

AWS認定ソリューションアーキテクト アソシエイト試験：短期突破講座

はじめに

本講座の内容

AWS認定ソリューションアーキテクトアソシエイト試験
の準備を最短で実施するための講座です。

本講座のコンセプト

アソシエイト試験対策講座は長い上に、また模擬試験も受けないと合格出来ない！

弊社のソリューションアーキテクトアソシエイト試験
コース

26時間

Udemyで最もユーザー数が多いアソシエイト試験
コース

18時間

Udemyで最も評価の高いアソシエイト試験コース

24時間

Udemyの最も時間が長いアソシエイト試験コース

83時間

本講座のコンセプト

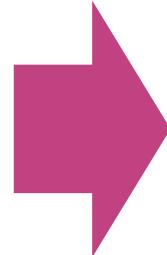
ハンズオンまで実施すると30時間以上は必要な上、模擬試験を3回以上は実施した方が良い。



本講座のコンセプト

実際に出題される試験範囲に絞って学習することが
合格への近道！！

実際に出題される
試験問題を確認



出題される問題
の範囲のみを学習

本講座のコンセプト

本番試験と模擬試験1625問から質問出題範囲を抽出・分析

本番試験3回分の試験パターン

195問

日本語のアソシエイト試験問題の最大ユーザー数の講座
(弊社所有)

390問

Udemyの最高評価のトップ3講座の1つ

260問

Udemyの最高評価のトップ3講座の1つ

390問

Udemyの最高評価のトップ3講座の1つ

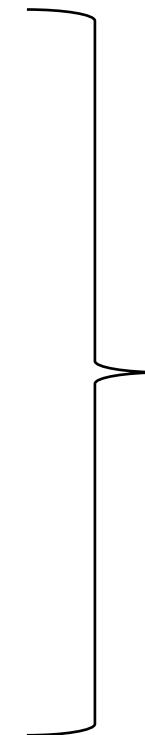
390問

合計：1625問

本講座のコンセプト

出題される範囲を数値的に算出して、学習すべき範囲と問題傾向をお教えします！

カテゴリー	出題数	出題率
S3	182	11.17%
EC2	145	8.90%
VPC	94	5.77%
Auto Scaling	76	4.66%
RDS	74	4.54%
EBS	65	3.99%
SQS	60	3.68%
ELB	58	3.56%
CloudFront	56	3.44%
IAM	54	3.31%
DynamoDB	52	3.19%
Lambda	50	3.07%
Route53	42	2.58%



62%

講座の内容

セクション	セクションで学ぶ内容
アソシエイト試験の概要	AWSの資格体系を把握しつつ、実際の試験問題からAWS認定ソリューションアーキテクト・アソシエイト試験の出題分野を確認します。
アソシエイト試験の出題問題の分析	1625問に及ぶアソシエイト試験問題から出題傾向を分析して、学習すべきAWSサービスの範囲を明確化します。
主要サービスの出題範囲① (IAM・S3・EC2・VPC)	6割以上が出題される主要サービスから、IAM・S3・EC2・VPCの問題形式を確認しながら、出題範囲を学習します。
主要サービスの出題範囲② (Auto Scaling・RDS・EBS・ELB)	6割以上が出題される主要サービスから、Auto Scaling・RDS・EBS・ELBの問題形式を確認しながら、出題範囲を学習します。
主要サービスの出題範囲③ (SQS・CloudFront・DynamoDB・Lambda・Route53)	6割以上が出題される主要サービスから、SQS・CloudFront・DynamoDB・Lambda・Route53の問題形式を確認しながら、出題範囲を学習します。

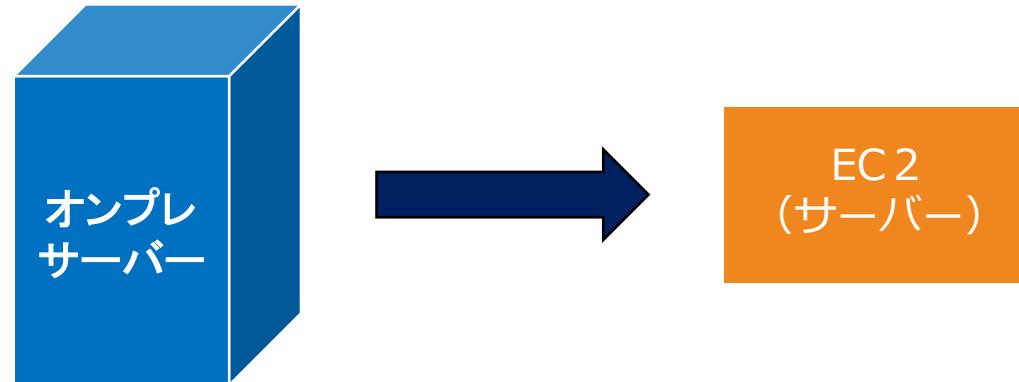
講座の内容

セクション	セクションで学ぶ内容
合格に必要なサービス群からの出題範囲	9割弱の問題に対応するための、残りの頻出問題を確認して、出題範囲を学習します。
高得点を目指すための出題範囲	95%以上の問題に対応するための、残りのレアな問題を確認して、出題範囲を学習します。
模擬試験	全てのレクチャーで出題された問題を模擬試験形式で復習します。

AWSとは何か？

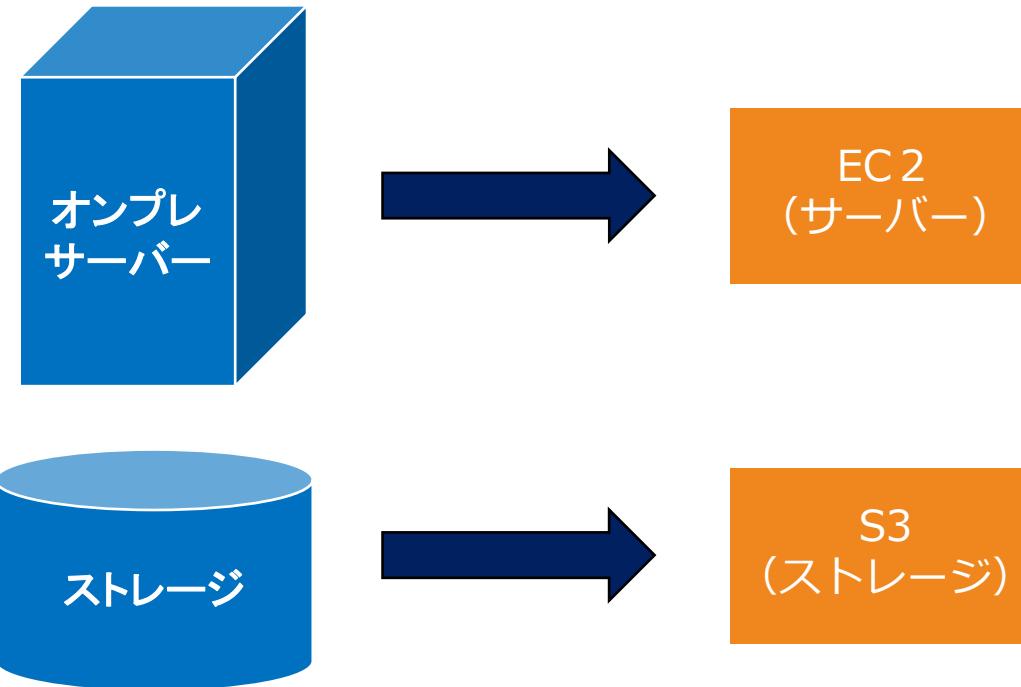
AWSとは

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

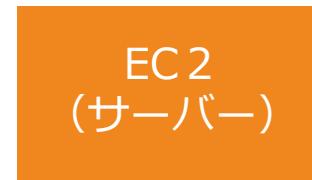


AWSとは

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



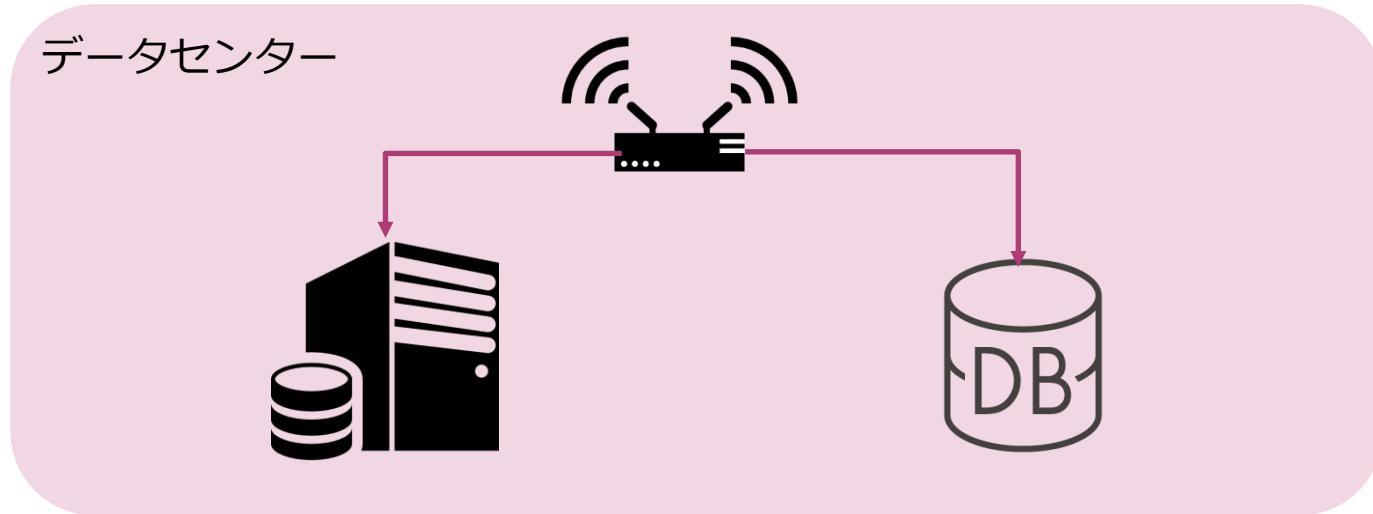
- ✓ 時間がかかる
- ✓ コストがかかる



- ✓ 数分で立ち上がる
- ✓ 無料から利用可能

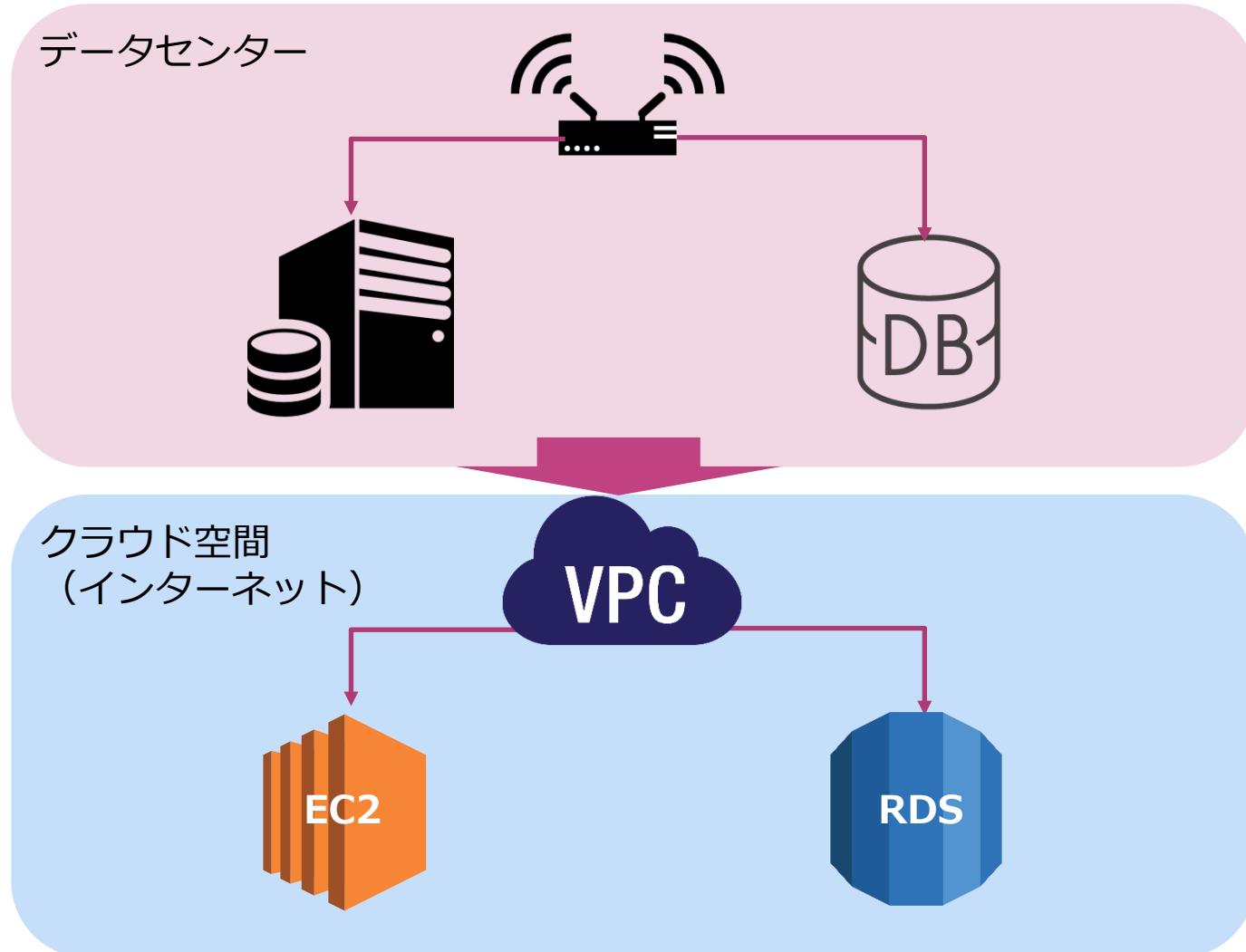
物理的な機器をネットサービスへ

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

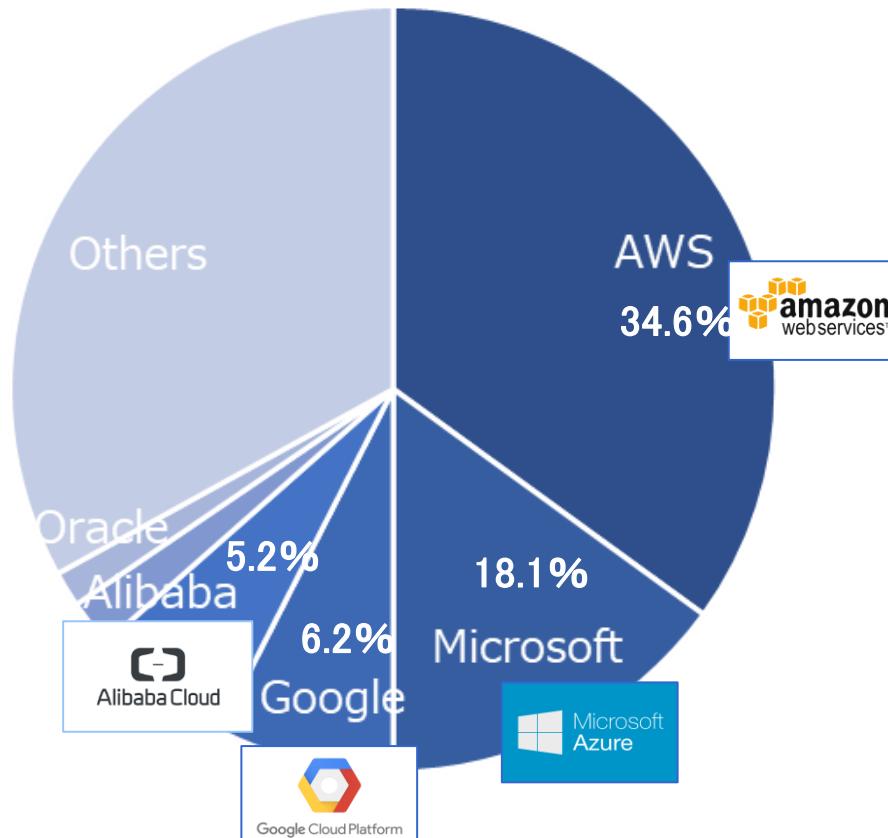
システム運用に必要な物理機器をインターネット経由で借りて
くることで、効率的なシステム管理が可能になる。



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ープしており圧倒的な存在である

2019年グローバルシェア



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

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

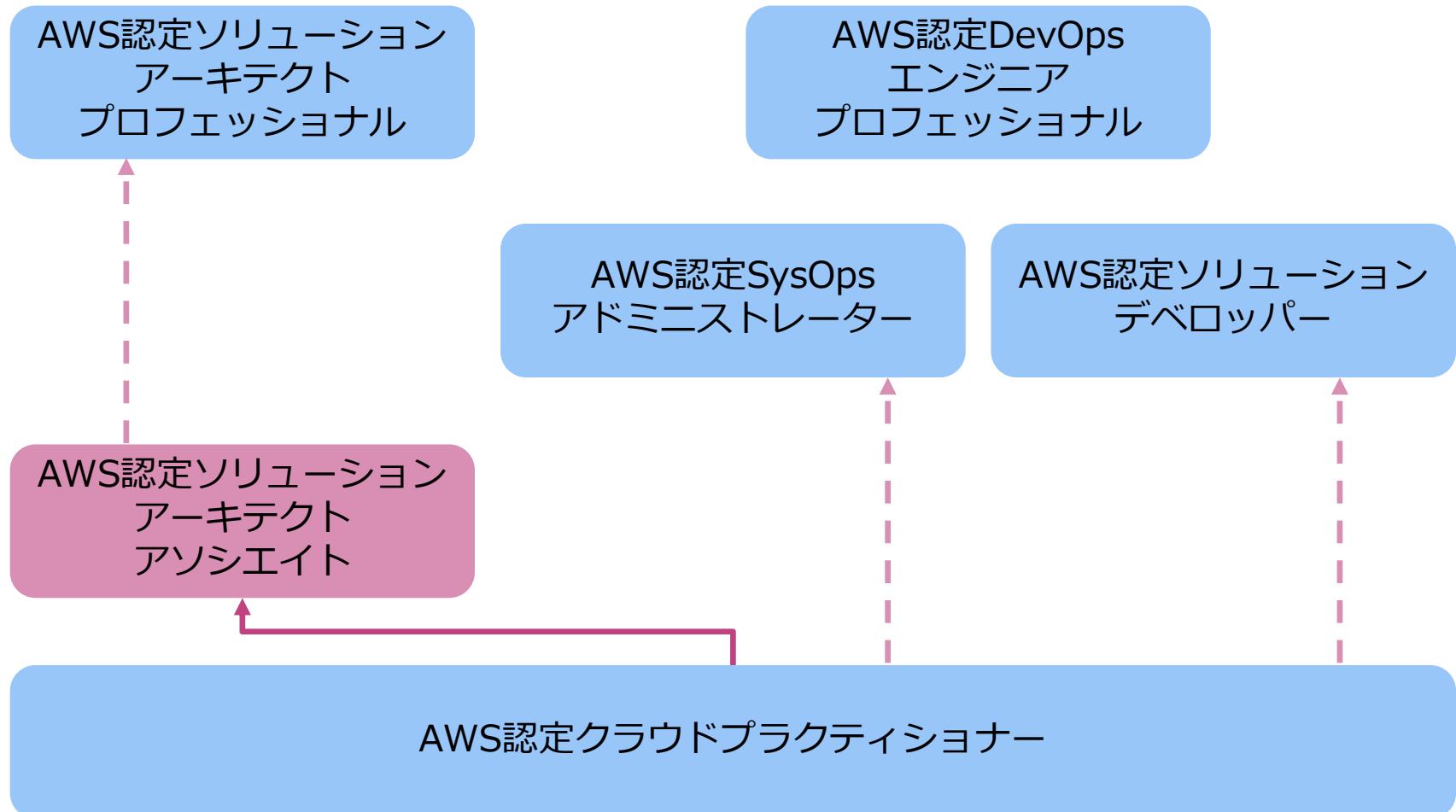
AWS認定ソリューション
アーキテクト
アソシエイト

AWS認定クラウドプラクティショナー



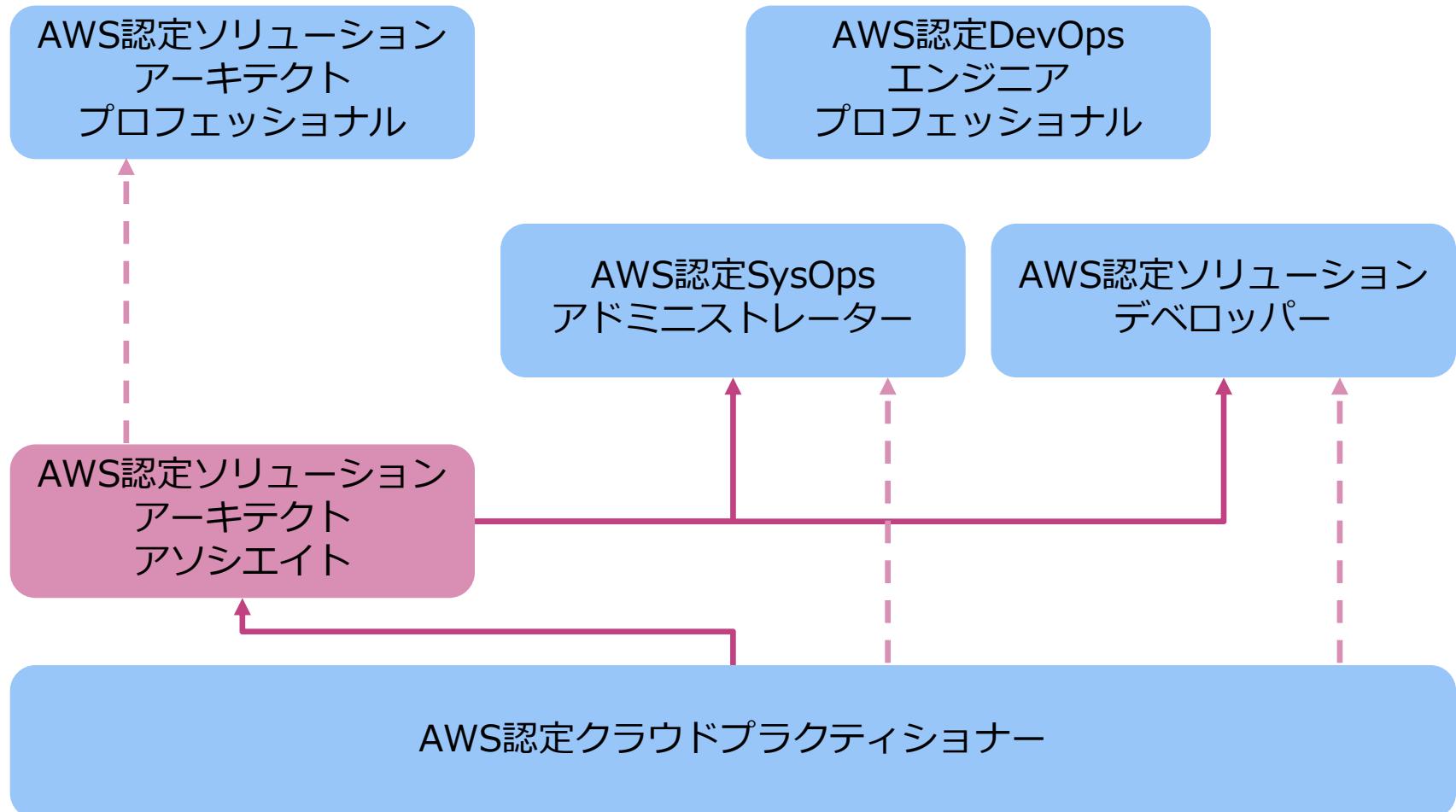
AWSの資格体系

AWS認定資格の取得レベルと理想的な取得順序



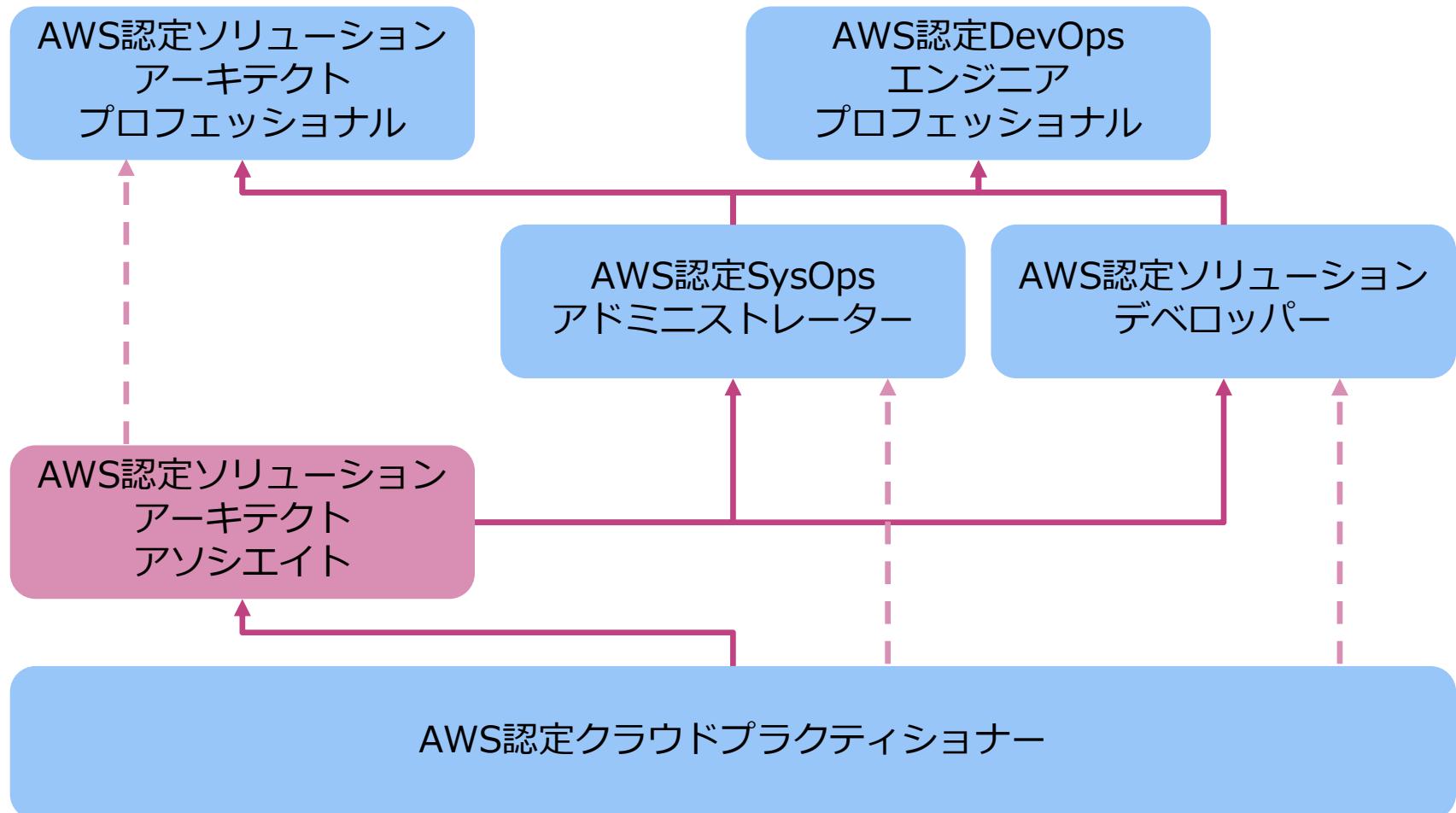
AWSの資格体系

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



アソシエイト 試験概要

受験生に求める能力

顧客要件に基づいてアーキテクチャ設計原則を使ったソリューションを定義する。

プロジェクトのライフサイクル全体を通じて、ベストプラクティスに基づいた実装ガイダンスを組織に提供する。

推奨される知識

- AWS 上で使用可能な、コスト効率が高く、フォールトトレラントでスケーラブルな分散システムを設計する 1 年間の実務経験
- コンピューティング、ネットワーキング、ストレージ、およびデータベース関連のAWS のサービスを使用した実務経験
- AWS のデプロイメントおよび管理サービスの実務経験
- AWS ベースのアプリケーションの技術要件を特定して定義する能力
- 特定の技術要件を満たす AWS のサービスを特定する能力
- AWS プラットフォーム上に安全で信頼性の高いアプリケーションを構築するために推奨されているベスト プラクティスに関する知識
- AWS クラウドで構築される基本的なアーキテクチャ原則の理解
- AWS グローバルインフラストラクチャの理解
- AWS に関連するネットワークテクノロジーの理解
- AWS が提供するセキュリティ機能とツール、およびそれらが従来のサービスとどのように関連しているかの理解

質問形式

- 選択問題: 正しい回答が 1 つと、間違った回答 (ディストラクタ) が 3 つあります。
- 複数回答: 5 つ以上のオプションのうち、正解が 2 つ以上あります。

合格基準

- 試験時間: 130分
- 質問数: 65問
- 得点範囲: 100点-1000点 (難易度調整された平均値)
- 合格点: 720点 (約72%)

質問パターン

【質問パターン①】

AWSサービスの選択／AWSサービスの特徴や機能の選択

質問パターン

【質問パターン①】

AWSサービスの選択／AWSサービスの特徴や機能の選択
⇒AWS認定クラウドプラクティショナーと重複

質問パターン

【質問パターン①】

AWSサービスの選択／AWSサービスの特徴や機能の選択
⇒AWS認定クラウドプラクティショナーと重複

あなたの会社はユーザーが動画を共有するアプリケーションを運用しています。このアプリケーションは、ユーザーによってアップロードされた動画を処理するためのEC2インスタンスにホストされています。ビデオを処理し公開するEC2ワーカープロセスを有しており、Auto Scalingグループが設定されています。

ワーカープロセスの信頼性を高めるため利用すべきサービスを選択してください。

- 1) Amazon SQS
- 2) Amazon SNS
- 3) Amazon SES
- 4) CloudFront

質問パターン

【質問パターン①】

AWSサービスの選択／AWSサービスの特徴や機能の選択
⇒AWS認定クラウドプラクティショナーと重複

【質問パターン②】

AWSサービスの適切な設定方法の選択

質問パターン

【質問パターン②】

AWSサービスの適切な設定方法やトラブル解消方法の選択

あなたはソリューションアーキテクトとして、AWS上にSFAを構築しています。このSFAには営業担当者が毎日売上高をアップロードする業務要件があります。さらに、その記録は営業レポート用に保存する必要があります。レポートの保存用には耐久性と可用性のあるストレージが求められます。SFAを利用する営業担当者が多いため、何らかの操作ミスなどで、これらの記録が誤って消去されないようになりますことが重要な要件となっています。これらの要件を満たすためのデータ保護施策を選択してください。

- 1) S3を利用してバージョニング機能を有効化する。
- 2) EBSにデータを蓄積してスナップショットを定期的に自動取得する
- 3) S3にデータを蓄積してスナップショットを定期的に自動取得する
- 4) RDSにデータを蓄積してスナップショットを定期的に自動取得する

質問パターン

【質問パターン①】

AWSサービスの選択／AWSサービスの特徴や機能の選択
⇒AWS認定クラウドプラクティショナーと重複

【質問パターン②】

AWSサービスの適切な設定方法の選択

【質問パターン③】

様々なAWSサービスを組み合わせた最適なアーキテクチャ構成の選択

質問パターン

【質問パターン③】

様々なAWSサービスを組み合わせた最適なアーキテクチャ構成の選択

あなたは、AWS上にトランザクション処理をしつつ、コンテンツを配信する2層Webアプリケーションを構築しています。データ層では、オンライントランザクション処理（OLTP）データベースを利用しています。WEB層では柔軟でスケーラブルなアーキテクチャ構成を実現する必要があります。

この要件を満たすための最適な方法を選択してください。

- 1) EC2インスタンスにELBとAuto Scalingグループを設定する。
- 2) RDSのマルチAZ構成を設定する。
- 3) EC2インスタンスをマルチAZに展開してRoute53によるフェイルオーバーラーティングを実施する
- 4) EC2インスタンスを予測キャパシティよりも多く設置する

アソシエイト試験の分野

試験範囲

Well Architected Frameworkの5つの設計原則のうちで、「運用上の優秀性」以外の4つが試験範囲

分野	比率
分野 1 レジリエントアーキテクチャの設計	30%
分野 2 高パフォーマンスアーキテクチャの設計	28%
分野 3 セキュアなアプリケーションとアーキテクチャの設計	24%
分野 4 コスト最適化アーキテクチャの設計	18%

分野 1: レジリエントアーキテクチャの設計

- 1.1 多層アーキテクチャソリューションの設計
- 1.2 可用性の高いアーキテクチャやフォールトトレラントなアーキテクチャの設計
- 1.3 AWS のサービスを使用したデカップリングメカニズムの設計
- 1.4 適切な回復力のあるストレージの選択

分野 1: レジリエントアーキテクチャの設計

■ 1.1 多層アーキテクチャソリューションの設計

あなたはソリューションアーキテクトとしてWebサーバとデータベースサーバからなるWebアプリケーションをAWSにホストする計画をしています。プライベートサブネットにデータベースサーバーを、パブリックサブネットにWEBサーバーを設置して、インスタンス間の通信を行う必要がありますが、上手く通信されません。

この問題を解決するための対応を選択してください。

- 1) セキュリティグループでトラフィックを制御する
- 2) VPCエンドポイントでトラフィックを制御する
- 3) ネットワークACLでトラフィックを制御する
- 4) IAMロールでWEBサーバにデータベースサーバへのアクセスを許可する。

分野 1: レジリエントアーキテクチャの設計

■ 1.1 多層アーキテクチャソリューションの設計

あなたはソリューションアーキテクトとしてWebサーバとデータベースサーバからなるWebアプリケーションをAWSにホストする計画をしています。プライベートサブネットにデータベースサーバーを、パブリックサブネットにWEBサーバーを設置して、インスタンス間の通信を行う必要がありますが、上手く通信されません。

この問題を解決するための対応を選択してください。

- 1) セキュリティグループでトラフィックを制御する
- 2) VPCエンドポイントでトラフィックを制御する
- 3) ネットワークACLでトラフィックを制御する
- 4) IAMロールでWEBサーバにデータベースサーバへのアクセスを許可する。

分野 1: レジリエントアーキテクチャの設計

■ 1.1 多層アーキテクチャソリューションの設計

あなたはソリューションアーキテクトとしてWebサーバとデータベースサーバからなるWebアプリケーションをAWSにホストする計画をしています。プライベートサブネットにデータベースサーバーを、パブリックサブネットにWEBサーバーを設置して、インスタンス間の通信を行う必要がありますが、上手く通信されません。この問題を解決するための対応を選択してください。

1) セキュリティグループでトラフィックを制御する

オプション1が正解となります。プライベートサブネットにデータベースサーバーを、パブリックサブネットにWEBサーバーを設置して、インスタンス間の通信を行うためには、その通信を許可する適切なセキュリティグループの設定が不可欠となります。セキュリティグループによりEC2インスタンス間でIPアドレスを指定することでトラフィックを制御することができます。

分野 1: レジリエントアーキテクチャの設計

1.2 可用性の高いアーキテクチャやフォールトトレラントなアーキテクチャの設計

カスタマーリレーションシップマネジメント (CRM) アプリケーションは、アプリケーションロードバランサーの背後にある複数のアベイラビリティゾーンの Amazon EC2 インスタンスで実行されます。

これらのインスタンスの1つに障害が発生した場合、どうなりますか？

- 1) ロードバランサーが、傷害が発生したインスタンスへのリクエストの送信を停止する。
- 2) ロードバランサーが、障害が発生したインスタンスを終了する。
- 3) ロードバランサーが、障害が発生したインスタンスを自動的に置換する。
- 4) ロードバランサーが、インスタンスが置換されるまで、504 ゲートウェイ タイムアウト エラーを返す。

分野 1: レジリエントアーキテクチャの設計

1.2 可用性の高いアーキテクチャやフォールトトレラントなアーキテクチャの設計

カスタマーリレーションシップマネジメント (CRM) アプリケーションは、アプリケーションロードバランサーの背後にある複数のアベイラビリティゾーンの Amazon EC2 インスタンスで実行されます。これらのインスタンスの1つに障害が発生した場合、どうなりますか？

- 1) ロードバランサーが、傷害が発生したインスタンスへのリクエストの送信を停止する。

オプション1が正解となります。アプリケーションロードバランサー (ALB) は、正常なインスタンスにのみリクエストを送信します。ALBは、ターゲットグループ内のターゲットに対して定期的なヘルスチェックを実行します。設定可能な回数だけ連続してヘルスチェックに不合格だったインスタンスは、正常ではないと見なされます。ロードバランサーは、次のヘルスチェックに合格するまで、インスタンスにリクエストを送信しなくなります。

分野 1: レジリエントアーキテクチャの設計

■ 1.3 AWS のサービスを使用したデカップリングメカニズムの設計

企業は非同期処理を実行する必要があり、分離されたアーキテクチャの一部として Amazon SQSを持っています。同社は、ポーリングリクエストからの空の応答件数を最小限に抑えることを望んでいます。

空の応答を減らすために、ソリューションアーキテクトは何をすべきでしょうか？

- 1) キューの最大メッセージ保存期間を増やす。
- 2) キューのリドライブポリシーの最大受信数を増やす。
- 3) キューの既定の可視性タイムアウトを増やす。
- 4) キューの受信メッセージ待機時間を延長する。

分野 1: レジリエントアーキテクチャの設計

■ 1.3 AWS のサービスを使用したデカップリングメカニズムの設計

企業は非同期処理を実行する必要があり、分離されたアーキテクチャの一部として Amazon SQSを持っています。同社は、ポーリングリクエストからの空の応答件数を最小限に抑えることを望んでいます。

空の応答を減らすために、ソリューションアーキテクトは何をすべきでしょうか？

4) キューの受信メッセージ待機時間を延長する。

キューの受信メッセージ待ち時間の秒数プロパティが 0 より大きい値に設定されている場合、ロングポーリング が有効になります。ロングポーリングでは、メッセージが受信メッセージリクエストに送信されるまで Amazon SQS が待機できるため、空のレスポンス件数が減ります。

分野 1: レジリエントアーキテクチャの設計

■ 1.4 適切な回復力のあるストレージの選択

企業は現在、オンプレミスアプリケーションのデータをローカルドライブに格納しています。最高技術責任者は、データを Amazon S3 に保存してハードウェアコストを削減したいのですが、アプリケーションに変更を加えたくないと考えています。レイテンシーを最小限に抑えるには、頻繁にアクセスするデータをローカルで使用できるようにする必要があります。

ローカルストレージのコストを削減するためにソリューションアーキテクトが実装できる、信頼性の高い耐久性のあるソリューションとは何ですか？

- 1) ローカルサーバーに SFTP クライアントをデプロイし、SFTP 用 AWS 転送を使用してデータを Amazon S3 に転送する。
- 2) キャッシュ型ボリュームモードで設定された AWS Storage Gateway のボリューム型ゲートウェイをデプロイする。
- 3) ローカルサーバーに AWS DataSyncエージェントをデプロイし、S3 バケットを転送先として設定する。
- 4) 保管型ボリュームモードで設定された AWS Storage Gateway ボリューム型ゲートウェイをデプロイする。

