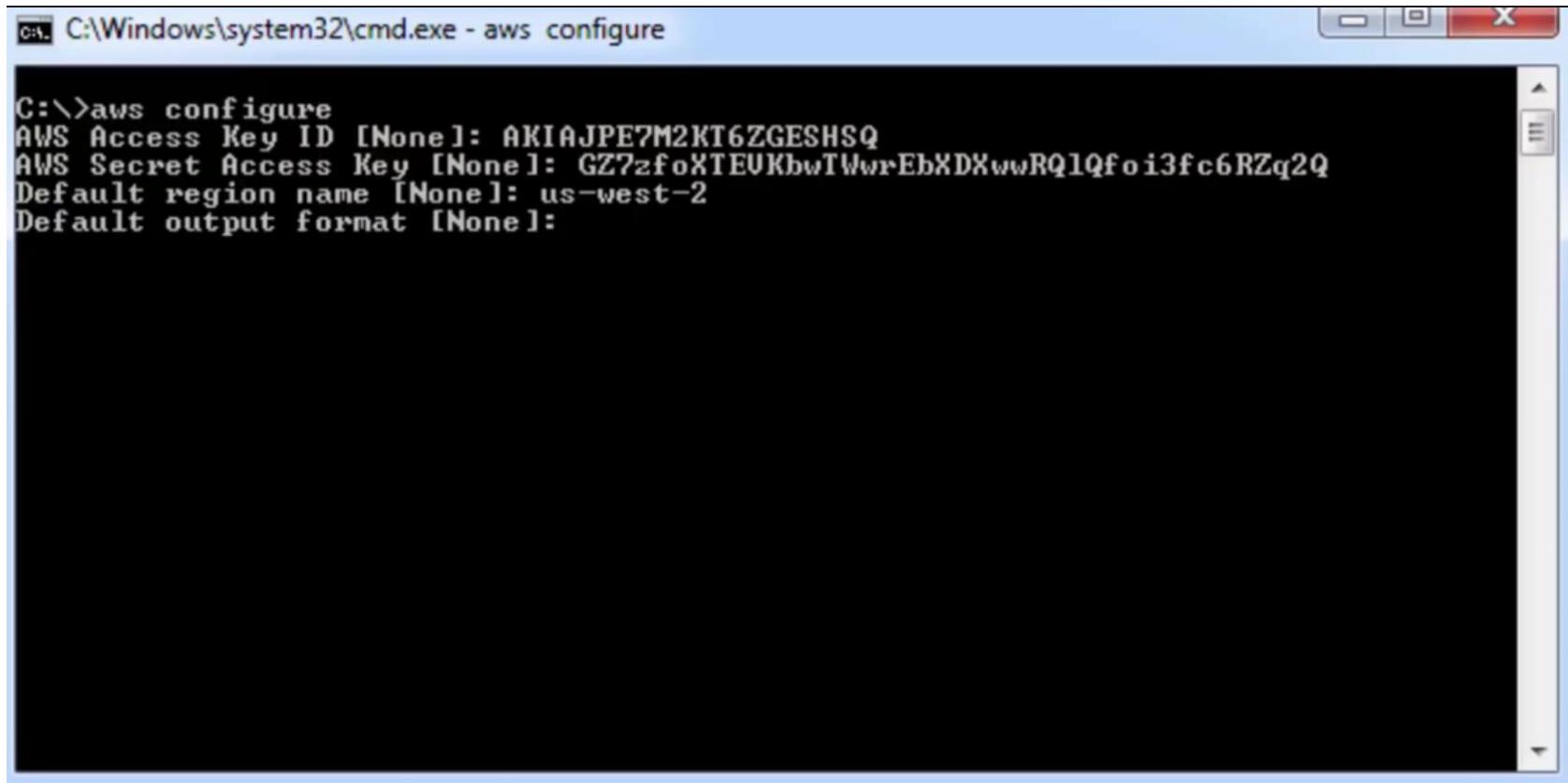


【インスタンス操作】 設置したインスタンス に接続して操作する

```
Connection to 52.17.142.65 closed by remote host.  
Connection to 52.17.142.65 closed.  
Ryans-iMac:Downloads ryankroonenburg$ clear  
  
Ryans-iMac:Downloads ryankroonenburg$ ssh ec2-user@52.48.51.207 -i MyEC2Key.pem  
The authenticity of host '52.48.51.207 (52.48.51.207)' can't be established.  
ECDSA key fingerprint is SHA256:idXGMyu3W1edahgRtDpNDSxtqM9aPfyLHuL2No.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '52.48.51.207' (ECDSA) to the list of known hosts.  
  
--| _ |-- )  
_ | ( _ / Amazon Linux AMI  
_ | \_ | _ |  
  
https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/  
20 package(s) needed for security, out of 39 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-36-83 ~]$
```

AWS CLI

AWS CLIはコマンドラインから複数のAWSサービスを制御・管理することが可能



The screenshot shows a Windows Command Prompt window titled "C:\Windows\system32\cmd.exe - aws configure". The command "aws configure" has been entered at the prompt. The output displays the configuration parameters being set:

```
C:\>aws configure
AWS Access Key ID [None]: AKIAJPE7M2KT6ZGESHSQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]:
```

【凡例】

ハンズオン

基本の座学

セクションの内容

レクチャー

レクチャーで学ぶ内容

サーバーの理解

WEBサービスを提供するサーバーと関連ソフトウェアについて基本知識を獲得します。

EC2の概要

AWSでサーバーを作成するEC2の機能や特徴を学習します。

AWSでサーバーを構築してみる①(ハンズオン)

AWSでサーバーの機能を提供するEC2インスタンスを立上げて、サーバー内にアクセスします。

AWSでサーバーを構築してみる②(ハンズオン)

EC2インスタンスにApacheのソフトウェアをインストールして、WEBサーバーとして設定します。

サーバーの役割の再確認

AWSで実行した内容に基づいて、サーバーの役割と動きを再度確認します。

セクションの内容

レクチャー	レクチャーで学ぶ内容
EBSの概要	EC2にアタッチして利用するストレージであるEBSの特徴を学習します。
EBSの設定 (ハンズオン)	改めてEC2設定画面におけるEBSを確認し、スナップショットを作成するなど操作を学習します。
サブネットの理解	サブネットマスクやサブネットといったネットワーク構成の概念を理解します。
VPCの概要	クラウド内にネットワークとサブネットを構成するVPCの特徴を理解します。
VPCによる ネットワーク構築 (ハンズオン)	VPCを利用してサブネットを作成し、サブネットマスクとサブネットの関係を確認します。

セクションの内容

レクチャー	レクチャーで学ぶ内容
通信プロトコルとOSI参照モデル	通信プロトコルの種類と、OSI参照モデルにおけるレイヤー間の役割を確認します。
セキュリティグループとネットワークACL	トラフィック制御に利用されるセキュリティグループとネットワークACLを理解します。
セキュリティグループの活用(ハンズオン)	EC2インスタンスのセキュリティグループによりプロトコルとポート番号を指定した通信制御設定を実施します。
ネットワークACLの活用(ハンズオン)	ネットワークACLを利用してVPCとサブネットに対するトラフィック制御を実施します。
Route53の概要	DNSサーバーの役割とAWSでDNSサーバーを提供するRoute53を学習します。

セクションの内容

レクチャー

Route53による
ドメイン登録

レクチャーで学ぶ内容

Route53にドメインを登録し、IPアドレスにドメインを設定します。

サーバーの理解

サーバーとは

サービスを提供するソフトウェアとその機能が稼働しているコンピュータのこと



サーバーソフトウェア

サーバーソフトウェア

サーバーソフトウェアがサーバーの役割と機能を提供する



サーバーのハードウェア

サーバーのハードウェアはデータセンターなどに設置された巨大なコンピューターなどが代表格



サーバーのハードウェア

PCやスマホでもサーバーソフトウェアをインストールしてサーバーとして機能させることができる



サーバーの役割

リクエストとレスポンスの処理を実行してくれるのがサーバーであり、サーバーがアプリケーションサービスを実行する



メルカリサーバー



基本は24時間稼働させることが必要！

サーバーの役割

その役割に応じて様々なサーバーが存在する。

- ✓ WEBサーバー
- ✓ アプリケーションサーバー
- ✓ バッヂサーバー
- ✓ データベースサーバー
- ✓ APIサーバー
- ✓ DNSサーバー
- ✓ メールサーバー

WEBサーバー

HTTPに対応しWEBページを表示させたりするサーバーのこと

- ✓ WEBサイトを作成・管理するソフトウェアによって起動するサーバー
- ✓ WEBページを作成して、HTML上に表示する。
- ✓ クライアントからのリクエストに対してWEBページや画像をレスポンスとして返す

データベースサーバー

リクエストに対して必要なデータを登録・更新・取得・削除などのデータ管理を実行するサーバーのこと

- ✓ データベース処理を管理するソフトウェアによって実行されるサーバー
- ✓ データの登録・更新・取得・削除などの処理を実行する
- ✓ データベースのバックアップなどの管理処理も実施

アプリケーション開発におけるDB

アプリケーション上のデータベースエンジンが導入されたデータベースサーバーの基本構成

WEBアプリケーション

アプリケーション開発におけるDB

アプリケーション上のデータベースエンジンが導入されたデータベースサーバーの基本構成



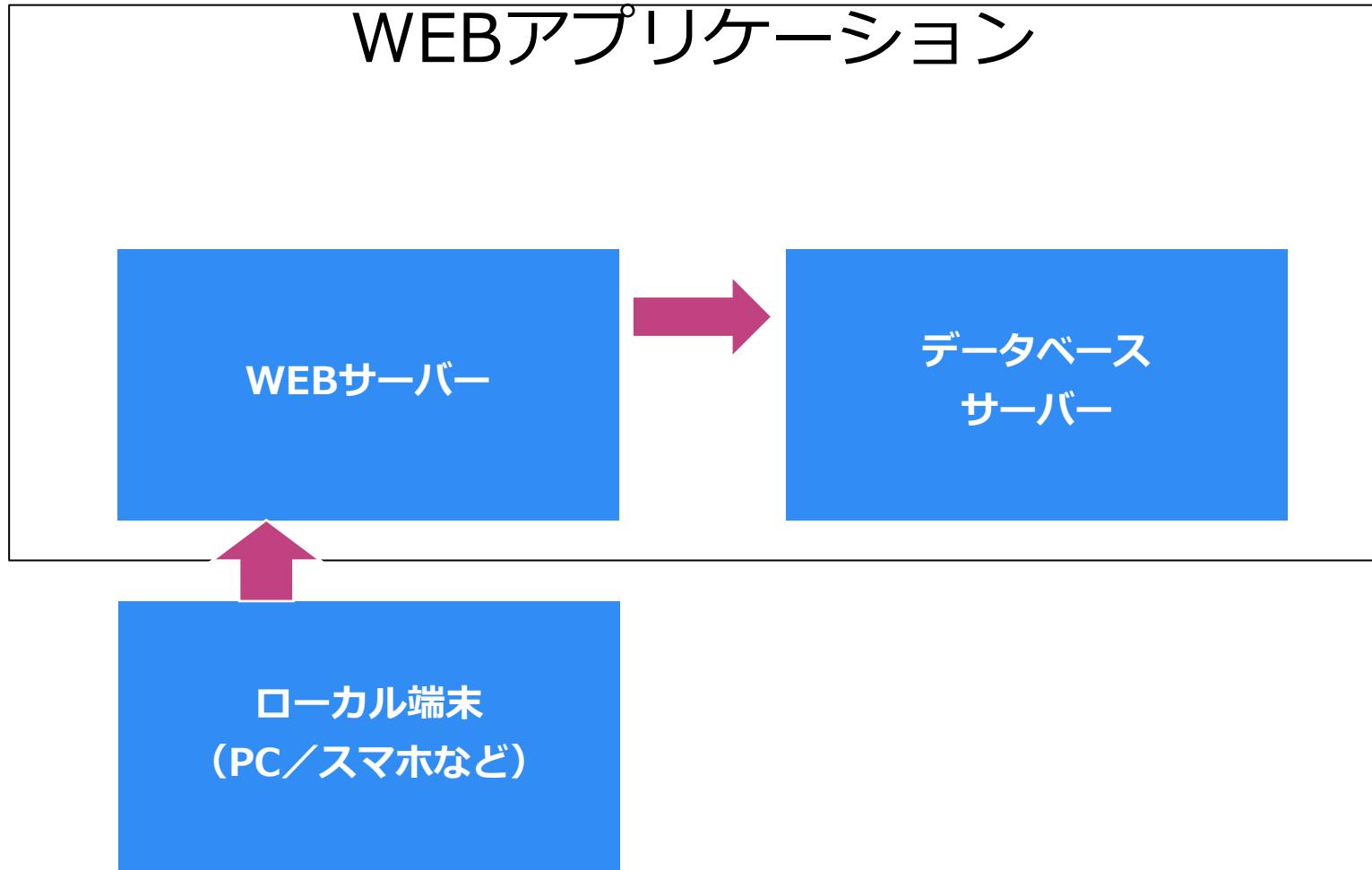
アプリケーション開発におけるDB

ローカル端末からWEBページやアプリケーションに対してDBを利用するリクエストを実行する。



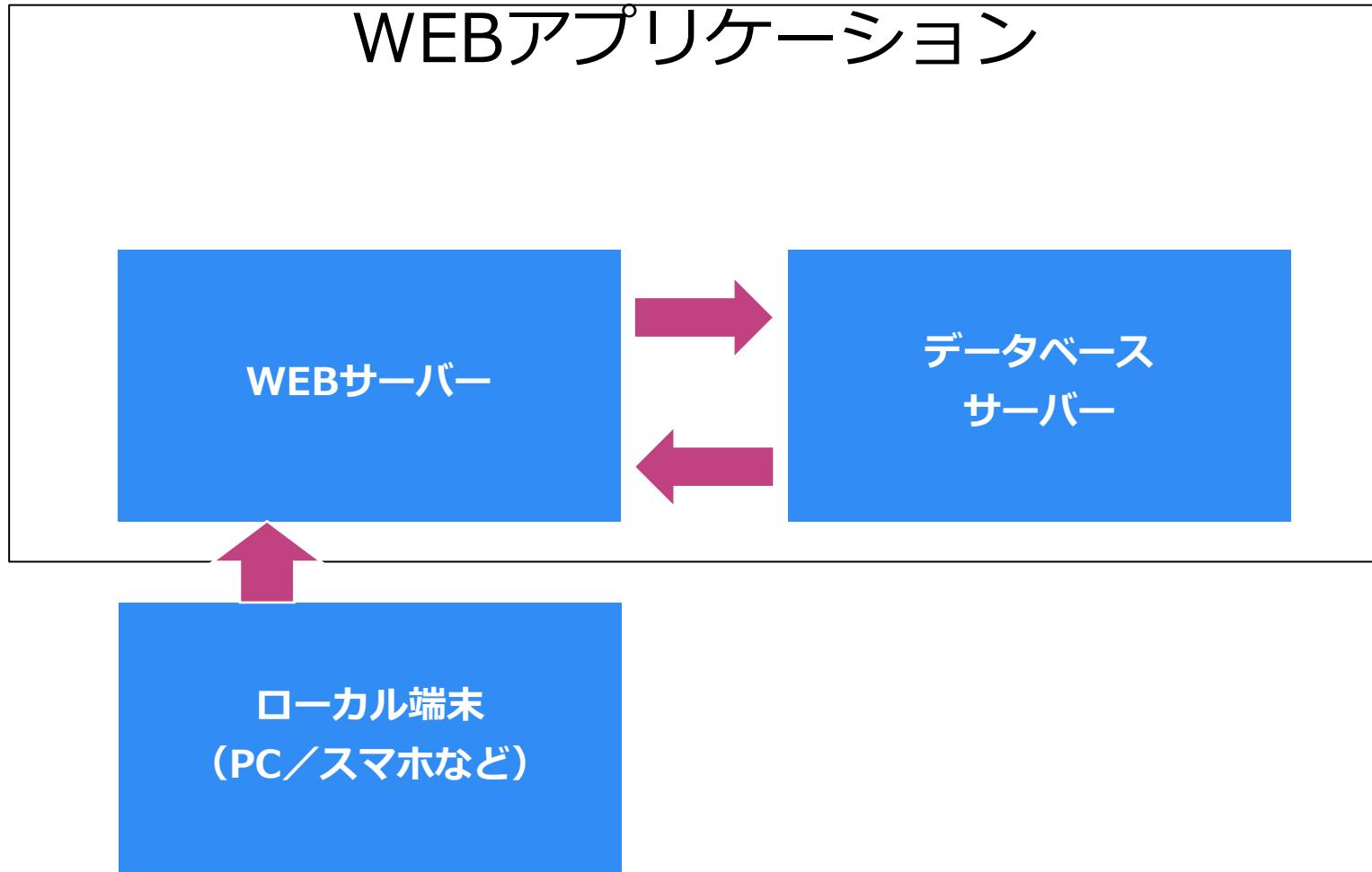
アプリケーション開発におけるDB

アプリケーションサーバー（またはWEBサーバー）からデータベースサーバーにDB処理がリクエストされる。



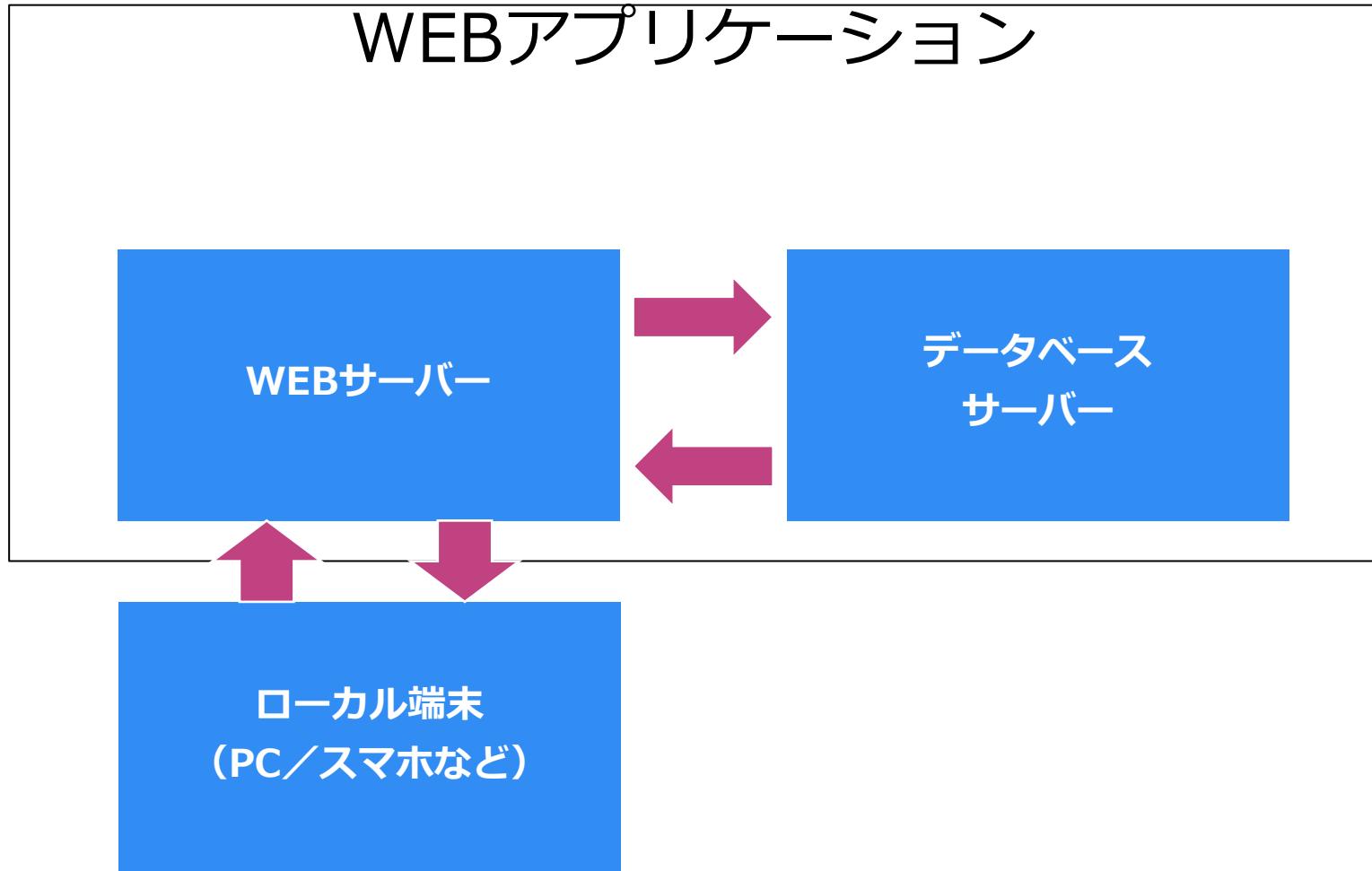
アプリケーション開発におけるDB

データベースサーバーがリクエストに応じたDBエンジンによるトランザクション処理を実行して、実行結果を返答する。



アプリケーション開発におけるDB

データベースサーバーの実行結果を含めた、アプリケーションの処理結果をローカル端末に返答する



EC2の概要

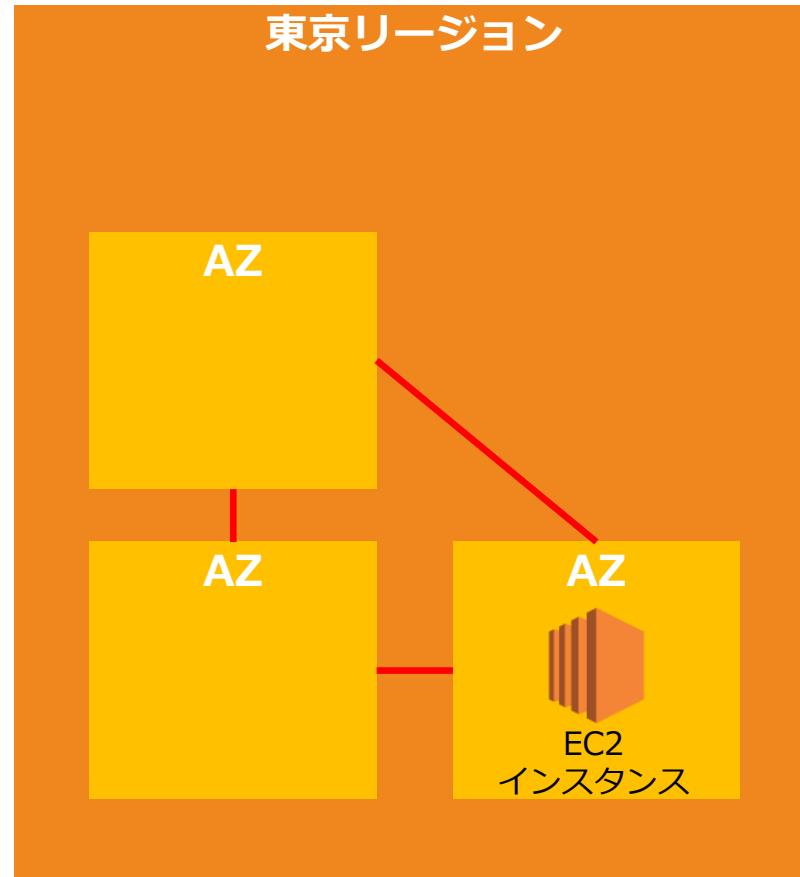
EC2とは

数分で利用可能となる従量課金（時間～秒単位）で利用可能な
仮想サーバー

- 起動・ノード追加・削除・マシンスペック変更が数分で可能
- 汎用的なIntelアーキテクチャを採用
- 管理者権限で利用可能
- WindowsやLinuxなどのほとんどのOSをサポート
- OSまでは提供されているタイプを選択することで自動設定され、OSより上のレイヤーを自由に利用可能
- 独自のAmazon Machine ImageにOS設定を作成し、保存して再利用が可能

EC2とは

利用する単位をインスタンスと呼び、任意のAZにインスタンスを立ち上げてサーバーとして利用する



EC2とは

EC2のセッティングは以下のように実施

利用するAMIイメージ（OSセッティング）を選択

インスタンスタイプを選択

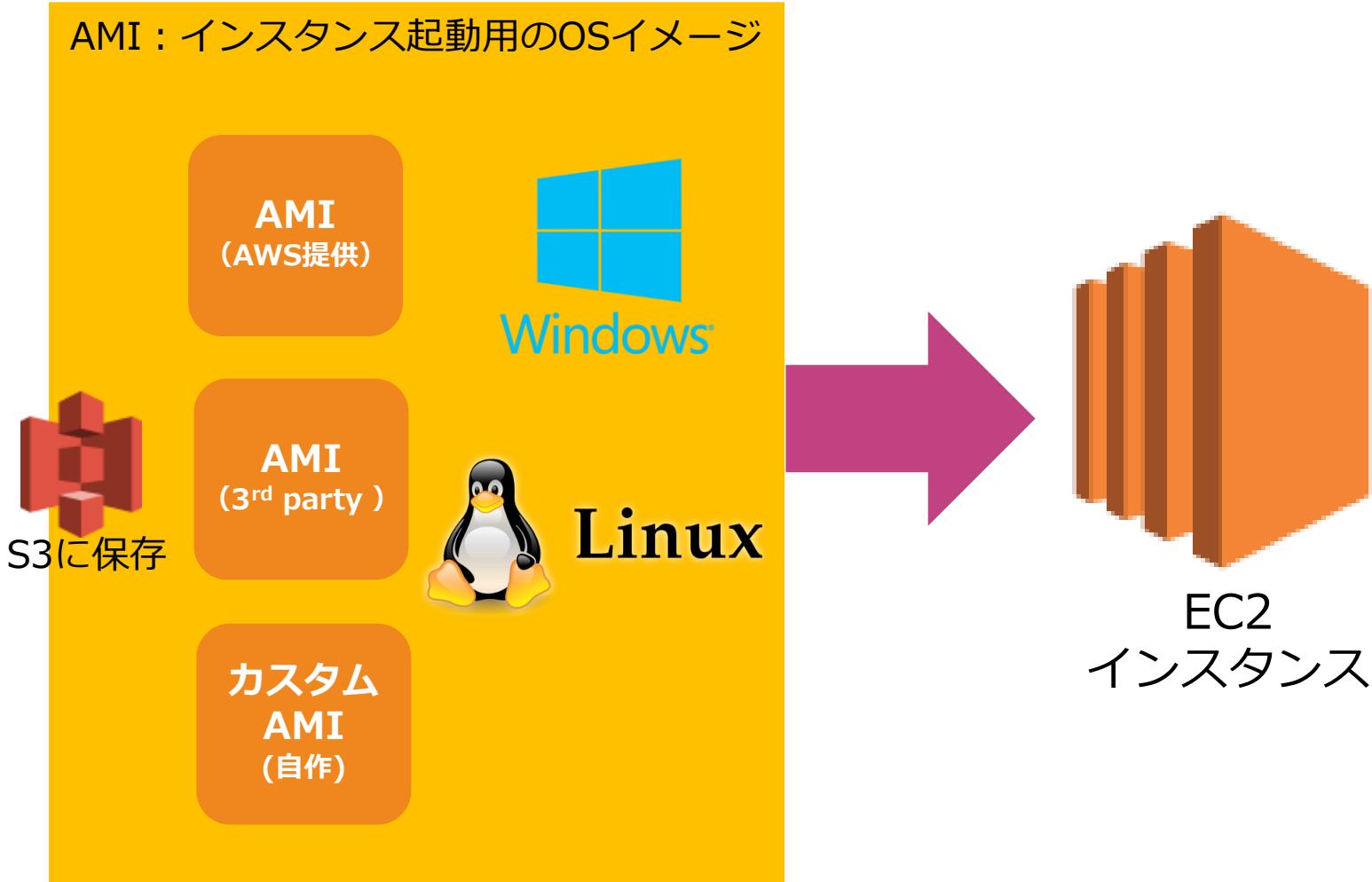
ストレージを選択

セキュリティグループを選択

キーペアを設定

AMIイメージ

AMIイメージはOSセッティング方式を選択すること



AMIイメージ

AMIイメージはOSセッティング方式を選択すること

The screenshot shows the AWS CloudFormation console with the 'Create New Stack' wizard open. The first step, 'Select template type', is selected. The left sidebar lists 'My Templates', 'AWS Marketplace', and 'Community Templates'. A checkbox for 'Only free-tier templates' is checked. The main area displays three template options:

- Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-92df37ed**
Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-92df37ed
- Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD ポリュームタイム - ami-2724cf58**
Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD ポリュームタイム - ami-2724cf58
- Microsoft Windows Server 2012 R2 with SQL Server 2016 Web - ami-e4e3089b**
Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Web edition. [English]

Each template entry includes a 'Select' button and a '64ビット' link. The top navigation bar shows the user 'udemy-aws-14days @ udemy...' and the region '東京'.

インスタンスタイプ

インスタンスタイプの選択はCPU・メモリ、ストレージ、ネットワークキャパシティなどのサーバーリソースの選択

The screenshot shows the AWS EC2 instance creation wizard at step 2: Instance Type Selection. The top navigation bar includes the AWS logo, service dropdown, resource group dropdown, and user information (udemy-aws-14days @ udemy...). The breadcrumb navigation shows steps 1 through 7. The main content area is titled "Step 2: Instance Type Selection". A descriptive text explains that Amazon EC2 offers various instance types for different use cases, allowing users to choose from a wide range of CPU, memory, storage, and network capabilities. It also mentions the "Free Usage Tier" for certain instance types.

Step 2: Instance Type Selection

Amazon EC2では、異なるユースケースに合わせて最適化されたさまざまなインスタンスタイプが用意されています。インスタンスは、アプリケーションを実行できる仮想サーバーです。CPU、メモリ、ストレージ、ネットワークキャパシティのさまざまな組み合わせが可能なため、アプリケーションに合わせて適切なリソースを柔軟に選択できます。インスタンスタイプおよびそれをコンピューティングのニーズに適用する方法に関する 詳細はこちら。

現在選択中: t2.micro (可変 ECU, 1 vCPU, 2.5 GHz, Intel Xeon Family, 1 GiB メモリ, EBS のみ)

ファミリー	タイプ	vCPU	メモリ (GiB)	インスタンス ストレージ (GB)	EBS 最適化利用	ネットワークパフォーマンス	IPv6 サポート
汎用	t2.nano	1	0.5	EBS のみ	-	低から中	はい
汎用	t2.micro 無料利用枠の対象	1	1	EBS のみ	-	低から中	はい
汎用	t2.small	1	2	EBS のみ	-	低から中	はい
汎用	t2.medium	2	4	EBS のみ	-	低から中	はい
汎用	t2.large	2	8	EBS のみ	-	低から中	はい

キャンセル 戻る 確認と作成 次の手順: インスタンスの詳細の設定

インスタンスタイプ

t2.nano

ファミリーと世代 インスタンスの容量

インスタンスファミリー

- M5 : 汎用
- T2 : 汎用
- C5 : コンピューティング最適化
- H1 : ストレージ最適化
- D2 : ストレージ最適化
- R4 : メモリ最適化
- X1 : メモリ最適化
- F1 : FPGA
- G3 : GPU

詳細は以下を参照

<https://aws.amazon.com/jp/ec2/instance-types/>

リザーブドインスタンス

利用期間を長期指定して利用する形式で、オンデマンドに比較して最大75%割安になる

	スタンダード	コンバータブル
利用期間	1年 (40%割引) 3年 (60%割引)	1年 (31%割引) 3年 (54%割引)
AZ／インスタンスサイズ／ネットワークタイプ変更可否	有	有
インスタンスファミリー／OS／テナント／支払オプションの変更可否	なし	有
リザーブドインスタンスマーケットプレイスでの販売可否	可能	今後可能となる予定
ユースケース	<ul style="list-style-type: none">□ 一定した状態または使用量が予測可能なワークフロー□ 災害対策などキャパシティ予約が可能なアプリケーション	

スポットインスタンス

予備のコンピューティング容量を、オンデマンドインスタンスに比べて割引（最大90%引き）で利用できるEC2インスタンス

- 予備用を入札式で利用するためとても安い（最大90%引き）
- 起動に通常よりも少し時間がかかる
- 予備用のため途中で削除される可能性がある
⇒一時的な拡張などの用途で利用

物理対応可能なインスタンス

物理サーバーにインスタンスを起動して制御が可能なタイプのインスタンス

ハードウェア専有インスタンス

- ✓ 専用HWのVPCで実行されるEC2インスタンス
- ✓ ホストHWのレベルで、他のAWSアカウントに属するインスタンスから物理的に分離する
- ✓ 同じAWSアカウントのインスタンスとはHWを共有する可能性がある

Dedicated Host

- ✓ EC2インスタンス容量を完全にお客様専用として利用できる物理サーバー
- ✓ サーバーにバインドされた既存のソフトウェアライセンスを利用可能

Bare Metal

- ✓ アプリケーションが基盤となるサーバーのプロセッサーとメモリーに直接アクセス可能なインスタンス
- ✓ AWSの各種サービスとの連携が可能でOSが直接下層のハードウェアにアクセス可能

ストレージ

EC2で直接利用するストレージは不可分なインスタンスストアと自分で設定するEBSの2つ

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でEC2と不可分のブロックレベルの物理ストレージ
- ✓ EC2の一時的なデータが保持され、EC2の停止・終了と共にクリアされる
- ✓ 無料

Elastic Block Store (EBS)

- ✓ ネットワークで接続されたブロックレベルのストレージでEC2とは独立して管理される
- ✓ EC2をTerminateしてもEBSは保持可能で、SnapshotをS3に保持可能
- ✓ 別途EBS料金が必要

ストレージ

EC2で直接利用するストレージは不可分なインスタンスストアと自分で設定するEBSの2つ

The screenshot shows the AWS EC2 instance creation process at Step 4: Storage Configuration. The top navigation bar includes the AWS logo, service dropdown, resource group dropdown, a bell icon, user information 'udemy-aws-14days @ udemy...', location '東京', and support dropdown.

The steps are numbered 1. AMI の選択, 2. インスタンスタイプの選択, 3. インスタンスの設定, 4. ストレージの追加, 5. タグの追加, 6. セキュリティグループの設定, and 7. 確認.

Step 4: ストレージの追加

説明文: インスタンスは次のストレージデバイス設定を使用して作成されます。インスタンスに追加の EBS ポリュームやインスタンスストアポリュームをアタッチするか、ルートポリュームの設定を編集することができます。また、インスタンスを作成してから追加の EBS ポリュームをアタッチすることもできますが、インスタンスストアポリュームはアタッチできません。Amazon EC2 のストレージオプションに関する [詳細](#)。

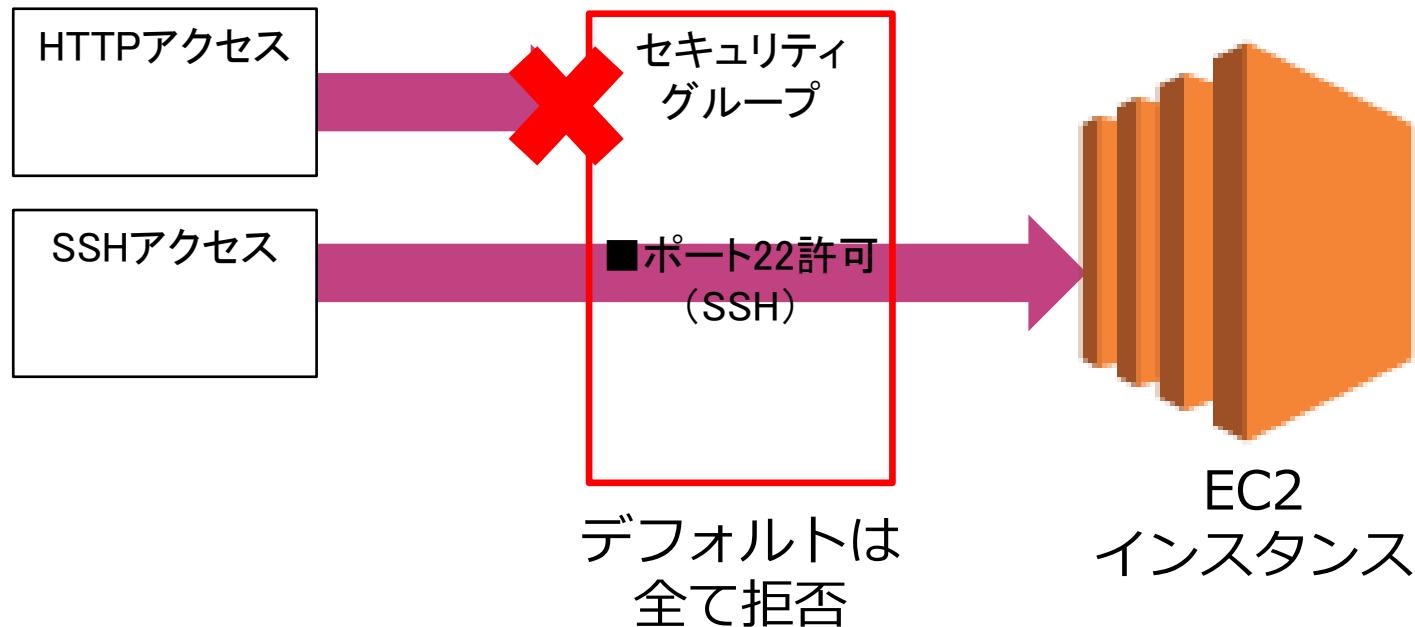
ポリュームタイプ	デバイス	スナップショット	サイズ (GiB)	ポリュームタイプ	IOPS	スループット (MB/秒)	合わせて削除	暗号化済み
ルート	/dev/xvda	snap-042e47fa6669a8b0b	8	プロビジョンド IOPS SSD (IO1)	400	該当なし	<input checked="" type="checkbox"/>	暗号化なし

新しいポリュームの追加

注意: 無料利用枠の対象であるお客様は 30 GBまでの EBS 汎用 (SSD) ストレージまたはマグネティックストレージを取得できます。無料利用枠の対象と使用制限に関する [詳細はこちら](#)。

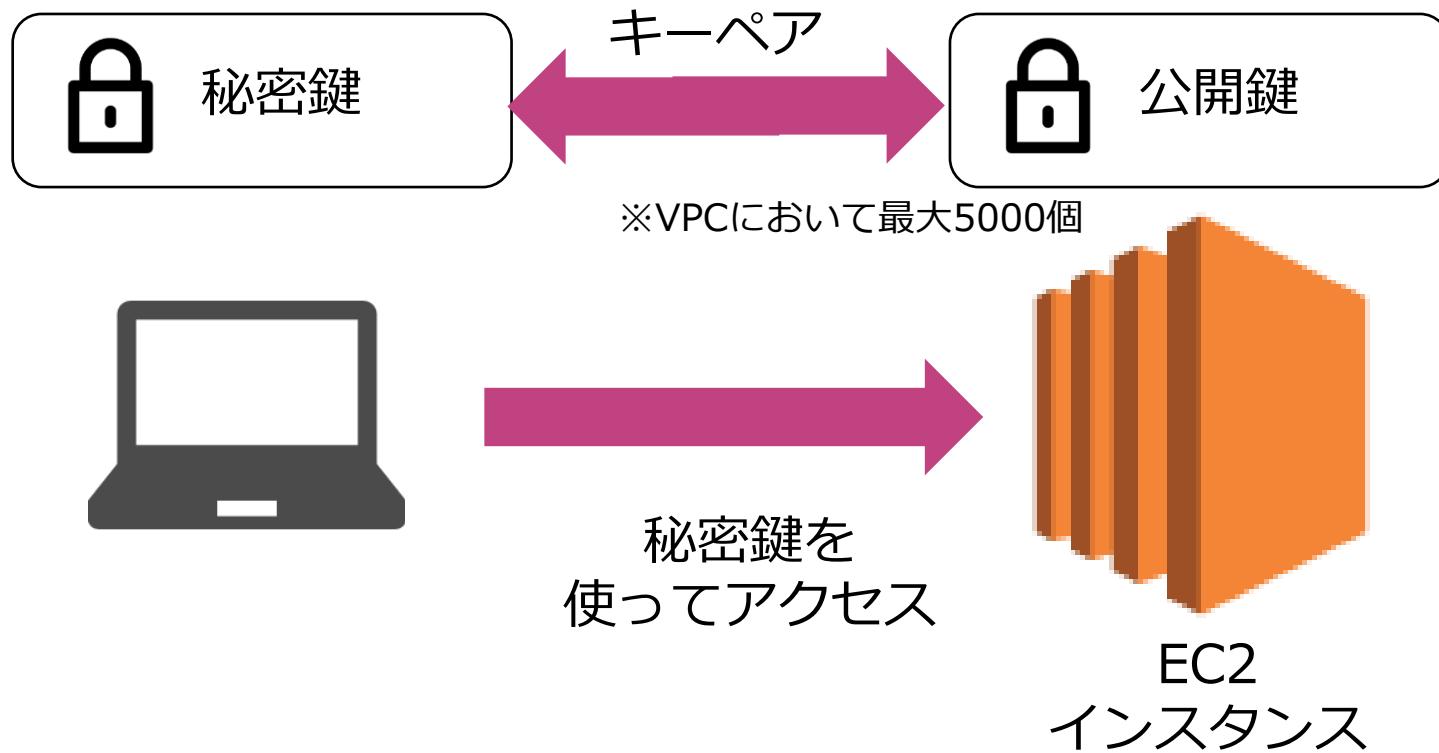
セキュリティグループ

インスタンスへのトラフィックのアクセス可否を設定するファイアーウォール機能を提供



キーペア

キーペアを利用して自身がダウンロードした秘密鍵とマッチした公開鍵を有するインスタンスにアクセスする



サーバーの役割の再確認

今回のサーバー設定

サーバーはサーバーとなるHWとサーバーソフトウェアを設定することで目的に応じた利用が可能になる



サーバーソフトウェア

今回のサーバー設定

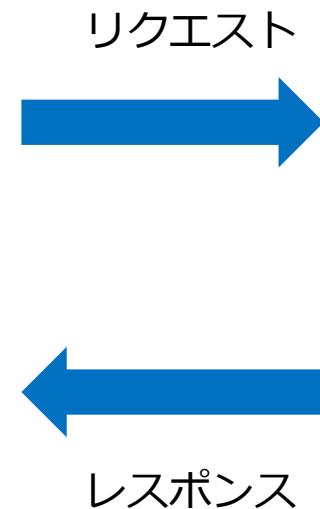
今回はEC2インスタンスをHWとして、APACHE HTTP SERVERをサーバーソフトウェアとして設定した。



今回のサーバー処理

リクエストとレスポンスがWEBアプリケーションの基本の動き

<https://13.230.87.16/>



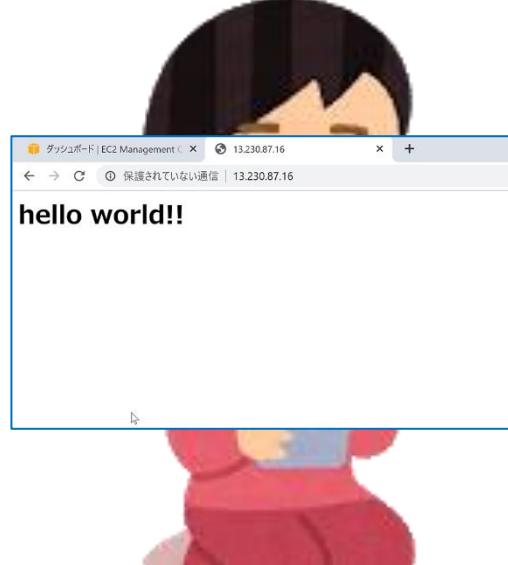
WEBサーバー



今回のサーバー処理

リクエストとレスポンスがWEBアプリケーションの基本の動き

<https://13.230.87.16/>



リクエスト



WEBサーバー



レスポンス



EBSの概要

EBSとは何か？

EBSはEC2インスタンスと共に利用されるブロックストレージ。
インスタンス上のワークロードなどに利用



EBSの選択

AWSは3つの形式のストレージサービスを提供

ブロックストレージ

- ✓ EC2にアタッチして活用するディスクサービス
- ✓ ブロック形式でデータを保存
- ✓ 高速・広帯域幅
- ✓ 例：EBS、インスタンスストア

オブジェクトストレージ

- ✓ 安価かつ高い耐久性をもつオンラインストレージ
- ✓ オブジェクト形式でデータを保存
- ✓ デフォルトで複数AZに冗長化されている。
- ✓ 例：**S3**、Glacier

ファイルストレージ

- ✓ 複数のEC2インスタンスから同時にアタッチ可能な共有ストレージサービス
- ✓ ファイル形式でデータを保存
- ✓ 例：EFS

EBSの選択

EC2が利用するのはインスタンスストアとEBSの2タイプのストレージ

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でEC2と不可分のブロックレベルの物理ストレージ
- ✓ **EC2の一時的なデータが保持**され、EC2の停止・終了と共にデータがクリアされる
- ✓ 無料

Elastic Block Store (EBS)

- ✓ ネットワークで接続されたブロックレベルのストレージでEC2とは独立管理
- ✓ EC2を終了してもEBSデータは保持可能
- ✓ SnapshotをS3に保持可能
- ✓ 別途EBS料金が必要

EBSの特徴

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



【基本】

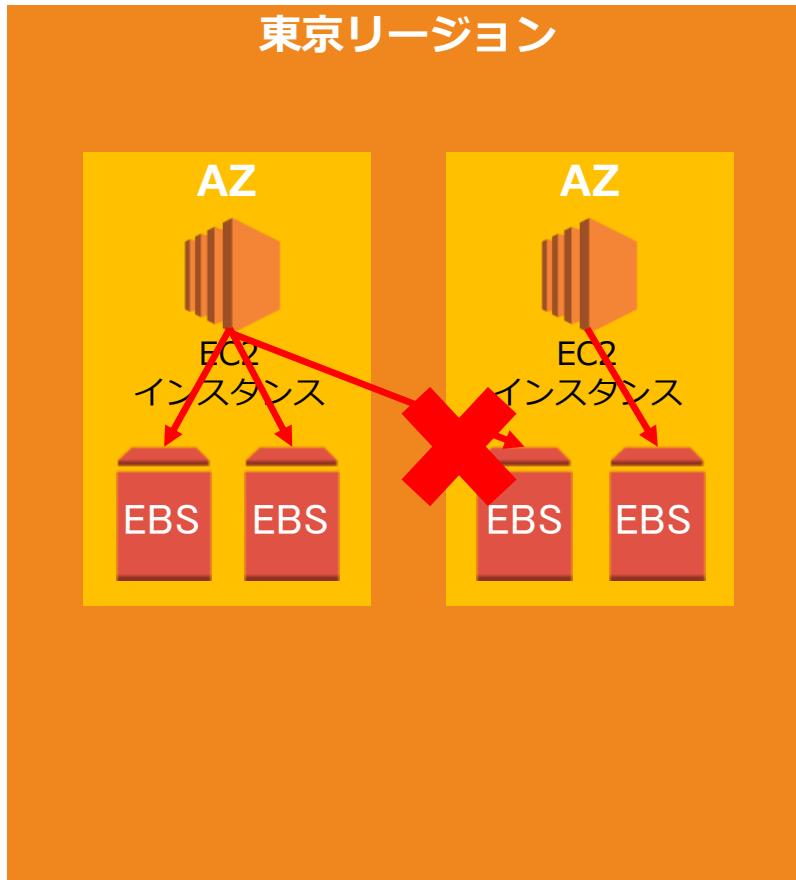
- ✓ OSやアプリケーション、データの置き場所など様々な用途で利用される
- ✓ 実体はネットワーク接続型ストレージ
- ✓ 99.999%の可用性
- ✓ サイズは1 GB～16TB
- ✓ サイズと利用期間で課金

【特徴】

- ✓ ボリュームデータはAZ内で複数のHWにデフォルトでレプリケートされており、冗長化されている。
- ✓ セキュリティグループによる通信制御対象外であり、全ポートを閉じてもEBSは利用可能
- ✓ データは永続的に保存

EBSの特徴

他のAZのインスタンスにはアタッチできない。

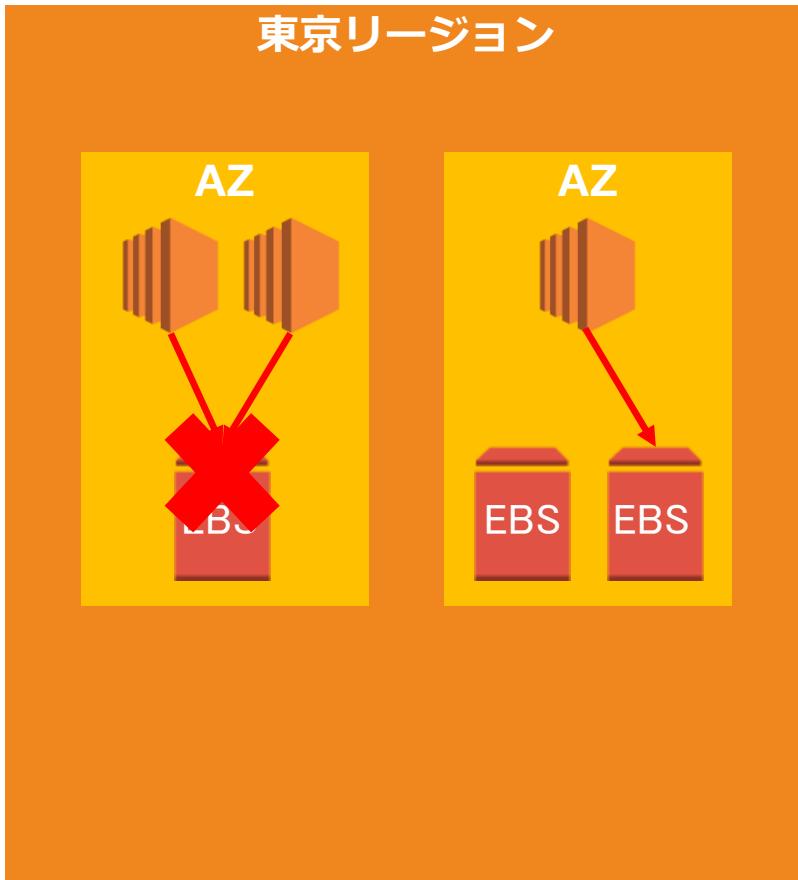


【特徴】

- ✓ EC2インスタンスは他のAZ内のEBSにアクセスできない

EBSの特徴

1つのEBSを複数のインスタンスで共有することはできない。

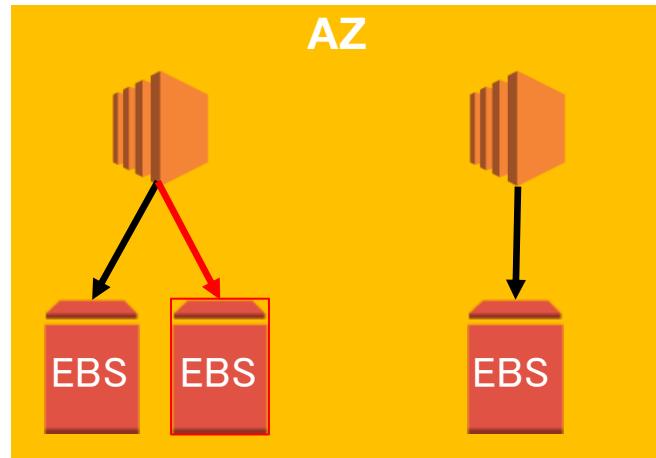


【特徴】

- ✓ EC2インスタンスに複数のEBSを接続することはできるが、EBSを複数のインスタンスで共有することはできない
- ✓ ただし、プロビジョンドIOPSのみ複数インスタンスで共有することが可能となった。

EBSの特徴

同じAZ内のインスタンスのみ付け替えが可能

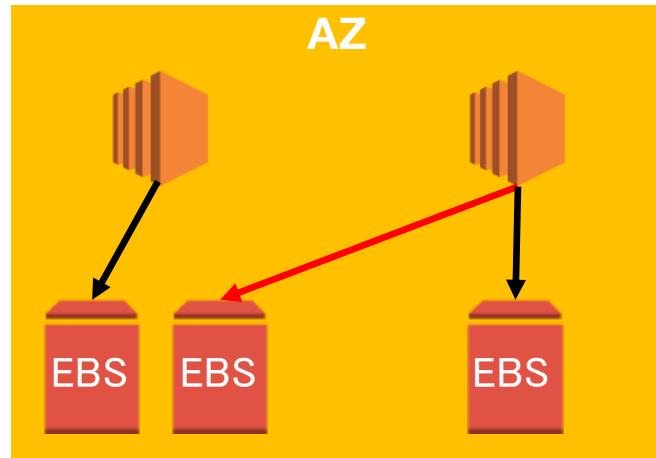


【特徴】

- ✓ 他のインスタンスに付け替えできる

EBSの特徴

同じAZ内のインスタンスのみ付け替えが可能



【特徴】

- ✓ 他のインスタンスに付け替えできる

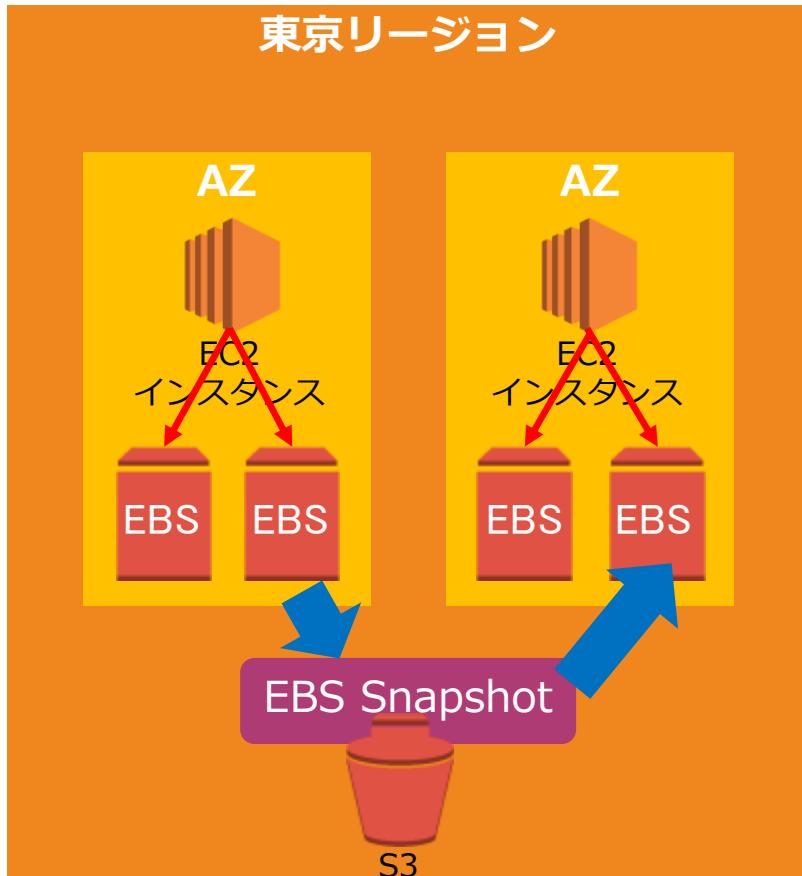
EBSのボリュームタイプ

ユースケースに応じて性能やコストが異なる5種類のボリュームタイプから選択

		ユースケース	サイズ
SSD	汎用SSD	<ul style="list-style-type: none">✓ 仮想デスクトップ✓ 低レイテンシーを要求するアプリ✓ 小～中規模のデータベース✓ 開発環境	1GB～16TB
	プロビジョンド IOPS	<ul style="list-style-type: none">✓ 高いI/O性能に依存するNoSQLやアプリ✓ 10,000IOPSや160MB/s超のワークロード大規模DB✓ Nitro システム Amazon EC2 インスタンス・EBS最適化インスタンスタイプで高速化	4GB～16TB
HDD	スループット最適化 HDD	<ul style="list-style-type: none">✓ ビッグデータ処理✓ DWH✓ 大規模なETL処理やログ分析✓ ルート（ブート）ボリュームには利用不可	500GB～16TB
	コールドHDD	<ul style="list-style-type: none">✓ ログデータなどアクセス頻度が低いデータ✓ バックアップやアーカイブ✓ ルート（ブート）ボリュームには利用不可	500GB～16TB
マグネティック(Magnetic)		<ul style="list-style-type: none">✓ 旧世代のボリュームで基本利用しない✓ データへのアクセス頻度が低いワークロード	1GB～1TB

スナップショットの特徴

EBSはスナップショットを利用してバックアップを取得する



【特徴】

- ✓ スナップショットでバックアップ
- ✓ スナップショットからEBSを別AZにも復元可能
- ✓ スナップショットはS3に保存される
 - スナップショットの2世代目以降は増分データを保存する増分バックアップとなる（1世代目を削除しても復元は可能）
 - スナップショット作成時にブロックレベルで圧縮して保管するため、圧縮後の容量に対して課金が行われる
 - スナップショット作成時でもEBSは利用可能である。

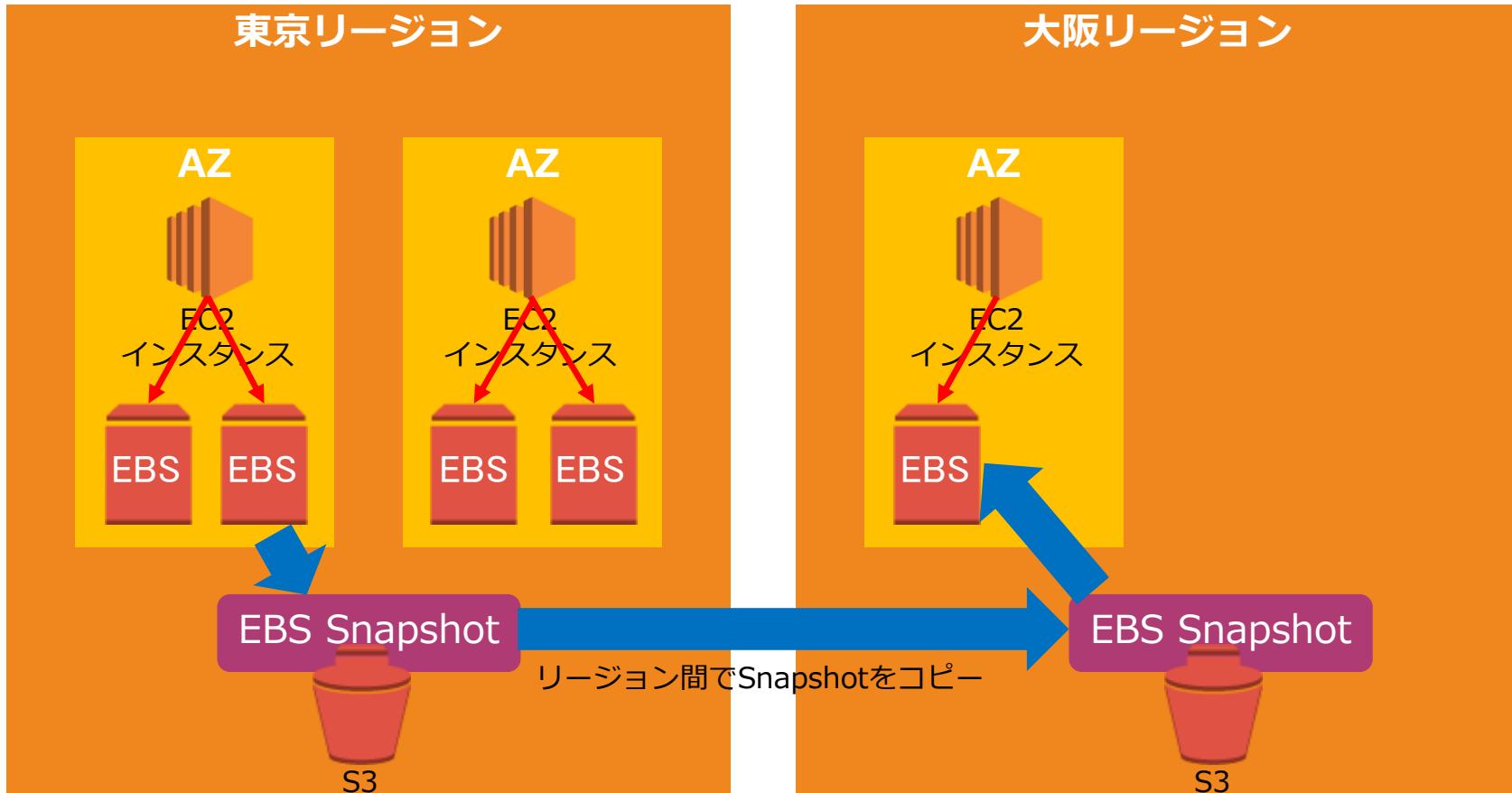
スナップショットの管理

スナップショットの作成時には静止点が推奨されているものの、いつでも実行可能でEBS操作に影響を与えない。DLMにより取得期間を設定可能

- スナップショット作成時はデータ整合性を保つため静止点の設定を推奨
 - ソフトウェアの機能を利用
 - ファイルシステムの機能を利用
 - バックアップソフトウェアの機能を利用
 - アプリケーションの停止
 - ファイルシステムのアンマウントなど
- 保存期間や世代数は無制限
- 世代管理が必要な場合はAWS CLIやAPI等で自動化する
- DLMを利用してスナップショット取得をスケジューリングできる。

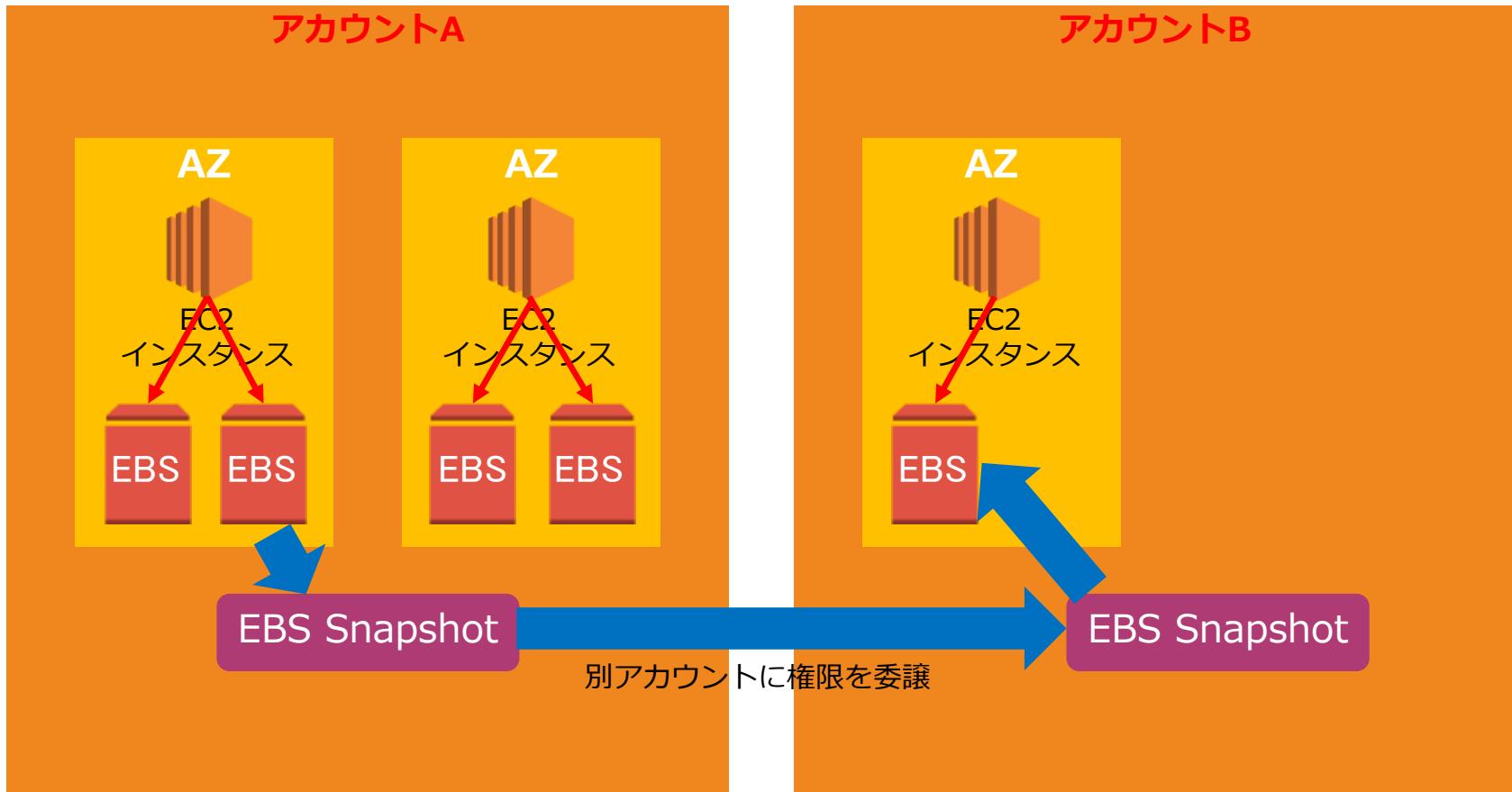
スナップショットの共有

スナップショットはリージョン間を跨いで利用可能



スナップショットの共有

スナップショットは権限を変更することで、他のアカウントに移譲することが可能



スナップショットとAMI

Amazon Machine ImageはOS設定のイメージであり、
Snapshotはストレージのバックアップとなる

AMI

- ✓ EC2インスタンスのOS設定などをイメージとして保持して、新規インスタンス設定に転用するもの
- ✓ 仮想サーバーのバックアップ

Snapshot

- ✓ ストレージ（EBS）のその時点の断面のバックアップとして保持するもの
- ✓ ストレージの復元や複製に利用

EBSボリュームの削除

EC2インスタンスの削除と共にEBSは削除されるため、データを保持したい場合は設定変更が必要

ルートボリュームのEBS

- ✓ EBS-backed AMIインスタンスにはルートボリュームにEBSが利用されている。
- ✓ デフォルト設定ではEC2インスタンスの削除と共にEBSボリュームも削除される。

DeleteOnTermination 属性

- ✓ TerminateOnDelete属性を有効化しているとEC2インスタンスの削除に応じてEBSも削除される
- ✓ 非有効化することでEBSボリュームのみ保持可能

EBSの暗号化

EBSはKMSのCMKを利用して、ボリューム作成時とスナップショット作成時に暗号化を実施する。

EBSの暗号化

- ✓ EBSボリュームやスナップショット作成時 AWS KMSの カスタマーマスターキー (CMK) を使用して暗号化を実施
- ✓ インスタンスとそれに接続された EBSストレージ間のデータ転送と保存データの両方に対して暗号化を実施する。

暗号化対象

- ✓ ボリューム内の保存データ
- ✓ ボリュームとインスタンスの間の転送データ
- ✓ ボリュームから作成されたすべてのスナップショット
- ✓ それらのスナップショットから作成されたすべてのボリューム

EBSのステータス

EBSは次の4つのステータス表示を理解することが必要

ボリュームのステータス	I/O 有効ステータス	I/O パフォーマンスステータス (プロビジョンド IOPS ボリュームでのみ使用可能)
ok	Enabled (I/O Enabled または I/O Auto-Enabled)	Normal (ボリュームパフォーマンスは想定どおり)
warning	Enabled (I/O Enabled または I/O Auto-Enabled)	Degraded (ボリュームのパフォーマンスが想定を下回っている) Severely Degraded (ボリュームのパフォーマンスが想定をかなり下回っている)
impaired	Enabled (I/O Enabled または I/O Auto-Enabled) Disabled (ボリュームがオフラインで復旧の保留中、またはユーザーによる I/O の有効化待ち)	Stalled (ボリュームのパフォーマンスは致命的な影響を受けている) Not Available (I/O が無効なため、I/O パフォーマンスの判定不能)
insufficient-data	Enabled (I/O Enabled または I/O Auto-Enabled) Insufficient Data	Insufficient Data ステータスチェックがまだ進行している場合も

Reference: https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/monitoring-volume-status.html

EBSのRAID構成

パフォーマンス向上と冗長化を高める目的で、EBSでは主に RAID0とRAID1の構成が実施される

RAID 0

- ✓ 目的：パフォーマンスを向上させる。
- ✓ RAID0は、複数のディスクを1台のディスクのように扱い読み書きを高速化する構成
- ✓ ストライピングと呼ぶ。

RAID 1

- ✓ 目的：ボリュームの冗長性を高める。
- ✓ RAID 1 では2つのボリュームを同時にミラーリングする。

サブネットマスクとサブネット

IPアドレスとサブネットマスク

IPアドレスは3桁 (0~255) ×4つの組合せで、各桁が8つのバイナリ値の集合を表す

【表記方法】

10.0.0.255

本当は2進数で8桁
00001010

本当は2進数で8桁
00000000

本当は2進数で8桁
11111111

IPアドレスとサブネットマスク

サブネットマスクはIPアドレス表記の後ろに／数値でくっついている

【表記方法】

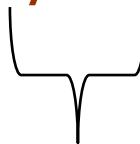
10.0.0.255/24

CIDR (Classless Inter-Domain Routing)

サブネットマスクの値を設定し、同じネットワークとして扱うIPアドレスの個数を調整できるIPアドレスの設定方法

【表記方法】

196.51.XXX.XXX/16



サブネット

左から16桁目までが同じネットワーク範囲と指定

CIDR (Classless Inter-Domain Routing)

2進数表記にしたときにサブネットが指定する数が利用できないようにロックされて変更不可となり、それ以外がIPアドレスとして利用できる

【表記方法】

10.0.0.255/8

00001010

⇒ロック！！！

CIDR (Classless Inter-Domain Routing)

2進数表記にしたときにサブネットが指定する数が利用できないようにロックされて変更不可となり、それ以外がIPアドレスとして利用できる

【表記方法】

10.0.0.255/16

00001010

⇒ロック!!!!

00000000

⇒ロック!!!!

CIDR (Classless Inter-Domain Routing)

2進数表記にしたときにサブネットが指定する数が利用できないようにロックされて変更不可となり、それ以外がIPアドレスとして利用できる

【表記方法】

10.0.0.255/24

00001010
⇒ロック!!!!

00000000
⇒ロック!!!!

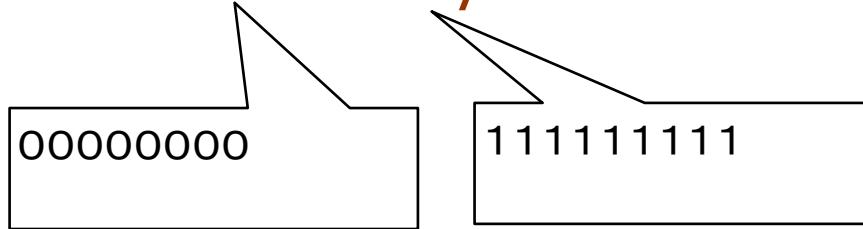
00000000
⇒ロック!!!!

CIDR (Classless Inter-Domain Routing)

ロックされていない16桁分のビットの間が有効なIPアドレスとして活用できる

【表記方法】

10.0.0.255/16



CIDR (Classless Inter-Domain Routing)

ロックされていない16桁分のビットの間が有効なIPアドレスとして活用できる

【最小値】

10.0.0.0

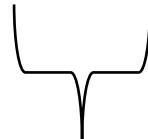
【最大値】

10.0.255.255

CIDR

IPアドレスの範囲は今後の拡張も踏まえて十分な余裕がありつつ、多すぎないレンジを指定する

10.0.0.255/16



推奨レンジ (65,534アドレス)

CIDR

CIDRに/XXを設定した際に設定可能となるIPアドレス数の組合せ

サブネットマスク	サブネット当たりのIPアドレス数
/18	16384
/20	4096
/22	1025
/24	256
/26	64
/28	16

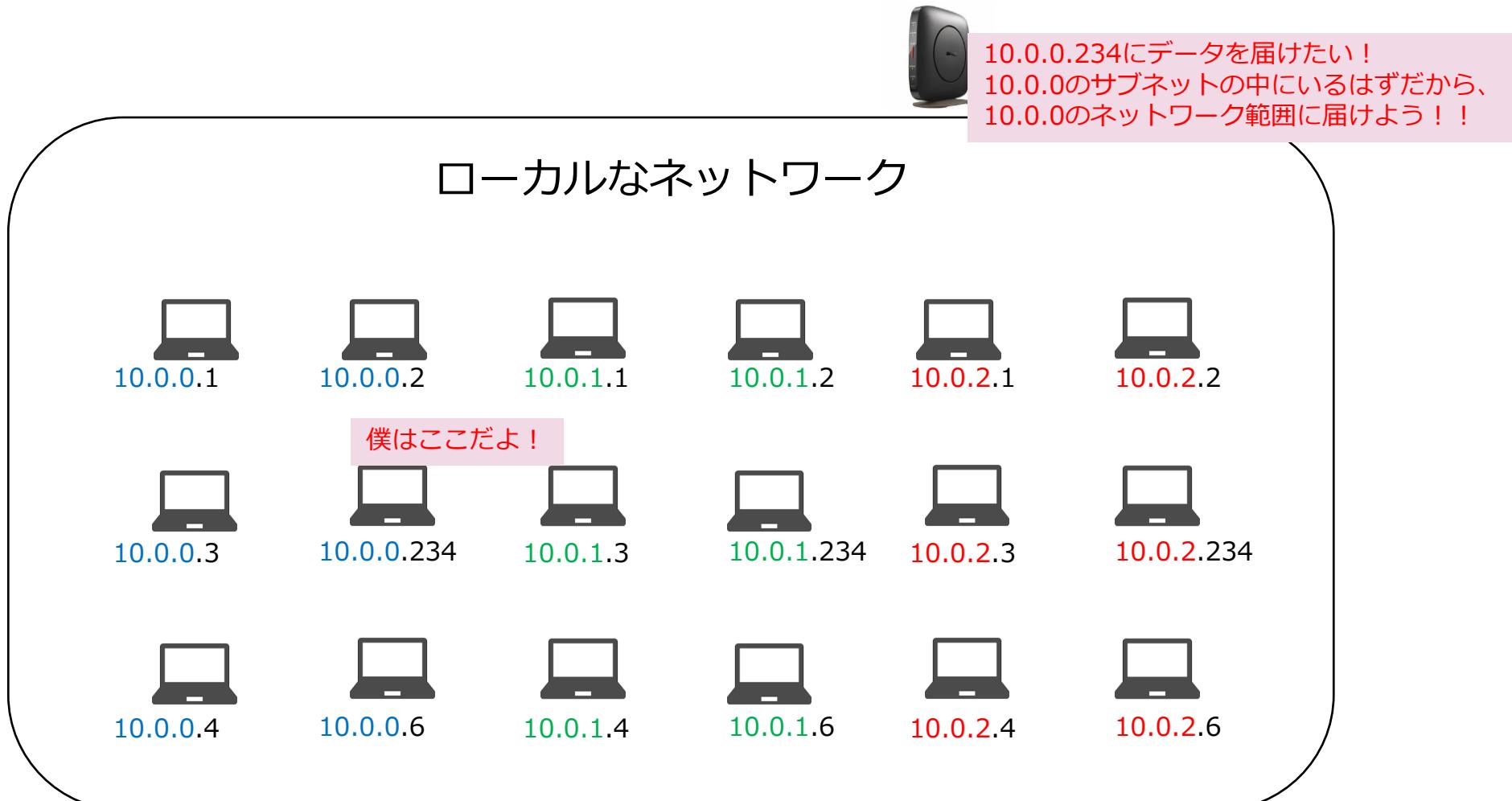
サブネットによるグループ化

ローカルなネットワークに沢山の機器がつながっていると特定の端末を発見しづらい



サブネットによるグループ化

サブネットマスクでアドレス範囲をグループ化することで、見つけやすくする。



サブネットによるグループ化

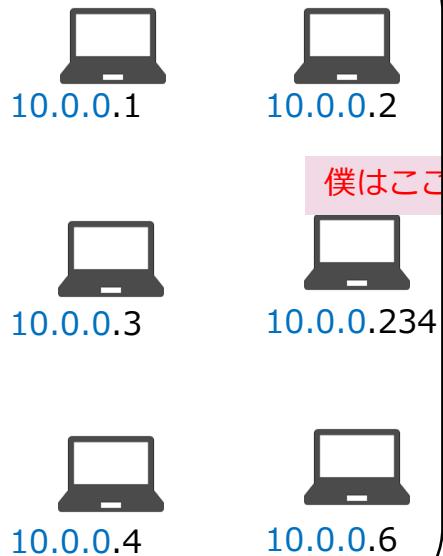
このサブネットマスクによるグループ化されたアドレス範囲内をサブネットと呼ぶ



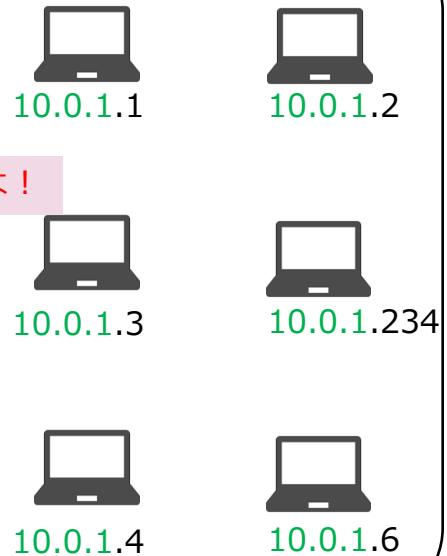
10.0.0.234にデータを届けたい！
10.0.0のサブネットの中にいるはずだから、
10.0.0のネットワーク範囲に届けよう！！

ローカルなネットワーク

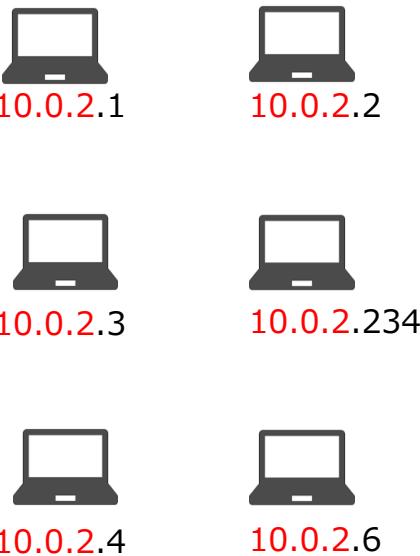
ブルーのサブネット



グリーンのサブネット



レッドのサブネット



サブネットによるグループ化

このサブネットマスクによるグループ化されたアドレス範囲内をサブネットと呼ぶ



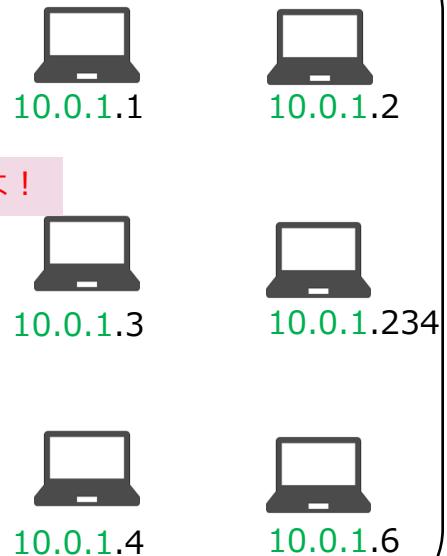
10.0.0.234にデータを届けたい！
10.0.0のサブネットの中にいるはずだから、
10.0.0のネットワーク範囲に届けよう！！

ローカルなネットワーク

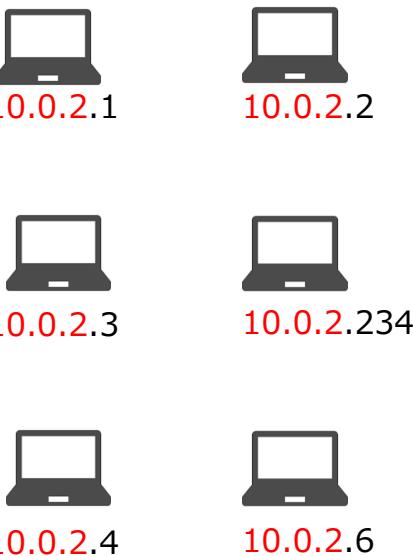
ブルーのサブネット



グリーンのサブネット



レッドのサブネット



10.0.0.0/24

10.0.1.0/24

10.0.2.0/24

VPCの概要

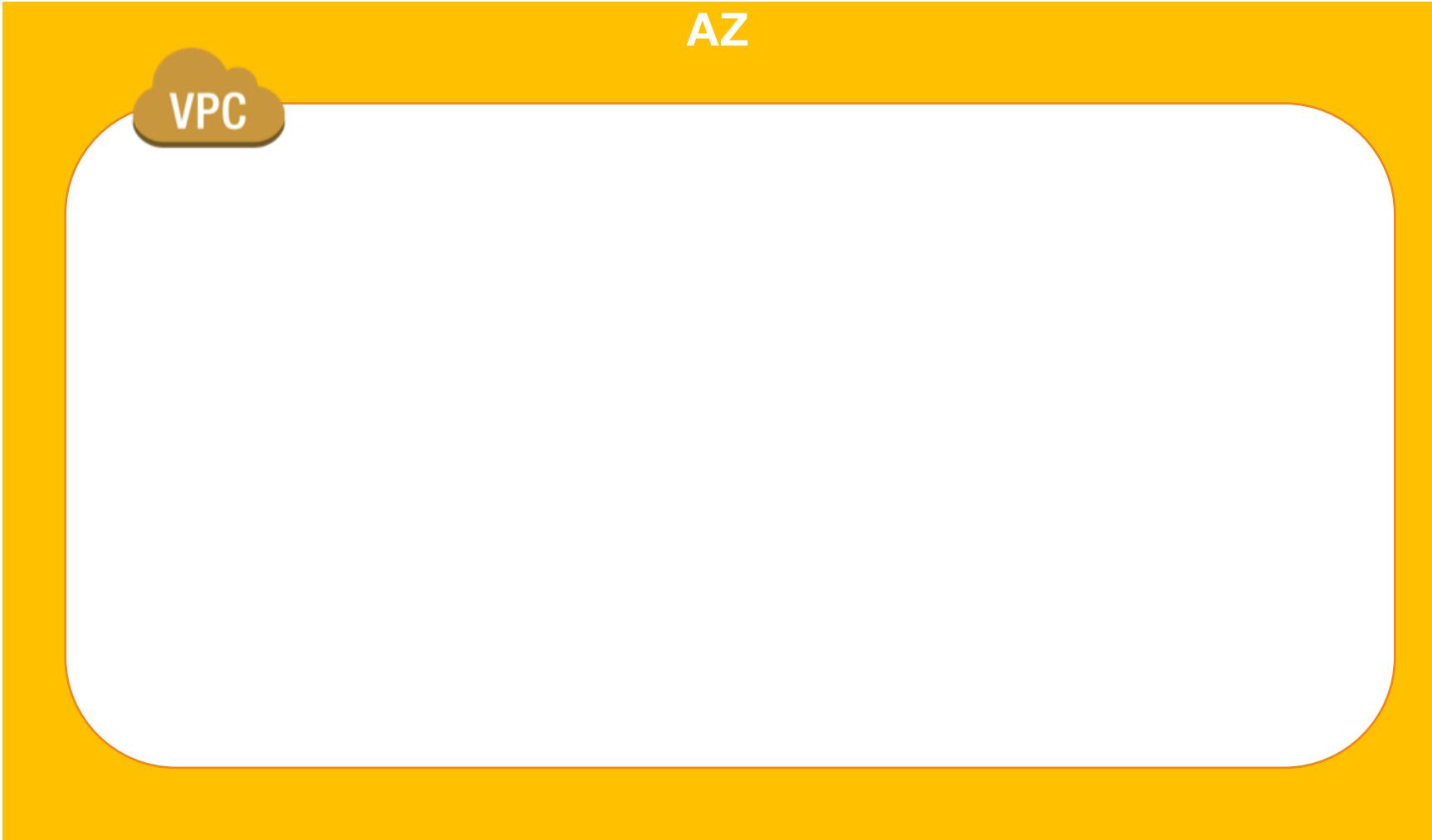
Virtual Private Cloud (VPC)

VPCはAWSクラウド内に論理的に分離されたセクションを作り、ユーザーが定義した仮想ネットワークを構築するサービス

- ✓ 任意の IP アドレス範囲の選択して仮想ネットワークを構築
- ✓ サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など仮想ネットワーキング環境を完全に制御可能
- ✓ 必要に応じてクラウド内外のネットワーク同士を接続することも可能
 - ✓ 複数の接続オプションが利用可能
 - インターネット経由
 - VPN/専用線(Direct Connect)

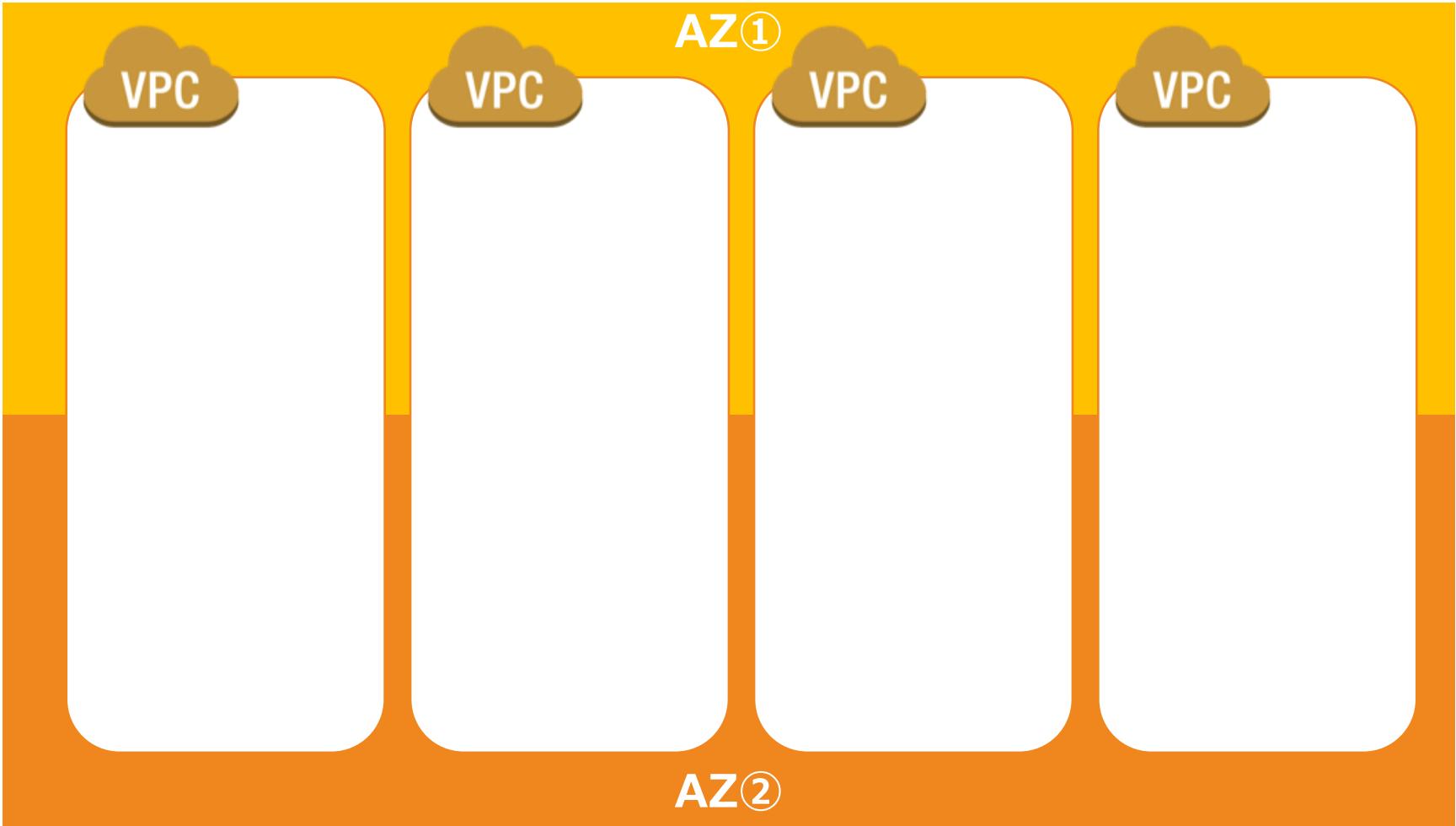
Virtual Private Cloud (VPC)

単一のVPCを構築すると単一AZの範囲に設定される。



Virtual Private Cloud (VPC)

同一リージョン内ではVPCは複数のAZにリソースを含めることができます



サブネットとVPC

VPCとサブネットの組合せでネットワーク空間を構築する
VPCはサブネットとのセットが必須



VPC設定手順



サブネット

サブネットはCIDR範囲で分割したネットワークセグメント

パブリックサブネット
10.0.1.0/24



トラフィックがインターネットゲートウェイにルーティングされるサブネット

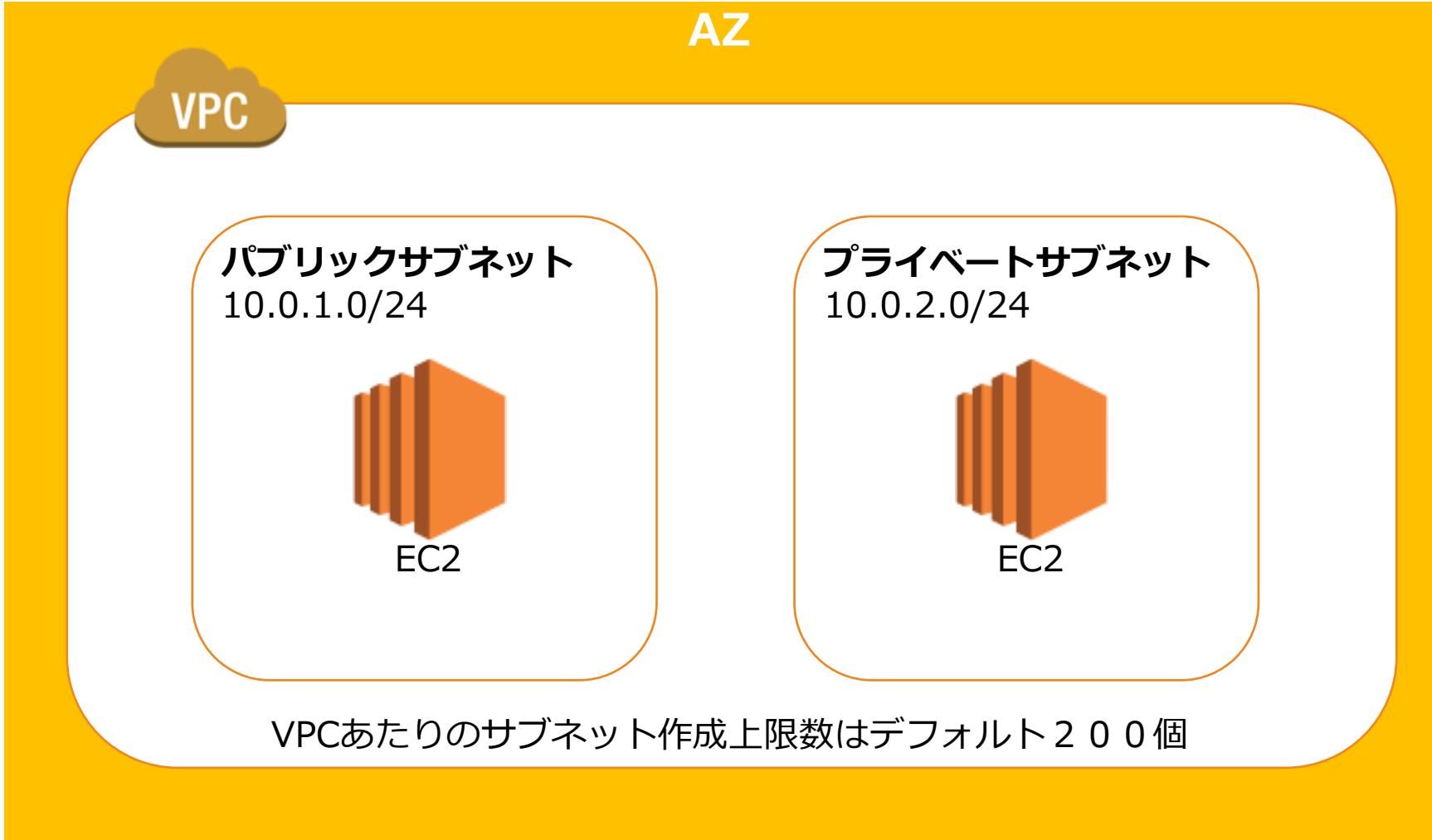
プライベートサブネット
10.0.2.0/24



インターネットゲートウェイへのルートがないサブネット

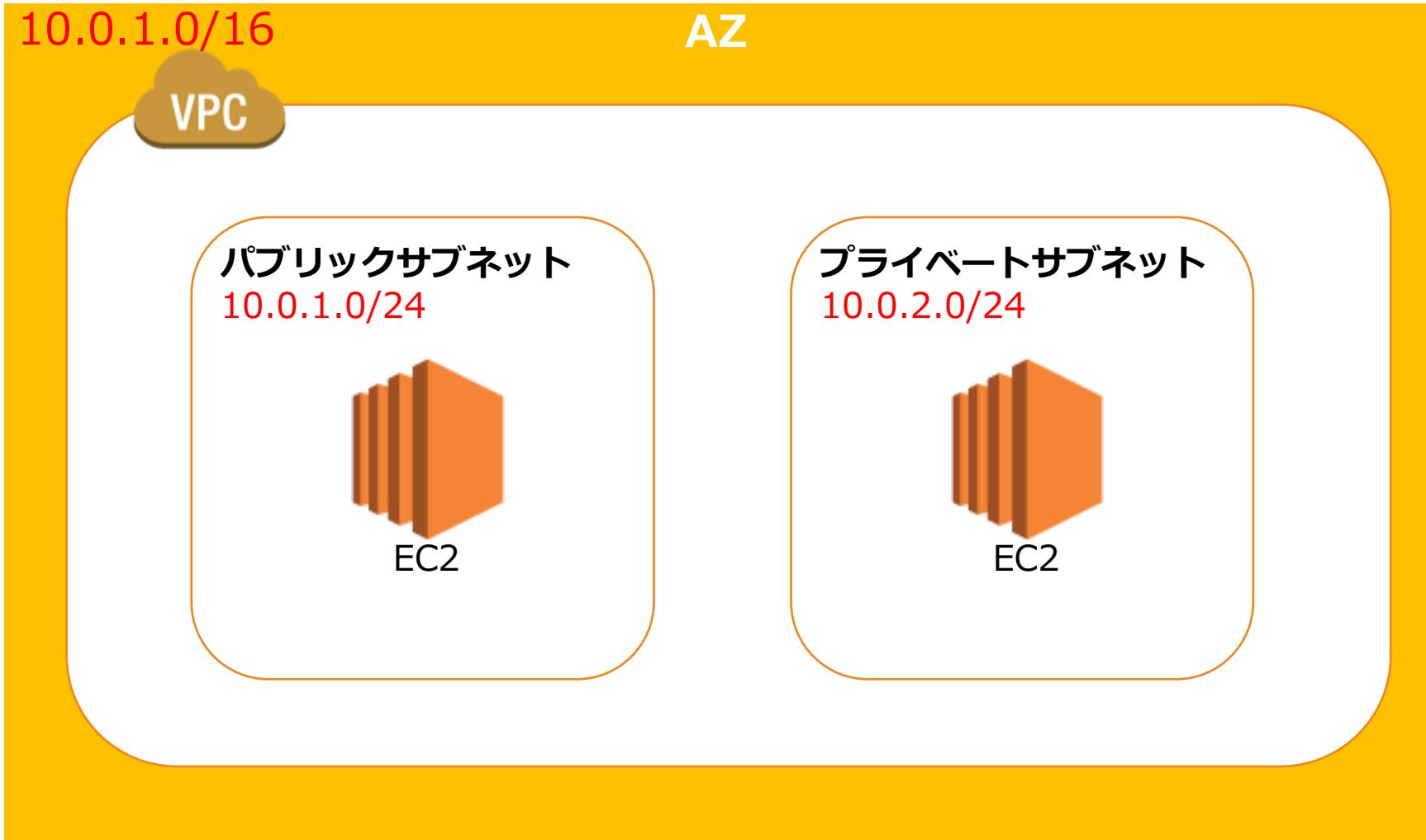
サブネット

サブネットはVPC内に複数設置でき、プライベートとパブリックに分かれる



CIDRの付与

VPCとサブネットにはCIDR（IPアドレス範囲）が付与され識別される



サブネット

インターネットゲートウェイへのルーティング有無でサブネットのタイプが分かれる

パブリックサブネット
10.0.1.0/24



トラフィックがインターネットゲートウェイにルーティングされるサブネット

プライベートサブネット
10.0.2.0/24



インターネットゲートウェイへのルートがないサブネット

サブネット

サブネットはインターネットアクセス範囲を定義するために利用する

パブリックサブネット
10.0.1.0/24



インターネットと接続が必要な
リソースを揃える

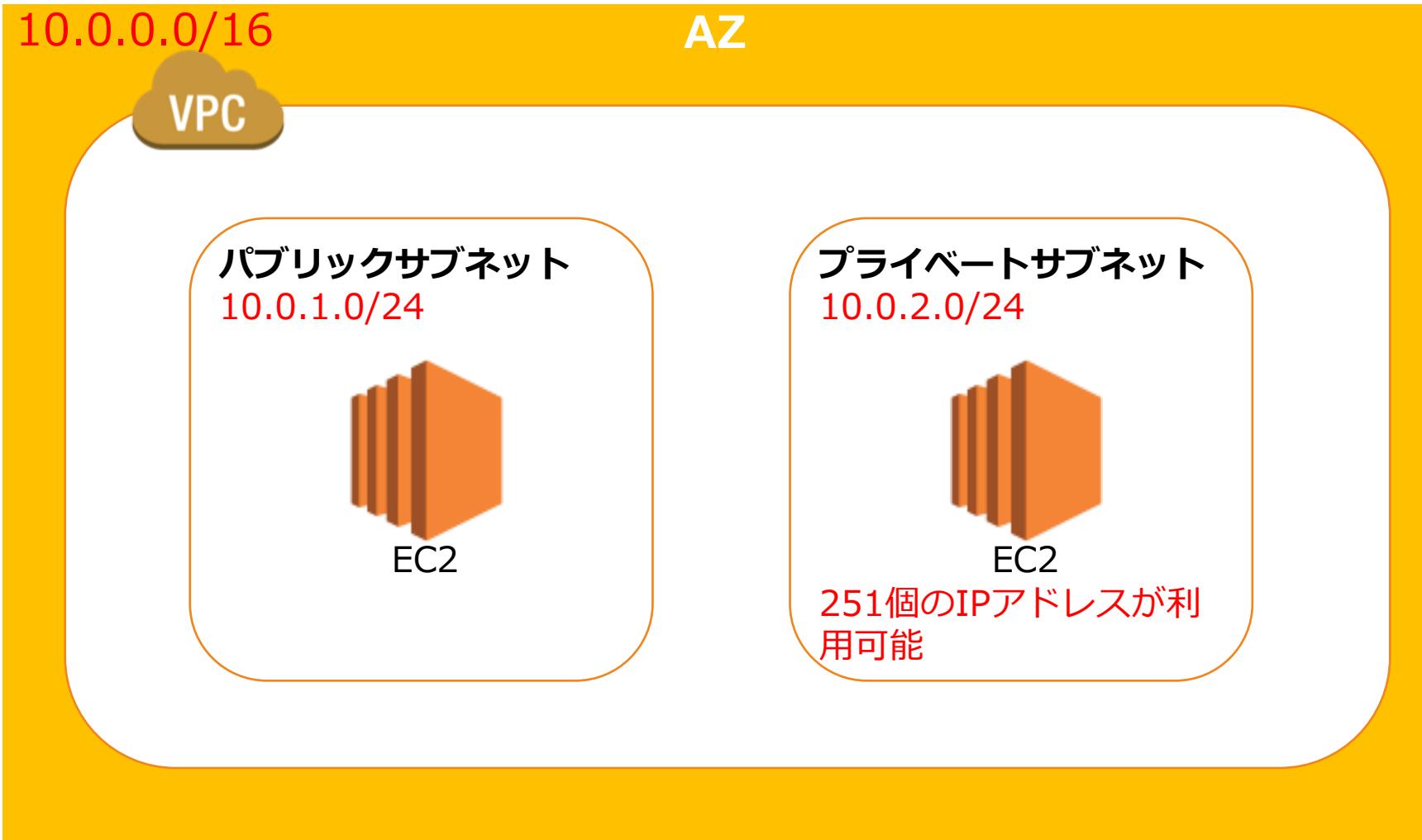
プライベートサブネット
10.0.2.0/24



インターネットから隔離することでセキュリティを高める

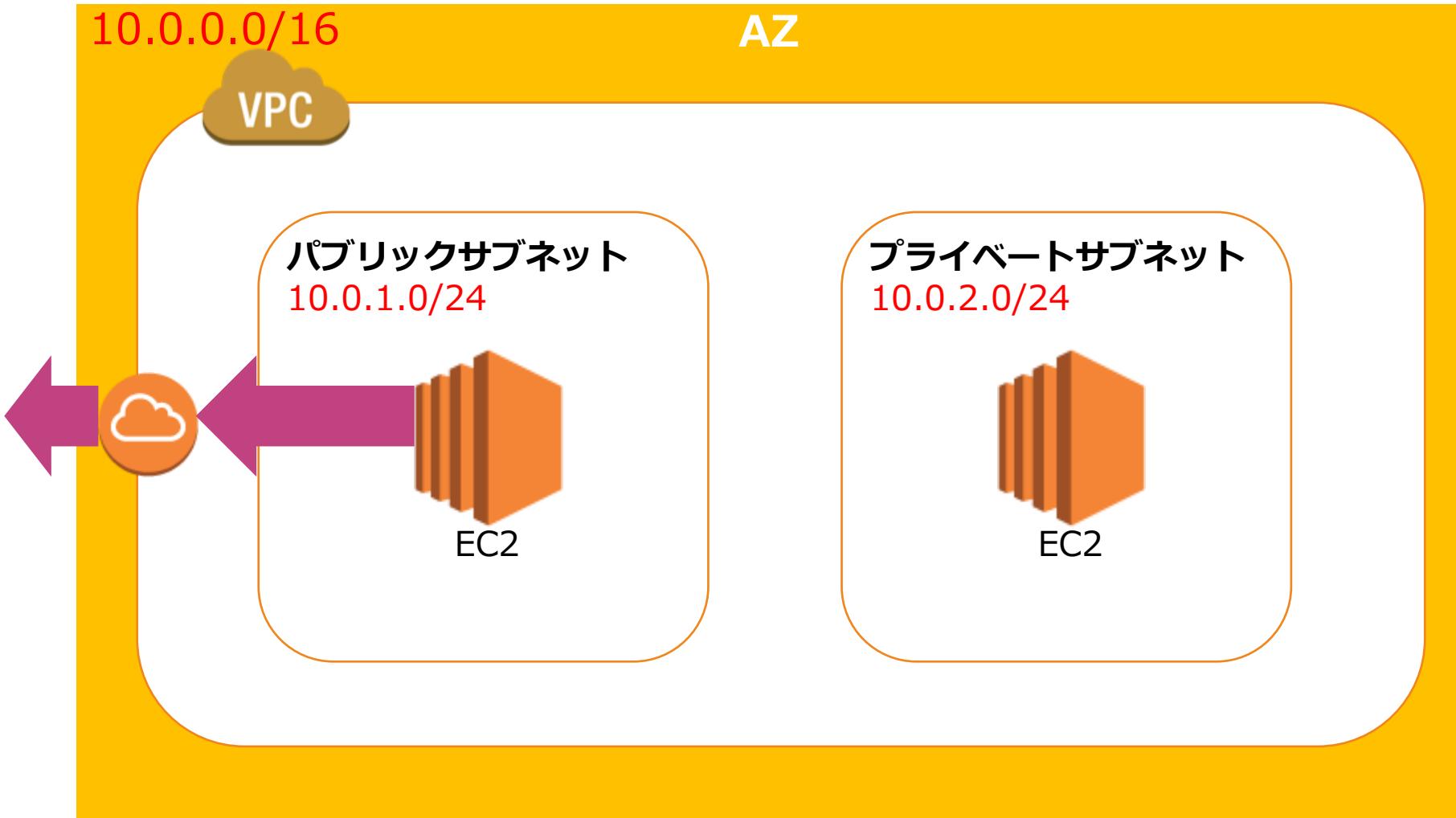
VPCにサブネットを設定

一般的にVPCにCIDR/16を設定し、サブネットに/24の設定が推奨されている。



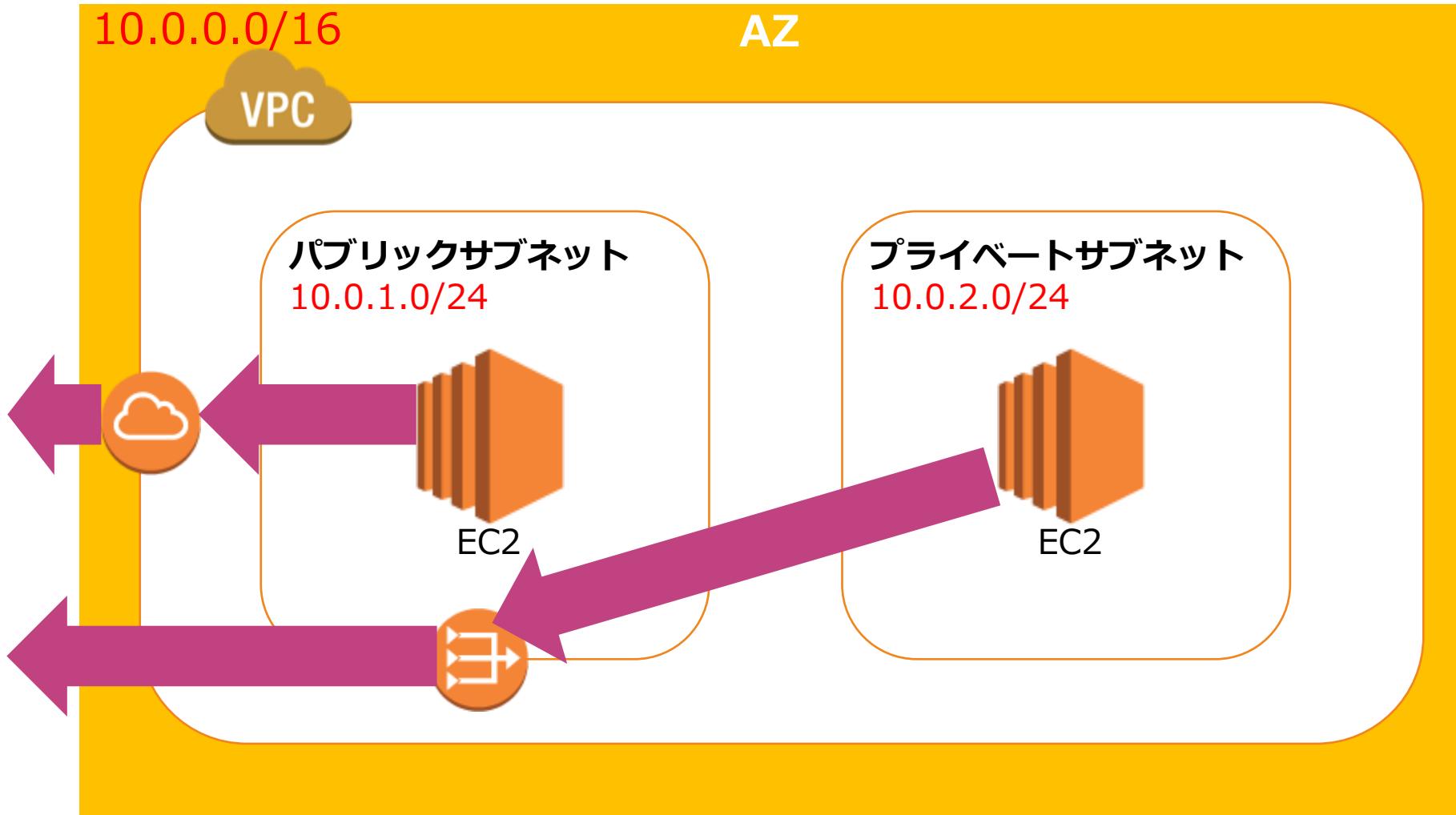
VPC外部接続

パブリックサブネットからインターネットに接続するにはインターネットゲートウェイが必要



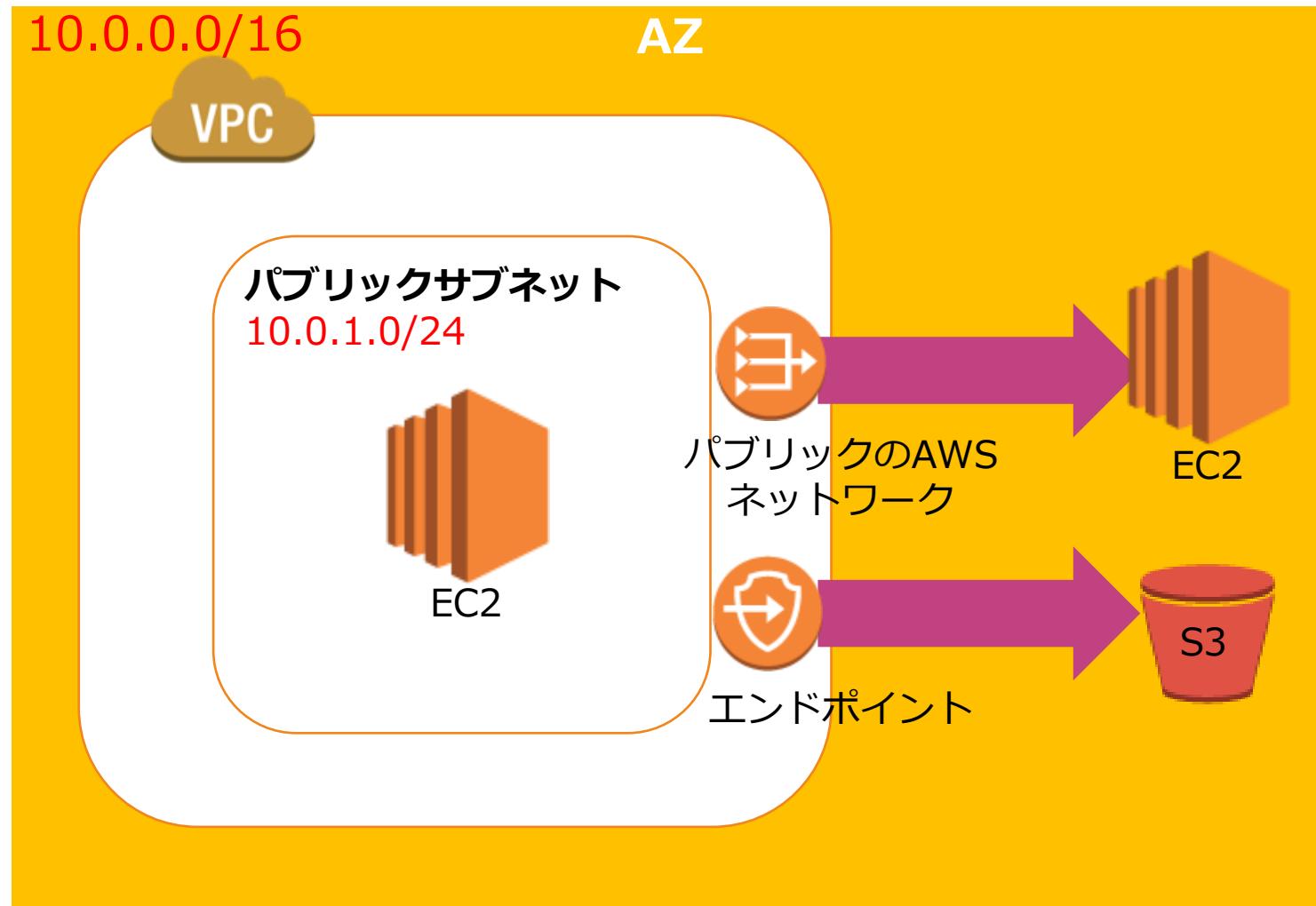
VPC外部接続

プライベートサブネットからインターネットに接続するには
NATゲートウェイがパブリックサブネットに必要



VPC外部接続

VPCの外側にあるリソースとの通信にはパブリックのAWSネットワークかエンドポイントを利用する



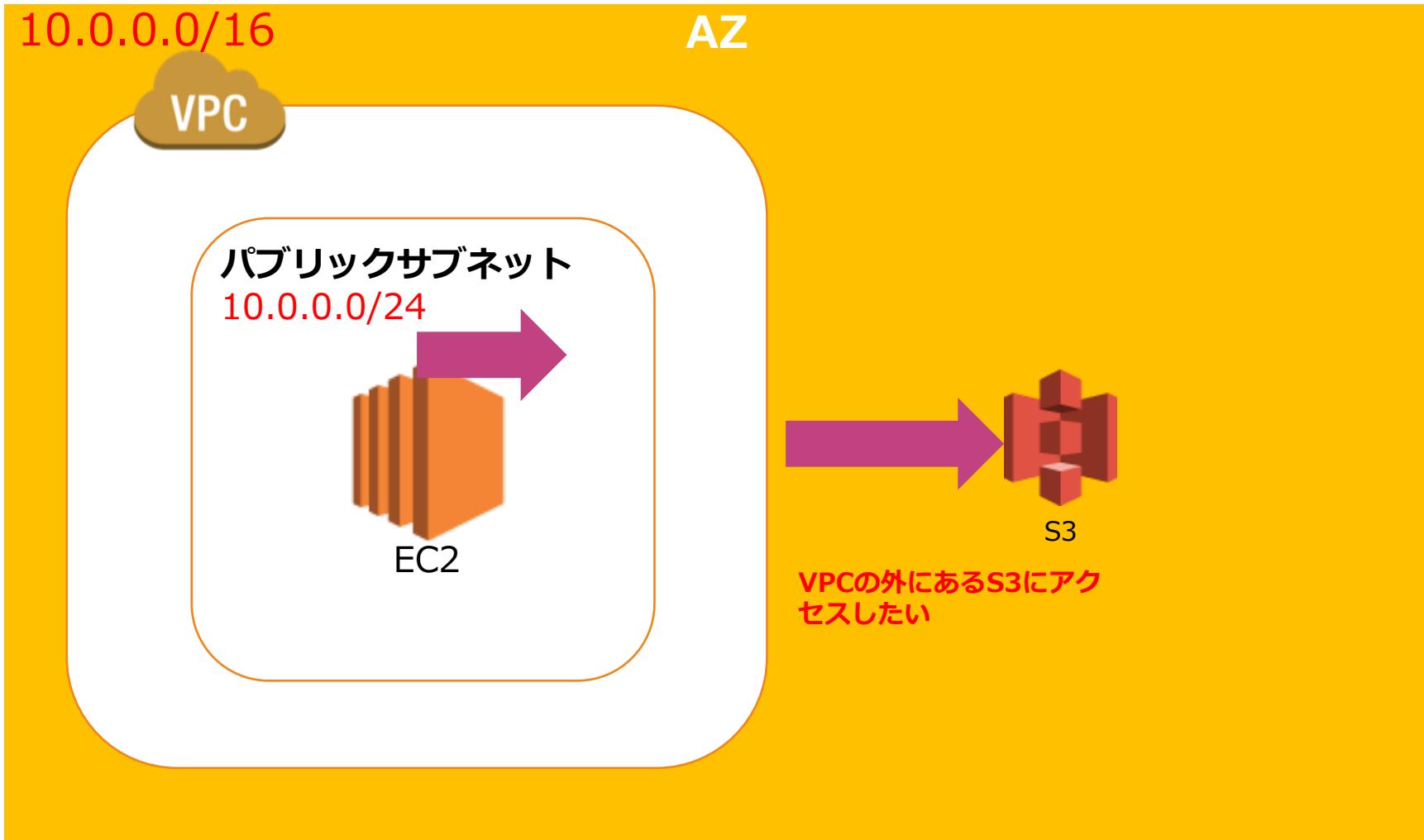
VPCとのオンプレミス接続

VPN接続

専用線接続
(Direct connect)

VPCエンドポイント

VPCエンドポイントはグローバルIPを持つAWSサービスに対して、VPC内から直接アクセスするための出口



NATゲートウェイ

NATゲートウェイによりプライベートサブネットのリソースがインターネットまたはAWSクラウドと通信が可能になる



【特徴】

- AWSによるマネージドNATサービス
- EIPの割り当て可能
- 最大10Gbpsの高パフォーマンス
- ビルトインで冗長化されている高可用性
- アベイラビリティゾーン毎に設置する

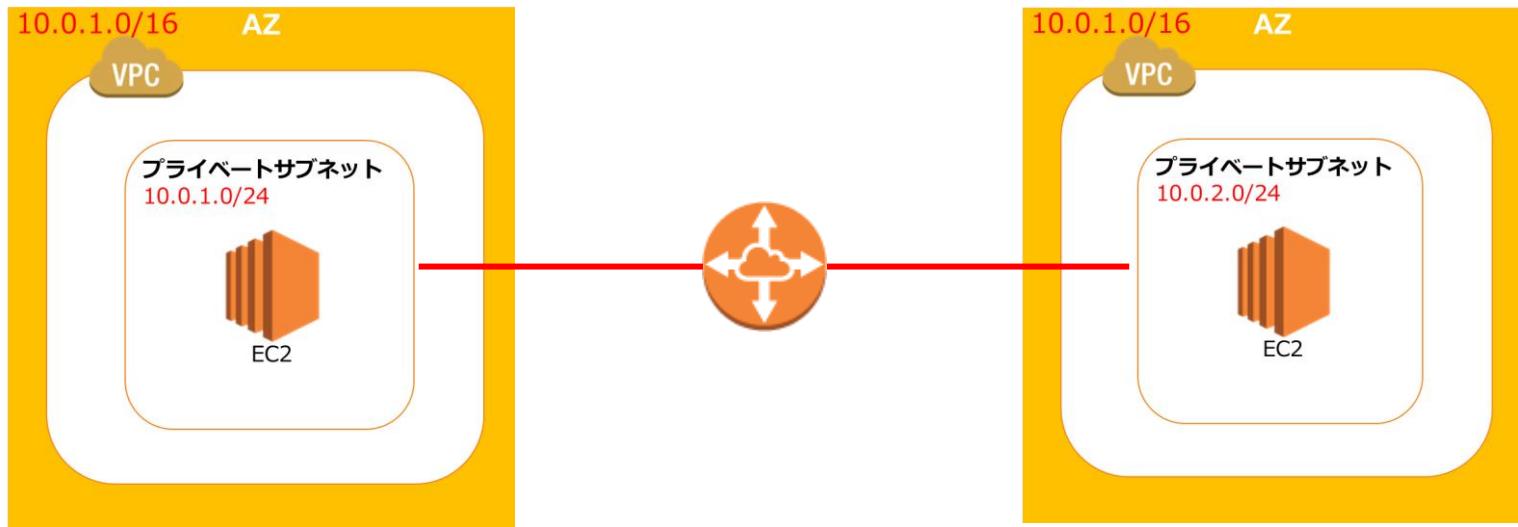
VPC Flow logs

VPC Flow Logsはネットワークトラフィックを取得し
CloudWatchでモニタリングできるようにする機能

- ネットワークインターフェースを送信元/ 送信先とするトラフィックが対象
- セキュリティグループとネットワークACLのルールでaccepted/rejectされたトラフィックログを取得
- キャプチャウインドウと言われる時間枠 (約10分間)で収集・プロセッシング・保存する
- RDS、Redshift、ElastiCache、WorkSpacesのネットワークインターフェーストラフィックも取得可能
- 追加料金はなし

VPC Peering

VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



- 異なるAWSアカウント間のVPC間をピア接続可能
- 一部のリージョン間の異なるVPC間のピア接続も可能
- 単一障害点や帯域幅のボトルネックは存在しない

VPCとの接続

VPCとのオンプレミス接続

VPN接続

専用線接続
(Direct connect)

Direct Connect

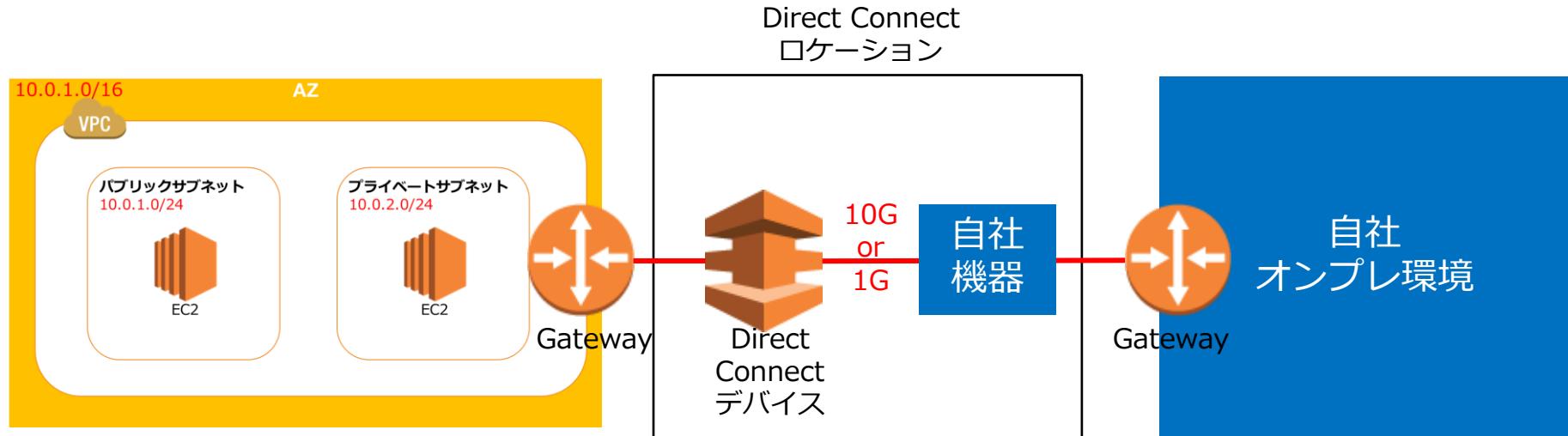
お客様のデータセンター やオフィスを専用線などを介して AWS ヘプライベートに接続するサービス

【Direct connectのメリット】

- 安価なアウトバウンドトラフィック料金
- ネットワーク信頼性の向上
- ネットワーク帯域幅の向上

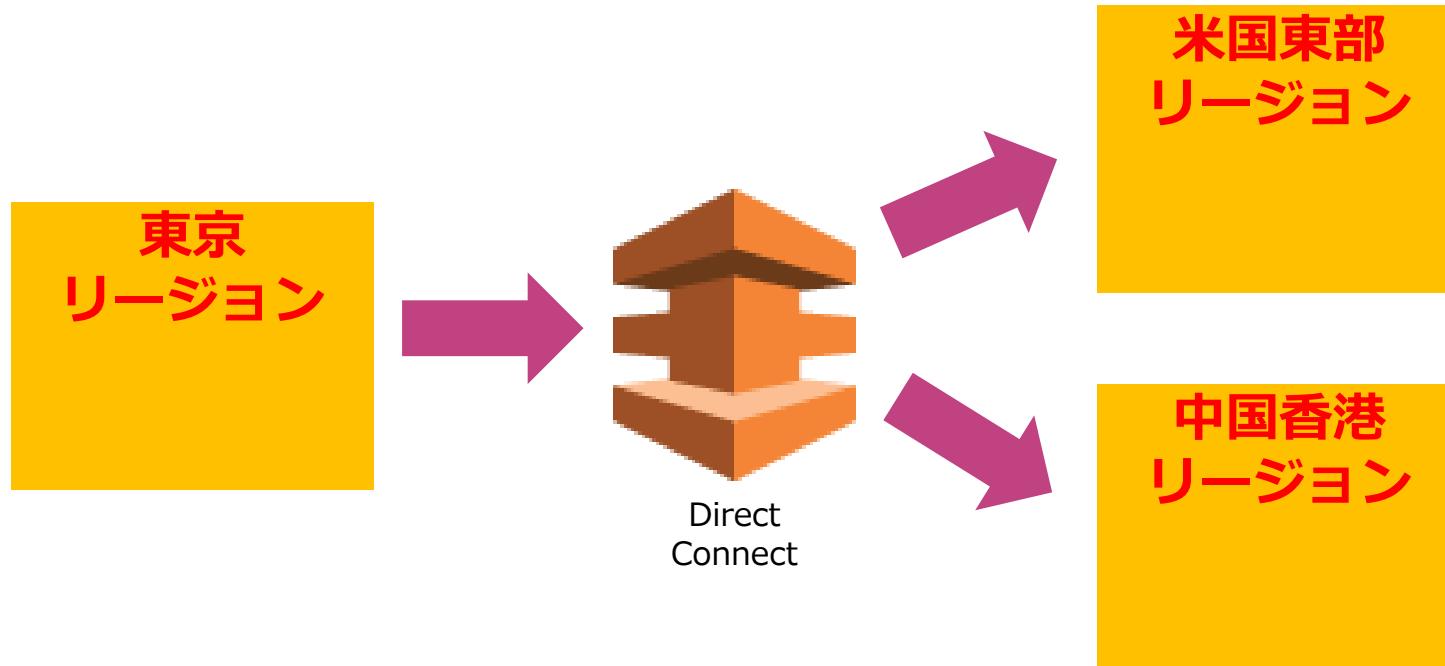
Direct Connect

Direct Connect口ケーションに物理的に自社オンプレ環境を接続することでAWS環境との専用線接続を実現する



Direct Connect gateway

Direct Connect gatewayにより、同一アカウントに所属する複数リージョンの複数AZから複数リージョンの複数VPCに接続



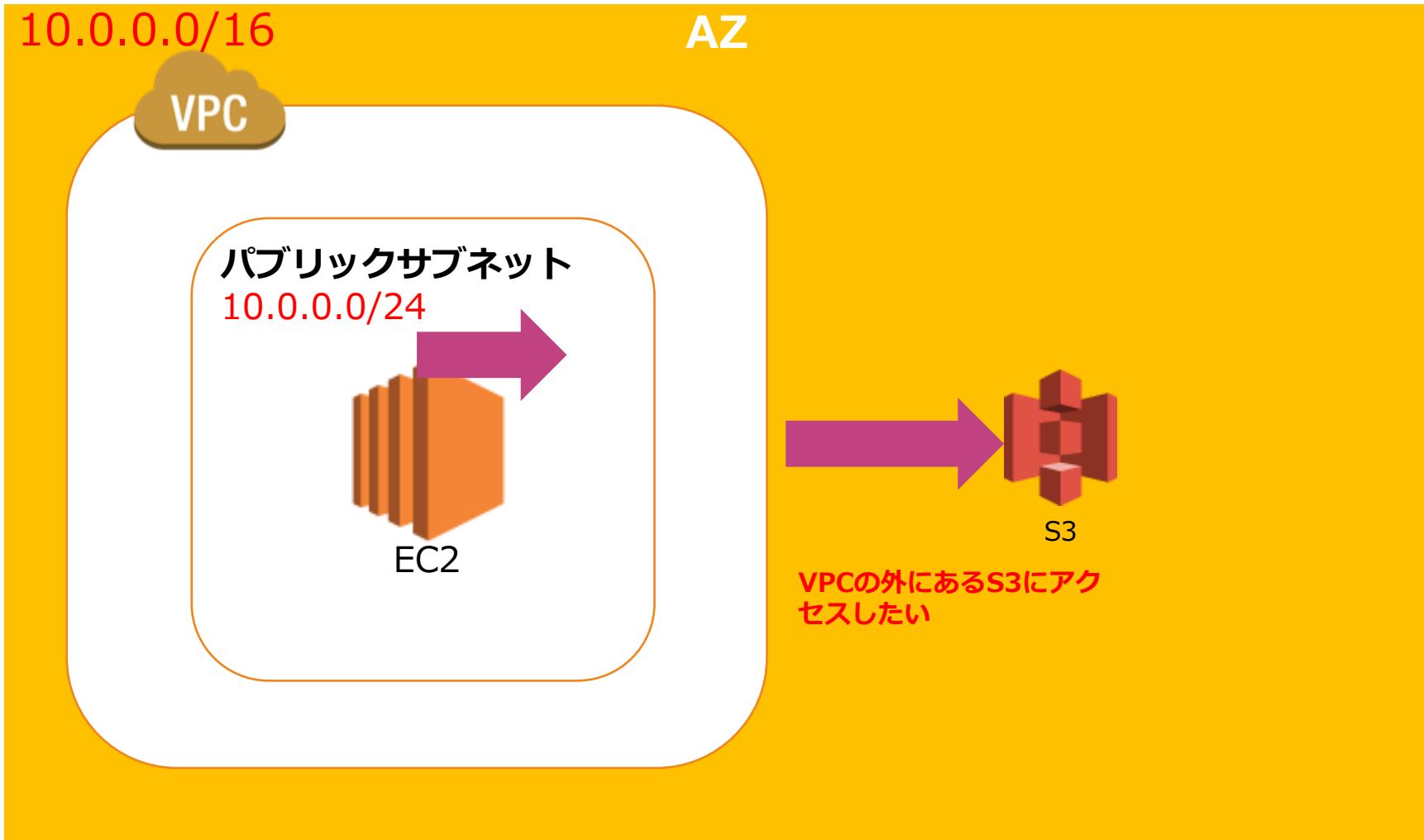
VPNとのDirect Connect

VPNの方が安く素早く利用できるが、信頼性や品質は専用線が勝る

	VPN	専用線
コスト	✓ 安価なベストエフォート回線が利用可能	✓ キャリアの専用線サービス契約が必要となりVPNより割高
リードタイム	✓ クラウド上での接続設定で可能なため即時	✓ 物理対応が必要なため数週間
帯域幅	✓ 暗号化のオーバーヘッドにより制限がある	✓ ポートあたり1G/10Gbps
品質	✓ インターネット経由のためネットワーク状態の影響を受ける	✓ キャリアにより高い品質が保証される
障害切り分け	✓ インターネットベースのため自社で保持している範囲以外の確認は難しい	✓ 物理的に経路が確保されているため比較的容易