分野 1: レジリエントアーキテクチャの設計

■ 1.4 適切な回復力のあるストレージの選択

企業は現在、オンプレミスアプリケーションのデータをローカルドライブに格納しています。最高技術責任者は、データを Amazon S3 に保存してハードウェアコストを削減したいのですが、アプリケーションに変更を加えたくないと考えています。レイテンシーを最小限に抑えるには、頻繁にアクセスするデータをローカルで使用できるようにする必要があります。ローカルストレージのコストを削減するためにソリューションアーキテクトが実装できる、信頼性の高い耐久性のあるソリューションとは何ですか？

2) キャッシュ型ボリュームモードで設定された AWS Storage Gateway のボリューム型ゲートウェイをデプロイする。

オプション 2 が正解となります。AWS Storage Gateway ボリュームゲートウェイは、オンプレミスのアプリケーションサーバーからインターネットスモールコンピュータシステムインターフェース (iSCSI) デバイスとしてマウントできるクラウドベースのストレージボリュームを、オンプレミスのソフトウェアアプリケーションに接続します。キャッシュ型ボリュームモードでは、すべてのデータが Amazon S3 に保存され、頻繁にアクセスするデータのコピーがローカルに保存されます。

分野2：高パフォーマンスアーキテクチャの設計

- 2.1 ワークロードに対する伸縮自在でスケーラブルなコンピューティングソリューションの識別
- 2.2 ワークロードに対するパフォーマンスとスケーラブルなストレージソリューションの選択
- 2.3 ワークロードに対するパフォーマンスが高いネットワーキングソリューションの選択
- 2.4 ワークロードに対するパフォーマンスの高いデータベースソリューションの選択

分野2：高パフォーマンスアーキテクチャの設計

■ 2.1 ワークロードに対する伸縮自在でスケーラブルなコンピューティングソリューションの識別

あなたは、AWS上にトランザクション処理をしつつ、コンテンツを配信する2層Webアプリケーションを構築しています。データ層では、オンライントランザクション処理(OLTP)データベースを利用しています。WEB層では柔軟でスケーラブルなアーキテクチャ構成を実現する必要があります。

この要件を満たすための最適な方法を選択してください。

- 1) EC2インスタンスにELBとAuto Scalingグループを設定する。
- 2) RDSのマルチAZ構成を設定する。
- 3) EC2インスタンスをマルチAZに展開してRoute53によるフェイルオーバーラーティングを実施する
- 4) EC2インスタンスを予測キャパシティよりも多く設置する

分野2：高パフォーマンスアーキテクチャの設計

■ 2.1 ワークロードに対する伸縮自在でスケーラブルなコンピューティングソリューションの識別

あなたは、AWS上にトランザクション処理をしつつ、コンテンツを配信する2層Webアプリケーションを構築しています。データ層では、オンライントランザクション処理(OLTP) データベースを利用しています。WEB層では柔軟でスケーラブルなアーキテクチャ構成を実現する必要があります。この要件を満たすための最適な方法を選択してください。

1) EC2インスタンスにELBとAuto Scalingグループを設定する。

オプション1が正解となります。AWSで柔軟でスケーラブルなサーバー処理を実現するために、EC2インスタンスに対してAuto ScalingとELBを設定することで達成することができます。ELBがトラフィックを複数インスタンスに分散することで冗長性を高め、かつAuto Scalingが高負荷時のスケーリングを自動で実行してくれます。

分野2：高パフォーマンスアーキテクチャの設計

■ 2.2 ワークロードに対するパフォーマンスとスケーラブルなストレージソリューションの選択

ある企業はAWSでホストされる一連のEC2インスタンスを運用しています。これらは全てLinuxベースのインスタンスであり、標準ファイルインターフェースを介して、共有データへとアクセスが必要となります。データが保存されるストレージは複数インスタンスから利用されるため、強い整合性やファイルロックが必要です。そこで、あなたはソリューションアーキテクトとして、最適なストレージを検討しています。

この要件を満たす最適なストレージを選択してください。

- 1) S3
- 2) EBS
- 3) Glacier
- 4) EFS

分野2：高パフォーマンスアーキテクチャの設計

■ 2.2 ワークロードに対するパフォーマンスとスケーラブルなストレージソリューションの選択

ある企業はAWSでホストされる一連のEC2インスタンスを運用しています。これらは全てLinuxベースのインスタンスであり、標準ファイルインターフェースを介して、共有データへとアクセスが必要となります。データが保存されるストレージは複数インスタンスから利用されるため、強い整合性やファイルロックが必要です。そこで、あなたはソリューションアーキテクトとして、最適なストレージを検討しています。この要件を満たす最適なストレージを選択してください。

4) EFS

オプション4が正解となります。EFSを利用してすることで、複数のEC2インスタンスが同時にEFSのファイルシステムにアクセスしてデータを共有することができます。EFSはファイルシステムインターフェイスとファイルシステムのアクセスセマンティクス(強い整合性やファイルのロックなど)が用意されており、最大数千のAmazon EC2インスタンスからの同時アクセスが可能です。

分野2：高パフォーマンスアーキテクチャの設計

■ 2.3 ワークロードに対するパフォーマンスが高いネットワーキングソリューションの選択

ある会社はAWSのプライベートサブネットとパブリックサブネットに配置されたインフラを運用しています。 プライベートサブネットにはデータベースサーバーが設置され、プライベートサブネット内のインスタンスがインターネット側へ返信トラフィックを送信するため、パブリックサブネットにNATインスタンスが設置されています。 あなたは最近になりNATインスタンスがボトルネックになりつつあることを発見しました。

あなたはどのように改善するべきでしょうか。

- 1) 広帯域幅にするためのVPCコネクションを利用する
- 2) VPCエンドポイントを利用したアクセス設定にする
- 3) NATインスタンスをNATゲートウェイに変更する
- 4) NATインスタンスのインスタンスを拡張・増強する。

分野2：高パフォーマンスアーキテクチャの設計

■ 2.3 ワークロードに対するパフォーマンスが高いネットワーキングソリューションの選択

ある会社はAWSのプライベートサブネットとパブリックサブネットに配置されたインフラを運用しています。プライベートサブネットにはデータベースサーバーが設置され、プライベートサブネット内のインスタンスがインターネット側へ返信トラフィックを送信するため、パブリックサブネットにNATインスタンスが設置されています。あなたは最近になりNATインスタンスがボトルネックになりつつあることを発見しました。あなたはどのように改善するべきでしょうか。

3) NATインスタンスをNATゲートウェイに変更する

オプション3が正解となります。NATゲートウェイは、NATインスタンスの代わりに使用できるマネージド型サービスです。これはAWS側で拡張性などの性能が保証されているため、NATゲートウェイを利用することでNATインスタンスのボトルネックの改善につながります。NATインスタンス自体のインスタンスタイプを変更するなどのスケーリングも効果がありますが、問題が将来発生しないことを保証するものではありません。したがって、NATインスタンスをNATゲートウェイへと変更することで、容易にパフォーマンスを向上して、ボトルネックを解消することができます。

分野2：高パフォーマンスアーキテクチャの設計

■ 2.4 ワークロードに対するパフォーマンスの高いデータベースソリューションの選択

あなたはゲーム会社のシステム開発担当として、開発中のゲームで利用するデータベースを構築しています。このゲームではユーザーの行動データ記録に応じてアイテムが出現する機能を実装する必要があり、ユーザー行動データの高速な処理が求められています。

この要件を満たすためのサービスを選択してください。

- 1) Redshift
- 2) ElastiCache
- 3) Aurora
- 4) RDS

分野2：高パフォーマンスアーキテクチャの設計

■ 2.4 ワークロードに対するパフォーマンスの高いデータベースソリューションの選択

あなたはゲーム会社のシステム開発担当として、開発中のゲームで利用するデータベースを構築しています。このゲームではユーザーの行動データ記録に応じてアイテムが出現する機能を実装する必要があり、ユーザー行動データの高速な処理が求められています。

この要件を満たすためのサービスを選択してください。

2) ElastiCache

オプション2が正解となります。ElastiCacheはインメモリによるキーバリューストア型の高性能データベースです。主な目的はデータのコピーに超高速（ミリ秒以下のレイテンシー）で低成本なアクセスを提供することです。よって、高速にデータ処理する場合には最適なデータベースであり、ユーザー行動データの高速な処理には最適で、行動データ記録に応じたリアルタイムのランキング処理やアイテム出現などを実現することが可能です。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

- 3.1 AWS リソースへのセキュアなアクセスの設計
- 3.2 セキュアなアプリケーション階層の設計
- 3.3 適切なデータセキュリティオプションの選択

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.1 AWS リソースへのセキュアなアクセスの設計

企業は、複数のアベイラビリティーゾーン全体にわたる VPC で、公開されている 3 層 Web アプリケーションを実行します。プライベートサブネットで実行されているアプリケーション層の Amazon EC2インスタンスでは、インターネットからソフトウェアパッチをダウンロードする必要があります。ただし、インターネットから直接インスタンスにアクセスすることはできません。

インスタンスが必要なパッチをダウンロードできるようにするために実行すべきアクションはどれですか? (2 つ選択してください。)

- 1) パブリックサブネットで NAT ゲートウェイを構成する。
- 2) インターネットトラフィック用の NAT ゲートウェイへのルートがあるカスタムルートテーブルを定義し、それをアプリケーション層のプライベートサブネットに関連付ける。
- 3) Elastic IP アドレスをアプリケーションインスタンスに割り当てる。
- 4) インターネットトラフィック用のインターネットゲートウェイへのルートがあるカスタムルートテーブルを定義し、それをアプリケーション層のプライベートサブネットに関連付ける。
- 5) プライベートサブネットで NAT インスタンスを設定する。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.1 AWS リソースへのセキュアなアクセスの設計

企業は、複数のアベイラビリティーゾーン全体にわたる VPC で、公開されている 3 層 Web アプリケーションを実行します。プライベートサブネットで実行されているアプリケーション層の Amazon EC2インスタンスでは、インターネットからソフトウェアパッチをダウンロードする必要があります。ただし、インターネットから直接インスタンスにアクセスすることはできません。インスタンスが必要なパッチをダウンロードできるようにするために実行すべきアクションはどれですか? (2 つ選択してください。)

- 1) パブリックサブネットで NAT ゲートウェイを構成する。
- 2) インターネットトラフィック用の NAT ゲートウェイへのルートがあるカスタムルートテーブルを定義し、それをアプリケーション層のプライベートサブネットに関連付ける。

オプション 1 と 2 が正解となります。NAT ゲートウェイは、プライベートサブネット内のインスタンスからインターネットまたは他の AWS サービスにトラフィックを転送し、その応答をインスタンスに送り返します。NAT ゲートウェイが作成された後、プライベートサブネットのルートテーブルを更新して、インターネットトラフィックを NAT ゲートウェイに向ける必要があります。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.2 セキュアなアプリケーション階層の設計

ある企業ではAWS上でホストしているアプリケーションを運用しています。このアプリケーションはVPCと2つのパブリックサブネットを利用しておおり、1つのサブネットではインターネット経由でユーザーがWebサーバーにアクセスし、もう1つはデータベースサーバーが設置されたサブネットです。あなたはセキュリティ担当者としてアーキテクチャのセキュリティを向上させる検討を開始しました。WEBサーバーへのアクセスは社内のイントラネットからのアクセスや社員PCからのインターネットアクセスに限られており、オープンなWEBサービスのようなインターネットアクセスは必要としません。

次のうち最もセキュリティが高い構成を選択してください。

- 1) データベースサーバーをプライベートサブネットに移動して、RDSに移行する。
- 2) パブリックサブネットにNATゲートウェイを設定して、プライベートサブネットにRDSを設置する。
- 3) WEBサーバーをプライベートサブネットに移動する。
- 4) データベースとWEBサーバーをプライベートサブネットに移動する。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.2 セキュアなアプリケーション階層の設計

ある企業ではAWS上でホストしているアプリケーションを運用しています。このアプリケーションはVPCと2つのパブリックサブネットを利用しておおり、1つのサブネットではインターネット経由でユーザーがWebサーバーにアクセスし、もう1つはデータベースサーバーが設置されたサブネットです。あなたはセキュリティ担当者としてアーキテクチャのセキュリティを向上させる検討を開始しました。WEBサーバーへのアクセスは社内のイントラネットからのアクセスや社員PCからのインターネットアクセスに限られており、オープンなWEBサービスのようなインターネットアクセスは必要としません。

次のうち最もセキュリティが高い構成を選択してください。

4) データベースとWEBサーバーをプライベートサブネットに移動する。

オプション4が正解となります。WEBサーバーへのアクセスは社内ネットからのアクセスや社員PCを利用したインターネットアクセスに限られており、オープンなWEBサービスのような不特定多数のインターネットアクセスは必要としているため、パブリックサブネットでのWEBサーバーへのインターネットアクセスは必要ありません。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.3 適切なデータセキュリティオプションの選択

企業のセキュリティチームは、クラウドに保存されているすべてのデータを、オンプレミスに保存された暗号化キーを使用して保管時に必ず暗号化する必要があります。

これらの要件を満たす暗号化オプションはどれですか。(2つ選択してください。)

- 1) Amazon S3 管理キー (SSE-S3) でサーバー側の暗号化を使用する。
- 2) AWS KMS 管理キー (SSE-KMS) でサーバー側暗号化を使用する。
- 3) 顧客が提供するキー (SSE-C) でサーバー側暗号化を使用する。
- 4) クライアント側の暗号化を使用して、保存時の暗号化を提供する。
- 5) Amazon S3 イベントによってトリガーされる AWS Lambda 関数を使用し、顧客のキーを使ってデータを暗号化する。

分野 3: セキュアなアプリケーションとアーキテクチャの設計

3.3 適切なデータセキュリティオプションの選択

企業のセキュリティチームは、クラウドに保存されているすべてのデータを、オンプレミスに保存された暗号化キーを使用して保管時に必ず暗号化する必要があります。これらの要件を満たす暗号化オプションはどれですか。(2つ選択してください。)

- 3) 顧客が提供するキー (SSE-C) でサーバー側暗号化を使用する。
- 4) クライアント側の暗号化を使用して、保存時の暗号化を提供する。

オプション 3 と 4 が正解となります。顧客が提供するキー (SSE-C) を使用したサーバー側の暗号化を使用すると、Amazon S3 は PUT リクエストで 提供される暗号化キーを使用してオブジェクトサーバー側を暗号化できます。Amazon S3 がオブジェクトを復号するには、GET リクエストに同じキーを指定する必要があります。顧客にはまた、Amazon S3 にアップロードしてダウンロード 後に復号化する前に、データクライアント側を暗号化するオプションもあります。AWS SDK は、プロセスを合理化する S3 暗号化クライアントを提供します。

分野 4: コスト最適化アーキテクチャの設計

- 4.1 コスト効率が高いストレージソリューションの識別
- 4.2 コスト効率が高いコンピューティングおよびデータベースサービスの識別
- 4.3 コスト最適化ネットワークアーキテクチャの設計

分野 4: コスト最適化アーキテクチャの設計

■ 4.1 コスト効率が高いストレージソリューションの識別

規制要件により、企業はアクセスログを最低5年間維持する必要があります。一度保存された後のデータにアクセスすることはほとんどありませんが、必要に応じて 1 日前に通知することでアクセスできなければなりません。

これらの要件を満たす最もコスト効率の高いデータストレージソリューションは何ですか？

- 1) Amazon S3 Glacier ディープアーカイブストレージにデータを保存し、ライフサイクルルールを使用して5 年後にオブジェクトを削除する。
- 2) データを Amazon S3 標準ストレージに保存し、ライフサイクルルールを使用して 30 日後に Amazon S3 Glacier に移行する。
- 3) Amazon CloudWatch ログを使用してデータをログに保存し、保存期間を5年に設定する。
- 4) Amazon S3 標準頻度の低いアクセス (S3 Standard-IA) ストレージにデータを保存し、ライフサイクルルールを使用して 5 年後にオブジェクトを削除する。

分野 4: コスト最適化アーキテクチャの設計

■ 4.1 コスト効率が高いストレージソリューションの識別

規制要件により、企業はアクセスログを最低5年間維持する必要があります。一度保存された後のデータにアクセスすることはほとんどありませんが、必要に応じて 1 日前に通知することでアクセスできなければなりません。

これらの要件を満たす最もコスト効率の高いデータストレージソリューションは何ですか？

- 1) Amazon S3 Glacier ディープアーカイブストレージにデータを保存し、ライフサイクルルールを使用して 5 年 後にオブジェクトを削除する。

オプション 1 が正解となります。データは、Amazon S3 Glacier Deep Archive に直接保存することができます。これは、最も廉価な S3 ストレージクラスです。

分野 4: コスト最適化アーキテクチャの設計

■ 4.2 コスト効率が高いコンピューティングおよびデータベースサービスの識別

企業は、データ処理ワークロードを実行するためにリザーブドインスタンスを使用しています。夜間のジョブは通常、実行に 7 時間かかり、10 時間以内に完了する必要があります。同社は、毎月末に需要が一時的に増加するため、現在のリソースの容量ではジョブが制限時間以内に終わらないと予想しています。いったん開始された処理ジョブは、完了する前に中断できません。同社は、できる限りコスト効率の高い容量を提供できるソリューションを実装したいと考えています。

ソリューションアーキテクトは、これを達成するために何をすべきでしょうか？

- 1) 需要の高い期間中にオンデマンドインスタンスをデプロイする。
- 2) 追加インスタンス用に 2 つ目の Amazon EC2 予約を作成する。
- 3) 需要が高まる期間中にスポットインスタンスを展開する。
- 4) ワークロードの増加をサポートするために、Amazon EC2 予約のインスタンスのインスタンスサイズを増やす。

分野 4: コスト最適化アーキテクチャの設計

■ 4.2 コスト効率が高いコンピューティングおよびデータベースサービスの識別

企業は、データ処理ワークロードを実行するためにリザーブドインスタンスを使用しています。夜間のジョブは通常、実行に 7 時間かかり、10 時間以内に完了する必要があります。同社は、毎月末に需要が一時的に増加するため、現在のリソースの容量ではジョブが制限時間以内に終わらないと予想しています。いったん開始された処理ジョブは、完了する前に中断できません。同社は、できる限りコスト効率の高い容量を提供できるソリューションを実装したいと考えています。

ソリューションアーキテクトは、これを達成するために何をすべきでしょうか？

- 1) 需要の高い期間中にオンデマンドインスタンスをデプロイする。

オプション 1 が正解となります。スポットインスタンスは、最もコストが安いオプションですが、中断できないジョブや一定期間内に完了すべき ジョブには適していません。オンデマンドインスタンスでは、実行秒数に対して請求が行われます。

分野 4: コスト最適化アーキテクチャの設計

■ 4.3 コスト最適化ネットワークアーキテクチャの設計

あなたはソリューションアーキテクトとして、グローバルな画像配信サイトの運用会社に勤務しています。画像配信の仕組みを効率化するためにCDNの利用を検討しています。そこで、あなたはCloudFrontを利用したコンテンツ配信にむけたコストを算出して報告することになりました。

次のうちCloudFrontのコスト算出の要素を選択してください。（2つ選択してください。）

- 1) リクエスト数
- 2) データ転送アウト
- 3) リソースタイプ
- 4) 利用するエッジロケーション数

分野 4: コスト最適化アーキテクチャの設計

■ 4.3 コスト最適化ネットワークアーキテクチャの設計

あなたはソリューションアーキテクトとして、グローバルな画像配信サイトの運用会社に勤務しています。画像配信の仕組みを効率化するためにCDNの利用を検討しています。そこで、あなたはCloudFrontを利用したコンテンツ配信にむけたコストを算出して報告することになりました。次のうちCloudFrontのコスト算出の要素を選択してください。（2つ選択してください。）

- 1) リクエスト数
- 2) データ転送アウト

オプション1と2が正解となります。Amazon CloudFrontの料金は以下の要素で決定されます。

- トラフィックの分散：データ転送とリクエストの価格は地域によって異なり、価格はコンテンツが配信されるエッジの場所によって異なる
- リクエスト：リクエスト（HTTPまたはHTTPS）の数と種類、およびリクエストが行われた地域。
- データ転送アウト：Amazon CloudFrontエッジロケーションから転送されたデータの量

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/>

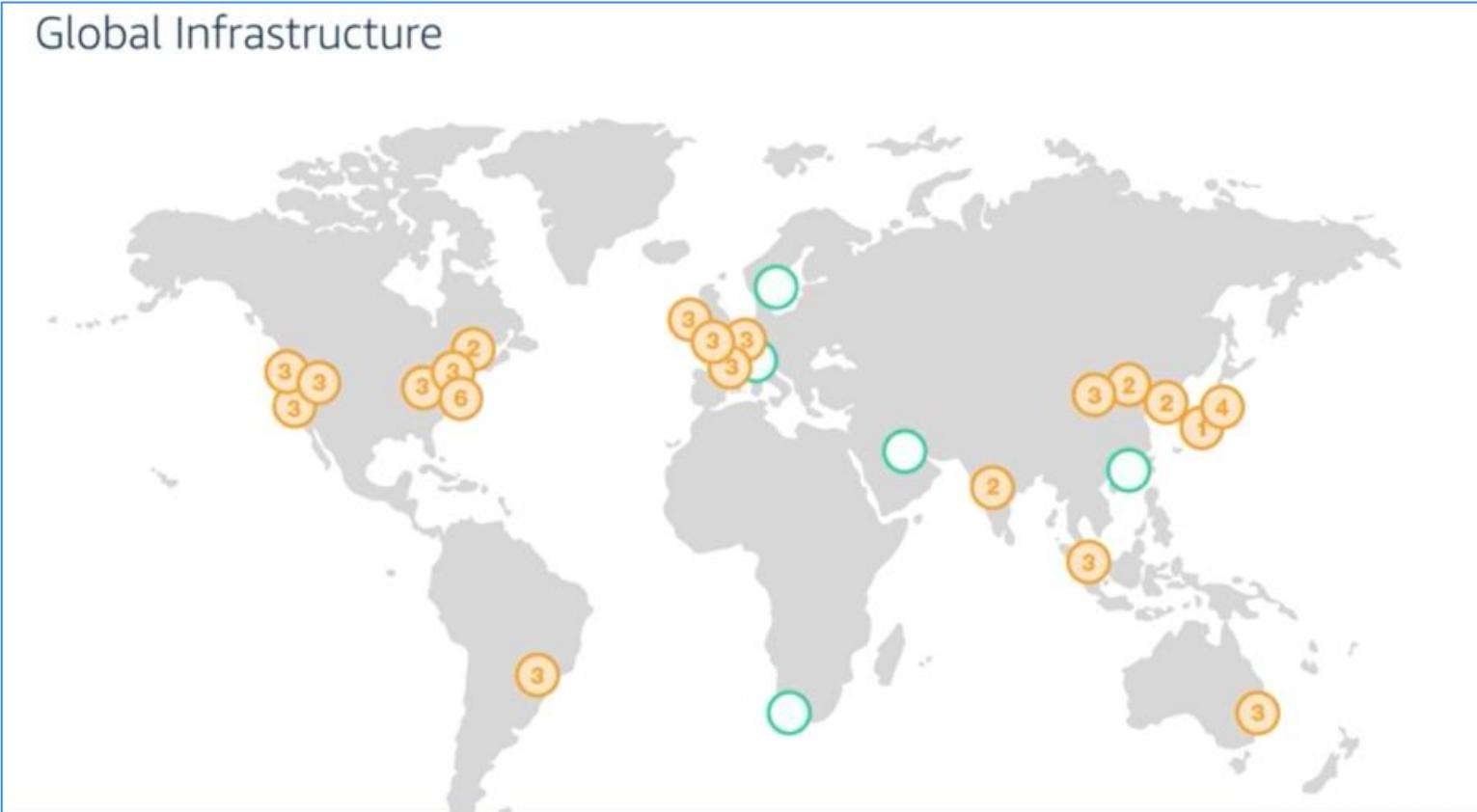
リージョン

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



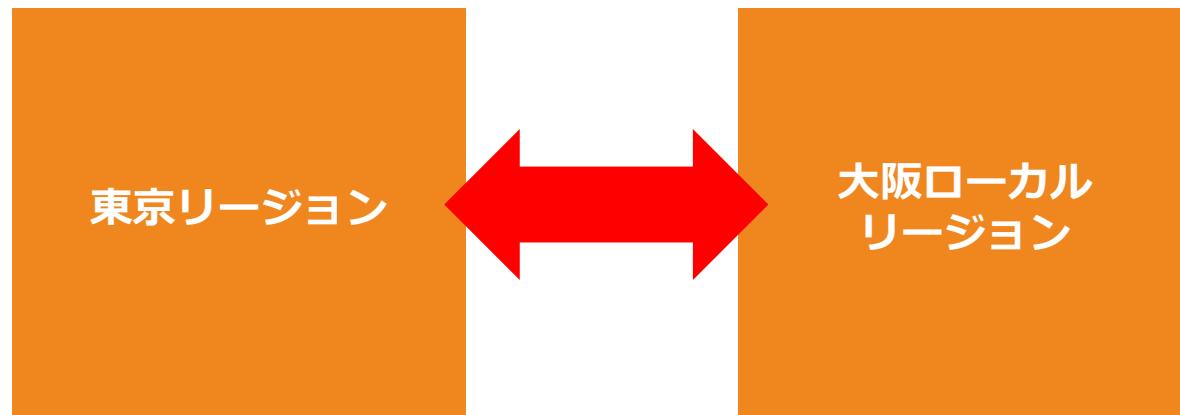
東京リージョン



大阪ローカル
リージョン

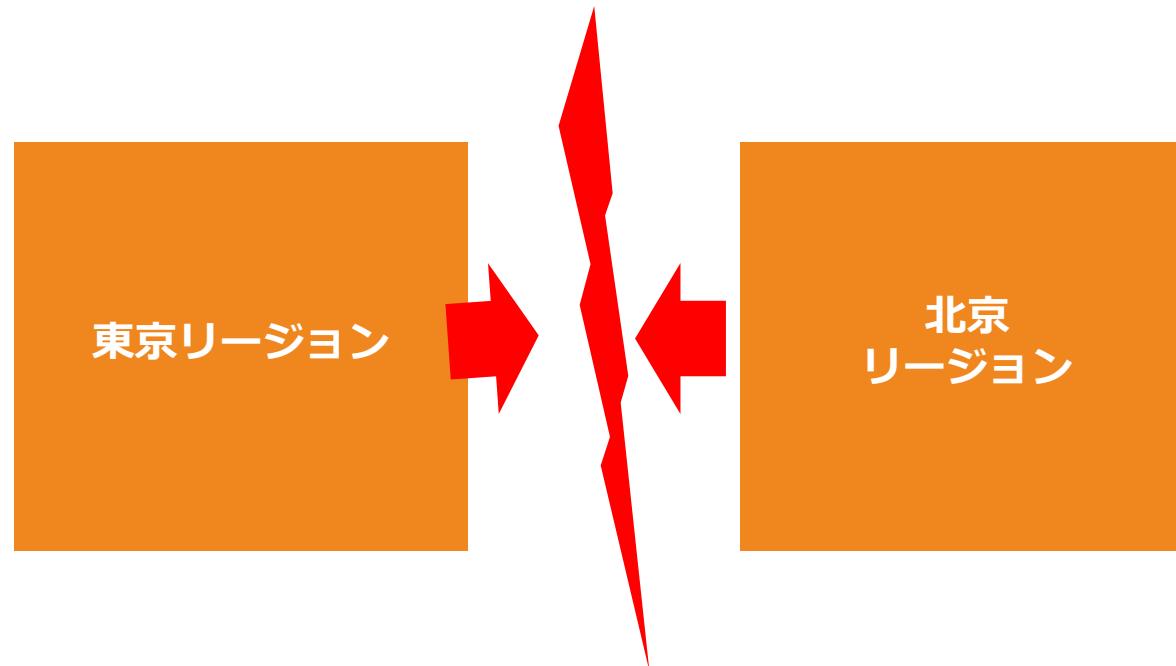
リージョン

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

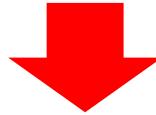
中国国内のリージョンは政治的な理由で他のAWSリージョンとは完全に断絶している



リージョン

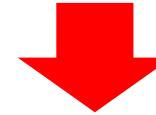
リージョンに応じてAWSサービスの利用可否と値段が異なる

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

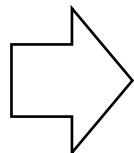
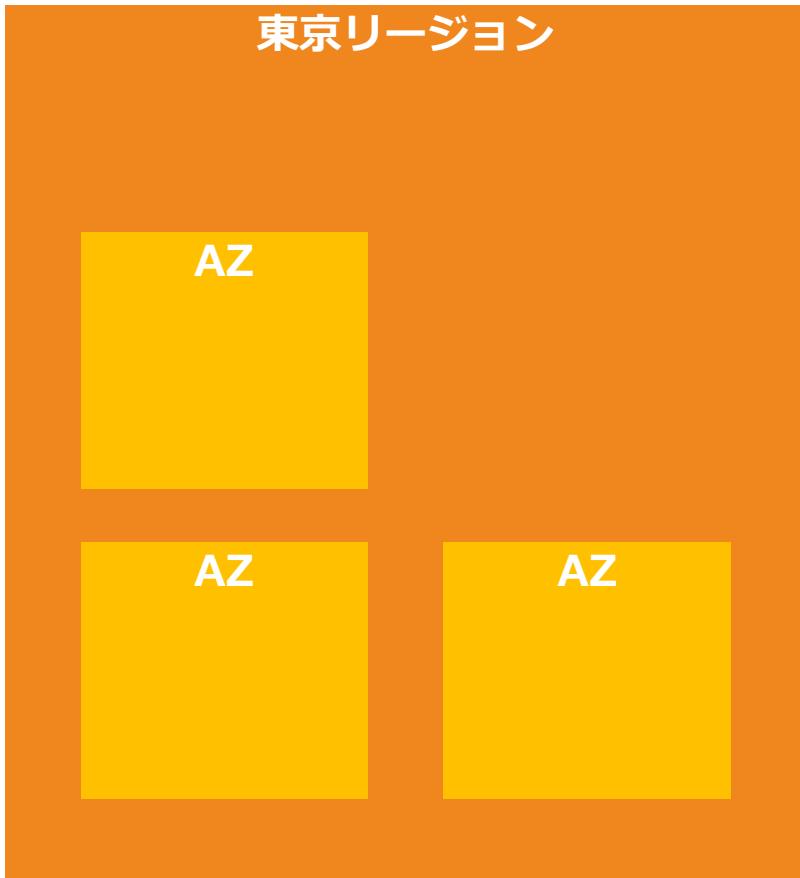
アベイラビリティゾーン

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

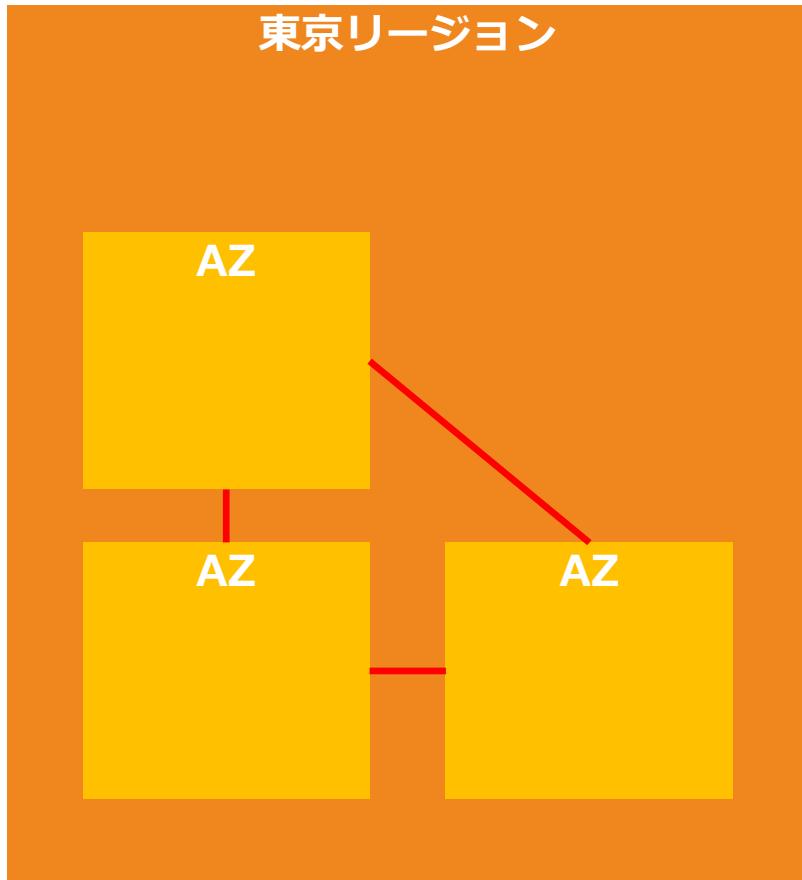
アベイラビリティゾーン 情報

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

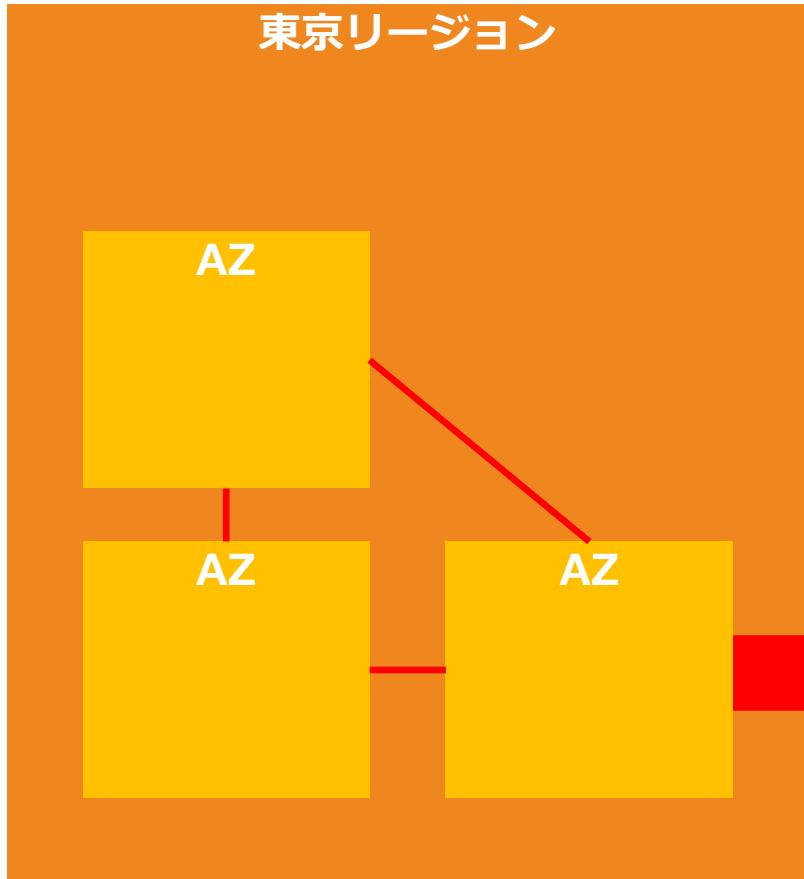
アベイラビリティゾーン (AZ)

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

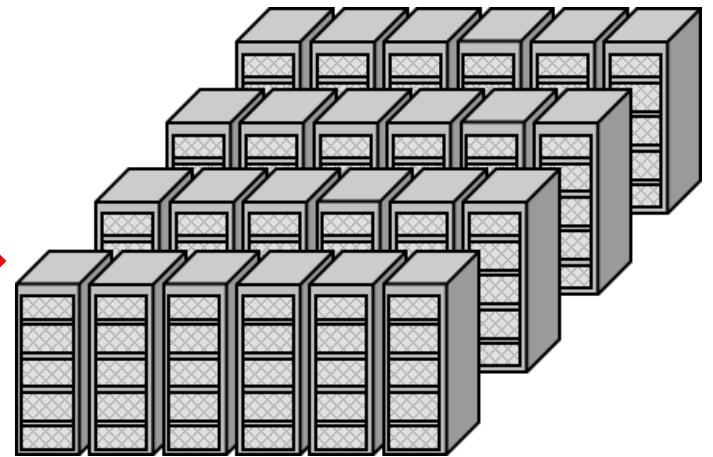


アベイラビリティゾーン (AZ)