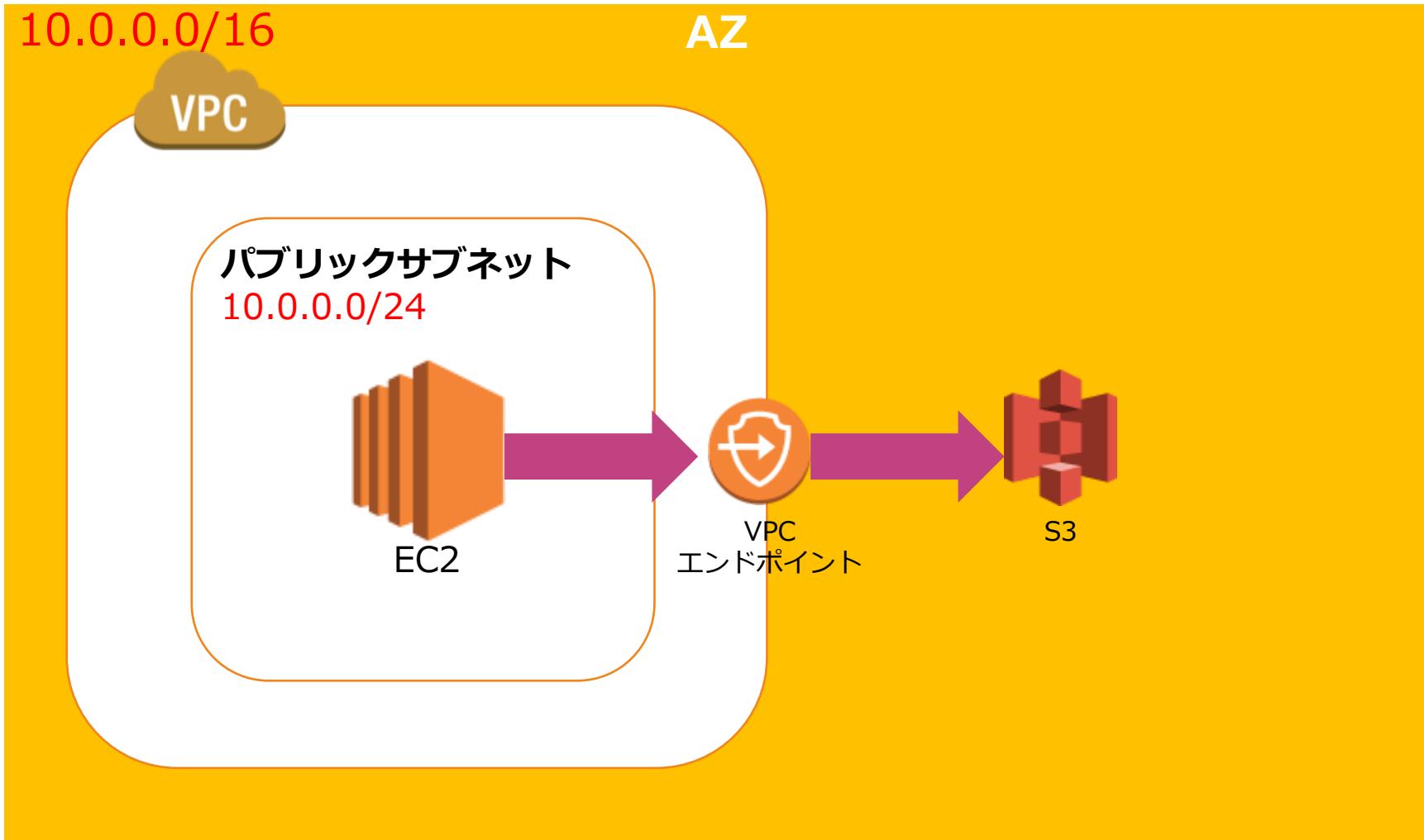
VPCエンドポイント

VPCエンドポイントはグローバルIPを持つAWSサービスに対して、VPC内から直接アクセスするための出口



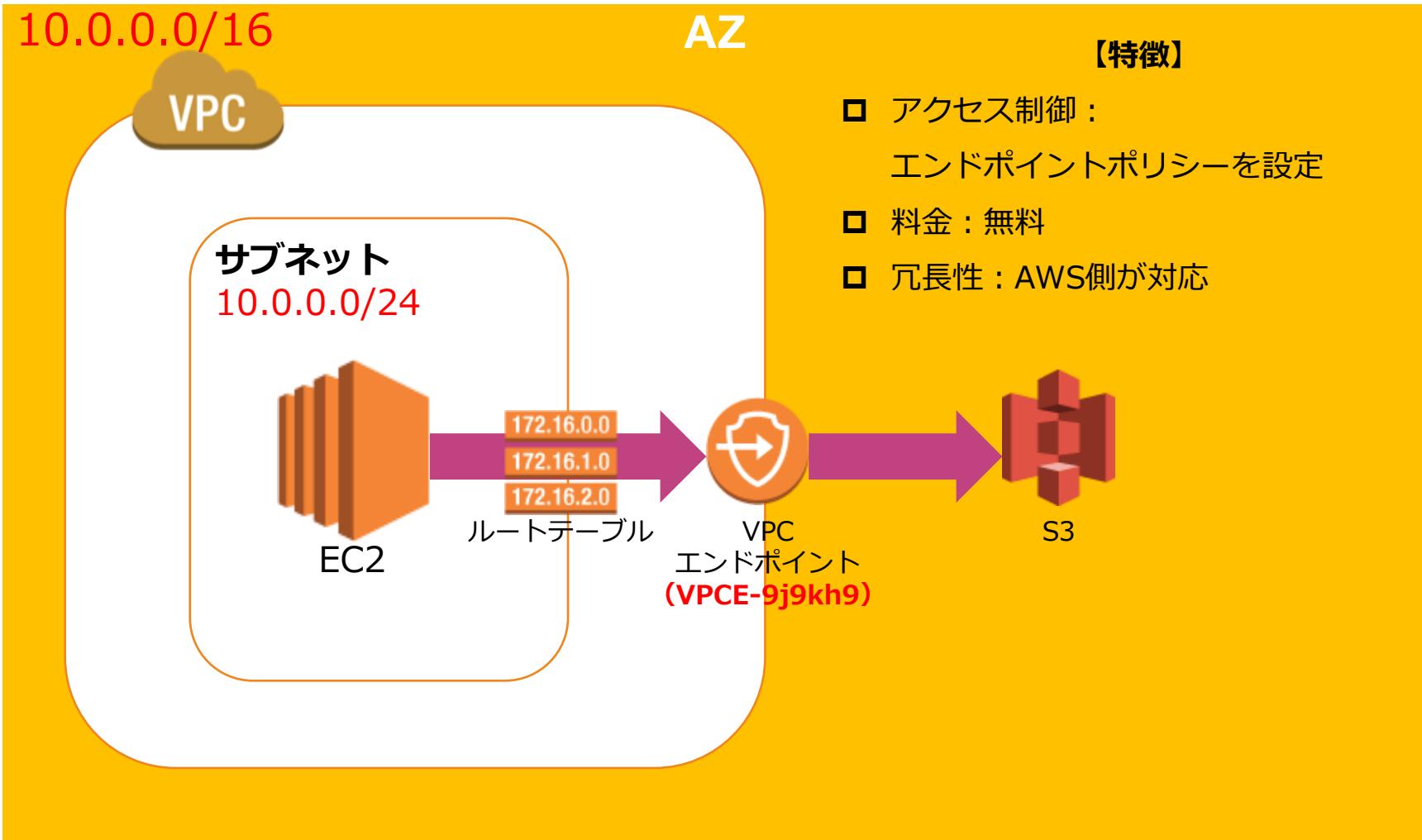
VPCエンドポイント

VPCエンドポイントはグローバルIPを持つAWSサービスに対して、VPC内から直接アクセスするための出口



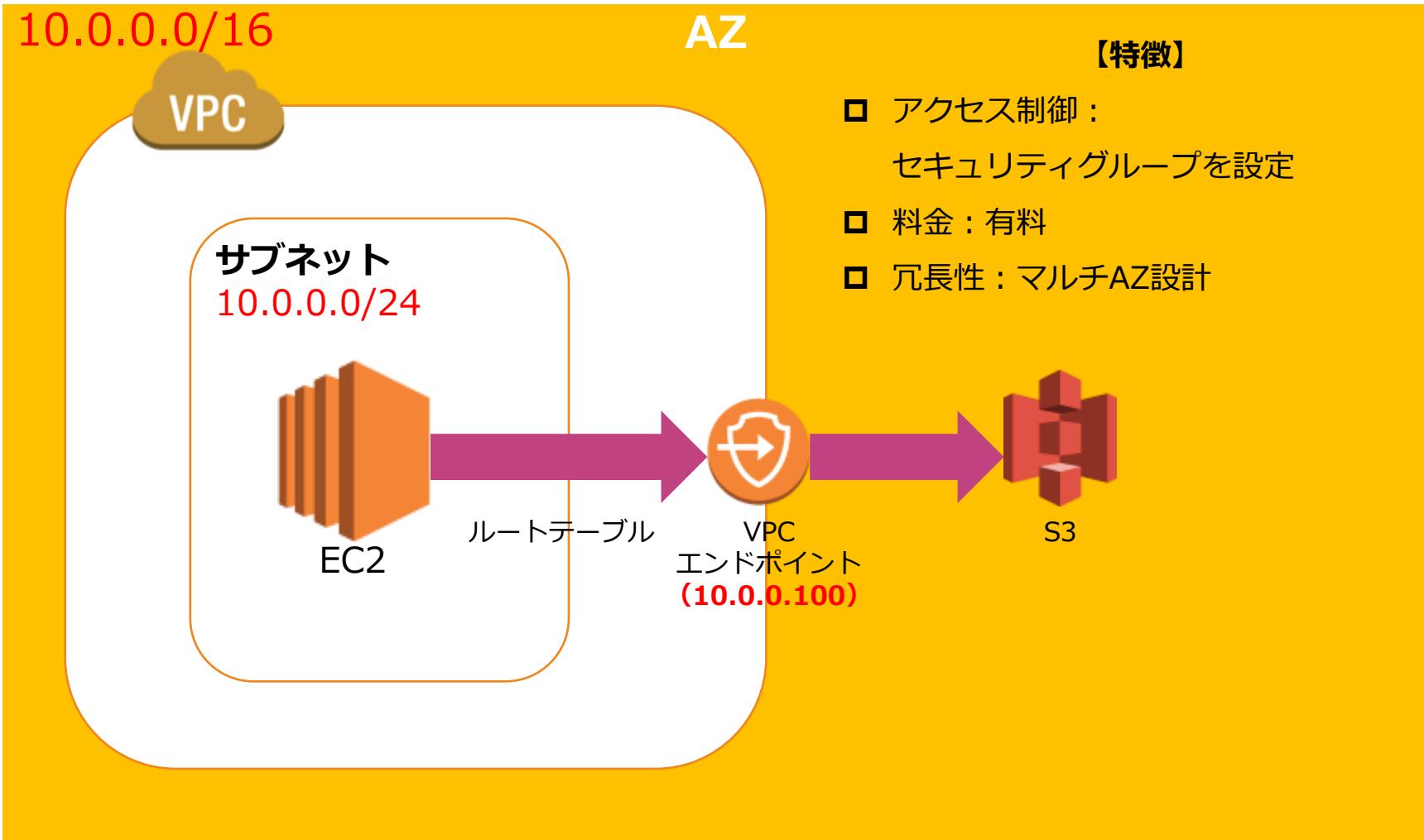
VPCエンドポイント

Gateway型はサブネットに特殊なルーティングを設定し、VPC 内部から直接外のサービスと通信する



VPCエンドポイント

PrivateLink型はサブネットにエンドポイント用のプライベートIPアドレスを生成し、DNSが名前解決でルーティングする



NATゲートウェイ

NATゲートウェイによりプライベートサブネットのリソースがインターネットまたはAWSクラウドと通信が可能になる



【特徴】

- AWSによるマネージドNATサービス
- EIPの割り当て可能
- 最大10Gbpsの高パフォーマンス
- ビルトインで冗長化されている高可用性
- アベイラビリティゾーン毎に設置する

VPC Flow logs

VPC Flow Logsはネットワークトラフィックを取得し
CloudWatchでモニタリングできるようにする機能

- ネットワークインターフェースを送信元/ 送信先とするトラフィックが対象
- セキュリティグループとネットワークACLのルールでaccepted/rejectされたトラフィックログを取得
- キャプチャウインドウと言われる時間枠 (約10分間)で収集・プロセッシング・保存する
- RDS、Redshift、ElasticCache、WorkSpacesのネットワークインターフェーストラフィックも取得可能
- 追加料金はなし

VPCの設定上限

VPCの各種設定においては上限数があるため、大規模に利用する場合は考慮する必要がある

リソース	数
リージョン当たりのVPCの上限数	5
VPC当たりのサブネットの上限数	200
AWSアカウント当たりの1 リージョン内のElasticIP数	5
ルートテーブル当たりのルート上限数	100
VPC当たりのセキュリティグループの上限数	500
セキュリティグループ当たりのルールの上限数	50

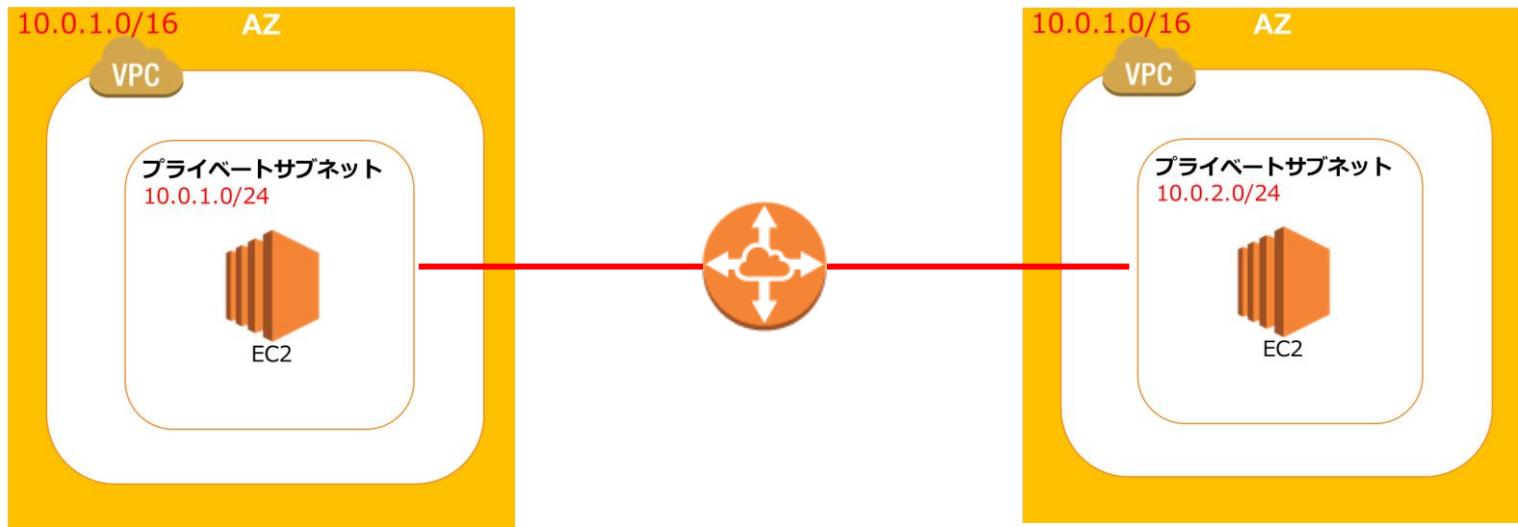
VPCを分割するケース

アプリサービスや組織構成などの用途に応じてVPCを分割する

- アプリケーションによる分割
- 監査のスコープによる分割
- リスクレベルによる分割
- 本番/検証/開発フェーズによる分割
- 部署による分割 共通サービスの切り出し

VPC Peering

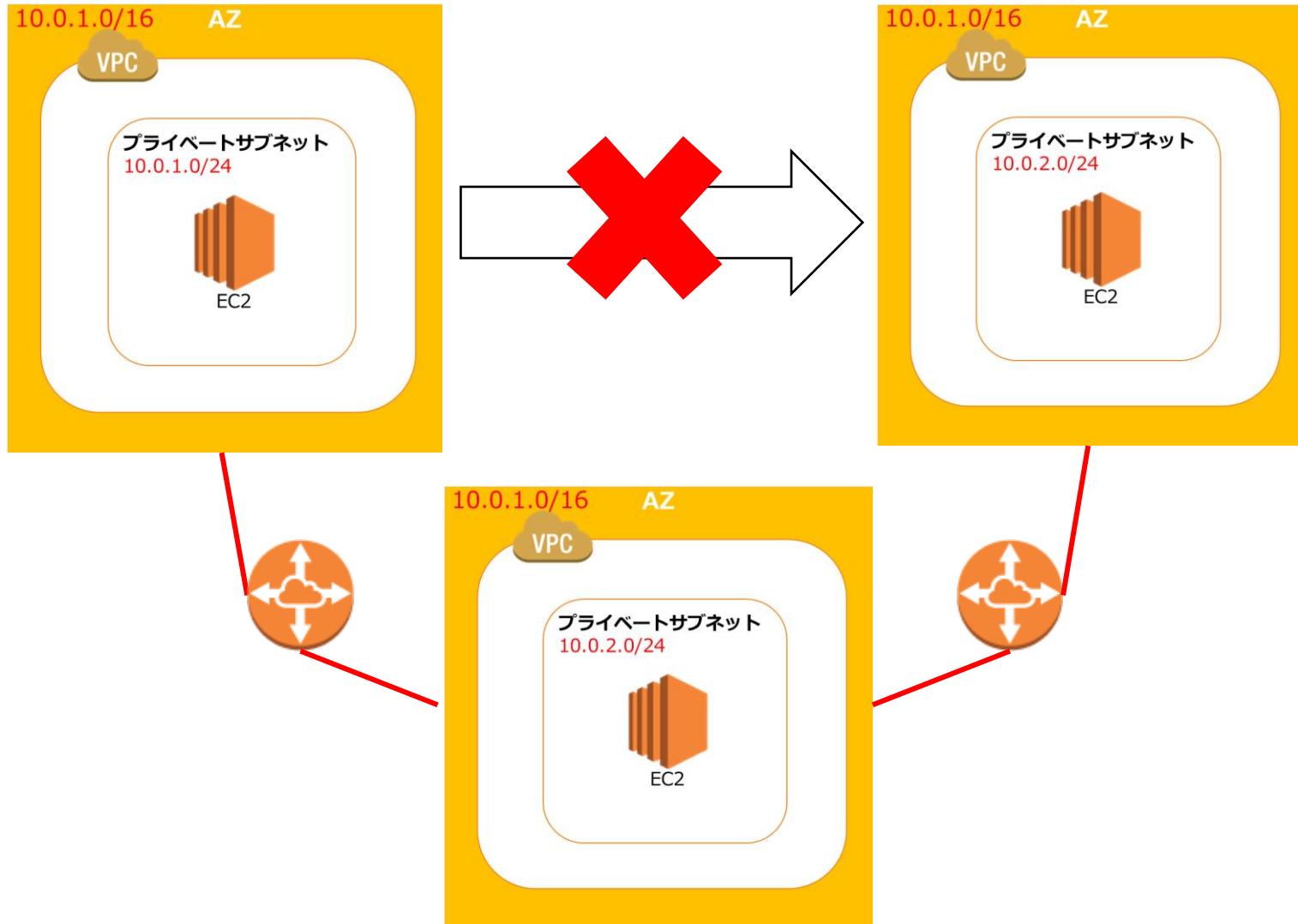
VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



- 異なるAWSアカウント間のVPC間をピア接続可能
- 一部のリージョン間の異なるVPC間のピア接続も可能
- 単一障害点や帯域幅のボトルネックは存在しない

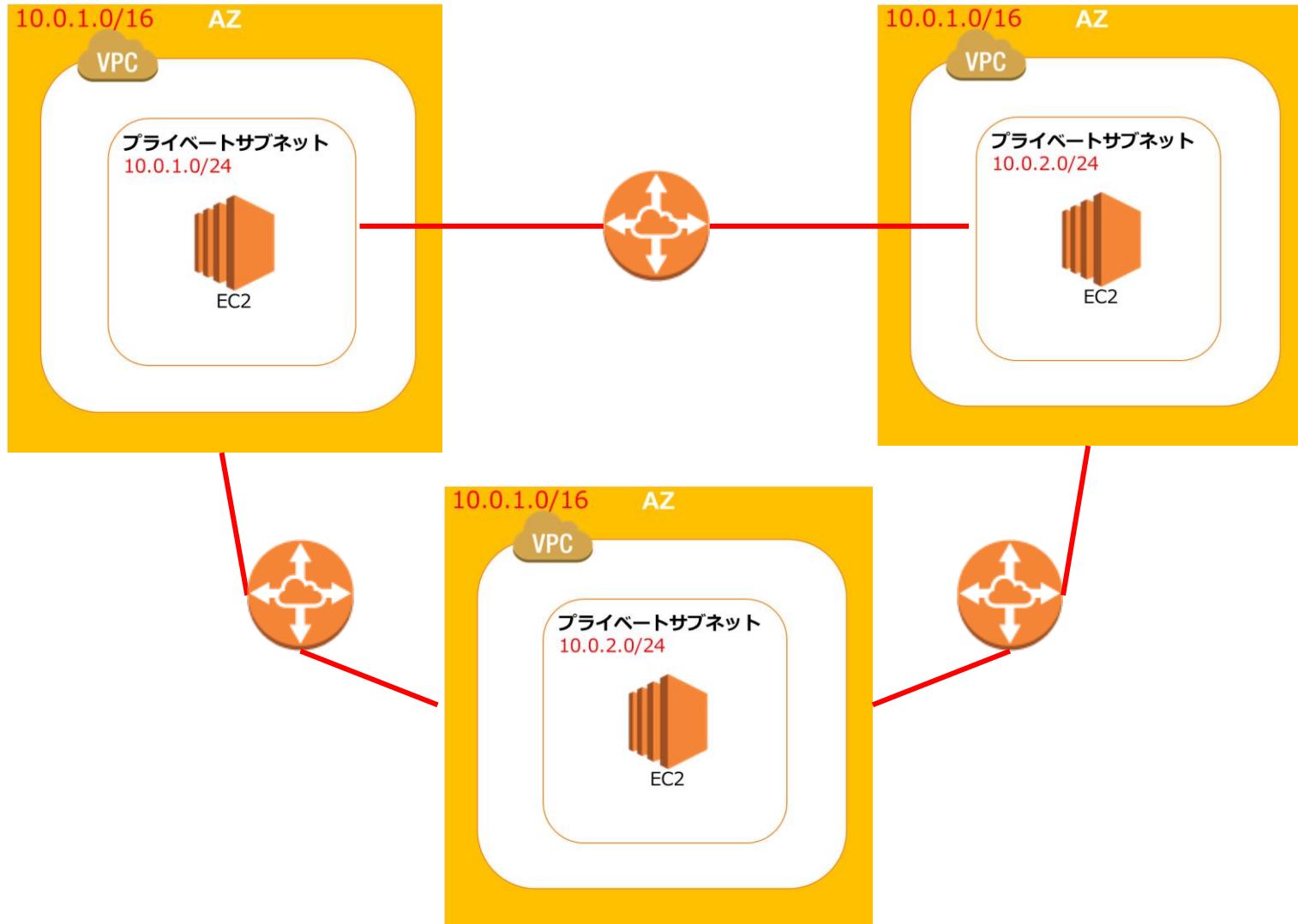
VPC Peering

VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



VPC Peering

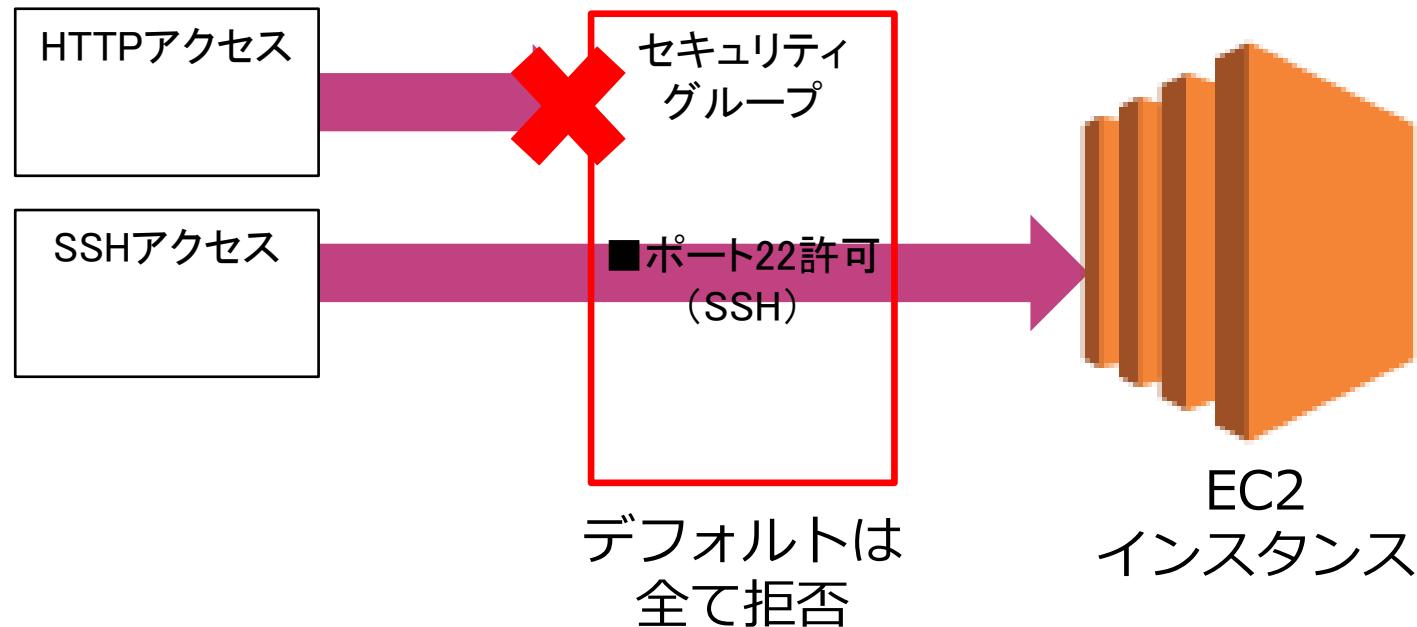
VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



セキュリティグループと ネットワークACL

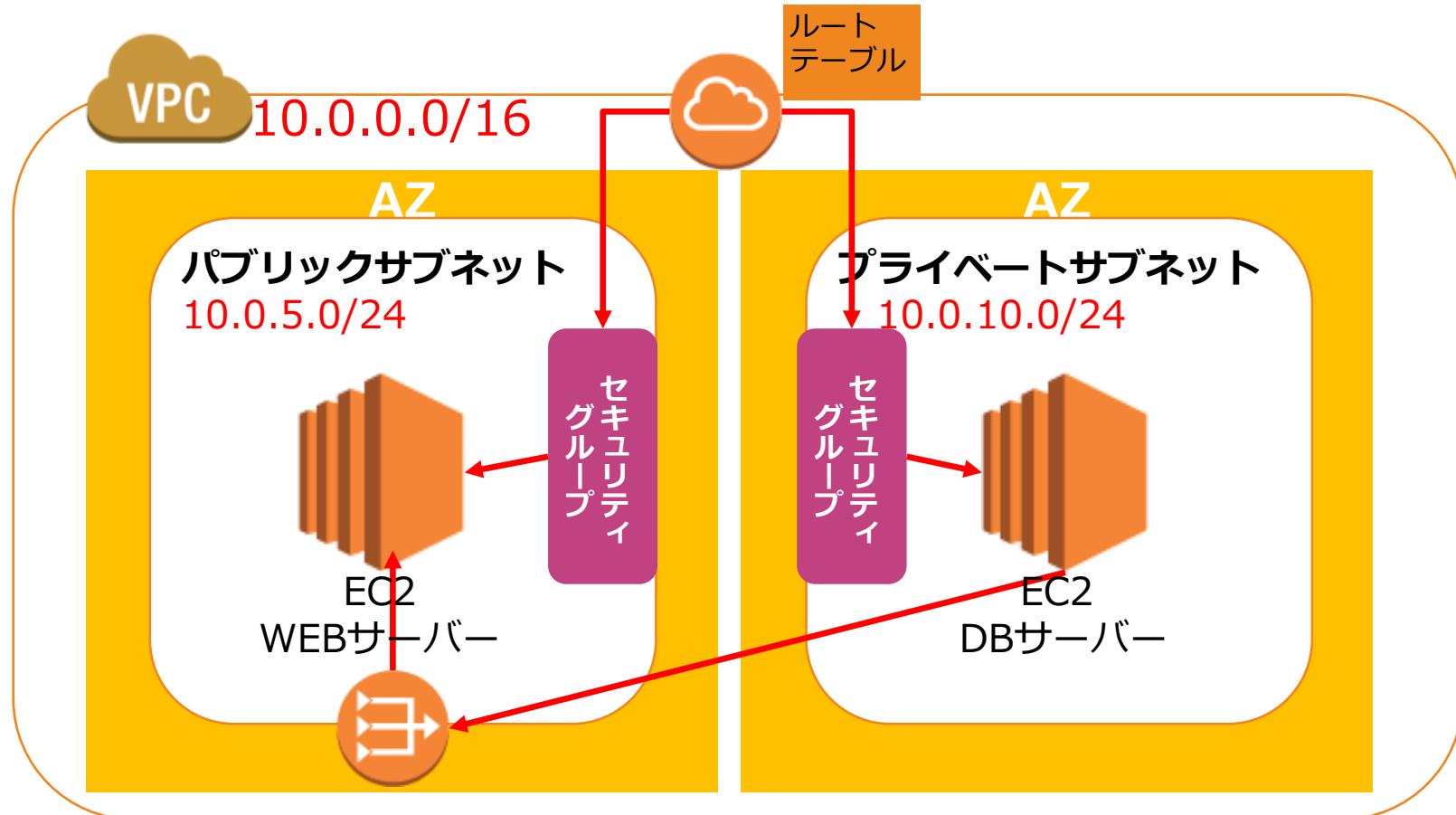
セキュリティグループ

インスタンスへのトラフィックのアクセス可否を設定するファイアーウォール機能を提供



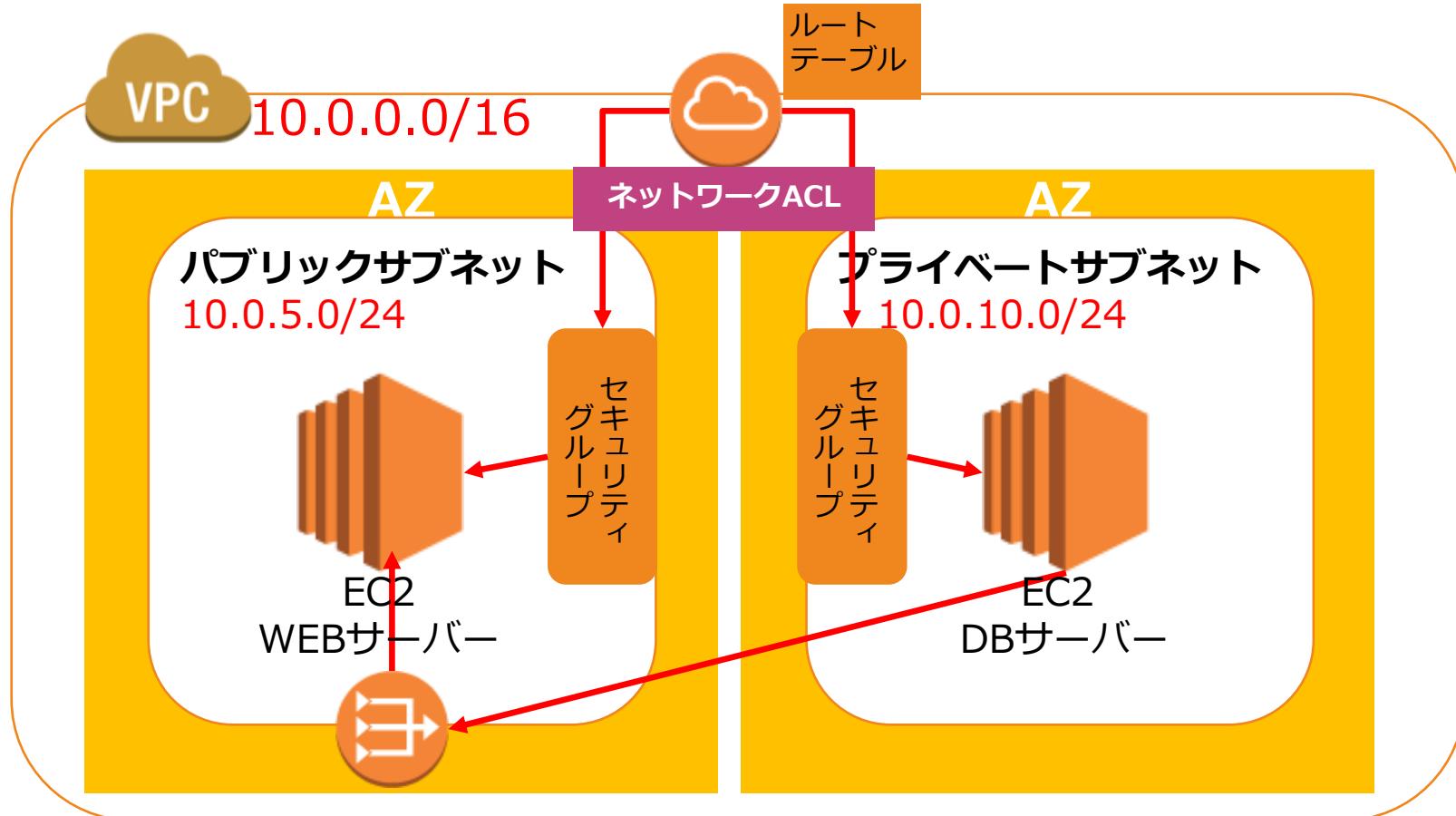
セキュリティグループ

EC2インスタンスに対するトラフィック制御を実施するファイアウォール機能を提供



ネットワークACL

サブネットに対するトラフィック制御を実施する



セキュリティグループとネットワークACL

トラフィック設定はセキュリティグループまたはネットワークACLを利用する

セキュリティグループ設定

- サーバー単位で適用
- ステートフル：インバウンドのみ設定すればアウトバウンドも許可される。（状態を維持）
- 許可のみをIn/outで指定
- デフォルトでは同じセキュリティグループ内通信のみ許可
- 全てのルールを適用

ネットワークACLs設定

- VPC／サブネット単位で適用
- ステートレス：インバウンド設定だけではアウトバウンドは許可されない。
- 許可と拒否をIn/outで指定
- デフォルトでは全ての通信を許可する設定
- 番号の順序通りに適用

Route53の概要

IPアドレスとURL

人が読みやすいURLに変換して、住所として利用している。

`https://134.128.24.16`



<https://www.mercari.com/jp/>

IPアドレスとURL

Domain Name SystemサーバーはURLとIPアドレスの対応関係を管理し、変換する



DNSサーバー

IPアドレスとURL

リクエストとレスポンスがWEBアプリケーションの基本の動き

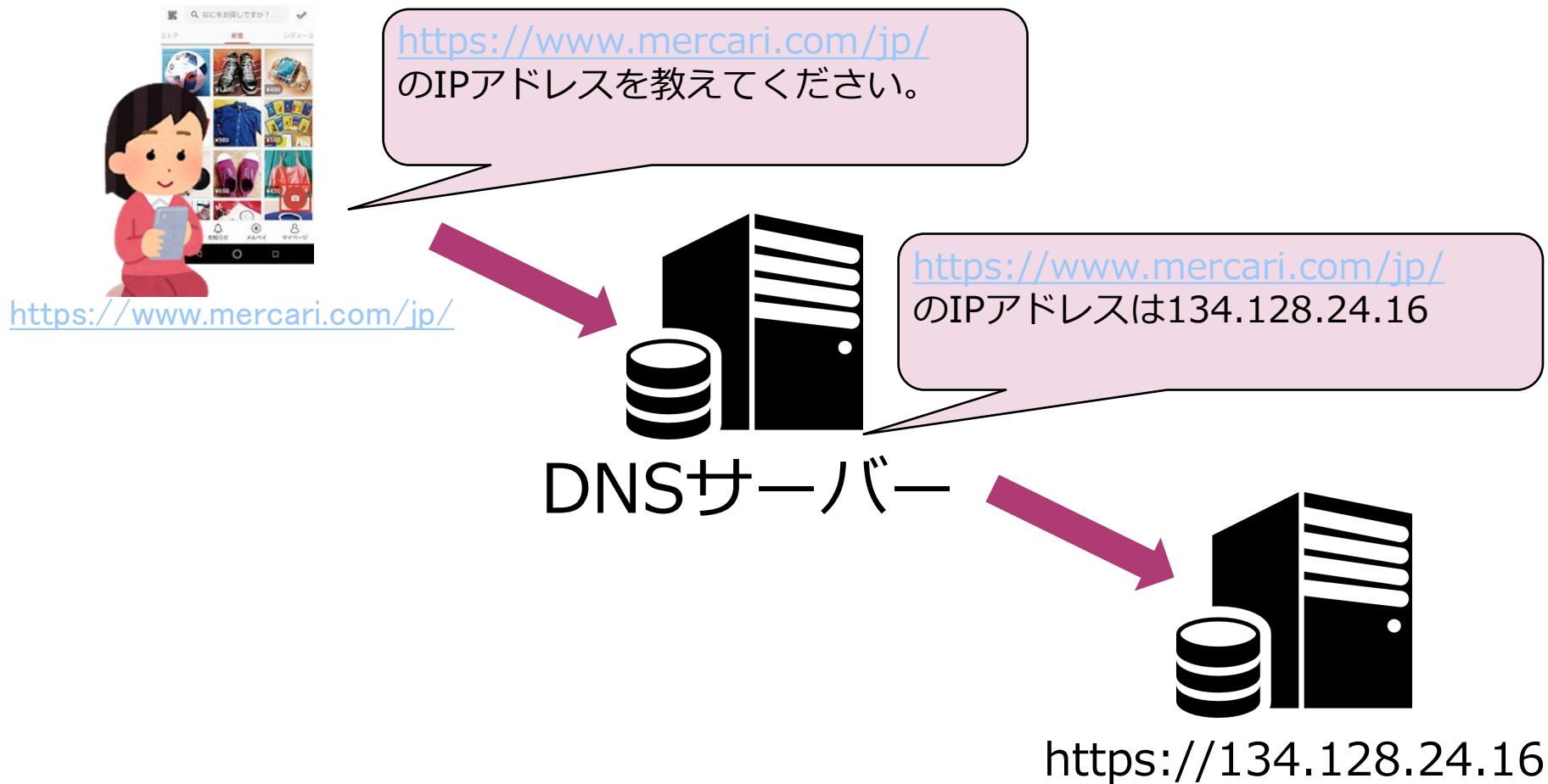


メルカリサーバー



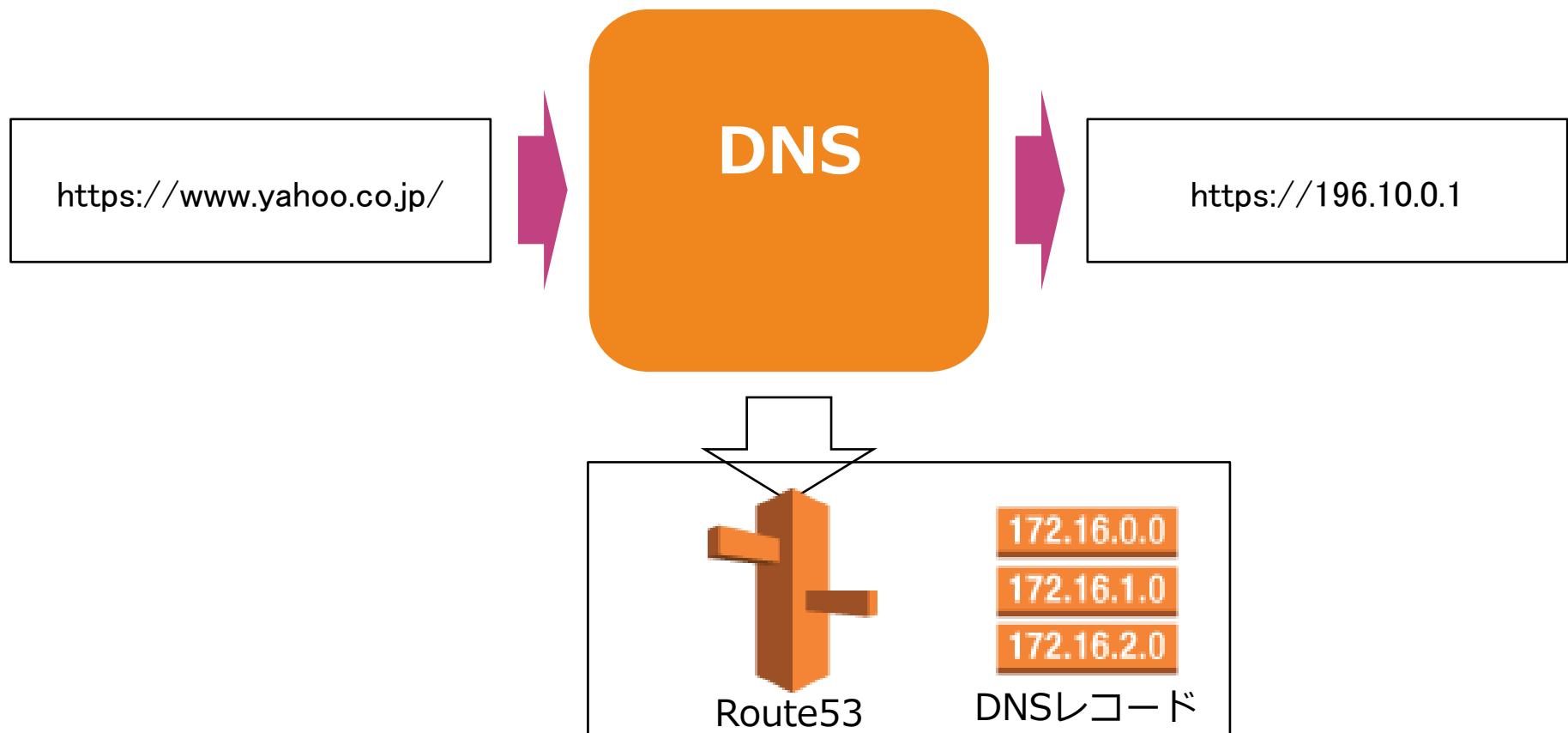
IPアドレスとURL

リクエストを送信する際にDNSサーバーにURLのIPアドレスを確認して、送信先を特定する。



Route53

DNSレコードというIPアドレスとURLを紐づけた表を確認してルーティングする



Route53

Route53は権威DNSサーバーの機能をマネジメント型で簡単に利用できるサービス

- 主要機能はドメイン登録／DNSルーティング／ヘルスチェックの3つ
- ポリシーによるルーティング設定
 - トラフィックルーティング／フェイルオーバー／トラフィックフローに基づく様々な条件のルーティング設定が可能
- AWS側で100%可用性を保証するSLA
- マネージドサービスとして提供しており、ユーザー側で冗長性などを考慮する必要がない

ホストゾーン

ドメイン (example.com) とそのサブドメイン (sub.example.com) のトラフィックのルーティングする方法についての情報を保持するコンテナ

パブリックホストゾーン

- インターネット上に公開されたDNSドメインレコードを管理するコンテナ
- インターネットのDNSドメインに対するトラフィックのルーティング方法を定義

プライベートホストゾーン

- VPCに閉じたプライベートネットワーク内のDNSドメインのレコードを管理するコンテナ
- VPC内のDNSドメインに対して、どのようにトラフィックをルーティングするかを定義
- 1つのプライベートホストゾーンで複数VPCに対応
- VPCが相互アクセス可能であれば複数リージョンのVPCでも、同じホストゾーンを利用可能

トラフィックルーティングのタイプ

様々なルーティング方式を選択して設計することが可能

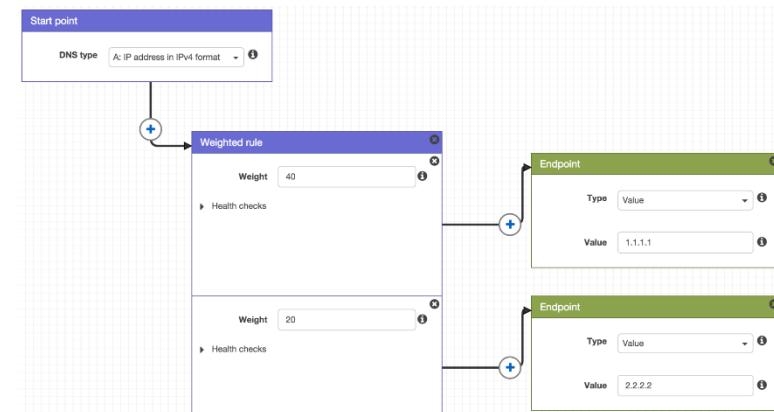
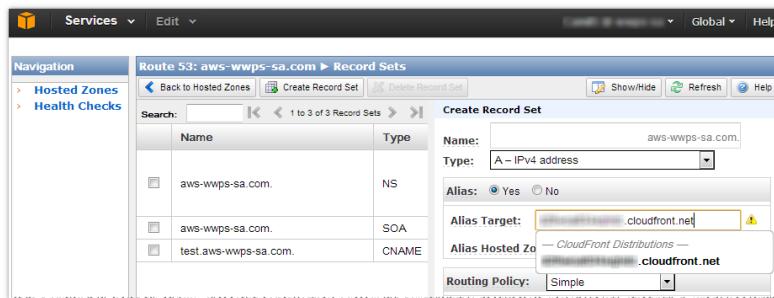
シンプルルーティング (Simple)	<ul style="list-style-type: none">□ レコードセットで事前に設定された値のみに基づいてDNSクエリに応答する□ 静的なマッピングによりルーティングを決定
加重ルーティング (Weighted)	<ul style="list-style-type: none">□ 複数エンドポイント毎の重み設定によりDNSクエリに応答する□ 重み付けの高いエンドポイントに多くルーティングする
レイテンシーグルーティング (Latency)	<ul style="list-style-type: none">□ リージョンの遅延によりDNSクエリに応答する□ リージョン間の遅延が少ない方へルーティングされる
フェイルオーバールーティング (Failover)	<ul style="list-style-type: none">□ ヘルスチェックの結果に基づいて、利用可能なリソースをDNSクエリに応答する□ 利用可能なリソースにのみルーティングされる
位置情報ルーティング (Geolocation)	<ul style="list-style-type: none">□ クライアントの位置情報に基づきDNSクエリに応答する□ 特定の地域・国からのDNSクエリに対して、特定のアドレスを応答
マルチバリュールーティング (Multivalue)	<ul style="list-style-type: none">□ 別々のレコードにIPアドレスを設定する□ IPアドレス単位でヘルスチェックを実施してルーティングする

トラフィックフロー

従来はALIASレコードを駆使して、複雑なルーティングポリシーを作成していたが、トラフィックフローによる視覚的なフローでの複雑なポリシー設定が可能となった

ルートレコードセット画面で
ルーティングポリシーを設定

トラフィックフローで
ルーティングポリシーを設定



セクションの内容

レクチャー	レクチャーで学ぶ内容
AWSアーキテクチャの設計原則	AWSの設計原則であるWell-Architected Frameworkについて学習します。
Well-Architected Toolの確認	AWSのWell-Architected Toolを実際に利用して、活用方法を確認します。
ELBの概要	ELBによってトラフィック分散する仕組みや、その特徴について学習します。
AutoScalingの概要	EC2インスタンスを自動拡張するAutoScalingの特徴を学習します。
ELBとAutoScalingによる冗長構成の構築	ELBを利用してEC2インスタンスのターゲットグループに対して、AutoScalingを設定した冗長構成を構築します。

AWSアーキテクチャ の設計原則

6つの設計原則

Well-Architected Frameworkは次の5つの原則で構成される。

5つの設計原則

回復性の高いアーキテクチャを設計する

→ Reliability

パフォーマンスに優れたアーキテクチャを定義する

→ Performance Efficiency

セキュアなアプリケーションおよびアーキテクチャを規定する

→ Security

コスト最適化アーキテクチャを設計する

→ Cost Optimization

オペレーションエクセレンスを備えたアーキテクチャを定義する

→ Operational Excellence

持続可能性が高いアプリケーション運用を実施する

→ Sustainability

サステイナビリティの追加

2021年12月に初の変更点として6つ目の柱であるサステイナビリティを追加

Reliability
信頼性

Performance
Efficiency
パフォーマンス
効率

Security
安全性

Cost
Optimization
コスト最適化

Operational
Excellence
運用上の
優秀性

Sustainability
持続可能性

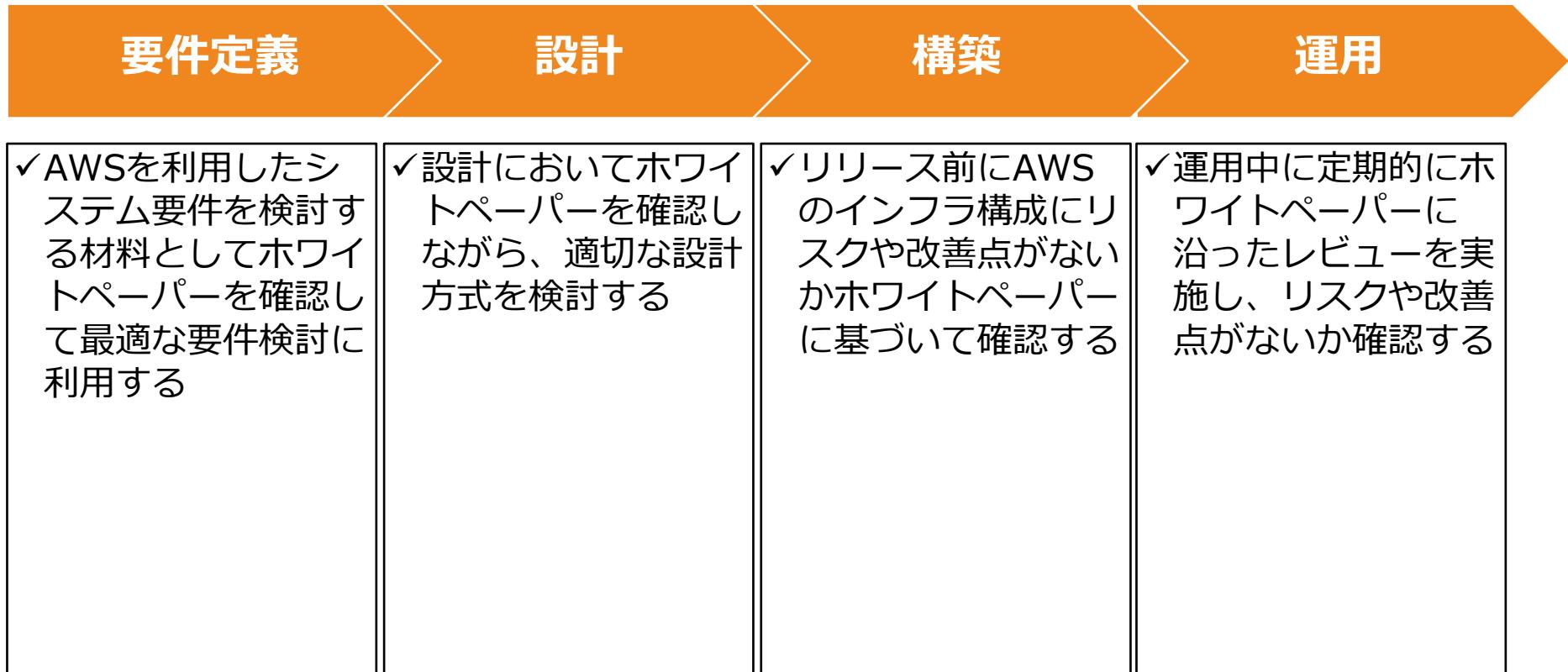
Well-Architected Framework

Well-Architected Frameworkは次の3つの内容で構成される



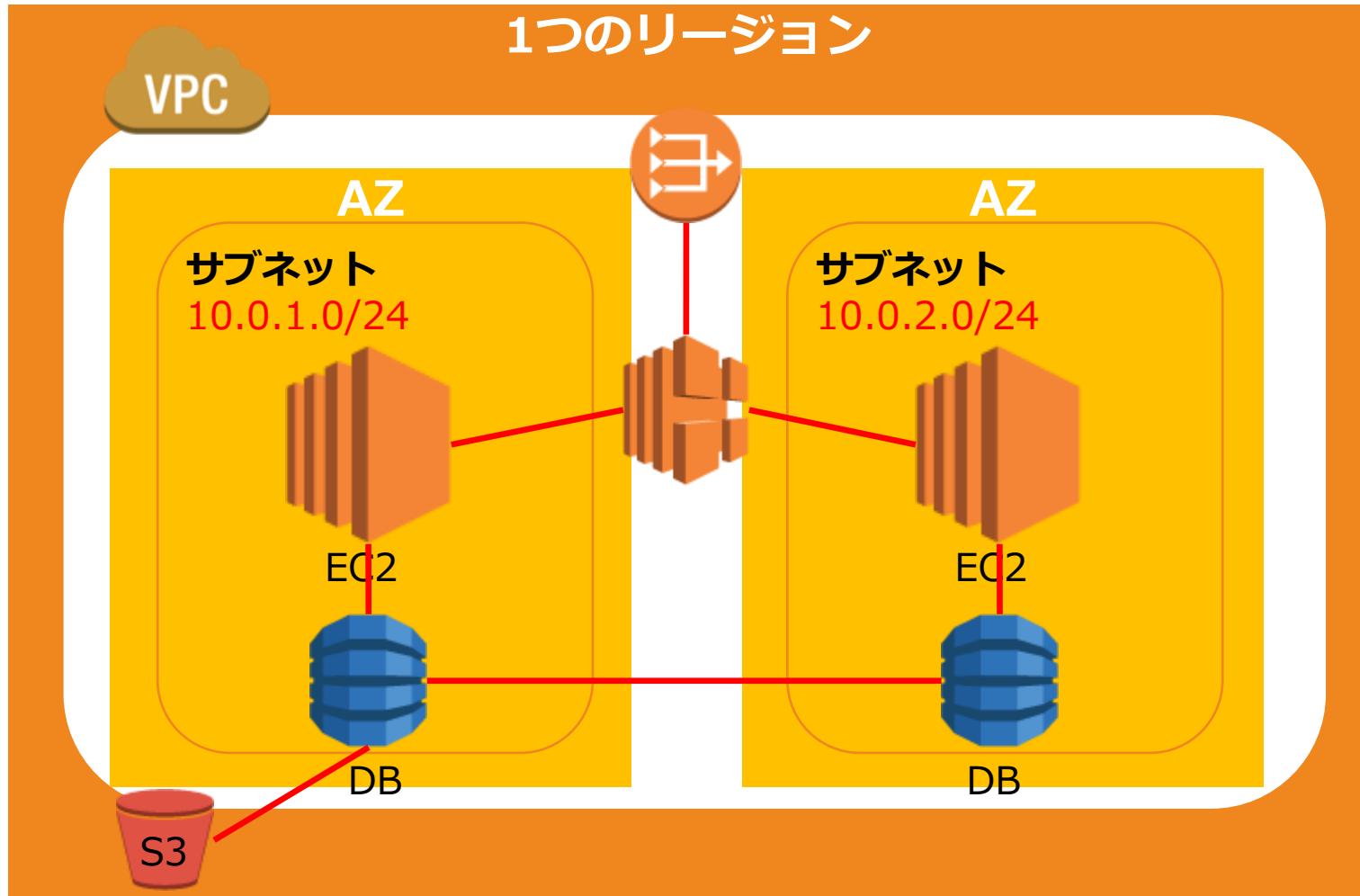
Well-Architected Framework

ベストプラクティスを利用してすることで最適解や改善点を把握する。あくまで参考であり絶対というものではない。



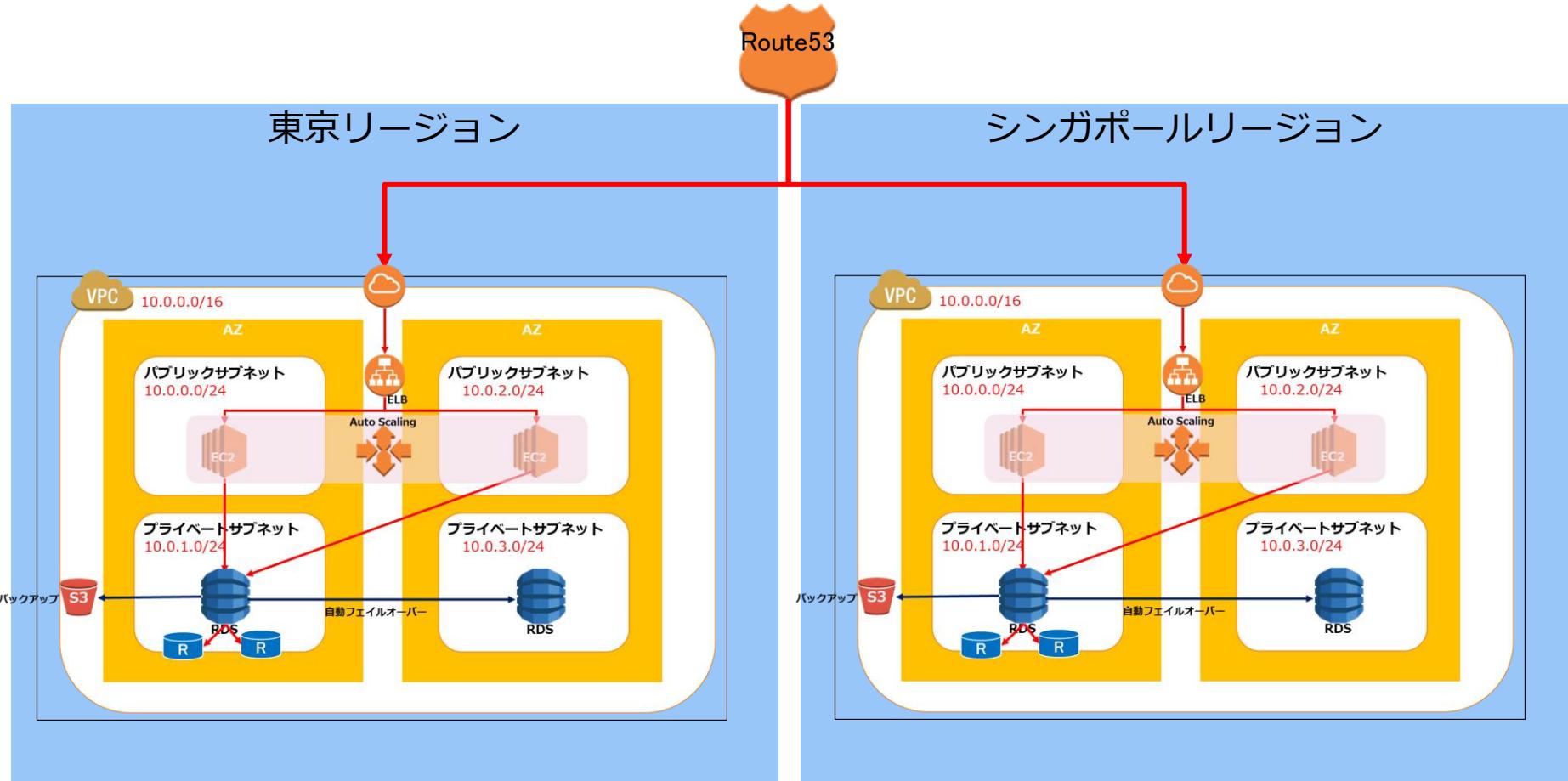
マルチAZ構成

マルチAZにサーバーやDBの冗長構成を確立させることで高い可用性を実現する



マルチリージョン構成

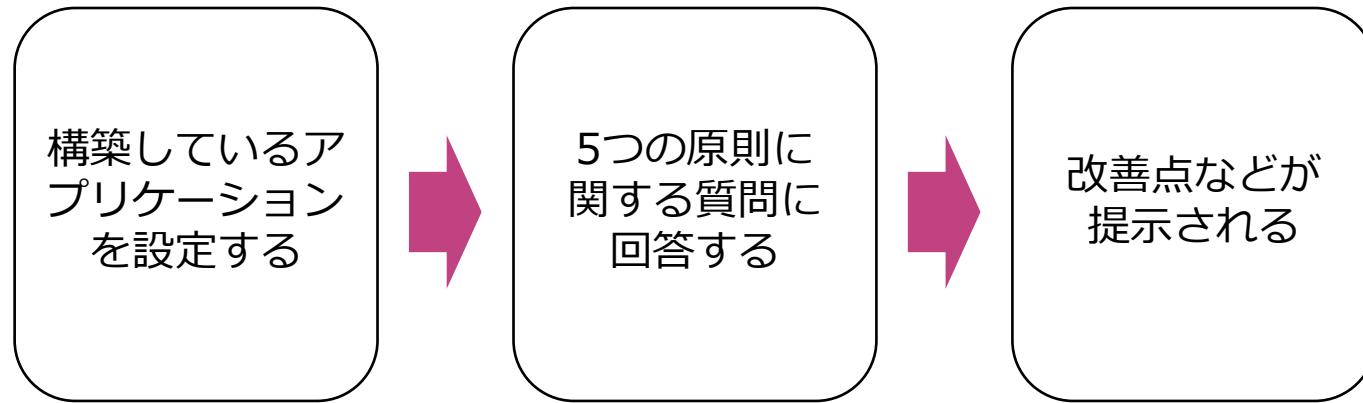
Route53を介して、2つの同じシステム構成をフェイルオーバーすることが可能



Well-Architected Toolの確認

Well-Architected Toolの利用方法

Well-Architected Toolは構築中または運用中のアプリケーションがベストプラクティスに沿っているかを検証できるツール



Well-Architected Toolの定義

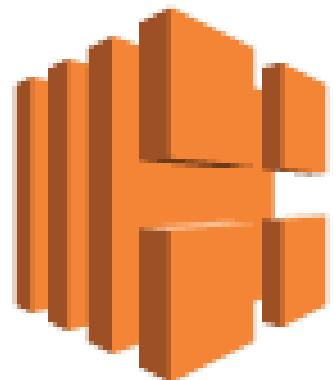
Well-Architected Toolの独特的な用語を理解して、利用していく

ワークロード	ウェブサイト、ECサイト、モバイルアプリのバックエンド、分析プラットフォームなどビジネス価値をもたらす一連のコンポーネントが特定する。
マイルストーン	設計、テスト、実稼働、本稼働の製品ライフサイクルを通して進歩するアーキテクチャでの重要な変更内容のこと
レンズ	ベストプラクティスに照らしてアーキテクチャを評価し、改善すべき分野を特定する一貫した方法
高リスクの問題 (HRI)	ビジネスに重大な悪影響を及ぼす可能性があるアーキテクチャおよび運用上の問題
中リスクの問題 (MRI)	その程度は HRI より低いビジネス上の問題

ELBの概要

ELB (Elastic Load Balancing)

マネージド型のロードバランシングサービスで、EC2インスタンスの処理を分散する際に標準的に利用する



ELB (Elastic Load Balancing)

マネージド型のロードバランシングサービスで、EC2インスタンスの処理を分散する際に標準的に利用する

- インスタンス間の負荷を分散する
- 異常なインスタンスを認識して対応する
- パブリック／プライベートどちらでも使用可能
- ELB自体も負荷に応じてキャパシティを自動増減するスケーリングを実施
- 従量課金で利用可能
- マネージドサービスなので管理が不要
- Auto Scaling, Route 53, Cloud Formationなどと連携

ELBの主要機能

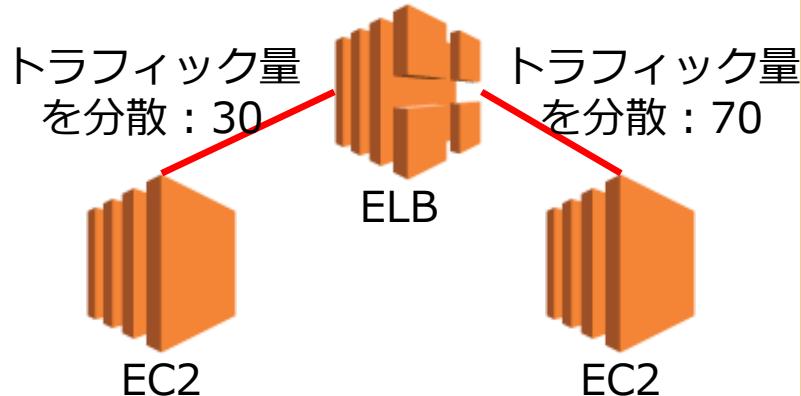
ヘルスチェック	EC2インスタンスの正常／異常を確認し、利用するEC2の振り分けを行う
負荷分散	配下のEC2の負荷に応じて、複数のAZに跨るEC2インスタンスの負荷分散を行う
SSLサポート	ELBでSSL Terminationできる
ステイッキー セッション	セッション中に同じユーザから来たリクエストを全て同じEC2インスタンスに送信する
Connection Draining	インスタンスが登録解除されるか異常が発生した場合に、そのバックエンドインスタンスへの新規リクエスト送信を中止する
S3へのログ保管	ELBのアクセスログを指定したS3に自動保管

ELBの主要機能

負荷分散によるスケーラビリティとヘルスチェックによる高可用性を実現

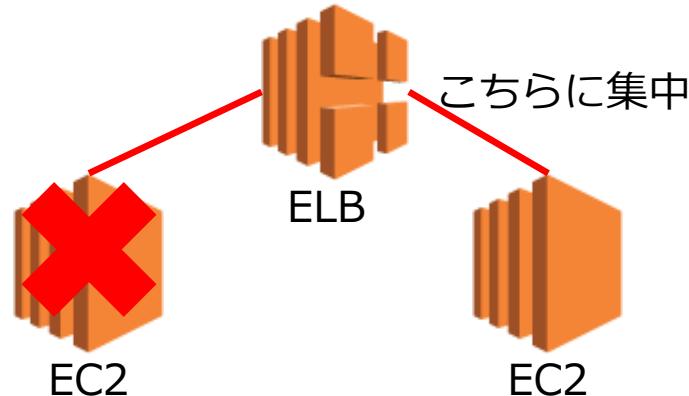
スケーラビリティの確保

複数のEC2インスタンス/ECS Serviceへの負荷分散



高可用性

複数のアベイラビリティゾーンにある複数のEC2インスタンスの中から正常なターゲットにのみ振り分け

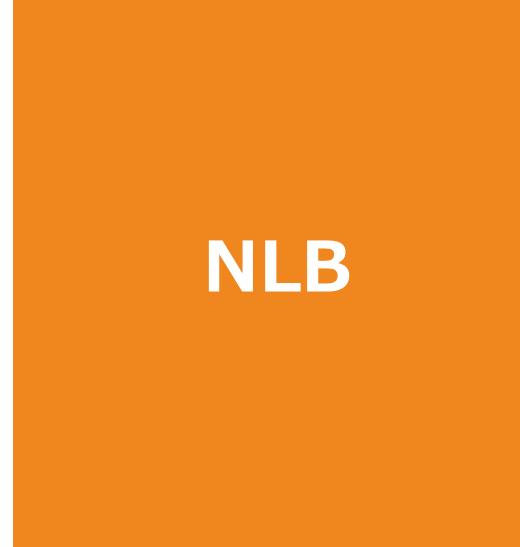


ELBのタイプ

現在利用できるロードバランサーは3タイプで用途に応じて使い分ける

A solid orange square containing the text "ALB" in white.

ALB

A solid orange square containing the text "NLB" in white.

NLB

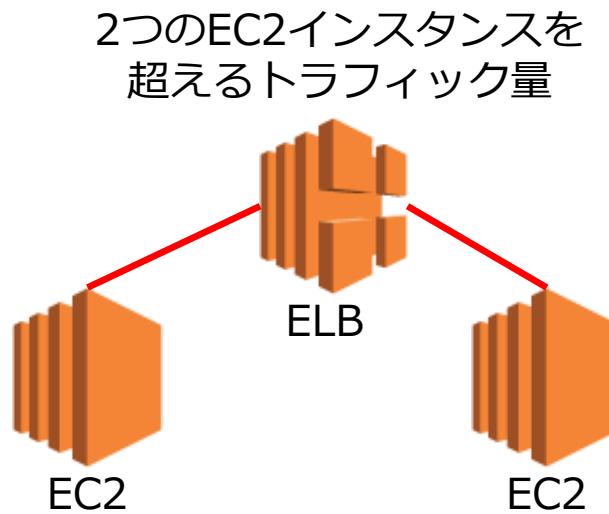
A solid orange square containing the text "CLB" in white.

CLB

Auto-Scalingの概要

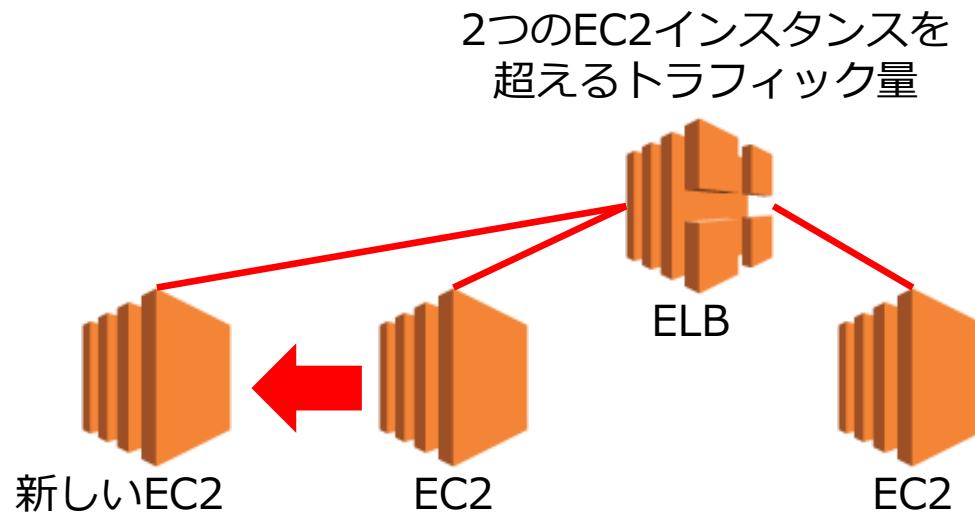
スケーラビリティの確保

需要増にトラフィック量が処理できなくなる前に、処理サーバーを拡張することで対処する必要がある



スケーラビリティの確保

需要増にトラフィック量が処理できなくなる前に、処理サーバーを拡張することで対処する必要がある



スケーリングのタイプ

スケーリングタイプは垂直スケーリングと水平スケーリングの2タイプ。Auto-scalingは水平スケーリング

垂直スケーリング

水平スケーリング

【拡張方法】

スケールアップ：メモリやCPUの追加・増強

【拡張方法】

スケールアウト：処理する機器／サーバー台数を増加する

【低減方法】

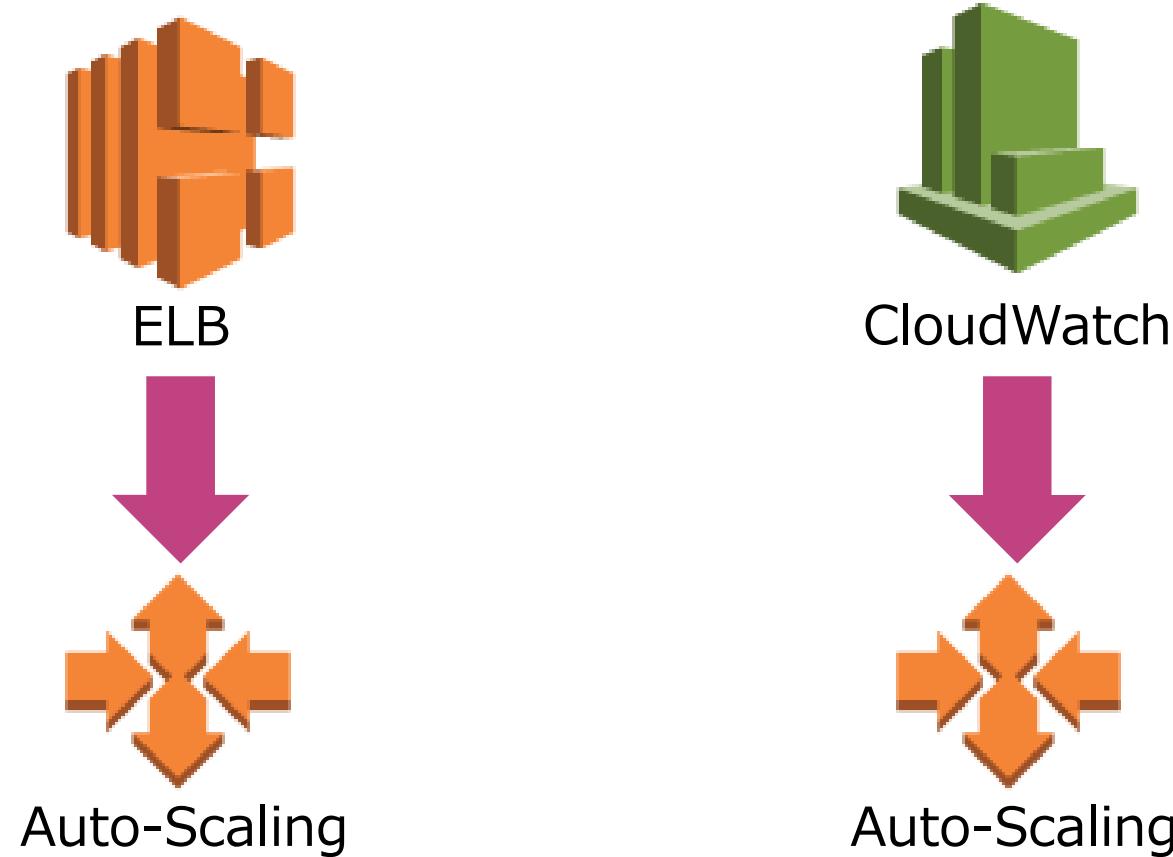
スケールダウン：メモリやCPUの削減・低性能化

【低減方法】

スケールイン：処理する機器／サーバー台数を低減する

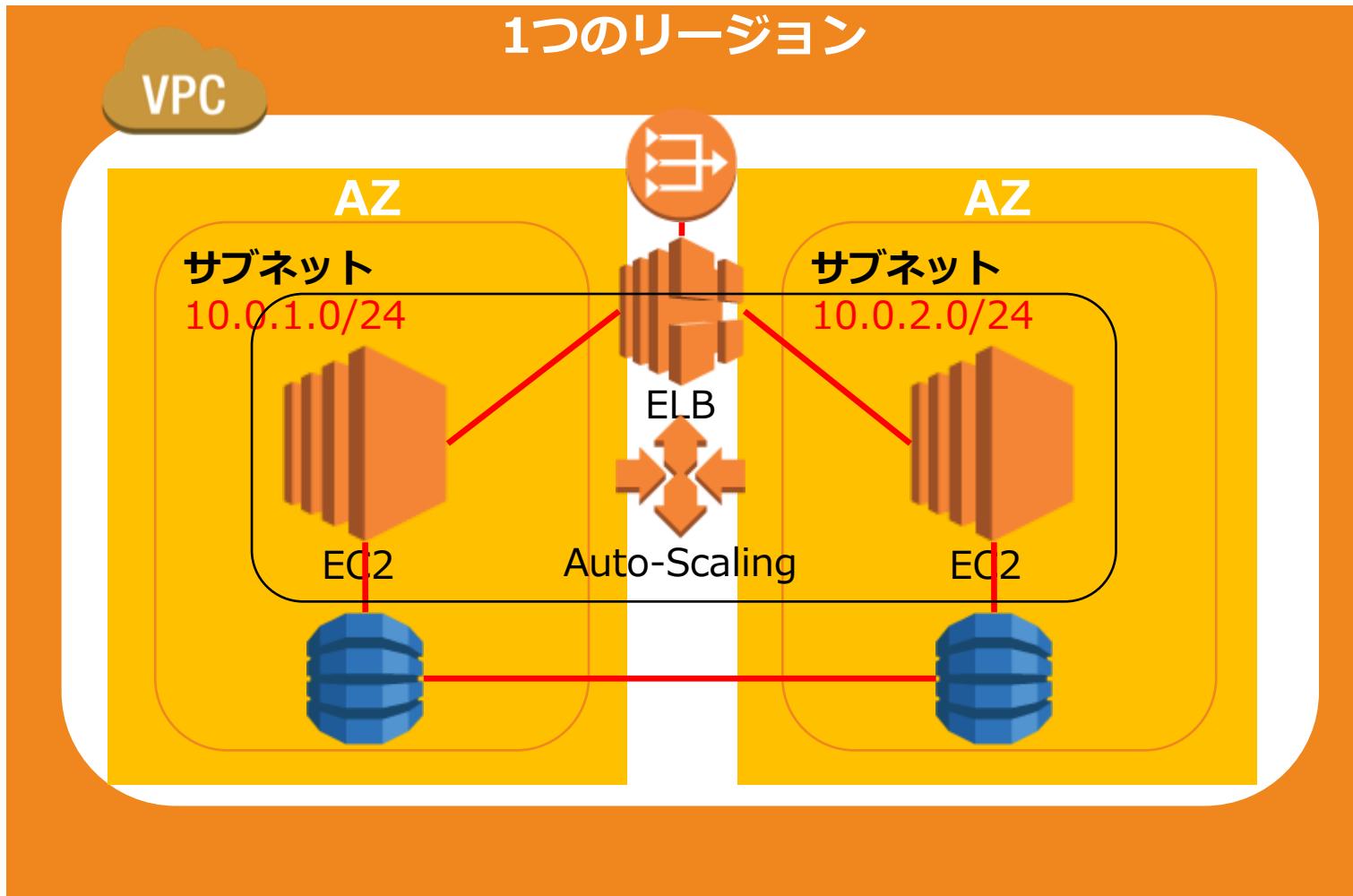
連携

ELBのヘルスチェックやCloudWatchのアラート機能をトリガーとして利用できる



基本アーキテクチャー

ELB構成で冗長化した上でAuto-Scalingを設定して自動拡張できるようにする



セクションの内容

レクチャー	レクチャーで学ぶ内容
S3の概要	AWSの主要ストレージサービスであるS3の特徴や機能について学習します。
S3の作成	S3バケットを作成して、データ保存方法を確認しつつ、その他の機能を確認します。
データベースの基礎	データベースの基本的な仕組みについて基礎的な内容を学習します。
RDSの概要	AWSの主要なリレーショナルデータベースサービスであるRDSの特徴や機能について学習します。
RDSの構築	RDSを利用したMySQLデータベースを実際に作成して、そのSQL操作を実施します。

S3の概要



AWSストレージサービス

AWSは3つの形式のストレージサービスを提供

ブロックストレージ

- ✓ EC2にアタッチして活用するディスクサービス
- ✓ ブロック形式でデータを保存
- ✓ 高速・広帯域幅
- ✓ 例：EBS、インスタンスストア

オブジェクトストレージ

- ✓ 安価かつ高い耐久性をもつオンラインストレージ
- ✓ オブジェクト形式でデータを保存
- ✓ 例：**S3**、Glacier

ファイルストレージ

- ✓ 複数のEC2インスタンスから同時にアタッチ可能な共有ストレージサービス
- ✓ ファイル形式でデータを保存
- ✓ 例：EFS



Simple Storage Service (S3)

ユーザがデータを容量制限なく保存可能なマネージド型で提供されるオブジェクト型ストレージ

特徴

- 高い耐久性

99.99999999%

- 安価なストレージ

容量単価:月額1GB / 約2.5円

- スケーラブルで安定した性能

データは冗長化されて保存されデータ容量に依存しない性能がAWS側で保証される

- 暗号化

転送中や保存時にデータを暗号化可能

データ保存形式

- バケット

オブジェクトの保存場所。名前はグローバルでユニークな必要あり

- オブジェクト

S3に格納されるファイルでURLが付与される。バケット内オブジェクト数は無制限

- データサイズ

データサイズは0KBから5TBまで保存可能



S3のオブジェクト構成

S3のオブジェクトは以下のような要素で構成されている

■Key

オブジェクトの名前であり、バケット内のオブジェクトは一意に識別する

■Value

データそのものであり、バイト値で構成される

■バージョンID

バージョン管理に用いるID

■メタデータ

オブジェクトに付随する属性の情報

■サブリソース

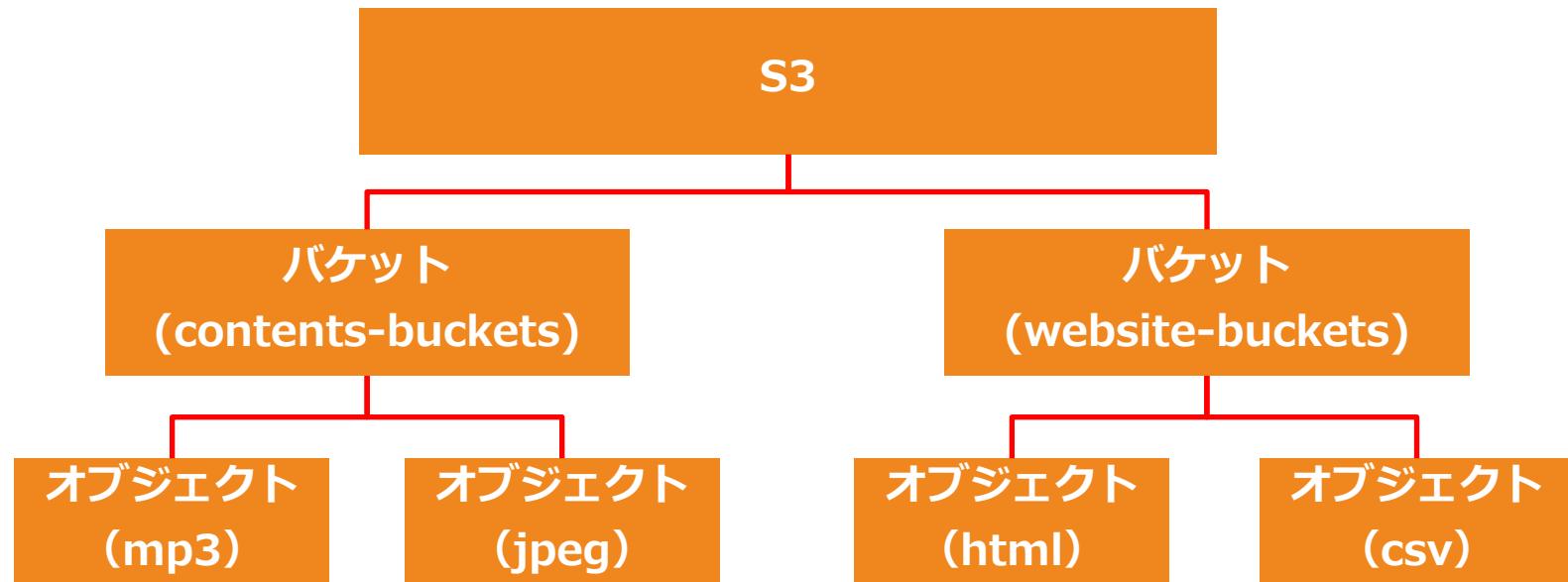
バケット構成情報を保存および管理するためのサポートを提供

例：アクセス制御リスト（ACL）



S3のデータ構造

S3はバケット単位で保存スペースを区分し、オブジェクトでデータを格納する



AWSストレージサービス

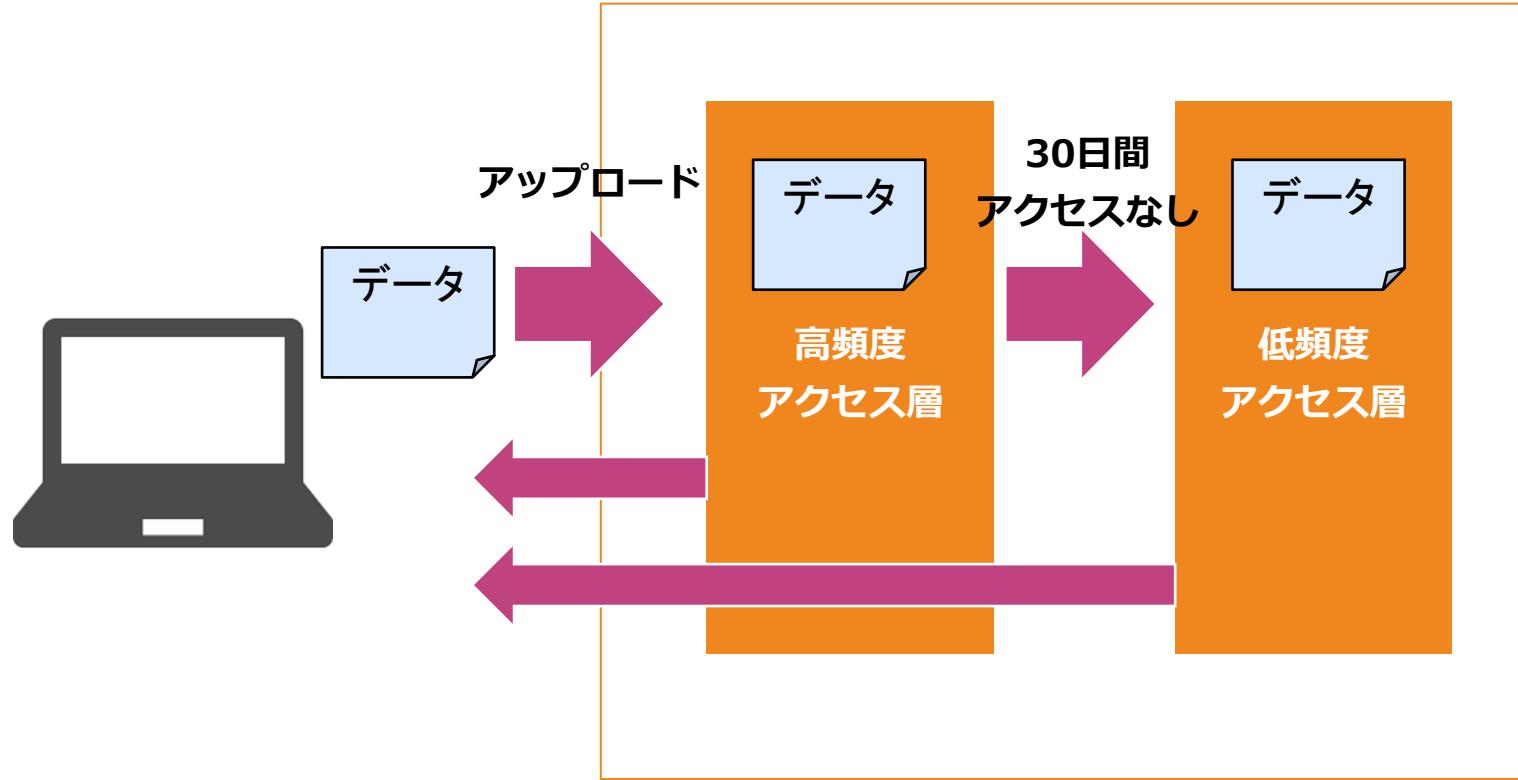
S3の用途に応じてストレージタイプを選択する

タイプ	特徴	性能
STANDARD	✓ 複数個所にデータを複製するため耐久性が非常に高い	■ 耐久性 99.99999999% ■ 可用性 99.99%
STANDARD-IA	✓ スタンダードに比べて安価 ✓ データの読み出し容量に応じた課金	■ 耐久性 99.99999999% ■ 可用性 99.9%
One Zone-IA	✓ アクセス頻度は低いが、必要に応じてすぐに取り出すデータ向け	■ 耐久性 99.99999999% ■ 可用性 99.5%
RRS	✓ Reduced Redundancy Storage 低冗長化ストレージ ✓ Glacierから取り出したデータ配置等	■ 耐久性 99.99% ■ 可用性 99.99%
Amazon Glacier	✓ 最安のアーカイブ用ストレージ ✓ データ抽出にコストと時間（3~5時間）を要する ✓ ライフサイクルマネジメントで指定 ✓ ボールロック機能でデータを保持	■ 耐久性 99.99999999% ■ 可用性 N/A



S3 Intelligent-Tiering

低頻度アクセスのオブジェクトを自動的に低頻度アクセス層に移動することでコストを削減する。



S3（標準）の値段

保存データ容量、データ取得リクエストおよびデータ転送アウトに応じて課金される。

容量当たりの料金	最初の 50 TB/月 0.025USD/GB 次の 450 TB/月 0.024USD/GB 500 TB/月以上 0.023USD/GB
データ取り出しリクエスト料金	PUT、COPY、POST、LIST リクエスト (1,000 リクエストあたり) : 0.0047USD GET、SELECT、他のすべてのリクエスト (1,000 リクエストあたり) : 0.00037USD
データ転送料金	データ転送 (イン)は無料 インターネットへのデータ転送 (アウト) は以下の通り 1 GB まで/月 0.00USD/GB 次の 9.999 TB/月 0.114USD/GB 次の 40 TB/月 0.089USD/GB 次の 100 TB/月 0.086USD/GB 150 TB /月より大きい 0.084USD/GB

※2020年7月あたりの標準ストレージのお値段です。値段は変動する可能性があります。



S3の整合性モデル

S3は高い可用性を実現するため、データ更新・削除には結果整合性モデルを採用。同時書き込みはタイムスタンプ処理を実施

データ処理	整合性モデル
新規登録	<ul style="list-style-type: none">✓ Consistency Read✓ 登録後即時にデータが反映される
更新	<ul style="list-style-type: none">✓ Eventual Consistency Read✓ 更新直後はデータ反映に時間がかかる
削除	<ul style="list-style-type: none">✓ Eventual Consistency Read✓ 削除直後はデータ反映に時間がかかる



S3のアクセス管理

S3のアクセス管理は用途に応じて方式を使い分ける

管理方式	特徴
IAMポリシー	<ul style="list-style-type: none">✓ IAMユーザー／サービスに対してS3サービスへのアクセス権限を設定することができる✓ 一元的にユーザーへのアクセス権限を管理
バケットポリシー	<ul style="list-style-type: none">✓ バケットへのアクセス権をJSONで設定✓ 他アカウントへの許可も可能✓ バケット単位の高度なアクセス管理向け
ACL	<ul style="list-style-type: none">✓ バケットと個々のオブジェクトへのアクセス権限をXMLで設定する✓ 他アカウントへの許可も可能✓ 簡易的にアクセス管理向け
署名付きURL	<ul style="list-style-type: none">✓ AWS SDKで生成した署名付きURLでS3のオブジェクトへの一定時間アクセスを許可



S3のアクセス管理

S3はインターネットからパブリックアクセスの設定が可能

パブリックアクセス (アカウント設定)

パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、アクセスポイントポリシーまたはそのすべてを介して、バケットとオブジェクトに許可されます。すべての S3 バケットおよびオブジェクトへのパブリックアクセスが確実にブロックされるようにするには、[パブリックアクセスをすべてブロック] をオンにします。これらの設定は、現在および将来のすべてのバケットとアクセスポイントに対してアカウント全体に適用されます。AWS は [パブリックアクセスをすべてブロック] をオンにすることをお勧めしますが、これらの設定を適用する前に、アプリケーションがパブリックアクセスなしで正しく機能することをご確認ください。バケットやオブジェクトへのある程度のパブリックアクセスが必要な場合は、特定のストレージユースケースに合わせて以下にある個々の設定をカスタマイズできます。[詳細はこちら](#)

編集

パブリックアクセスをすべてブロック

△ オフ

新しいアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
△ オフ

任意のアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
△ オフ

新規のパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
△ オフ

あらゆるパブリックバケットポリシーまたはアクセスポイントポリシーを介したバケットとオブジェクトへのパブリックアクセスとクロスアカウントアクセスをブロックする
△ オフ



S3の暗号化

S3へのデータ保管時に暗号化形式として以下の4つの形式から選択する

暗号化方式	特徴
SSE-S3	<ul style="list-style-type: none">✓ S3の標準暗号化方式で簡易に利用可能✓ 暗号化キーの作成・管理をS3側で自動で実施✓ ブロック暗号の1つである256ビットのAdvanced Encryption Standard (AES-256) を使用してデータを暗号化
SSE-KMS	<ul style="list-style-type: none">✓ AWS KMSに設定した暗号化キーを利用した暗号化を実施✓ ユーザー側でAWS KMSを利用して暗号化キーを作成・管理することが可能✓ クライアント独自の暗号キーを利用可能
SSE-C	<ul style="list-style-type: none">✓ ユーザーが指定したキーによるサーバー側の暗号化 (SSE-C) を使用することが可能✓ 利用設定や管理が煩雑になるのがデメリット
クライアントサイド 暗号化 (CSE)	<ul style="list-style-type: none">✓ クライアント側の暗号化では、Amazon S3に送信する前にデータを暗号化する方式✓ AWS KMSなどを利用して暗号化キーを作成・実施✓ アプリケーション内に保存したマスターキーを使用



S3アクセスポイント

S3 上の共有データセットを使用するアプリケーションへの大規模なデータアクセス管理を実施



アクセスポイントの作成
アプリケーション向けに
S3バケット内にアクセス
するためのアクセスポイントを作成する。

アクセス制限設定
特定のIPアドレスやウェ
ブサービスにアクセスを
限定するアクセス制限を
設定

VPCアクセス制限設定
VPCに対して特定のS3
バケットへのアクセス制
限を設定する

アクセス管理の実行
アプリケーション向けの
アクセス対象を拡大・制
限するなど容易にコント
ロール可能



S3アクセスアナライザー

アクセスポリシーに沿っているかを確認し、不正なアクセスが発生していないか、アクセスポリシーを監視する機能

- ✓ IAM アクセスアナライザーに連動したS3向けの機能
- ✓ バケットポリシー／ACLのモニタリング
- ✓ パブリックまたは共有バケットアクセスを検出
- ✓ バケットポリシー、バケット ACL、またはその両方。バケットアクセスのソースを検索して確認する場合は、この列の情報をまず使用して、迅速で正確な是正措置を実行する
- ✓ すべてのパブリックバケットと共有バケットの結果を表示する
- ✓ バケットの実際のアクセス状況を確認する。



ライフサイクル管理

バケット内のオブジェクト単位でストレージクラスの変更や削除時期などを設定することで実行を自動化する

設定方法

- バケット全体やPrefixに設定
- オブジェクト更新日を基準にして日単位で指定し、毎日0:00UTCにキューを実行
- 最大1000ルール
- IAに移動できるのは128KB以上のオブジェクト
- MFA Deleteが有効だと設定不可

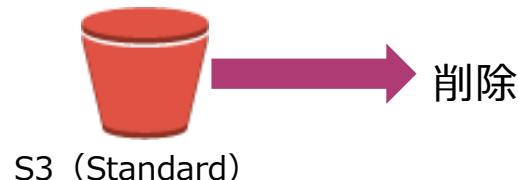
一定期間で自動アーカイブ



一定期間で自動で安価な保存場所へ



一定期間で自動で削除



レプリケーション

リージョン間を跨ぐクロスリージョンレプリケーションにより
耐障害性を高める

レプリケーションのトリガー

- バケットに対するオブジェクト作成・更新・削除をトリガーにレプリケーションを実行する

設定

- バージョニング機能を有効にする
- バケットは各別リージョンを指定
- 双方向レプリケーションも可能
- データ転送費用が発生



バージョン管理

ユーザーによる誤操作でデータ削除などが発生してもバージョンから復元できる

設定

- バケットをバージョン管理する
- バージョン保管されたオブジェクトを参照可能
- ライフサイクル管理によって保存する期間の指定も可能
- バケット削除時に古いバージョンの別途削除が必要

【現在】
バージョンID
00011

データA

データB

データC

【過去分】
バージョンID
00010

データA

データB

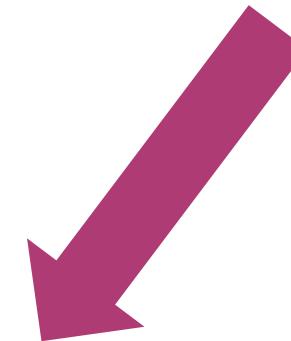
データC

バージョンID
00012

データA

データB

データC



バックアップ

Glacierを利用してバックアップと復元が実施可能

アーカイブ

- 複数リージョンでレプリケートすることが可能
- S3オブジェクトデータをライフサイクル設定によりGlacierに移動

リストア

- バージョン管理機能によって削除されたデータを復元するのが基本



利用状況の確認

S3の利用状況やS3のイベント発生を確認することができる

S3の分析

- データのアクセスパターンの簡易可視化
- CSV形式で出力可能
- バケット内の分析を実施
- アクセス頻度の低いデータや保存期間を確認して、ライフサイクルポリシー設定に活かしていく

S3のイベント通知

- バケット内イベントの発生をトリガーにして、SNS/SQS/Lambdaに通知設定が可能
- シームレスなシステム連携処理を実現



S3データの解析

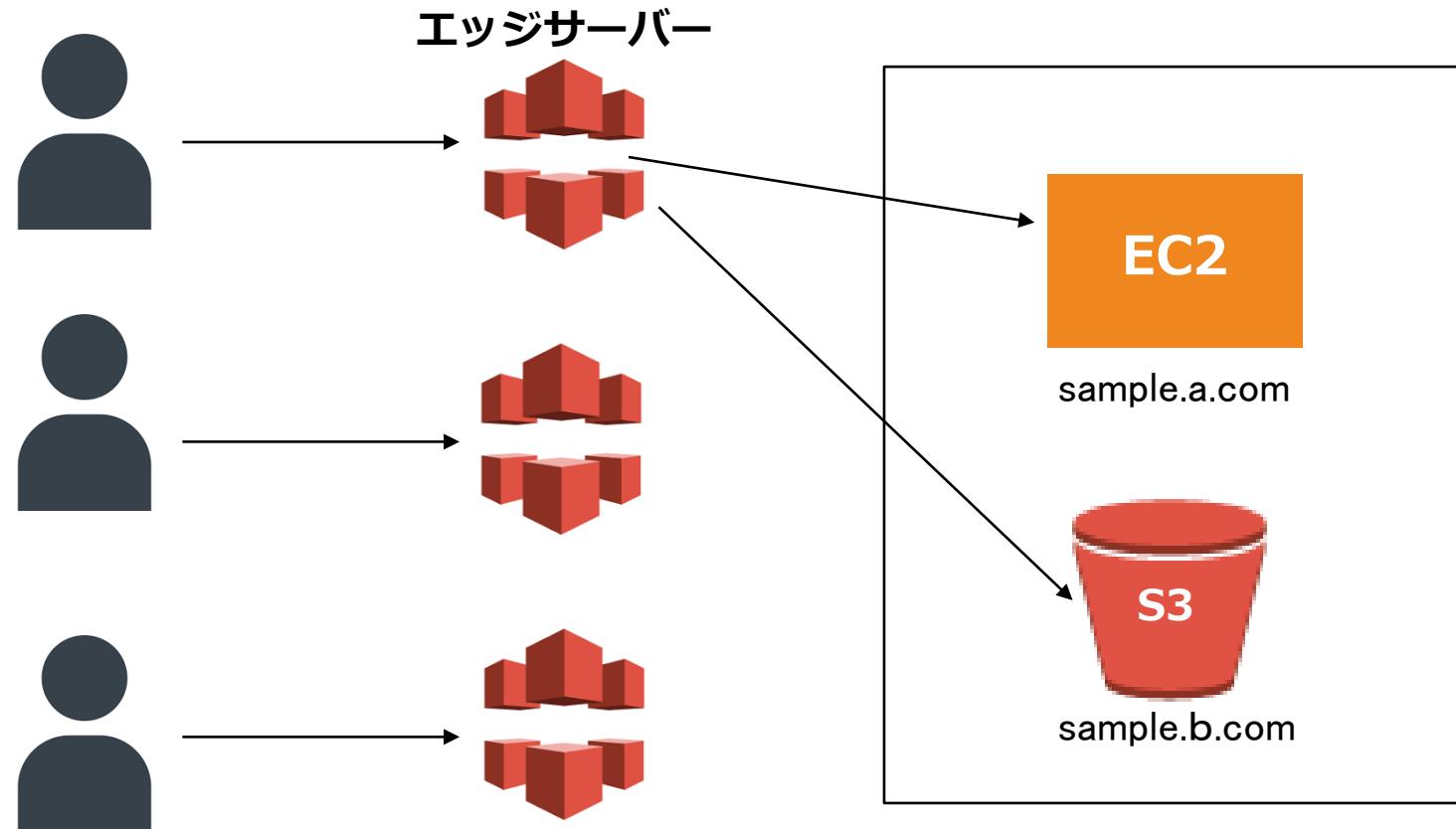
S3内のデータ検索・解析には用途に応じて複数サービスから選択が可能

分析サービス	特徴
S3 Select (Glacier Select)	<ul style="list-style-type: none">✓ S3の内部機能として有している検索機能で、S3内で直接にクエリを実行し、データを取得できる✓ GZIP圧縮データやCSVやJSONに対して実行可能
Amazon Athena	<ul style="list-style-type: none">✓ Amazon S3 内のデータを直接、簡単に分析できるようにするインタラクティブなクエリサービス✓ Athena SQL クエリで SageMaker 機械学習モデルを呼び出し、機械学習による推論も実行可能
Amazon Macie	<ul style="list-style-type: none">✓ 機械学習によりAmazon S3 の機密データを検出、分類、保護する、フルマネージド型サービス✓ 機密データ検出や調査を実施する
Amazon Redshift Spectrum	<ul style="list-style-type: none">✓ Amazon S3の格納データに対して、Amazon Redshiftから直接クエリを実行出来る機能✓ Redshiftクラスターが起動されている前提であるため、Redshiftを利用している場合にお勧め



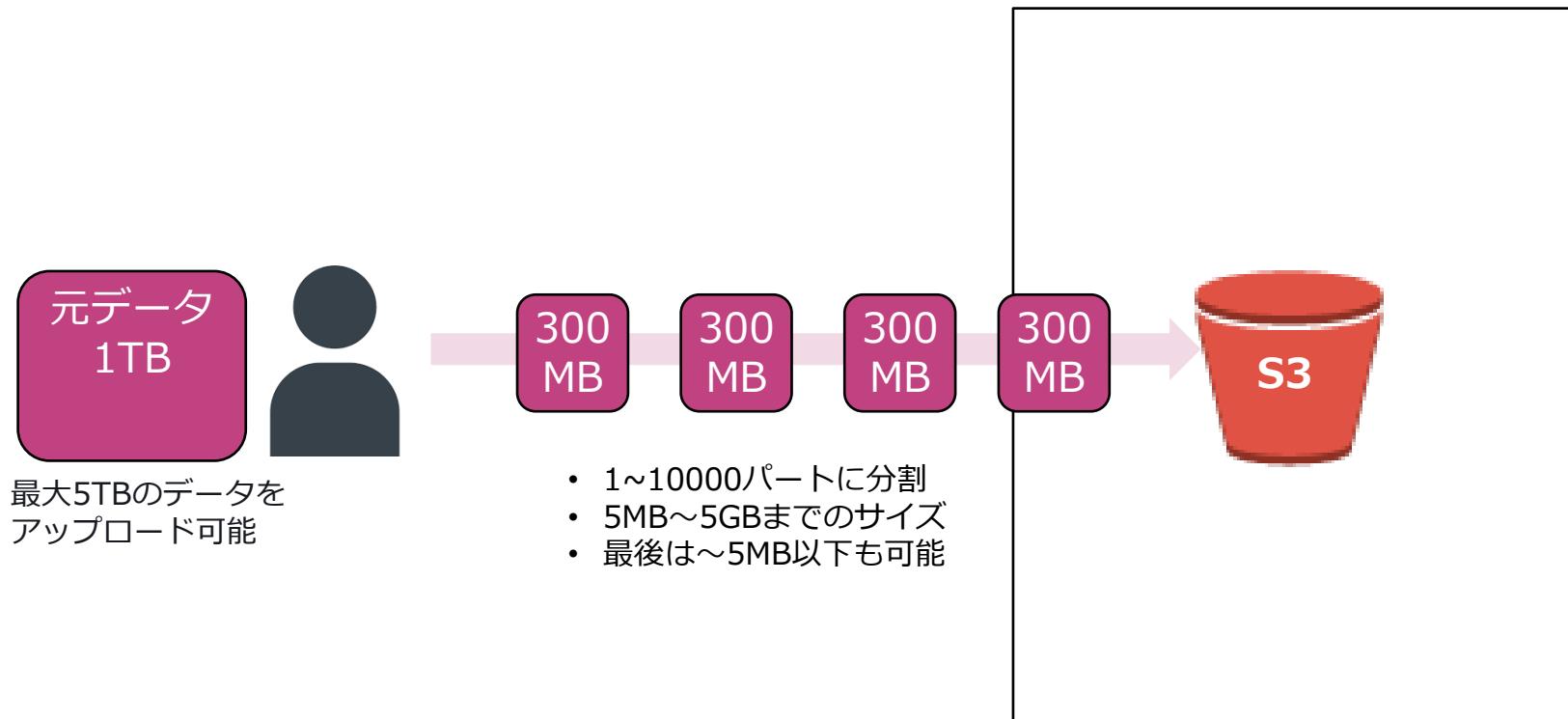
CORS

クロスオリジンリソースシェアリング (CORS) により、特定のドメインにロードされたアプリケーションが異なるドメイン内のリソースと通信する方法を定義



マルチパートアップロード

大容量オブジェクトをいくつかに分けてアップロードする機能



【失敗した場合】

- アップロードを中止するとパートデータが残る
- ライフサイクル管理でクリーンアップ設定が可能



バッチオペレーション

S3 オブジェクトの大量データに対して一括処理を実行することが可能

ジョブ

- ✓ ジョブはS3 バッチオペレーション の機能の基本単位で、ジョブを作成することでバッチオペレーションを作成
- ✓ ジョブにはオブジェクトのリストに対して指定された操作を実行するために必要なすべての情報を登録
- ✓ S3バッチオペレーション にオブジェクトのリストを渡し、それらのオブジェクトに対して実行するアクションを指定

マニフェスト

- ✓ マニフェストとは、Amazon S3 が作用するオブジェクトキーをリストする Amazon S3 オブジェクト
- ✓ マニフェストオブジェクトキー、ETag、およびオプションでバージョン ID を指定
- ✓ Amazon S3 インベントリレポート／CSVファイルの2つの形式で設定

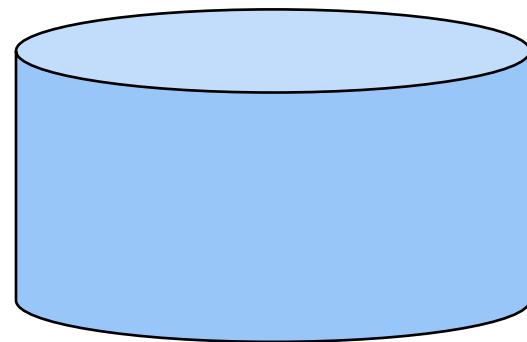


データベースの基礎

データベース

データベースは関連したデータを形式を揃えて収集・整理して、検索などの操作やデータ管理を実行するシステム

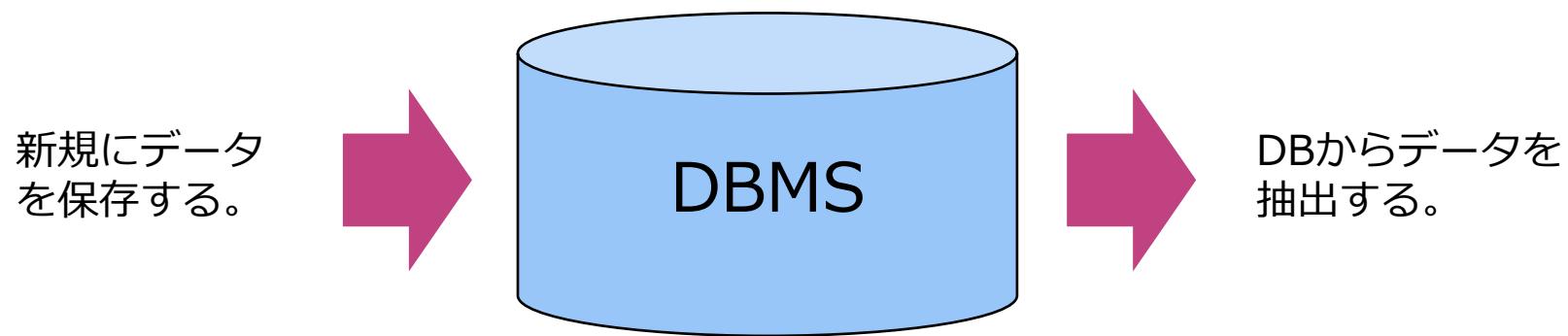
新規にデータ
を保存する。



DBからデータを
抽出する。

データベース

データベースを実現したシステムをDBMS（データベースマネジメントシステムという）



データベース

基本的なデータベースはテーブルという形式でデータを格納している。

社員名簿テーブル

ID	名前	部署	生年月日
1001	佐藤周大	営業	19870621
1002	小林隆文	開発	19830821
1003	元木博夫	経理	19820524

データベース

データベースは追加・参照・更新・削除などのデータ操作を容易に実行するソフトウェアやデータモデルと一体

- 追加：データを整理して保存したい。
- 参照：必要なデータを参照または抽出したい。
- 更新：データの変化に応じて好きなときに更新したい。
- 削除：不要ないデータを削除したい。

データベース

追加・参照・更新・削除を総称してCRUDと呼ぶ。このCRUD操作を実現するのがデータベースとなる。

- Create 追加：データを整理して保存したい。
- Read 参照：必要なデータを参照または抽出したい。
- Update 更新：データの変化に応じて好きなときに更新したい。
- Delete 削除：不要ないデータを削除したい。

データベースとストレージ

ストレージはデータベースの記憶装置を構成する1つの要素

ストレージ

- コンピュータの主要な構成要素の一つで、データを永続的に記憶する装置

データベース

- データベース内のデータを保存する装置はストレージであるが、データベースそのものではない。
- ストレージ+データを管理・操作するデータベースソフトウェア

データベースの役割

データベースはデータ操作を異状なく実行でき、データを安全に保護しつつ、保存・操作ができる仕組みを提供している。

【データ操作にかかる様々な課題】

- システムがクラッシュしたときにデータが消えないか？
- データを誤って削除してしまった場合に対処できないか？
- データ抽出に誤りが発生しないか？
- 2人が同時に同じデータにアクセスした際にどうするか？
- 大量のデータを上手く検索できないか？

データベースの役割

データベースの役割を支える仕組みを理解する。

トランザクション

データベースをある一貫した状態から別の一貫した状態へ変更する1つの処理の束のこと

データモデル

実世界におけるデータの集合を、DBMS上で利用可能な形に落とし込むためのモデル

トランザクション

データベースをある一貫した状態から別の一貫した状態へ変更する1つの処理のこと。

- 同時アクセスした場合に上手く処理する。
- データ処理に失敗したら、元に戻してくれる。
- システムがクラッシュしてもデータを保護する。

トランザクション：ACID

ACIDは信頼性のあるトランザクションシステムの持つべき性質のこと

- Atomicity (原子性)

トランザクションが「すべて実行される」か「一つも実行されない」のどちらかの状態になるという性質

- Consistency (整合性)

トランザクションの前後でデータの整合性が保たれ、矛盾の無い状態が継続される性質

- Isolation (独立性)

トランザクション実行中の処理過程が外部から隠蔽され、他の処理などに影響を与えない性質

- Durability (耐久性)

トランザクションが完了したら、その結果は記録され、クラッシュしても失われることがないという性質

トランザクション：耐久性

データを更新する際にCOMMITとする更新が反映されるが、COMMITされないとデータがロールバックして保護する。

データ更新
(COMMIT実施)

データ更新
(COMMIT未実施)

氏名データ：高橋を佐藤に更新する。



氏名データの更新がCOMMITされる。



データベースがクラッシュする。



氏名データ：佐藤でデータを保護

氏名データ：高橋を佐藤に更新する。

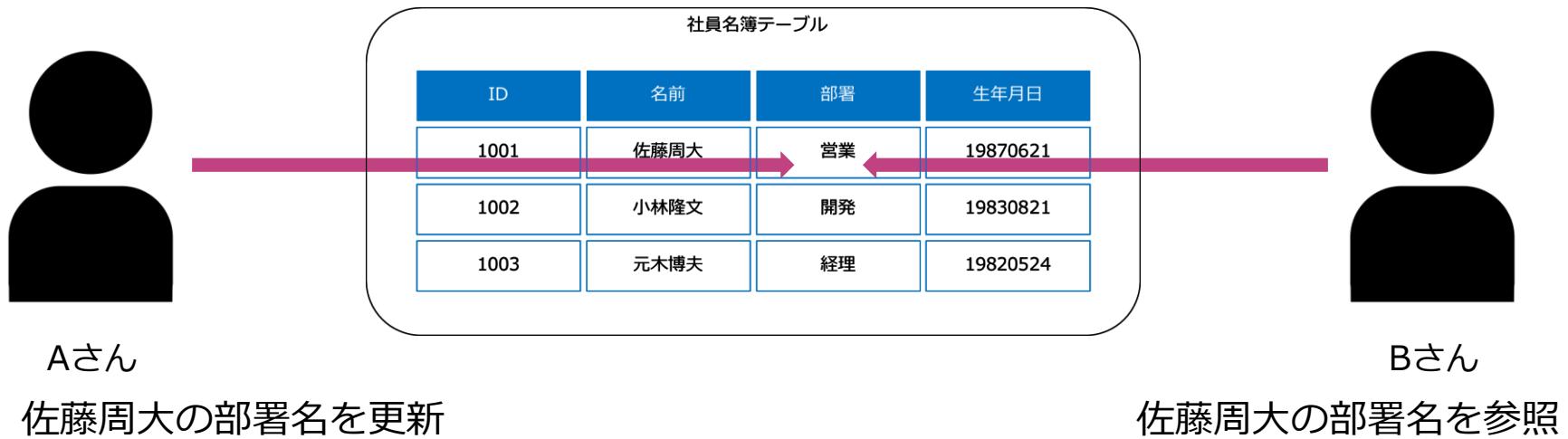


データベースがクラッシュする。

ロールバックする。

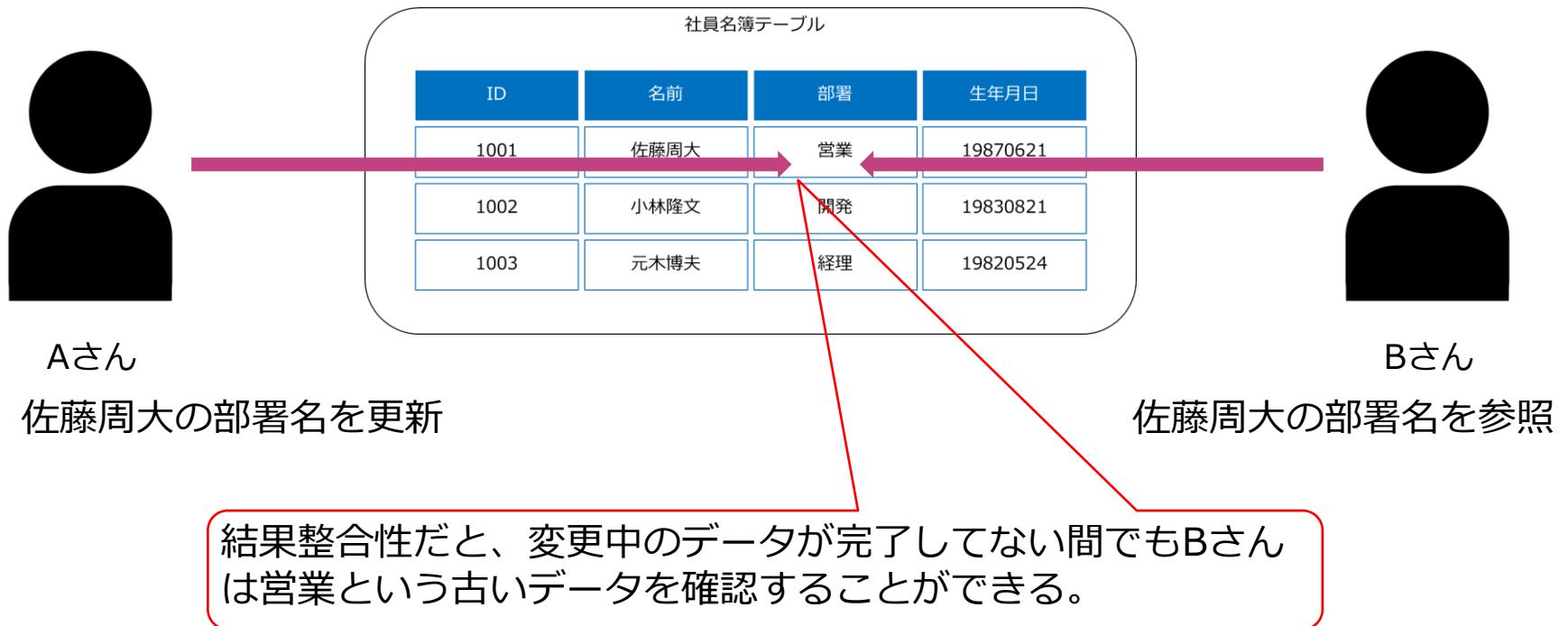
トランザクション：整合性

同時に複数人がアクセスした場合などにデータ整合性を維持する必要がある。



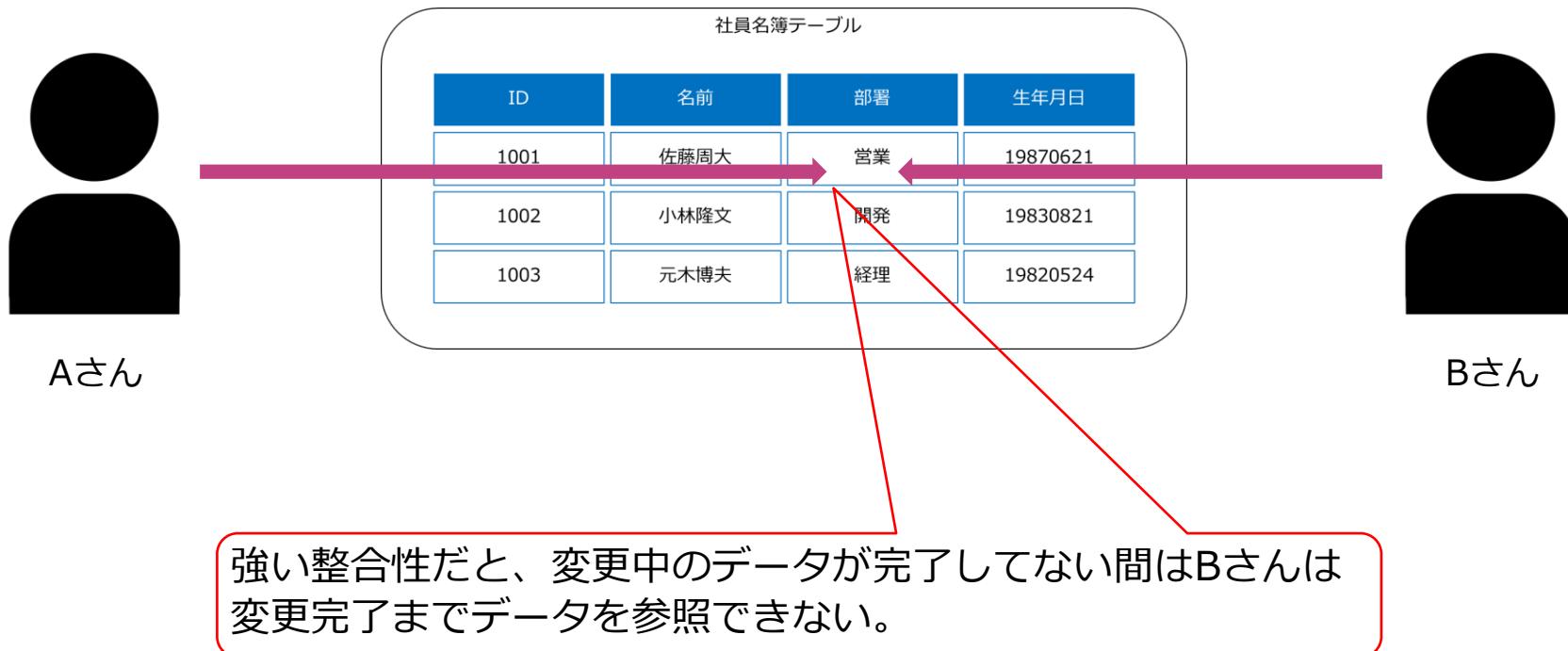
整合性モデル

同時に複数人がアクセスした場合などの、データのデータ整合性を維持するための方式（結果整合性や強い整合性など）



整合性モデル

同時に複数人がアクセスした場合などの、データのデータ整合性を維持するための方式（結果整合性や強い整合性など）



データモデル

データモデルはデータベースのデータの持ち方などの構造や処理を定めるデータの論理的な表現方法

データモデルに応じたトランザクション機能

データモデル

データモデル

データベースには様々なデータモデルが存在し、利用目的に応じて使い分ける

- リレーションナルモデル
- グラフモデル
- キーバリューストア
- オブジェクト
- ドキュメント
- ワイドカラム
- 階層型

RDSの概要

RDS

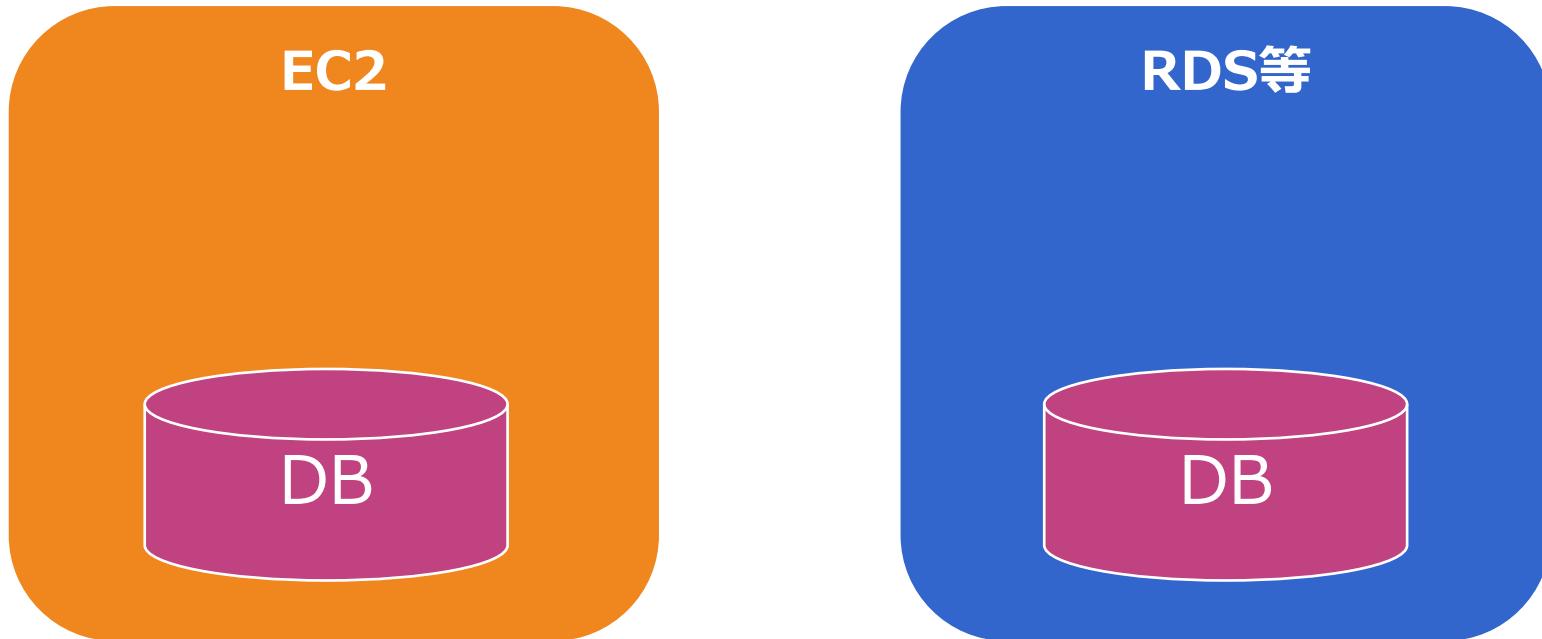
RDSは様々なデータベースソフトウェアに対応したフルマネージドなリレーショナルデータベース