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

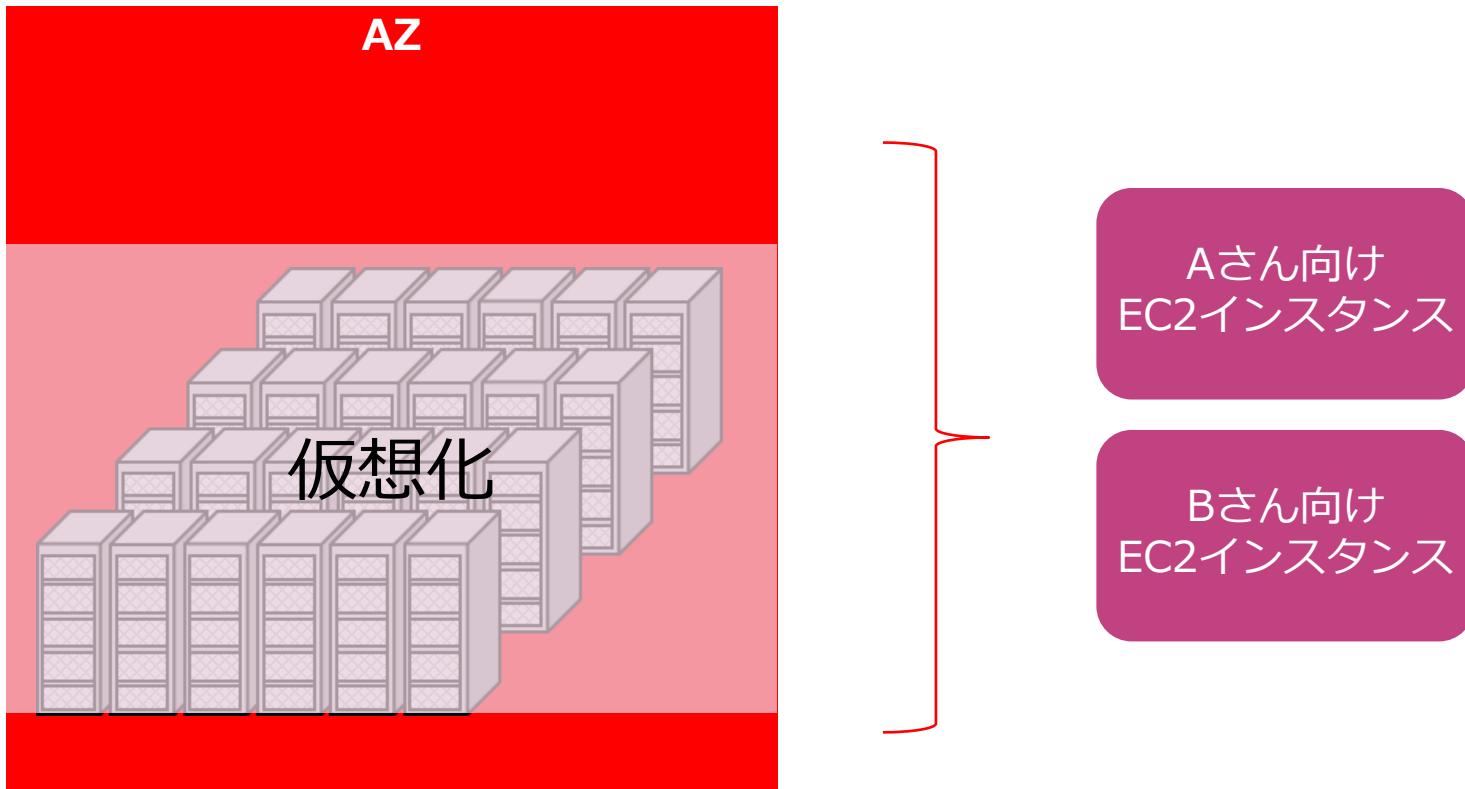


- ✓ AZは1つ以上のデータセンターで構成されている。
- ✓ データセンターにある多数のサーバーがAWSサービスを提供している



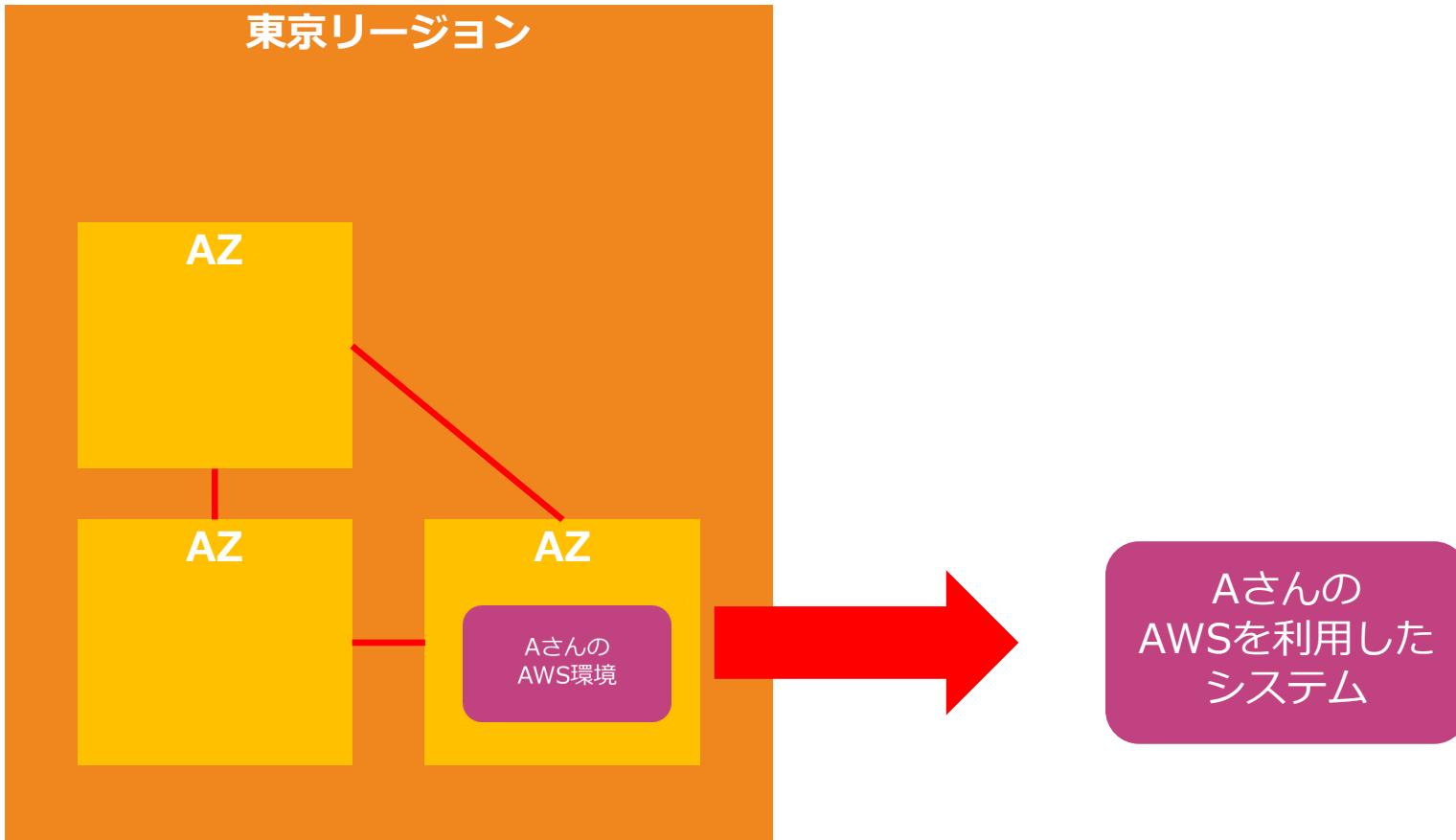
アベイラビリティゾーン (AZ)

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



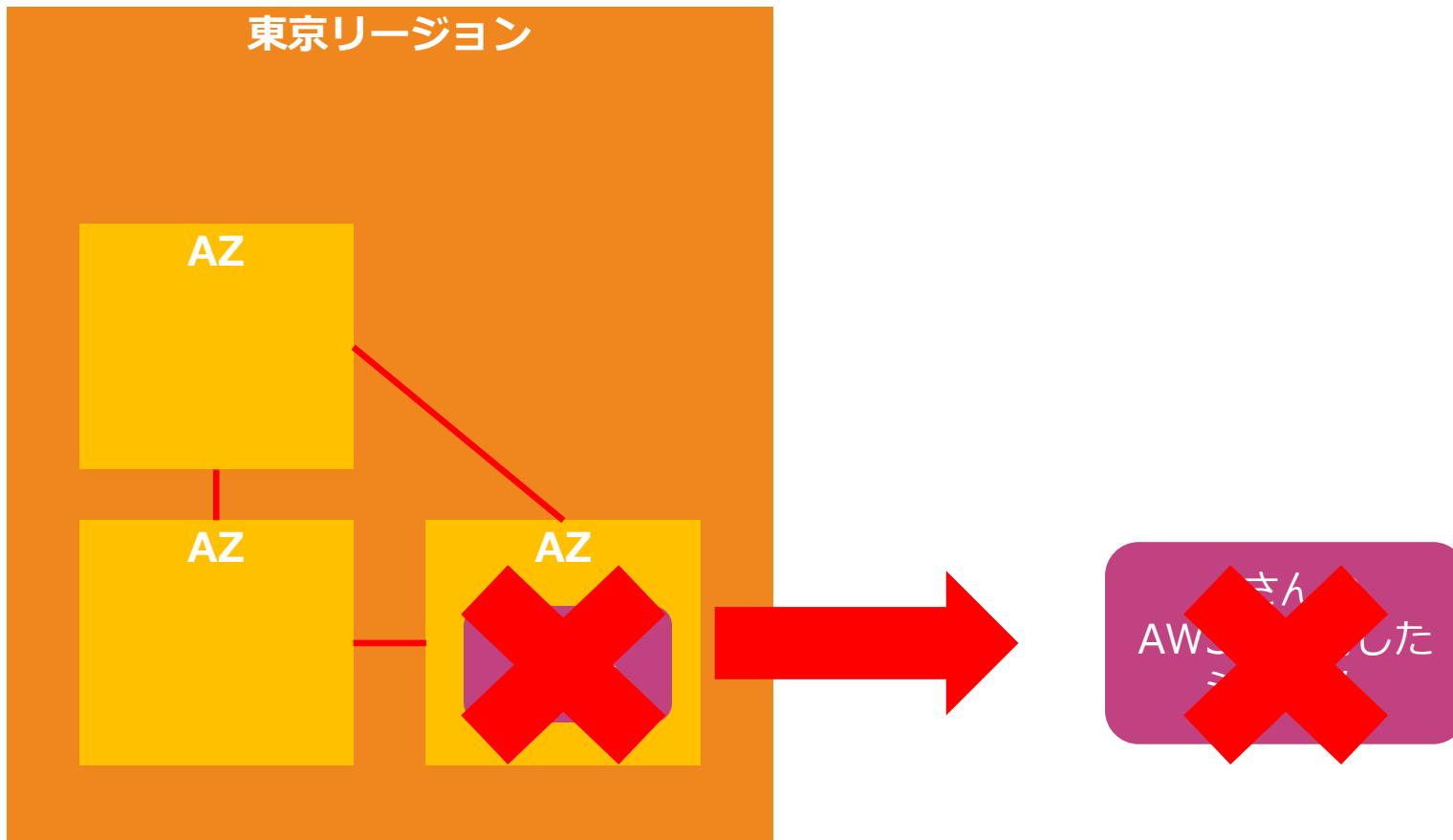
アベイラビリティゾーン (AZ)

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



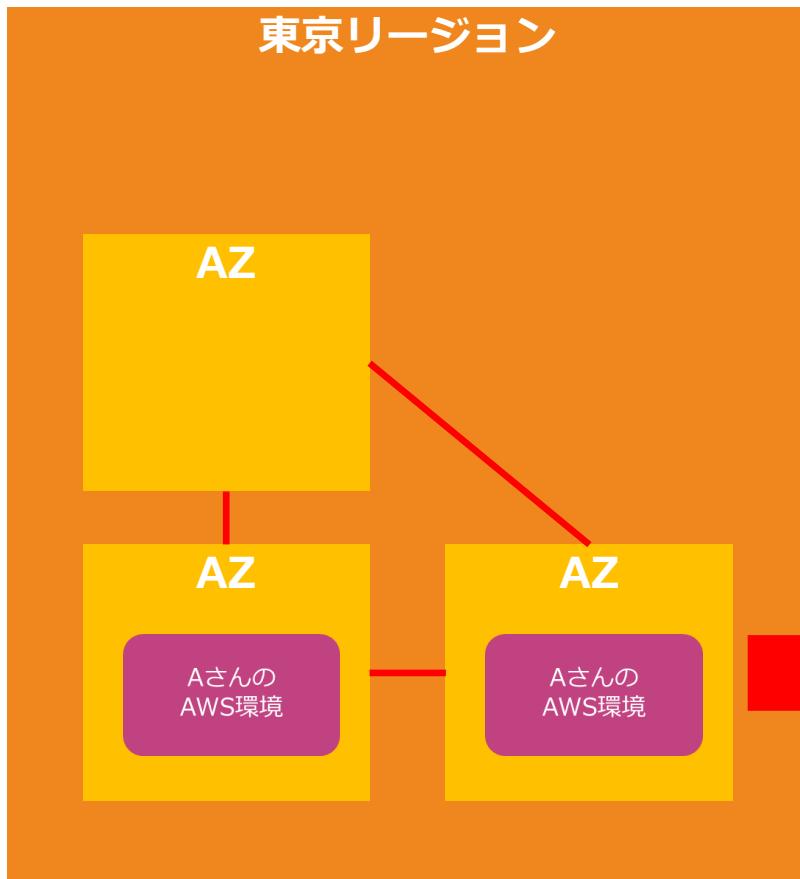
アベイラビリティゾーン (AZ)

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

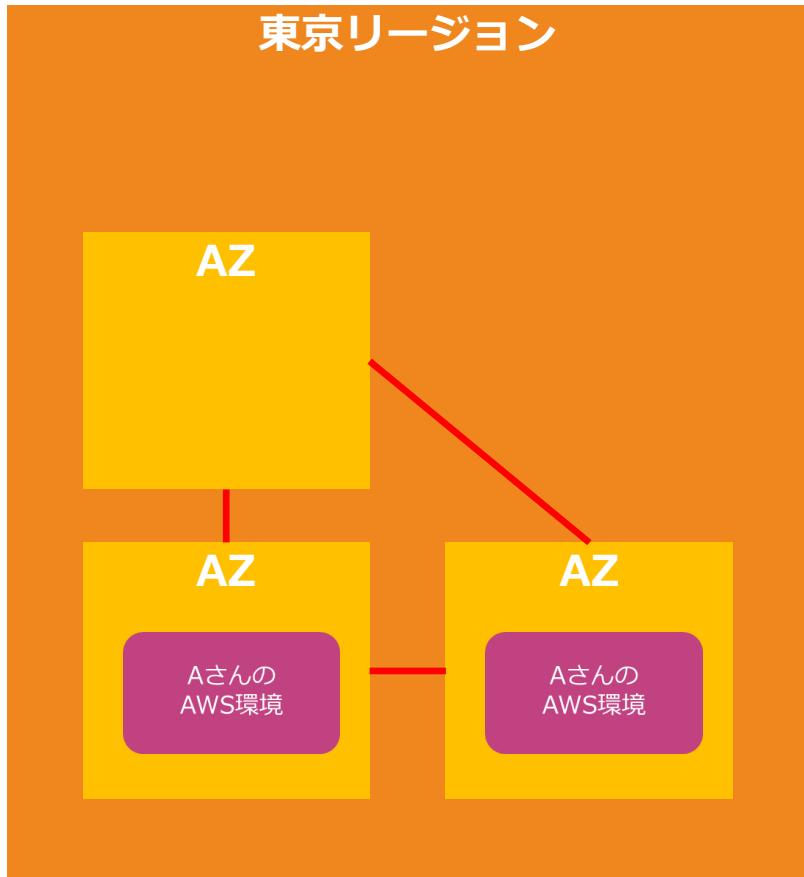


【推奨】
1つのリージョンに2つのAZから始める

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)

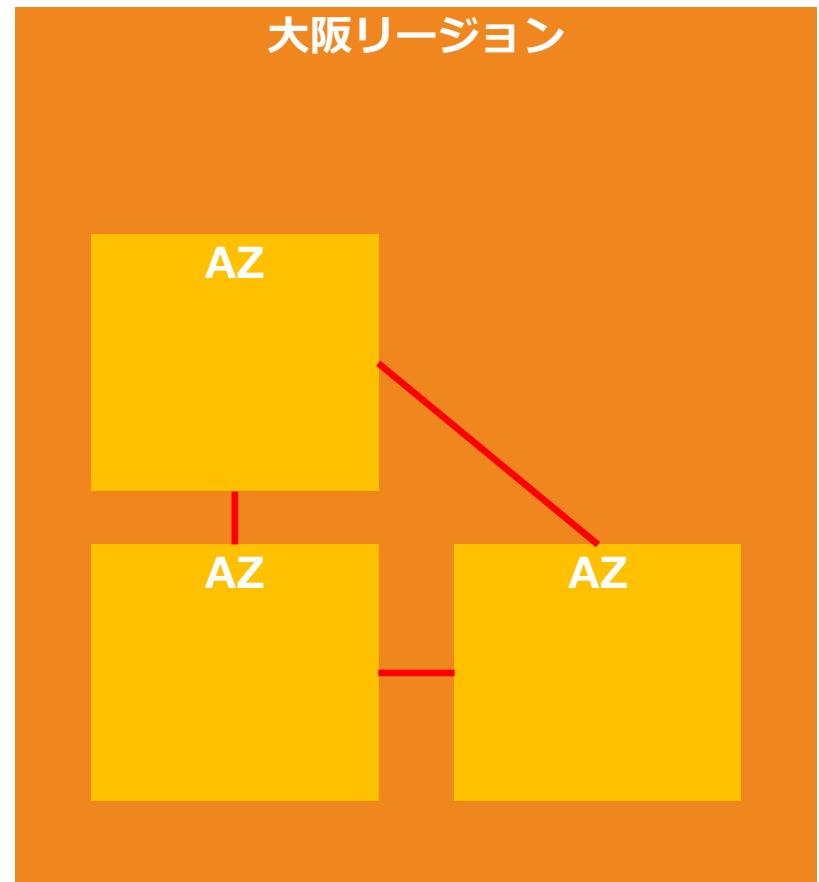
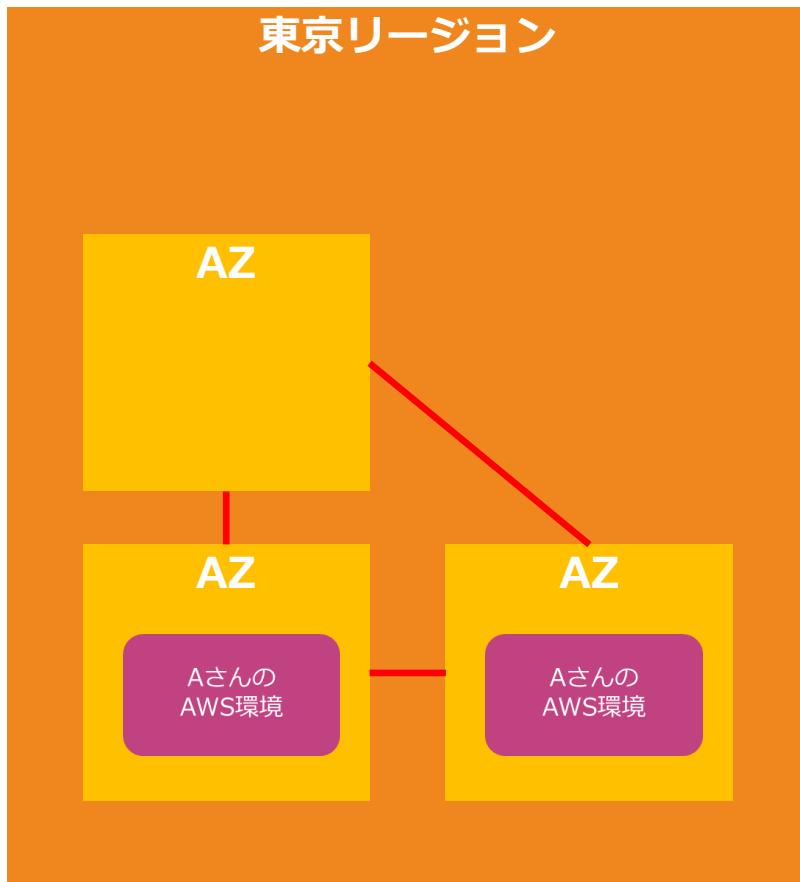
複数AZを跨ぐと物理的な耐久性などが向上するが、システム間の連携や共有が制限される



- ✓ 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

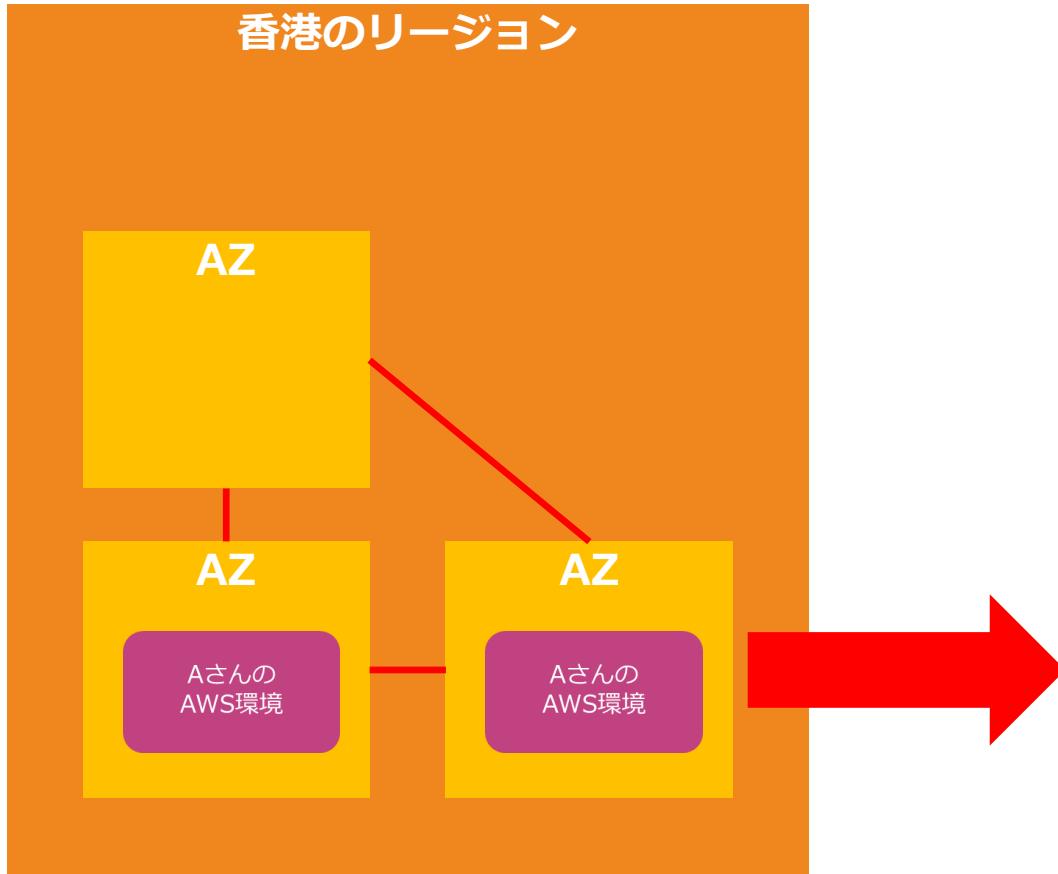
リージョンの選択

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

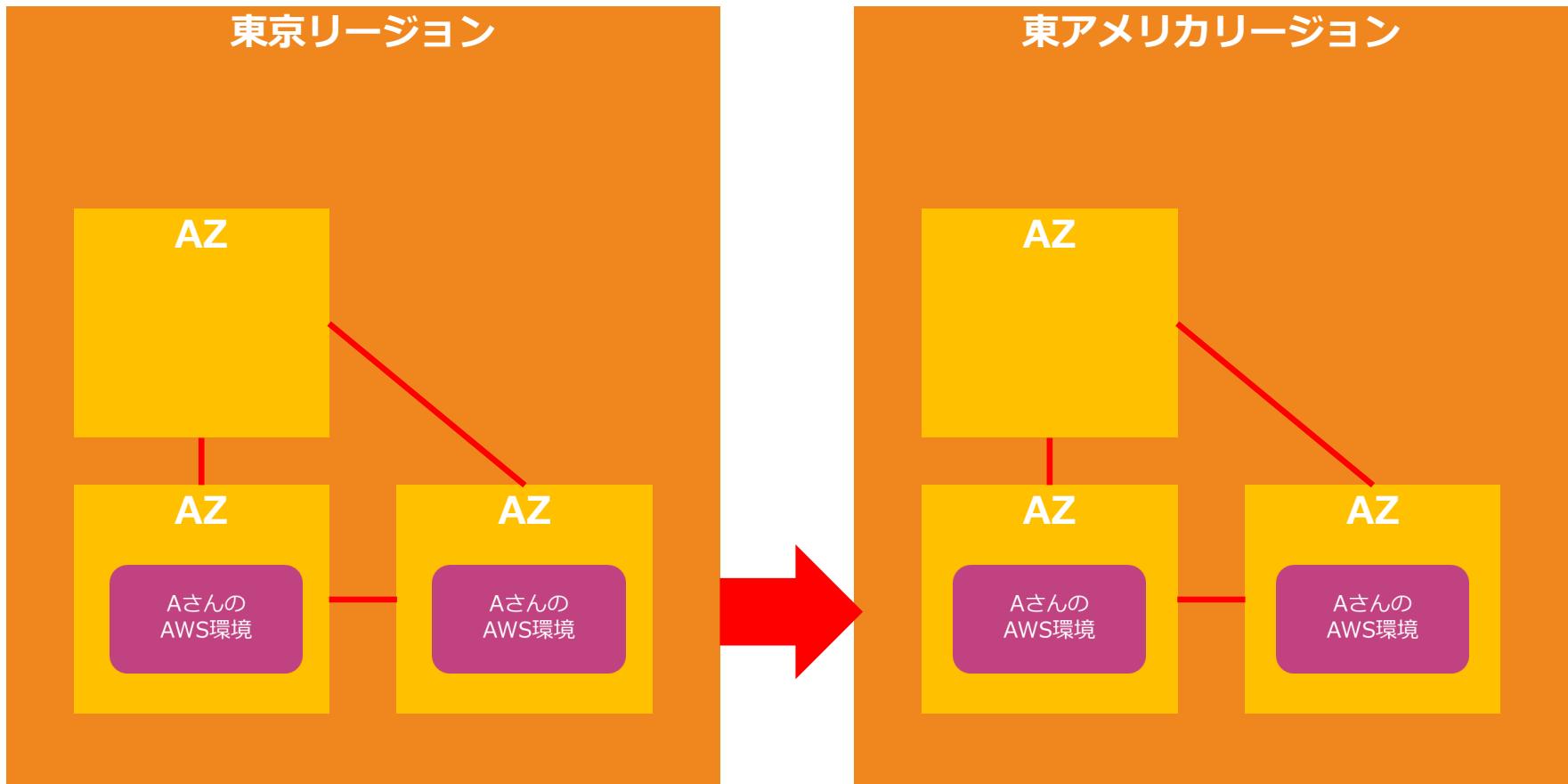
リージョンのある国の法律に影響される可能性も考慮する



- ✓ 中国政府の要請に従いAWS中國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



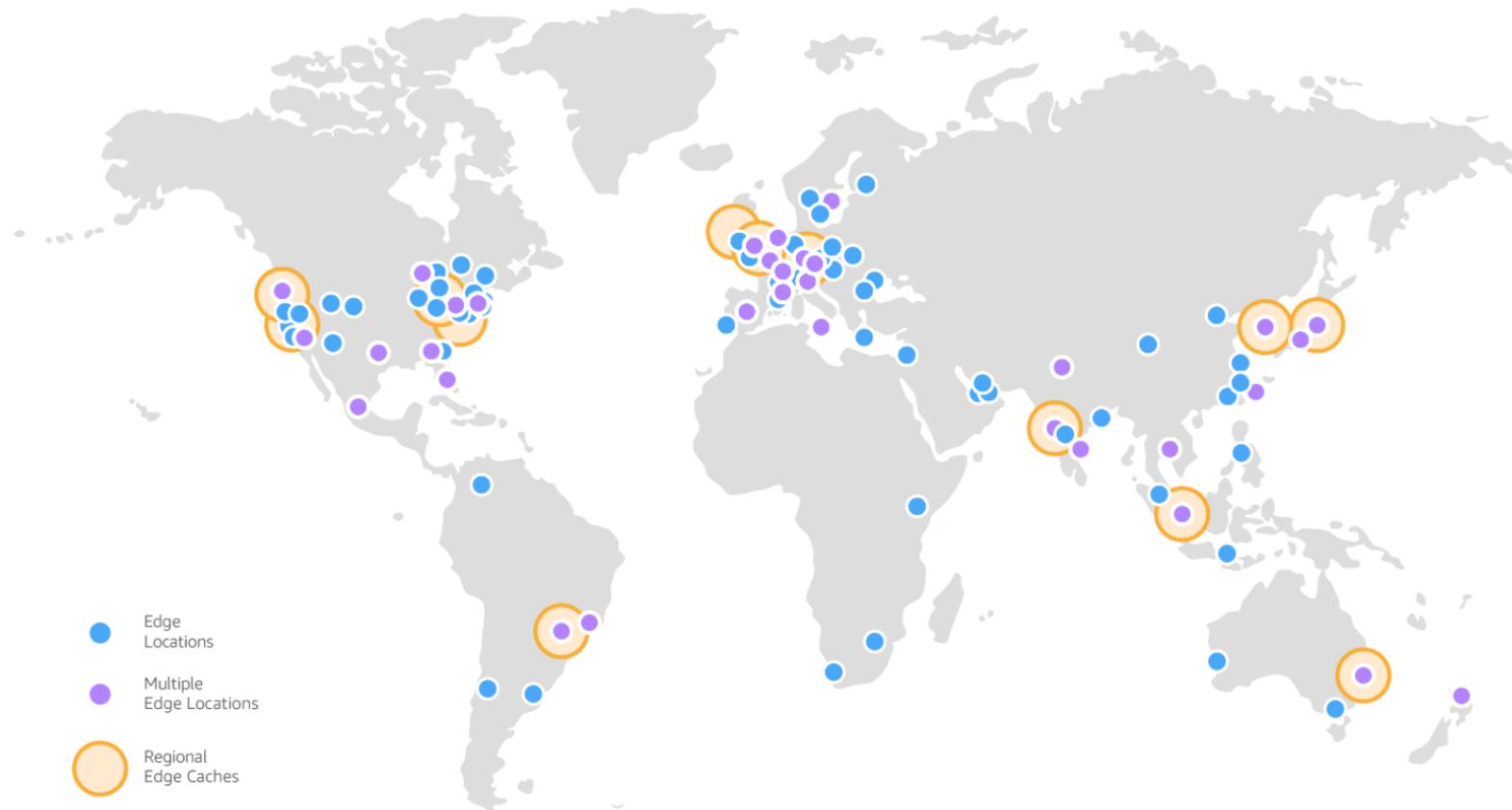
エッジロケーション

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

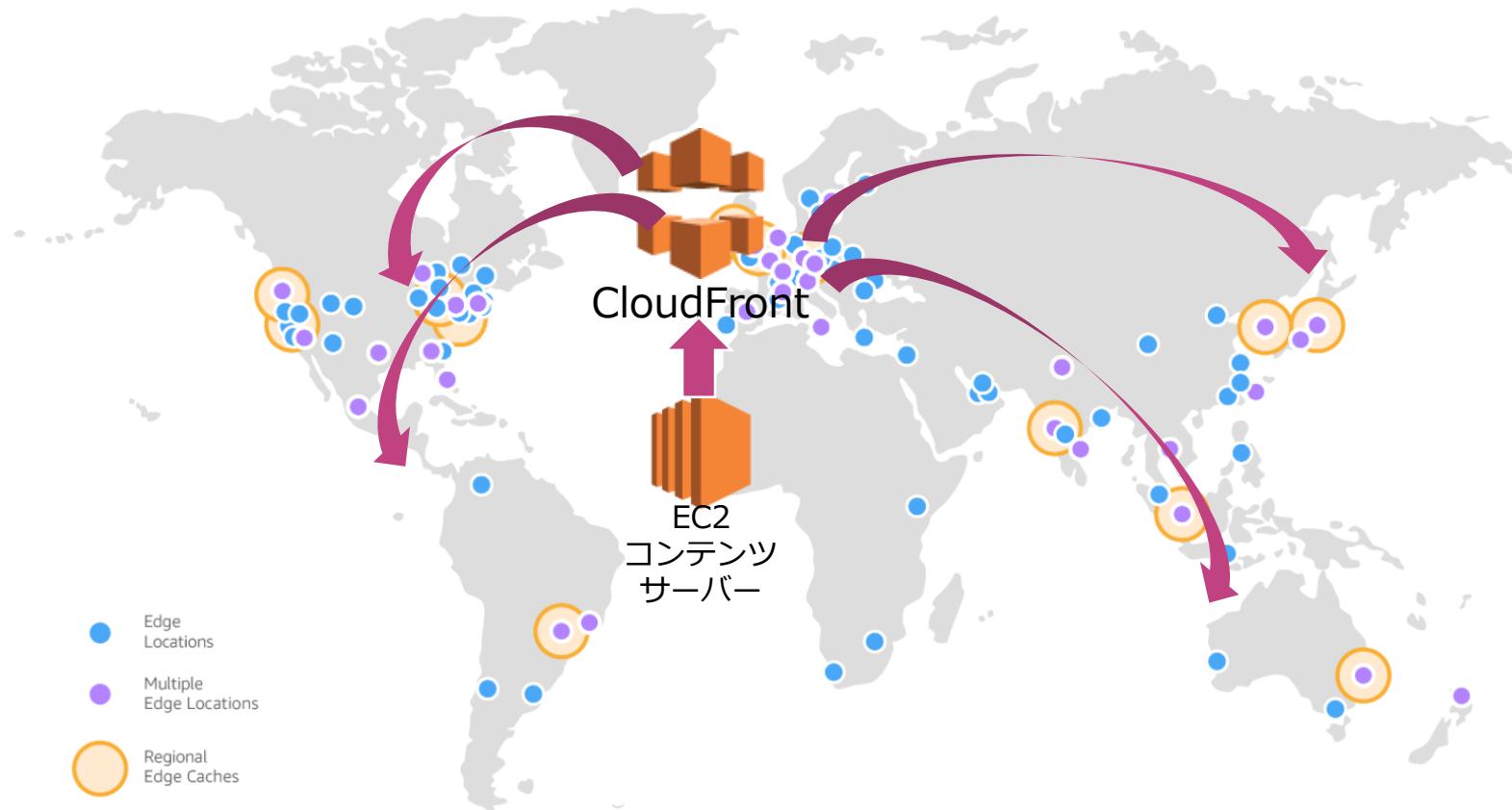
グローバルにコンテンツ配信に利用されるロケーションのこと



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

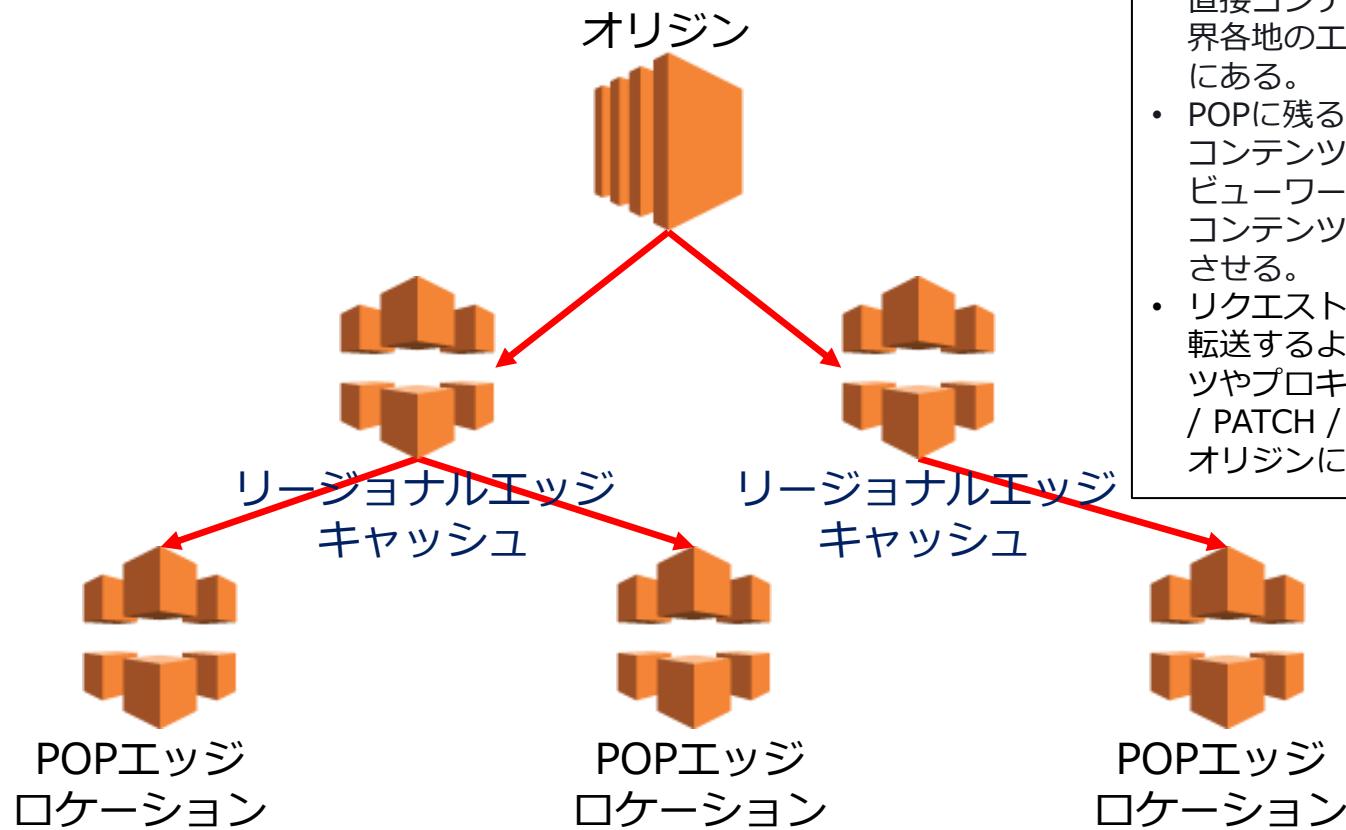
グローバルにコンテンツ配信に利用されるロケーションのこと



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

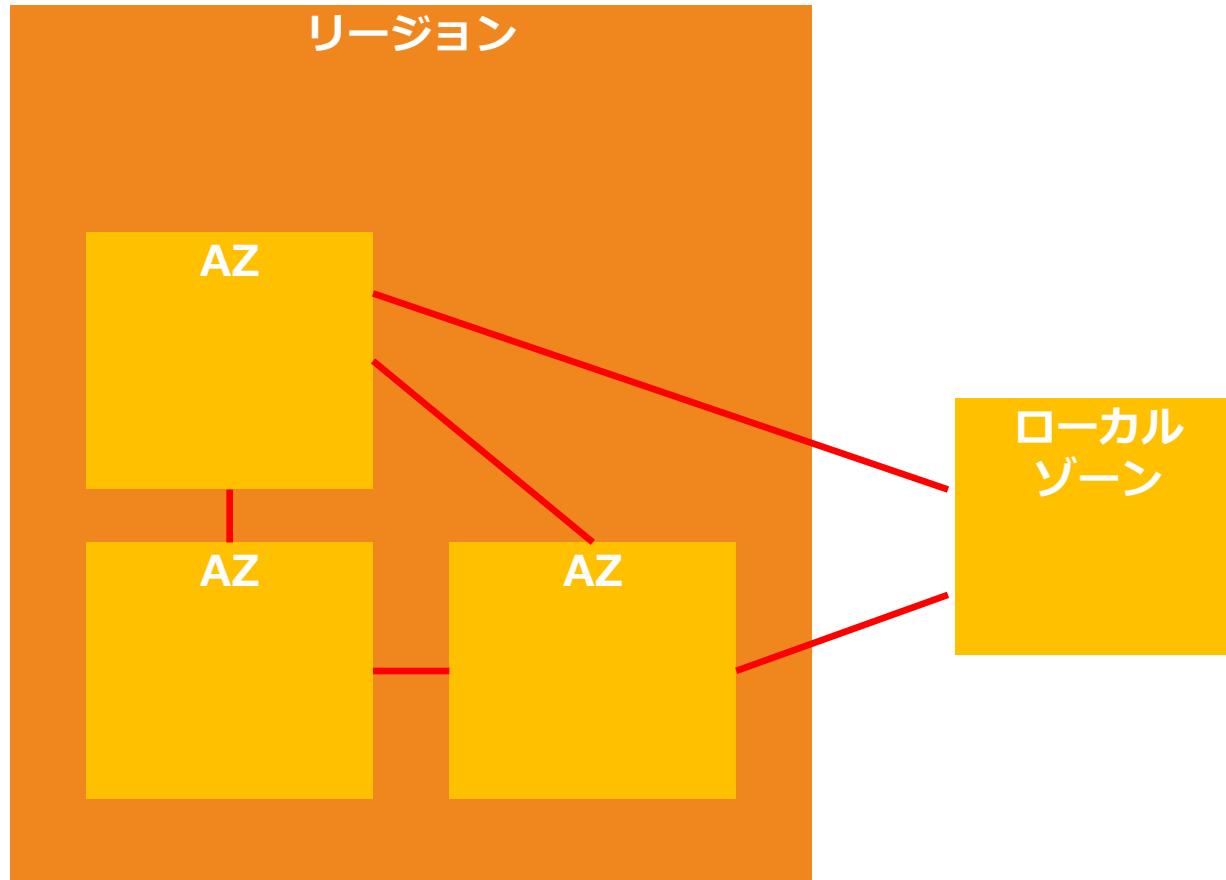
AWSローカルゾーン

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。



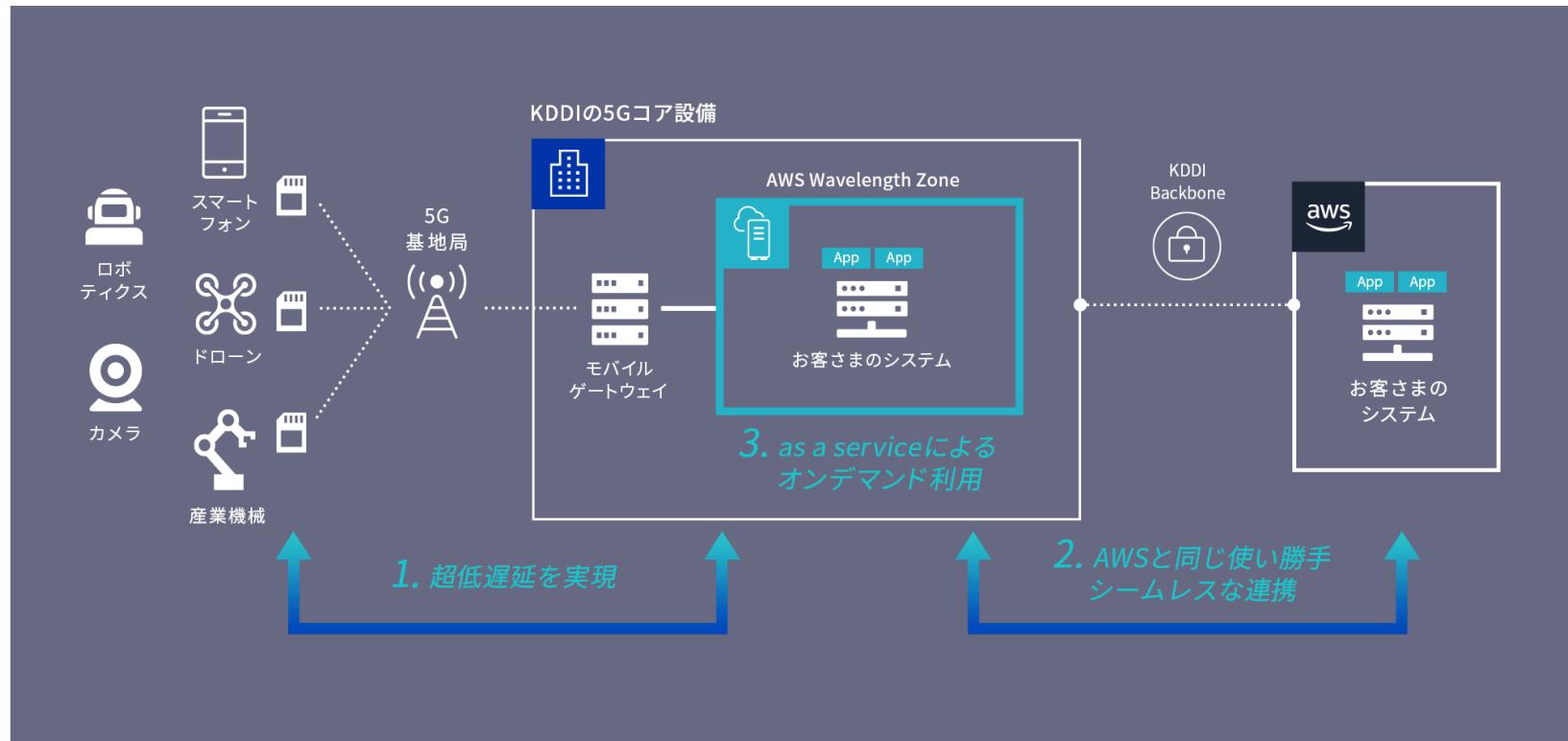
Wavelength Zone

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/

試験範囲となる
AWSサービス

試験出題範囲の分析

本番試験と模擬試験1625問から質問出題範囲を抽出・分析

本番試験3回分の試験パターン

195問

日本語のアソシエイト試験問題の最大ユーザー数の講座
(弊社所有)