以下のような標準ソフトウェアを利用したデータベースを構築できる

- MySQL
- ORACLE
- Microsoft SQL Server
- PostgreSQL
- MariaDB
- Amazon Aurora

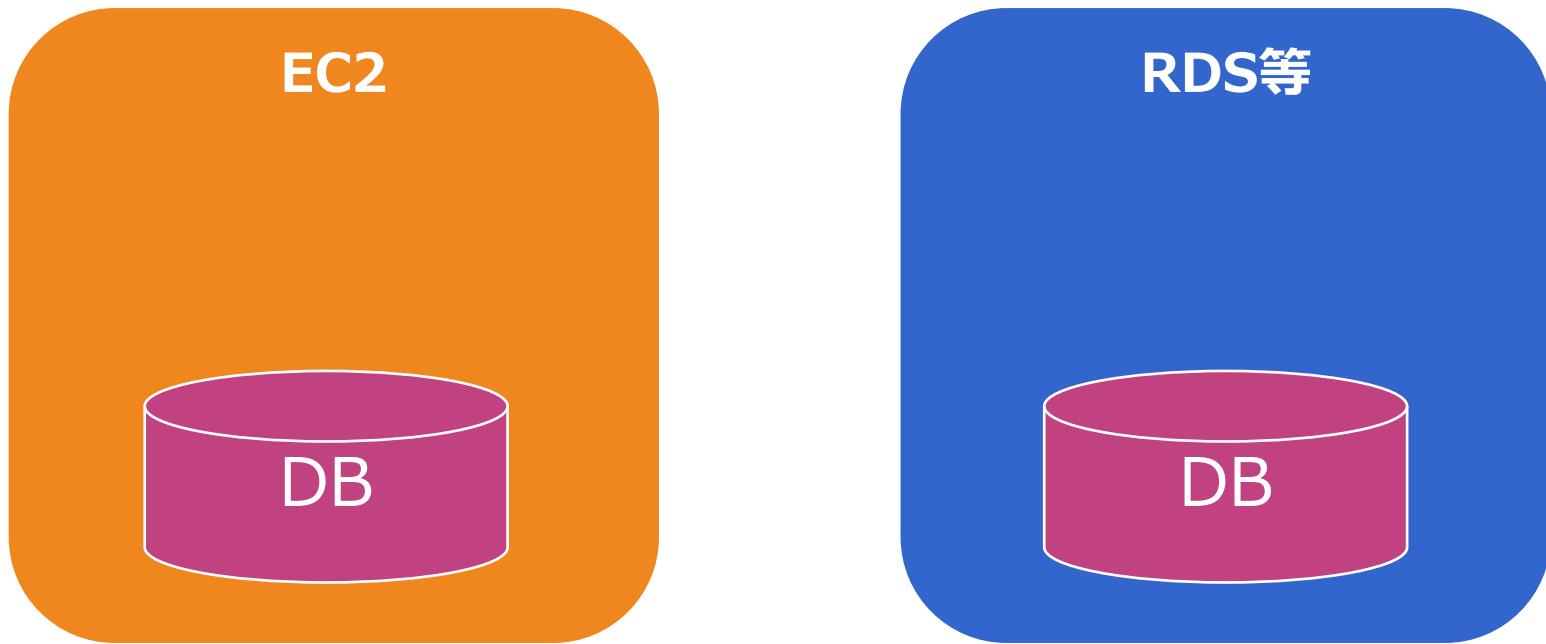
AWSのデータベース構築

AWSにおけるデータベース構築はEC2に自らインストールして構築するか、専用DBサービスを利用するかの2通り



AWSのデータベース構築

AWSにおけるデータベース構築はEC2に自らインストールして構築するか、専用DBサービスを利用するかの2通り

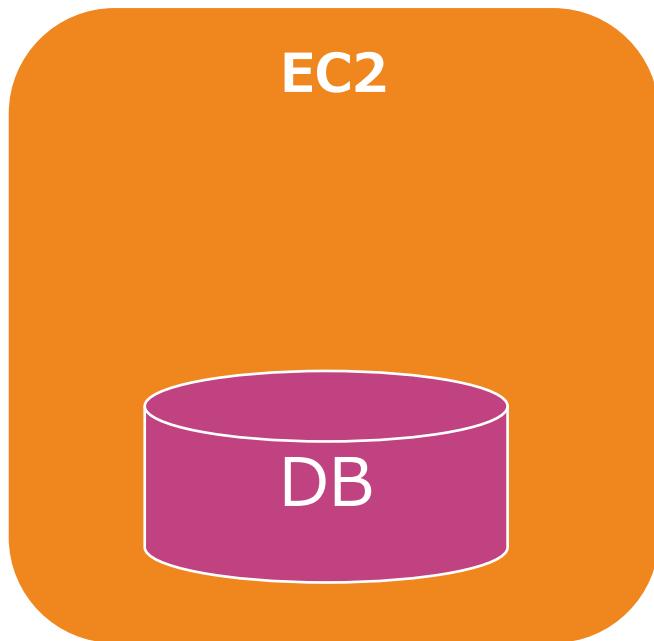


メリット：自由にDB構成や機能を利用

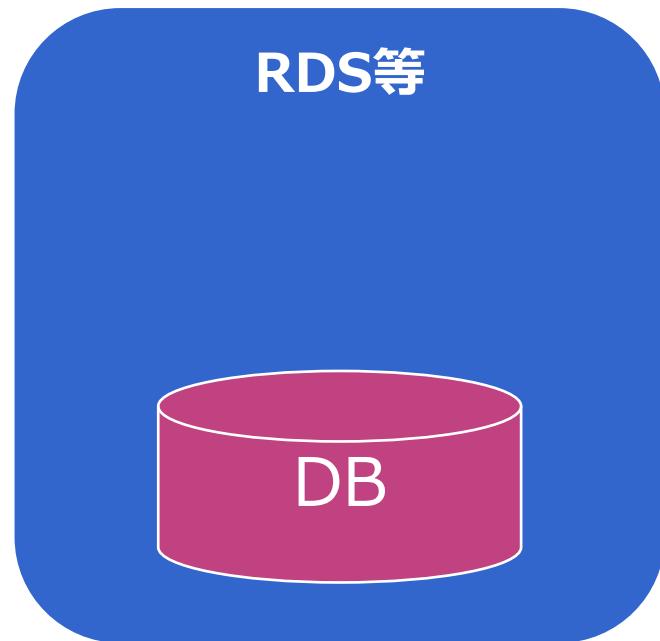
デメリット：構築・運用が手間

AWSのデータベース構築

AWSにおけるデータベース構築はEC2に自らインストールして構築するか、専用DBサービスを利用するかの2通り



メリット：自由にDB構成や機能を利用
デメリット：構築・運用が手間



メリット：構築・監理が楽（大部分がAWS側）
デメリット：AWS提供の範囲内での利用制限

RDSの制約事項

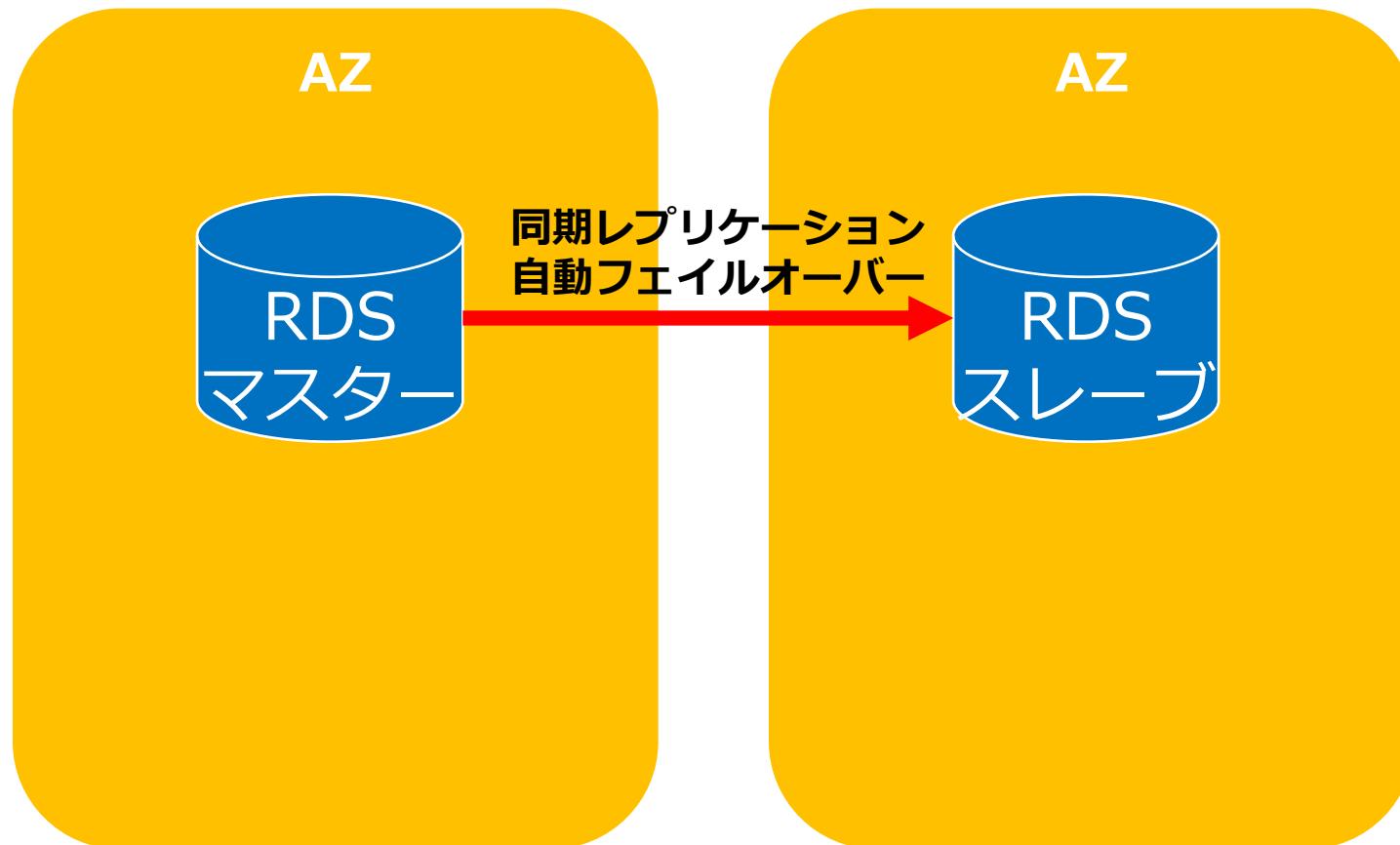
RDSはマネージド型で楽な反面、AWSから提供される機能範囲内の制限を受ける

RDSの主な制限事項

- バージョンが限定される
- キャパシティに上限がある
- OSへのログインができない
- ファイルシステムへのアクセスができない
- IPアドレスが固定できない
- 一部の機能が使えない
- 個別パッチは適用できない

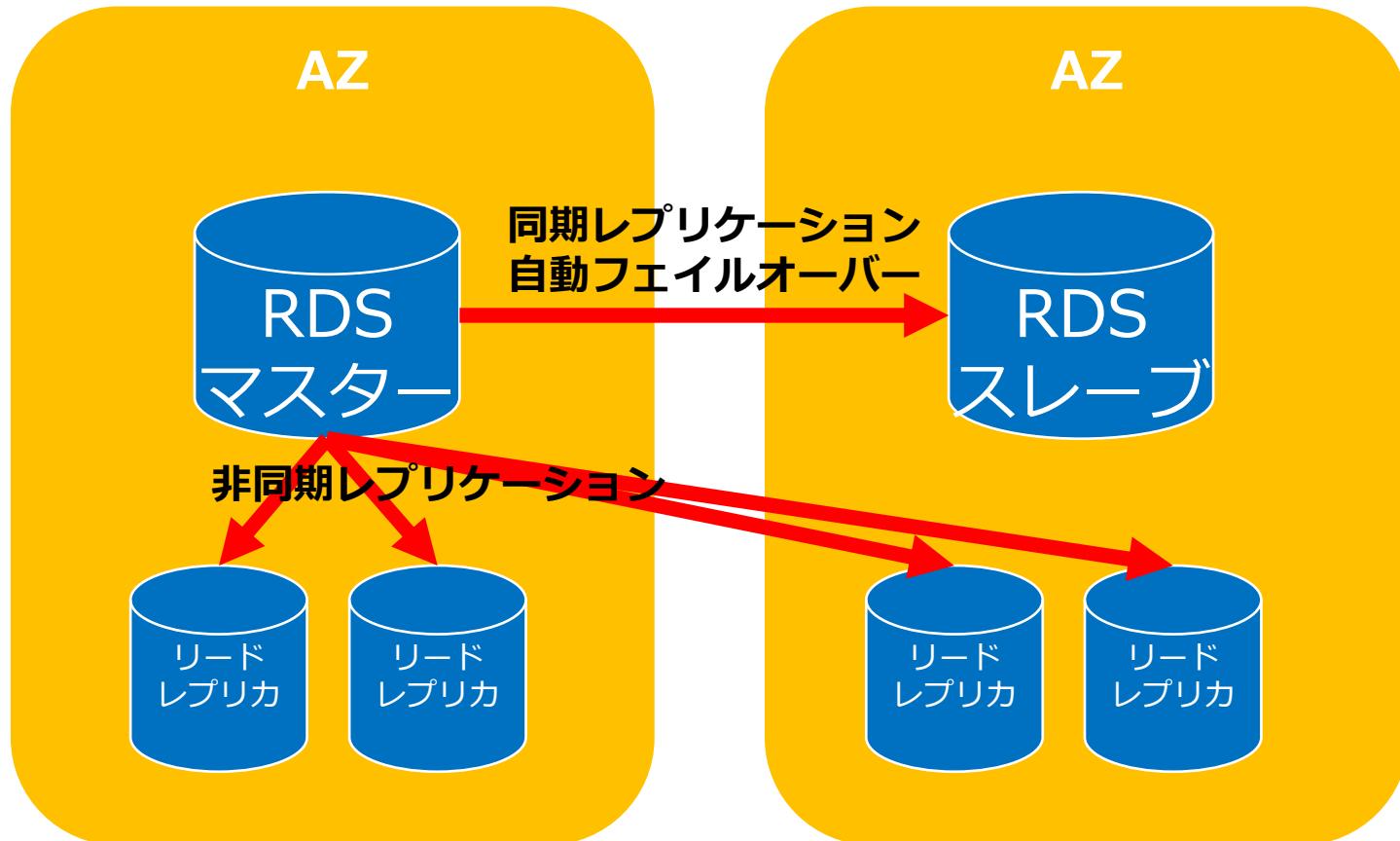
RDSの特徴

RDS自体がマネージド型の高可用なのに加え、マルチAZによるMaster／Slave構成を容易に構築することができる



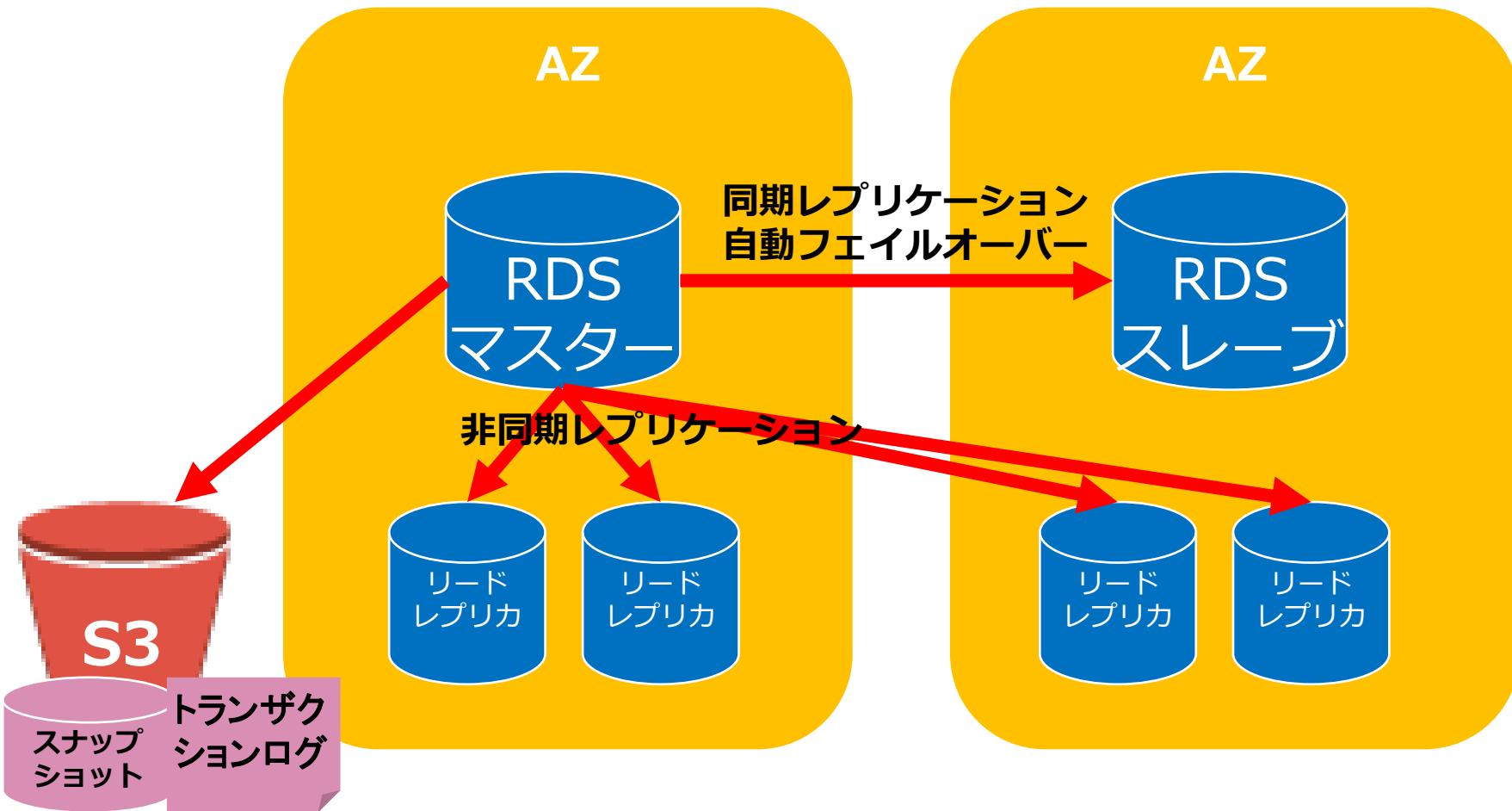
RDSの特徴

参照専用のレプリカを最大5台（Auroraは15台）設置し、DBの読み取り処理をスケールアウトできる



RDSの特徴

自動／主導でスナップショットを取得して保存管理し、耐障害性を確保



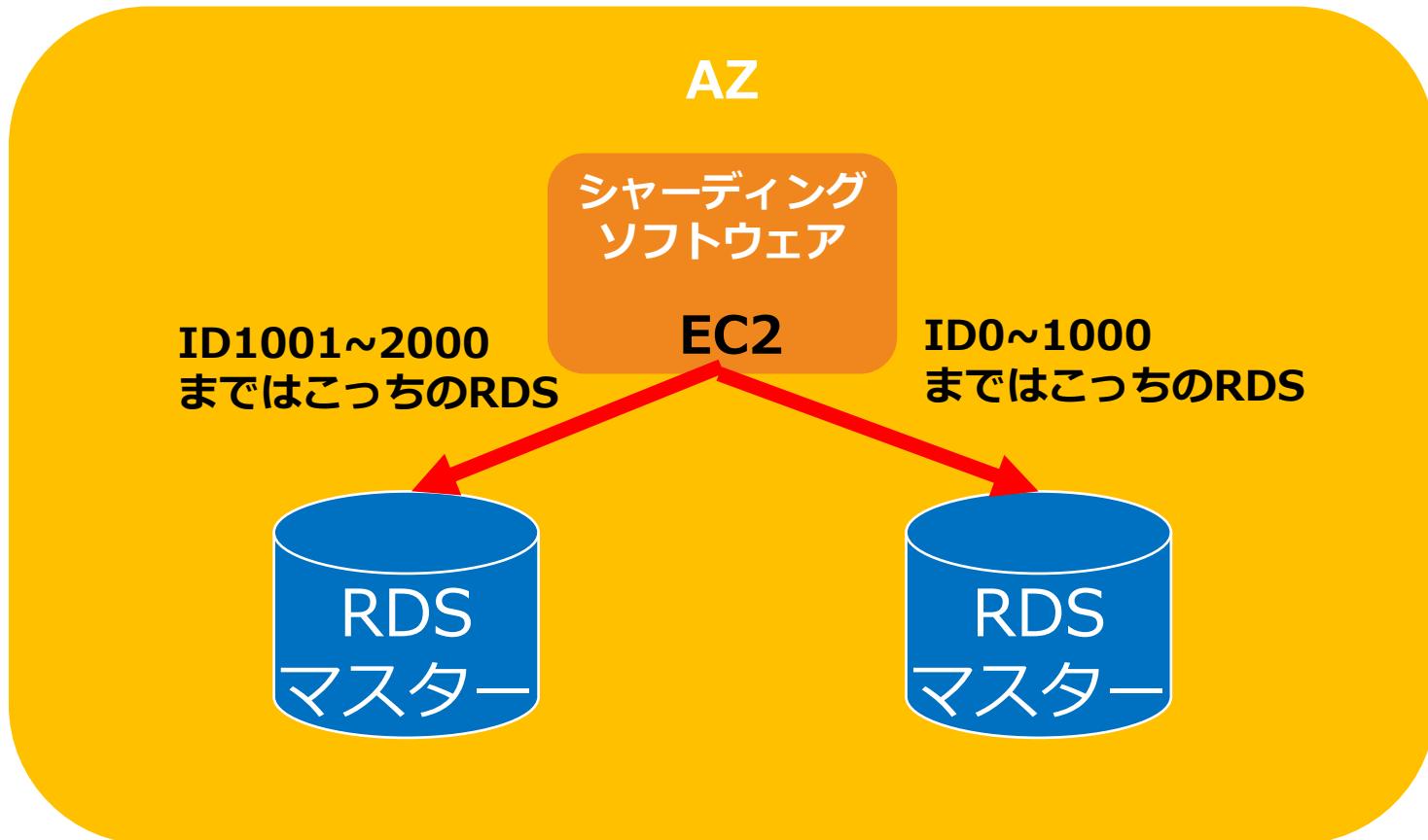
スケーリング

マネージメントコンソールやAPIからスケールアップ可能

- インスタンスタイプを変更してスケールアップ／ダウンを実施
- コマンドライン (AWS CLI) やAPIからストレージを数クリックで
容易にスケールアップ／ダウンをする
- 一時的にインスタンスタイプを大きくして、その後戻すことも可能
- ストレージサイズは、拡張はできるが縮小はできない

スケーリング

データベースシャーディングを利用してRDSの書き込み処理をスケーリングする



DBインスタンスの暗号化

保管時のインスタンスとスナップショットの暗号化が可能

暗号化対象

- DBインスタンス
- 自動バックアップ
- リードレプリカ
- スナップショット

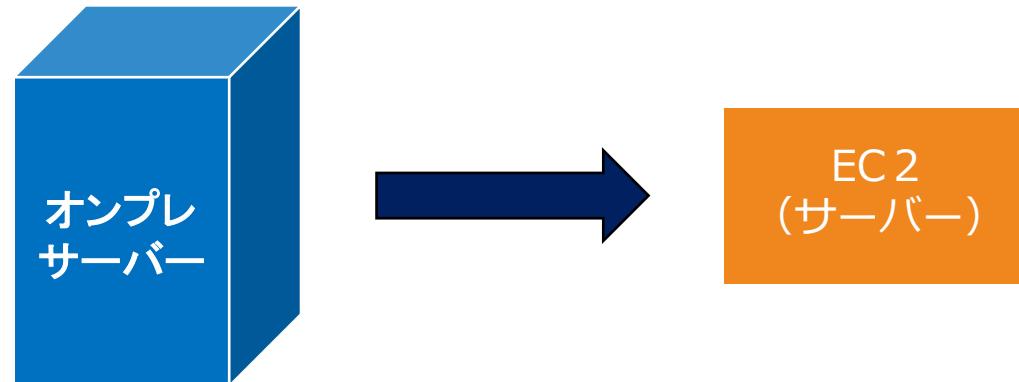
暗号化方式

- AES-256暗号化
- AWS KMSによる鍵管理
- リードレプリカも同じ鍵を利用
- インスタンス作成時にのみ設定可能
- スナップショットのコピーの暗号化／リストア可能

RDSの構築

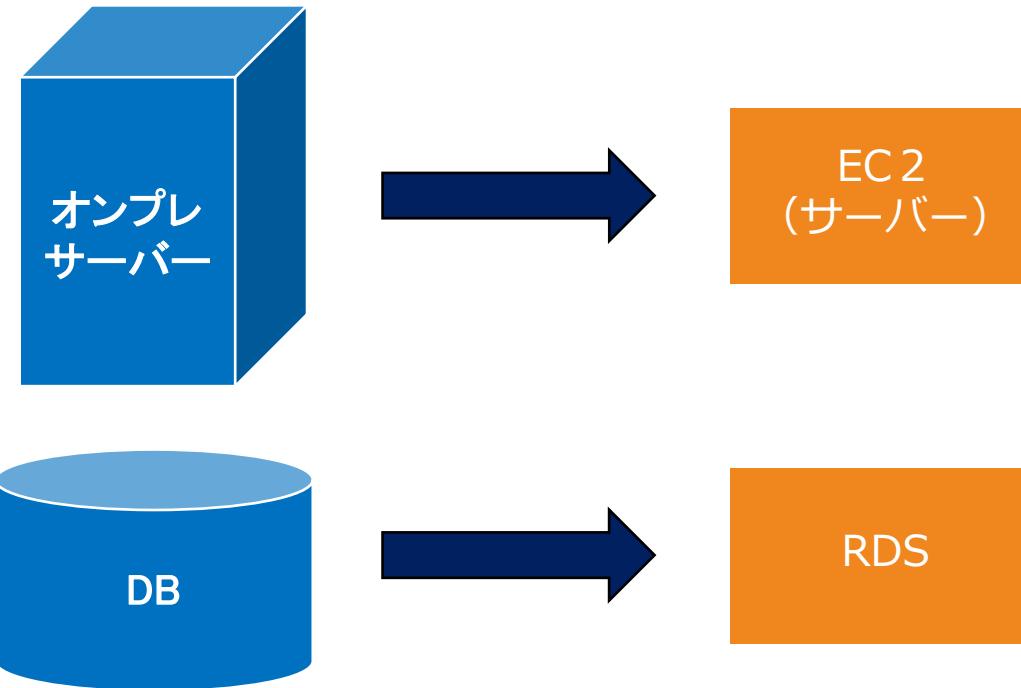
AWSの仕組み

インフラやアプリ開発に必要な機能がオンデマンドのパーティ¹サービスとして提供されている



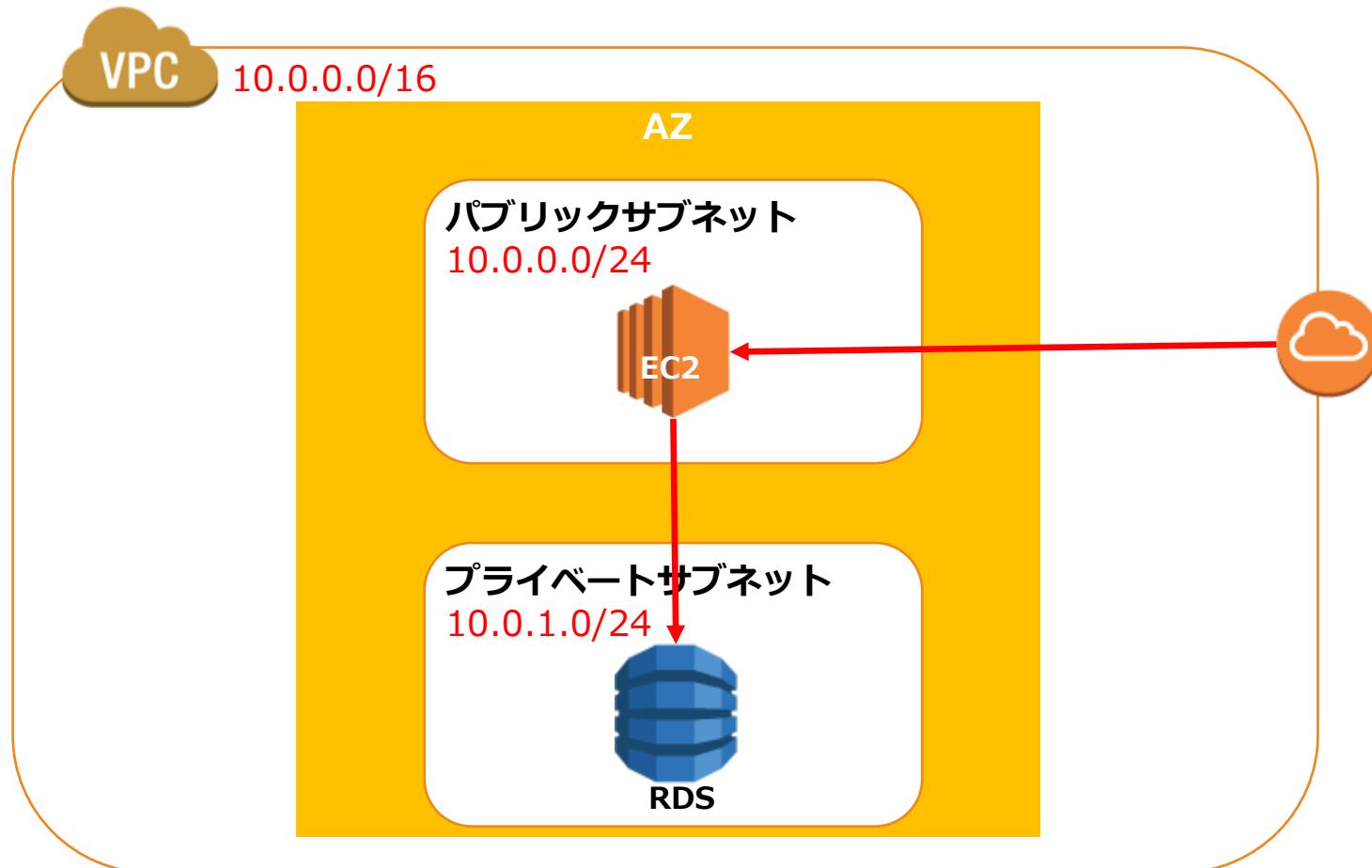
AWSの仕組み

インフラやアプリ開発に必要な機能がオンデマンドのパーツ
サービスとして提供されている



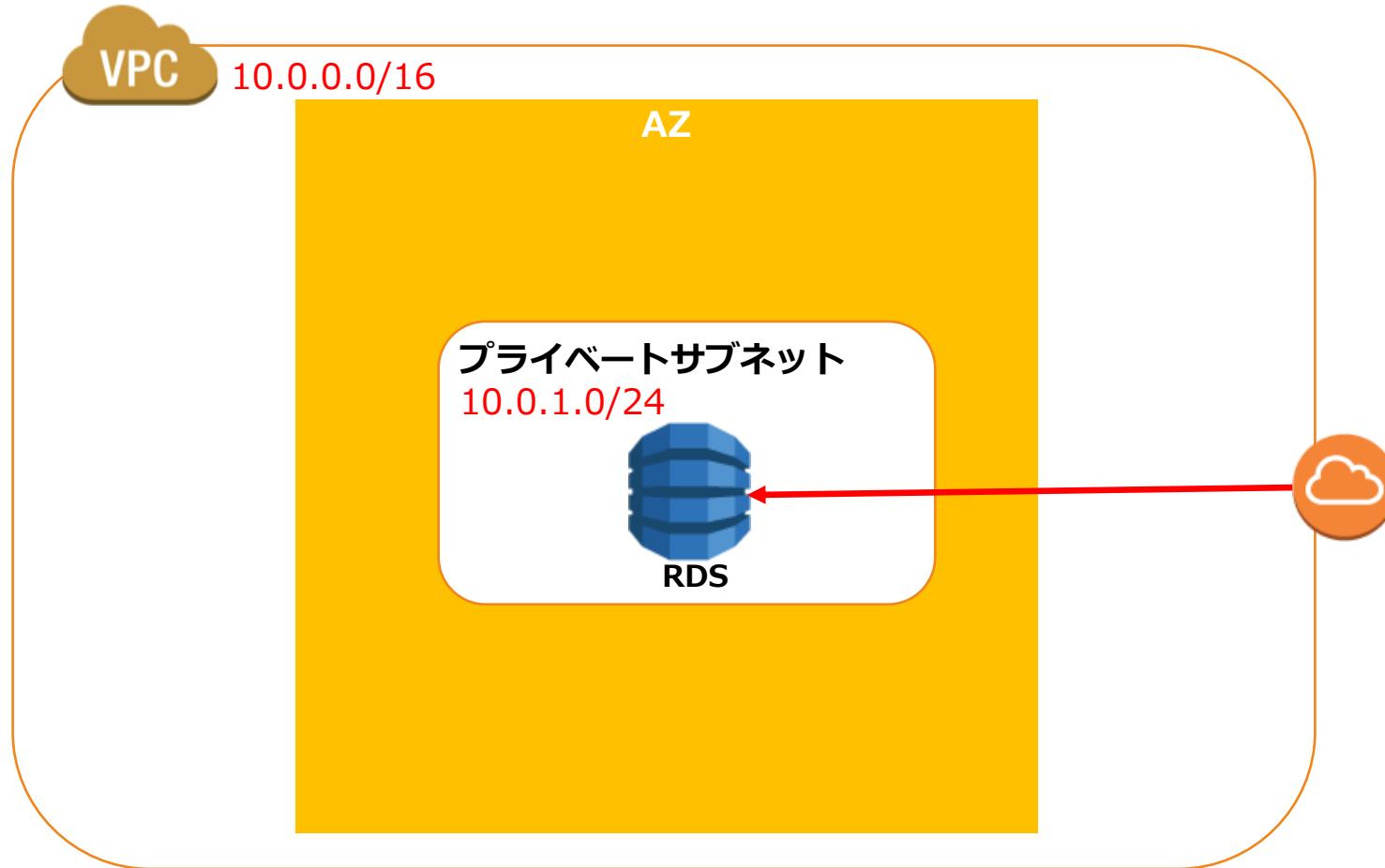
このレクチャーで作成するDB構成

RDSはEC2というサーバーを介して接続して操作することが一般的な利用方法となる



このレクチャーで作成するDB構成

最初は直接接続して操作する方法を学習する



セクションの内容

レクチャー	レクチャーで学ぶ内容
AWS責任共有モデル	AWSのセキュリティ対応の基本原則であるAWS責任共有モデルについて学習します。
IAMの概要	AWSアカウント内のユーザー管理やアクセス権限管理を実施するIAMを学習します。
IAMユーザーの作成	実際にIAMユーザーとグループを作成して、その設定方法を確認します。
CloudTrailの概要	CloudTrailの特徴や機能について学習します。
CloudTrailの設定	CloudTrailの証跡確認を有効化して、アクティビティログが取得できるように設定します。

セクションの内容

レクチャー	レクチャーで学ぶ内容
CloudWatchの概要	CloudWatchの特徴や機能について学習します。
CloudWatchの設定	CloudWatchによるモニタリングを実際に設定して、モニタリング方法を確認します。

AWS責任共有モデル

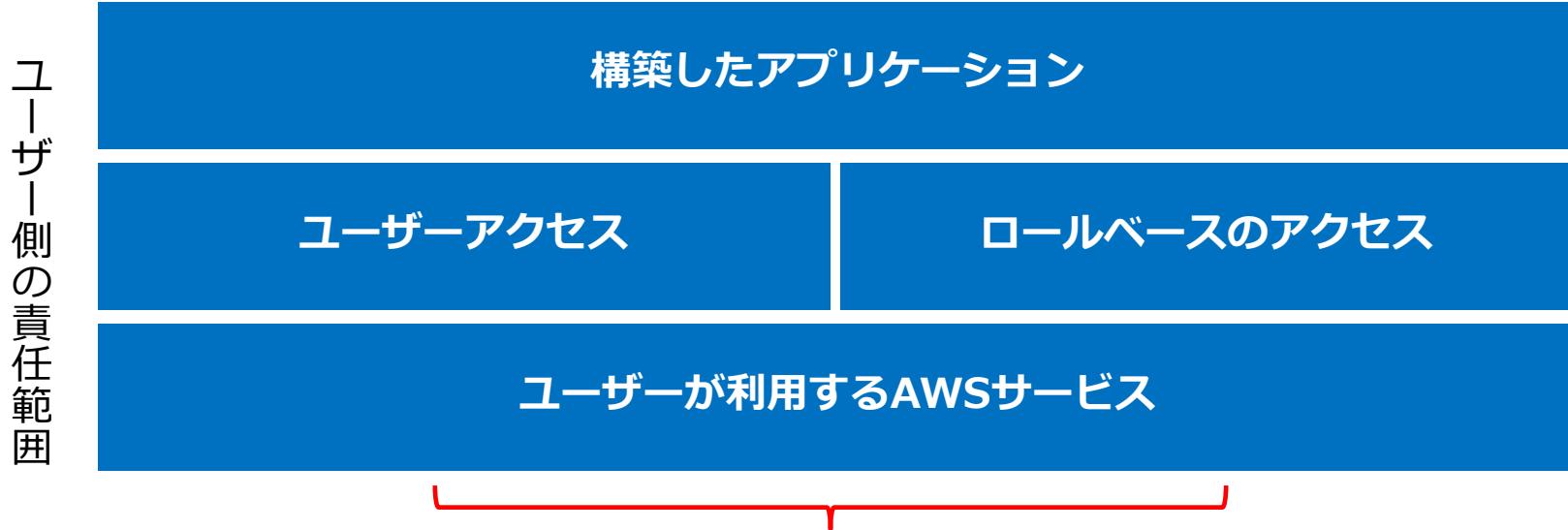
責任共有モデル

セキュリティに対してAWSとユーザーとで責任分界して対応する責任共有モデルとなっている



責任共有モデル

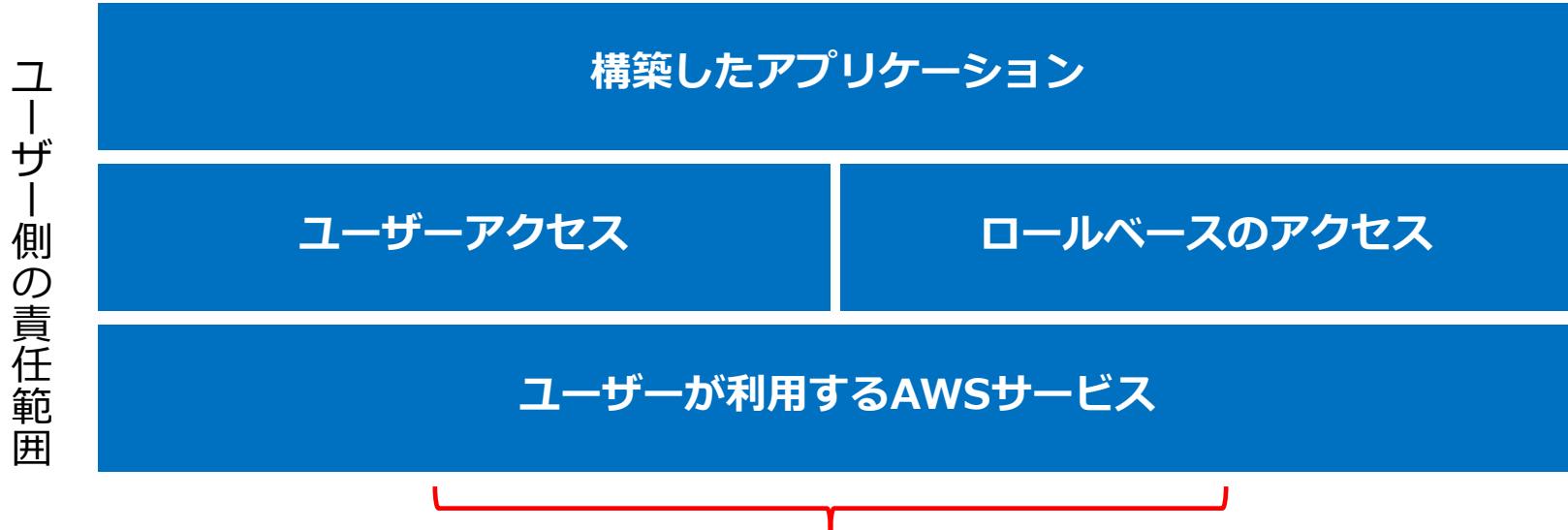
セキュリティに対してAWSとユーザーとで責任分界して対応する責任共有モデルとなっている



- IAMによるアカウント管理／パスワードルールの設定
- セキュリティグループの設定など適切なネットワーク設定やトラフィック保護
- 構築したアプリケーションのセキュリティ対応
- ネットワーク／インスタンスオペレーションシステム（バッチ）などの設定
- OSやミドルウェアの脆弱性対応
- 通信トラフィックの暗号化／保有しているデータの暗号化

責任共有モデル

セキュリティに対してAWSとユーザーとで責任分界して対応する責任共有モデルとなっている



- IAMによるアカウント管理／パスワードルールの設定
- セキュリティグループの設定など適切なネットワーク設定やトラフィック保護
- 構築したアプリケーションのセキュリティ対応
- ネットワーク／インスタンスオペレーションシステム（バッチ）などの設定
- OSやミドルウェアの脆弱性対応
- 通信トラフィックの暗号化／保有しているデータの暗号化

責任共有モデル

セキュリティに対して AWS とユーザーとで責任分界して対応する責任共有モデルとなっている

継承される統制		<p>ユーザーが AWS から完全に継承する統制 物理統制と環境統制がある。</p>
共有統制	パッチ管理	AWS がインフラストラクチャの不具合に対するパッチ適用および修復に責任を負うが、ユーザーはゲスト OS およびアプリケーションのパッチ適用に責任を負う。
	構成管理	AWS がインフラストラクチャデバイスの構成を保守するが、ユーザーは独自のゲストオペレーティングシステム、データベース、アプリケーションの構成に責任を負う
	意識とトレーニング	AWS が AWS 従業員のトレーニングを実施しするが、ユーザーの従業員のトレーニングはユーザーが実施する
ユーザー固有の統制		AWSサービスにデプロイするアプリケーションに基づいて、ユーザーがすべての責任を負う統制。データをルーティングまたは区分する必要があるサービスおよびデータ通信の保護またはゾーンセキュリティなど

IAMの概要

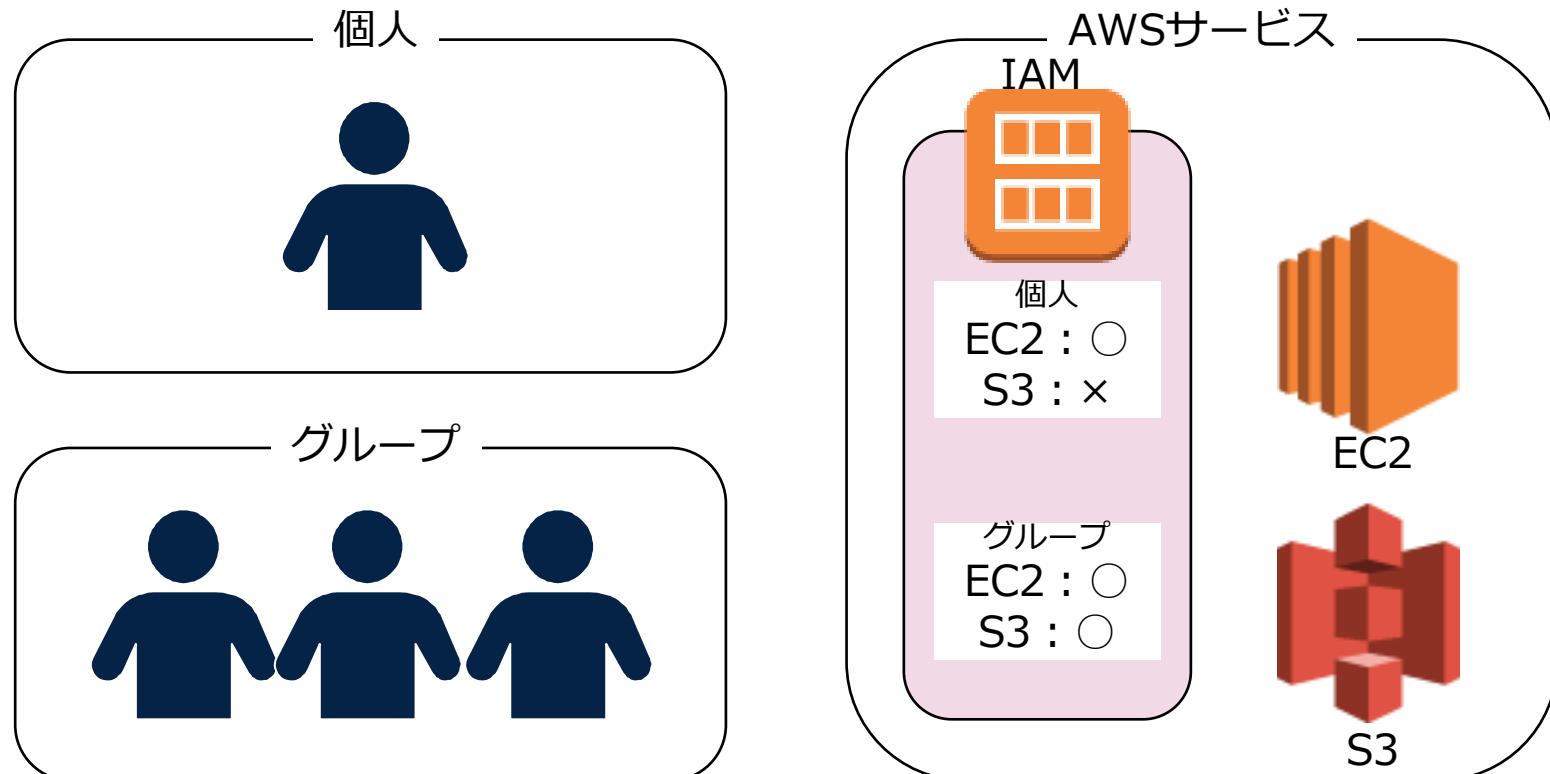
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み

- AWS利用者認証の実施
- アクセスポリシーの設定
- ユーザー個人またはグループ毎に設定

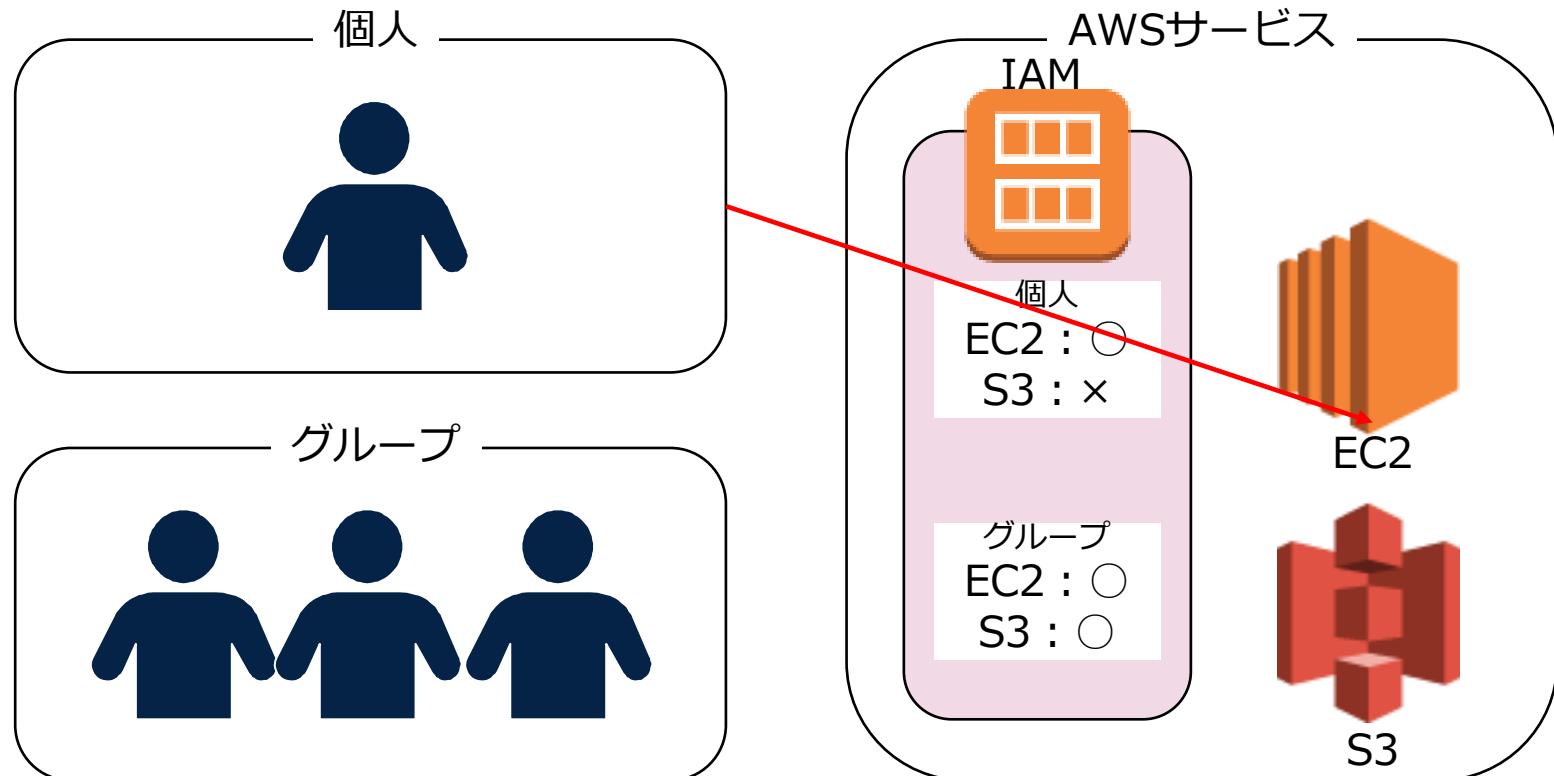
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み



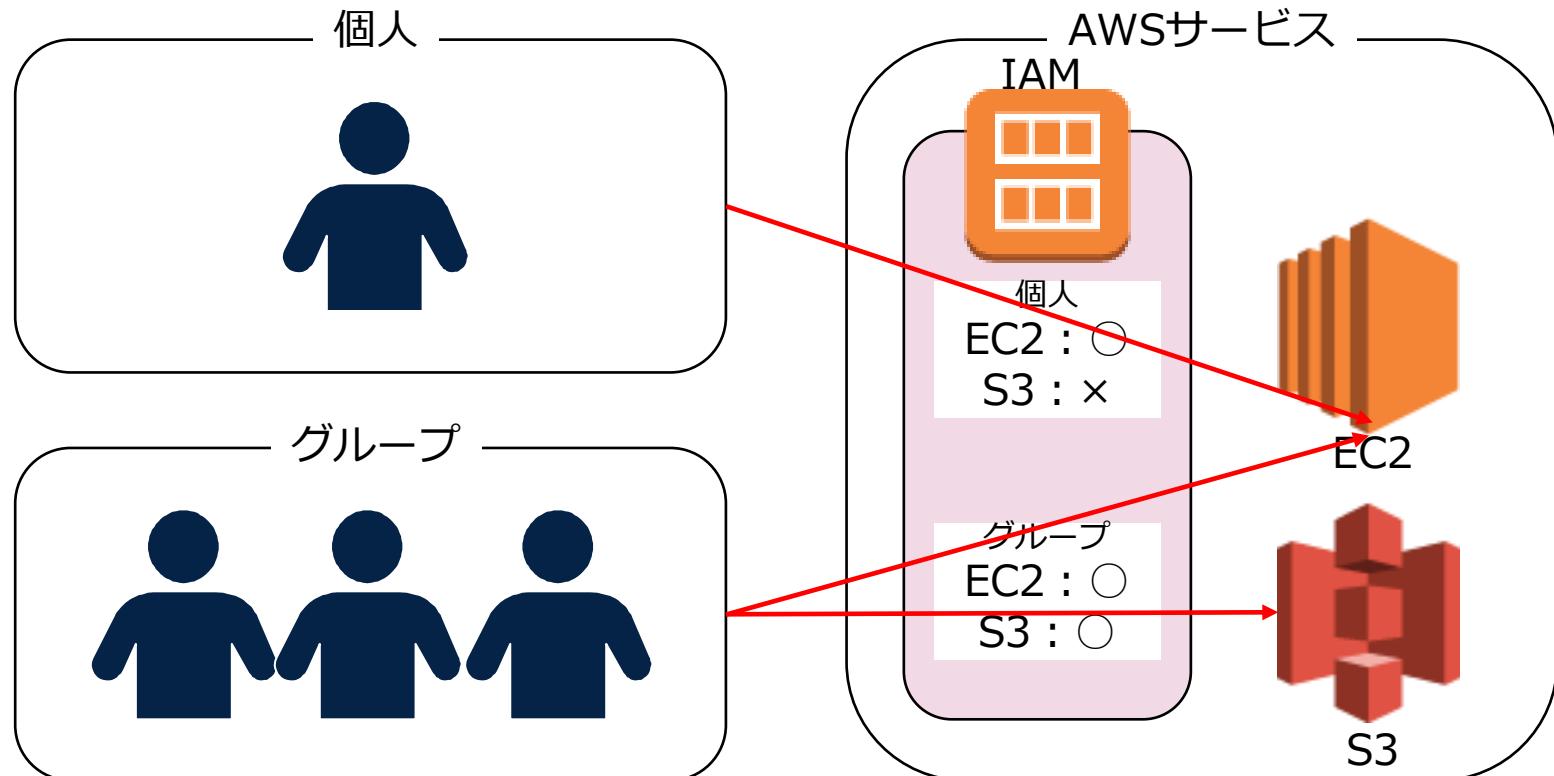
IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み



IAMとは

AWS Identity and Access Management (IAM)は安全にAWS操作を実施するための認証・認可の仕組み

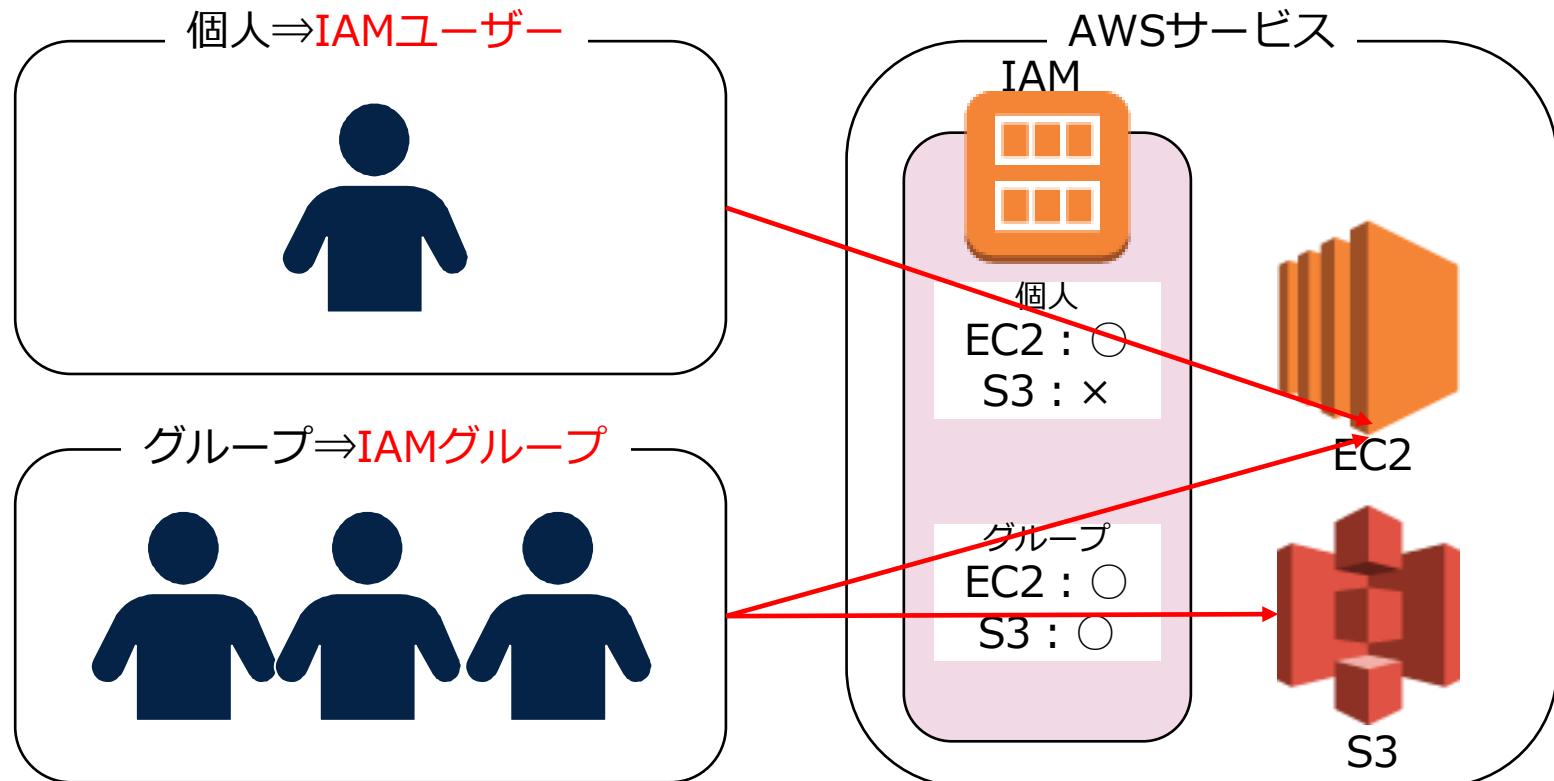


ユーザー

- ルートユーザー
- IAMユーザー

IAMユーザー／IAMグループ

IAMポリシー内でAWSサービスを利用するユーザー。基本操作はIAMユーザーで実施することになる



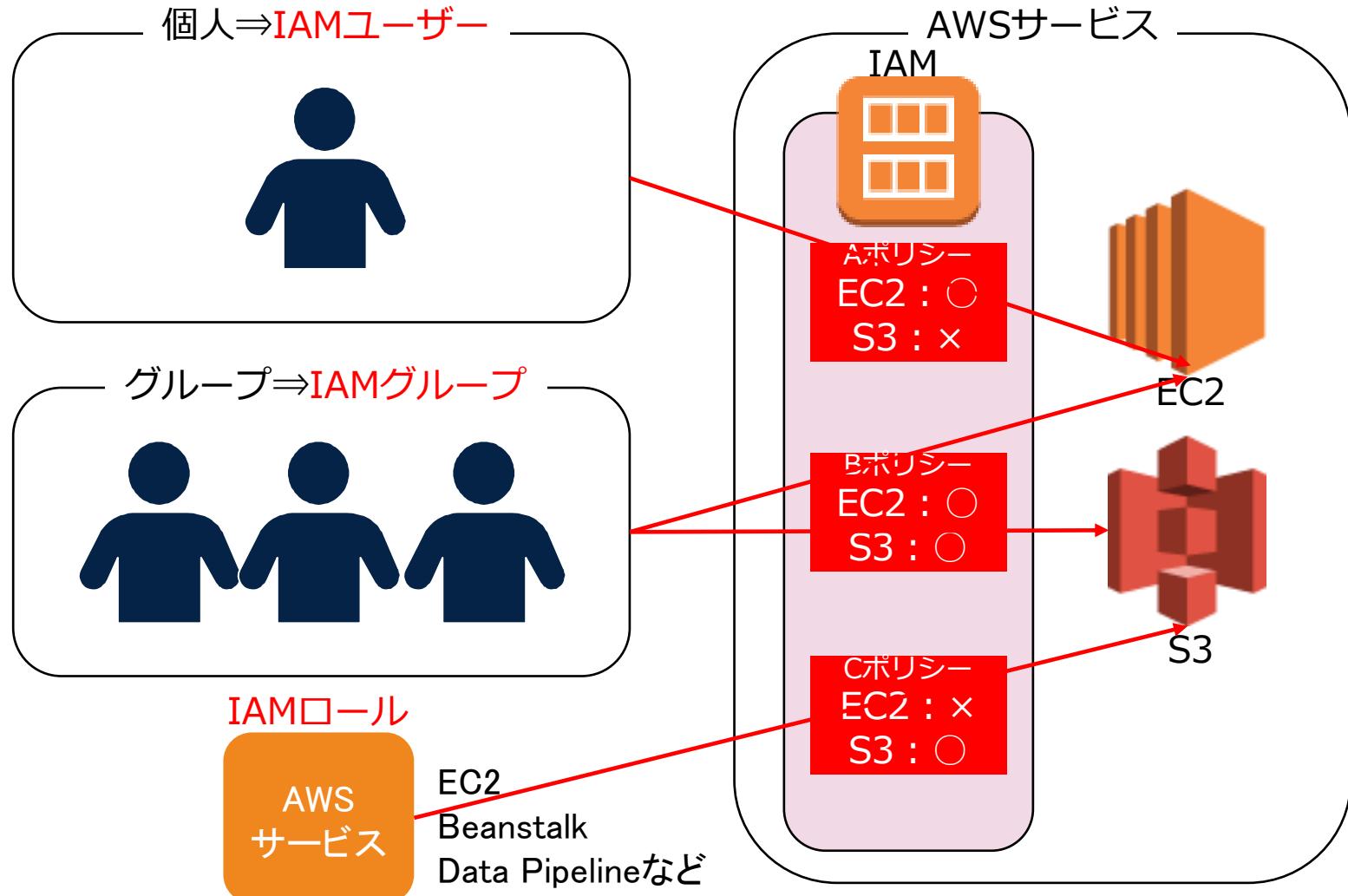
IAMポリシー

IAMポリシーはJSON形式で設定される

{ "Effect": "Allow", "Action": ["s3>ListBuckets", "s3:Get *"], "Resource": ["arn:aws:s3:::mybucket"], "Condition": { "IpAddress": { "aws:SourceIP": ["176.32.92.49/32"] } } }	Effect	"Allow"⇒許可 "Deny"⇒拒否
	Action	対象のAWSサービス 例："s3:Get"
	Resource	対象のAWSリソース ARNで記述
	Condition	アクセス制御 が有効となる条件

IAMロール

AWSリソースに対してアクセス権限をロールとして付与できる



ユーザーのアクティビティの記録

Access Advisor のService Last Accessed Data	IAMエンティティ(ユーザー、グループ、ロール)が、最後にAWSサービスにアクセスした日付と時刻を表示する機能
Credential Report	利用日時などが記録されたIAM認証情報に係るレポートファイル
AWS Config	IAMのUser、Group、Role、Policyに関して変更履歴、構成変更を管理・確認することができる機能
AWS CloudTrail	AWSインフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的に監視し、保持することができる機能

アクセス権限の一時付与

一時的なアクセス権限の付与を可能にする

AWS Security
Token Service(STS)

動的にIAMユーザーを作り、一時的に利用する
トークンを発行するサービス

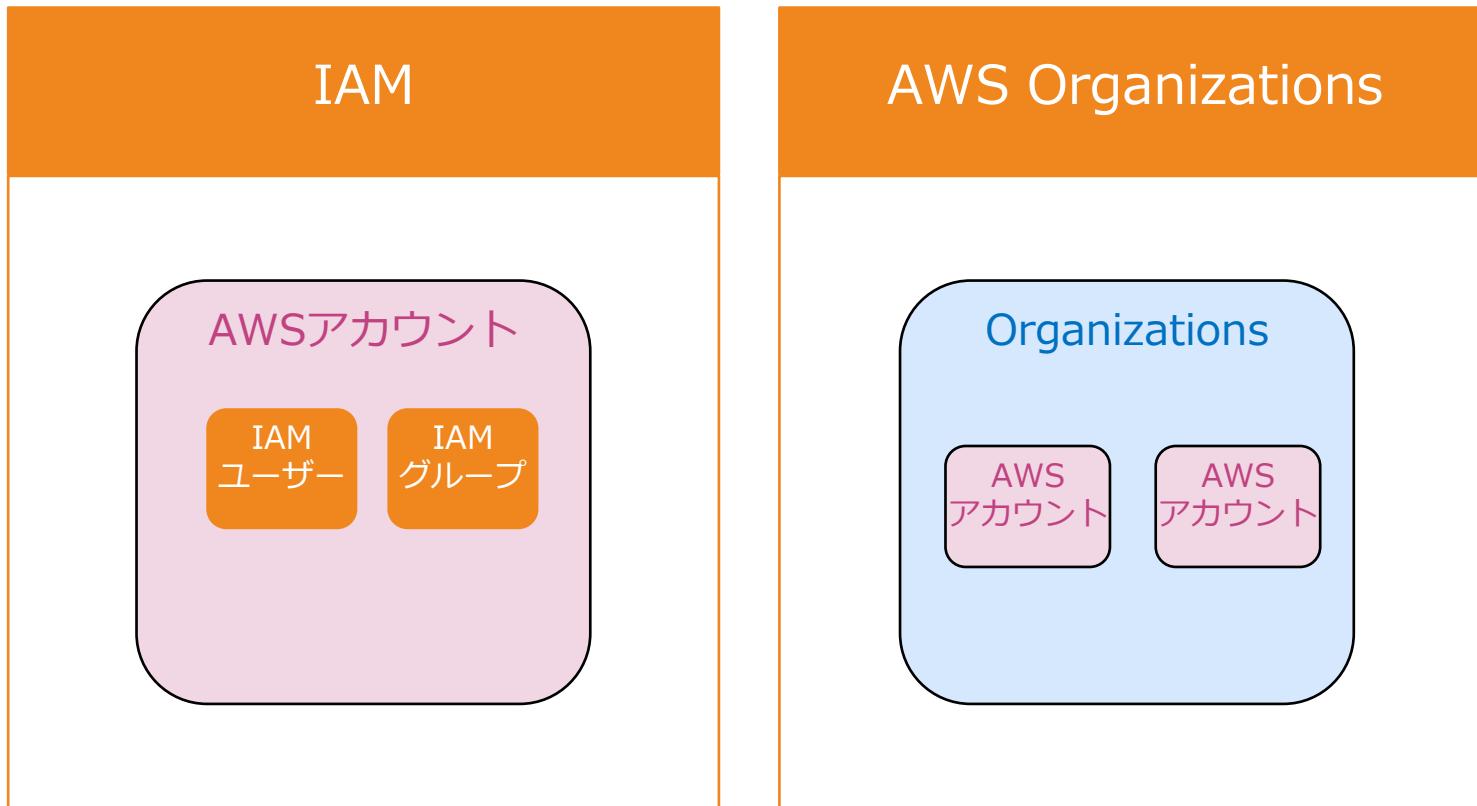
Temporary Security
Credentials

AWSに対して一時的な認証情報を生成する仕組み

IAMとAWS Organizations

IAMはAWSアカウント内のユーザー管理を実施。

Organizationsは複数のAWSアカウント自体の管理を実施。



AWS Organizations

AWS OrganizationsはIAMのアクセス管理を大きな組織でも楽に実施できるようにするマネージド型サービス

複数アカウントの一元管理

AWSアカウントをグループ化してポリシーを適用して一元的に管理する

新規アカウント作成の自動化

コンソール／SDK／CLIでAWSアカウントを新規作成して、作成内容をログ管理できる

一括請求

複数AWSアカウントの請求を一括化する

AWS Organizations

組織という単位を構成して、マスターアカウントがメンバーアカウントを管理するという仕組み

組織（一元管理対象）

管理者ルート

マスター
アカウント

組織ポリシー
サービス
管理ポリ
シー

組織単位 (OU)