390問

Udemyの最高評価のトップ3講座の1つ

260問

Udemyの最高評価のトップ3講座の1つ

390問

Udemyの最高評価のトップ3講座の1つ

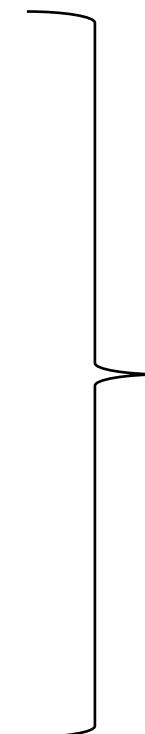
390問

合計：1625問

絶対に出題される範囲

出題サービス数（約100）に対して、上位の13サービスだけで62%の問題が出題されている。

カテゴリー	出題数	出題率
S3	182	11.17%
EC2	145	8.90%
VPC	94	5.77%
Auto Scaling	76	4.66%
RDS	74	4.54%
EBS	65	3.99%
SQS	60	3.68%
ELB	58	3.56%
CloudFront	56	3.44%
IAM	54	3.31%
DynamoDB	52	3.19%
Lambda	50	3.07%
Route53	42	2.58%



62%

絶対に出題される範囲

出題サービス数（約100）に対して、上位の13サービスだけで62%の問題が出題されている。

Amazon Simple Storage Service (S3)	99.999999999% (9 x 11) の耐久性がある高可用なオブジェクトストレージサービス。インターネットからアクセス可能で、大量データの保存やデータの長期保存に利用するストレージ
Amazon Elastic Compute Cloud (Amazon EC2)	プロセッサ、ストレージ、ネットワーキング、オペレーティングシステム、購入モデルを選択して、WindowsやLinuxなどの仮想サーバーを立ち上げるサービス
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 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 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専用のブロックストレージ
ELB	Elastic Load Balancing は、アプリケーションへのトラフィックを複数インスタンスに自動的に分散するロードバランサー
Auto Scaling	EC2インスタンスの負荷に応じて自動でスケーリングを実行するサービス

絶対に出題される範囲

出題サービス数（約100）に対して、上位の13サービスだけで62%の問題が出題されている。

Amazon SQS	完全マネージド型のポーリング型のメッセージキューイングサービス。ワーカーの並列分散処理に利用する。
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 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 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データベース
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代表的なサーバレスサービス
Amazon Route53	DNSサーバーの機能を提供するドメイン変換とルーティングを実施するサービス

合格に必要なサービス群

出題数が2桁のサービスを加えると90%の出題範囲をカバー

カテゴリー	出題数	出題率
Security Group	35	2.15%
Kinesis	31	1.90%
EFS	30	1.84%
API Gateway	30	1.84%
CloudWatch	30	1.84%
Aurora	29	1.78%
ElastiCache	28	1.72%
Connection	28	1.72%
CloudFormation	23	1.41%
ECS	22	1.35%
Redshift	21	1.29%
SNS	18	1.10%
AWS Storage Gateway	17	1.04%
Organizations	17	1.04%
Multi AZ	16	0.98%
Amazon FSX for Windows	13	0.80%
Instance Store	11	0.67%
KMS	11	0.67%
Snowball	10	0.61%
Glacier	10	0.61%
AWS DataSync	10	0.61%
DR対応	10	0.61%
CloudTrail	10	0.61%

28% ⇒ 90%

※CloudWatch、CloudTrailはCAA01では頻出でしたが、CAA02では単独のトピックスとしては出題分野から除外

合格に必要なサービス群

出題数が2桁のサービスを加えると90%の出題範囲をカバー

Security Group	インスタンスやELBの通信トラフィックを制御するファイアウォールとなるサービス
Kinesis	ストリーミングデータをリアルタイムで収集、処理、分析するための、データ処理サービス
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 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
Amazon CloudWatch (SAA-01用)	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
Amazon Aurora	MySQL および PostgreSQL と互換性のあるクラウド向け分散・高速化されたリレーショナルデータベース
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データストア

合格に必要なサービス群

出題数が2桁のサービスを加えると90%の出題範囲をカバー

サイト間接続方式 (Direct Connect / VPN)	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 VPNはサイト間VPNによりAWSとオンプレミス環境を接続
AWS CloudFormation	コードによりテンプレートを作成し、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
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
Amazon Redshift	高速かつシンプルに利用できる費用対効果の高いデータウェアハウス
Amazon SNS	pub/sub機能を有するプッシュ型のメッセージングサービス メッセージ通知やアラーム設定に利用する。
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
AWS Organizations	複数のAWS アカウント全体の一元管理と一括請求

合格に必要なサービス群

出題数が2桁のサービスを加えると90%の出題範囲をカバー

Multi AZ	Availability Zoneを2つ以上利用した可用性の高いインフラ構成をマルチAZと呼ぶ。AWSの基本的なアーキテクチャの構成方法
Amazon FSx for Windows	業界標準のサーバーメッセージブロック (SMB) プロトコルを介してアクセスできる、信頼性が高くスケーラブルな完全マネージド型のファイルストレージ
Instance Store	EC2インスタンスと物理的に接続されているブロックストレージで、一時的なデータの保存を利用する。
AWS Key Management Service	暗号化キーを簡単に作成して管理し、幅広い AWS サービスやアプリケーションの暗号化を実現するサービス
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ために利用する非常に安全なポータブルなストレージデバイスやトレーラー
Amazon Glacier	安全性と耐久性に優れ、きわめて低コストの Amazon S3 クラウドストレージクラス。データのアーカイブや長期バックアップに使用する
AWS DataSync	大量のオンラインデータを、オンプレミスマシンと S3 または Amazon EFS、Amazon FSx for Windows File Server との間で、簡単かつ迅速に移動させるサービス

合格に必要なサービス群

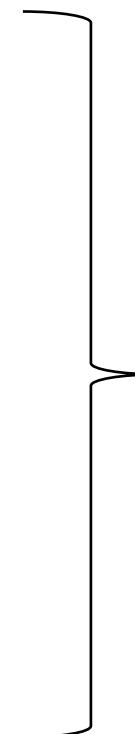
出題数が2桁のサービスを加えると90%の出題範囲をカバー

DR対応	別のリージョンを利用したバックアップの取得方法などのAWSを利用したDR構成方法
CloudTrail (SAA-01用)	ユーザー活動と API 使用状況の追跡するログ取得・監視するサービス

高得点を目指すための範囲

出題数が4問以上のサービスを加えると95%の範囲をカバーしており、ここまで抑えれば問題ない。

カテゴリー	出題数	出題率
AWS WAF	9	0.55%
AWS Global Accelerator	8	0.49%
AWS Elastic BeanStalk	8	0.49%
EMR	8	0.49%
ACM	8	0.49%
OpsWorks	7	0.43%
DMS	7	0.43%
Cognito	7	0.43%
Athena	7	0.43%
Amazon MQ	6	0.37%
AWS Directory Service	6	0.37%
AWS SSO	6	0.37%
Amazon FSX for Lustre	5	0.31%
AWS Transit Gateway	5	0.31%
AWS Step Functions	5	0.31%
SWF	5	0.31%
CloudHSM	4	0.25%
STS	4	0.25%



7% ⇒ 97%

高得点を目指すための範囲

出題数が4問以上のサービスを加えると97%の範囲をカバーしており、ここまで抑えれば問題ない。

AWS WAF	SQL インジェクションやクロスサイトスクリプティングなど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
AWS Global Accelerator	2 つのグローバルな静的 IP が提供され、トラフィックを最も近い、正常なエンドポイントに自動的に再ルーティングして、インターネットユーザーのパフォーマンスを最大 60% 向上させる
AWS Elastic BeanStalk	AWS に 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デプロイし、バージョン管理を自動化するサービス
Amazon EMR	Apache Spark、Apache Hive、Apache HBase、Apache Flink、Apache Hudi、Presto などのツールを使用して標準的な Apache Spark の 3 倍以上の速さでペタバイト規模の分析を実行
AWS Certificate Manager (ACM)	Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書のプロビジョニング、管理、デプロイを実施するサービス
AWS OpsWorks	Chef や Puppet のコードを使用してサーバーの構成を自動化することができる構成管理サービス
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な、データベース移行ツール

高得点を目指すための範囲

出題数が4問以上のサービスを加えると97%の範囲をカバーしており、ここまで抑えれば問題ない。

Amazon Cognito	ウェブアプリケーションおよびモバイルアプリに素早く簡単にユーザーのサインアップ/サインインおよびアクセスコントロールの機能を追加できるサービス
Amazon Athena	インタラクティブなクエリサービスで、Amazon S3 内のデータを標準 SQL を使用して簡単に分析する際に利用する
Amazon MQ	業界標準 API やプロトコルを利用して、クラウド内のメッセージブローカーを利用する、Apache ActiveMQ 向けのマネージド型メッセージブローカーサービス
AWS Directory Service	オンプレミス環境のADとの統合や、新規にAWS内にADを利用して、AWS 内のマネージド型 Active Directory (AD) を使用することを可能にする
AWS Single Sign-On (SSO)	複数の AWS アカウントとビジネスアプリケーションへのアクセスの一元的な管理を容易にし、シングルサインオンアクセスをユーザーに提供できるようにする AWS サービス
Amazon FSx for Lustre	機械学習、高性能コンピューティング (HPC)、ビデオレンダリング、金融シミュレーションといった多くのワークフローに最適な高性能共有ストレージ
AWS Transit Gateway	複数のVPCやオンプレミスネットワークを相互接続する際に中央ハブを介して ハブアンドスポークスを構成するネットワークが簡素化され、複雑なピア接続関係を管理する

高得点を目指すための範囲

出題数が4問以上のサービスを加えると97%の範囲をカバーしており、ここまで抑えれば問題ない。

AWS Step Functions	AWS Lambda 関数および AWS の複数のサービスを、ビジネスに不可欠なアプリケーション内に簡単に配列することができるサーバーレスのワークフロー作成・管理サービス
Amazon Simple Workflow (SWF)	デベロッパーが並行したステップまたは連続したステップがあるバックグラウンドジョブを構築、実行、スケールするワークフローの作成・管理サービス
AWS CloudHSM	PKCS#11、JCE、CNGライブラリなど業界標準に準拠した法令遵守のための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ハードウェアベースキーストレージ
AWS Security Token Service (AWS STS)	IAMユーザーなどの認証されたユーザーに対して一時的な制限付き特権の認証情報をリクエストできるようにするWebサービス

学習の進め方

本講座のコンセプト

実際に出題される試験範囲に絞って学習することが
合格への近道！！

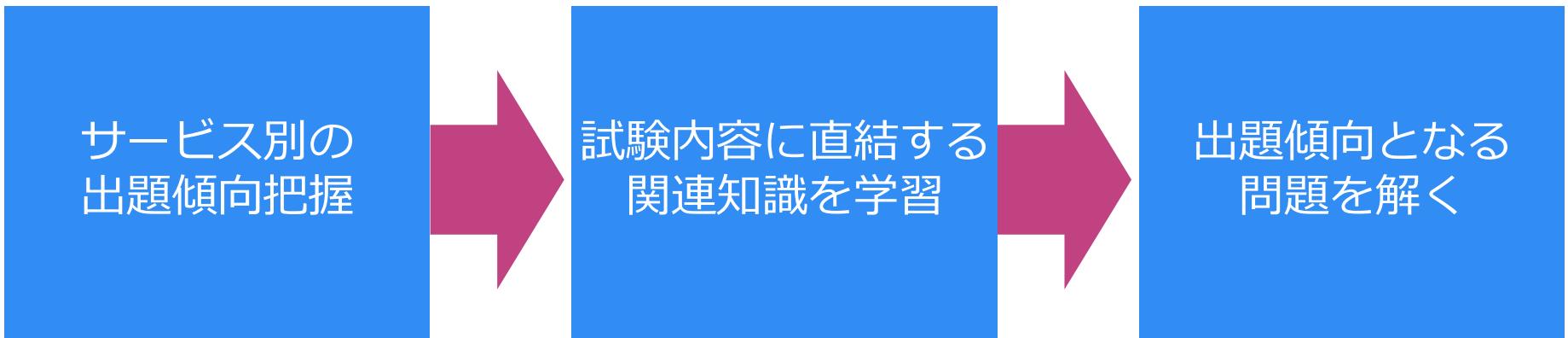
実際に出題される
試験問題を確認



出題される問題
の範囲のみを学習

本講座のコンセプト

サービス別の出題傾向に基づいて知識を身に着けて、その知識を模擬試験で確認して仕上げる！



S3の出題範囲

1625問から抽出したS3に関する質問出題範囲は以下の通り

S3ストレージの特徴	<ul style="list-style-type: none">✓ シナリオのストレージ要件を満たすストレージを選択する質問✓ S3ストレージの特徴を回答させる質問
S3のデータ容量制限	<ul style="list-style-type: none">✓ S3のデータ容量に関するシンプルな質問
ストレージクラスの選択	<ul style="list-style-type: none">✓ シナリオのストレージ要件を満たすS3のストレージクラスを選択する。✓ ライフサイクル管理と一緒に出題されるパターンも多い。
S3の利用コスト	<ul style="list-style-type: none">✓ S3におけるコストが発生する要素が質問として出題される。✓ リクエストに応じた課金設定が可能な機能が問われることも。
ライフサイクル管理	<ul style="list-style-type: none">✓ ライフサイクル管理によってデータ保存期間に応じて、ストレージクラスを移動させたり、削除させる適切な設定パターンが出題される。出来る組合せ／出来ない組合せがある。

ストレージクラスの選択

あなたはソリューションアーキテクトとして、社内アプリケーションにおいて生成されるレポートを保存・共有する仕組みを構築しているところです。このレポートはAWS Step Functionsによって生成プロセスを自動化して実行する予定ですが、レポートに利用されるデータが数テラバイト発生するため、これをS3に保存することが必要です。

ソリューションアーキテクトとして、最もコスト効率が良いストレージタイプを選択してください。

- 1) S3 Standard-IA
- 2) S3 Standard
- 3) S3 Intelligent Tiering
- 4) S3 Glacier

ストレージクラスの選択

あなたはソリューションアーキテクトとして、社内アプリケーションにおいて生成されるレポートを保存・共有する仕組みを構築しているところです。このレポートはAWS Step Functionsによって生成プロセスを自動化して実行する予定ですが、レポートに利用されるデータが数テラバイト発生するため、これをS3に保存することが必要です。

ソリューションアーキテクトとして、最もコスト効率が良いストレージタイプを選択してください。

- 1) S3 Standard-IA
- 2) S3 Standard
- 3) S3 Intelligent Tiering
- 4) S3 Glacier

【問題の使い方】

- 問題自体は例示として提示していますが、時間を短縮するため、問題を読み上げたり説明したりする時間は省略させていただきます。
- その代わりに、レクチャーの最後の模擬試験の問題として収録しておりますので、そちらでご回答と解説をしてもらい、総復習に利用いたします。

ストレージクラスの選択

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	<ul style="list-style-type: none">✓ 複数個所にデータを複製するため耐久性が非常に高い。✓ 頻繁に利用するデータを大量に保存するのに向いている。	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.99%
STANDARD-IA	<ul style="list-style-type: none">✓ IAはInfrequency Accessの略であり、低頻度アクセスデータ用のストレージ。 One Zone-IAより重要なマスターデータ向け。データ取得は早い✓ Standard に比べて安価だが、One Zone-IAよりは高い。	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.9%
One Zone-IA	<ul style="list-style-type: none">✓ 低頻度アクセス用のストレージだが、マルチAZ分散されていないため可用性が低く、重要ではないデータ向け。その分Standard IAよりも更に安い	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.5%
RRS	<ul style="list-style-type: none">✓ 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に利用する。✓ 現在は非推奨ストレージであり、利用されない。今ではStandardよりも値段が高い	<ul style="list-style-type: none">■ 耐久性 99.99%■ 可用性 99.99%

模擬試験の実施

★ 質問49:

ある企業はAWSにホストされた業務アプリケーションを利用して、毎日の業務にかかる記録管理を行っています。業界規定に基づいて、5年間は記録データを保管し続ける必要があります。これらの保存記録の大部分はアクセスされることは少ないですが、監査要求に対して、24時間以内にデータを提供する必要があります。

次の内で、コスト最適なストレージとして、どのストレージを選択するべきでしょうか。

Amazon Glacier (標準)

Amazon S3 Glacier Deep Archive

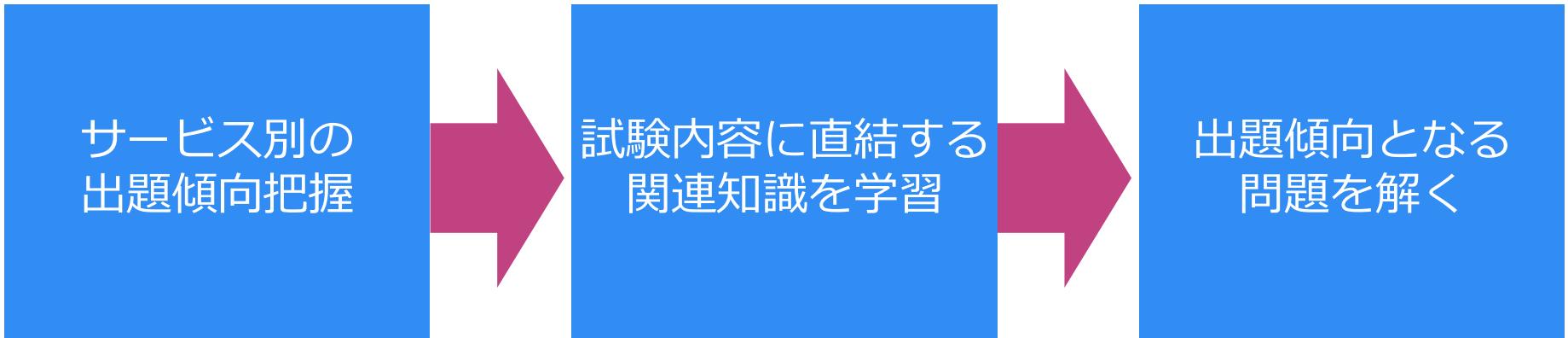
S3 Standard

S3 One-Zone IA

S3 Standard IA

本講座のコンセプト

サービス別の出題傾向に基づいて知識を身に着けて、その知識を模擬試験で確認して仕上げる！



セクションの内容

レクチャー	レクチャーで学ぶ内容
IAMの出題範囲	AWSでユーザー管理を実施する主要サービスであるIAMにおける出題問題を確認して、その範囲の知識を詳細に学習します。
S3の出題範囲	AWSでストレージを構築する主要サービスであるS3における出題問題を確認して、その範囲の知識を詳細に学習します。
EC2の出題範囲	AWSで仮想サーバーを構築する主要サービスであるEC2における出題問題を確認して、その範囲の知識を詳細に学習します。
VPCの出題範囲	AWS内のネットワーク領域を切り出す主要サービスであるVPCにおける出題問題を確認して、その範囲の知識を詳細に学習します。

IAMの出題範囲

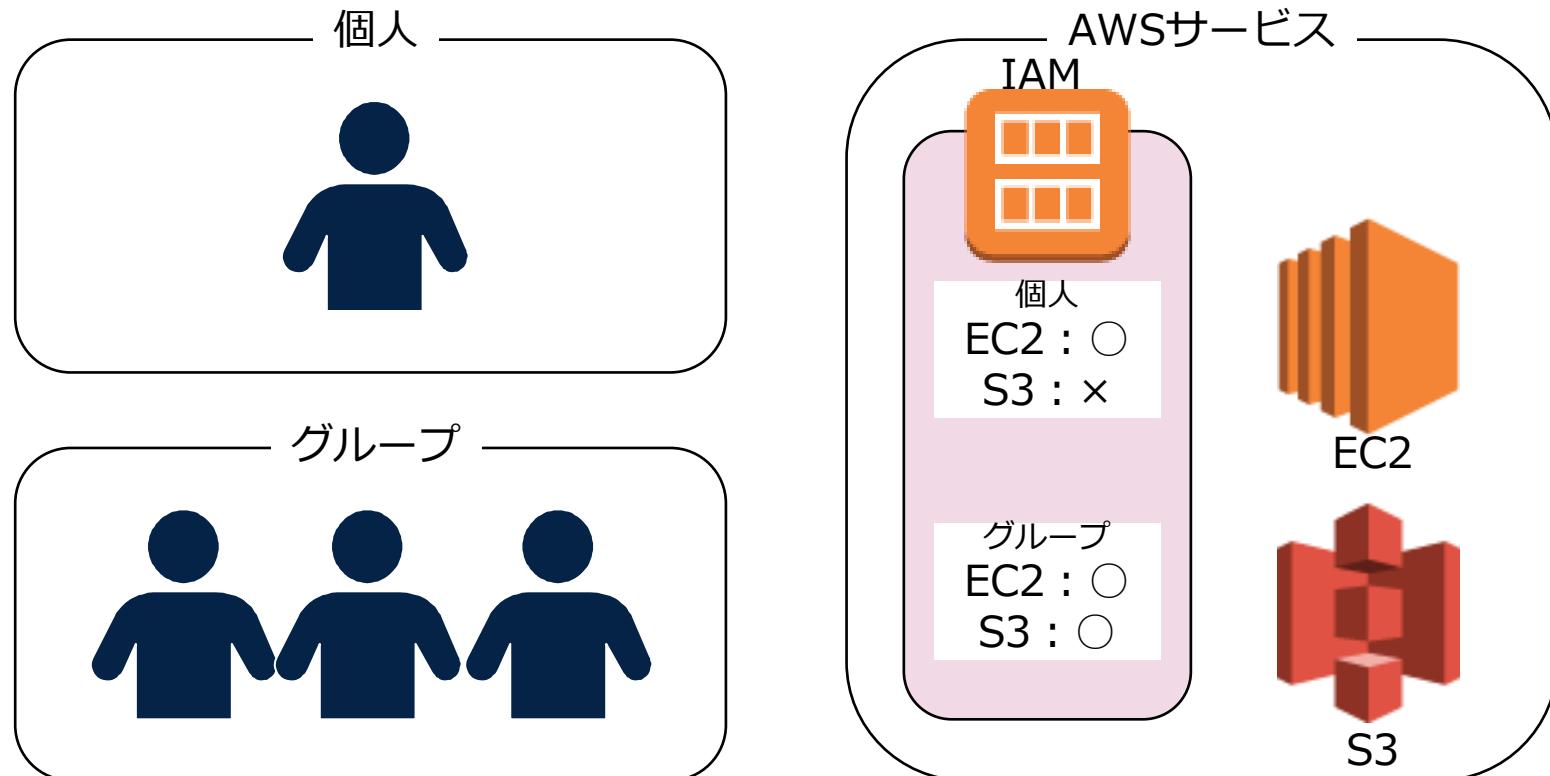
IAMとは

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
- 個人またはグループに設定

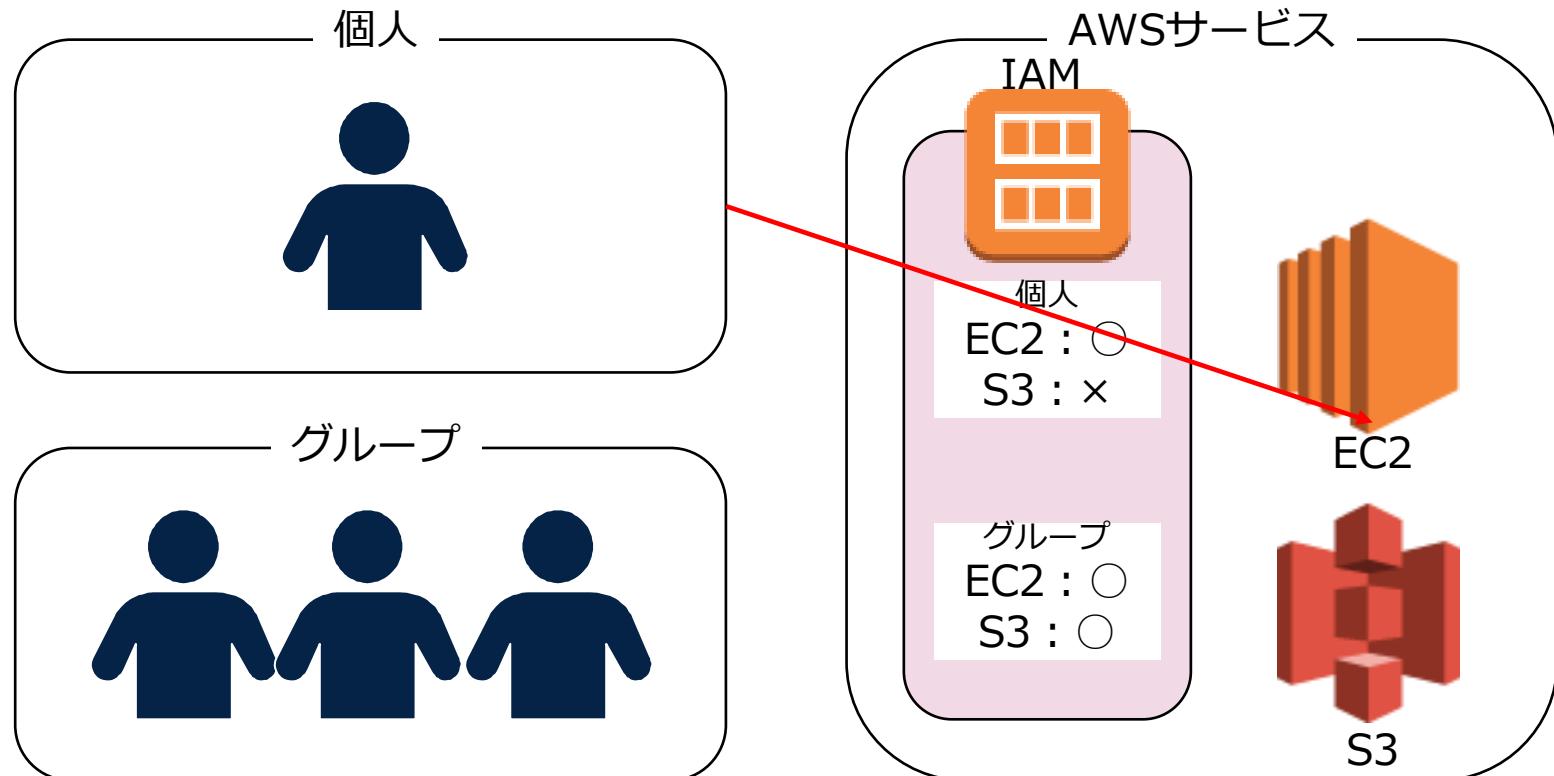
IAMとは

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



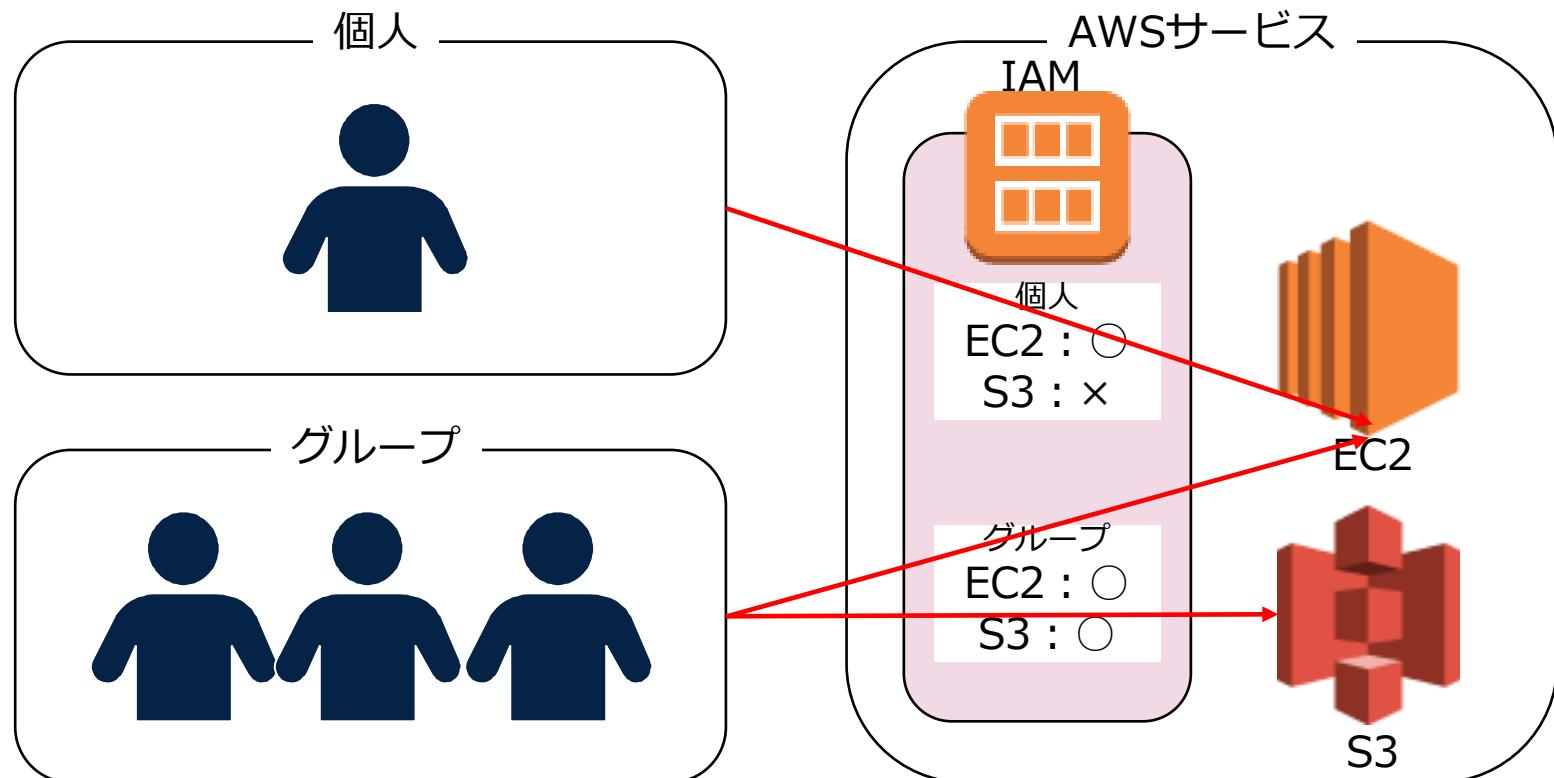
IAMとは

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



IAMの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

IAMユーザー	✓ IAMユーザーの設定方法や利用方法が問われる。
ルートアカウント	✓ ルートアカウントの権限範囲が問われる。 ✓ ルートアカウントの利用制限に関するベストプラクティスが問われる。
IAMグループ	✓ IAMグループの利用目的や設定方法が問われる。
IAMポリシー	✓ IAMポリシーのドキュメントを読み込んで、その設定が示す許可状況が問われる。
IAMポリシーのタイプ	✓ IAMポリシーの各タイプの内容や利用目的が問われる。 ✓ また、MFAの利用、パスワードの強化などの基本的な推奨事項が問われる。

IAMの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

IAMロールの設定	✓ IAMロールを設定する場合のケース内容が問われる。
IAMの認証方式	✓ アクセスキーとシークレットアクセスキーが必要な認証ケースが問われる。 ✓ MFAの認証が必要なベストプラクティスが問われる。
IAMデータベース認証	✓ 主にRDSの認証設定に使われる方式としてIAMデータベース認証の利用が問われる。
ユーザーのアクティビティの記録	✓ IAMユーザーのアクティビティなどの記録管理に利用されるツールの利用方法が問われる。
IAM権限のベストプラクティス	✓ 主に最小権限に基づいた権限設定などのベストプラクティスが問われる。

主要トピック

ユーザー、グループ、ポリシー、ロールがIAMの主要な要素

ユーザー

グループ

ポリシー

ロール

[Q] IAMポリシー

次のIAMポリシーでAWSリソースに対する権限設定を行っています。

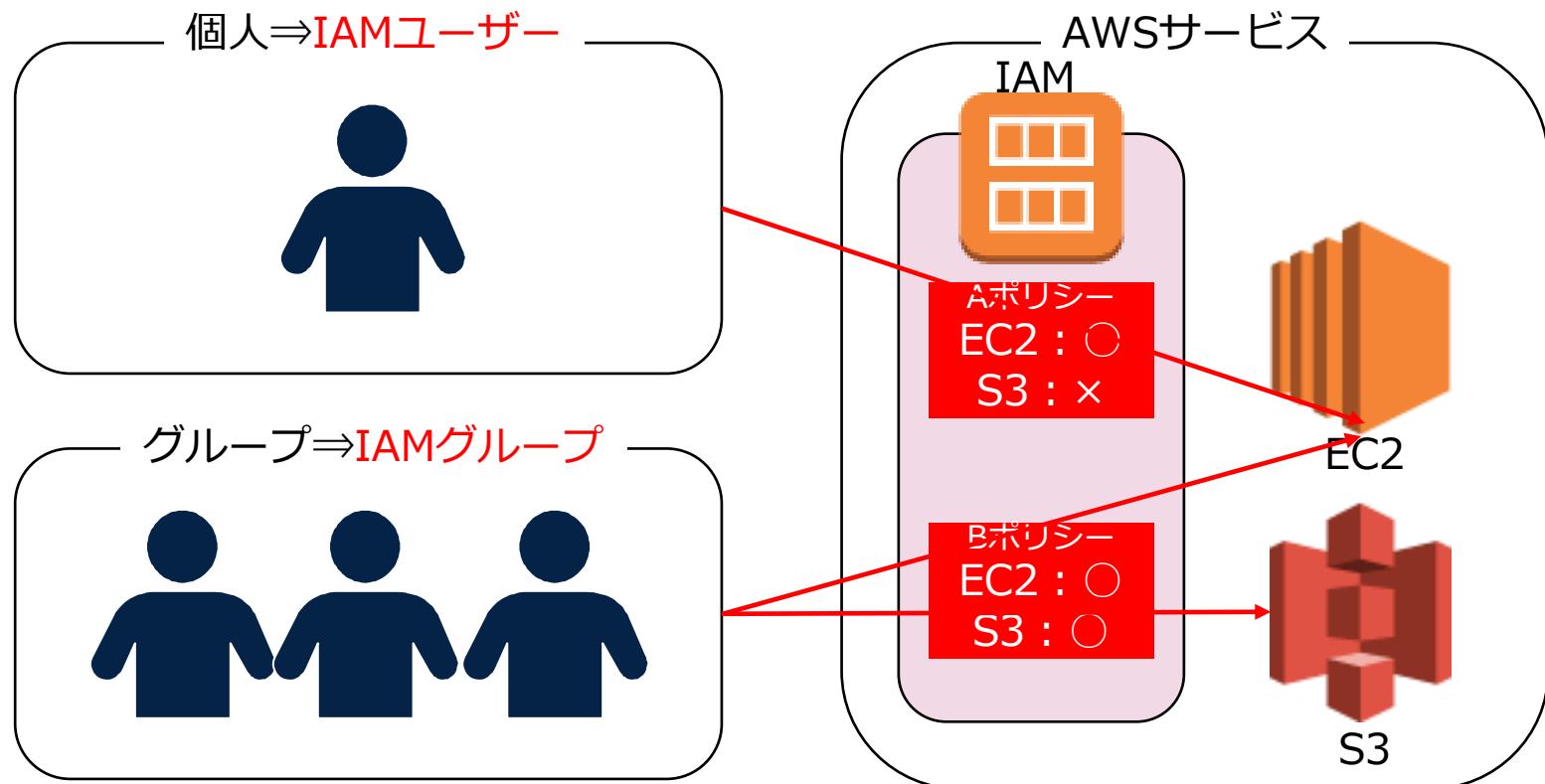
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "*",  
            "Resource": "*",  
            "Condition": {  
                "NotIpAddress": {  
                    "aws:SourceIp": [  
                        "172.103.1.38/24"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

この設定内容として正しい内容を選択してください。

- 1) IPアドレス（172.103.1.38）以外は全てのリソースのアクセス権限を拒否されている。
- 2) IPアドレス（172.103.1.0）は全てのリソースのアクセス権限を有している。
- 3) IPアドレス（172.103.1.3）は全てのリソースのアクセス権限を拒否されている。
- 4) IPアドレス（172.103.1.3）は全てのリソースのアクセス権限を有している。

IAMポリシー

ユーザーなどへのアクセス権限を付与するための設定ドキュメントのこと（JSON形式の文書）



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

[Q] IAMユーザー

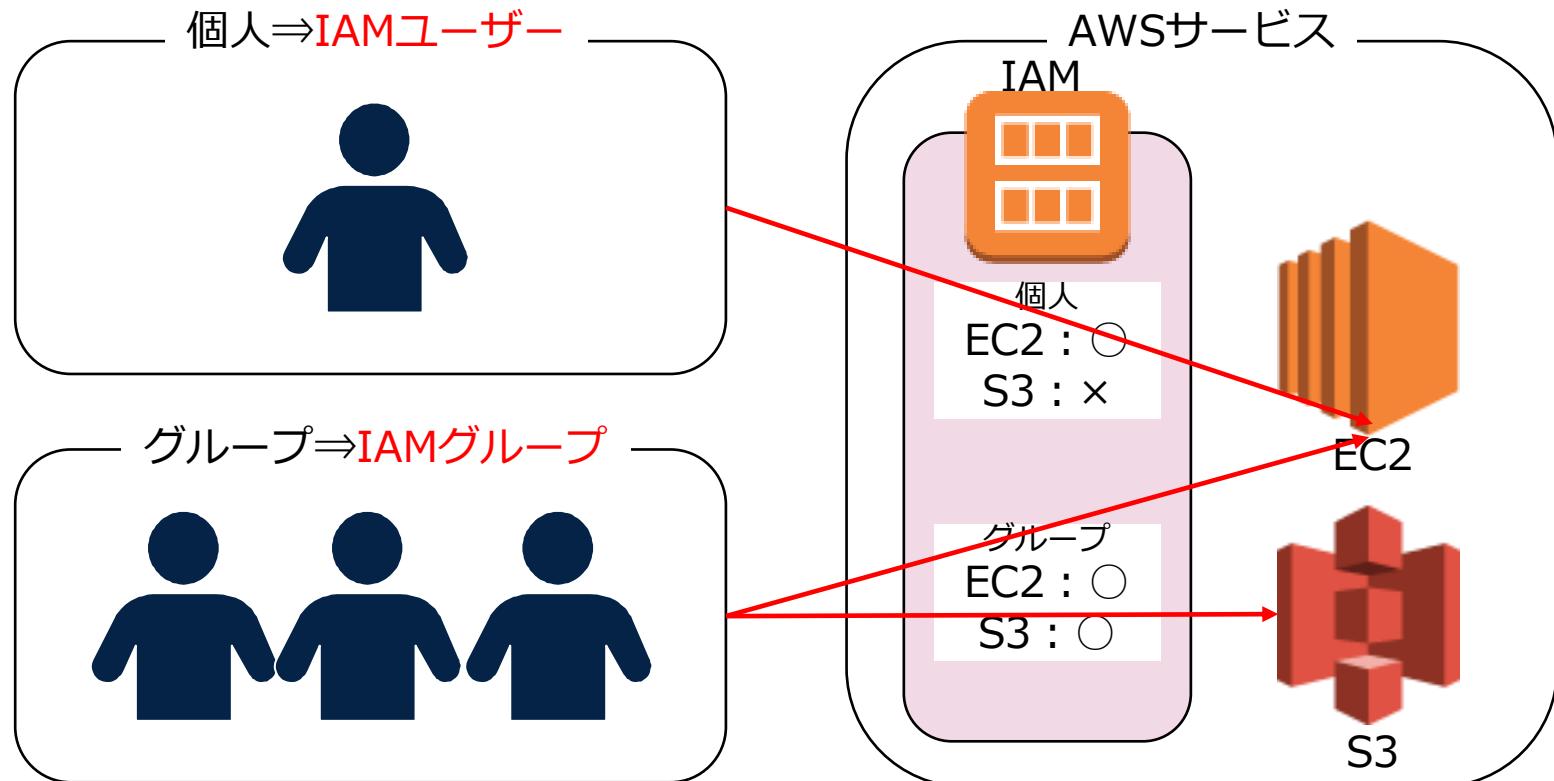
あなたはソリューションアーキテクトとして、部署内で新人のAWS担当者にAWSへのアクセス権限を設定しているところです。IAMユーザーを複数作成しましたが、作成されたIAMユーザーにはデフォルトでどのような権限が含まれているか確認することが必要です。

次の中でIAMユーザーのデフォルト権限として正しい説明はどれでしょうか？

- 1) 制限的な許可が設定されている。
- 2) 管理者権限以外のリソースへのアクセス許可が設定されている。
- 3) 何も権限を有していない。
- 4) デフォルトで基本リソースへの許可設定が付与されている。

IAMユーザー

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ユーザー

AWS上の利用者はIAMユーザーという権限を付与されたエンティティとして設定される。

ルートアカウント (IAMではない)	<ul style="list-style-type: none">• AWSアカウント作成時に作られるIDアカウント• 全てのAWSサービスとリソースを使用できる権限を有する• 日常的なタスクはルートユーザーを使用しないことが強く推奨される
管理者権限 (IAMユーザー)	<ul style="list-style-type: none">• 管理者権限の許可が付与されたIAMユーザーのこと• IAMの操作権限まであり• ルートアカウントしかできない権限は付与されない。
パワーユーザー (IAMユーザー)	<ul style="list-style-type: none">• パワーユーザーはIAM以外の全てのAWSサービスにフルアクセス権限を有するIAMユーザー• IAMの操作権限なし

[Q]ルートアカウント

あなたは新規にAWSの利用を開始しました。AWSにアカウント登録するとルートアカウントと呼ばれるアカウントが1つ作成されて、AWS操作を実行できます。AWSではIAM管理者権限を有するIAMユーザーを利用して管理を実施することが推奨されていますが、ルートアカウントでしか実行できない操作があるようです。

ルートアカウントのみに実施可能な対応を選択してください。（2つ選択してください。）

- 1) IAMユーザーに対して課金情報へのアクセス許可を設定する。
- 2) AWSアカウント内のユーザー管理を実施する。
- 3) Route53を利用したドメイン登録を実施する。
- 4) AWSサポートへの連絡を行う。
- 5) AWS Organizationsにおいてメンバーアカウントになる。

ルートアカウント

ルートアカウント（ルートユーザー）にしかできない操作権限が存在する

【ルートユーザーのみの実施権限】

- AWSルートアカウントのメールアドレスやパスワードの変更
- IAMユーザーの課金情報へのアクセスに関するactivate/deactivate
- 他のAWSアカウントへのRoute53のドメイン登録の移行
- AWSサービス（サポート等）のキャンセル
- AWSアカウントの停止
- コンソリディテッドビリングの設定
- 脆弱性診断フォームの提出
- 逆引きDNS申請

[Q] IAMグループ

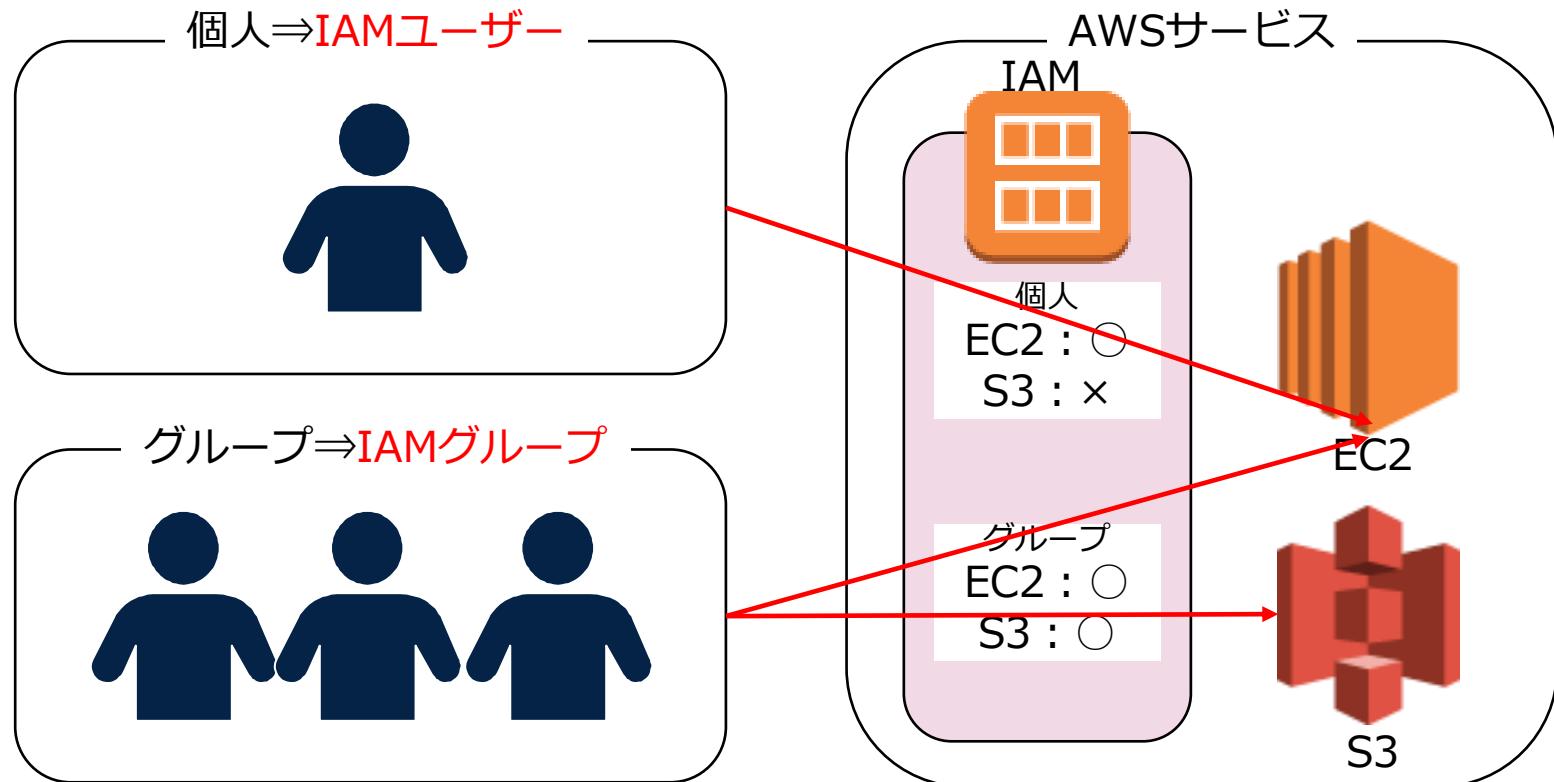
会社は300人以上のAWS利用者を設定することが必要です。これらのユーザーは3つの部署に分かれており、各部署の担当部門ごとに利用するAWSリソースが異なります。あなたはソリューションアーキテクトとして、これらのユーザーへの最適な権限設定を検討するように依頼されました。

最小権限の原則に基づいて、どのように権限を設定するべきでしょうか？

- 1) 各ユーザーに必要な最小権限を設定したIAMポリシーを作成して、IAMユーザーに設定する。
- 2) 各ユーザーに必要な最小権限を設定したIAMポリシーを作成して、IAMグループに設定する。IAMユーザーを各IAMグループに配置する。
- 3) 各ユーザーに必要な最小権限を設定したIAMポリシーを作成して、IAMユーザーに設定する。さらに、これらのIAMユーザーをIAMグループに配置する。
- 4) 各部署に対してIAMグループを作成して、各ユーザーに必要な最小権限を設定したIAMポリシーを設定する。

IAMグループ

グループとして権限をまとめて設定された単位のこと。グループには通常は複数のIAMユーザーが設定される



[Q]IAMロール

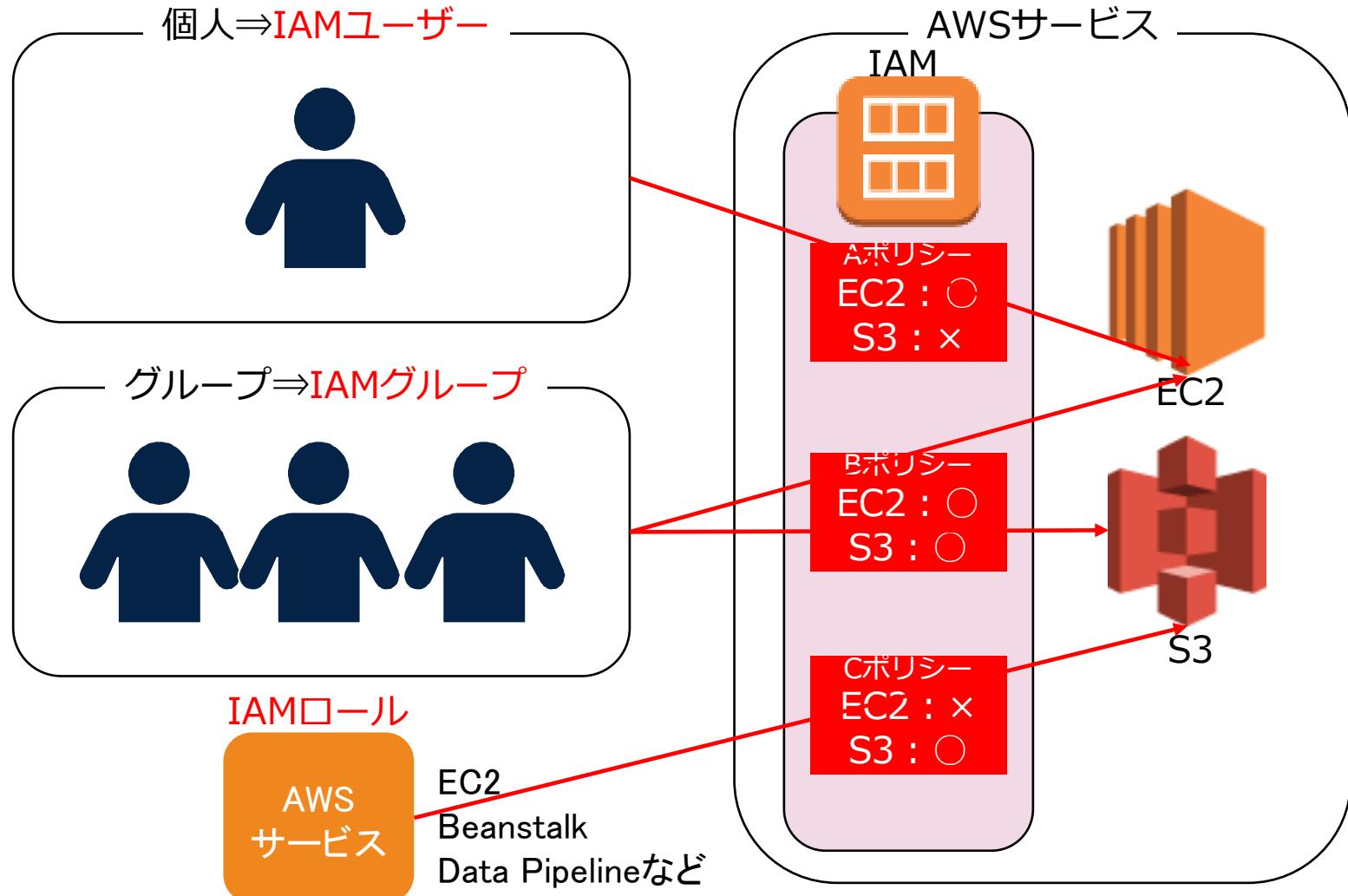
ソリューションアーキテクトは、Lambda関数を利用したデータベースオペレーションを実行するアプリケーションを構築しています。このサーバレスアプリケーションは、Amazon DynamoDBテーブルにアクセスして、データを取得して加工する処理を実行します。

Lambda関数にDynamoDBテーブルへのアクセスを許可する最も安全な手段は何ですか？

- 1) DynamoDBテーブルにアクセスするために必要な権限を持つIAMロールを作成し、そのロールをLambda関数に割り当てる。
- 2) DynamoDBテーブルにアクセスするために必要な権限を持つIAMポリシーを作成し、そのロールをLambda関数に割り当てる。
- 3) DynamoDBテーブルにアクセスするために必要な権限を持つIAMグループを作成し、そのロールをLambda関数に割り当てる。
- 4) DynamoDBテーブルにアクセスするために必要な権限を持つIAMユーザーを作成し、そのロールをLambda関数に割り当てる。

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



[Q] IAMポリシーのタイプ

大手IT企業では、1つのAWSアカウントを利用して開発者グループにパワーアクセス権限のあるアカウントを用意して開発を進めていました。しかしながら、1人の開発担当者が本番環境にあるRoute53を不用意に削除したことで、重要なアプリケーションが長時間ダウンするトラブルが発生していました。このインシデントが報告された後、セキュリティのベストプラクティスによる制御を実施するように依頼されました。各グループごとにIAM管理者が権限管理をしているため、あらかじめグループ毎に付与される権限を制限することが必要です。

このようなインシデントが再発しないように適切な対応を選択してください。

- 1) ルートアカウントを利用して、管理者権限をルートアカウントのみに制限する。
- 2) SCPを利用して、開発担当者がIAMアイデンティティに付与できる最大権限を制御する。
- 3) IAMグループを利用して、開発者グループの担当者の権限設定を制限する。
- 4) アクセス許可の境界を使用して、開発担当者のIAMアイデンティティに付与できる最大権限を制御する。

IAMポリシーのタイプ

IAMポリシーはユーザーベースのポリシーと呼ばれるポリシーであり、他にも多数のポリシーが存在する。

ユーザーベースの ポリシー

- ✓ 管理ポリシーとインラインポリシーを IAM エンティティ(ユーザー、ユーザーのグループ、ロール) にアタッチされるポリシー。
- ✓ ユーザー ポリシーのアクセス許可はエンティティに付与される。

リソースベースの ポリシー

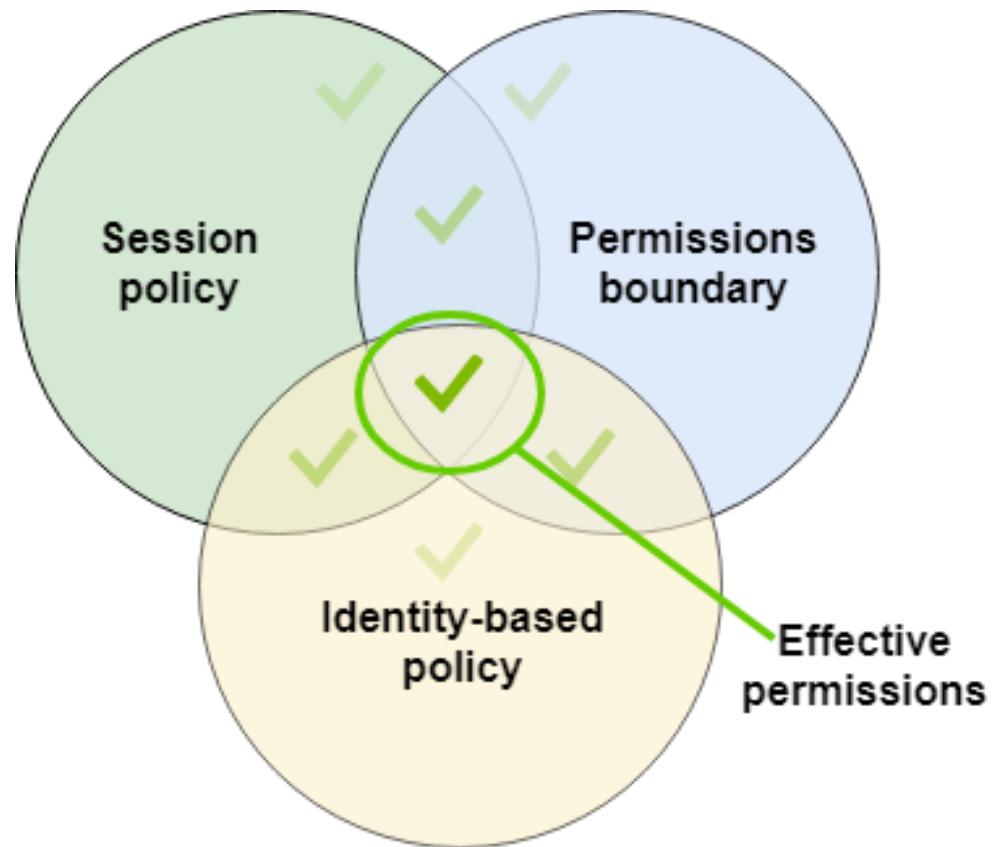
- ✓ バケットポリシーなどの JSON 形式のドキュメントで定義されたインラインポリシーをリソースにアタッチするポリシー
- ✓ 例は Amazon S3 バケットポリシー や IAM ロールの信頼ポリシー

アクセス許可 の境界

- ✓ アクセス許可の境界はユーザーベースポリシーが IAM エンティティ に付与できるアクセス許可の上限を設定する。アクセス許可自体は付与しない。
- ✓ IAM エンティティはユーザーベースポリシーとアクセス許可境界の両方で許可されているアクションのみ許可される。

アクセス許可の境界

アクセス許可の境界で許可設定の上限を設定してから、他のポリシーで許可を設定することができる。



IAMポリシーのタイプ

IAMポリシーはユーザーベースのポリシーと呼ばれるポリシーであり、他にも多数のポリシーが存在する。

SCP

- ✓ 組織または組織単位 (OU) のメンバーアカウントのアクセス許可の上限を定義するポリシー
- ✓ アクセス許可の境界と同様にこれ自体はアクセス許可は付与しない。
- ✓ メンバーアカウント内のIAMユーザーはSCPとIAMポリシーの両方で許可されているアクションのみ実行できる。

ACL

- ✓ ACL がアタッチされているリソースへのアクセス許可・拒否を制御
- ✓ JSON ポリシードキュメント構造を使用しない点がリソースベースのポリシーと異なる。
- ✓ 定されたプリンシパルにアクセス許可を付与するクロスアカウントのアクセス許可ポリシー

セッションポリシー

- ✓ ロールまたはフェデレーティッドユーザーの一時セッションをプログラムで作成する際にパラメータを渡す機能
- ✓ 作成したセッションのアクセス許可が制限されますが、アクセス許可は付与されない。

[Q] ユーザーベースのポリシータイプ

あなたはソリューションアーキテクトとして、AWSを利用したアカウント管理を実施しています。まずはIAMユーザーを作成して、AWS利用者へのアカウント権限を発行する必要があります。アカウント権限として管理者権限を有するユーザー2人へのIAMポリシーが必要です。

この権限管理を実施するために、最も容易に利用できるIAMポリシータイプを選択してください。

- 1) AWS管理ポリシーの管理者権限を利用する
- 2) インラインポリシーを利用する
- 3) サードパーティのポリシーを利用する
- 4) カスタマー管理ポリシーを利用する

ユーザーベースのポリシータイプ

IAMポリシーを作成してユーザーなどへのアクセス権限を付与

管理ポリシー

【AWS管理ポリシー】

AWSが作成および管理する管理ポリシー

【カスタマーマネジメントポリシー】

AWSアカウントで作成・管理する管理ポリシー。
同じポリシーを複数のIAMエンティティにアタッチできる

インラインポリシー

ユーザーが作成および管理するポリシー

1つのプリンシパルエンティティ（ユーザー、グループ、またはロール）に埋め込まれた固有ポリシーで、プリンシパルエンティティにアタッチすることができる

[Q] IAMロールの信頼ポリシー

あなたの会社はAWSを利用してアプリケーションを構築しています。このアプリケーションにベンダーA社のソリューションを組み込むために、その会社の担当者に対して一時的なアクセスが必要です。あなたはソリューションアーキテクトとして、この担当者にアクセス権限を委任して、一部のリソースにアクセスできるようにしたいと考えています。

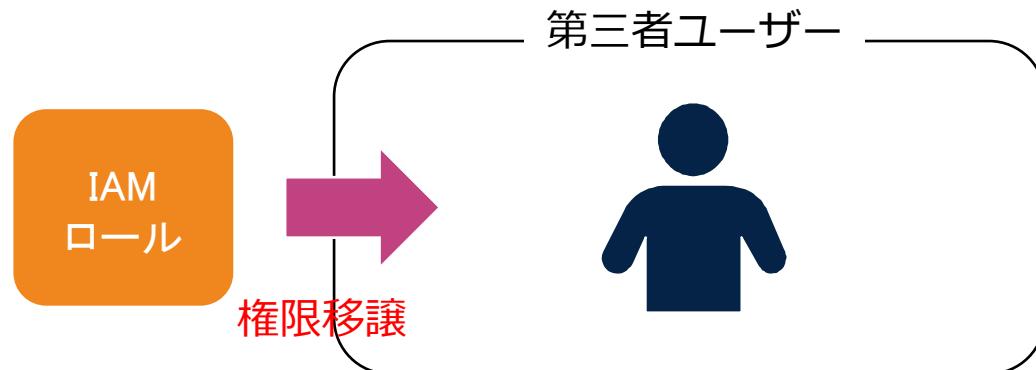
ソリューションアーキテクトとして、次のどの対応を実施するべきでしょうか？

- 1) 新しいIAMユーザーを作成して、必要なAWSリソースへの権限を設定した上で、A社の担当者に付与する。
- 2) 一時認証用の仕組みであるSTSを作成して、必要なAWSリソースへの権限を設定した上で、A社の担当者に付与する。
- 3) アクセスキーを発行して、必要なAWSリソースへの権限を設定した上で、A社の担当者に付与する。
- 4) 新しいIAMロールを作成して、必要なAWSリソースへの権限を設定した上で、A社の担当者に付与する。

IAMロールの信頼ポリシー

IAMロールは監査人などに一時的な権限を委譲する際にも利用される。

- ✓ IAMロールの権限移譲操作に特化したポリシー
- ✓ 当該の信頼ポリシーを関連づけたIAMロールが保有する権限を、信頼ポリシーの操作主体であるPrincipalに移譲(を許可)することができる。



[Q] IAMの認証方式

あなたはソリューションアーキテクトとして、WEBアプリケーションをAWS上で開発しています。このアプリケーションはHTTPSを使用して別のWEBアプリケーションを呼び出すことが必要であり、IAMによってWebサービスに直接アクセスして、連携する機能が必要です。

アプリケーションがコード上でIAMと連携するための最適な設定方法を選択してください。

- 1) IAMロールを作成して、アプリケーション上で実行する。
- 2) IAMユーザーを作成して、アプリケーション上で実行する。
- 3) ユーザー用のアクセスキーのセットを作成して、アプリケーション上で実行する。
- 4) Cognitoをアプリケーション上に実装して、STSを発行して連携する。

IAMの認証方式

IAMによるユーザー認証方式は利用するツールに応じて異なる。

アクセスキーID／
シークレット
アクセスキー

- EC2インスタンス接続などREST/Query形式
- AWS CLI やAPI利用時の認証に使用する

X.509 Certificate

- SOAP形式のAPIリクエスト用の認証方式

AWSマネジメントコン
ソールへの
ログインパスワード

- AWSアカウントごとにパスワードを設定してログイン認証する。
- デフォルトは未設定（ログインできない）

MFA(多要素認証)

- 物理デバイスなどを利用したピンコードによる認証方式。ルートアカウントなどはMFAを付与してセキュリティを強化することが推奨される。

[Q] IAMデータベース認証

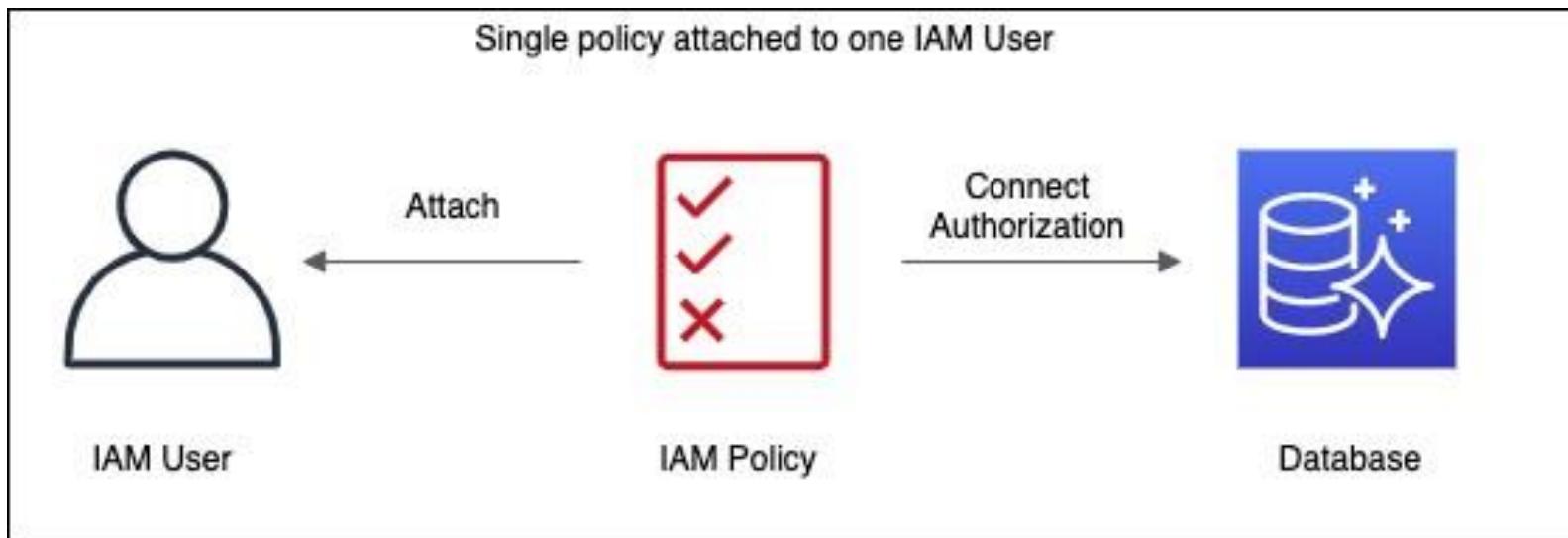
あなたの会社ではAWSを利用したデータベースソリューションを構築しており、複数のAmazon RDS MySQLデータベースを利用しています。現在、ユーザーIDによるMySQLの通常の認証方式を利用してアプリケーションからデータベースに接続をしていますが、コード上でパスワードを実行することはセキュリティ上の懸念があります。

セキュリティを向上させるために、短期間の資格情報を使用して安全なユーザーアクセスを有効化する方法はどれでしょうか？

- 1) IAMデータベース認証を利用する。
- 2) AWS STSを使用するようにMySQLデータベースを設定する
- 3) AUTHコマンドをデータベース認証を実行する。
- 4) IAMロールを利用した一時的な認証をアプリケーション上で実行する。

IAMデータベース認証

IAM DB認証を利用してIAM ユーザーまたはIAMロール認証と認証トークンを使用して Amazon RDS DBに接続可能
(通常DBはユーザーIDとパスワードで認証する)



Reference: <https://aws.amazon.com/jp/blogs/news/using-iam-authentication-to-connect-with-pgadmin-amazon-aurora-postgresql-or-amazon-rds-for-postgresql/>

[Q]ユーザーのアクティビティの記録

あなたの会社では一部のS3バケットについてIAMポリシーによって、外部の第三者のアプリケーションによるファイル読み込みを許可しています。したがって、これらのアクセスが想定された外部利用者に正しく利用されており、想定外の利用がされていないかを確認することが必要です。

この確認する仕組みとして最適な方法を選択してください。

- 1) CloudTrail
- 2) サーバーアクセスログ
- 3) ストレージクラス分析
- 4) IAM Access Analyzer

ユーザーのアクティビティの記録

目的に応じて様々なツールを利用して記録を取得できる。

IAMアクセス アナライザー	外部エンティティと共有されている S3 バケットや IAM ロールなど分析し、セキュリティ上のリスクであるリソースとデータへの意図しないアクセスを特定
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
Credential Report	利用日時などが記録されたIAM認証情報のレポートファイル
AWS Config	AWS ConfigはIAMのユーザー、グループ、ロール、ポリシーの変更履歴、構成変更を管理するサービス
AWS CloudTrail	AWS CloudTrailは各種アカウントアクティビティやAPIコールをログに記録し、モニタリングするサービス

[Q] IAM権限のベストプラクティス

あなたはAWSアカウントを新規に作成して、 AWSの設定を行っているところです。 AWSでは新規に作成したアカウントに対して設定すべきベストプラクティスが定義されています。 これは実行しなければAWSを利用できないわけではありませんが、 実行が推奨されているため、 あなたは対応することになりました。

ソリューションアーキテクトとして、 AWSの初期に対応するべき事項を選択してください。 (3つ選択してください。)

- 1) 全てのユーザーに対してMFA認証を有効化する。
- 2) CloudTrailの証跡実行を有効化する。
- 3) CloudWatchのモニタリングを有効化する。
- 4) Configのモニタリングを有効化する。
- 5) パスワードで二段階認証を有効化する。
- 6) 強度の高いパスワードポリシーを設定する。

IAM権限のベストプラクティス

IAMを利用する際はベストプラクティスに沿った運用をする。

- ✓ AWS アカウントのルートユーザーのアクセスキーをロックして通常はルートアカウントを使用しない。
- ✓ 個々の IAM ユーザーを作成して、IAMユーザーで管理を行う。
- ✓ IAMユーザーへのアクセス許可を割り当てにIAMグループを利用する。
- ✓ IAMユーザーとIAMグループには最小権限のみを設定する。
- ✓ 新しくポリシーを作るのではなく、AWS管理ポリシーを使用する。
- ✓ インラインポリシーではなくカスタマー管理ポリシーを使用する。
- ✓ アクセスレベルを使用して、IAM アクセス許可を確認する
- ✓ ユーザーのために強度の高いパスワードポリシーを設定する。
- ✓ MFA を有効化する。
- ✓ Amazon EC2 インスタンスで実行するアプリケーションにはIAMロールを使用する
- ✓ 第三者に一時的に認証を付与する場合はIAMロールを使用してアクセス許可を移譲する
- ✓ アクセスキーを共有しない
- ✓ 認証情報を定期的にローテーションする。
- ✓ 不要な認証情報の削除する。
- ✓ AWS アカウントのアクティビティを監視する。

S3の出題範囲

S3とは何か？

S3は耐久性と可用性が非常に高くデータの中長期保存に最適なストレージ

ファイルやフォルダのアップロードや、バケットのバージニング、タグ、デフォルトの暗号化など、バケットの追加設定を行うには、[詳細の表示] を選択します。

Amazon S3

① S3 コンソールの新しいバージョンは引き続き改善されますが、バケットの以前のコンソールエクスペリエンスに一時的に切り替えることができます。エクスペリエンスの向上に役立てるため、フィードバックをお寄せください。

バケット (4)

バケットは S3 に保存されたデータのためのコンテナです。詳細

Q バケットを名前で検索

名前	リージョン	アクセス	作成日
elasticbeanstalk-ap-northeast-1-860853660447	アジアパシフィック (東京) ap-northeast-1	オブジェクトは公開することができます	2020/06/17 04:59:48 PM JST
test20200714-2	アジアパシフィック (東京) ap-northeast-1	非公開のバケットとオブジェクト	2020/07/14 08:09:04 PM JST
udemv-vpc111111	アジアパシフィック (東京) ap-northeast-1	非公開のバケットとオブジェクト	2020/07/01 10:35:38 PM JST
udemv2020108	アジアパシフィック (東京) ap-northeast-1	オブジェクトは公開することができます	2019/12/08 06:39:46 PM JST

Amazon S3 > test20200714-2

概要 プロパティ アクセス権限 管理 アクセスポイント

Q ブレフィックスを入力し、Enter キーで検索します。ESC を押してクリアします。

▲ アップロード + フォルダの作成 ダウンロード アクション ▾

アジア

名前	最終更新日時	サイズ	ストレ
2594890_d1eb_2.jpg	7月 14, 2020 8:10:50 午後 GMT+0900	17.6 KB	スタン

S3とは何か？

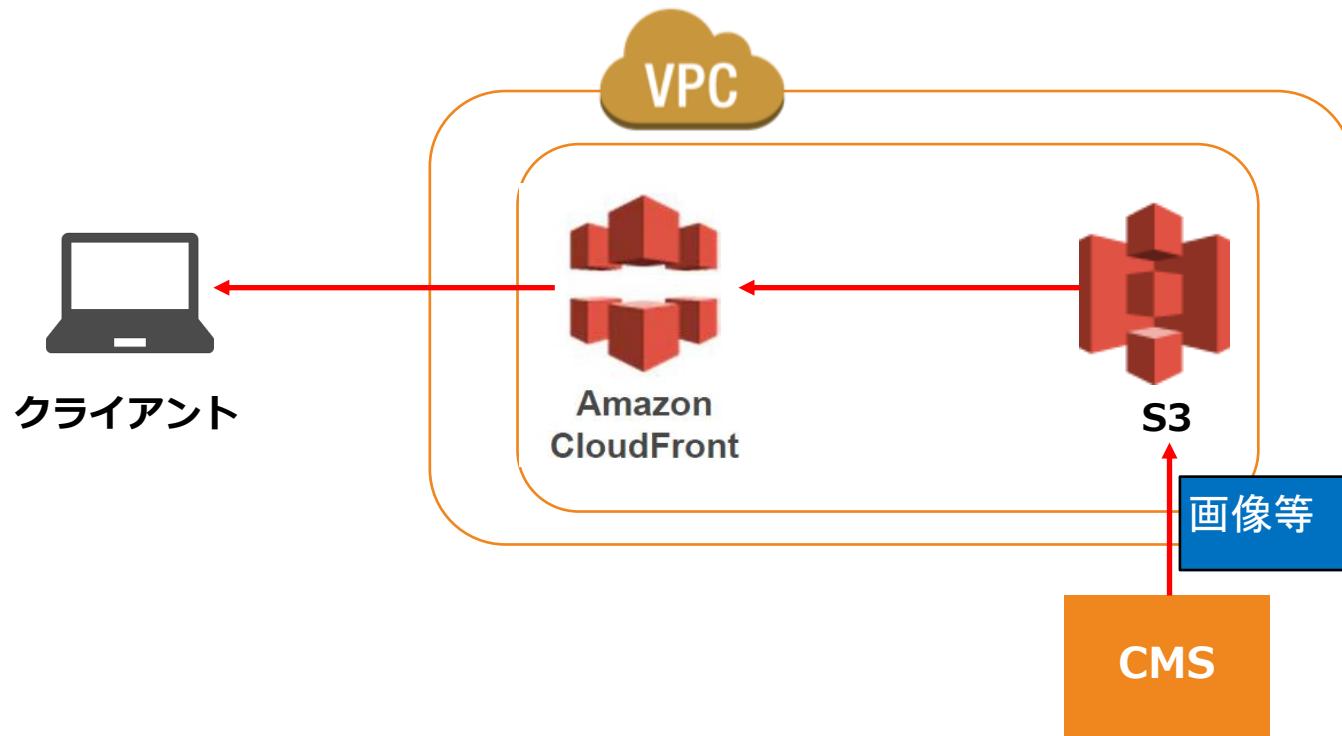
S3は耐久性と可用性が非常に高くデータの中長期保存に最適なストレージ

The screenshot shows the Amazon S3 console interface. The file path is `test20200714-2 > 2594890_d1eb_2.jpg`. The file name is `2594890_d1eb_2.jpg`, and the version is `最新バージョン`. The file was created by `shingoshibata` on `7月 14, 2020 8:10:50 午後 GMT+0900`. The ETag is `34e638997f57f722d3c4b34b1bd9c61`. The storage class is `スタンダード`. There is no server-side encryption. The size is `17.6 KB`. The key is `2594890_d1eb_2.jpg`. A red box highlights the `オブジェクト URL` field, which contains the value `https://test20200714-2.s3-ap-northeast-1.amazonaws.com/2594890_d1eb_2.jpg`. A red arrow labeled ③ points from this URL to the AWS logo in the next image.