組織単位 (OU)

メンバー
アカウント

CloudTrailの概要

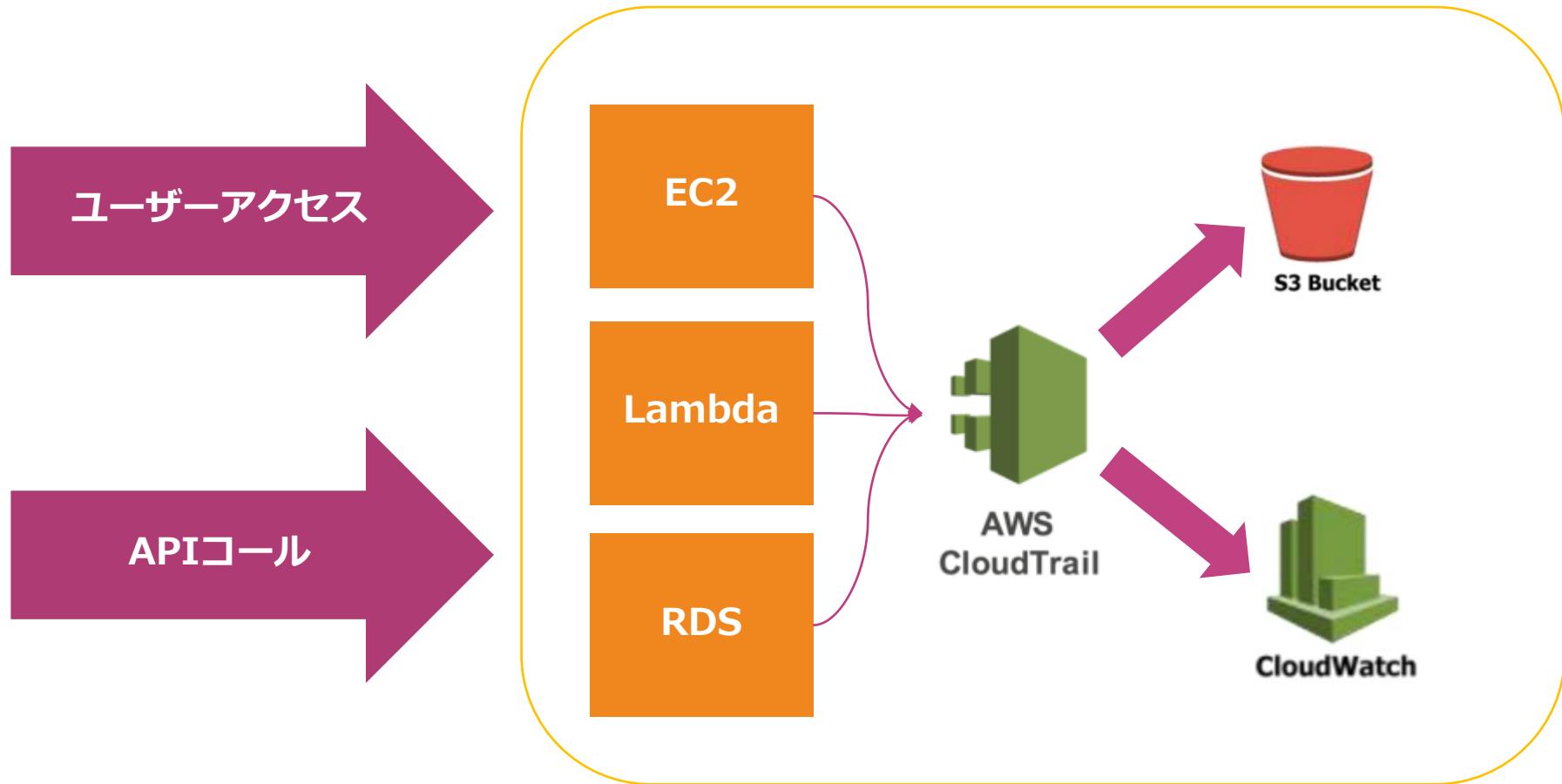
AWS CloudTrail

AWSユーザの操作（API操作やユーザのサインインアクティビティ）をロギングするサービス

- ルートアカウント/IAMユーザのオペレーションをトラッキングしてログを取得するサービス
- CloudTrail ログファイルは暗号化されてS3に保存
- KMSによる暗号化もサポート
- 無料

AWS CloudTrail

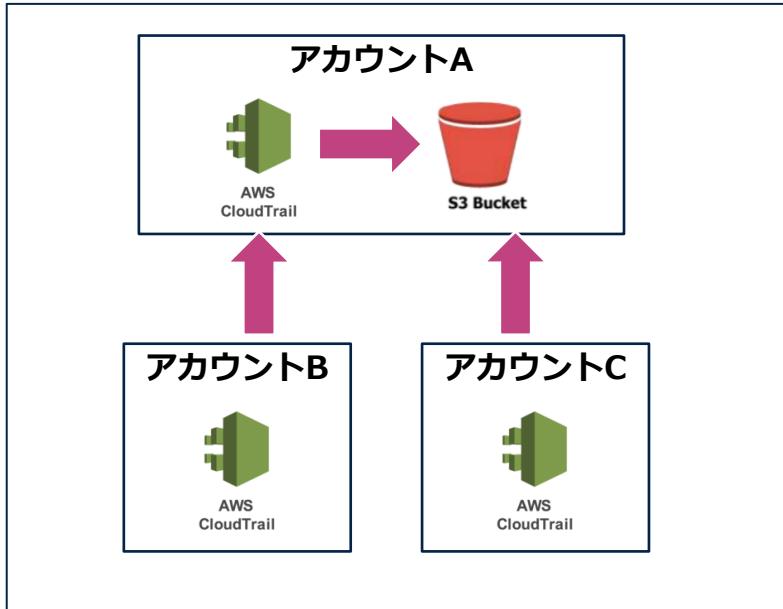
ユーザーアクセスとAPIコールのログ情報をS3バケットに保存し、CloudWatch上で解析できる。



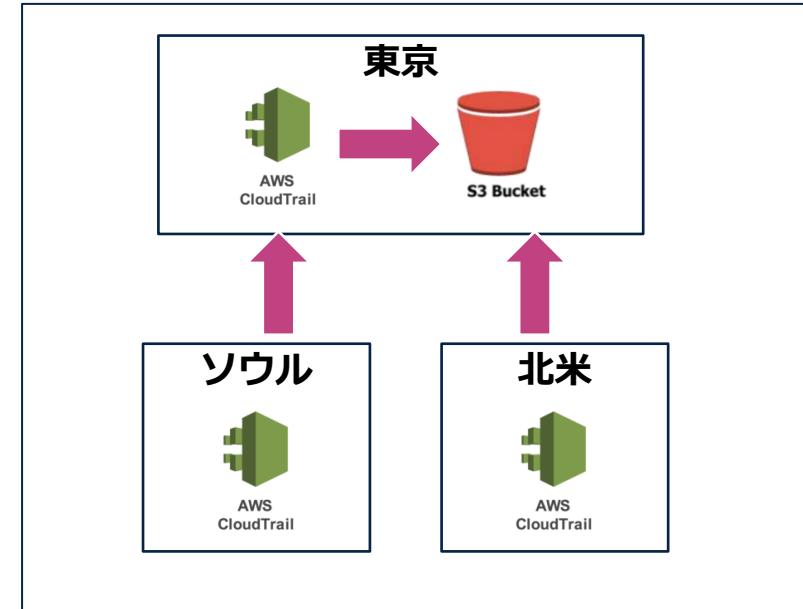
AWS CloudTrail

マルチアカウントで利用可能で、複数AWSアカウントの情報を集約可能

マルチアカウント



マルチリージョン



CloudWatchの概要

CloudWatch

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる



CloudWatch

AWSリソースとAWSで実行するアプリケーションのモニタリングサービスで、様々なログやメトリクスを監視できる

CloudWatch (メトリクス監視)

AWS上で稼働するシステム監視サービスで、死活監視、性能監視、キャパシティ監視を実施
有料枠では確認内容や設定の柔軟性が充実化する

CloudWatch Logs

CloudWatchと連動したログ管理プラットフォームサービス。EC2上のOS・アプリケーションのログやAWSマネジドサービスのログを取得する

CloudWatch Events

CloudWatchはAWSリソースに対するイベントをトリガーにアクションを実行。オペレーションの変更に応答し、応答メッセージ送信、機能のアクティブ化。変更、状態情報収集による修正アクションを実行する

CloudWatch

CloudWatchメトリクスを利用して、多くのメトリクスを取得することが可能

標準メトリクス

- CPUUtilization／ディスク利用率／読み込みIOPSなど 一般的なメトリクスの多くが取得可能
- 5分間隔でのメトリクス取得

カスタムメトリクス (拡張モニタリング実行時)

- 標準では取得できないメトリクス
- 1秒から60秒でのリアルタイムでのメトリクス取得

CloudWatchダッシュボード

必要なRDSのメトリクスを選択してダッシュボードで可視化することが可能



拡張モニタリングの実施

DB インスタンスが実行されているオペレーティングシステム (OS) のリアルタイムのメトリクスを取得できる。

- ✓ 50種類以上のOSメトリクスを利用可能
- ✓ 1秒から60秒間隔でメトリクスを取得可能（標準は5分）
- ✓ 取得したメトリクスはCloudWatch Logs に保存される。
- ✓ 料金は、Amazon CloudWatch Logs に示された無料利用枠を超えた拡張モニタリングに対してのみ発生
- ✓ 拡張モニタリングはdb.m1.small を除くすべての DB インスタンス クラスに使用できます。
- ✓ APIコール時のスロットリング対策

CloudWatchアラーム

CloudWatchアラームにより、特定のメトリクスのしきい値に応じたアラーム通知や自動アクションを実行可能

メトリクス

CloudWatchに発行された時系列のデータポイントをセットのこと
リージョンごとのメトリクスを取得

名前空間

CloudWatchメトリクスのコンテナのこと
異なる名前空間のメトリクスは相互に分離される。

ディメンジョン

メトリクスを一意に識別する名前／値のペア
(例：Instancedid = i-123948576)

AWSコスト管理

レクチャー

レクチャーで学ぶ内容

コスト最適化の概要

コスト最適化の概念を説明し、AWSのコスト最適化に利用可能なサービスやツールを一通り確認します。

請求ダッシュボードの確認

AWSアカウントの請求情報やツールを利用できる請求ダッシュボードを一通り確認します。

AWSのコストと使用状況 レポートの活用

AWSのコストと使用状況の一覧を抽出するための設定方法を確認します。

コストカテゴリーの活用

コストカテゴリーを利用して細分化してコストを確認するための手順を確認します。

コスト配分タグの活用

コスト配分タグを設定して、タグに応じた使用状況レポートの抽出を実施します。



AWSコスト管理

レクチャー	レクチャーで学ぶ内容
AWS Cost Explorer の活用	AWSのコスト状況を可視化して、様々な切り口でグラフ表示させる方法を確認します。
AWS Budgetsの設定	AWSリソースに対する予算設定を行い、閾値に基づいてアクションを実施する設定を行います。
AWS Budgets report の設定	予算設定に基づいてレポートを配信する設定を行います。
AWS Pricing Calculator の活用	AWSの見積もりツールを利用して、リソースの見積もりを実施します。



コスト最適化



5つの設計原則と11のベストプラクティ

信頼性

スケーラビリティの確保

単一障害点
の排除

コンポーネント
の疎結合

環境の自動化

パフォーマンス 効率

キャッシュ
の利用

増大するデータ
量対応

最適なデータ
ベース選択

サーバーではな
くサービス

使い捨て
リソースの使用

安全性

セキュリティ
の確保

コスト最適化

コスト最適化

運用の優秀性

環境の自動化



Cost Optimization : コスト最適化

不必要的リソースを削減し、最適な料金選択によりコストを最適化すること

【設計事項】

- ✓ 不必要なリソース削減
- ✓ 透明性のある費用賦課
- ✓ マネージド型サービスの利用によるコスト削減
- ✓ 固定の償却コストを変動コストへと転換
- ✓ スケールによるコストメリット
- ✓ データセンターへの投資不要化



コスト最適化の主要サービス

需要と供給
の一一致

Auto
Scaling

コスト効率
の高いリソース

EC2
購入方式

Trusted
Advisor

支出の認識

Cloud
Watch

見積もり
ツール

継続した
最適化

AWS
最新情報

Trusted
Advisor



AWSを安く使う

最もシンプルで一番最初にやるべきコスト最適化は無料利用枠
の最大利用と最適な料金オプションの選択

AWSの無料利用枠

最適な料金
オプションを選択



AWSの無料利用枠

AWSでは3種類の無料利用枠が提供されている。

オファーの種類

無料利用枠を活用して100を超えるサービスを試し、AWSで構築を開始しましょう。ご使用の製品によって、3種類の異なる無料オファーをご利用いただけます。下のアイコンをクリックすると、キャンペーン情報が表示されます。



無料トライアル

短期の無料トライアルは、特定のサービスをアクティベートした日から開始されます



12か月間無料

AWSに最初にサインアップした日から12か月間、これらのサービスをご利用いただけます



常に無料

これらの無料利用枠に有効期限はなく、AWSのすべてのお客様が利用可能です

参照：<https://aws.amazon.com/free>



AWSの無料利用枠

無料利用枠の期間であっても、利用される時間や量に応じて制限が設けられており、超過すると課金される。

コンピューティング	ストレージ	データベース
無料利用枠 Amazon EC2 750 時間 /月 クラウド内でサイズ変更可能なコンピューティング性能。 リージョンに応じて、750 時間/月の Linux、 ▼	無料利用枠 Amazon S3 5 GB の標準ストレージ 安全性と耐久性を持つスケーラブルなオブジェクトストレージインフラストラクチャ。 ▼	無料利用枠 Amazon RDS 750 時間 /月の db.t2.micro データベース使用 (適用可能な DB エンジン) MySQL、PostgreSQL、MariaDB、Oracle BYOL または SQL Server のためのマネージド型リレーショナルデータベース ▼

参照 : <https://aws.amazon.com/free>



AWSの課金方式

AWSは利用量に応じた柔軟な価格設定となっている

従量課金	予約による低価格	使うほど安い
従量課金による利用料に応じた価格設定が基本	EC2などの特定のサービスにはリザーブド価格（予約による低価格販売）が実施されている。また、前払いをすることで更に割引が適用される。	AWS ではボリュームディスカウントを受けることができ、使用量が増えるほど節約できる



AWSの料金改定

他のクラウドサービスとの競争のため頻繁に料金改定がなされるため利用毎に料金表を確認することが基本

【日本語公式サイト】

<https://aws.amazon.com/jp/pricing/>



料金表を確認する

公式ページ・サービス料金表にて各サービスの料金を確認

サービス料金表



コンピューティング



ストレージ



データベース



移行



ネットワークとコンテンツ配信

Amazon EC2
クラウド内の仮想サーバー

Amazon Elastic Container Service
Docker コンテナを実行および管理

Amazon Elastic Container Registry
Docker イメージの保存と取得

Amazon Lightsail
仮想プライベートサーバーを起動および管理

AWS Batch
あらゆる規模でバッチジョブを実行

AWS Elastic Beanstalk
ウェブアプリの実行と管理

AWS Fargate
サーバーやクラスターの管理が不要なコンテナの使用

AWS Lambda
イベント発生時にコードを実行

Amazon Elastic Container Service for Kubernetes
マネージド型の Kubernetes を AWS で実行



開発者用ツール



管理ツール



メディアサービス



セキュリティ、アイデンティティ、コンプライアンス



分析



Machine Learning



モバイルサービス



AR とバーチャルリアリティ



アプリケーション統合



カスタマーエンゲージメント



ビジネスの生産性



デスクトップとアプリケーションのストリーミング



IoT



ゲーム開発



価格算定ツールを利用する

AWS公式ツールを利用して見積もりや価格比較を実施する

簡易見積りツール

利用するAWSサービスに対する月額料金を見積ることができます。

⇒[廃止に伴いAWS Pricing Calculatorに移行](#)

TCO計算ツール

AWS利用した場合とオンプレミス環境やコロケーション環境との価格比較ができます。

⇒[廃止に伴いAWS Pricing Calculatorに移行](#)

AWS料金見積り ツール (Pricing Calculator)

ビジネスや個人のニーズに沿った個別の予測コスト見積りを実施することができます。



AWS料金見積りツール (Pricing Calculator)

ビジネスや個人のニーズに沿った個別の予測コスト見積りを実施する新サービス

EC2 インスタンスの仕様 [情報](#)

オペレーティングシステム
Amazon EC2 インスタンスを実行するオペレーティングシステムを選択してください。

Linux

インスタンスタイプ
名前で検索するか要件を入力して、ニーズに合った最低コストのインスタンスを見つけます。

各インスタンスの最小要件を入力してください。
 名前でインスタンスを検索します。

vCPU: 4 削除
メモリ (GiB): 16 削除

[要件を追加](#)

入力に基づいて、これは最も低いコストの EC2 インスタンスです。

t4g.xlarge

オンデマンドの 1 時間あたりのコスト 0.1728	vCPU 4	GPU NA
1 年間のスタンダードリザーブの 1 時間あたりのコスト 0.1088	メモリ (GiB) 16 GiB	ネットワークパフォーマンス Up to 5 Gigabit

数量
必要な Amazon EC2 インスタンスの数を入力する。
1

使用率
Amazon EC2 インスタンスの予想使用量を入力します。オンデマンド料金戦略が選択されている場合にのみ適用されます。
100 使用率 (%) /月



AWS料金見積りツール (Pricing Calculator)

ビジネスや個人のニーズに沿った個別の予測コスト見積りを実施する新サービス

Amazon EC2 見積り

Amazon Elastic Block Storage (EBS) の料金 (monthly)	3.60 USD
Amazon EC2 Instance Savings Plans のインスタンス (monthly)	79.42 USD
合計月額コスト:	83.02 USD

[キャンセル](#) [見積りに追加](#)



My Estimate [編集](#) [共有](#)

前払いコスト 0.00 USD	1ヶ月あたりのコスト 83.02 USD	合計 12ヶ月間のコスト 996.24 USD
--------------------	-------------------------	-----------------------------------

AWS の開始方法

[お問い合わせ](#) [コンソールへサインイン](#)

Services (1)

Amazon EC2 リージョン: アジアパシフィック (東京)	編集 アクション ▾
クイック見積り	
オペレーティングシステム (Linux), 数量 (1), 價格戦略 (EC2 Instance Savings Plans 1年 前払いなし), ストレージ量 (30 GB), インスタンスタイプ (t4g.xlarge)	毎月: 83.02 USD



EC2の購入オプション

EC2の購入オプションは利用形態や利用期間などに応じて多岐にわたるため、コスト最適な選択をすることが重要

- オンデマンドインスタンス
- スポットインスタンス
- リザーブドインスタンス
- ハードウェア専有インスタンス
- Dedicated Host
- ベアメタル



EC2のリザーブドインスタンス

利用期間を長期指定して利用する形式で、オンデマンドに比較して最大72%割安になる

	スタンダード	コンバータブル
利用期間	1年 (40%割引) 3年 (60%割引)	1年 (31%割引) 3年 (54%割引)
AZ／インスタンスサイズ／ネットワークタイプ変更可否	有	有
インスタンスファミリー／OS／テナント／支払オプションの変更可否	なし	有
リザーブドインスタンスマーケットプレイスでの販売可否	可能	今後となる可能
ユースケース	<ul style="list-style-type: none">□ 一定した状態または使用量が予測可能なワークフロー□ 災害対策などキャパシティ予約が可能なアプリケーション	



EC2のスポットインスタンス

予備のコンピューティング容量を、オンデマンドインスタンスに比べて割引（最大90%引き）で利用できるEC2インスタンス

- 予備用を入札式で利用するためとても安い（最大90%引き）
- 起動に通常よりも少し時間がかかる
- 予備用のため途中で削除される可能性がある
⇒一時的な拡張などの用途で利用



物理対応可能なインスタンス

物理サーバーにインスタンスを起動して制御が可能なタイプのインスタンス

ハードウェア専有インスタンス

- ✓ 専用HWのVPCで実行されるEC2インスタンス
- ✓ ホストHWのレベルで、他のAWSアカウントに属するインスタンスから物理的に分離する
- ✓ 同じAWSアカウントのインスタンスとはHWを共有する可能性がある

Dedicated Host

- ✓ EC2インスタンス容量を完全にお客様専用として利用できる物理サーバー
- ✓ サーバーにバインドされた既存のソフトウェアライセンスを利用可能

Bare Metal

- ✓ アプリケーションは基盤となるサーバーのプロセッサーとメモリーに直接アクセス可能なインスタンス
- ✓ AWSの各種サービスとの連携が可能でOSが直接下層のハードウェアにアクセス可能



Savings Plans

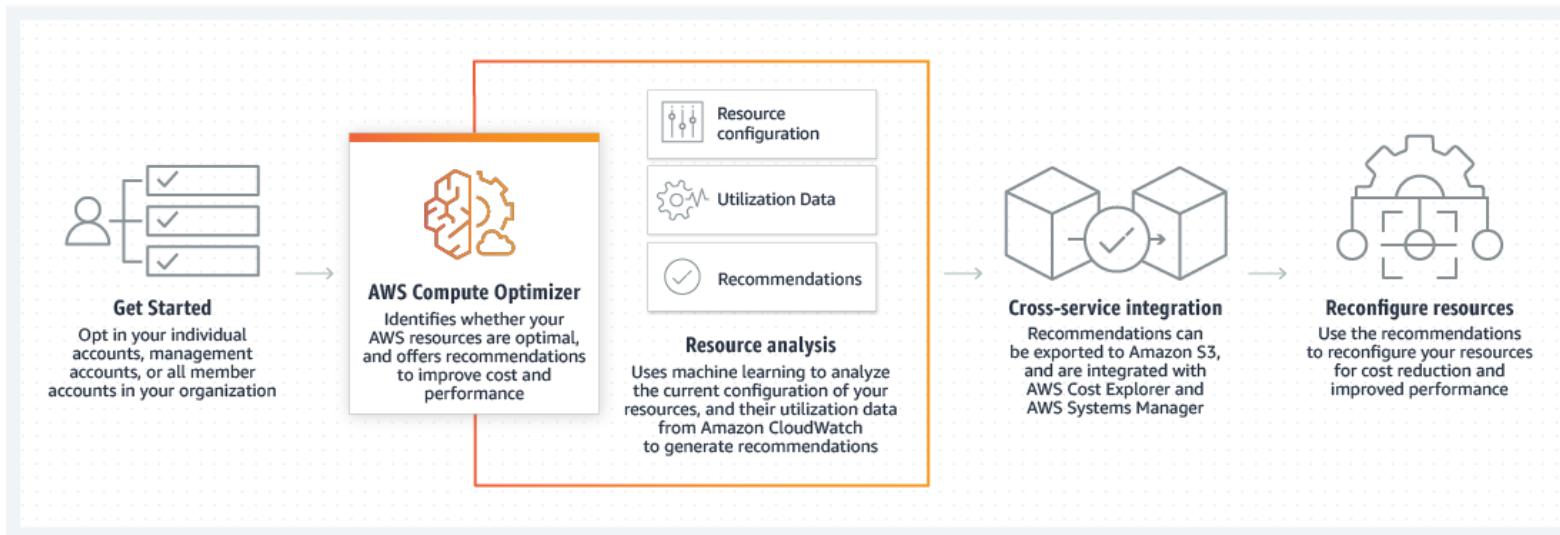
1~3 年の期間に一定の使用量を守ることによりコストを削減

- リザーブドインスタンスと同様に、1 年または 3 年の期間に特定の量の処理能力 (USD/時間で測定) を使用する契約を結ぶことで適用される割引契約
- AWS コンピューティング使用料金を最大 72% 節約できる
- Amazon EC2、AWS Fargate、AWS Lambda に適用可能



AWS Compute Optimizer

使用率データに基づいて、EC2インスタンスタイプ、EBSボリュームおよびLambda 関数の最適な設定を選択できる。最大25%コスト削減を実施



参照 : <https://aws.amazon.com/jp/compute-optimizer/?track=costma>



コスト最適化の主要サービス

ユースケース	機能	AWS のリソース
整理する	独自のタグ付け戦略で、コスト配分とガバナンスの基盤を構築する	AWS コスト配分タグ AWS Cost Categories
レポート	詳細かつ割り当て可能なコストデータを使用して、クラウド支出の認識と説明責任を高める	AWS Cost Explorer AWS のコストと使用状況レポート AWS Application Cost Profiler
アクセス	統合的な表示で組織全体の請求情報を追跡	AWS 一括請求 AWS Purchase Order Management AWS クレジット
管理	適切な枠組みを設定して効果的なガバナンスメカニズムを確立	AWS Cost Anomaly Detection AWS Identity and Access Management AWS Organizations AWS Control Tower AWS Service Catalog
予測	作成した予測ダッシュボードを使用して、リソース使用率と支出を見積る	AWS Cost Explorer (セルフサービス) AWS Budgets (イベント駆動)
予算	予算のカスタムしきい値と自動アラート通知により支出を管理	AWS Budgets AWS Budget Actions AWS Service Catalog
購入	ワークフローのパターンとニーズに基づいて、無料トライアルとプログラムによる割引を活用する	AWS 無料利用枠 AWS リザーブドインスタンス AWS Savings Plans AWS スポットインスタンス Amazon DynamoDB オンデマンド
伸縮性	予想される使用パターンとニーズに基づいて、サービスをスケーリングおよびスケジューリングする	AWS Instance Scheduler Amazon Redshift の一時停止と再開 EC2 Auto Scaling AWS Trusted Advisor
適切なサイズ設定	サービスの割り当てサイズを実際のワークフローの需要に合わせる	AWS Cost Explorer の適切なサイズ設定に関する推奨事項 AWS Compute Optimizer Amazon Redshift のサイズ変更 Amazon S3 Intelligent Tiering
検査	リソースのデプロイとコスト最適化を常に最新の状態にする	AWS Cost Explorer

参照:<https://aws.amazon.com/jp/aws-cost-management/>



整理：AWSコスト配分タグ

タグごとに使用量とコストをグループ化したコスト配分レポートを生成することができる。

ユーザー定義のコスト配分タグ (1/8) 情報

タグキー

タグキー	ステータス
AWSNetworkFirewallManaged	非アクティブ
CreatedBy	非アクティブ
Description	非アクティブ
Ec2ImageBuilderArn	非アクティブ
Firewall	アクティブ
Name	非アクティブ
description	非アクティブ
sqlworkbench-resource-owner	非アクティブ



Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal



整理 : AWS Cost Categories

コストと使用量をチーム、コストセンター、地域、用途、その他の組織構造とコスト配分の必要性に応じて正確に分類できる

Cost Categories

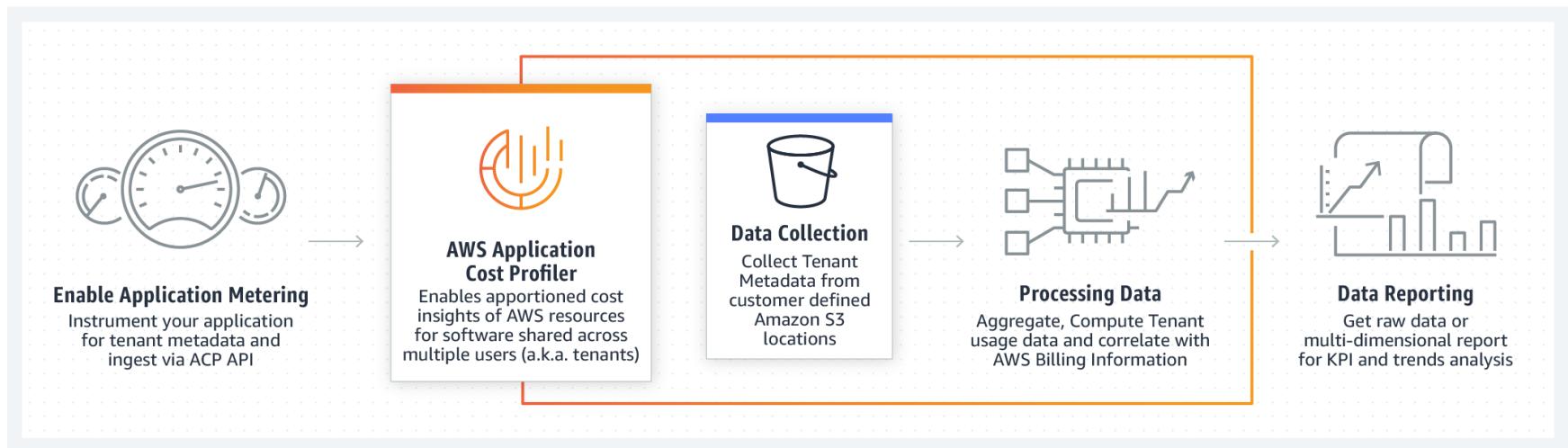
Cost Categories automatically categorizes your cost information into custom groups. [Learn more](#)

Cost categories (4)			
<input type="text"/> Filter categories			
Cost category	▲	Number of rules	▼
○ AccountGroup		5	Explore category costs View in AWS Cost Explorer
○ Application		5	Explore category costs View in AWS Cost Explorer
○ Department		4	Explore category costs View in AWS Cost Explorer
○ Project		7	Explore category costs View in AWS Cost Explorer



レポート : AWS Application Cost Profiler

アプリケーションによって使用される共有 AWS リソースの消費を追跡し、全体の詳細なコスト内訳をレポートする。



参照: <https://aws.amazon.com/jp/aws-cost-management/aws-application-cost-profiler/?track=costma>



レポート：コストと使用状況レポート

AWS のコストと使用状況に関する最も包括的データを提供

アカウント/IAMユーザーが使用した各サービスカテゴリのAWS使用状況が、時間単位または日単位の明細項目として一覧表示する。

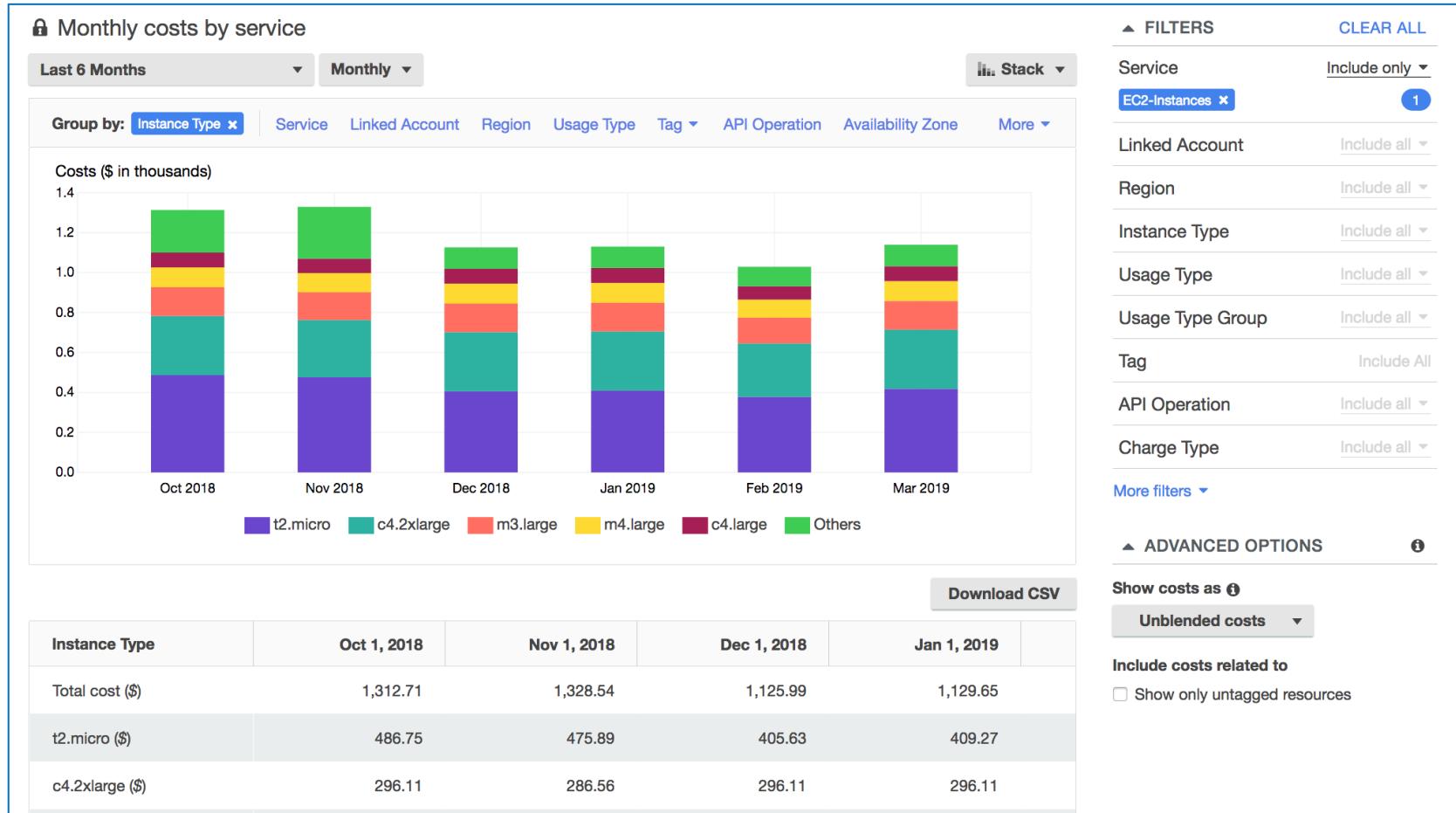
M	N	O	P	R	S	T	
1	lineItem/ProductCode	lineItem/UsageType	lineItem/Operation	lineItem/AvailabilityZone	lineItem/UsageAmount	lineItem/CurrencyCode	lineItem/LineItemDescription
2	AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
3	AmazonS3	Requests-Tier1	ListAllMyBuckets		2	USD	\$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier
4	AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
5	AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
6	AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
7	AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
8	AmazonEC2	USW2-USE1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.00 per GB - data transfer out under the monthly global free tier
9	AmazonEC2	USW2-USE1-AWS-In-Bytes	PublicIP-In		0.00000138	USD	\$0.00 per GB - US West (Oregon) data transfer from US East (Northern Virginia)
10	AmazonEC2	USW2-USW1-AWS-In-Bytes	PublicIP-In		0.00000149	USD	\$0.00 per GB - US West (Oregon) data transfer from US West (Northern California)
11	AmazonS3	Requests-Tier1	ListAllMyBuckets		2	USD	\$0.00 per request - PUT, COPY, POST, or LIST requests under the monthly global free tier
12	AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00038144	USD	\$0.00 per GB - data transfer out under the monthly global free tier
13	AmazonEC2	USW2-USW1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.00 per GB - data transfer out under the monthly global free tier
14	AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00030951	USD	\$0.00 per GB - data transfer in per month
15	AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
16	AmazonEC2	USW2-USW1-AWS-Out-Bytes	PublicIP-Out		0.00000349	USD	\$0.00 per GB - data transfer out under the monthly global free tier
17	AmazonEC2	USW2-USW1-AWS-In-Bytes	PublicIP-In		0.00000276	USD	\$0.00 per GB - US West (Oregon) data transfer from US West (Northern California)
18	AmazonEC2	APS2-EBS:VolumeUsage.gp2	CreateVolume-Gp2		0.01344086	USD	\$0.00 per GB-month of General Purpose (SSD) provisioned storage under monthly free tier
19	AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms
20	AmazonEC2	USW2-BoxUsage:t2.micro	RunInstances:0002	us-west-2a	1	USD	\$0.00 per Windows t2.micro instance-hour (or partial hour) under monthly free tier
21	AmazonEC2	USW2-DataTransfer-Regional-Bytes	PublicIP-Out		0.00000349	USD	\$0.00 per GB - regional data transfer under the monthly global free tier
22	AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00032071	USD	\$0.00 per GB - data transfer in per month
23	AmazonEC2	USW2-DataTransfer-Regional-Bytes	PublicIP-In		0.00000302	USD	\$0.00 per GB - regional data transfer under the monthly global free tier
24	AmazonEC2	USW2-USE1-AWS-Out-Bytes	PublicIP-Out		0.00000174	USD	\$0.00 per GB - data transfer out under the monthly global free tier
25	AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00045736	USD	\$0.00 per GB - data transfer out under the monthly global free tier
26	AmazonEC2	USW2-DataTransfer-In-Bytes	RunInstances		0.00036737	USD	\$0.00 per GB - data transfer in per month
27	AmazonEC2	USW2-APN2-AWS-In-Bytes	PublicIP-In		0.00000005	USD	\$0.00 per GB - US West (Oregon) data transfer from Asia Pacific (Seoul)
28	AmazonEC2	USW2-APN2-AWS-Out-Bytes	PublicIP-Out		0.00000018	USD	\$0.00 per GB - data transfer out under the monthly global free tier
29	AmazonEC2	USW2-USE1-AWS-In-Bytes	PublicIP-In		0.00000153	USD	\$0.00 per GB - US West (Oregon) data transfer from US East (Northern Virginia)
30	AmazonEC2	USW2-DataTransfer-Out-Bytes	RunInstances		0.00039945	USD	\$0.00 per GB - data transfer out under the monthly global free tier
31	AmazonEC2	CW:AlarmMonitorUsage	Unknown		0.00134409	USD	\$0.00 per alarm-month - first 10 alarms

<https://aws.amazon.com/jp/aws-cost-management/aws-cost-and-usage-reporting/>



検査・レポート：Cost Explorer

AWS のコストと使用量の経時的変化を可視化して、カスタムレポートを作成してコストと使用量のデータを分析する。



アクセス

AWSの請求関連の追跡や確認に利用するサービス

AWS一括請求	<ul style="list-style-type: none">■ 一括請求機能を使用して、複数の AWS アカウント の請求と支払いを統合して、追跡・管理することができる。■ 料金のボリューム割引、リザーブドインスタンスの割引、および Savings Plans を共有
AWS Purchase Order Management	AWSに対する発注書 (PO) を作成・管理するサービスで、複数の PO の管理を一元化できる。
AWSクレジット	AWS クレジットは、対象サービスに関連するコストを貯め、請求に適用される販促用クレジットで、クーポンのようなもの。



AWS Organizationsによる一括請求

AWS Organizationsの一括請求で、メンバーアカウント間でリザーブドインスタンスを共有化したり、S3などの利用量に応じた課金がお得になる。

ボリュームディスカウト適用

S3などのボリューム料金階層があるサービスの場合、多く利用するほど価格が低くなると



一括請求で複数アカウントをまとめてボリューム料金に統合することでコスト削減が可能

リザーブドインスタンスの共有

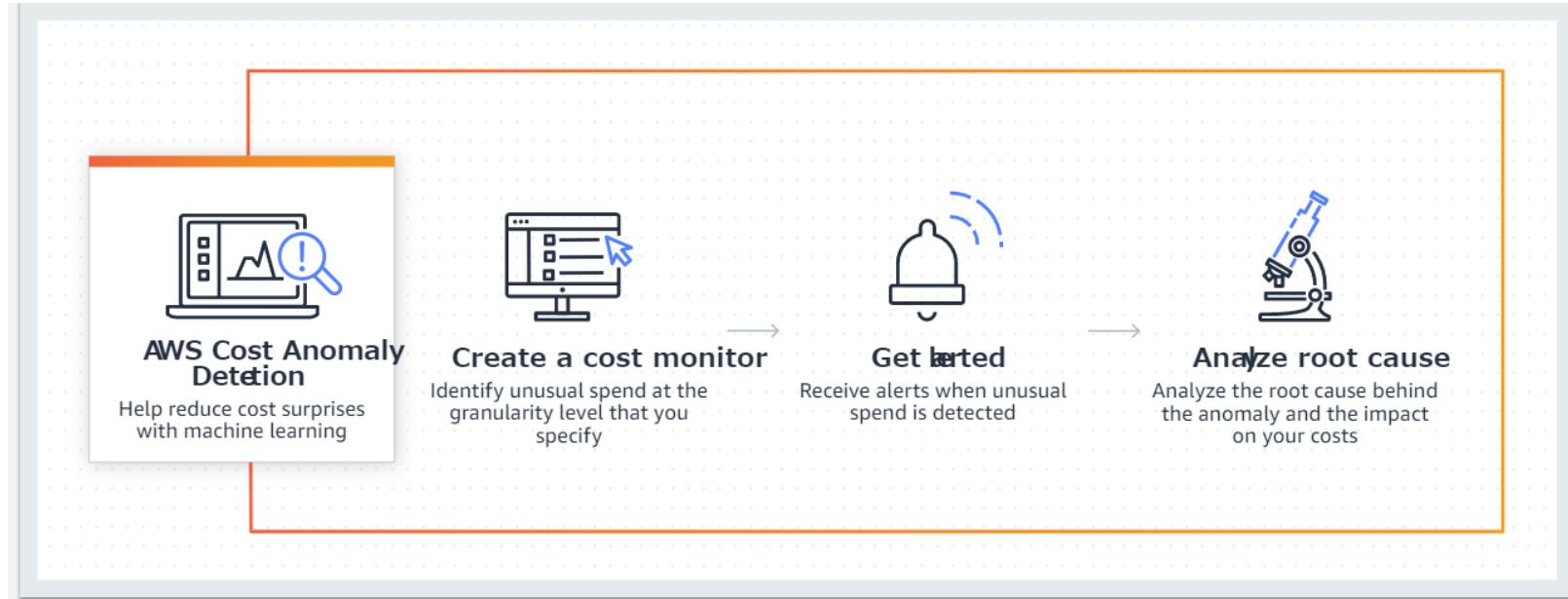
一定の条件においてメンバーアカウント間で購入したリザーブドインスタンスが共有される

- AWS Organizationsで有効化
- 同じAZ内に購入する
- 同じインスタンスタイプである



管理 : AWS コスト異常検出

機械学習により異常な支出と根本原因を特定して、想定外のコストが発生する回数を減らし、コントロールを強化する。



参照:<https://console.aws.amazon.com/cost-management/home?#/anomaly-detection/home>



管理 : CloudWatch

CloudWatchのbilling機能により請求額に対するアラーム設定が可能

Create Alarm

Billing Alarm

You can create a billing alarm to receive e-mail alerts when your AWS charges exceed a threshold you choose. Simply:

1. Enter a spending threshold
2. Provide an email address
3. Check your inbox for a confirmation email and click the link provided

When my total AWS charges for the month

exceed: \$ USD

send a notification to: [New list](#)

Reminder: for each address you add, you will receive an email from AWS with the subject "AWS Notification - Subscription Confirmation". Click the link provided in the message to confirm that AWS may deliver alerts to that address.

[showing simple options](#) | [show advanced](#)

Alarm Preview

This alarm will trigger when the blue line goes above the red line

EstimatedCharges ≥ 200

Date	EstimatedCharges (USD)
10/25 00:00	120
10/27 00:00	130
10/29 00:00	140

More resources

[AWS Billing console](#)
[Getting started with billing alarms](#)
[More help with billing alarms](#)
[AWS Billing FAQs](#)

[Cancel](#) [Previous](#) [Next](#) **Create Alarm**



予算 : AWS Budgets

カスタム予算を設定して、コストまたは使用量が予算額や予算量を超えた場合に細かくアラームを設定することができる。

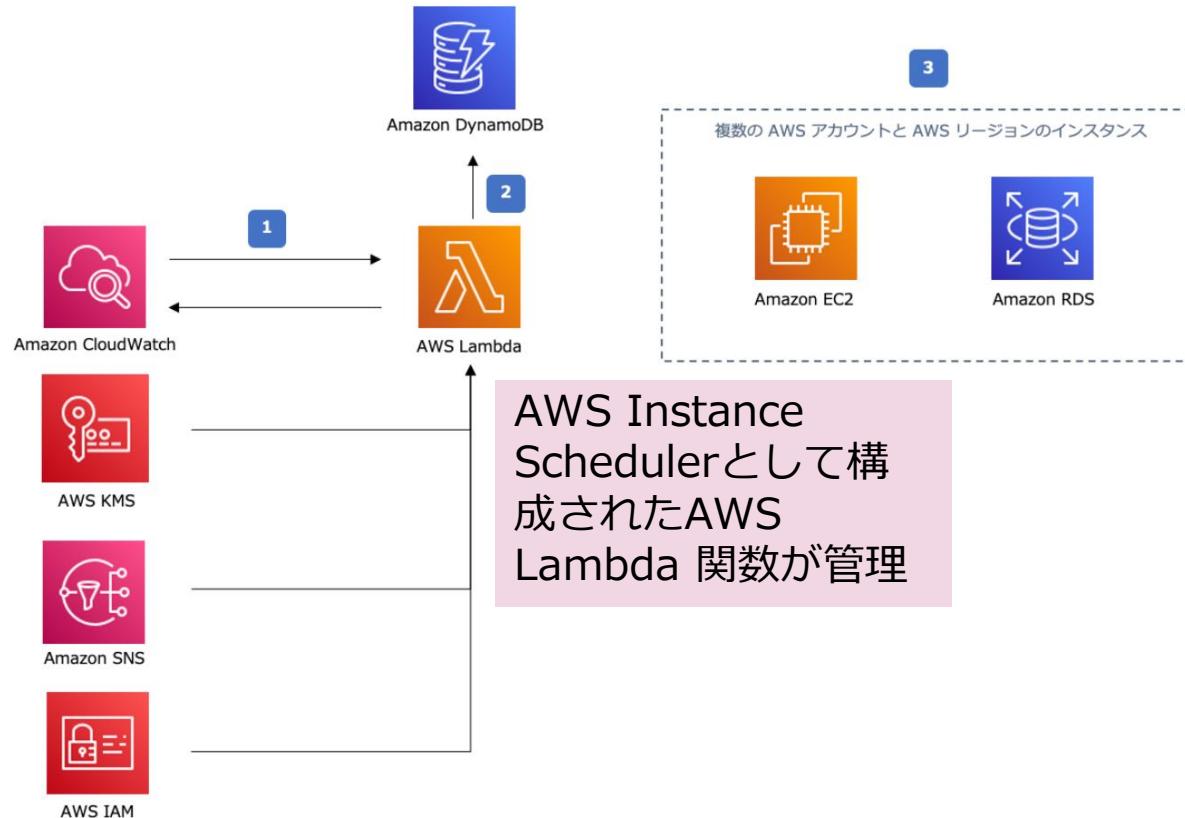
AWS Budgets								?
Filter by budget name						Download CSV		Create budget
All budgets (7)	Cost budgets (5)	Usage budgets (2)	Reservation budgets (0)					
Budget name	Budget type	Current	Budgeted	Forecasted	Current vs. budgeted	Forecasted vs. budgeted		
Project Nemo Cost Budget	Cost	\$43.90	\$45.00	\$56.33	<div style="width: 97.55%; background-color: #0070C0;"></div> 97.55%	<div style="width: 125.17%; background-color: #E74C3C;"></div> 125.17%	...	
Eastern US Regional Budget	Cost	\$85.21	\$100.00	\$125.28	<div style="width: 85.21%; background-color: #0070C0;"></div> 85.21%	<div style="width: 125.28%; background-color: #E74C3C;"></div> 125.28%	...	
Total Monthly Cost Budget	Cost	\$141.50	\$175.00	\$187.00	<div style="width: 80.86%; background-color: #0070C0;"></div> 80.86%	<div style="width: 106.86%; background-color: #E74C3C;"></div> 106.86%	...	
Total EC2 Cost Budget	Cost	\$136.90	\$200.00	\$195.21	<div style="width: 68.45%; background-color: #0070C0;"></div> 68.45%	<div style="width: 97.61%; background-color: #0070C0;"></div> 97.61%	...	
S3 Usage Budget	Usage	3,601 Requests	5,500 Requests	4,675.75 Requests	<div style="width: 65.47%; background-color: #0070C0;"></div> 65.47%	<div style="width: 85.01%; background-color: #0070C0;"></div> 85.01%	...	
Monthly DataTransfer Usage Budget	Usage	2.28 GB	4 GB	3.07 GB	<div style="width: 57.05%; background-color: #0070C0;"></div> 57.05%	<div style="width: 76.63%; background-color: #0070C0;"></div> 76.63%	...	
Quarterly Budget	Cost	\$133.10	\$550.00	\$516.10	<div style="width: 24.2%; background-color: #0070C0;"></div> 24.2%	<div style="width: 93.84%; background-color: #0070C0;"></div> 93.84%	...	

<https://aws.amazon.com/jp/aws-cost-management/aws-budgets/>



伸縮性 : AWS Instance Scheduler

EC2および RDSインスタンスの開始スケジュールと停止スケジュールを設定して、AWS リソースコストを管理する



参照 : <https://aws.amazon.com/jp/solutions/implementations/instance-scheduler/>



セクションの内容

レクチャー	レクチャーで学ぶ内容
コンピューティング	サーバーなどのシステム実行に利用するコンピューティング関連のAWSサービスを確認します。
ストレージ	データ保存に利用するストレージ関連のAWSサービスを確認します。
ネットワーキングと コンテンツ配信	VPCやRoute53以外のネットワークや配信関連のAWSサービスを確認します。
データベース	データ分析やデータ処理に利用するデータベース関連のAWSサービスを確認します。
アイデンティティ・セキュリティ・コンプライアンス	セキュリティやコンプライアンスに関連するAWSサービスを確認します。

セクションの内容

レクチャー	レクチャーで学ぶ内容
マネジメントとガバナンス	CloudWatchとCloudTrail以外の主要な運用管理に利用するAWSサービスを確認します。
アプリケーション統合	アプリケーション構築時のコンポーネント間連携に利用するAWSサービスを確認します。
移行と移転	AWSクラウドへと移行する際に利用するAWSサービスを確認します。
その他のサービス	これまでの主要分野以外に試験範囲にたまに出題されるようなサービスを確認します。

コンピューティング

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

コンピューティング

アプリケーションを構築する際にサーバーなどのコンピューティングを起動・実行する関連サービス

Amazon EC2	AWSを利用して仮想サーバーを立ち上げるサービス ELB／AutoScaling／セキュリティグループも必須
AWS Lambda	サーバレスでプログラミングコード処理を実行するサービス
Amazon Lightsail	仮想サーバー、ストレージ、データベース、およびネットワーキングを予測可能な低価格で提供
Amazon Elastic Container Service (ECS)	Docker コンテナをサポートする拡張性とパフォーマンスに優れたコンテナオーケストレーションサービス

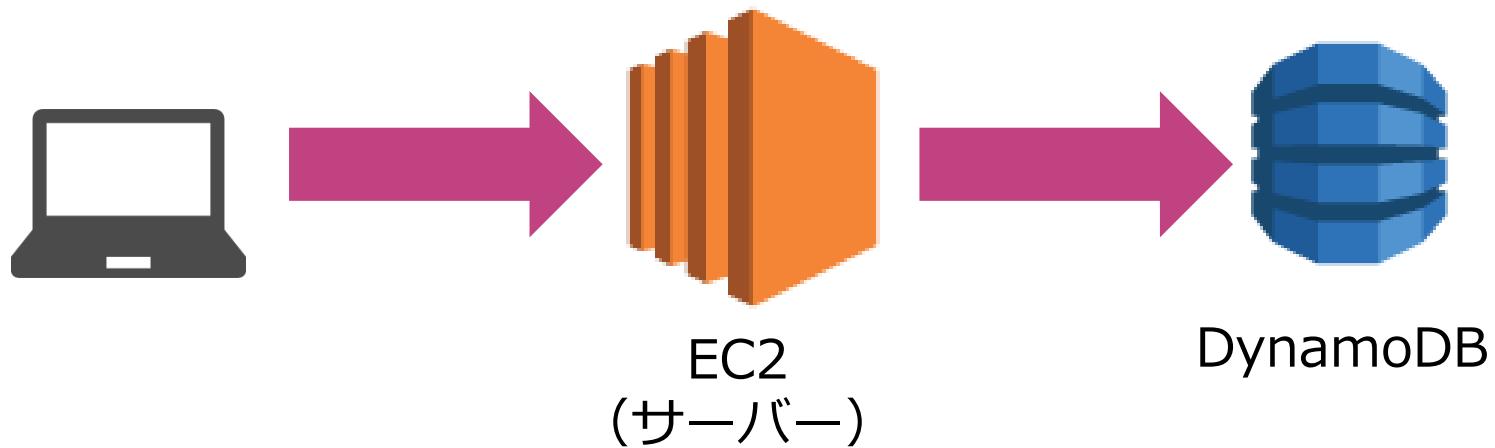
Lambda

インフラを気にすることなくアプリケーションコードを実行できるデータ処理サービス



Lambda

クライアントからのアクセスに対してデータを登録する単純な処理をEC2インスタンスに実行させていれば



Lambda

Lambdaに置き換えてサーバレスに実行処理することが可能



Lambdaの特徴

サーバレスによりEC2インスタンスの代わりコードを実行することで効率的なアーキテクチャを実現する

- 実行基盤は全てAWSが管理
- AWSサービスと連携させることで簡単にイベントドリブンなアプリケーションを実装可能
- Node.js/Javaで書かれたコードを実行
- 100ミリ秒単位でコード実行時間に対しての課金でありコスト効率が非常に高い
- オートスケール

Lambdaの仕組み

利用方法もシンプルでWEBアプリやモバイルアプリから簡単に利用可能

Lambdaファンクションを用意する
(コーディング)

アプリからLambdaを呼び出す

Amazon Lightsail

秒単位で簡単にWEBサーバー構成を実現することができるサーバーフルセットを提供するVPSサービス

Lightsail

- 簡易的に小規模のアプリケーションやWEBサイトを構築するために利用するVPSを立ち上げる
- サーバー／ストレージ／ネットワーク／スナップショット、ロードバランサー機能、ファイアウォール、DNS機能などいくつもの機能が予め揃ったオールインワンで利用することが可能

EC2

- 仮想サーバーを立上げて、クラウド上で利用するサービス。小規模なWEBサーバーとしても大規模システム用のサーバーとしても利用可能
- ネットワーク、ストレージ、DNSなどは他のAWSサービスを構築してアーキテクチャを構成することが必要となる。

Amazon Lightsailのユースケース

小規模WEBサイトやアプリケーションを構築する際や、スモールスタートする際はLightsailが利用可能

Lightsail

- シンプルなWEBサイトを構築する。
- 小規模なアプリケーションを構築する。
- テスト・開発環境で一時的に利用する。
- 社内ツールや小規模なビジネス用ソフトウェアウェアを起動する際に利用する。
- スモールスタートでアプリ開発を実施する際に利用する。

EC2

- 小規模アプリケーションを構築する。
- 複数台／複数レイヤーに及ぶ多層アーキテクチャを構成する際に利用する。
- 複数AZにAutoScalingする冗長性の高い構成を実現する。
- データ処理やビッグデータ分析用のインスタンスとして処理を実行する。
- 厳密な運用監視によって大規模システムを構築する際に利用する。

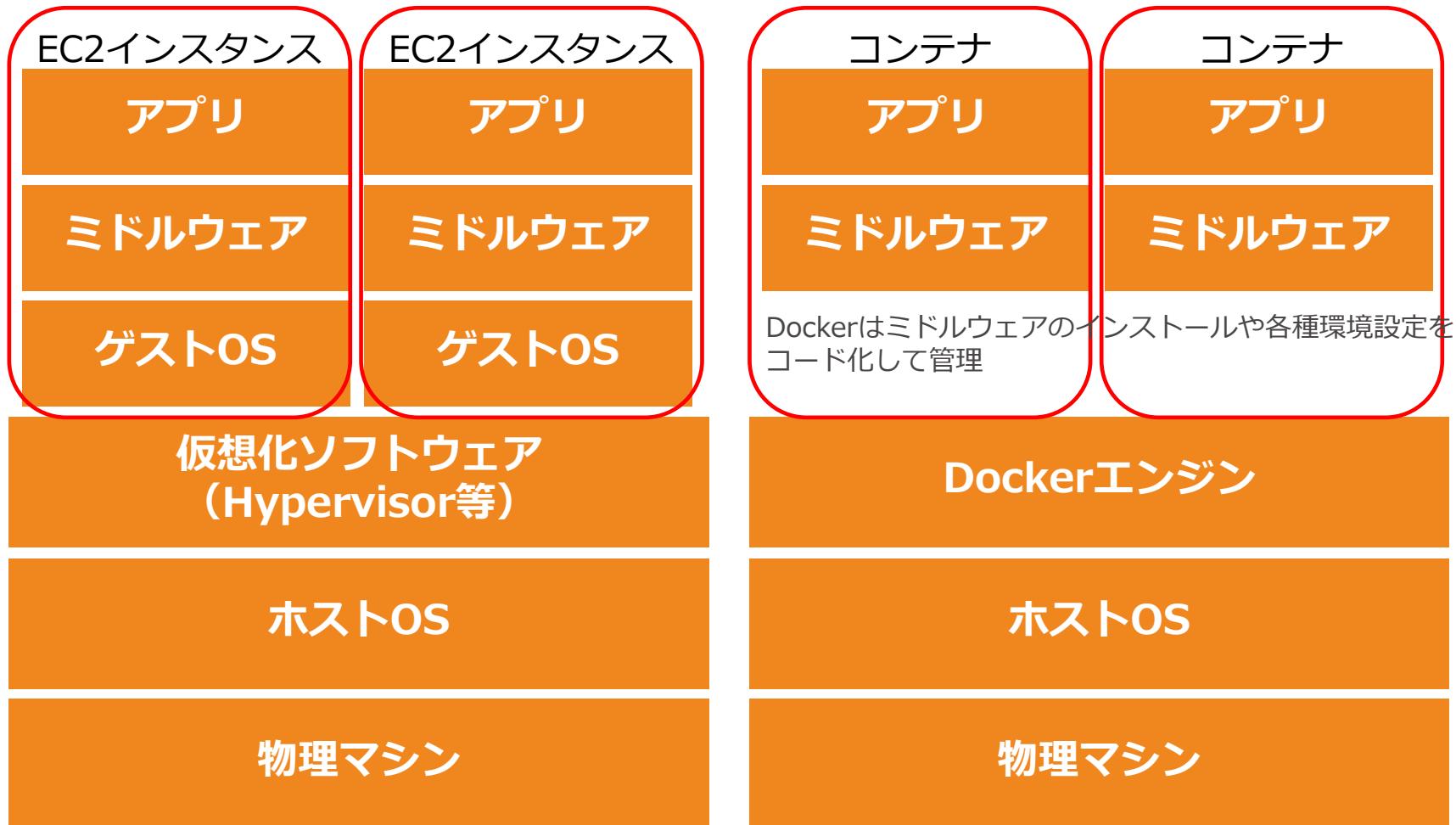
Amazon Lightsail

性能に応じた7つの利用プランから選択して利用可能。オールインワンで値段が設定されており、イメージがつきやすい。

最初の1か月無料!							>
\$3.5 USD	\$5 USD	\$10 USD	\$20 USD	\$40 USD	\$80 USD	\$160 USD	
\$3.50 USD	\$5 USD	\$10 USD	\$20 USD	\$40 USD	\$80 USD	\$160 USD	月次料金
512 MB	1 GB	2 GB	4 GB	8 GB	16 GB	32 GB	メモリ
1 vCPU	1 vCPU	1 vCPU	2 vCPU	2 vCPU	4 vCPU	8 vCPU	処理中
20 GB の SSD	40 GB の SSD	60 GB の SSD	80 GB の SSD	160 GB の SSD	320 GB の SSD	640 GB の SSD	ストレージ
1 TB	2 TB	3 TB	4 TB	5 TB	6 TB	7 TB	転送

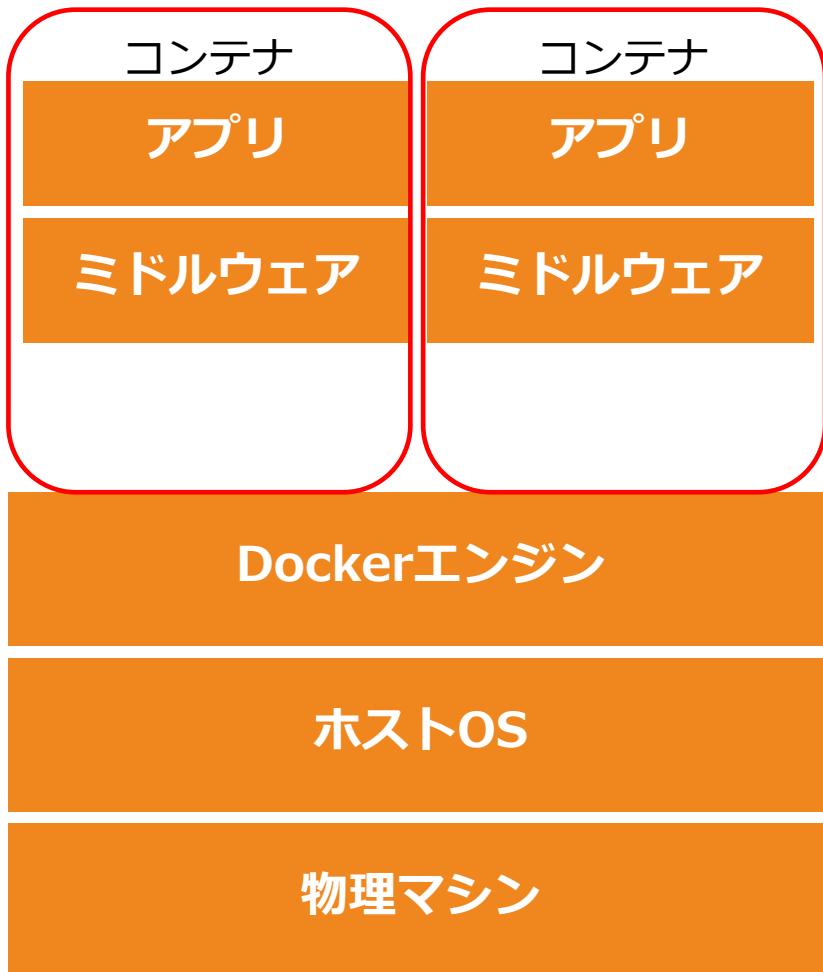
コンテナ

コンテナはホストマシンのカーネルを利用し、プロセスやユーザなどを隔離する仮想化方式



Docker

Dockerはコンテナ型の仮想環境を作成、配布、実行するためのプラットフォーム



- ✓ コンテナはホストマシンのカーネルを利
用し、プロセスやユーザなどを隔離する
- ✓ Dockerはミドルウェアのインストールや
各種環境設定をコード化して管理

1. コード化されたファイルを共有するた
め誰でも同じ環境構築が容易に可能
2. 作成した環境を配布共有が容易
3. 環境の即時構築・削除が容易なため、
CI/CDによる開発ができる

Amazonのコンテナサービス

AWSでDockerを実現するための関連サービスはECR／ECS／EKSとFargateの4タイプ

レジストリ

コンテナエンジンに実行されるイメージが保管される場所

Amazon ECR

コントロール プレーン

コンテナを管理するサービス

Amazon ECS
Amazon EKS

データプレーン

コンテナが実行される環境

AWS Fargate

ユースケース分け

ユースケースに応じた使い分けを理解して、実際の試験問題に対応できるようにする。

Amazon EC2	仮想サーバーを単体で利用してアプリケーションを一から構成することや、大規模インフラを構成する場合に利用する。
AWS Lambda	単発のジョブなどのシステム処理をサーバレスでコスト最適に実行する場合はEC2ではなくLambda関数を利用する。
Amazon Lightsail	安価にシンプルなWEBサイトやアプリを利用したい場合にはEC2 + EBS + Route53などを構成するよりもLightsail
Amazon Elastic Container Service (ECS)	環境構築を自動化しつつ、CI/CDを実現したい場合はDockerを利用する。