S3のユースケース

コンテンツ配信用の画像データなどをS3に保存して、CloudFrontを利用して配信する。



S3の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

S3ストレージの特徴	<ul style="list-style-type: none">✓ シナリオのストレージ要件を満たすストレージを選択する質問✓ S3ストレージの特徴を回答させる質問
S3のデータ容量制限	<ul style="list-style-type: none">✓ S3のデータ容量に関するシンプルな質問
ストレージクラスの選択	<ul style="list-style-type: none">✓ シナリオのストレージ要件を満たすS3のストレージクラスを選択する。✓ ライフサイクル管理と一緒に出題されるパターンも多い。
S3の利用コスト	<ul style="list-style-type: none">✓ S3におけるコストが発生する要素が質問として出題される。✓ リクエストに応じた課金設定が可能な機能が問われることも。
ライフサイクル管理	<ul style="list-style-type: none">✓ ライフサイクル管理によってデータ保存期間に応じて、ストレージクラスを移動させたり、削除させる適切な設定パターンが出題される。出来る組合せ／出来ない組合せがある。

S3の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

バージョン管理	<ul style="list-style-type: none">✓ S3ストレージ内のデータを誤って削除してしまった場合の予防策が問われる。✓ MFA削除がセットで回答されるパターンが多い。
S3のアクセス管理	<ul style="list-style-type: none">✓ バケットポリシー、ACL、IAMの利用方法と使い分けの問題✓ バケットポリシー自体の設定内容を問う問題✓ 事前署名付きURLによるアクセス制限に関する問題
ブロック パブリックアクセス	<ul style="list-style-type: none">✓ オブジェクトのインターネットへの公開設定方法の問題が出題される。
クロスアカウント アクセス	<ul style="list-style-type: none">✓ 他のアカウントにバケットを利用させる設定方法の問題が出題される。
S3アクセスポイント	<ul style="list-style-type: none">✓ S3アクセスポイントの利用目的を問う問題が出題される。

S3の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

静的WEBホスティング	✓ 静的WEBホスティングを実行するための設定方法や、静的コンテンツを実施する機能を選択させる質問が出題される。
Route53によるドメイン設定	✓ 静的WEBホスティングに対してRoute53によるドメインを設定する方法が問われる。
クロスオリジンリソースシェアリング(CORS)	✓ オリジンとしてドメインが設定されたS3バケットを別のドメインに共有する方法が問われる。
S3イベント	✓ S3イベントが利用可能なサービスを選択する質問が出題される。 ✓ S3イベントを利用した実装方法が出題される。
S3の暗号化	✓ S3で利用できる暗号化方式が問われる。

S3の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

レプリケーション	✓ S3でのレプリケーション方式やその設定方法が問われる。
S3のデータ解析	✓ S3と連携してデータ解析するサービスの選択が問われる。
S3の利用状況の確認	✓ S3のデータ利用状況やアクセス状況を確認・分析する方法が問われる。
S3の整合性モデル	✓ S3の読み込みや書き込みの整合性モデルに起因した問題が問われる。
マルチパートアップロード	✓ 大きなファイルをアップロードする際の最適な手法が問われる。

S3の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

S3 Transfer Acceleration	<ul style="list-style-type: none">✓ S3へのデータアップロードをグローバルに最適化するために必要な対応として出題される。
パフォーマンスの向上	<ul style="list-style-type: none">✓ データの取得リクエストなどを効率化する方法が問われる。✓ オブジェクトを多数アップロードする際に大量リクエストを処理する効率的な設定が問われる。

[Q] S3ストレージの特徴

ベンチャー企業は複数のEC2インスタンスを利用してWEBアプリケーションを構築しています。このアプリケーションはアクセスやAPIコールに応じたログファイルを作成し続けるため、大量のログファイルを保存するストレージを必要としています。ストレージには頻繁にアクセスが発生し、大量のデータを安価に保存することが求められています。

次の中で、どのストレージサービスが最も費用効果が高いですか？

- 1) Amazon EFS
- 2) Amazon EBS
- 3) Amazon S3
- 4) Amazon EC2 インスタンスストア

S3ストレージの特徴

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

S3ストレージの特徴

S3はデータをオブジェクトとして保存。オブジェクトは以下の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

■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

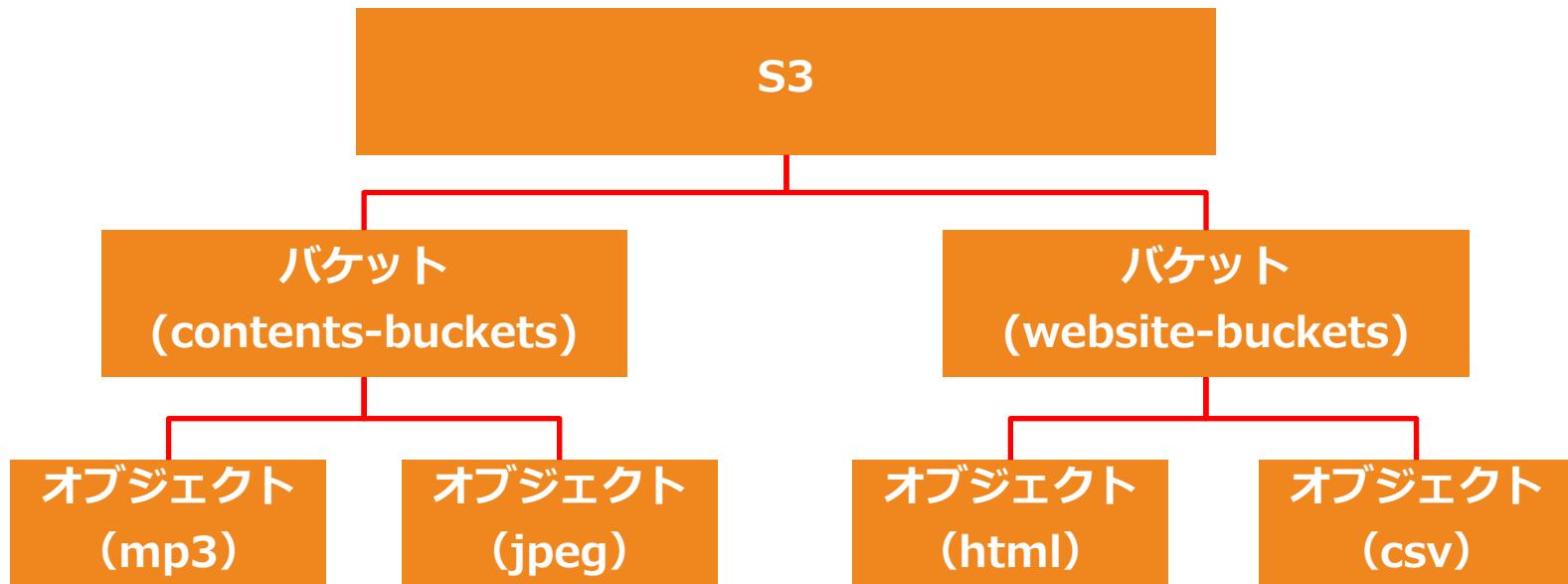
■サブリソース

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：アクセスコントロールリスト（ACL）

S3ストレージの特徴

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



[Q] S3のデータ容量制限

あなたは大手製造企業のエンジニアとして働いています。現在、あなたは社内に大量にある製造ドキュメントを効率的に保存・共有するための文書管理アプリケーションを構築しています。このソリューションではS3を利用してデータを保存することが決まっていますが、保存データに関する制限の確認が必要です。

次の中で、Amazon S3のデータ保存の制約として正しい説明はどれですか？（2つ選択してください。）

- 1) S3のストレージ容量はバケット作成時に設定し、その後自動でスケーリングする。
- 2) ストレージのデータ量と保存できるオブジェクトの数は無制限である。
- 3) 1つのPUTでアップロードできる最大のオブジェクトは5GBである
- 4) 1つのPUTでアップロードできる最大のオブジェクトは5TBである
- 5) S3は、ファイルシステムアクセスセマンティクス（強力な整合性やファイルロックなど）と、同時にアクセス可能なストレージを提供する。
- 6) S3のアクセスにはマウントヘルパーを利用する。

S3のデータ容量制限

S3のストレージ容量は無制限であり、 0KBから5TBまでのデータを保存可能

S3のデータ容量制限

■バケット

オブジェクトの保存場所。リージョンに設置されるため、名前はグローバルでユニークにする。**データ保存容量は無制限であり、自動でストレージ容量が拡張される。**

■オブジェクト

S3に格納されるファイル形式で、オブジェクトに対してURLが付与される。バケット内に**保存可能なオブジェクト数は無制限**

■保存可能なオブジェクトサイズの制限

オブジェクトあたりのデータサイズは**0KBから5TBまで保存可能**

[Q] ストレージクラスの選択

世界4大監査法人の1つであるA社は、様々な監査レポートを作成しています。これらの監査レポートはセキュリティを強固にした上で、一定期間保存することが必要となります。また、これらの監査レポートを作成するための基礎となるデータはS3に保存され、数百テラバイトに達します。監査レポートの元データと監査レポートは頻繁にアクセスが発生します。

このユースケースに最適な最も費用効果の高いストレージクラスはどれですか？

- 1) S3 Standard-IA
- 2) S3 Standard
- 3) S3 Intelligent Tiering
- 4) S3 Glacier

ストレージクラスの選択

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	<ul style="list-style-type: none">✓ 複数個所にデータを複製するため耐久性が非常に高い。✓ 頻繁に利用するデータを大量に保存するのに向いている。	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.99%
STANDARD-IA	<ul style="list-style-type: none">✓ IAはInfrequency Accessの略であり、低頻度アクセスデータ用のストレージ。 One Zone-IAより重要なマスターデータ向け。データ取得は早い✓ Standard に比べて安価だが、One Zone-IAよりは高い。	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.9%
One Zone-IA	<ul style="list-style-type: none">✓ 低頻度アクセス用のストレージだが、マルチAZ分散されていないため可用性が低く、重要ではないデータ向け。その分Standard IAよりも値段が安い	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.5%
RRS	<ul style="list-style-type: none">✓ 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に利用する。✓ 現在は非推奨ストレージであり、利用されない。今ではStandardよりも値段が高い	<ul style="list-style-type: none">■ 耐久性 99.99%■ 可用性 99.99%

ストレージクラスの選択

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
Amazon Glacier	<ul style="list-style-type: none">✓ 安価な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✓ 迅速取り出しで(2~5分)で取り出し可能✓ 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 N/A
Amazon Glacier Deep Archive	<ul style="list-style-type: none">✓ 最安のアーカイブ用ストレージ✓ 1年に1~2回アクセスするデータ用✓ データ抽出にコストと時間（12時間以内）✓ 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 N/A
S3 Intelligent Tiering	<ul style="list-style-type: none">✓ 高頻度と低頻度という2つのアクセス階層を利用し、 アクセスがあるファイルは高頻度（標準クラス） に維持しつつ、アクセスがないファイルは低頻度 (標準IAクラス) に自動で移動する。✓ アクセスパターンがわからない場合に利用	<ul style="list-style-type: none">■ 耐久性 99.99999999%■ 可用性 99.99%

[Q] S3の利用コスト

あなたはAWSを利用してWEBアプリケーションを構築しています。このアプリケーションでは、EC2インスタンスからストレージにアクセスして、データを保存したり、取得するといった処理が多数発生する予定です。ストレージに必要なI/O性能やレイテンシーなどを比較したところ、S3、EBS、EFSのどれでも対応が可能なようです。そのため、あなたはソリューションアーキテクトとして、最もコストが安いストレージを選択することにしました。また、いづれのストレージにおいても標準ストレージまたは汎用ストレージを利用します。

これら3つのストレージを、コストが安い順番で左から並べてください。

- 1) S3標準 < EBS汎用ボリューム < EFS標準
- 2) S3標準 < EFS標準 < EBS汎用ボリューム
- 3) EBS汎用ボリューム < EFS標準 < S3標準
- 4) EBS汎用ボリューム < S3標準 < EFS標準

S3の利用コスト

ストレージのコストを比較するとインスタンスストアを除けば、最も値段が安いのはS3およびGlacier

S3のデータ容量
に応じたコスト

- ✓ 標準 : 1 GBあたり 0.025USD／月
- ✓ S3 Intelligent Tiering:標準と標準IAの組合せ
- ✓ 標準IA : 1 GBあたり 0.019USD／月
- ✓ One Zone IA : 1 GBあたり 0.0152USD／月
- ✓ Glacier : 1 GBあたり 0.005USD／月
- ✓ Glacier deep archive : 1 GBあたり 0.002USD／月

EBSの汎用
ストレージのコスト

- ✓ 汎用 : 1 GBあたり 0.12USD／月
- ✓ コールドHDD:1 GBあたり 0.03USD／月

EFS
ストレージのコスト

- ✓ 標準 : 1 GBあたり 0.36USD／月
- ✓ 低頻度アクセス : 0.0272USD／月

インスタンスストア

- ✓ EC2インスタンスに含まれる。

[Q] S3の利用コスト

あなたはソリューションアーキテクトとして、AWSを利用した画像加工アプリケーションを構築しています。このアプリケーションでは、ユーザーが画像をAmazon S3にアップロードして加工処理を行います。大きな画像のアップロードするためにS3 Transfer Accelerationを使用していますが、転送処理に失敗してしまったようです。

このシナリオの場合では、画像転送料金はどのように発生しますか？

- 1) 画像のアップロードにS3 Transfer Accelerationは利用した分だけの料金を支払う。
- 2) 画像のアップロードにS3 Transfer Accelerationは無料で利用できる。
- 3) 画像のアップロードにS3転送料金のみを支払う
- 4) 画像のアップロードに転送料金を支払う必要はない。

S3の利用コスト

S3はデータ量とリクエストとデータ転送に対して料金が発生

リージョン	<ul style="list-style-type: none">✓ リージョン：リージョン毎に価格が異なる。
データ容量	<ul style="list-style-type: none">✓ データ容量：データ量と保存期間に応じて料金がかかる。 (GBあたり)✓ S3 Intelligent Tiering、IAストレージには、最低 30 日間の料金
リクエストとデータ取得	<ul style="list-style-type: none">✓ データに対するリクエストに応じて料金がかかる。 (1000リクエストあたり)✓ データを取得した量に応じて料金がかかる (GBあたり)
データ転送	<ul style="list-style-type: none">✓ データ転送イン：無料✓ インターネットへのデータ転送アウト (GBあたり)✓ S3からAWS内のデータ転送アウト (GBあたり)

S3の利用コスト

S3はボリュームディスカウントの価格帯が設定されている

ストレージ料金表

S3 標準 - 頻繁にアクセスするデータに一般的に使用される、あらゆるタイプのデータの汎用ストレージ

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

S3 Intelligent - Tiering * - アクセスパターンが不明または変化するデータの自動コスト削減

高頻度アクセスティア、最初の 50 TB/月	0.025USD/GB
高頻度アクセスティア、次の 450 TB/月	0.024USD/GB
高頻度アクセスティア、500 TB/月を超える	0.023USD/GB
低頻度アクセスティア、すべてのストレージ/月	0.019USD/GB
モニタリングおよびオートメーション、すべてのストレージ/月	オブジェクト 1,000 件あたり 0.0025USD

S3 標準 - 低頻度アクセス * - ミリ秒単位のアクセスが必要な、長期保管だがアクセス頻度の低いデータの場合

すべてのストレージ/月	0.019USD/GB
-------------	-------------

S3 1 ゾーン - 低頻度アクセス * - ミリ秒単位のアクセスが必要な、再作成可能なアクセス頻度の低いデータの場合

すべてのストレージ/月	0.0152USD/GB
-------------	--------------

S3 Glacier ** - 1 分から 12 時間の取り出しオプションを使用した長期バックアップとアーカイブの場合

すべてのストレージ/月	0.005USD/GB
-------------	-------------

S3 Glacier Deep Archive ** - 1 年に 1~2 回アクセスされ、12 時間以内に復元できる長期のデータアーカイブの場合

すべてのストレージ/月	0.002USD/GB
-------------	-------------

[Q] ライフサイクル管理

あなたはソリューションアーキテクトとして、自社のドキュメント管理ストレージを設定・管理しています。保存しているデータ量が大変多いためにS3ストレージの利用コストが高いことが問題となっており、あなたはコスト削減を実施するようにボスより依頼されました。ライフサイクルルールを新規に設定して、時間の経過とともにオブジェクトをより安いストレージクラスへと移行する設定が必要です。しかしながら、いくつかのライフサイクルルールは設定することができませんでした。

次の中で、設定することができないライフサイクルルールはどれでしょうか？（2つ選択してください）

- 1) S3 Standard ⇒ S3 Intelligent-Tiering
- 2) S3 Standard-IA ⇒ S3 Intelligent-Tiering
- 3) S3 Standard-IA ⇒ S3 One Zone-IA
- 4) S3 Intelligent-Tiering ⇒ S3 Standard
- 5) S3 One Zone-IA ⇒ S3 Standard-IA
- 6) S3 Glacier ⇒ S3 Standard-IA

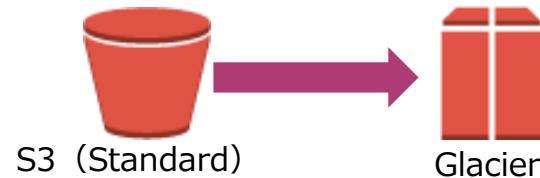
ライフサイクル管理

時間に応じてオブジェクトのストレージクラスの変更や削除を自動的に行うルールを設定できる。

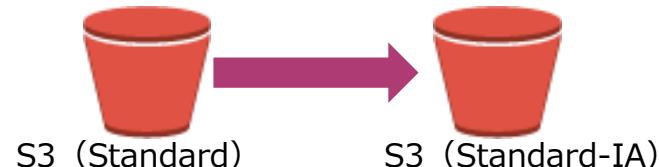
設定方法

- 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

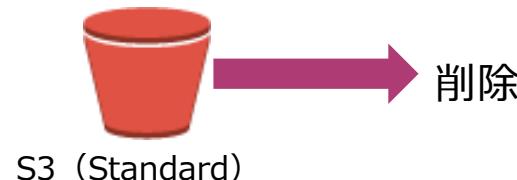
一定期間で自動アーカイブ



一定期間で自動で安価な保存場所へ

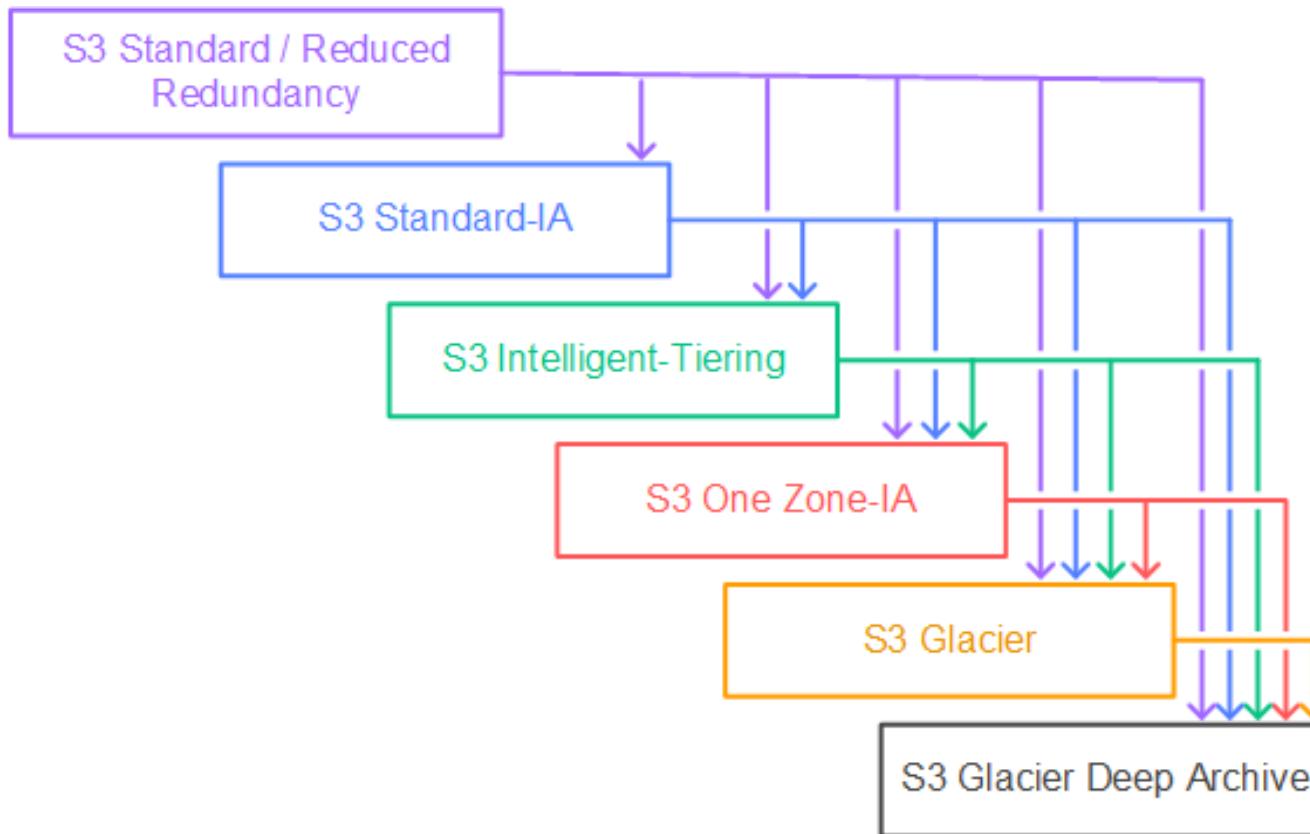


一定期間で自動で削除



ライフサイクル管理

ライフサイクルポリシーを設定可能なパスは以下の通り



Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

[Q]バージョン管理

シリコンバレーのベンチャー企業はAmazonS3を利用してデータを従業員間で共有しています。これらのデータが誤って削除したりしないように、オブジェクトを保護する設定が必要です。

ソリューションアーキテクトとして、要件を満たすことができる対応を選択してください。（2つ選択してください）

- 1) バケットでバージョン管理を有効にする。
- 2) S3オブジェクトを削除したときにイベントトリガーを作成して、SNSによる通知を設定する。
- 3) バケットでライフサイクルルールを有効にする。
- 4) MFA削除を有効にする。
- 5) バケットの設定でデータ削除不可を有効にする。

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

- バケット全体をバージョン管理する
- バージョンごとにオブジェクトが保管される。
- ライフサイクル管理によりバージョンが保存される期間を設定
- オブジェクトとは別に古いバージョン削除を実施する必要がある。

【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

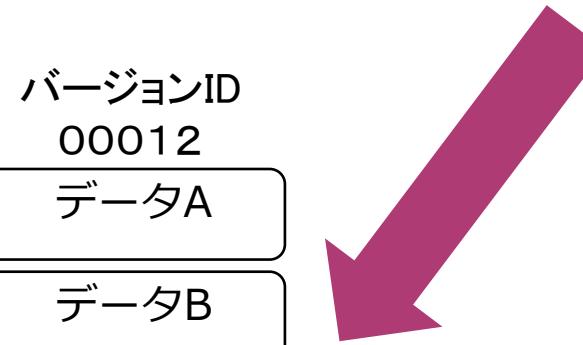
データC

バージョンID
00012

データA

データB

データC



S3 MFA Delete

バージョニング機能のオプションとして、オブジェクト削除時にMFA認証を必須にできる。

The screenshot shows the AWS IAM 'Your Security Credentials' page. The left sidebar lists navigation options: Dashboard, Search IAM, Details, Groups, Users, Roles, Policies, and Identity Providers. The main content area is titled 'Your Security Credentials' and contains instructions for managing credentials. It mentions using this page for AWS accounts and the IAM Console for IAM users. It also links to the AWS General Reference for more information on AWS credentials. A list of credential types is shown, with 'Multi-Factor Authentication (MFA)' being expanded. Below this, a note explains that AWS MFA increases security by requiring both a user name and password plus an authentication code from an AWS MFA device. A blue 'Activate MFA' button is visible at the bottom of this section.

AWS Services Edit Laurence Gellert Global Support

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Activate MFA

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

+ Password

- Multi-Factor Authentication (MFA)

You use AWS MFA to increase the security of your AWS environments when you sign in AWS websites. When AWS MFA is enabled, you must provide not only a user name and password but also an authentication code from an AWS MFA device.

[Q] S3のアクセス管理

あなたはソリューションアーキテクトとして、AWS上でドキュメント共有アプリケーションを構築しています。このアプリケーションは、AmazonS3バケットに保存されたデータを読み込むプロセスをEC2インスタンス上で実行しています。これらのデータは、このWEBアプリケーションを介してのみ特定のユーザーにのみ閲覧できるように制限することが必要です。

WEBアプリケーションからのみデータにアクセスするための設定はどれでしょうか？

- 1) バケットポリシーにより、Webアプリケーション上のURLからの参照のみを許可する設定を行う。
- 2) IAMロールにより、WebアプリケーションのみがS3バケットへのアクセスを許可する設定を行う。
- 3) ACLにより、WebアプリケーションのみがS3バケットへのアクセスを許可する設定を行う。
- 4) 署名付きURLにより、Webアプリケーション上のURLからの参照のみを許可する設定を行う。

[Q] S3のアクセス管理

あなたはAWSでデータ解析システムを構築しています。このシステムはIoTセンサーからデータを取得してKinesis Data Streamsがストリーミング処理したデータをKinesis Data Firehoseを介してAmazonS3バケットに保存します。その後、S3バケット内のデータに対してSQLクエリを使用して暗号化されたデータを簡易にクエリ処理して、結果をS3バケットに書き戻す必要があります。データは機密性が高いため、S3バケットへのアクセスに対してきめ細かい制御を実装する必要があります。

これらの要件を満たすことができるソリューションの組合せを選択してください。
(2つ選択してください)

- 1) Athenaによりデータをクエリ処理して、結果をバケットに保存する。
- 2) Redshiftによりデータをクエリ処理して、結果をバケットに保存する。
- 3) バケットACLを使用して、バケットへのアクセスを制限する。
- 4) Amazon EMRによりデータをクエリ処理して、結果をバケットに保存する。
- 5) バケットポリシーを使用して、バケットへのアクセスを制限する。
- 6) IAMポリシーを使用して、バケットへのアクセスを制限する。

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 ユーザー policy	<ul style="list-style-type: none">✓ IAMユーザーに対してAWSリソースとしてのS3へのアクセス権限を設定✓ 内部のIAMユーザーやAWSリソースへの権限管理
バケットポリシー	<ul style="list-style-type: none">✓ バケットのアクセス権をJSONで設定✓ 外部のユーザーも含めたアクセス管理
ACL	<ul style="list-style-type: none">✓ バケット／オブジェクト単位でのアクセス権限をXMLで設定することができる✓ オブジェクトに個別に設定可能
事前署名付きURL	<ul style="list-style-type: none">✓ AWS SDKで生成した事前署名付きURLでS3オブジェクトURLにアクセスできる権利を一定期間付与する。✓ インターネット上の第三者にURLを閲覧させる。

[Q] S3バケットポリシー

次のバケットポリシーでS3バケットに対する権限設定を行っています。

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicReadForGetBucketObjects",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::mybucket/*"  
        }  
    ]  
}
```

この設定内容として正しい内容を選択してください。

- 1) このS3バケットの全てのアクションが許可されている。
- 2) このS3バケットを利用した静的ホスティングを有効化できる。
- 3) このS3バケットは該当バケットの所有者は削除以外の操作が全て実行できる。
- 4) このS3バケットはオブジェクトのアップロードが可能である。

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

ポリシーのバージョン。
必ず先頭に記載する。

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

Statementがポリシー内容を記述する部分

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

Sid (ステートメント ID) は、ユーザーが
ポリシーに与える任意の識別子

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": ["AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]],  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

許可するポリシーか、拒否するポリシーかを決める。

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

対象となるプリンシパル(IAMユーザー
やルートアカウントなど)を指定

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"],  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

Effectを適用するアクションを指定

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": "public-read"}}  
    }  
  ]  
}
```

ポリシーを適用する対象バケットを指定

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

S3バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {"AWS": ["arn:aws:iam::11122223333:root", "arn:aws:iam::444455556666:root"]},  
      "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",  
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}  
    }  
  ]  
}
```

ポリシーを適用する場合の条件を指定

Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html

[Q]事前署名付きURL

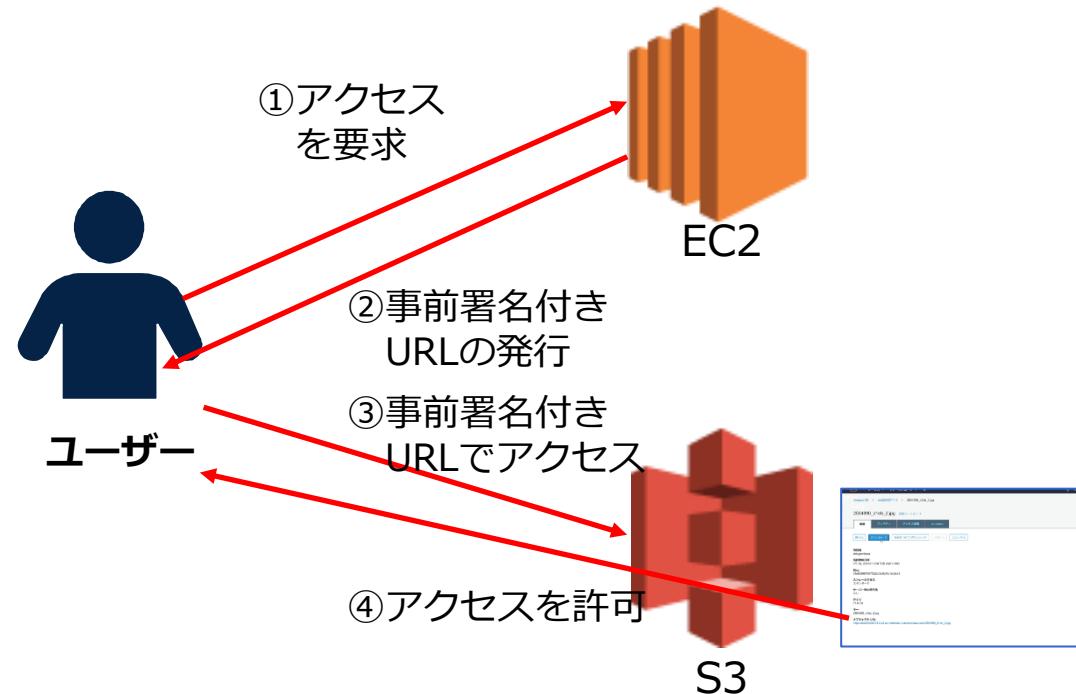
あなたはソリューションアーキテクトとして、動画共有アプリケーションを構築しています。このアプリケーションでは、S3バケットにビデオファイルを大量に保存して、EC2インスタンスを介してユーザーに一時的に共有されます。その際に、許可されたユーザーのみが動画データにアクセスできるようにする必要があります。

このアクセスを有効にするためのS3の設定を選択してください。

- 1) S3バケットのブロックパブリックアクセスを無効にして、URLが閲覧できるようになる。
- 2) CloudFrontを使用して、キャッシュに基づいて画像を配布する。
- 3) ACLを利用して、動画が共有されるユーザーに対するアクセスを許可する。
- 4) 事前署名URLを生成し、動画が共有されるユーザーに配布する。

事前署名付きURL

事前署名付きURLにより、特定のユーザーのみがアクセスできる特別なURLが利用可能になる。



[Q]パブリックアクセス

あなたはメディア会社のソリューションアーキテクトです。現在、WEBメディアをAWS上で運用しており、このWEBメディアの静的コンテンツを提供するためにAmazonS3バケットを設定する必要があります。

S3バケットにアップロードされたすべてのオブジェクトをインターネットに公開するための設定はどれでしょうか？（2つ選択してください。）

- 1) ブロックパブリックアクセスを無効化する。
- 2) パブリックアクセス設定を有効化する。
- 3) バケットポリシーでインターネットからのアクセスを許可する。
- 4) ACLでインターネットからのアクセスを許可する。
- 5) IAMでインターネットからのアクセスを許可する。

ブロックパブリックアクセス

インターネットからのアクセスをブロックする機能で、バケット作成時に初期設定で有効化されている。

The screenshot shows the AWS S3 Bucket Properties interface. The top navigation bar has tabs: 概要 (Overview), プロパティ (Properties), アクセス権限 (Access Permissions), and 管理 (Management). The Management tab is selected. Below it, there are four sub-tabs: ブロックパブリックアクセス (selected), アクセスコントロールリスト (Access Control List), バケットポリシー (Bucket Policy), and CORS の設定 (CORS Settings). The main content area is titled "ブロックパブリックアクセス (バケット設定)" (Block Public Access (Bucket Settings)). It contains a section titled "パブリックアクセスをすべてブロック" (Block all public access) with the status "オフ" (Off). There are four options listed under this section:

- 新しいアクセスコントロールリスト (ACL) を介して許可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) を介して許可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
- 新しいパブリックバケットポリシーを介して許可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
オン
- 任意のパブリックバケットポリシーを介して、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
オン

A blue "編集" (Edit) button is located in the top right corner of the settings panel.

[Q]クロスアカウントアクセス

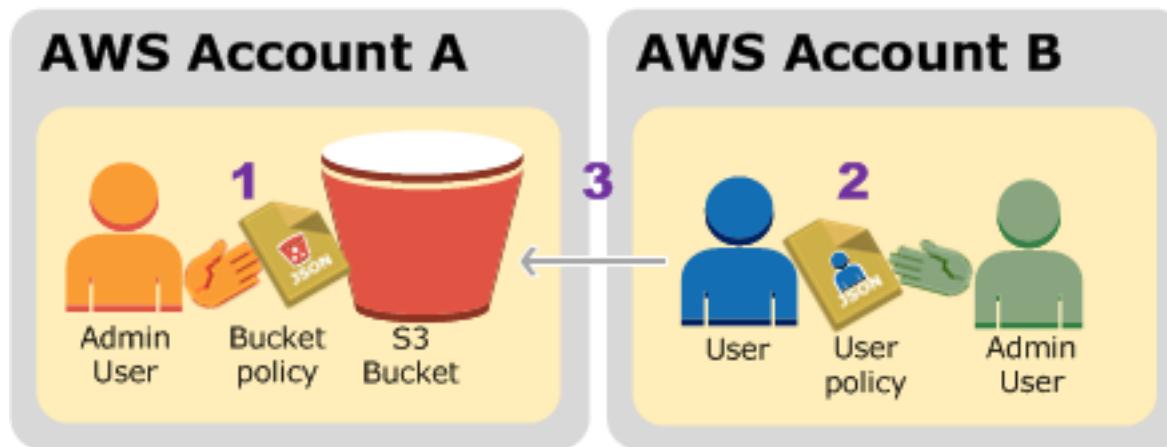
大手製造企業は5000人の従業員を有する大企業です。複数の部門がAWSアカウントを使用しているため、多数のAWSアカウントを管理することが必要です。Aアカウントが所有するS3バケット内のオブジェクトを、Bアカウントに属する別のS3バケットにコピーする要件が発生しました。あなたはソリューションアーキテクトとして、コピーされたオブジェクトを送信先アカウントが所有する設定を行っています。

この要件を満たすための設定方法を選択してください。

- 1) AアカウントのS3バケットでリクエスタ支払機能を有効にして、Bアカウントへのコピーを実施する。
- 2) AアカウントのオブジェクトをBアカウントにコピーできるようにするIAMカスタマーマネジメントポリシーを作成して、S3でクロスオリジンリソースシェアリングを設定する。
- 3) Aアカウントのバケットから、Bアカウントのバケットへとレプリケーションを設定して、S3でクロスオリジンリソースシェアリングを設定する。
- 4) AアカウントのオブジェクトをBアカウントにコピーできるようにするIAMカスタマーマネジメントポリシーを作成して、S3でクロスアカウントアクセスを許可して、IAMユーザーに設定する。

クロスアカウントアクセス

アカウントAの所有するバケットに対して、アカウントBへのアクセス許可を与えることが可能



Reference: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-walkthroughs-managing-access-example2.html

クロスアカウントアクセス

クロスアカウントアクセスを許可する設定は3つの方式がある

設定方式	詳細
バケットポリシーと IAMポリシーによる 許可	<ul style="list-style-type: none">✓ S3バケットにアクセスを許可するIAMポリシーを設定する。✓ S3バケットへのクロスアカウントアクセスを許可する場合はバケットポリシーでアカウントを指定して許可を行う。✓ IAMユーザーとロールに設定
ACLとIAMポリシー による許可	<ul style="list-style-type: none">✓ S3バケットにオブジェクトへの操作を許可するIAMポリシーを設定する。✓ S3バケットの特定オブジェクトへのクロスアカウントアクセスを許可する場合はACLでアカウントを指定して許可を設定✓ AWSアカウントに設定
IAMロールによる 許可	<ul style="list-style-type: none">✓ AssumeRoleを利用してS3バケットオブジェクトへのプログラムによるアクセスまたはコンソールアクセス用のクロスアカウントの IAM ロールを設定する。✓ ユーザAからAssumeRoleの実行を許可したロールBに対して権限を付与する

[Q] S3アクセスポイント

ある会社ではAWS上にドキュメント管理システムを構築しているところです。このストレージはグローバルに複数部門や複数のアプリケーションが利用するため、様々なアクセス制御ルールを設定することが必要です。したがって、あなたはソリューションアーキテクトとして、S3 の共有データセットへの大規模なデータアクセス管理を簡素化する設定を検討しています。

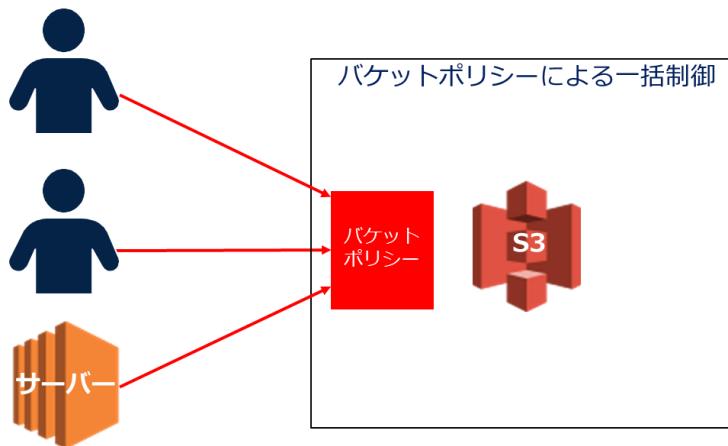
この要件を満たすことができるアクセス設定を選択してください。

- 1) Amazon S3 Transfer Accelerationを利用する。
- 2) S3 アクセスポイントを利用する。
- 3) VPC エンドポイントを利用する。
- 4) マルチパートアップロードを有効化する。

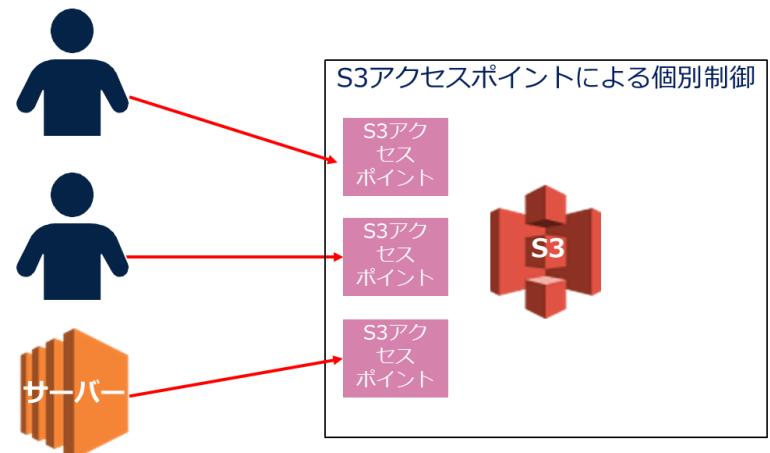
S3アクセスポイント

アクセス先に応じてアクセスポイントを作成して、ポリシーを適用してアクセス設定が可能になる。

バケットポリシーでアクセスを管理



アクセスポイントポリシーでアクセスを管理



静的WEBホスティング

あなたは会社のコーポレイトサイトをAWS上に構築しています。このサイトはシンプルな静的WEBサイトであり、なるべくコスト抑えるためにAmazonS3にデプロイしました。

出来上がったサイトのAmazon S3 Webサイトエンドポイントとして正しいものを選択してください。（2つ選択してください）

- 1) <http://bucket-name.s3-website.Region.amazonaws.com>
- 2) <http://s3-website-Region.bucket-name.amazonaws.com>
- 3) <http://bucket-name.s3-website-Region.amazonaws.com>
- 4) <http://s3-website.Region.bucket-name.amazonaws.com>
- 5) <http://bucket-name.Region.s3-website.amazonaws.com>

静的WEBホスティング

静的サイトを構築する場合は、静的WEBホスティングによる安価なWEBページを構築可能

静的WEBホスティング メリット

- サーバーなしにWEBサイトをホスティング可能。
- サーバーが必要ないため値段が安い。
- マルチAZの冗長化を勝手にしてくれており、運用いらず
- Route53で独自ドメインを設定可能
- CloudFrontによる配信可能

静的WEBホスティング デメリット

- サーバーサイドスクリプト言語を実行するなどの動的サイト不可
- 単独ではSSLが利用できず、SSL設定にはCloudFrontが必要

WEBサイト エンドポイント

使用しているリージョンに応じて、Amazon S3 ウェブサイトエンドポイントは以下の 2 つの形式のいずれかになる。

- ✓ <http://bucket-name.s3-website-Region.amazonaws.com>
- ✓ <http://bucket-name.s3-website.Region.amazonaws.com>

静的WEBホスティング

静的サイトを構築する場合は、静的WEBホスティングによる安価なWEBページを構築可能

ロックパブリックアクセスを無効化する。

バケットポリシーでバケットの読み取り許可を設定する。

Index.htmlなどのインデックスドキュメントをバケット内に保存する。

静的WEBホスティングの設定画面で
Index.htmlなどのインデックスドキュメントを
設定し、有効化する。

[Q] Route53によるドメイン設定

あなたは会社のコーポレイトサイトをAWS上に構築しています。このサイトはシンプルな静的WEBサイトであり、なるべくコスト抑えるためにAmazonS3にデプロイしました。あなたは更に、Route 53を使用して新しいドメイン名をこのWEBサイトに設定したいと考えています。

Route53を使用してS3静的Webサイトにトラフィックをルーティングする設定を選択してください。（2つ選択してください。）

- 1) バケットとドメインと同じ名前に設定する。
- 2) CNAMEレコードを利用してドメインを設定する。
- 3) エイリアスレコード（Aレコード相当）を利用してドメインを設定する。
- 4) エイリアスレコード（AAAAレコード相当）を利用してドメインを設定する。
- 5) オブジェクトとドメインと同じ名前に設定する。

Route53によるドメイン設定

S3の静的WEBホスティングのサイトにドメインを設定できる。

- トライフィック先としてS3 Webサイトエンドポイントへのエイリアス[Region(地域)]を選択します。
- レコードタイプとしてエイリアスレコードのA レコード（IPv4）タイプを利用してドメインを設定する。
- ターゲットの正常性の評価にはデフォルト値を設定する。
- バケット名とドメイン名またはサブドメイン名と同じにすることが必要

[Q] クロスオリジンリソースシェアリング(CORS)

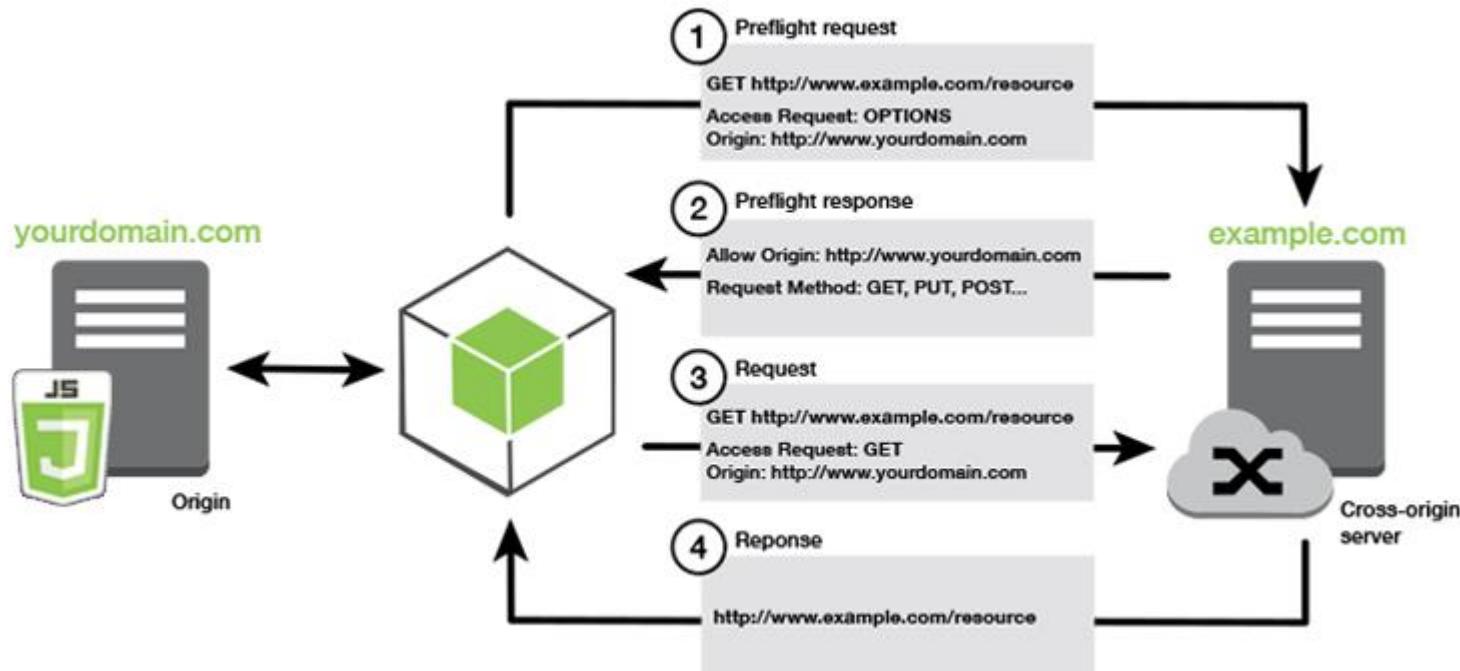
あなたの会社ではS3を利用したドキュメント管理システムを構築しています。このシステムはドメインを利用してユーザーからアクセスされていますが、ファイルを他のドメインから連携して、利用する機能が必要です。

この要件を満たすためのソリューションを選択してください。

- 1) レプリケーション
- 2) クロスアカウントアクセス
- 3) クロスオリジンリソースシェアリング (CORS)
- 4) S3アクセスポイント

クロスオリジンリソースシェアリング(CORS)

1つのWEBサイトを複数のドメインで共有して利用できる。



Reference: https://docs.aws.amazon.com/ja_jp/sdk-for-javascript/v2/developer-guide/cors.html

[Q] S3イベント

あなたは写真共有アプリケーションをAWS上に構築しています。写真はS3バケットに保存され、画像処理を複数のEC2インスタンスにホストされたアプリケーションが実行します。ソリューションアーキテクトは、アップロードされたデータに応じて、EC2インスタンスのうちの1つで画像処理を実行する仕組みを構成しています。

要件を満たすために、どのようにS3と他のAWSサービスを構成するべきでしょうか？

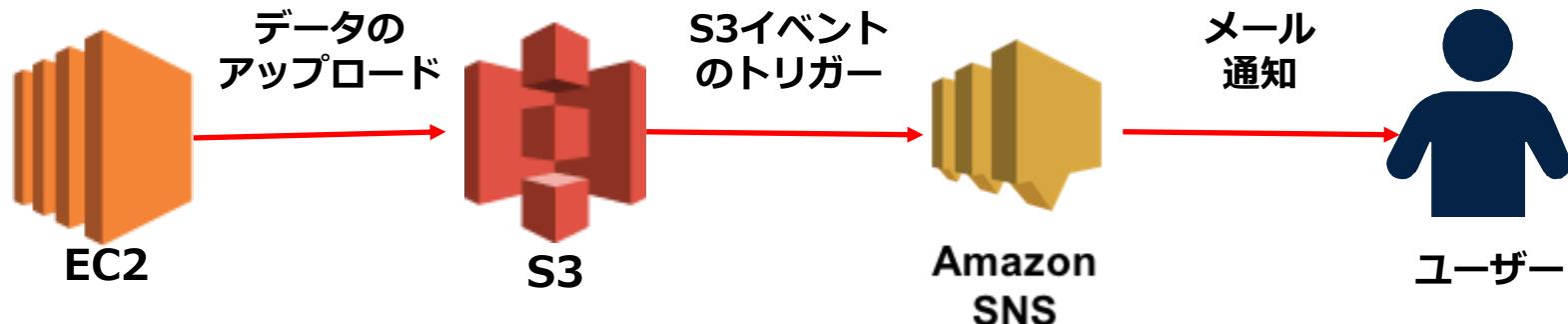
- 1) データアップロードをトリガーとするS3イベント通知を作成して、SQSを起動する。SQSキューからの処理メッセージをEC2インスタンスがポーリングして、画像処理を並行処理する。
- 2) データアップロードをトリガーとするS3イベント通知を作成して、SNSを起動する。SNSメッセージをトリガーにしてEC2インスタンスが画像処理を並行処理する。
- 3) データアップロードをトリガーとするS3イベント通知を作成して、Lambda関数を起動する。Lambda関数をトリガーにしてEC2インスタンスが画像処理を並行処理する。
- 4) データアップロードをトリガーとするS3イベント通知を作成して、SWFを起動する。SWFをトリガーにしてEC2インスタンスが画像処理を並行処理する。

S3イベント

S3オブジェクト操作と連動したシステム連携処理を実現

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
- S3オブジェクト操作と連動したシームレスなシステム連携処理を実現
 - S3へのデータアップロードをSNSでメッセージ通知
 - S3オブジェクトのアップロードをトリガーにLambda関数を実行



[Q] S3の暗号化

法律事務所のA社ではドキュメント管理システムをAmazon S3を利用して構築しているところです。保存される文書は法律業務に関わる非常に機密性が高いものが多く、暗号化が必須となっています。この会社では会社独自のアルゴリズムを使用して暗号化することがセキュリティーポリシーで決められています。そこで、あなたはソリューションアーキテクトとして、利用するべき暗号化方式を検討しています。

次の中で、どの暗号方式を利用するべきでしょうか？

- 1) CSE
- 2) SSE-KMS
- 3) SSE-S3
- 4) SSE-C

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



[Q]レプリケーション

あなたの会社は複数リージョンを利用してAWSリソースを利用しています。現在シンガポールリージョンにAmazonS3バケットを設置し、大量のデータを保存していますが、このデータをシドニーリージョンにレプリケーションして、データのバックアップを実施したいと考えています。

次の中で、レプリケーションの正しい構成方法はどれでしょうか？（2つ選択してください。）

- 1) 両方のリージョンのバケットでバージョン管理を有効化する。
- 2) シンガポールリージョンにレプリケーション対象の新しいバケットを作成する。
- 3) シンガポールリージョンのバケットからのクロスオリジンリソースシェアリングを構成する。
- 4) シドニーリージョンに新たにS3バケットを作成し、クロスオリジンリソースシェアリングを構成する。
- 5) シドニーリージョンに新たにS3バケットを作成し、リージョン間のレプリケーションを構成する

クロスリージョンレプリケーション

S3は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

- ✓ バケットにおけるオブジェクトの作成・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

- ✓ 事前にバージョニング機能を有効にする必要がある。
- ✓ レプリケーション先となるバケットは別リージョンに設置
- ✓ 双方向レプリケーションも可能
- ✓ データ転送費用が発生

[Q] S3データの解析

B社ではAmazonS3を利用したデータレイクを構成し、ビッグデータ解析を実行しています。あなたはソリューションアーキテクトとして、データレイク内のデータアセットに直接にクエリを実行して、ビッグデータ解析を実行するソリューションを整備したいと考えています。

この対応で使用するべきサービスを選択してください。

- 1) Redshift Spectrumによる複雑なクエリによる解析
- 2) Amazon Athenaによる複雑なクエリによる解析
- 3) S3 Selectによる複雑なクエリによる解析
- 4) Amazon EMRによる複雑なクエリによる解析

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



S3 Select

SQLクエリを実行してS3バケット内のファイルを抽出・操作することができる。

```
Python
import boto3

s3 = boto3.client('s3')

resp = s3.select_object_content(
    Bucket='s3select-demo',
    Key='sample_data.csv',
    ExpressionType='SQL',
    Expression="SELECT * FROM s3object s where s.\"Name\" = 'Jane'",
    InputSerialization = {'CSV': {"FileHeaderInfo": "Use"}, 'CompressionType': 'NONE'},
    OutputSerialization = {'CSV': {}},
)

for event in resp['Payload']:
    if 'Records' in event:
        records = event['Records'][ 'Payload'].decode('utf-8')
        print(records)
    elif 'Stats' in event:
        statsDetails = event['Stats'][ 'Details']
        print("Stats details bytesScanned: ")
        print(statsDetails[ 'BytesScanned'])
        print("Stats details bytesProcessed: ")
        print(statsDetails[ 'BytesProcessed'])
        print("Stats details bytesReturned: ")
        print(statsDetails[ 'BytesReturned'])
```