ストレージ

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

ストレージ

AWSにおいてデータを保存する際に利用する多様なストレージ

Amazon Simple Storage Service (S3)	スケーラビリティ、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクトストレージサービス
Amazon Elastic Block Store (EBS)	EC2にアタッチして利用する専用のブロックストレージ
Amazon Elastic File System (EFS)	AWS クラウドサービスおよびオンプレミスリソースで使用するための、シンプルでスケーラブル、かつ伸縮自在な完全マネージド型の NFS ファイルシステム
Amazon S3 Glacier	安全性と耐久性に優れ、きわめて低成本の Amazon S3 クラウドストレージクラスで、データのアーカイブや長期バックアップに使用する

EFS (Elastic File System)

複数のEC2インスタンスからアクセス可能な共有ストレージ

S3

- オブジェクトストレージでリージョンに設置
- HTTPによるAPI経由でアクセス
- 大容量のデータを長期保存するためのもの

EBS

- ブロックストレージでAZに設置
- EC2インスタンスのディスクボリュームとして利用するが、物理的ではなくネットワーク経由で利用
- 複数のEC2インスタンスにアタッチできない

EFS

- NASに似たファイルストレージ
- ファイルシステムとして利用し、複数のEC2インスタンスでの共有アクセスが可能
- S3と異なりインターネットから直接アクセスができない

EFS (Elastic File System)

その特徴はシンプルでスケーラブルで柔軟に利用できるファイルストレージであること

シンプル

- フルマネージド型サービス
- 既存のNFSv4などのツールや標準プロトコル／APIでアクセス可能

スケーラブル

- ペタバイトまでスケーラブルにデータを蓄積
- スループット／IOPS性能は自動的にスケーリングし、低レイテンシーを維持

柔軟性

- ファイルの減少に合わせて自動で拡張・縮小
- 事前に容量を設定する必要なし
- 使った分だけの従量課金

Amazon S3 Glacier

バックアップなど中長期保存用のS3よりも安価なストレージ

S3と同じ耐久性で
値段が安い！

データ取得などの
迅速性がない！

Glacierの特徴

バックアップなど中長期保存用のS3よりも安価なストレージ

- ✓ Amazon S3 Glacier では、データは「アーカイブ」に保存される
- ✓ 1 つのアーカイブの最大サイズは 40 TB
- ✓ 保存可能なアーカイブ数とデータ量に制限なし
- ✓ 各アーカイブには作成時に一意のアーカイブ ID が割り当てられ、作成後はアーカイブを更新できない。
- ✓ アーカイブを保存するためのコンテナとして「ボルト」を使用（1 つの AWS アカウントでは、最大 1,000 個のボルトを使用）
- ✓ Amazon S3 のライフサイクルルールと連携させることにより、Amazon S3 データのアーカイブを自動化し、全体的なストレージコストを削減
- ✓ Advanced Encryption Standard (AES) 256 ビット対称鍵を使用してデフォルトで自動的に暗号化
- ✓ S3と違って直接データをアップロード・取得という処理ができないため、S3ライフサイクル管理からか、プログラム処理によるアップロード／ダウンロードが必要
- ✓ Glacierの最低保持期間は90日

ストレージクラスの選択

Glacierでは3つのストレージタイプから選択する

タイプ	特徴	性能
S3 Glacier Flexible Retrieval (通常のGlacier)	<ul style="list-style-type: none">✓ 1年に1~2回アクセスされ、非同期で取り出されるアーカイブデータ向け✓ 通常のデータ検索で(3~5時間)を要する✓ 迅速取り出しで(2~5分)で取り出し可能✓ 一括検索で(5~12時間)で無料でデータ取り出し✓ ライフサイクルマネジメントで指定✓ ボールトロック機能でデータを保持	<ul style="list-style-type: none">■耐久性 99.99999999%■可用性 99.99%
S3 Glacier Instant Retrieval	<ul style="list-style-type: none">✓ アクセスされることがほとんどなく、ミリ秒単位の取り出しが必要な長期間有効なデータ向け✓ 医用画像やニュースメディアなど✓ S3 Standardと同じパフォーマンスのミリ秒単位でのデータの取り出し	<ul style="list-style-type: none">■耐久性 99.99999999%■可用性 99.9%
Amazon Glacier Deep Archive	<ul style="list-style-type: none">✓ 最安のアーカイブ用ストレージ✓ 7~10年以上保持される長期間使用されるものの、めったにアクセスされないデータ向け✓ 標準の取り出し速度で12時間以内にデータを取得✓ 大容量取り出しで48時間以内にデータを取得✓ ライフサイクル管理で指定	<ul style="list-style-type: none">■耐久性 99.99999999%■可用性 99.99%



Glacierのデータ取出タイプ

Glacierのデータ取得タイプの設定に応じてデータ取得時間と取得時の料金が変わる

タイプ	特徴
迅速	<ul style="list-style-type: none">✓ 迅速取り出しへは、アーカイブのサブセットが迅速に必要になった場合にデータにすばやくアクセスするモード。通常 1~5 分以内で使用可能になる
プロビジョニングキャパシティ	<ul style="list-style-type: none">✓ プロビジョンドキャパシティーは、迅速取り出しの取得容量を必要なときに利用できることを保証する仕組み
標準	<ul style="list-style-type: none">✓ 標準取り出しへは、数時間以内にすべてのアーカイブにアクセスできるデフォルト設定。通常、標準取り出しへは 3~5 時間で完了
大容量	<ul style="list-style-type: none">✓ 大容量取り出しへは、最も安価な取り出しオプションであり、大量のデータ(ペタバイトのデータを含む)を 1 日以内に低コストで取得できます。通常、大容量取り出しへは 5~12 時間で完了

Glacier Deep Archive

Glacierよりも値段が安くデータ保存が可能だが、データ取得はさらに遅くなる中長期保存用ストレージタイプ



Glacierよりさらに
値段が安い！



Glacierよりさらに
データ取得が遅い！

Glacier Deep Archive

Glacierよりも値段が安くデータ保存が可能だが、データ取得はさらに遅くなる中長期保存用ストレージタイプ

- ✓ 基本的なデータモデル・管理はGlacierと同じ
- ✓ 1 GBあたりの月額料金 0.00099 USD から利用可能でAWSの**最低価格**
- ✓ データは 3 つ以上の AWS アベイラビリティゾーンにまたがって保存され、S3と同様に99.99999999% の耐久性を実現
- ✓ 標準取り出しで、データは12 時間以内に取りだすことが可能
- ✓ 大量取り出しで、48 時間以内にデータを取り出す大容量取り出しをすることで取得コストを低減できる。

ユースケース分け

ユースケースに応じた使い分けを理解して、実際の試験問題に対応できるようにする。

Amazon Simple Storage Service (S3)	インターネットアクセス／EC2インスタンス間で共有／大容量データを保存したいケースは基本はS3を利用する。
Amazon Elastic Block Store (EBS)	EC2インスタンスにアタッチして、アプリケーションを構成するためのボリュームディスクとして利用する場合はEBSを利用
Amazon Elastic File System (EFS)	インターネットアクセスは不可で、EC2インスタンス間でのデータ共有をする場合はEFSを共有ストレージとして利用
Amazon S3 Glacier	データバックアップなど中長期にアクセス頻度が低いデータを保存する場合にコスト最適を目指してGlacierを選択する。

ネットワーキングと コンテンツ配信

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

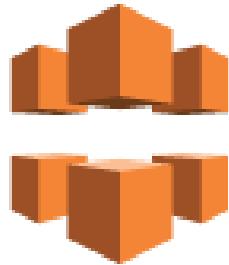
ネットワーキングとコンテンツ配信

ネットワークやコンテンツ配信・AWS環境への接続設定に利用するサービス

Amazon VPC	IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーキング環境を構築するサービス
Amazon CloudFront	低レイテンシーの高速転送により世界中の視聴者に安全に配信する高速コンテンツ配信ネットワーク (CDN) サービス
Amazon Route 53	DNSサーバーの機能を提供し、ドメイン変換とルーティングを実施するサービス
AWS Direct Connect	AWS とデータセンター、オフィス、またはコロケーション環境との間にプライベート接続を確立する専用線サービス
Amazon API Gateway	リアルタイム双方向通信アプリケーションを実現する RESTful API および WebSocket API を作成・管理する
AWS Storage Gateway	オンプレミスから実質無制限のクラウドストレージへのアクセスを提供するハイブリッドクラウドストレージサービス

CloudFront

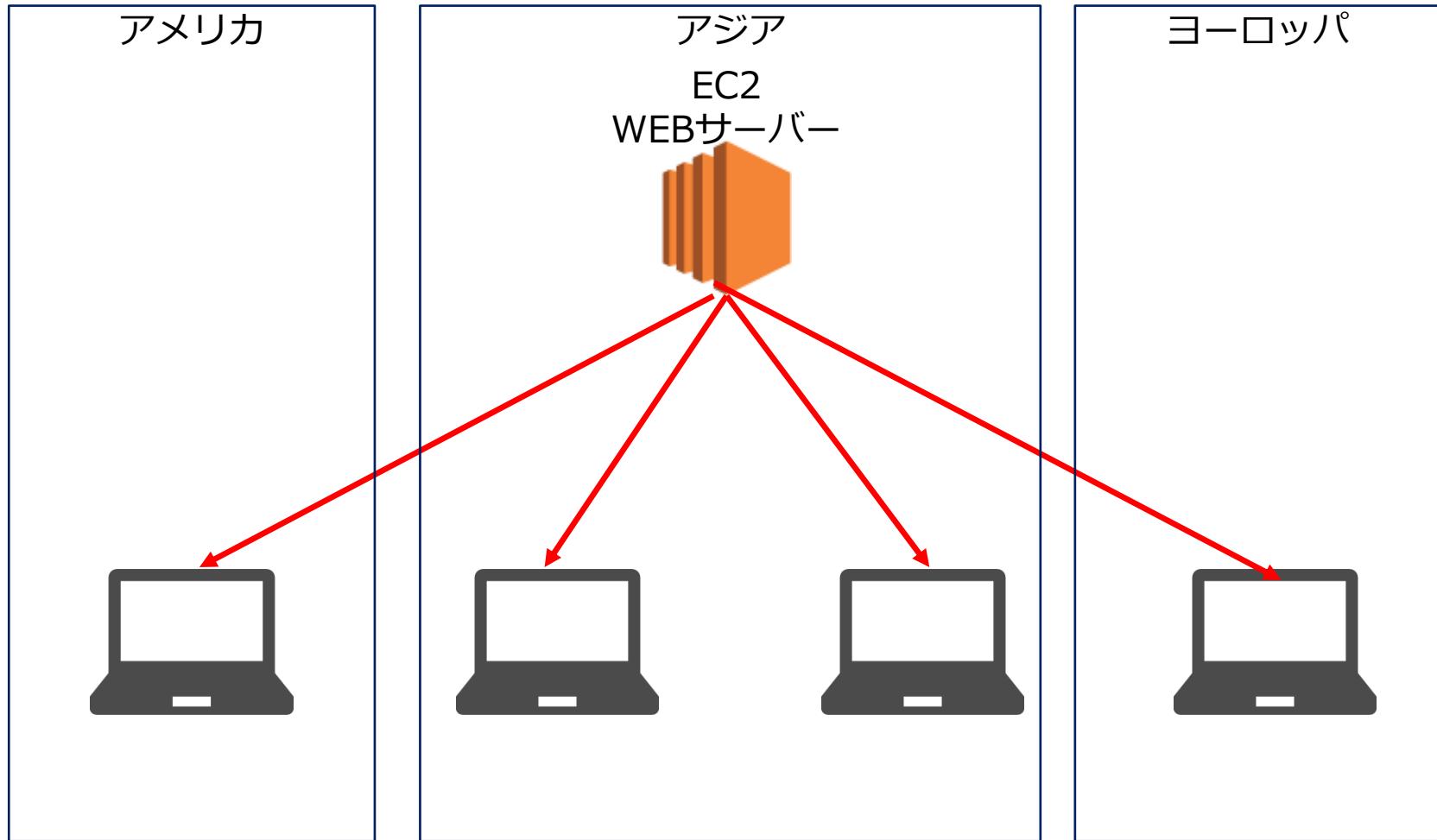
AWSが提供するCDN（Content Delivery Network）サービス



CloudFront

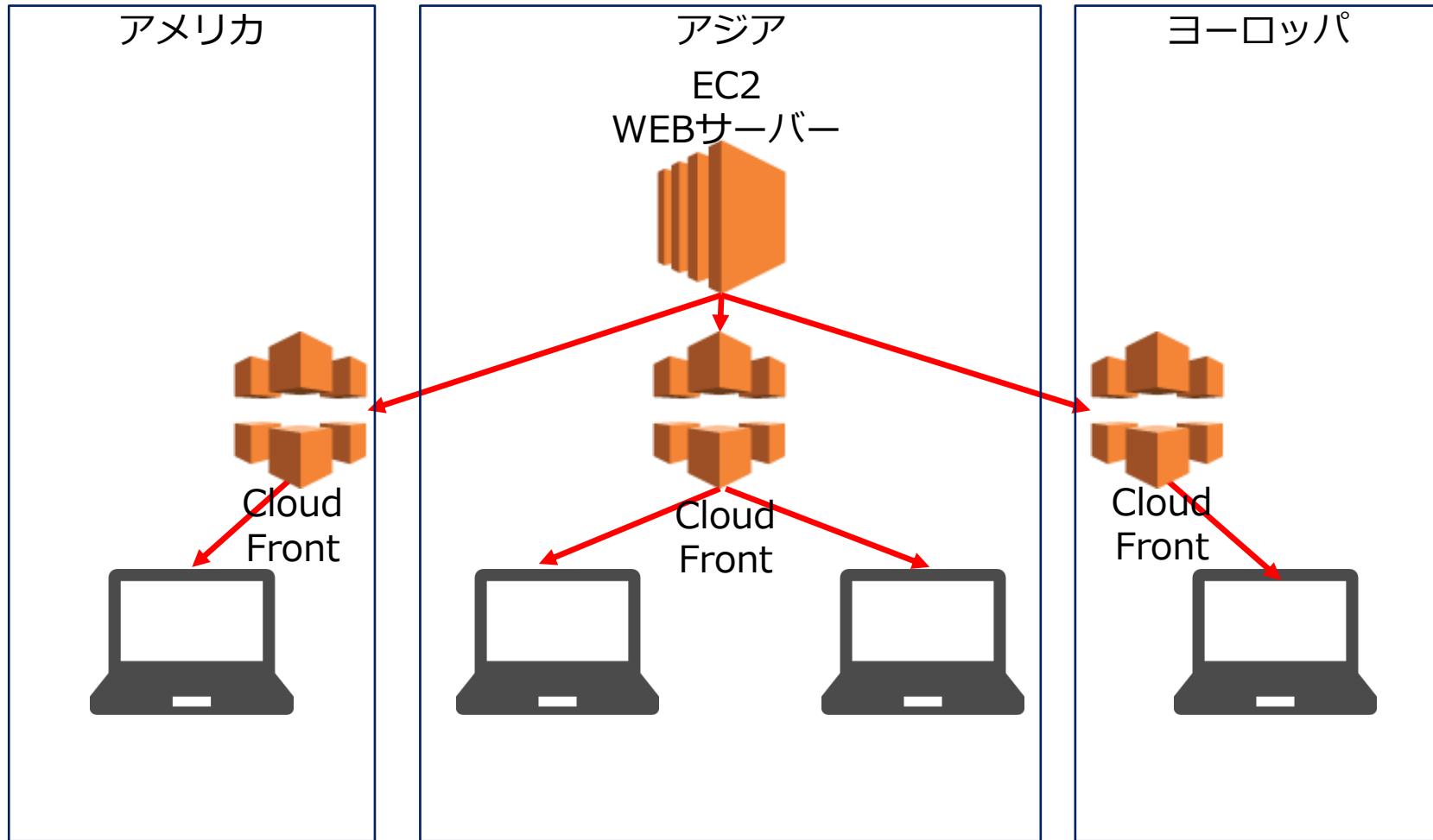
CloudFront

CDNはWEBコンテンツ配信処理を高速化するためのサービス



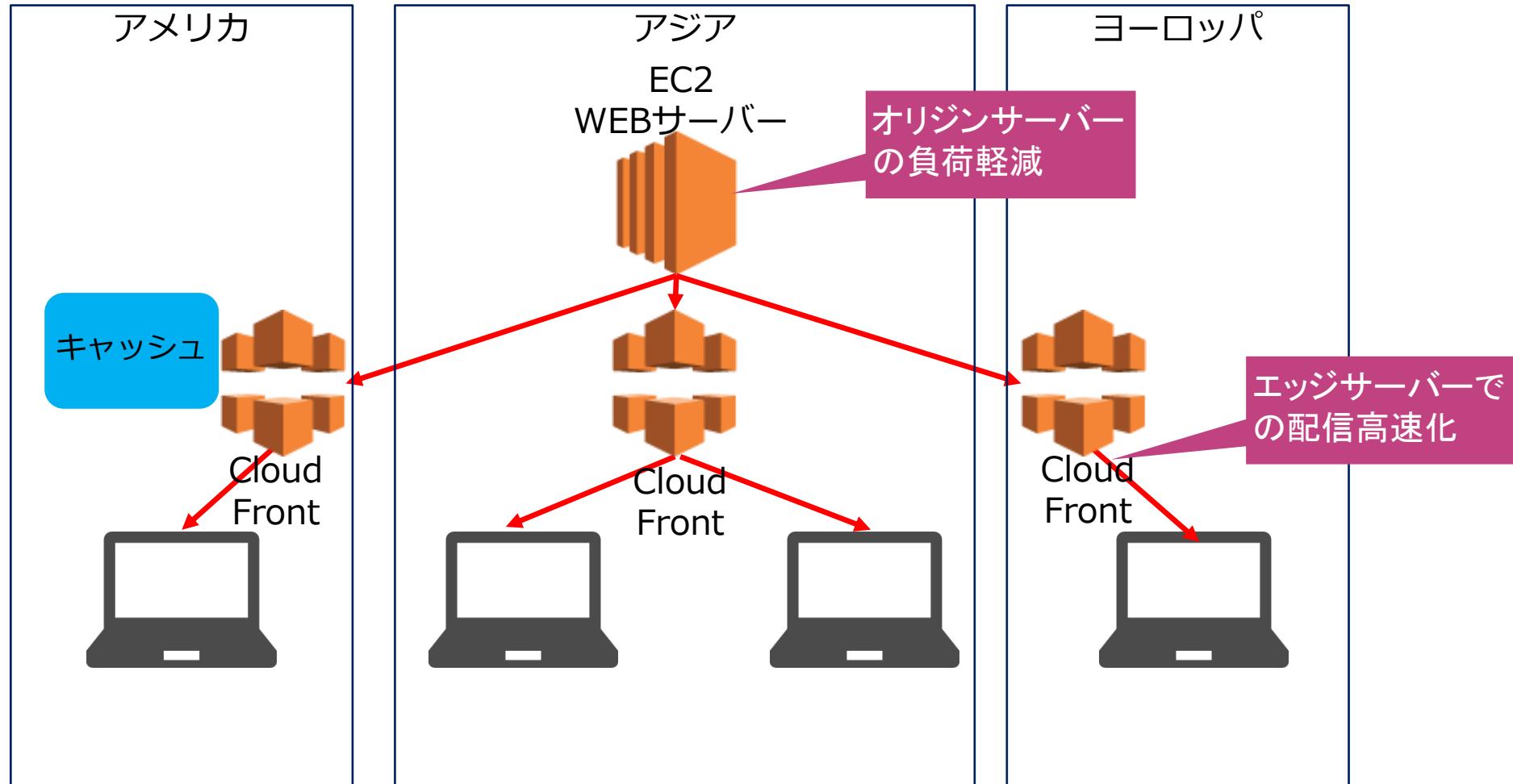
CloudFront

CDNはWEBコンテンツ配信処理を高速化するためのサービス



CloudFront

CDNはWEBコンテンツ配信処理を高速化するためのサービス



CloudFront

大規模なアクセスも世界中にあるエッジのキャパシティを活用して効率的かつ高速にコンテンツ配信が可能なサービス

- 200以上のエッジサーバによる高性能な分散配信
- 高いパフォーマンス
- AWS WAF／AWS Shield／AWS Certificate Managerとの連携やDDoS対策によるセキュリティ機能
- オリジンに対してHeader／Cookie／Query Stringsによるフォワード指定で、動的なページ配信が可能

Direct Connect

お客様のデータセンター やオフィスを専用線などを介して AWS ヘプライベートに接続するサービス

【Direct connectのメリット】

- 安価なアウトバウンドトラフィック料金
- ネットワーク信頼性の向上
- ネットワーク帯域幅の向上

Direct Connectの特徴

VPNの方が安く素早く利用できるが、信頼性や品質は専用線が勝る

	VPN	専用線
コスト	✓ 安価なベストエフォート回線が利用可能	✓ キャリアの専用線サービス契約が必要となりVPNより割高
リードタイム	✓ クラウド上での接続設定で可能なため即時	✓ 物理対応が必要なため数週間
帯域幅	✓ 暗号化のオーバーヘッドにより制限がある	✓ ポートあたり1G/10Gbps
品質	✓ インターネット経由のためネットワーク状態の影響を受ける	✓ キャリアにより高い品質が保証される
障害切り分け	✓ インターネットベースのため自社で保持している範囲以外の確認は難しい	✓ 物理的に経路が確保されているため比較的容易

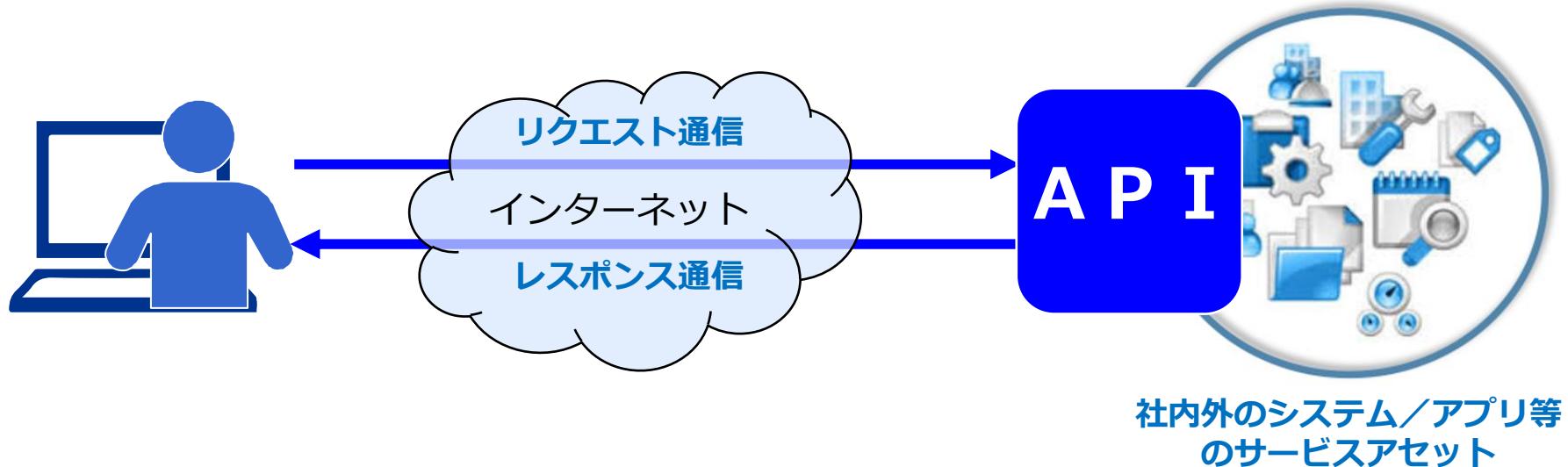
API Gateway

API GatewayはAPI作成/管理をフルマネージド型サービスで提供

- 最大数十万個のAPI同時呼び出し・受付が可能
- アクセス制御の管理
- DDoS攻撃対応やスロットリングによるバックエンド保護
- EC2／Lambda／任意のウェブアプリケーションのワークロード処理を実行する
- Lambdaと密接に統合されている
- WebSocketを利用したリアルタイムかつ双方向通信のAPIも処理可能（2019年より）

API Gateway : APIとは

APIを通してリクエストとレスポンスにより、他サービスの機能やデータを呼び出すことができる

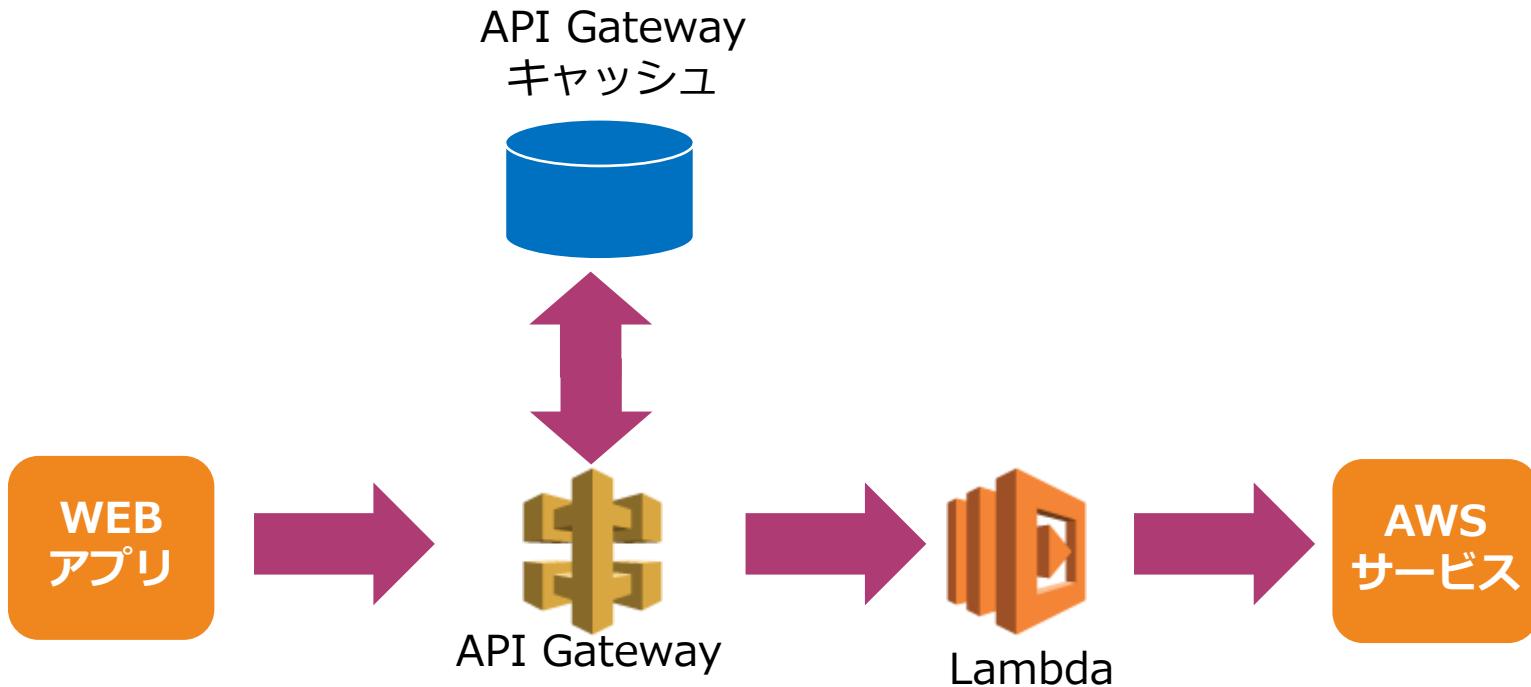


【専門的には】

- ✓ APIはアプリケーションソフトウェア開発に利用される標準的なインターフェース群のこと
- ✓ 中でもWEB APIはWEB上で他のサービスを呼び出す方式や取り決め

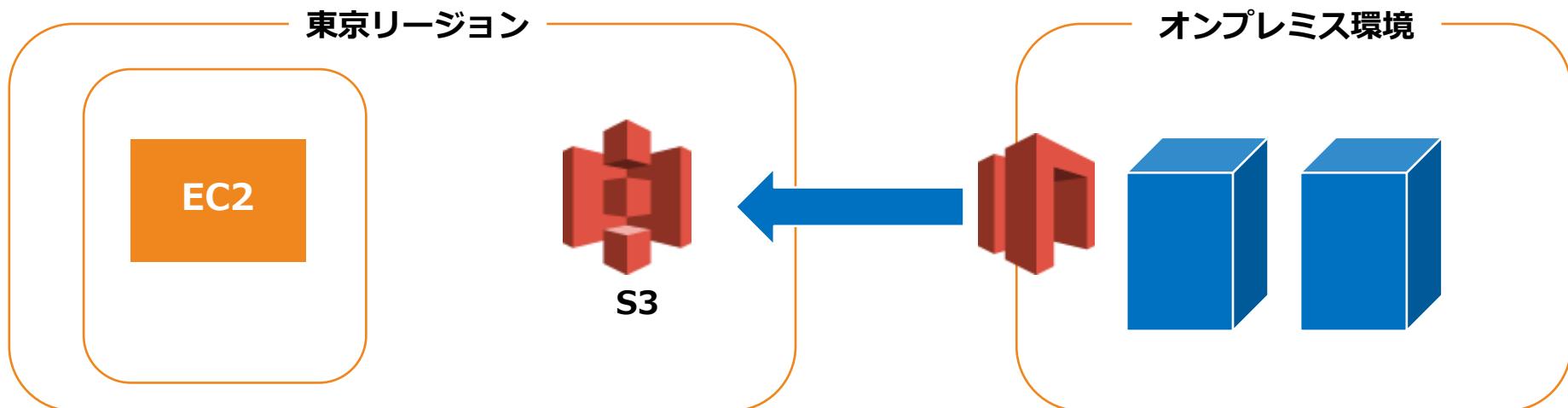
API Gatewayのユースケース

API Gatewayを連携口として外部アプリとの連携を実現する



AWS Storage Gateway

標準的なストレージプロトコルを利用して外部システム環境とAWSのストレージサービスとを接続するサービス



AWS Storage Gatewayの利点

AWSが有する機能や性能を活用できることが大きな利点

- 標準的なストレージプロトコルを活用したシームレスな統合
- キャッシュを活用した低レイテンシーなアクセスが可能
- AWSストレージサービスの堅牢性・低コスト・拡張性
- 効率的なデータ転送
- AWSのモニタリング・管理・セキュリティとの統合

AWS Storage Gatewayの用途

データ移転や保存などAWSストレージを利用したい場合に用いる

- ビッグデータ処理／クラウドバースティング／システム移行のため
にデータをAWSストレージに移動させたいケース
- バックアップ・アーカイブ・災害対策としてAWSにデータを保持
- オンプレミス環境で容易にAWSストレージを活用

Storage Gatewayのタイプ

利用するデータタイプに応じて4つのゲートウェイを利用する

ファイルゲートウェイ

Amazon S3 オブジェクトにStorage Gatewayを経由してファイルデータを格納

キャッシュ型ボリューム ゲートウェイ

頻繁にアクセスされるデータはローカルのストレージゲートウェイに保持しながら、Amazon S3 をプライマリデータストレージとして使用

保管型ボリューム ゲートウェイ

保管型ボリュームを使用すると、プライマリデータをローカルに保存する一方で、そのデータを非同期に AWS にバックアップ

テープゲートウェイ

Amazon S3 と Glacier にデータを保管する仮想テープストレージとVTL管理

データベース

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

データベース

AWSでは様々なタイプのデータベースサービスがマネージド型サービスで提供されている

Amazon RDS	MySQL、PostgreSQL、Oracle、SQL Server、MariaDB 向けのマネージドリレーショナルデータベースサービス
Amazon Aurora	MySQL および PostgreSQL と互換性のあるクラウド向けの分散・高速化されたリレーショナルデータベース
Amazon DynamoDB	規模に関係なく数ミリ秒台のパフォーマンスを実現する、key-value およびドキュメント型のNoSQL型のデータベース
Amazon ElastiCache	Redis または Memcached に互換性のある完全マネージド型のインメモリ・キヤッシュDB（NoSQL型）
Amazon Redshift	高速かつシンプルで、費用対効果の高いデータウェアハウス

Aurora

クラウド時代の新しい分散型のリレーショナルデータベースとして誕生

- Amazonがクラウド時代に適したリレーショナルDBを一から考えて構築された新RDB
- その特徴はNoSQL型の分散高速処理とRDBとしてのデータ操作性を両立させたこと

Aurora

MySQLと2.5~5倍の性能を商用データベースの10分の1の価格で提供する高性能・低コストDB

性能5倍

Sysbench4インスタンスと
r3.8xlargeAuroraとの比較

性能約2.5~5倍

TPC-Cをr3.8xlargeのAuroraとの比較

Aurora

RDSにおいてデータベースソフトウェアの一つとして選択

エンジンのオプション

Amazon Aurora

Amazon
Aurora

MySQL



MariaDB



PostgreSQL



Oracle

ORACLE®

Microsoft SQL Server



Auroraの特徴

高い並列処理性能によって大量の読み書きをするのに適したDB

- 高い並列処理によるストレージアクセスによってクエリを高速処理することが可能
- Auroraは大量の書き込みや読み込みを同時に扱うことができる
- データベースの集約やスループット向上が見込まれる
- ただし、すべてが5倍高速というわけではなく、適用すべき領域を見つけて利用する

Auroraの特徴

MySQL／PostgreSQLと互換性があり、同じ操作方法とそのコミュニティを利用することができる

MySQL5.6互換
を選択可能

PostgreSQL互換
を選択可能

Auroraの特徴

分散型で耐障害性と自己回復性を備えたスケーラブルな新しいタイプのフルマネージド型RDB

耐障害性／自己回復性

- 3つのAZに2つのコピーを設置可能で合計6つのコピーを保持
- 過去のデータがそのままS3に継続的バックアップ
- リストアも差分適用がなく高速
- どのタイミングでも安定したリストア時間を実現
- 99.99%の高可用性・高耐久性

スケーラビリティ

- 10GBから最大64TBを提供するSSDデータプレーンを利用してシームレスに拡張可能
- Auto-Scalingなどのクラウド独自のスケーラブルが可能
- 最大15のリードレプリカを利用した高速読み込みが可能

DynamoDB

完全マネージド型のNoSQLデータベースサービス

- ハイスケーラブルで無制限に性能を拡張できる
- 負荷が高くなつても応答速度が低下しない低レイテンシー
- 高可用性 (SPOFなしでデータは3箇所のAZに保存)
- マネージド型のためメンテナンスフリー : CloudWatchで運用

- **プロビジョンドスループット**
テーブルごとにReadとWriteに、必要なスループットキャパシティを割り当てる
例) Read:100／Write:1000
- **ストレージの容量制限がない**
データ容量の増加に応じたディスクやノードの増設は一切不要

DynamoDBの出来る事

キー バリュー（ワイドカラム型）でデータを簡易に操作することができる。

出来る事

- キーに対するバリュー（値）のCRUD操作
- 簡易なクエリやオーダー
- 例えば、数万人以上が同時アクセスして処理が必要になるアプリケーションのセッションデータ処理など

出来ない事／向いていない事

- JOIN／TRANSACTION／COMMIT／ROLLBACKは不可
- 詳細なクエリやオーダー（データの検索や結合処理などには向いていない）
- 大量のデータ読み書きにはコストがかかる

DynamoDBの整合性モデル

デフォルトで結果整合性モデルであり、一部処理に強い整合性モデルを利用している

Write

少なくとも2つのAZでの書き込み
完了が確認された時点で完了

Read

□ デフォルト：結果整合性モデル

最新の書き込み結果が即時読み取り
処理に反映されない可能性がある

□ オプション：強い整合性モデル

GetItem/Query/Scanでは強い
整合性のある読み込みオプション
が指定可能

ユースケース

ビッグデータ処理向けか大量データ処理が必要なアプリケーション向けに利用する

ビッグデータ

- 大量のデータを収集・蓄積・分析するためのデータベースとして活用
- Hadoopと連携してビッグデータ処理が可能

アプリケーション

- 大規模サービスでのデータ高速処理が必要なアプリケーション向けに活用
- 多数のユーザーが一度にアクセスするようなアプリケーションのデータ処理など

ユースケース

例えば、大量に発生しうるWEB行動データやログ管理など

ユーザー行動 データ管理

ユーザー情報やゲーム、広告などのユーザー行動データ向けDB
ユーザーIDごとに複数の行動履歴管理

バックエンド データ処理

モバイルアプリのバックエンド／バッチ処理の
ロック管理／フラッシュマーケティング／ストレージのインデックス

ElastiCache

分散インメモリキャッシュサービスの構築・管理及びスケーリングを容易に実施することができるサービス

- キャッシュクラスタを数クリックで起動
- フルマネージド型でモニタリング、自動障害検出、復旧、拡張、パッチ適用、バックアップに対応し高可用性を実現
- 広く利用されている2種類のエンジンmemcached, /redisから選択可能

インメモリキャッシュ

ElastiCacheはメモリ+キャッシュというデータベース

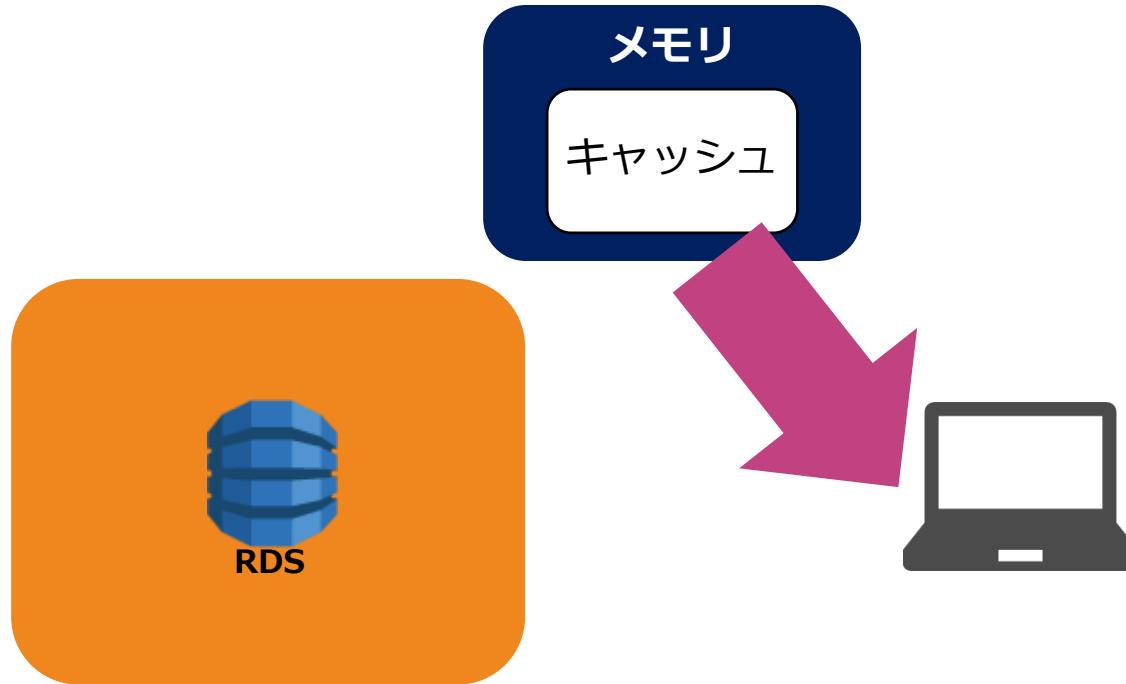
メモリ



キャッシュ

インメモリキャッシュとは

メモリを活用して高速にキャッシュへのアクセスを可能にしたデータベースの仕組み



次にアクセスした際はキャッシュから
データを取得する

ElastiCache

オープンソースのRedisとMemcachedを利用可能で汎用性あり

Redis

- 高速に値をRead/Writeできるインメモリキッシュ型DB
- シングルスレッドで動作するインメモリキッシュDBで全てのデータ操作は排他的
- スナップショット機能がある
- データを永続化できる

Memcached

- 高速に値をRead/Writeできるインメモリキッシュ型DB
- マルチスレッドで動作するインメモリキッシュDB
- スナップショット機能がない
- データを永続化できない
- フェイルオーバーや復元ができない。

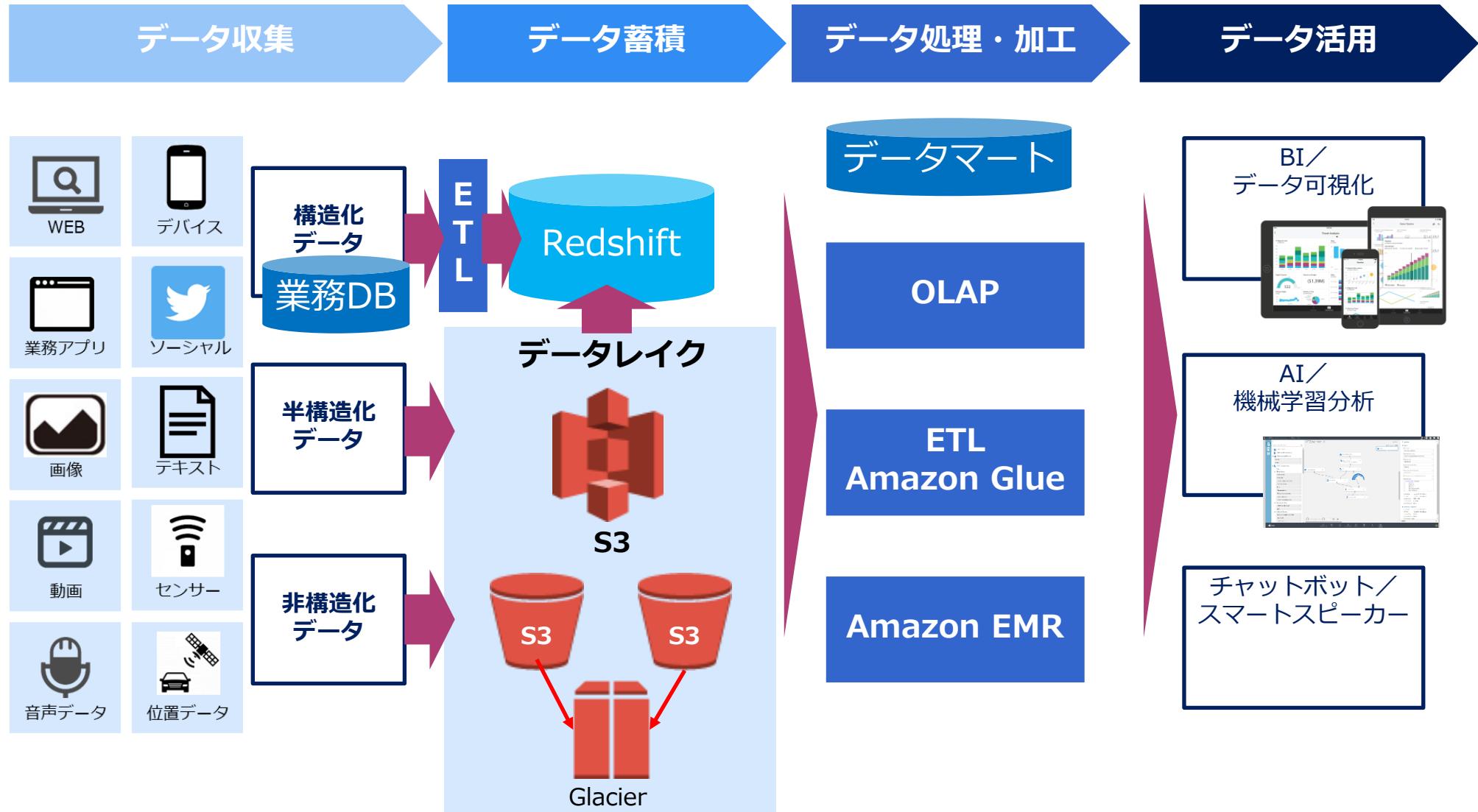
Redshift

高速でスケーラブルな費用対効果の高いマネージド型のDWH／データレイク分析サービス

- 数百ギガバイトのデータから開始して、ペタバイト以上まで拡張
- 1 テラバイトあたり年間 1,000 USD 以下で利用可能
- 自動ワークロード管理など自動テーブルメンテナンスなど多くのメンテナンスタスクやデータ配置が自動化されているフルマネージド型
- PostgreSQL互換の列指向データモデル
- 複数ノードをまとめたクラスター構成。単一AZで起動し、マルチAZ構成は不可
- RA3インスタンスで最大で他のクラウドデータウェアハウスの 3 倍に達するパフォーマンス
- AQUAによる分散キャッシュで、Redshift が他のクラウドデータウェアハウスに比べて最大 10 倍の速度で動作

データレイク

S3はデータレイクとしてデータ活用のハブとして利用できる



ユースケース分け

ユースケースに応じた使い分けを理解して、実際の試験問題に対応できるようにする。

Amazon RDS	AWSでリレーショナルデータベースを構築するケースではRDSを選択する。
Amazon Aurora	高速分散処理が必要なリレーショナルデータベースと限定された場合はAuroraを選択する。
Amazon DynamoDB	AWSでNoSQL型のデータベースを利用する場合は、まずはDynamoDBを選択する。
Amazon ElastiCache	NoSQL型のデータベースの中で、インメモリ型／キャッシュ型のDBと限定された場合はElastiCacheを選択する。
Amazon Redshift	AWSでデータウェアハウスと限定された場合はRedshiftを選択する。

アイデンティティ・セキュリティ
コンプライアンス

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

アイデンティティ・セキュリティ・コンプライアンス

AWSでのセキュリティやコンプライアンスに寄与するサービス

AWS Identity & Access Management (IAM)	AWS のサービスやリソースへのアクセスを安全に管理するアクセス管理サービス
Amazon GuardDuty	悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービス
Amazon Inspector	自動化されたセキュリティ評価サービスで、AWS にデプロイしたアプリケーションのセキュリティとコンプライアンスを向上させることができる
AWS Key Management Service	暗号化キーを簡単に作成して管理し、幅広い AWS のサービスやアプリケーションでの使用を制御する
AWS CloudHSM	法令遵守のためのハードウェアベースキーストレージ
AWS WAF	一般的なウェブの脆弱性からウェブアプリケーションまたは API を保護するウェブアプリケーションファイアウォール

アイデンティティ・セキュリティ・コンプライアンス

AWSでのセキュリティやコンプライアンスに寄与するサービス

AWS Shield

マネージド型の分散サービス妨害 (DDoS) 保護サービス

AWS Artifact

AWS のコンプライアンスレポートにオンデマンドでアクセスできる無料のセルフサービスポータル

AWSリソースの暗号化

通信・保存されるデータ・リソースの暗号化と接続の暗号化を実施可能

通信の暗号化

- ✓ SSL/TLSを使用してDB インスタンスへの接続を暗号化する。

保管データの暗号化

- ✓ 保管時のデータリソースを暗号化する。

AWSリソースの暗号化

通信・保存されるデータ・リソースの暗号化と接続の暗号化を実施可能

通信の暗号化

- ✓ AWS Certificate Managerを利用してSSL/TLS 証明書を発行・管理することが可能
- ✓ ACMとCloudFrontやRoute53 を連携してSSL/TLS通信を可能にする。

保存データの暗号化

- ✓ AWS が所有するキーを使用して、デフォルトでデータを暗号化する。
- ✓ AWS KMSを利用して作成したデータ暗号化とキー管理プロセスを管理することも可能
- ✓ CloudHSMという世界中のセキュリティ基準に準拠するためのハードウェア型キー管理サービスも利用可能

AWS KMS

AWS KMSは簡単にデータを暗号化するためのマネージド型暗号化サービス

- ✓ 暗号鍵の作成・管理・運用を実施するマネージドサービスでAWS マネジメントコンソール、AWS SDK またはCLI を使用して、キーを作成、インポート、ローテーション、削除、管理する。
- ✓ IAMと連携して鍵のアクセス管理を実施
- ✓ カスタマーマスターキー (CMK) の無効化・有効化・削除を実施し、1年ごとの自動キーローテーションすることが可能
- ✓ CMKを外部から持ち込んで管理することも可能
- ✓ キーを保護するために FIPS 140-2 の検証済みまたは検証段階のハードウェアセキュリティモジュールを使用
- ✓ AWS CloudTrail と統合されており、すべてのキーの使用ログを表示
- ✓ RDSやS3などの多数のAWSサービスに適用可能
- ✓ KMS SDKを利用することで、アプリケーションにおける暗号化も可能

AWS KMS

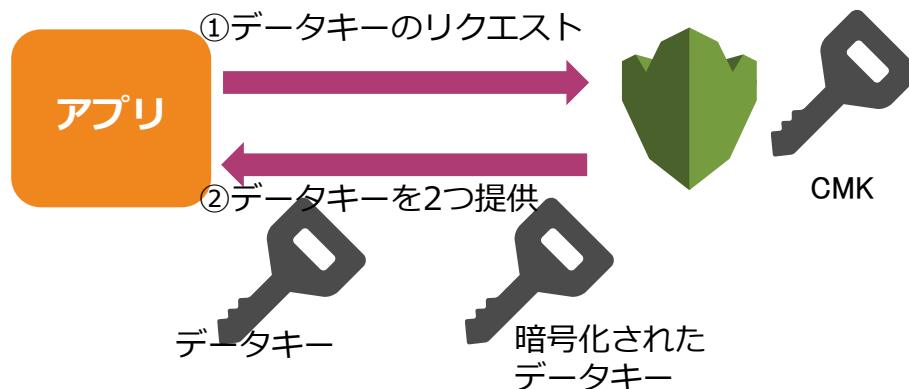
RDSでは保存されるデータ・リソースの暗号化と接続の暗号化を実施可能

カスタマーマスターキー	<ul style="list-style-type: none">✓ 暗号化を実行する上で、最初に作成されるマスターキー✓ 暗号化キーを暗号化する✓ ローテーションされる
カスタマーデータキー (暗号キー)	<ul style="list-style-type: none">✓ 実際のデータの暗号化を利用するキー✓ KMSで生成されてCMKで暗号化される
エンベロープ暗号化	<ul style="list-style-type: none">✓ マスターキーで暗号化をせずに、暗号化したデータキーを利用して暗号化する暗号化方式

エンベロープ暗号化

AWS KMSは簡単にデータを暗号化するためのマネージド型暗号化サービス

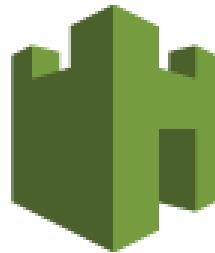
- データキーとマスターキーによる暗号化を実施
- カスタマーマスターキー（CMK）を利用してデータキーを暗号化する



- ③ アプリ／ユーザーはデータキーを利用して暗号化
- ④ アプリ／ユーザーは暗号化データキーと暗号化データを送付

データの保護：暗号化

CloudHSMは不正使用防止策がとられている専用HWモジュール（HSM）により暗号キーを保護するサービス。厳しい暗号化要件に対応するために利用



CloudHSM

権限管理 : AWS Directory Service

ディレクトリサービスとはユーザに関わる各種情報を保管して
ユーザー認証を実現する仕組み

管理するユーザー情報

ID
ユーザ名
姓名氏名
部署
グループ
担当
電話番号
メールアドレス
パスワード

実現する機能

IDとアクセス管理
運用効率の向上
コンプライアンス向上
セキュリティの強化など

アプリのアクセス制御

ファイル共有
パッチ管理など

権限管理 : AWS Directory Service

AWSに新しいディレクトリを作成するか、既存のActive Directory認証を利用した制御を実現

Simple AD

AWSに新規ディレクトリを作成

AD Connector

既存のディレクトリをAWSに接続

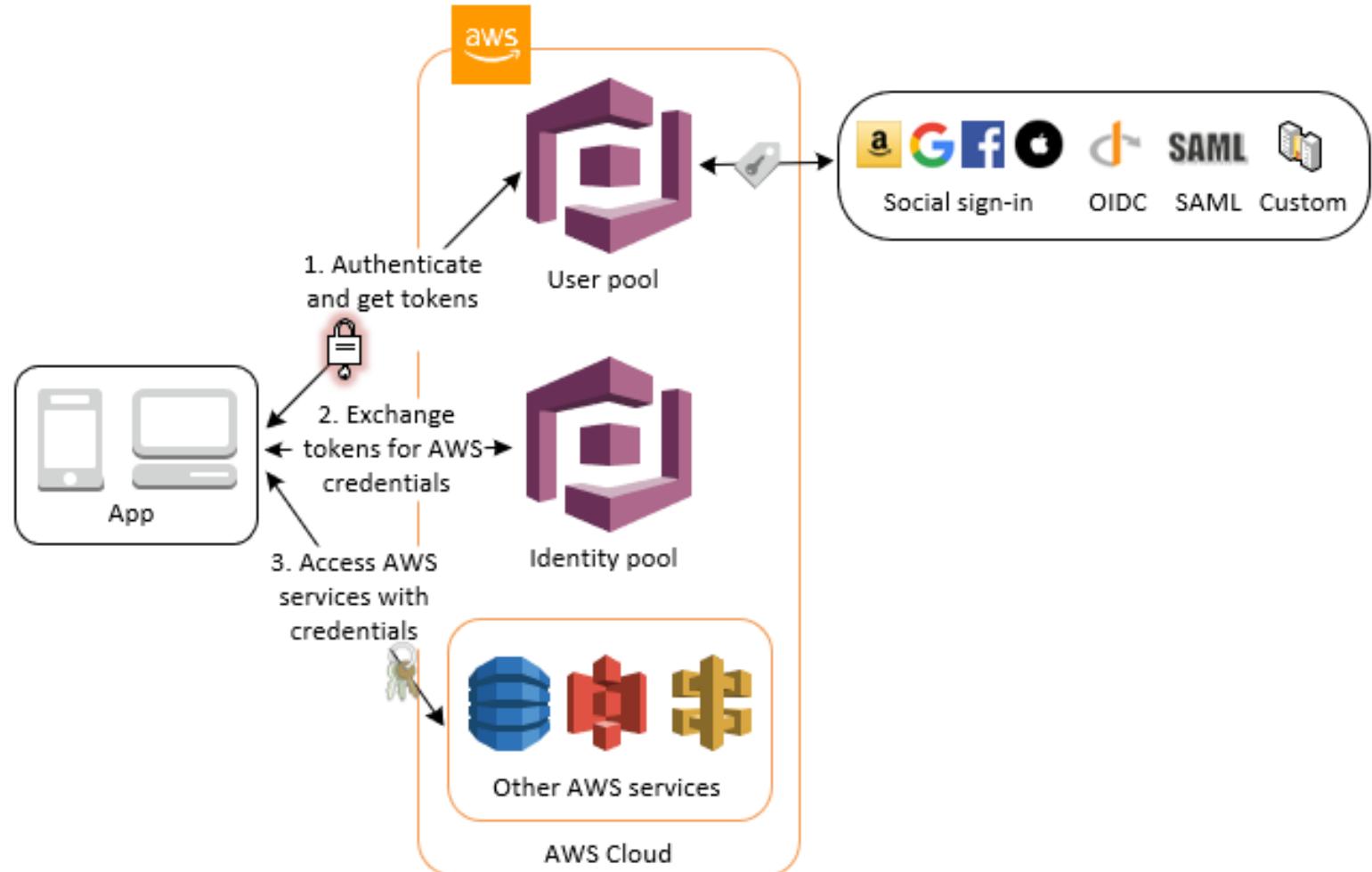
権限管理 : Security Token Service (STS)

STSは限定的で一時的なセキュリティ認証情報を提供するサービス



ユーザー認証機能：Cognito

アプリケーションにユーザー認証機能を付与したい場合は
Cognitoを利用する



検出制御

監視やモニタリングを継続的に実施してセキュリティを高める

CloudTrail

AWSユーザーの行動ログを取得し、ガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援する

CloudWatch

AWSリソースとAWSで実行するアプリケーションに対して、様々なメトリクスやログを収集・追跡するモニタリングサービス

AWS GuardDuty

AWS上での悪意のある操作や不正な動作を継続的にモニタリングする脅威検出サービス

Amazon Inspector

自動的にアプリケーションを検証し、その露出、脆弱性、ベストプラクティスからの逸脱状況を確認し、セキュリティ評価を実施するサービス

IAM Access Analyzer

監視やモニタリングを継続的に実施してセキュリティを高める

IAM > Access Analyzer

Last scan: a minute ago

Access Analyzer [Info](#)

Analyzer

AWS_Organizations_IAM_Access_Analyzer
Zone of trust: Current organization (o-ari... 7x)

Active | Archived | Resolved | All

Active findings

Organization ID o-ari... 7x

Filter active findings

Finding ID	Resource	Resource Owner Account	External principal	Condition	Access level	Upd...
9263c1a8...	S3 Bucket my-acce...	58 ... 7	AWS Account 267 ... 13	-	Read	a few s...
73638211...	IAM Role aws-serv...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
7e6762d0...	IAM Role aws-test-...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
4fbcd1d5...	IAM Role ReadOnly	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
7292c388...	IAM Role audit-rol...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...

IAM > Access Analyzer

Last scan: a minute ago

Access Analyzer [Info](#)

Analyzer

AWS_Organizations_IAM_Access_Analyzer
Zone of trust: Current organization (o-ari... 7x)

Active | Archived | Resolved | All

Active findings

Organization ID o-ari... 7x

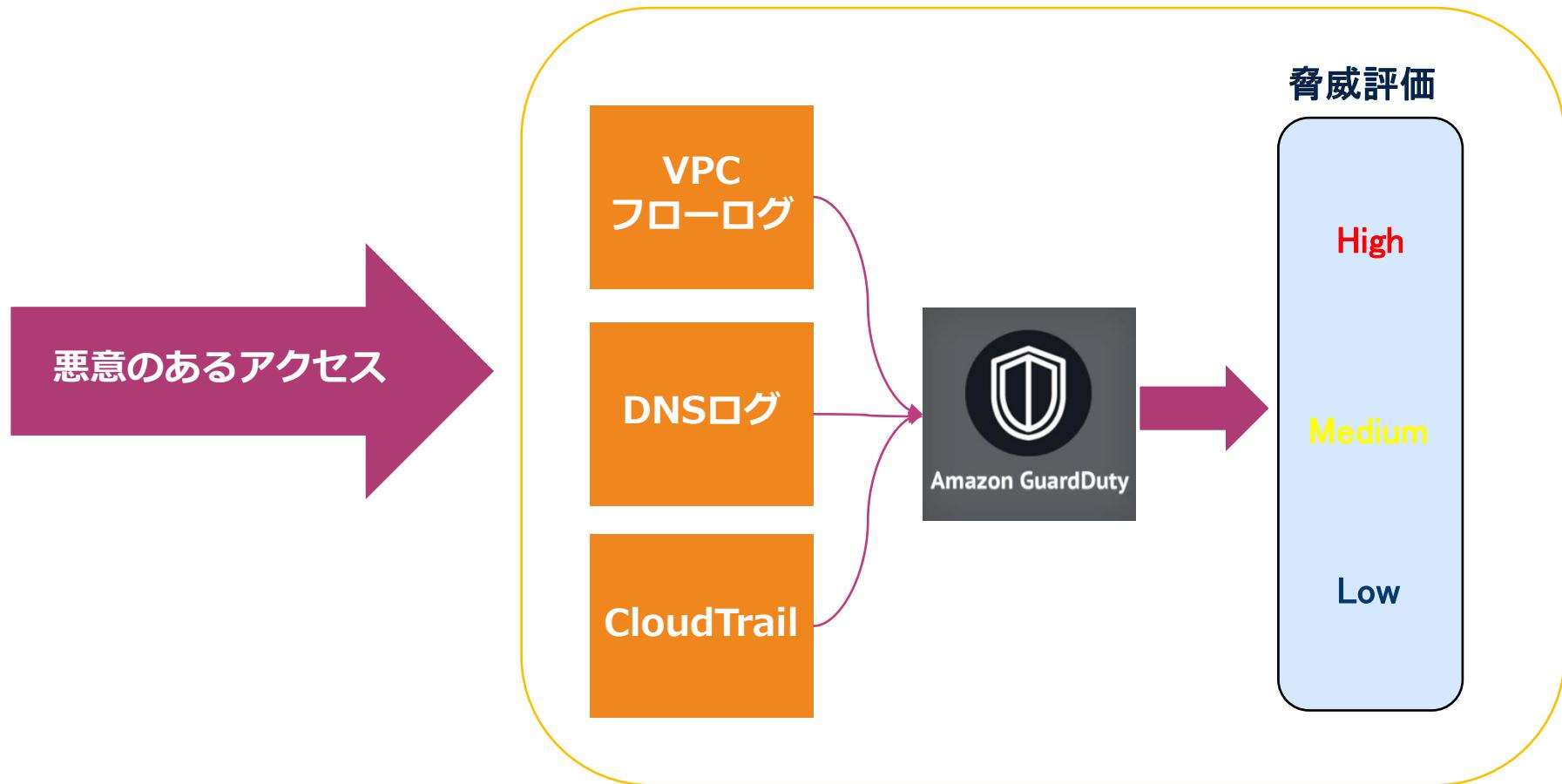
Filter active findings

Finding ID	Resource	Resource Owner Account	External principal	Condition	Access level	Upd...
9263c1a8...	S3 Bucket my-acce...	58 ... 7	AWS Account 267 ... 13	-	Read	a few s...
73638211...	IAM Role aws-serv...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
7e6762d0...	IAM Role aws-test-...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
4fbcd1d5...	IAM Role ReadOnly	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...
7292c388...	IAM Role audit-rol...	58 ... 7	AWS Account 727 ... 95	-	Write	a minut...

<https://aws.amazon.com/jp/blogs/news/identify-unintended-resource-access-with-aws-identity-and-access-management-iam-access-analyzer/>

AWS GuardDuty

機械学習などを利用してAWSインフラやアプリへのセキュリティ上の脅威リスクを検知するサービス



Amazon Inspector

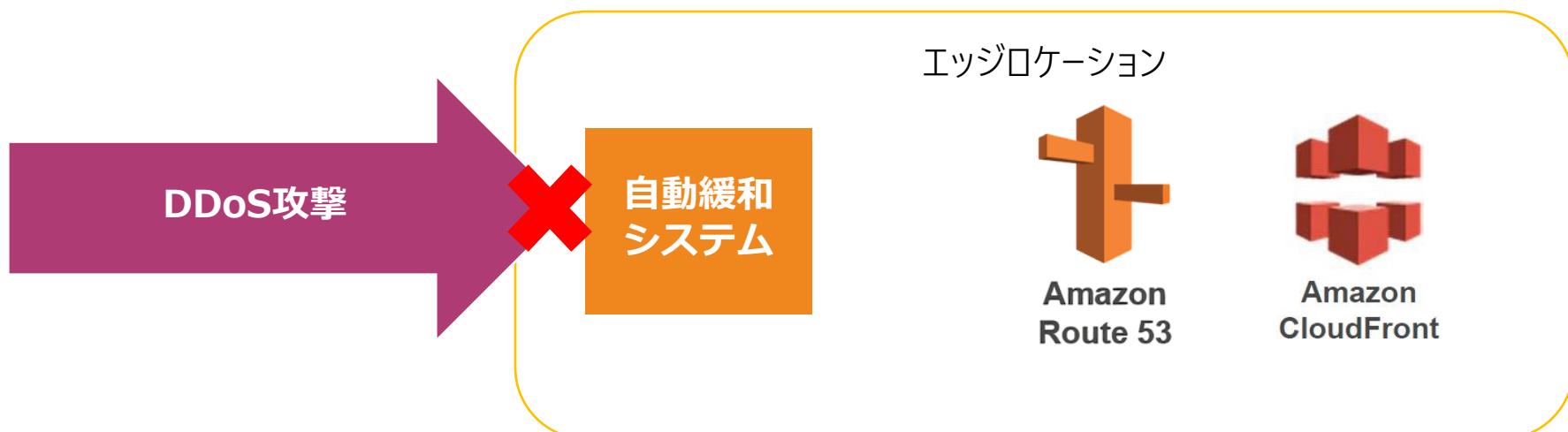
Amazon EC2にエージェントを導入し、プラットフォームの脆弱性を診断する、ホスト型診断サービス

- AWSリソースに対して、オンデマンドで自動的にシステム設定や振る舞いを分析することが可能
- 組み込みルールパッケージ
 - CVE (Common Vulnerabilities & Exposures)
 - CIS (Center for Internet Security)
 - ベストプラクティスに基づいたルール
 - 実行時のふるまい分析
- 推奨対応手順が含まれた詳細レポート
- API連携による開発プロセスとの統合

AWS Shield

L3/L4におけるDDoS攻撃に対する自動緩和システムをCloudFrontとRoute53に対して自動適用する無料サービス

- ✓ L3/L4における自動緩和システムをエッジロケーションで適用する
- ✓ 対象となるのはCloudFrontとRoute53のエッジロケーションの前にインラインで配置され、全ての着信パケットを検査
- ✓ DDoS攻撃の96%を自動軽減
- ✓ Standard版は無料／Advanced版は有料



AWS Shield

Advanced版を利用することで、WAFと連携して大規模な攻撃から強力な防御を実行可能

Standard

- ✓ L3/L4のDDoS攻撃に対応
- ✓ 無料で全ユーザーに適用される
- ✓ SYN/UDPフラッド、反射攻撃などから防御
- ✓ 自動検知と自動緩和を実行
- ✓ CloudFrontとRoute53などのサービスに組み込まれて自動で実行

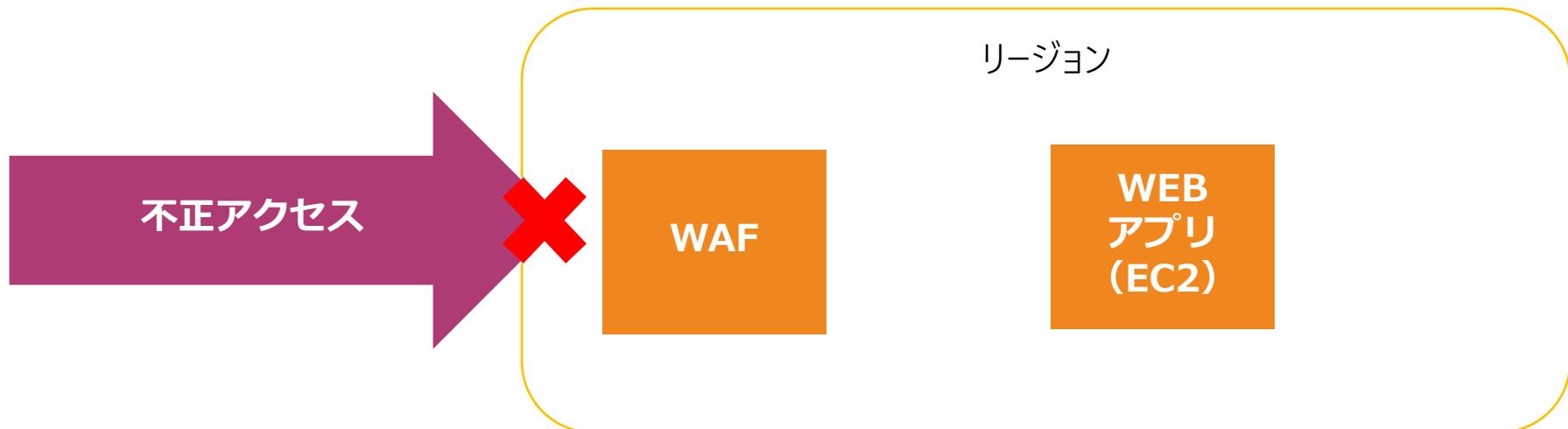
Advanced

- ✓ L3/L4に加えてWAFと連携してL7のDDoS攻撃への防御を実施
- ✓ より大規模な攻撃から防御する
- ✓ AWS DDoS レスポンスチーム(DRT)に 24 時間 365 日アクセス
- ✓ リソースの使用量の急増から AWS の請求を保護する「スケーリングへの DDoS コスト保護」が可能
- ✓ レポーティング

AWS WAF

WEBアプリケーションのトラフィック通信を検査して脆弱性への攻撃や不正アクセスを遮断するファイアウォールサービス

- ✓ SQLインジェクション、クロスサイトスクリプトなど悪意のあるリクエストを遮断
- ✓ 遮断方式でカスタムルールを設定 (Rate-basedルール／IPベースフィルター／正規表現パターン／サイズ制限／アクション許可・拒否設定)
- ✓ CloudWatchと連携したモニタリング



AWS Artifact

重要なコンプライアンス関連情報の頼りになる一元管理型のリソース

AWS Artifact Reports

世界各地にある監査機関の指定する基準や規制を遵守状況をテストおよび確認したコンプライアンスレポートを提供

AWS Artifact Agreements

AWSアカウントとの契約の確認・受諾・管理を実施

マネジメントとガバナンス

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

マネジメントとガバナンス

運用保守やサポートに関する支援ツールやサービス



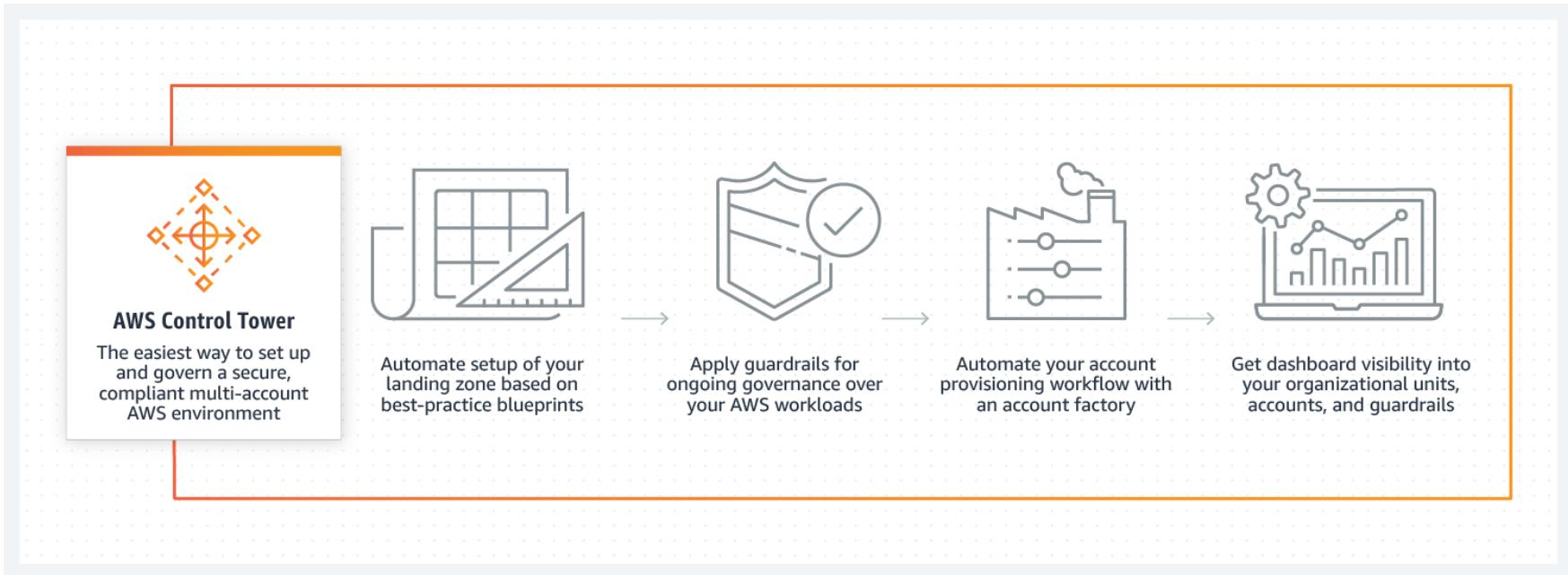
準備系サービス

運用保守やサポートに関する支援ツールやサービス

AWS Control Tower	ベストプラクティスに基づき安全性と適合性を備えた、複数アカウントの AWS 環境を設定および管理するサービス
AWS Organizations	複数のAWS アカウント全体の一元管理と一括請求
AWS Budgets	予算のしきい値を超えたときにアラートを発信するカスタム予算を設定
AWS License Manager	ソフトウェアベンダーからのソフトウェアライセンスを簡単に管理するサービス
AWS Well-Architected Tool	AWSのアーキテクチャ設計原則の確認とワークフローの見直しと改善を支援

AWS Control Tower

ベストプラクティスに基づき安全性と適合性を備えた、複数アカウントの AWS 環境を設定および管理するサービス



AWS License Manager

ソフトウェアベンダーからのソフトウェアライセンスを簡単に
管理するサービス

- ライセンスの利用数やライセンスの利用条件を登録
- ライセンスの利用状況を追跡して管理することが可能
- コンプライアンス違反などのライセンスルールに反する利
用状況を可視化する。
- 既存ライセンスを自動検出するなどの一元的な管理を実現
- ダッシュボードを利用して可視化して、管理可能

展開系サービス

運用保守やサポートに関する支援ツールやサービス

AWS CloudFormation	AWSクラウド環境内の全インフラリソースを記述してテンプレート化して展開する環境自動設定サービス
AWS Elastic Beanstalk	WEBアプリケーションの定番構成の構築・デプロイの自動化サービス
AWS OpsWorks	OpsWorksはChefまたはPuppetを使用してアプリケーションを設定および運用するための設定管理サービス
AWS Service Catalog	AWS上でデプロイされているITサービスの一元的な管理を実施するサービス
AWS Marketplace	EC2インスタンスの起動に使用できるAMIなど、AWSで実行されるソフトウェアを購入できるオンラインストア

CloudFormation

AWSクラウド環境内の全インフラリソースを記述してテンプレート化して展開する環境自動設定サービス

- プロビジョニングされたリソースの変更・削除が可能
- 追加リソースへの通常課金のみで追加料金なし
- JSON/YAMLで記述する
- クロスリージョンとクロスアカウントで管理
- 直接サポートされていないリソースや機能を利用する場合はカスタムリソースでスタック作成の一部に独自ロジックを組み込むことが可能

CloudFormation

JSON/YAMLなどのコードでインフラ構築方式がポリシーとして定義されており、それに基づいて仮想化インフラが構築可能

```
AWSTemplateFormatVersion: '2010-09-09'  
Description:  
Metadata:  
Parameters:  
Mappings:  
Conditions:  
Transform:  
Resources:  
  FirstVPC:  
    Type: AWS::EC2::VPC  
    Properties:  
      CidrBlock: 10.0.0.0/16  
      Tags:  
        - Key: Name  
          Value: FirstVPC  
  AttachGateway:  
    Type: AWS::EC2::VPCGatewayAttachment  
    Properties:  
      DependOn:  
        VpcId: !Ref FirstVPC  
        InternetGatewayId: !Ref InternetGateway  
Outputs:
```



仮想化
インフラ
の構築

Elastic Beanstalk

WEBアプリケーションの定番構成の構築・デプロイの自動化
サービス

- 速く簡単にアプリケーションをデプロイするサービス
- Java, PHP, Ruby, Python, Node.js, .NET, Docker, Goに対応して
WEBアプリケーションを展開できる
- Apache、Nginx、Passenger、IIS など使い慣れたサーバーでデプ
ロイおよびスケーリングが可能
- コードをアップロードすればキャパシティのプロビジョニング、
ロードバランシング、Auto Scaling からアプリケーションのヘルス
モニタリングまでデプロイを自動化できる

Elastic Beanstalkのユースケース

WEBアプリケーションのデプロイを容易にすることや、タスク時間の長いワークロードの展開に利用する

ウェブサーバー環境

- ELB + Auto Scalingでスケーラブルな構成をコード化してバージョンすることで、スケーラブルなウェブアプリケーションを実行できる
- 単一コンテナのDockerコンテナを実行可能
- 複数コンテナはECSを使用した環境実行が可能

ワーカー環境

- SQS + Auto Scalingでスケーラブルなバッチ処理ワークを実現
- 定期的なタスク実行基盤の作成：毎日深夜1時に動作するバックアップ処理
- ワーカーホスト内でWebアプリケーションを動作させ、ワークロードの時間が係る処理を実行させる

OpsWorks

OpsWorksはChefまたはPuppetを使用してアプリケーションを設定および運用するための設定管理サービス

OpsWorksスタック

OpsWorks for
Chef Automation

OpsWorks for
Puppet Enterprise

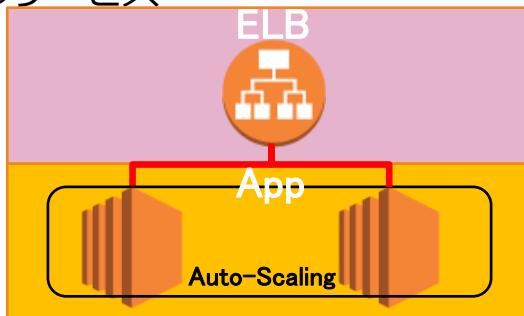
Elastic Beanstalk VS OpsWorks

WEBアプリのデプロイに特化したElastic Beanstalkに対して、OpsWorksは様々なアプリケーションに対応する高度なインフラ環境構築が可能

Elastic Beanstalk

アプリケーションのデプロイ自動化

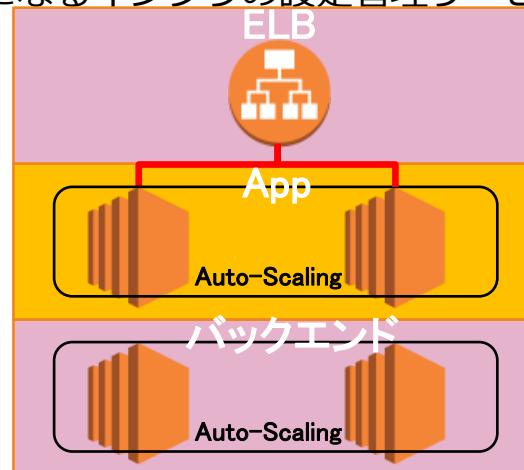
ウェブアプリケーションやサービスを使い慣れたサーバーにおいてデプロイとスケーリングするためのサービス



OpsWorks

インフラの設定自動化

ChefやPuppet のマネージド型インスタンスのサーバーの設定・デプロイ・管理を自動化できるようになるインフラの設定管理サービス



AWS Service Catalog

AWSで承認されたITサービスのカタログを作成および管理する
支援サービス

IT運用管理者

CloudFormationのテンプレートを利用して、管理されるAWSリソース定義や、これらの利用権限をカタログとして一元管理する機能を提供

ユーザ部門

IT運用管理者が作成したカタログより、権限がなくとも求める機能に応じたAWS環境を必要に応じて起動が可能になる

AWS Marketplace

AWSで利用できるソフトウェアウェアなどが売り買いくできるオンラインストア

The screenshot shows the AWS Marketplace search results for "Operating Systems" (726 results). The results page includes a sidebar with filters for Categories (All Categories, Infrastructure Software, Operating Systems), Vendors (Cognosys Inc., Amazon Web Services, clkwrk Ltd, Supported Images, Frontline, Center for Internet Security, Canonical Group Limited, ProComputers.com, Cloud Infrastructure Services, CloudMint), and Pricing Plan (Hourly, Annual, Free, Bring Your Own License, Monthly). The main content area displays four items:

- Microsoft Windows Server 2019 Base**: Version 2020.06.10 | Sold by Amazon Web Services. 2 AWS reviews. Description: Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run compatible Windows-based solutions on AWS' high-performance, reliable, cost-effective, cloud computing platform. Tags: Windows, Windows Server 2019 Base 10 - 64-bit Amazon Machine Image (AMI).
- Microsoft Windows Server 2016 Base**: Version 2020.06.10 | Sold by Amazon Web Services. Description: Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any compatible Windows-based solution on AWS' high-performance, reliable, cost-effective, cloud computing platform. Common... Tags: Windows, Windows Server 2016 Base 10 - 64-bit Amazon Machine Image (AMI).
- CentOS 7 (x86_64) - with Updates HVM**: Version 2002_01 | Sold by Centos.org. 62 AWS reviews | 193 external reviews. Description: This is the Official CentOS 7 x86_64 HVM image that has been built with a minimal profile, suitable for use in HVM instance types only. The image contains just enough packages to run within AWS, bring up an SSH Server and allow users to login. Please note that this is the default CentOS-7 image... Tags: Linux/Unix, CentOS 7 - 64-bit Amazon Machine Image (AMI).
- Microsoft Windows Server 2012 R2**: Version 2020.06.10 | Sold by Amazon Web Services. Description: Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any

運用・操作系のサービス

運用保守やサポートに関する支援ツールやサービス

Amazon CloudWatch	アプリケーションを監視し、リソース使用率の最適化を行い、運用上の健全性を統括的に把握するモニタリングサービス
AWS CloudTrail	ユーザー活動と API 使用状況の追跡するログ取得サービス
AWS Config	AWS リソースの設定を評価、監査、審査できるサービス
AWS Systems Manager	AWS のさまざまなサービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化する運用支援サービス
AWS Personal Health Dashboard	AWS のサービス状態のパーソナライズされた状況をダッシュボード形式で確認できる。
AWS サポート	AWSによるサポートサービス ベーシック／開発者／ビジネス／エンタープライズプランの4つ

AWS Config

AWSリソースのレポジトリ情報からリソース変更履歴や構成変更を管理するサービス

- AWSリソースの構成変更をロギングして保存する
(30日から7年)
- 履歴も定期的に構成情報スナップショットとして取得し、S3に保存
- 構成情報に基づきシステム構成があるべき状態になっているかを評価
- 評価基準にはAWSルールまたは独自ルールを適用

AWS Config

AWS Configには構成変更を管理するストリームと履歴管理するヒストリーと構成要素を保存するスナップショットがある

Configuration Stream

- リソースが作成・変更・削除に対して作成され、構成ストリームに追加される
- SNSトピック連携して通知設定が可能

Configuration History

- 任意の期間における各リソースタイプの構成要素を履歴として蓄積
- S3バケットに保存

Configuration Snapshot

- ある時点での構成要素の集合
- 自動で定期的あるいは変更トリガーで作成
- S3バケットに保存

AWS Systems Manager

利用中のAWSサービスやリソースをモニタリングして、運用タスクを自動化する統合監視サービス

問題検出の時間短縮

EC2などをリソースグループごとに運用データを確認できるため、アプリケーションに影響を与えるリソースの問題をすばやく特定可能

運用の自動化

EC2のパッチ、更新、設定変更・削除・停止およびデプロイなどを自動化

可視化と制御

各リソースグループの最新状態を簡単に可視化して制御できる

ハイブリッド管理

AWSサーバーとオンプレミスのサーバーとを1つのインターフェイスで管理可能

AWS Personal Health Dashboard

AWS のサービス状態のパーソナライズされた状況をダッシュボード形式で確認できる。

Current Status	Details	RSS
Amazon Elastic Compute Cloud (API)	Service is operating normally.	
Amazon Elastic Compute Cloud (Instances)	Service is operating normally.	
Amazon Flexible Payments Service	Service is operating normally.	
Amazon Mechanical Turk (Requester)	Service is operating normally.	
Amazon Mechanical Turk (Worker)	Service is operating normally.	
Amazon SimpleDB	Service is operating normally.	
Amazon Simple Storage Service (EU)	Service is operating normally.	
Amazon Simple Storage Service (US)	Service is operating normally.	
Amazon Simple Queue Service	Service is operating normally.	

AWSサポート

AWSによる人的なオペレーターによる問い合わせや不具合サポートプラン

	ベーシック	開発者	ビジネス	エンタープライズ On-Ramp	エンタープライズ
ケース			各種サービスをお試しの方、テスト環境向け	本番環境のワークロード向け	プロダクション・ビジネスクリティカルなワークロード向け
事前対応型支援 ・トレーニング	なし	サポートオートメーションワークフロー (SAWF) の利用	SAWFの利用。追加料金でインフラストラクチャイベント管理を利用	SAWFの利用。インフラストラクチャイベント管理を利用	SAWFの利用。インフラストラクチャイベント管理/事前対応型の評価、ワークショップ、ディープダイブ/トレーニングラボの利用
アカウント支援	○				コンシェルジュサポート
Trusted Advisor	ベーシックチェックのみ			全項目チェックの利用	
技術サポート へのアクセス	サポート画面からの問い合わせ	メール対応 (平日9時～18時)	電話/チャット/メール (24時間365日) 、ライブ共有画面	ビジネスの内容に加えて、プロアクティブなガイダンス提供、TAMプールの利用/ Well-Architected対応支援	ビジネスの内容に加えて、TAMが環境を事前に監視して支援/ Well-Architected対応支援
技術サポート対応 ユーザー数		1	無制限	無制限	無制限
緊急度/ 初回応答時間		システム障害に対して12時間以内	本番システムのダウンに最短1時間以内	ビジネスクリティカルなシステムのダウンに最短30分以内	ビジネスクリティカルなシステムのダウンに最短15分以内



アプリケーション統合

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

アプリケーション統合

アプリケーション間の通信制御やフロー作成・データ連携などに利用するサービス

SNS

完全マネージド型 pub/sub メッセージング

SQS

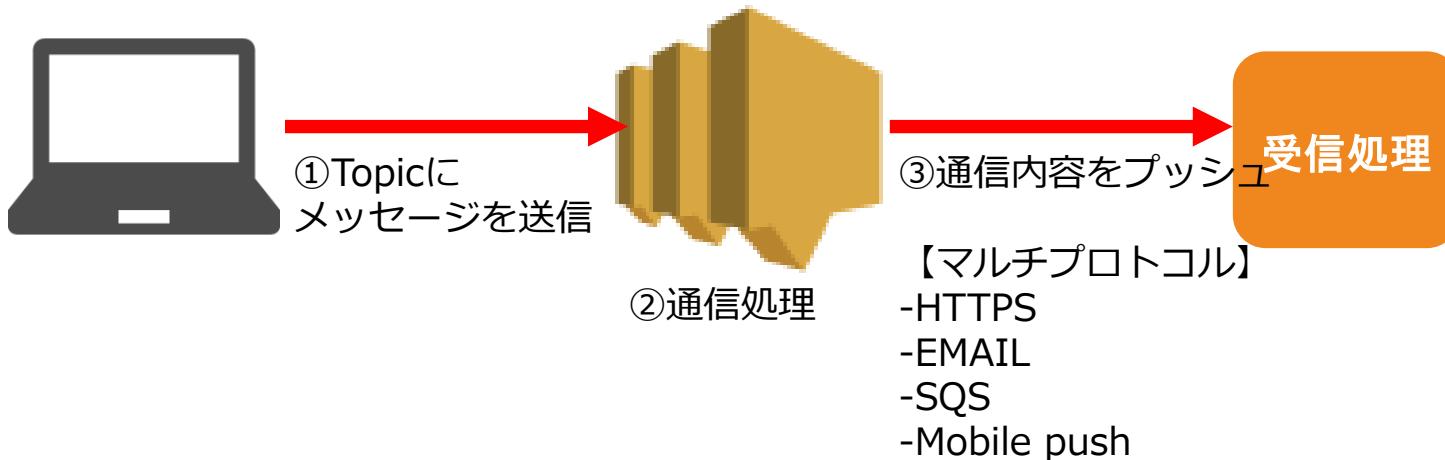
完全マネージド型のメッセージキューイングサービス

SES

Eメール送受信サービス

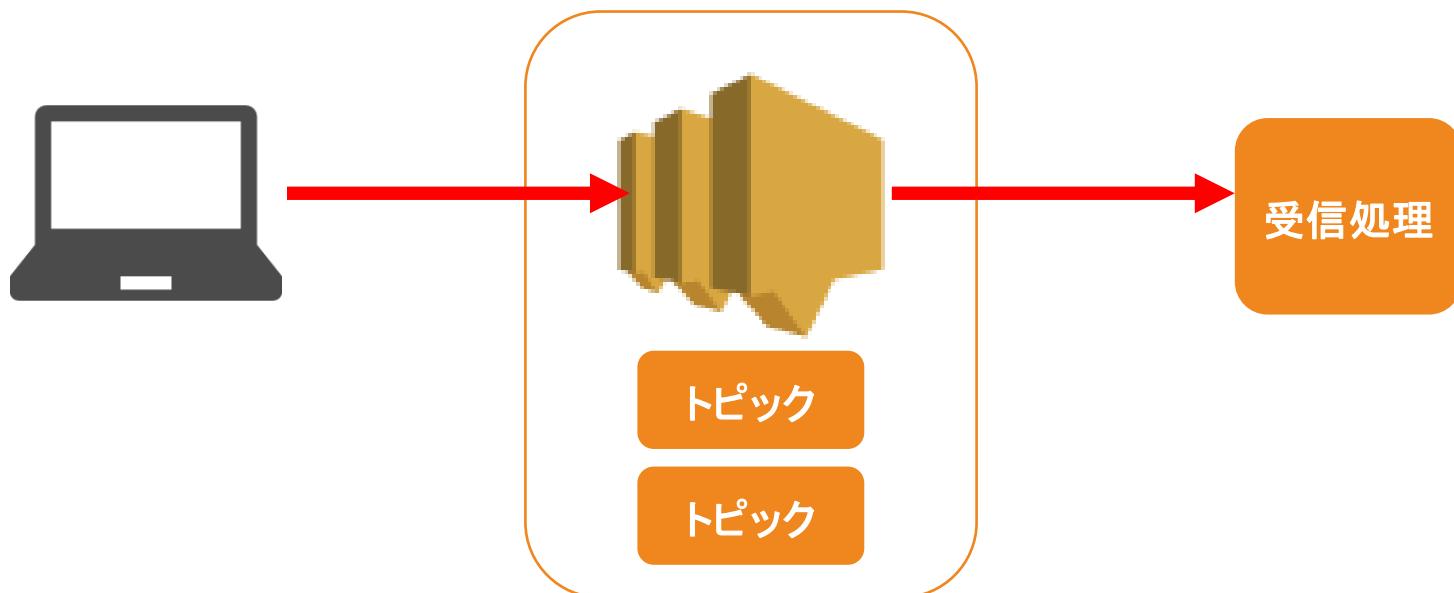
Amazon Simple Notification Service(SNS)

Amazon SNSはフルマネージド型のプッシュ型通知サービスで他のサービスとの非同期通信を可能にする



Amazon Simple Notification Service(SNS)

送信側がトピックを作成して受信側をポリシー指定することで
制御された非同期通信を実現する



SNSの特徴

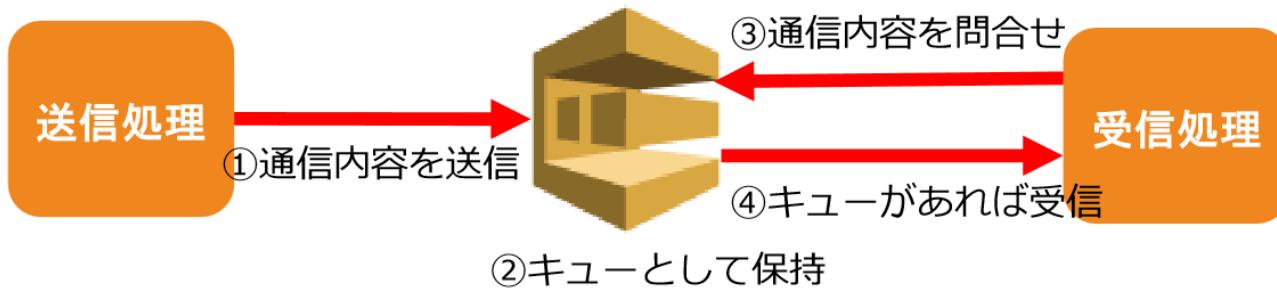
AWSの様々なサービスと連携して通知可能で、疎結合アーキテクチャに利用できる

- 単一発行メッセージ
- メッセージ通信順番は保証されない
→FIFOタイプを利用すると保証される。
- 取り消し不可
- 配信ポリシーによる再試行を実施
- メッセージサイズは最大256KB



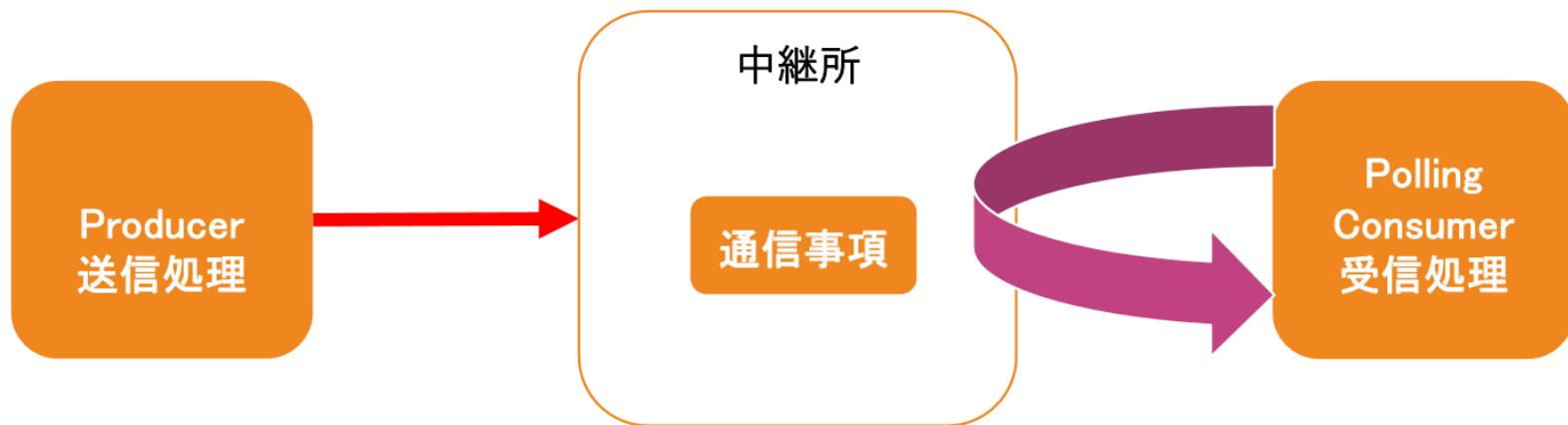
SQS

SQSはキューをため込んでポーリング処理を実施するサービス



ポーリングとは

一旦中継所に通信内容を貯めておいて、受信側のタイミングが良いときに通信を行う



SQSの特徴

フルマネージド型で提供され、高可用性・高スケーラビリティ・高スループット・低コストを実現

- 複数のサーバー/データセンターにメッセージを保持する高可用性構成
- 多数の送信者と受信者に対応可能なスケーラビリティの確保
- メッセージが増加しても高スループットを維持できる
- 無料枠と従量課金による低コスト

Amazon Simple Email Service(SES)

フルマネージド型／サーバレス型のコスト効率に優れたメールサービス

- スケーラブルな構成で信頼性が高いマネージド型
- メール送信：トランザクションメールなどの高品質なコンテンツを顧客に送信可能
- メール受信：受信したメールをトリガーにS3やLambdaなどを起動可能
- バウンス処理：メールが送れなかつた場合の処理を規定

ユースケース分け

ユースケースに応じた使い分けを理解して、実際の試験問題に対応できるようにする。

SNS	AWS上でイベント通知やメッセージング処理／プッシュ通知をするといった場合はSNSを利用する。
SQS	AWS上でキューイング処理／タスク並列分散処理／ポーリング・Pull型の通知をする場合はSQSを利用する。
SES	Eメール送受信機能を利用する場合はSESを利用する。

移行と移転

AWSサービス

製品を調べる



分析



アプリケーション統合



AR およびバーチャルリアリティ



AWS コスト管理



ブロックチェーン



ビジネスアプリケーション



コンピューティング



コンテナ



カスタマーエンゲージメント



データベース



開発者用ツール



エンドユーザーコンピューティング



Game Tech



IoT (モノのインターネット)



Machine Learning



マネジメントとガバナンス



メディアサービス



移行と転送



モバイル



ネットワーキングとコンテンツ配信



量子テクノロジー



ロボット工学



人工衛星



セキュリティ、アイデンティティ、コンプライアンス



ストレージ

移行と移転

AWSクラウドへのインフラ移行やデータ移行に利用するサービス

AWS Application Discovery Service	サーバーの設定データ、使用状況データ、動作データが収集してサーバーの使用率データや依存関係のマッピングなどの移行に必要な情報を提供するサービス
AWS Database Migration Service	データベースを短期間で安全に AWS に移行することが可能、データベース移行ツール
AWS Server Migration Service	数千のオンプレミスワークロードを従来よりも簡単に、かつ短時間で AWS に移行できるエージェントレスサービス
AWS Snow ファミリー	エッジでデータを収集して処理し、AWS との間でデータを移行する、非常に安全なポータブルデバイス

移行と移転

AWSクラウドへのインフラ移行やデータ移行に利用するサービス



- AWS TCO Calculator
- AWS Application Discovery Service

- VM Import/Export
- AWS Server Migration Service
- **AWS Database Migration Service**
- **AWS Schema Conversion Tool**
- AWS Storage Gateway
- AWS Snowball
- VMware on AWS

- AWS CloudWatch
- AWS Config
- AWS CloudFormation
- AWS CloudTrail
- AWS Service Catalog
- AWS Trusted Advisor
- AWS サポート

AWS Application Discovery Service

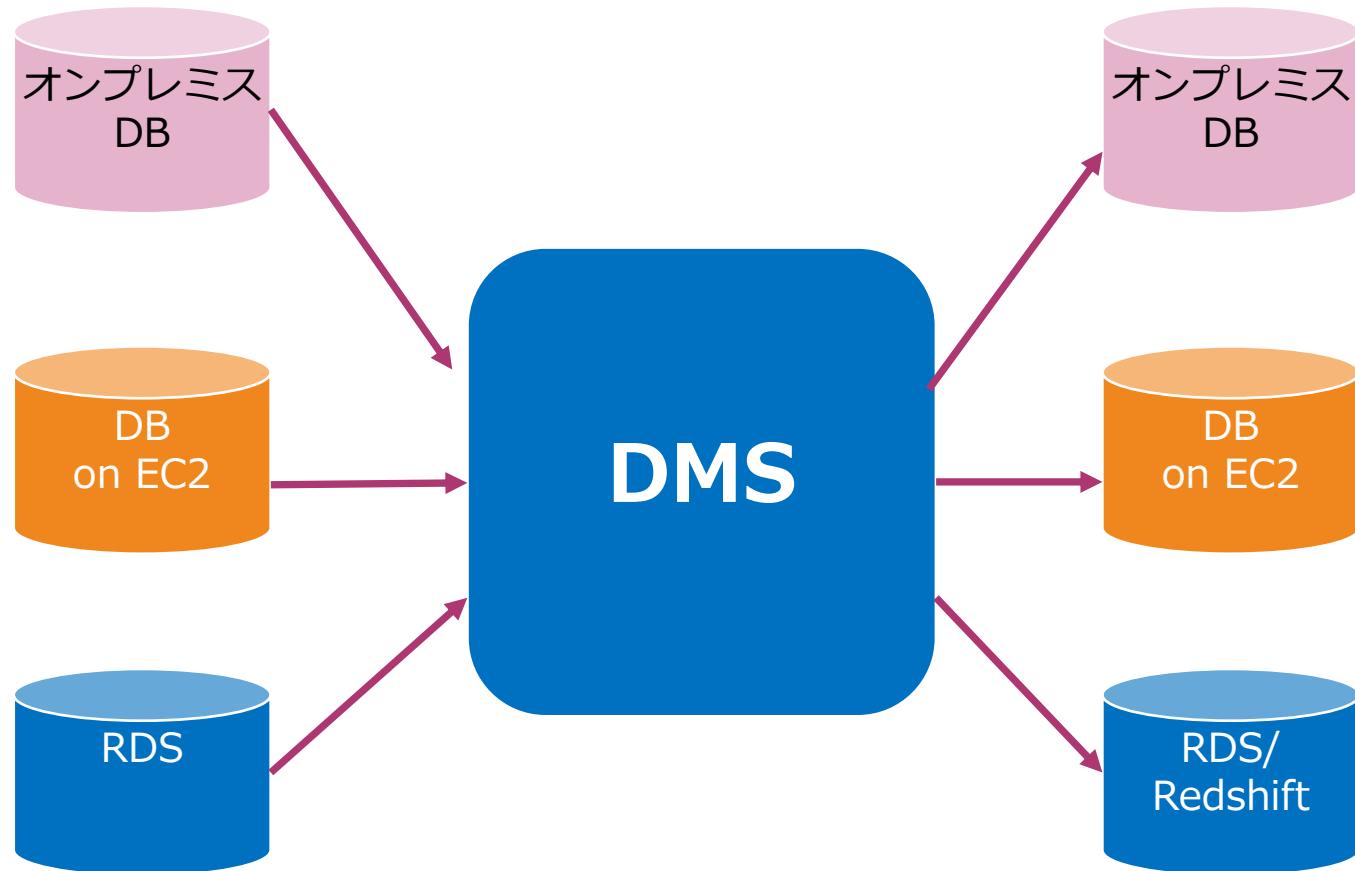
サーバーの使用率データや依存関係のマッピングなどの移行に必要な情報を提供するサービス



- ✓ クラウドに何を移行するのか
対象機器の情報把握
(VMware/Windows/Linux環境の情報把握)
- ✓ 現状の機器やソフトウェアの依存関係の把握
- ✓ 手作業による手間を省く

AWS Database Migration Service

データベースを短期間で安全に AWS に移行することが可能な
データベース移行ツール



AWS Server Migration Service

数千のオンプレミスワークロード・サーバーを従来よりも簡単に、かつ短時間で AWS に移行できるエージェントレスサービス

- ✓ 簡単に大量のサーバーを移行できるサービスで、1アカウントで同時に50VMまで移行可能
- ✓ エージェントレス型で移行を実施
- ✓ オンプレミスのVMwareに対して増分変更をキャプチャして、AWSに自動的に転送するVM専用の移行ツール
- ✓ 移行先のAWSでAMIを作成して、EC2インスタンスに移行することが可能

AWS Snowファミリー

物理ストレージデバイスを使用し、インターネットを迂回して
AWSに直接大容量データを転送するサービス

Snowball



ペタバイト規模のデータ移動
(現在は非推奨)

Snowball Edge



ペタバイト規模のデータ移動
+
コンピューティング
とストレージ機能

Snowmobile



エクサバイト規模の
データ移動

Snowball

ペタバイト規模のデータ移行の際に利用するアプライアンスで、現在はSnowball Edgeに世代交代済



- オンプレミスのデータストレージロケーションと Amazon S3 との間でデータのインポートおよびエクスポートができる。
- Snowball ではすべてのリージョンで 80 TB モデルを使用可能
- 暗号化が強制、保管中や輸送中のデータを保護
- AWS Snowball マネジメントコンソール を使用
- オンプレミスのデータセンターと Snowball 間でローカルデータ転送を実行
- Snowball はそれ自体が配送コンテナ

【ユースケース】

移行／災害対策のデータ移行／データセンター統合／コンテンツ配信に伴るデータ移行

SnowballとSnowball Edge

Snowball EdgeはSnowball+コンピューティングという高性能な機能を有し、現在AWSはSnowball Edge利用を推奨

Snowball

- クライアント側で暗号化を実施
 - クライアント側にリッチなリソースが必要で、クライアント側のソフトウェアによるデータ転送を実施
 - 容量：80TB／アプライアンス
 - 用途：データ移行
 - クラスタリング：不可
 - ラックマウント：不可
 - 最大保持日数：90日
- 現在はSnowball Edgeを利用することが推奨されている。

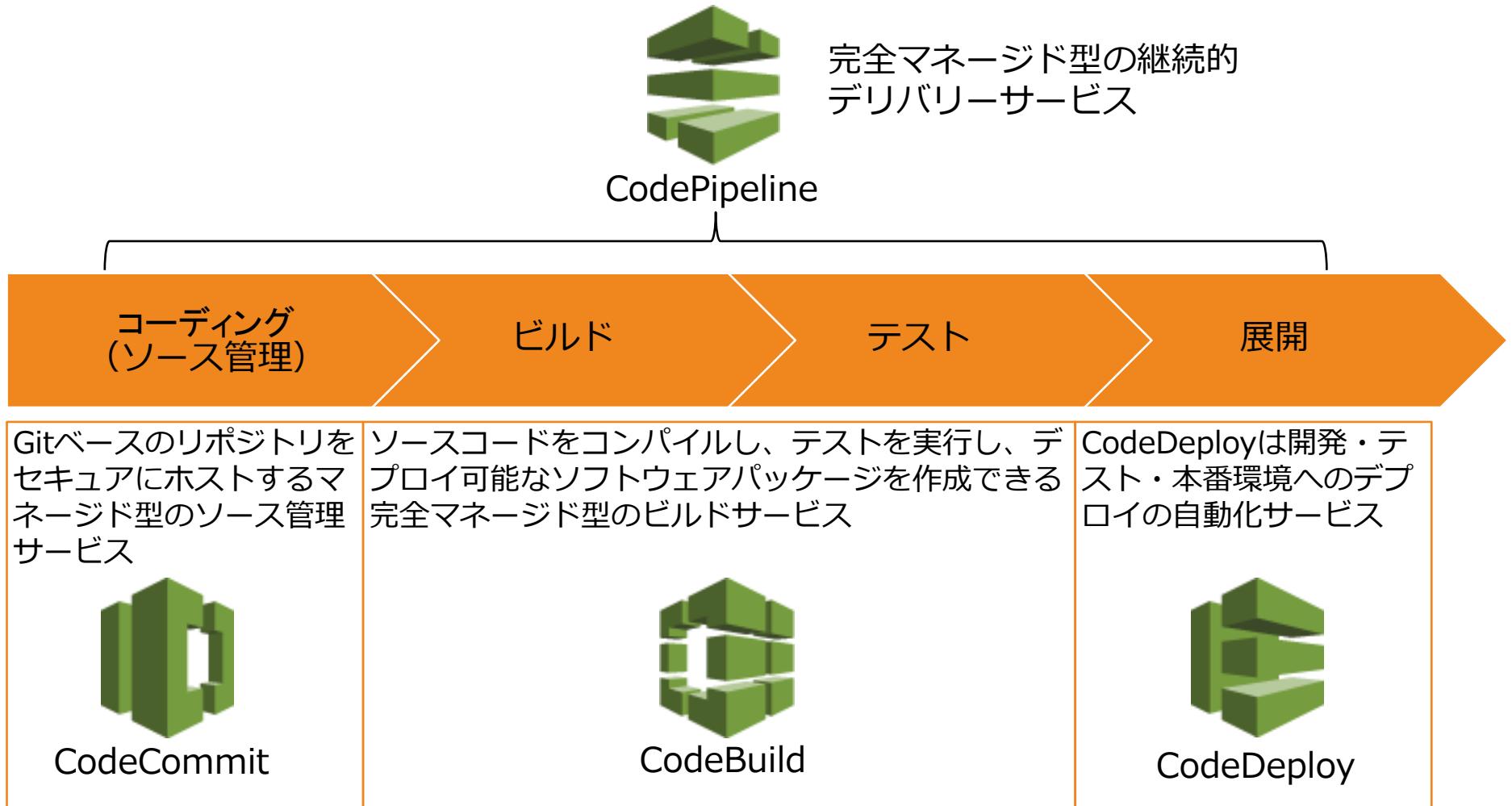
Snowball Edge

- Edge側で暗号化を実施
- 書込時にLambda関数を利用したデータ処理可能
アプライアンスに組み込まれたS3 Adapter For Snowballによりデータ転送を実施
- 容量：100TB（80TB利用）／アプライアンス
- 用途：データ移行+ローカルプロセッシング・ストレージとして利用
- クラスタリング：可
- ラックマウント：可
- 最大保持日数360日
- Snowball Edge Compute OptimizedのSnowball Edge Storage Optimizedの2タイプ

その他のサービス

Codeシリーズ

開発コードのGitベースのリポジトリ上でのコミット・実行・デプロイを自動化する一連のサービス



Kinesis

ストリームデータを収集・処理するためのフルマネージド型サービスで主に3つのサービスで構成される

Amazon Kinesis Data Streams

ストリームデータを処理するアプリケーションを構築

Amazon Kinesis Data Firehose

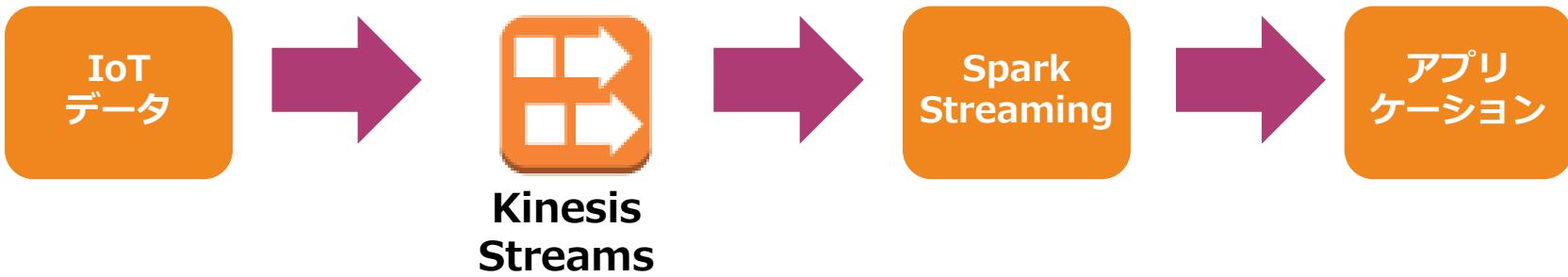
ストリームデータをS3やRedshiftなどへ簡単に配信

Amazon Kinesis Data Analytics

ストリームデータを標準的なSQLクエリでリアルタイムに可視化・分析

Amazon Kinesis Data Streams

ストリームデータ処理用の分析システムやアプリケーションを構築するサービス



Amazon Athena

Amazon S3 内のデータを直接、簡単に分析できるようにする
インタラクティブなクエリサービス



Amazon Rekognition

深層学習に基づいた画像認識および画像分析機能を提供する
サービス

Screenshot of the Amazon Rekognition Facial analysis demo interface.

The sidebar navigation includes:

- AWS logo
- Services dropdown
- Resource Groups dropdown
- Support dropdown
- Amazon Rekognition
- Metrics
- Demos
 - Object and scene detection
 - Image moderation
 - Facial analysis** (selected)
 - Celebrity recognition
 - Face comparison
 - Text in image
- Video Demos
- Video analysis
- Additional Resources
 - Getting started guide
 - Download SDKs
 - Developer resources
 - Pricing
 - FAQ
 - Forum

The main content area shows a family photo with facial detection boxes around each person and a dog. The results panel displays the following analysis:

Result	Confidence Score
looks like a face	99.9 %
appears to be male	99.8 %
age range	60 - 90 years old
smiling	98.7 %
appears to be happy	99.8 %
not wearing glasses	99.8 %

Buttons include "Choose a sample image", "Upload" (with "or drag and drop" option), "Use image URL", and "Go".

Amazon Polly

高度なディープラーニング技術を使用したテキストから音声を合成するサービス

Text-to-Speech

Listen, customize, and download speech. Integrate when you're ready.

Type or paste your text in the window, choose your language and region, choose a voice, choose Listen to speech, and then integrate it into your applications and services.

Plain text **SSML** **?**

Hi! My name is Jeff. I will read any text you type here.

944 characters remaining (1000 maximum) [Show default text](#) [Clear text](#)

Language and Region **Voice** [▶ Listen to speech](#)

English, US [▼](#)

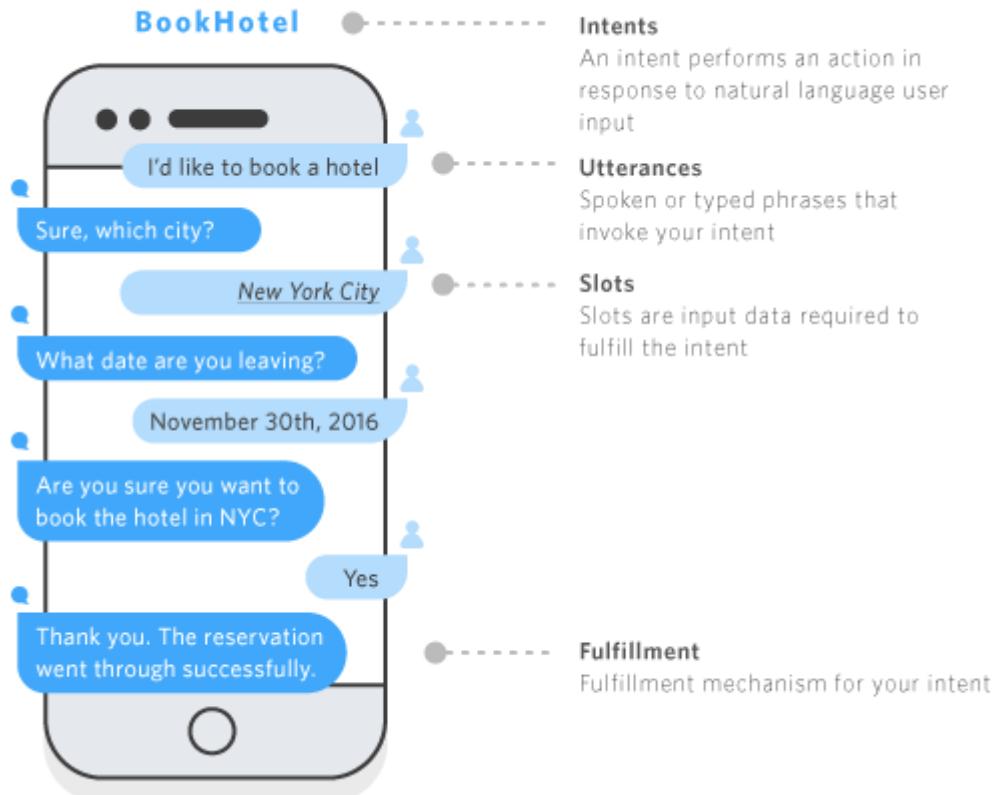
- Joanna, Female
- Salli, Female
- Kimberly, Female
- Kendra, Female
- Ivy, Female
- Justin, Male
- Joey, Male

[Save speech as MP3](#) [Change file format](#)



Amazon Lex

音声やテキストを使用して、任意のアプリケーションにチャットボットを構築するサービス



<https://aws.amazon.com/jp/lex/features/>

Amazon Transcribe

開発者が音声をテキストに変換する機能を提供するサービス

The screenshot shows a browser window with the URL `127.0.0.1:8000`. The page title is "Transcribe Medical" and it says "USING THE AMAZON TRANSCRIBE WEB SOCKET API". It includes fields for "Access ID" and "Secret Key", both of which are masked with dots. There is also a "Session Token (if using MFA)" field containing the text "SESSION TOKEN". Below these fields, there is a text area containing the following text:

The liver attachments to the adrenal kidney were divided and the liver was reflected superiorly. The vena cava was identified. The main renal vein was identified. Coming superior to the main renal vein, staying right on the vena cava, all small vessels were clipped and then divided. Coming along the superior pole of the kidney, the tumor was dissected free from top of the kidney with clips and Bovie. The harmonic scalpel was utilized superiorly and laterally. Posterior attachments were divided between clips and once the whole adrenal was mobilized, the adrenal vein and one large adrenal artery were noted, doubly clipped, and divided

Below this text area, there is a smaller text box containing the following text:

The liver attachments to the adrenal kidney were divided and the liver was reflected superior early.
The vena cava was identified.
The main renal vein was identified.
Coming superior to the main renal vein, staying right on the vena cava.
All small vessels were clipped and then divided.
Coming along the superior Pole of the kidney. The tumor was dissected free from top of the kidney.

At the bottom of the page, there are three buttons: "Start" (blue), "Stop" (blue), and "Clear Transcript" (grey). To the right of the "Stop" button is the AWS logo.

Amazon SageMaker

機械学習 (ML) モデルを迅速に構築、トレーニング、デプロイできるようにする完全マネージド型サービス

The screenshot shows the Amazon SageMaker Studio interface. On the left, a Jupyter notebook titled "xgboost_customer_churn.ipynb" is open, displaying Python code and corresponding output cells. The code is for preparing a dataset, splitting it into training, validation, and test sets, and uploading files to S3. The output cells show the execution of these commands. To the right of the notebook are two panels: a "Trial Component Chart" showing training loss over time, and a "Trial Component List" showing a table of completed training jobs.

Code snippets from the Jupyter notebook:

```
[ ]: model_data = pd.get_dummies(churn)
model_data = pd.concat([model_data['Churn?_True.'], model_data.drop(['Churn?', ...]]))

[ ]: train_data, validation_data, test_data = np.split(model_data.sample(frac=1), [int(len(model_data)*0.7), int(len(model_data)*0.15), len(model_data)-int(len(model_data)*0.15)])
train_data.to_csv('train.csv', header=False, index=False)
validation_data.to_csv('validation.csv', header=False, index=False)

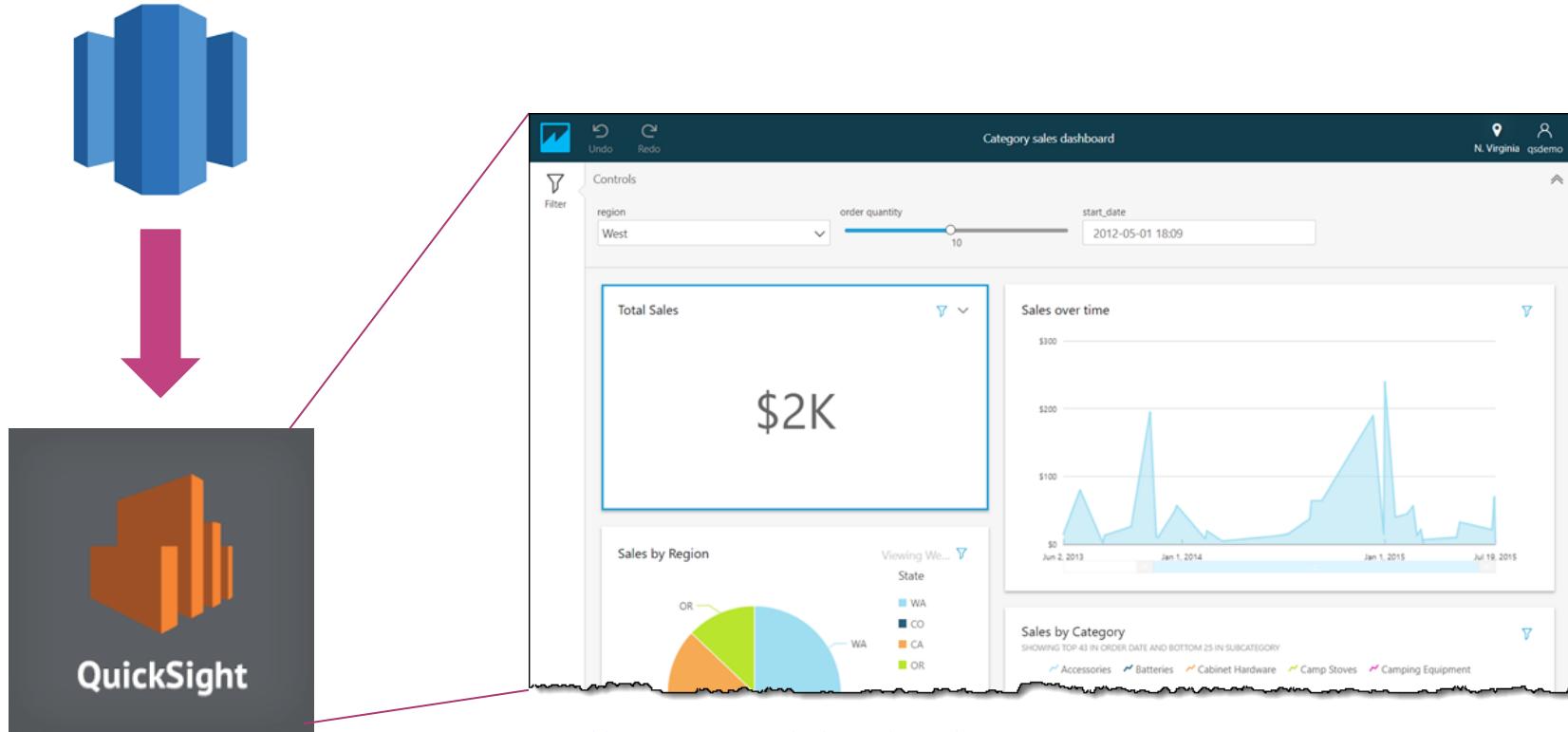
[ ]: boto3.Session().resource('s3').Bucket(bucket).Object(os.path.join(prefix, ...)).put_object(Body=...)
```

Trial Component List:

Status	Experiment	Type	Trial	...
Completed	customer-churn-pred...	Training job	Trial-3	Train...
Completed	customer-churn-pred...	Training job	Trial-2	Train...
Completed	customer-churn-pred...	Training job	Trial-1	Train...
Completed	customer-churn-pred...	Training job	Trial-0	Train...

Amazon QuickSight

QuickSightはデータを可視化・解析するためのBIツール。
RedShiftデータを可視化可能



<https://aws.amazon.com/jp/blogs/news/new-pay-per-session-pricing-for-amazon-quicksight-another-region-and-lots-more/>

AWS Glue

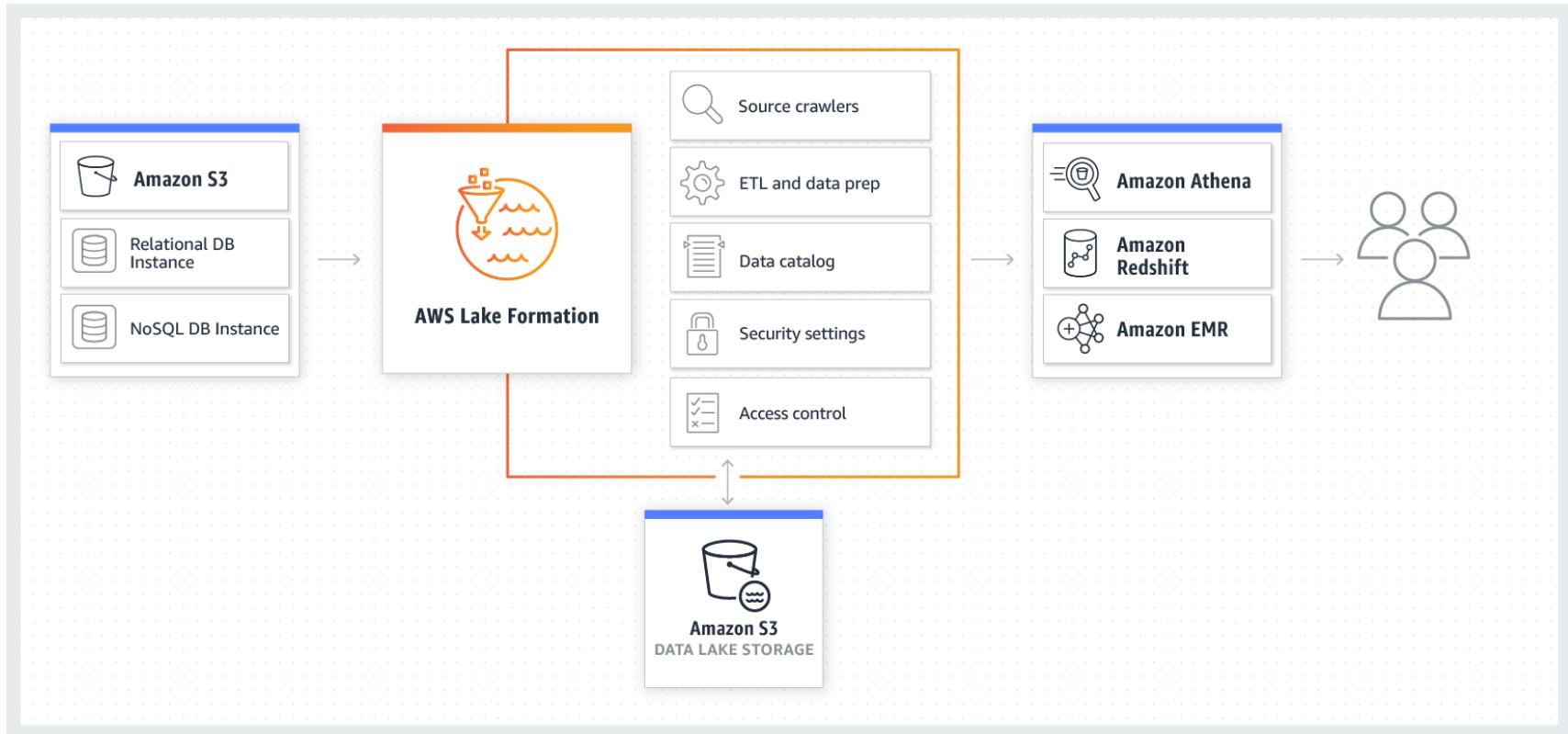
データを抽出、変換、ロード (ETL) を行う完全マネージド型のサービス



<https://aws.amazon.com/jp/glue/>

AWS Lake Formation

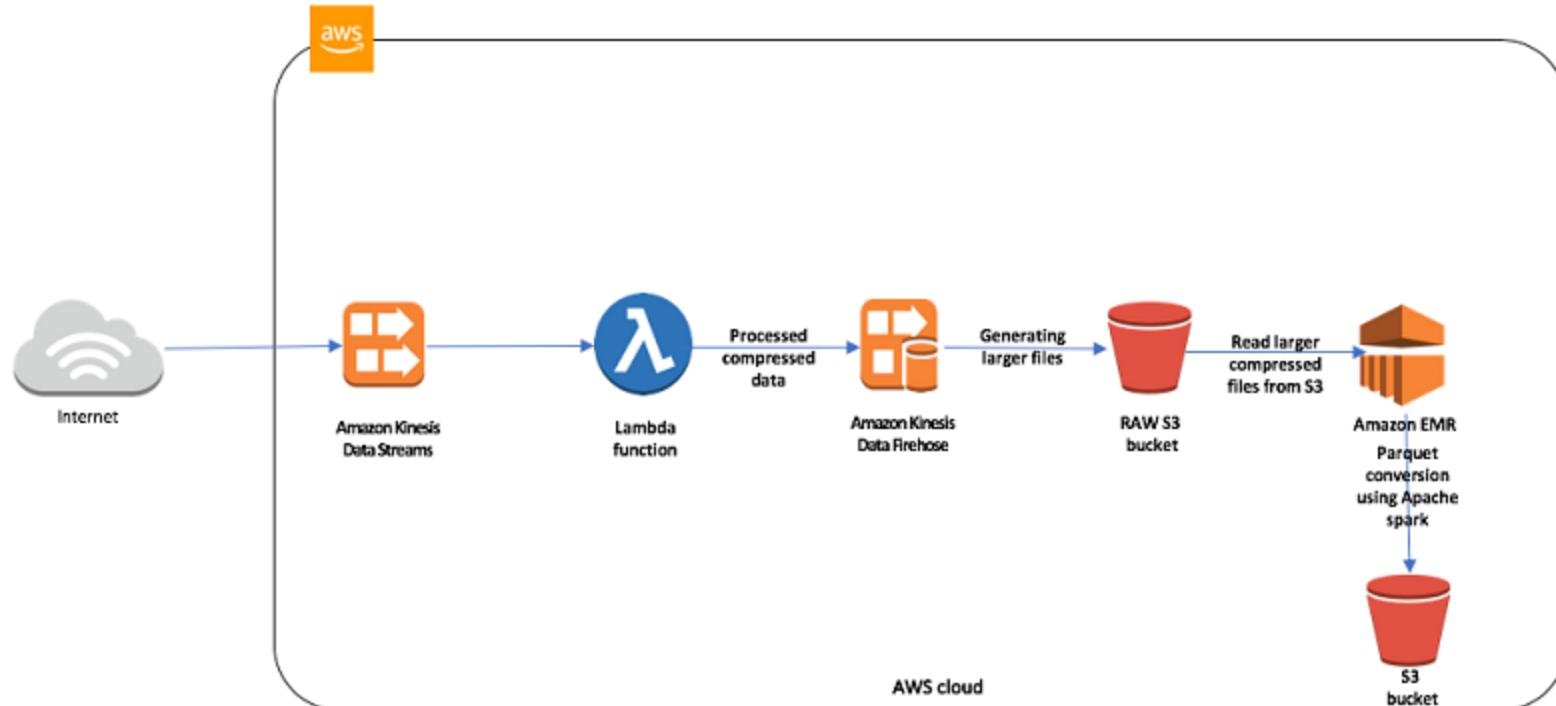
本来なら複雑な設定が必要なデータレイクの構成を簡単に素早く実現するサービス



<https://aws.amazon.com/jp/lake-formation/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>

Amazon EMR

Apache Spark、Apache Hive、Prestoなどのビッグデータフレームワークを使用して、大量データを処理・分析する



<https://aws.amazon.com/jp/blogs/news/optimizing-downstream-data-processing-with-amazon-kinesis-data-firehose-and-amazon-emr-running-apache-spark/>