```
Bash
python jane.py
```

以下の出力が得られます。

```
Jane,(949) 555-6704,Chicago,Developer

Stats details bytesScanned:
326
Stats details bytesProcessed:
326
Stats details BytesReturned:
38
```

【参照】<https://aws.amazon.com/jp/blogs/news/querying-data-without-servers-or-databases-using-amazon-s3-select/>

[Q] EMRとの連携

B社ではAmazonS3を利用したデータレイクを構成し、ビッグデータ解析を実行しています。S3に保存されたWEBアプリケーションのアクセスログをApache Sparkを使用してデータ処理する必要があります。

この要件を満たすために利用するべきサービスの構成を選択してください。

- 1) EC2にApache Sparkをインストールして、S3内のデータを解析する。
- 2) RedShift Spectrum使用してログファイルを処理する。
- 3) Kinesis Data Analyticsを使用してログファイルを処理する。
- 4) Amazon EMRを使用してログファイルを処理する。

S3データの解析

S3にビッグデータを蓄積して、EMRでビックデータ解析を実施



行動履歴データやログ
ファイルゲノムデータ
などを蓄積

Apacheによるビッグ
データ解析を実施

解析結果をS3に保存

[Q]利用状況の確認

あなたはソリューションアーキテクトとして、S3バケットを利用したドキュメント管理アプリケーションを構築しています。現在、ドキュメントデータを用いてレポートを生成する機能を追加開発しており、S3バケットへのすべてのリクエストアクセスとバケットのオブジェクトレベルの操作を詳細に把握できるようにする必要があります。

要件を満たすことができる最適な方法はどれでしょうか？

- 1) Amazon S3バケットにCloudWatchログを設定する。
- 2) Amazon S3バケットにS3アクセスアナライザーを有効にする。
- 3) Amazon S3バケットのサーバーアクセスログを有効にする。
- 4) Amazon S3バケットにCloudTrailを設定する。

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

サーバーアクセスログ

S3にアクセスした際のログを取得することが可能。バケットと
プレフィックスをターゲットに設定する。

[アップロード](#) [フォルダの作成](#)[ダウンロード](#)[アクション ▾](#)

<input type="checkbox"/>	名前 ▾	最終更新日時 ▾
<input type="checkbox"/>	2019-05-10-17-55-948B7CEB7E063A7D	5月 10, 2019 7:17:5 GMT+0900
<input type="checkbox"/>	2019-05-10-18-11-DDD3C1EB69550551	5月 10, 2019 7:18:1 GMT+0900
<input type="checkbox"/>	2019-05-10-19-46-5B472ED82D8B552A	5月 10, 2019 7:19:4 GMT+0900
<input type="checkbox"/>	2019-05-10-20-00-1F137BA23771B806	5月 10, 2019 7:20:0 GMT+0900

S3アクセスアナライザー

S3のアクセス状況がアクセスポリシーに沿っているか確認し、不正なアクセスの有無を監視する

- ✓ IAM アクセスアナライザーと連動したS3向けの機能
- ✓ バケットポリシー／ACLに沿ってポリシー違反がないかをモニタリング
- ✓ パブリックバケットまたは共有バケットアクセスを解析して、その解析結果を表示する
- ✓ バケットアクセスのソースを検証する場合は、列の情報を使用して、迅速で正確な措置を実行する
- ✓ バケットの実際のアクセス状況を確認する。



[Q] S3の読み取り整合性モデル

あなたの会社はWEBアプリケーションをAWS上で運用しています。このアプリケーションではログファイルをAmazonS3に保存しています。このログファイルは広告表示のリアルタイム処理で利用されているため、頻繁に読み取り処理が発生していますが、ログファイルに変更が発生した際に、古いログファイルが読み取られてしまうようです。

この問題の最も可能性がある原因はどれでしょうか？

- 1) S3バケットでは既存のオブジェクトを置換し、すぐにそのオブジェクトの読み取りを試みると変更が完全に反映されるまで古いデータを返すことがある。
- 2) S3バケットでは既存のオブジェクトを置換し、すぐにそのオブジェクトの読み取りを試みると読み取工ラーが発生することがある。
- 3) S3バケットは強い整合性モデルを利用しているため、更新中のオブジェクトデータを読み取ることができないため、古いデータが表示されてしまう。
- 4) S3バケットはオブジェクトの共有を設定しないと、更新中のオブジェクトデータを読み取ることができないため、古いデータが表示されてしまう。

S3の整合性モデル

S3はデータ登録・更新・削除などの処理時に強い整合性モデルを採用している。

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">✓ 2020年12月より強い整合性モデルに変更された。そのため、齟齬は発生しない。
削除	<ul style="list-style-type: none">✓ 2020年12月より強い整合性モデルに変更された。そのため、齟齬は発生しない。

[Q]アップロード時のデータ整合性確認

AIベンチャー企業はAIベースの顔認識アプリケーションを構築しています。顔認証を実現するためにS3バケットに数百万の画像を保存して、これを利用した顔認識の学習を行います。新規に顔認証対象ユーザーを登録するには、S3バケットに対象ユーザーの顔写真を追加することが必要です。その際にアップロードされた画像が変更されることなく、整合性を保ったまま保存されていることが重要です。

オブジェクトが正常に保存されたことを示すために、何を実施すれば良いでしょうか？

- 1) S3バケットの整合性チェックを有効化する。
- 2) S3 API呼び出しで、HTTP200結果コードとMD5チェックサムを取得する。
- 3) S3イベントを設定して、アップロード後にAmazon SNSによるメッセージ通知を実施する。
- 4) S3のプレフィックスにおいてハッシュ値を設定して、整合性を確認する。

アップロード時のデータ整合性確認

Content-MD5 ヘッダーを使用してアップロードされたオブジェクトの整合性を確認することができる。

1. オブジェクトの base64 でエンコードされた MD5 チェックサム値を取得します。
2. アップロード中のオブジェクトの整合性を確認します。

ただし、アップロードが AWS 署名バージョン 4 で署名されている場合、代わりに x-amz-content-sha256 ヘッダーを使用する必要があります。

[Q] アップロードの高速化

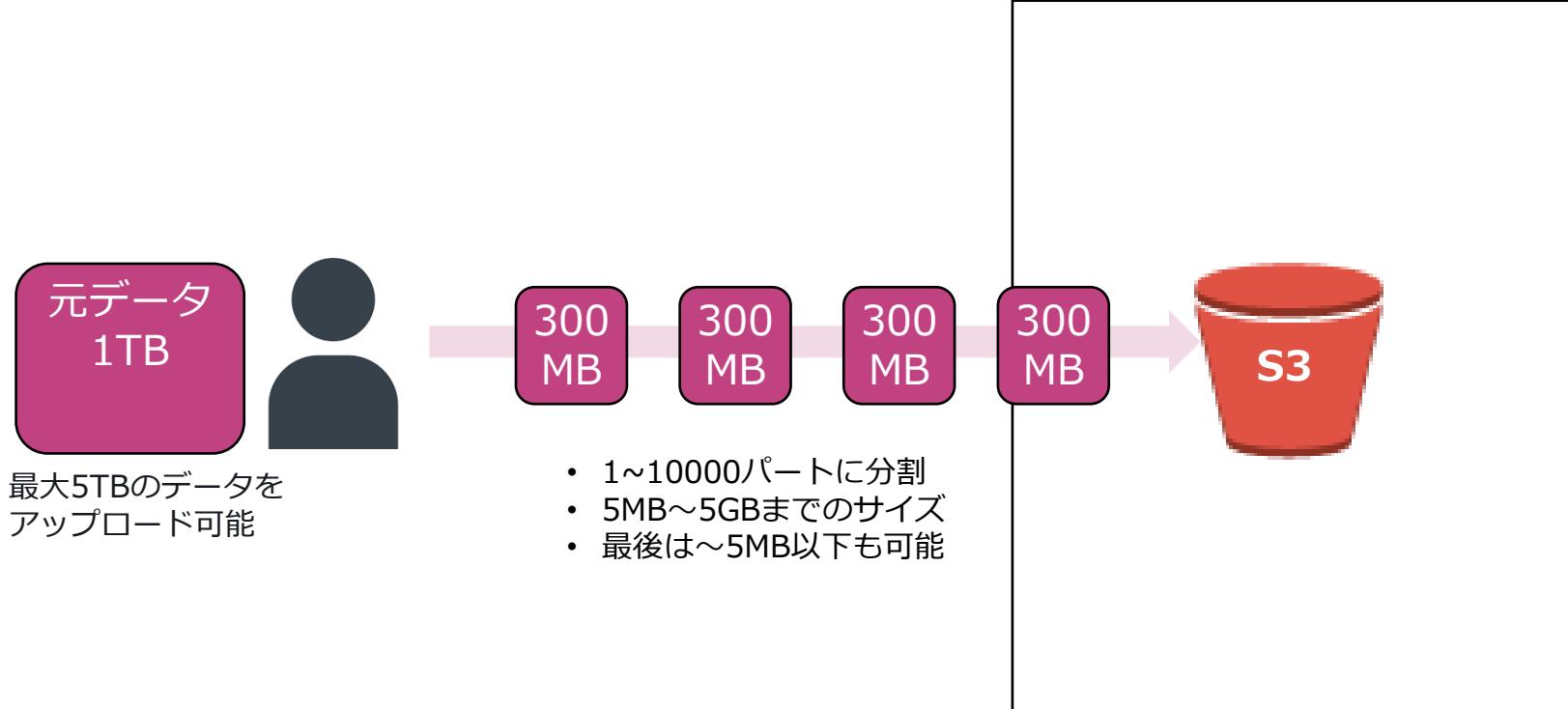
あなたはソリューションアーキテクトとして、AWS上で動画共有アプリケーションを構築しています。このアプリケーションはAmazon S3バケットに保存されたビデオデータを利用する動画処理アプリケーションをEC2インスタンスにホストする構成をとっています。利用ユーザーはグローバルに存在しており、大容量なデータがアップロードされます。そのために、大きなビデオファイルを宛先のS3バケットにアップロードするのが大幅に遅れており、クレームが発生しています。

S3へのファイルのアップロード速度を向上させる方法を選択してください。（2つ選択してください。）

- 1) Amazon S3 Transfer Accelerationを使用して、宛先S3バケットへのファイルのアップロードを高速化する。
- 2) Direct Connectを利用してS3へのファイルのアップロードを高速化する。
- 3) AWS Global Acceleratorを使用して、宛先S3バケットへのファイルのアップロードを高速化する。
- 4) AWS Transit Gatewayを使用して、宛先S3バケットへのファイルのアップロードを高速化する
- 5) マルチパートアップロードを利用してアップロードを高速化する。

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



S3 Transfer Acceleration

地理的に一番近いエッジロケーションを利用して高速にデータアップロードを実施する。



[Q]パフォーマンスの向上

リクエストは数百から2000程度まで同時に実行される可能性があり、パフォーマンスを効率化する処理が必要です。

ソリューションアーキテクトとして、最適なパフォーマンス向上策を選択してください。（2つ選択してください）

- 1) 単一のバケット内に固有のカスタムプレフィックスを作成し、それらのプレフィックス付きの日次ファイルをアップロードする。
- 2) 単一のバケット内でTransfer Accelerationを有効化した上で、ファイルをアップロードする。
- 3) S3のマルチパートアップロードを有効化して、アップロード処理を実行する。
- 4) 単一のバケット内にハッシュを利用したランダムなカスタムプレフィックスを作成したファイルをアップロードする。

パフォーマンスの向上

並列リクエストとカスタムプレフィックスでパフォーマンスを向上させる

並列リクエストの実行

- 並列リクエストを Amazon S3 サービスエンドポイントに水平にスケールすることでリクエストを分散し、ネットワーク経由で複数のパスに負荷を分散する
- 複数の接続で データを同時に GET または PUT するアプリケーションを使用することで高スループット転送が可能

カスタム プレフィックスの利用

- パフォーマンスを最適化するためにカスタムプレフィックスを設定して、日付ベースの順次命名を使用する。
- 1 秒あたり 3,500 回以上の PUT/COPY/POST/DELETE リクエストと 5,500 回の GET/HEAD リクエストを送信可能

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

- 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
【データ紐づけ】
- S3 : 8KBオブジェクト/メタデータ
- Glacier : 32KBオブジェクト/メタデータ

リストア

- オブジェクト毎に復元が可能
- 一時的に指定日数間複製する
- 復元に要する時間を選択
- 復元期間はGlacierで課金

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

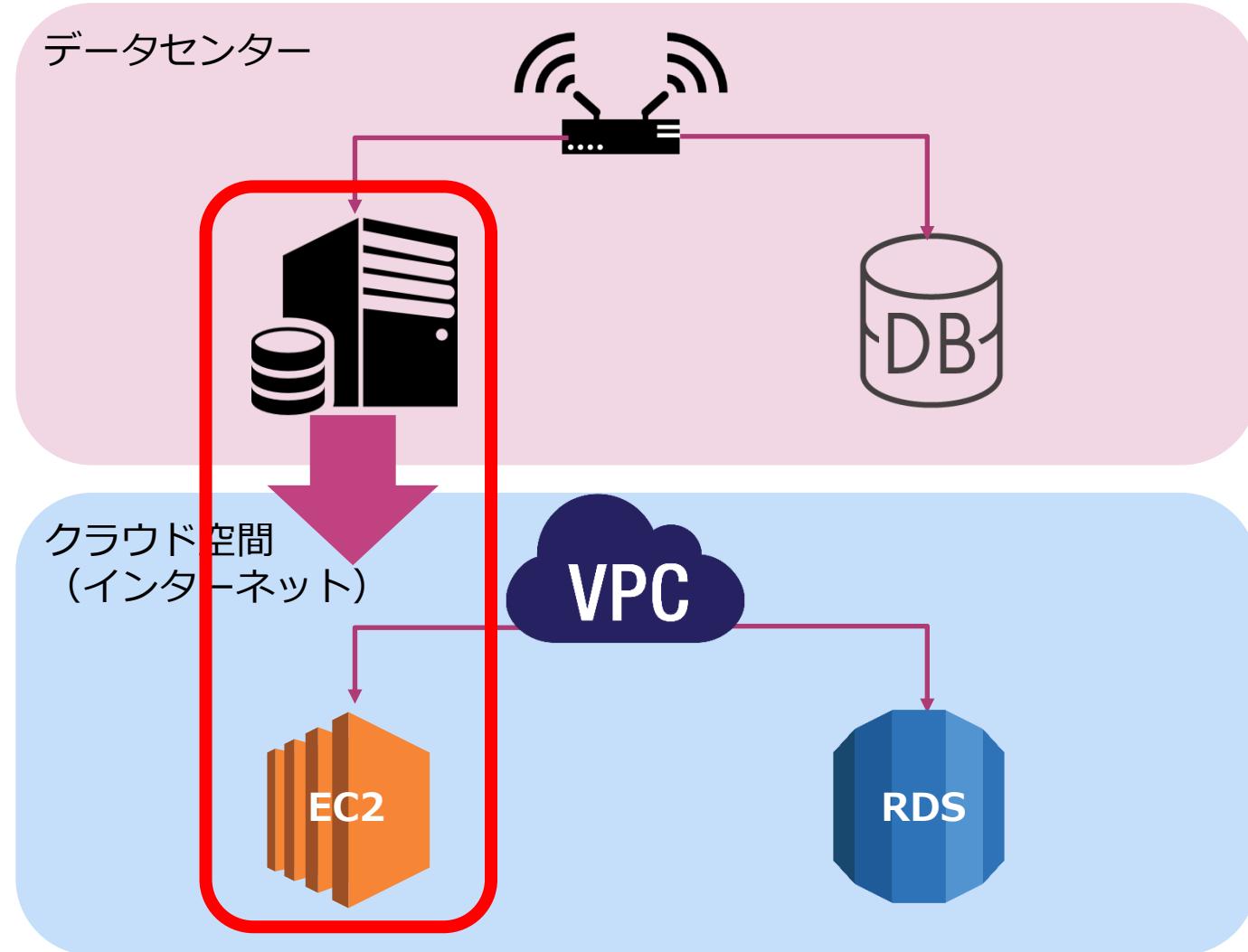
- ✓ マニフェストとは、Amazon S3 が作用するオブジェクトキーをリストする Amazon S3 オブジェクト
- ✓ マニフェストオブジェクトキー、ETag、およびオプションでバージョン ID を指定
- ✓ Amazon S3 インベントリレポート／CSVファイルの2つの形式で設定



EC2の出題範囲

EC2とは何か？

オンプレミス環境にあるサーバーと同じ性能を持ったサーバーをインターネット上で瞬時に作成することができるサービス



EC2の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

EC2の特徴	✓ EC2を利用するケースが問われるシンプルな質問が問われる。
EC2の利用コスト	✓ EC2の利用コストを削減するための対応が問われる
AMIの利用	✓ AMIを別リージョンで利用するための方法が問われる。 ✓ AMIを利用して最適なEC2インスタンスを効率的に起動する方法が問われる。
インスタンスタイプの選択	✓ シナリオで利用したいインスタンスの要件が提示され、最適なインスタンスタイプが問われる。
ユーザーデータの利用	✓ EC2インスタンスを起動時にスクリプトを利用した自動設定を実行する方法が問われる。

EC2の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

タグ設定	<ul style="list-style-type: none">✓ EC2インスタンスに追加の情報を付与する機能を選択する質問が出題される。
キーペアの利用	<ul style="list-style-type: none">✓ EC2インスタンスへのアクセスする認証方式が問われる。✓ キーペアを他のアカウントやリージョンで使用する方法が問われる。
インターネットアクセス	<ul style="list-style-type: none">✓ 起動したEC2インスタンスにインターネット経由でアクセスする際に必要な設定や方法が問われる。
インスタンスの購入形式	<ul style="list-style-type: none">✓ インスタンスのコスト効率が良い購入形式の選択が問われる。✓ シナリオに基づいて最適なインスタンスの選択が問われる。
リザーブドインスタンスの特徴	<ul style="list-style-type: none">✓ リザーブドインスタンスのタイプや特徴に基づいて、タイプを選択する質問が問われる。✓ リザーブドインスタンスの販売や属性変更に関する内容が問われる。

EC2の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

スポットインスタンス の特徴	✓ シナリオに基づいてスポットインスタンスの特徴を選択する質問が出題される。
スポットフリート の利用	✓ スpotトフリートを利用してスポットインスタンスを購入する構成方法が問われる。
スポットブロック の利用	✓ シナリオに基づいて要件を満たすために、スポットブロックを選択する質問が出題される。
EC2フリート	✓ シナリオに基づいて要件を満たすために、EC2フリートを選択する質問が出題される。
プレイスメントグループ の利用	✓ シナリオに基づいて要件を満たすために、クラスタープレイスマントグループを選択する質問が出題される。 ✓ プレイスマントグループのタイプを選択する必要が問われる。

EC2の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

拡張ネットワーキング	<ul style="list-style-type: none">✓ EC2インスタンスのネットワークを高パフォーマンスする設定方法が問われる。
Elastic Fabric Adapter の利用	<ul style="list-style-type: none">✓ HPCワークロードなどのユースケースを実現するために、Elastic Fabric Adapterを選択する質問が出題される。
Run Command	<ul style="list-style-type: none">✓ Windowsサーバーのコマンドをコンソール上から実行する方法として、Run Commandを選択する質問が出題される。
EC2の自動リカバリー	<ul style="list-style-type: none">✓ シナリオに基づいて要件を満たすために、EC2インスタンスがリカバリーした際のステータス状況に関する質問が出題される。✓ EC2のバックアップの方法が問われる。
インスタンスの停止と起動	<ul style="list-style-type: none">✓ インスタンス起動時のトラブルに関する質問が出題される。✓ インスタンスの停止・起動に関するインスタンスのステータス状況に関する質問が出題される。

EC2の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

ハイバネーション	✓ EC2インスタンスでハイバネーションを実行する際の目的が問われる。
メタデータの取得	✓ EC2インスタンスからメタデータを取得する方法が問われる。

[Q]EC2の特徴

ベンチャー企業はAWS上にWEBアプリケーションを有しています。このWEBアプリケーションはRDSをデータベースとして利用して、毎日午前7時にバッチジョブを実行しています。その際に、過去1日の業務オペレーションのログファイルを処理して、シェルスクリプトを介してバッチジョブで多数のレコードを順次実行することが必要です。この処理には1時間以上かかるため、バッチジョブの負荷は高いです。

このバッチジョブを実行するために、どのコンピューティングエンジンを利用するべきでしょうか？

- 1) AWS Lambda
- 2) Amazon EC2
- 3) Amazon EMR
- 4) Fargate

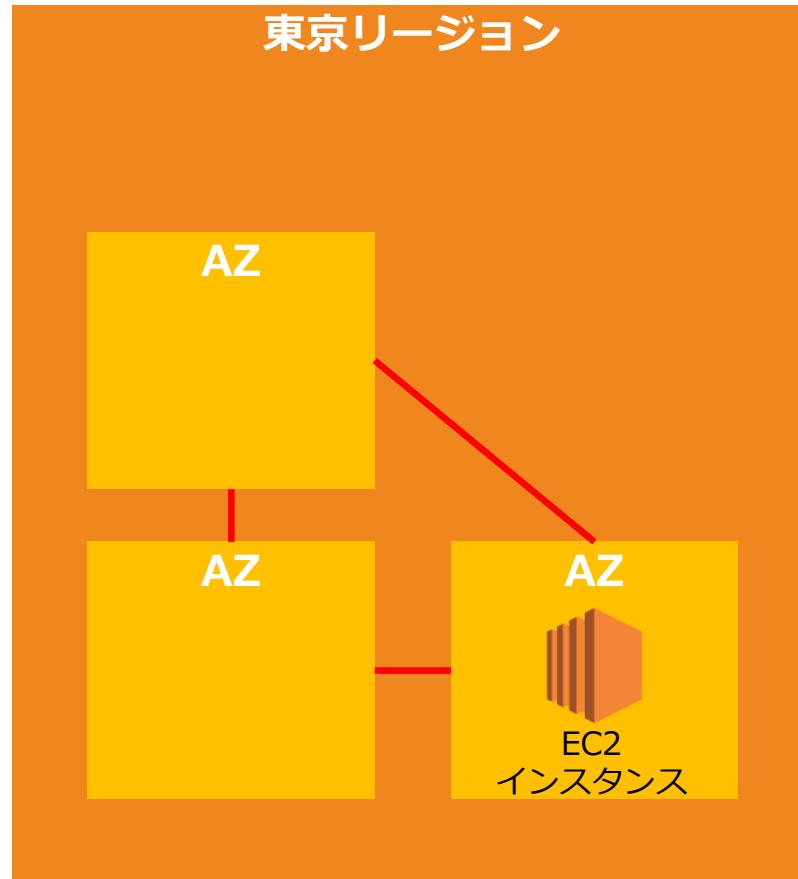
EC2の特徴

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の特徴

EC2の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



[Q] EC2の利用コスト

大手ECマース企業は多数のEC2インスタンスを利用してECサイトや業務処理などを実現しています。そのために、EC2インスタンスの利用コストが甚大となっており、あなたはソリューションアーキテクトとして、コスト最適化を実現するように依頼されました。あなたはEC2インスタンスの請求方式を確認して、最適な対応を検討することが必要です。

EC2のコスト発生に関する正しい説明は次のうちどれですか？（2つ選択してください。）

- 1) オンデマンドインスタンスが保留状態になってもコストが発生する。
- 2) スポットインスタンスが停止準備中にもコストが発生する。
- 3) オンデマンドインスタンスが休止中でもコストが発生する。
- 4) リザーブドインスタンスが終了状態となってもコストが発生する。
- 5) オンデマンドインスタンスが停止状態または休止状態になる準備をしている際はコストが発生する。

EC2の利用コスト

EC2の利用コストはインスタンスタイプや購入方式に応じて価格帯が決定する。

購入方式

購入形式に応じて様々な利用料金が設定されている。

- ✓ オンデマンド：通常価格
- ✓ リザーブド／Saving Plan：予約と事前支払の割引を適用
- ✓ スポットインスタンス：最大90%割引を適用

インスタンスタイプ に応じた料金設定

- ✓ インスタンスタイプに応じて価格が決定される。利用時間によって価格を決定する。
- ✓ a1.mediumは0.0255USD/時間

時間課金の設定

- ✓ 1時間単位または秒単位（最低 60 秒）で支払う
- ✓ Linux インスタンスの使用は 1 秒単位で課金
- ✓ その他のインスタンスは時間単位で課金

EC2の利用コスト

リージョンに応じて価格が異なり、利用時間に加えてデータ転送アウトにも課金される。

リージョン	<ul style="list-style-type: none">✓ リージョン：リージョン毎に価格が異なる。
データ転送	<ul style="list-style-type: none">✓ データ転送イン：無料✓ インターネットへのデータ転送アウト（GBあたり）✓ S3からAWS内のデータ転送アウト（GBあたり）
ボリューム	<ul style="list-style-type: none">✓ アタッチされたEBSでのデータ容量にも課金される。インスタンスを停止してもEBS分は課金が継続されるために注意が必要。✓ インスタンスストアには課金されない。

EC2の利用コスト

EC2インスタンスの状態に応じて課金発生が異なる。



EC2の利用コスト

EC2インスタンスを停止することで課金を抑えることが可能

Running／開始／再起動

- ✓ 実行時間に応じて料金が発生する。
- ✓ 利用中のEBSボリュームの料金が発生する。

停止／Stop

- ✓ EC2の料金発生は停止する。
- ✓ 利用中のEBSボリュームの料金が発生する。

終了／Terminate

- ✓ EC2の料金発生は停止する。
- ✓ デフォルト設定ではルートボリュームに設定されたEBSボリュームも削除され、料金発生は停止する。

EC2の起動方法

EC2の起動は以下のステップで実行します。

AMI (OSセッティング) を選択

インスタンスタイプを選択

インスタンスタイプの詳細の設定

ストレージを選択

タグの追加

セキュリティグループを選択

キーペアを設定

[Q]AMIの利用

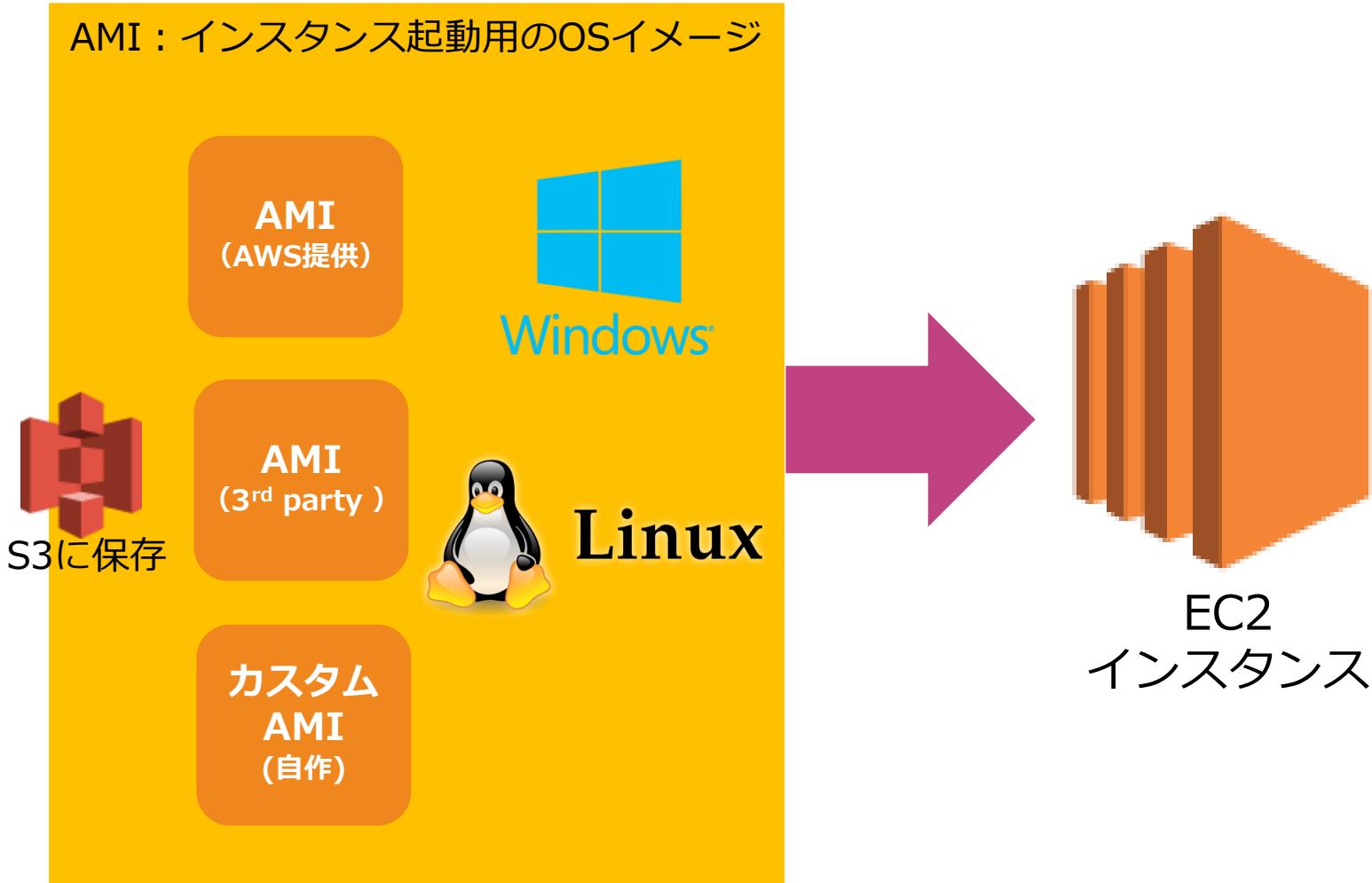
B社はAWSを子会社やグループ企業を含めて全社で標準的に利用することを決定しました。そのためには、標準的に利用するAMIを準備して異なるAWSアカウントでも利用できるようにする必要があります。あなたはソリューションアーキテクトとして、東京リージョンにあるAMIをシンガポールリージョンでも利用できるようにする設定を行っています。また、シンガポールリージョンのアカウントは別アカウントになっています。

この要件に対応するために利用できるAMIの機能は次のうちどれですか？（2つ選択してください）

- 1) AWSリージョン間でAMIをコピーできる。
- 2) AWSリージョン間でAMIを共有できる。
- 3) 暗号化されたスナップショットが利用されているAMIは利用できない。
- 4) AMIを別のAWSアカウントと共有することはできない。
- 5) AMIを別のAWSアカウントと共有することができる。

AMI (OSセッティング) を選択

AMIはOSセッティング方式を選択すること



AMI (OSセッティング) を選択

AMI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, 'Step 1: Set template parameters', is displayed. In the top navigation bar, the region is set to '東京 (Tokyo, JP)'. The main area shows a table of available Amazon Machine Images (AMIs). The table includes columns for AMI name, description, and bit size (64ビット). The first item listed is 'Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-92df37ed', which is selected, indicated by a blue '選択' (Select) button. Other items shown include 'Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD ポリュームタイム - ami-2724cf58' and 'Microsoft Windows Server 2012 R2 with SQL Server 2016 Web - ami-e4e3089b'.

AMIs	Description	Bit Size
Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-92df37ed	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
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 は、EC2 に合わせて調整された更新バージョンの Linux Kernel (4.14)、systemd のサポート、より新しいコンパイラ (gcc 7.3)、更新された C ランタイム (glibc 2.26)、より新しいツール (binutils 2.29.1)、および追加のメカニズムを通じた最新のソフトウェアパッケージを提供します。	64 ビット
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]	64 ビット

[Q] AMIの利用

あなたはAWSに大量のEC2インスタンスを起動するタスクを依頼されました。効率的にタスクを実行するためには、同じ構成と同じ状態となる新しいコンピューティングリソースを展開するプロセスを自動化することが求められています。

この要件を満たすために、どのアプローチが適切ですか？（2つ選択してください。）

- 1) ブートストラップの実行
- 2) AWSが提供するAMIの活用
- 3) AMIのコピーによる共有化
- 4) ゴールデンイメージの活用
- 5) 起動設定の利用

AMIの利用

EC2インスタンスはAMIを利用して起動・バックアップ・共有することができる。

OSの選択	<ul style="list-style-type: none">✓ 利用したいサーバーのOSの選択としてAMIを利用✓ 利用していたサーバーを復元する際にAMIを利用
EC2のバックアップ	<ul style="list-style-type: none">✓ 既存のEC2インスタンスからAMIを作成できる。✓ EC2インスタンスをバックアップとして構成内容を保存する。EBSボリュームのスナップショットも含まれる。
ゴールデンイメージ	<ul style="list-style-type: none">✓ 最適なEC2インスタンスの構成をAMIとした上で、構成を複数利用することができる。✓ 最適なEC2インスタンス構成を反映したAMIをゴールデンイメージと呼ぶ
AMIの共有	<ul style="list-style-type: none">✓ AMI を共有するユーザーの AWS アカウント番号を指定することで他アカウントに共有可能
リージョンの移動	<ul style="list-style-type: none">✓ AMIはリージョン内でのみ利用可能✓ 別リージョンにコピーは可能。このAMIはそのリージョンのAMIとして別AMIとなる。

EC2の起動方法

EC2の起動は以下のステップで実行します。



インスタンスタイプの選択

インスタンスタイプの選択では、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リソースを選択する

The screenshot shows the AWS EC2 console interface for selecting an instance type. The top navigation bar includes the AWS logo, service dropdown, resource group dropdown, and user information (udemy-aws-14days @ udemy...). Below the navigation is a breadcrumb trail: 1. AMI の選択, 2. インスタンスタイプの選択 (which is underlined), 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, 7. 確認.

ステップ 2: インスタンスタイプの選択

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。

フィルタ条件: **すべてのインスタンスタイプ** 現行世代 列の表示/非表示

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
<input type="checkbox"/>	汎用	t2.nano	1	0.5	EBS のみ	-	低から中	はい
<input checked="" type="checkbox"/>	汎用	t2.micro 無料利用枠の対象	1	1	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.small	1	2	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.medium	2	4	EBS のみ	-	低から中	はい
<input type="checkbox"/>	汎用	t2.large	2	8	EBS のみ	-	低から中	はい

Buttons at the bottom: キャンセル, 戻る, 確認と作成 (highlighted in blue), 次の手順: インスタンスの詳細の設定

[Q]インスタンスタイプの選択

大手ECマース企業はAWSを利用してWEBアプリケーションを構築しています。このアプリケーションでは、顧客情報を解析して最適な商品を提示する機能を作る必要があります。その際には、ローカルストレージ上の非常に大きなデータセットに対して高いシーケンシャルな読み取りおよび書き込みアクセスを必要とするワークフローを実行します。

このシナリオで使用するのに最適なインスタンスタイプは次のうちどれですか？

- 1) ストレージ最適化インスタンス
- 2) メモリ最適化インスタンス
- 3) コンピューティング最適化インスタンス
- 4) 汎用インスタンス

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

ユースケースに応じてインスタンスタイプを選択する。

汎用	ファミリー：A1、M5、T3など バランスの取れたコンピューティング、メモリ、ネットワークのリソースを提供し、多様なワークロードに使用。ウェブサーバーやコードリポジトリなど、インスタンスのリソースを同じ割合で使用するアプリケーションに最適なインスタンス
コンピューティング最適化	ファミリー：C5、C6gなど 高パフォーマンスプロセッサが必要なコンピューティングバウンドなアプリケーションに利用。ユースケースはバッチ処理ワークロード、メディアトランスクード、高性能ウェブサーバー、ハイパフォーマンスコンピューティング（HPC）、科学モデリング、専用ゲームサーバーおよび広告サーバーエンジン、機械学習推論
メモリ最適化	ファミリー：X1、R5、ハイメモリ、z1dなど メモリ内の大きいデータセットを処理するワークロードに対して高速なパフォーマンスに最適なインスタンス
ストレージ最適化	ファミリー：H1、D2、I3、I3enなど ローカルストレージの大規模データセットに対する高いシーケンシャル読み取りおよび書き込みアクセスを必要とするワークロード用。ストレージ最適化インスタンスは、数万 IOPS の低レイテンシーなランダム I/O オペレーションに最適
高速コンピューティング	ファミリー：P3、Inf1、G4（GPU）、F1（FPGA）など 高速コンピューティングインスタンスはハードウェアアクセラレーター（コプロセッサ）を使用して、浮動小数点計算、グラフィックス処理、データパターン照合などの機能をCPUで実行するソフトウェアに最適

EC2の起動方法

EC2の起動は以下のステップで実行します。

AMI (OSセッティング) を選択

インスタンスタイプを選択

インスタンスタイプの詳細の設定

ストレージを選択

タグの追加

セキュリティグループを選択

キーペアを設定

[Q]ユーザーデータの利用

ある企業はAWS上でEC2インスタンスを利用したWEBアプリケーションを構築しています。これらのEC2インスタンスを起動する際に、全てのインスタンスで利用することになるApacheサーバーを自動的に設定することが必要です。

この要件を満たすために利用するべきEC2インスタンスの機能を選択してください。

- 1) ユーザーデータ
- 2) メタデータ
- 3) タグ
- 4) 自動設定機能の有効化

ユーザーデータの利用

ユーザーデータを利用してEC2インスタンス起動時に実行されるスクリプトを設定できる。

ユーザーデータ

- ✓ EC2インスタンスの詳細設定の自動化に利用
- ✓ Bashスクリプトなどを設定して、インスタンス起動時に実行されるように準備できる。

ブートストラップ

- ✓ インスタンスにユーザーデータを渡すことで、起動時に実行される処理のこと

ユーザーデータの利用

インスタンスの詳細設定において、高度な詳細にあるユーザーデータを利用して実行スクリプトを設定することが可能

ステップ 3: インスタンスの詳細の設定

ください。休止状態を使用するには、ルートボリュームが暗号化された EBS ボリュームを有効にしてください。

終了保護の有効化 誤った終了を防止します

モニタリング CloudWatch 詳細モニタリングを有効化
追加料金が適用されます。

テナント 共有 - 共有ハードウェアインスタンスの実行
専有テナントには追加料金が適用されます。

Elastic Inference Elastic Inference アクセラレーターを追加
追加料金が適用されます。

Credit specification Unlimited
追加料金が適用される場合があります

ファイルシステム ファイルシステムの追加

▼ 高度な詳細

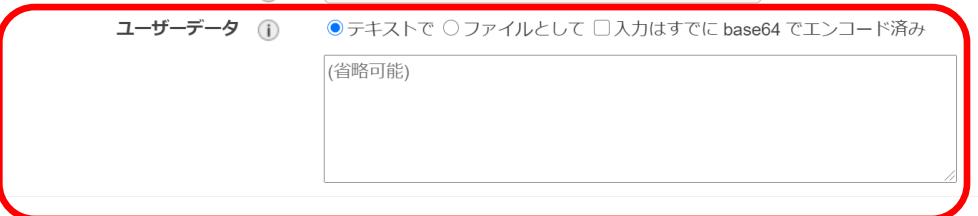
Enclave 有効
Nitro Enclave と Hibernation を同じインスタンスで有効にすることはできません。

Metadata accessible Enabled

Metadata version V1 and V2 (token optional)

Metadata token response hop limit 1

ユーザーデータ テキストで ファイルとして 入力はすでに base64 でエンコード済み
(省略可能)



EC2の起動方法

EC2の起動は以下のステップで実行します。

AMI (OSセッティング) を選択

インスタンスタイプを選択

インスタンスタイプの詳細の設定

ストレージを選択

タグの追加

セキュリティグループを選択

キーペアを設定

ストレージの選択

EC2で直接利用するストレージを追加する。

The screenshot shows the AWS EC2 instance creation wizard at Step 4: Storage Selection. The top navigation bar includes the AWS logo, service dropdown, resource group dropdown, a bell icon, user information (udemy-aws-14days @ udemy...), location (Tokyo), 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.

ステップ 4: ストレージの追加

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 ボリュームやインスタンスマウントボリュームをアタッチするか、ルートボ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 ボリュームをアタッチすることもできますが、インスタンスマウントボ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

[新しいボリュームの追加](#)

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](#)。

ストレージの選択

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・終了と共にデータは消去される
- ✓ 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はデータを保持可能で、SnapshotをS3に保存する。
- ✓ 別途EBS料金が必要

EC2の起動方法

EC2の起動は以下のステップで実行します。



[Q]タグ設定

あなたの会社は複数部門でAWSを利用しておおり、様々なユーザーがAWSを利用しています。そのために、AWSリソースの管理を効率的に実施することが必要となります。あなたはソリューションアーキテクトとして、部門ごとにAmazonEC2リソースを識別できるように分類する設定を行っています。

どのAWS機能を利用して、リソースの分類を実施できるでしょうか？

- 1) パラメーター
- 2) メタデータ
- 3) タグ
- 4) ユーザーデータ

タグ設定

タグを追加で設定して名前を付与することができ、EC2などのリソースのグループ分けや権限分けに利用する。

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 7. 確認

ステップ 5: タグの追加

タグは、大文字と小文字が区別されるキーと値のペアから構成されます。たとえば、キーに「Name」、値に「Webserver」を使用してタグを定義することができます。タグのコピーは、ボリューム、インスタンス、または両方に適用できます。タグは、すべてのインスタンスとボリュームに適用されます。Amazon EC2 リソースのタグ付けに関する [詳細はこれら](#)。

キー (最大 128 文字)	値 (最大 256 文字)	インスタンス (複数選択可)
Name	udemy	<input checked="" type="checkbox"/>
別のタグを追加 (最大 50 個のタグ)		

EC2の起動方法

EC2の起動は以下のステップで実行します。

AMI (OSセッティング) を選択

インスタンスタイプを選択

インスタンスタイプの詳細の設定

ストレージを選択

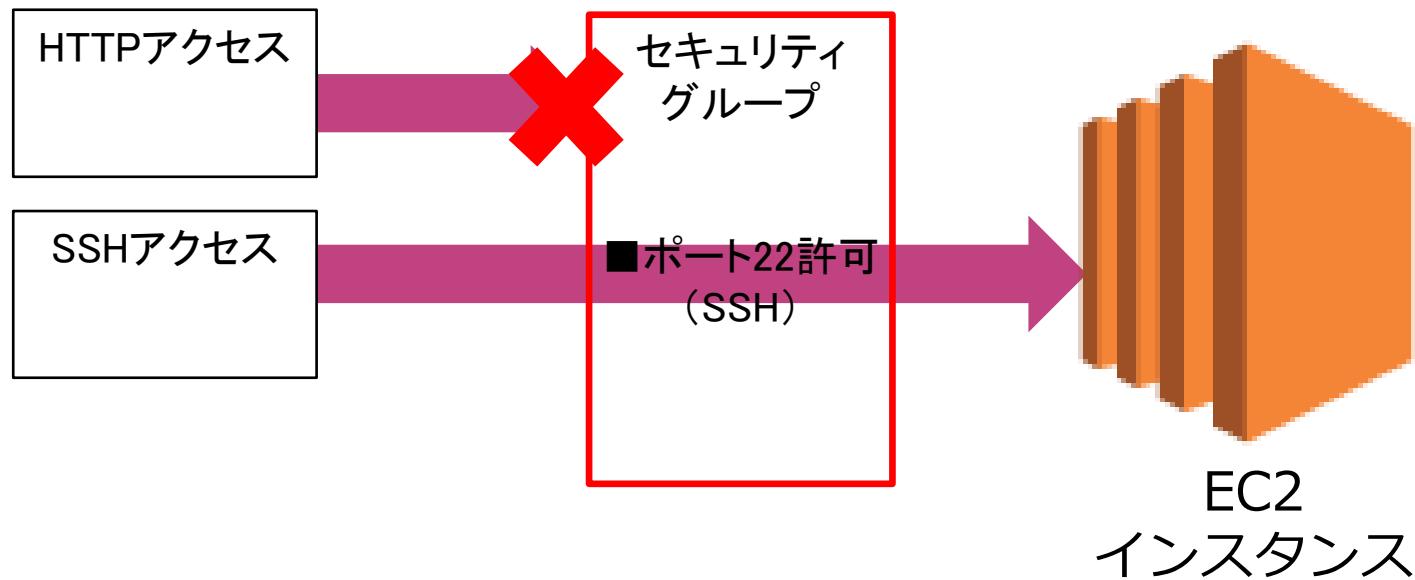
タグの追加

セキュリティグループを選択

キーペアを設定

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



EC2の起動方法

EC2の起動は以下のステップで実行します。

AMI (OSセッティング) を選択

インスタンスタイプを選択

インスタンスタイプの詳細の設定

ストレージを選択

タグの追加

セキュリティグループを選択

キーペアを設定

[Q] キーペアの利用

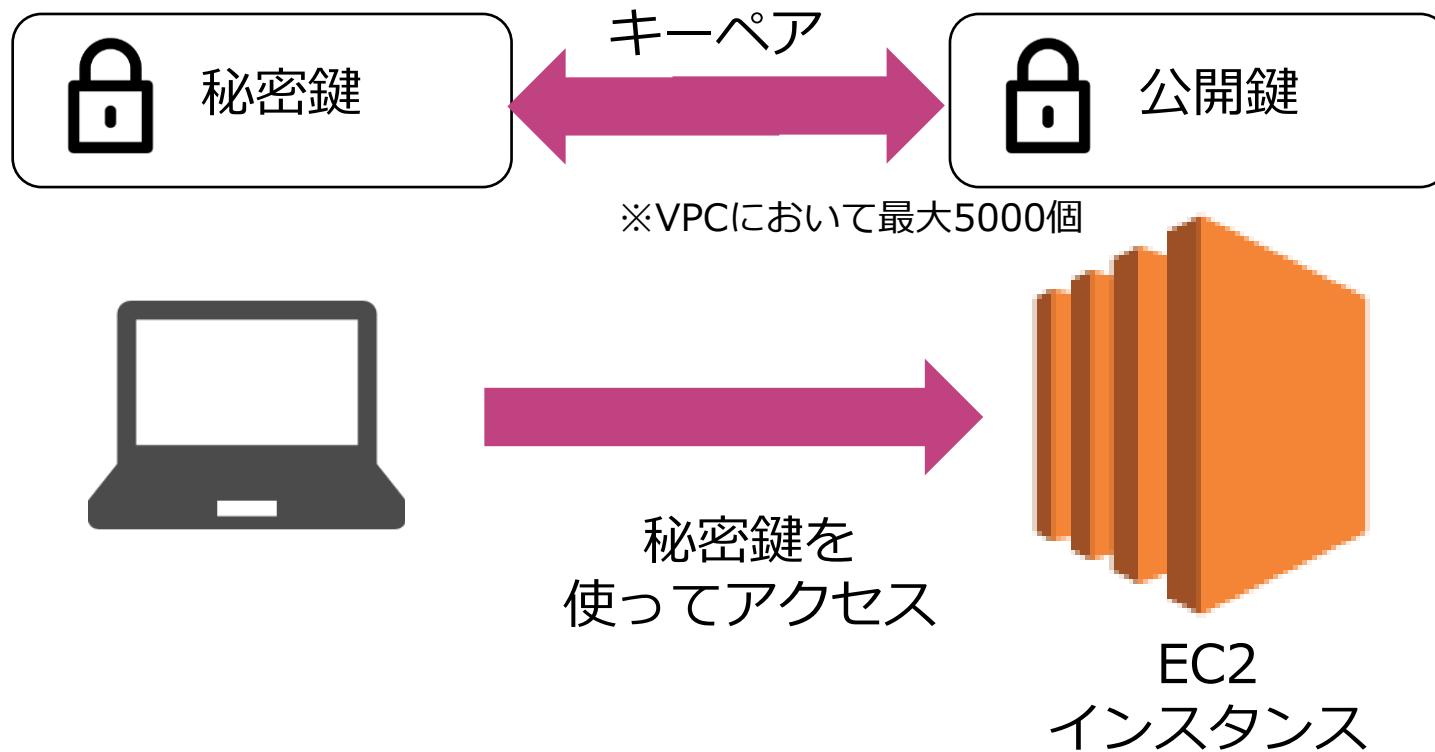
あなたはAWSアカウントを作成して、初めてLinux EC2インスタンスを起動しました。このインスタンスにアクセスしてサーバーソフトウェアをインストールして、WEBサーバーとして設定する対応が必要です。ローカル端末からインスタンスにアクセスして設定することになります。

インスタンスに安全にアクセスするために利用する認証方式を選択してください。

- 1) キーペア
- 2) アクセスキー
- 3) シークレットアクセスキー
- 4) パスワード

キーペアの利用

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



[Q]起動テンプレート

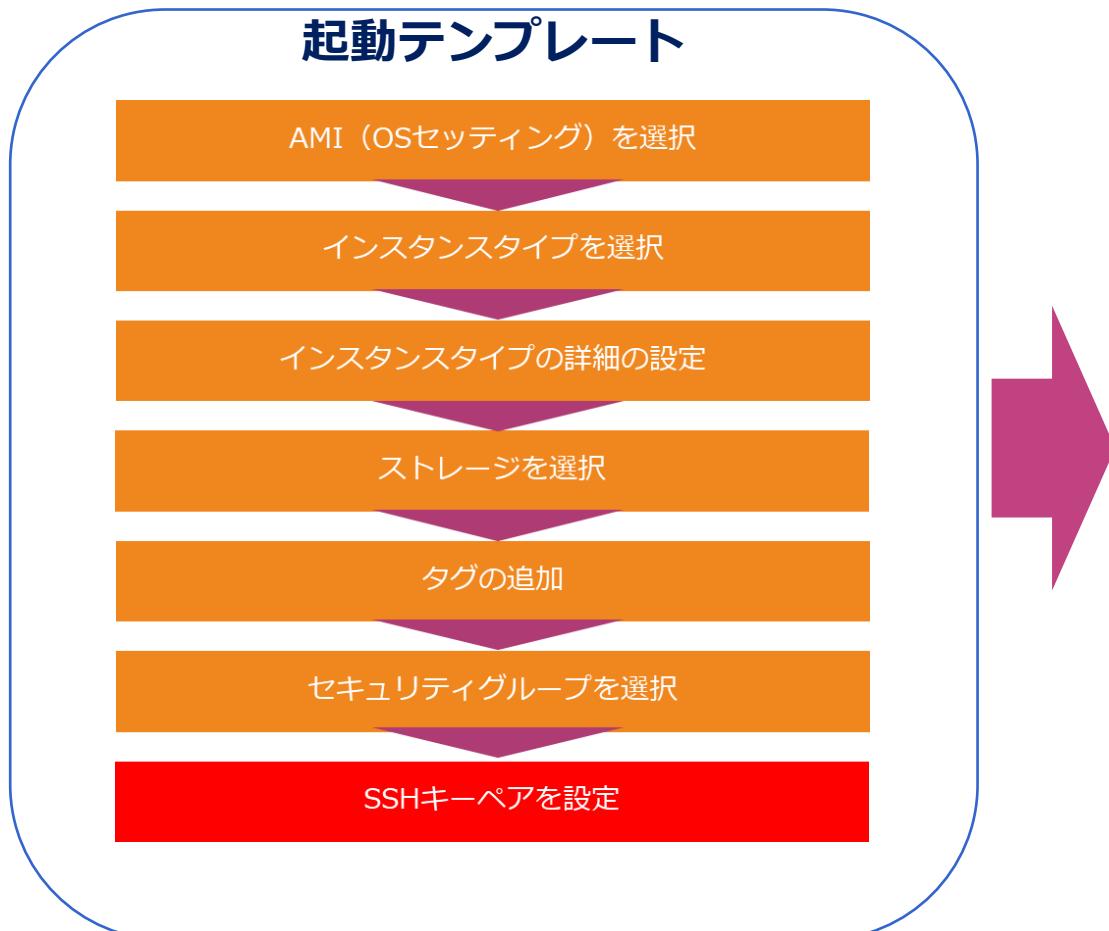
あなたはソリューションアーキテクトとして、社内のAWS利用を標準化する対応を実施しています。通常利用するEC2インスタンスの構成を事前に設定することで、EC2インスタンスを定期的に手動で起動し、プロセスを合理化して管理オーバーヘッドを削減する対応を検討しています。その際には、EC2インスタンスのAMIの選択、インスタンスタイプ、キーペア、セキュリティグループなどの設定を保存することが必要です。

この要件を満たすEC2インスタンスの機能を選択してください。

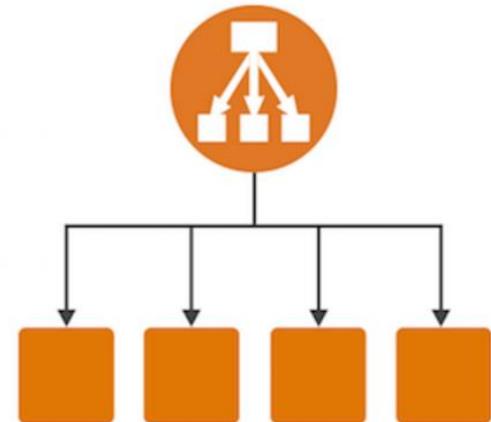
- 1) 起動テンプレートを利用する。
- 2) 起動設定を利用する。
- 3) AMIを利用する。
- 4) 起動グループを利用する。

起動テンプレート

起動テンプレートは起動の詳細な設定内容をテンプレート化して保存することができる。



Auto Scaling



[Q]インターネットアクセス

ソリューションアーキテクトはAWSアカウントを新規に作成して、ITインフラストラクチャーを構成しています。Amazon VPCに新しいサブネットを作成し、そのサブネットにAmazonEC2インスタンスを起動しました。あなたはEC2インスタンスの設定をするために、インターネットからEC2インスタンスに直接アクセスを試みましたが、接続ができないようです。

EC2インスタンスへの接続失敗に対処するために、どの手順を確認する必要がありますか？（2つ選択してください）

- 1) パブリックサブネットにNATゲートウェイが設置されている。
- 2) セキュリティグループにアウトバウンドトラフィックのルールが適切に設定されている。
- 3) インスタンスにパブリックIPアドレスが設定されている。
- 4) インスタンスにプライベートIPアドレスが設定されている。
- 5) サブネットに関連付けられているルートテーブルにインターネットゲートウェイにインターネットへのアクセスルートが適切に構成されている。

インターネットアクセス

起動したインスタンスにアクセスする際はパブリックIPを利用してアクセスする。

The screenshot shows the AWS Management Console interface for the EC2 service. At the top, there's a navigation bar with tabs for 'Instancesの作成', '接続', and 'アクション'. Below it is a search bar and a filter section for 'Name' and 'インスタンス ID'. A table lists one instance: 'i-0b02b822d692a0499' (t2.micro, ap-northeast-1c, running, 2/2のチェック, なし, ec2-54-199-94-166.ap-northeast-1.compute.amazonaws.com, 54.199.94.166). The main content area displays detailed information for this instance. The '説明' tab is selected. Key details include:

項目	値
インスタンス ID	i-0b02b822d692a0499
インスタンスの状態	running
インスタンスタイプ	t2.micro
プライベート DNS	ip-172-31-4-132.ap-northeast-1.compute.internal
プライベート IP	172.31.4.132
セカンダリプライベート IP	
VPC ID	vpc-940724f3
プラットフォーム	Amazon Linux
パブリック DNS (IPv4)	ec2-54-199-94-166.ap-northeast-1.compute.amazonaws.com
IPv4 パブリック IP	54.199.94.166
IPv6 IP	-
Elastic IP	
アベイラビリティーゾーン	ap-northeast-1c
セキュリティグループ	launch-wizard-5, インバウンドルールの表示, アウトバウンドルールの表示
予定されているイベント	予定されているイベントはありません
AMI ID	amzn2-ami-hvm-2.0.20200917.0-x86_64-gp2 (ami-0ce107ae7af2e92b5)
サブネット ID	subnet-51ffa00a

インターネットアクセス

インターネットからのEC2インスタンスへのアクセスが不能な場合は以下のような原因が考えられる。

パブリック
IPアドレスがない

- ✓ デフォルトサブネットでインスタンスを起動するとパブリックIPアドレスが自動で付与される。
- ✓ ユーザーが作成するサブネットをデフォルト設定で利用すると「パブリックIPの自動割り当て設定」が有効化されてない。
- ✓ 割り当てがされていないとインスタンスを作成しなおすか、EIPを利用する。

アクセス許可設定

- ✓ セキュリティグループまたはネットワークACLにより適切なアクセス許可が設定されていない。
- ✓ 利用しているオンプレミス側のネットワーク環境の問題

ネットワーク
構成のミス

- ✓ パブリックサブネットにインスタンスを配置していない（サブネットとVPCにインターネットゲートウェイが設定されていない）

[Q]インスタンスの購入方式

あなたの会社はデータセンターにホストされているITインフラストラクチャをAWSクラウドに移行しようとしています。会社はアプリケーションで利用するサーバーソフトウェアのライセンスを所有しており、AWSに移行されても、それらのライセンスを引き続き利用したいと考えています。あなたはソリューションアーキテクトとして最適なサーバーの移行先を検討しています。

最も費用効果の高いインスタンスの購入方式を選択してください。

- 1) ベアメタルインスタンスを利用する。
- 2) ハードウェア専有インスタンスを使用する。
- 3) オンデマンドインスタンスを使用する
- 4) Dedicated Hostを使用する

インスタンスの購入方式

インスタンスの購入方式に応じて割引価格が提供されるため、用途に応じて割引価格を利用するすることが重要となる。

オンデマンドインスタンス	<ul style="list-style-type: none">✓ 通常のインスタンス購入方式✓ 長期契約なしで、コンピューティング性能に対して秒単位で支払う。そのライフサイクルを完全に制御できるため、いつ起動、停止、休止、開始、再起動、または終了するかを決定できる。
リザーブドインスタンス	<ul style="list-style-type: none">✓ Amazon EC2 リザーブドインスタンス (RI) は、1年または3年の期間利用を予約することで、通常のオンデマンド料金に比べて大幅な割引価格 (最大 75%) が適用されるインスタンスの購入形式。✓ 特定のアベイラビリティーゾーンまたはリージョンで使用するキャパシティーを予約できる2つのタイプがある。
スケジュールドリザーブドインスタンス (利用停止)	<ul style="list-style-type: none">✓ 1年間にわたり毎日、毎週、または毎月ベースの指定された開始時間および期間で繰り返しキャパシティー予約を購入する。あらかじめキャパシティーを予約しておき、必要なときに使用できる。✓ 繙続的には実行されないが定期的なスケジュールで実行されるワークロードに利用する。2021年に利用停止となった。
スポットインスタンス	<ul style="list-style-type: none">✓ オンデマンド価格より低価で利用できるAWS管理用に保持されているが未使用的 EC2 インスタンス。ユーザーは未使用的 EC2インスタンスを静止状態割引 (最大 90% 割引ほど) でリクエストできる。✓ 実行時間に柔軟性がある場合や、中断できる処理に利用する。

Saving Plan

1~3 年の期間に一定の使用量を守ることにより Amazon EC2 のコストを削減する

- 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

キャパシティの予約

キャパシティを事前に予約して購入形式に適用する。リザーブドインスタンスとはセットで利用する。

キャパシティ予約

- ✓ インスタンスタイプが起動可能であるという確保権のこと。予めキャパシティを確保しておくことで実行時のキャパシティ不足エラーを抑制する。

オンデマンドキャパシティ予約

- ✓ 必要な期間中のみオンデマンドの利用料でキャパシティが予約できる機能

ゾーンリザーブドインスタンス

- ✓ 指定したアベイラビリティーゾーン(AZ)内で1年間または3年間の間のキャパシティを予約する
- ✓ AZは指定した場所のみ利用可能

リージョンリザーブドインスタンス

- ✓ 指定したリージョン内で1年間または3年間の間のキャパシティを予約する
- ✓ AZはどこでも利用可能

キャパシティーの予約

特定のアベイラビリティーゾーンの EC2 インスタンスに対して任意の期間キャパシティーを予約する

	オンデマンドの キャパシティーの予約	リザーブド インスタンス	Saving Plan
期間	コミットメントは不要で、 必要に応じて作成および キャンセル可能	固定の 1 年または 3 年のコミットメントが必要	
キャパシティーの利点	特定のAZのキャパシティ を予約して利用可能	特定のAZ またはリージョンで予約 して利用可能	なし
請求割引	なし	有	有
インスタンスの制約	リージョンごとの オンデ マンドインスタンス数に 制限	AZまたはリージョンあたり 20の制限 制限引上げ申請可	なし

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ユーザー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

[Q]リザーブドインスタンスの特徴

あなたの会社では3年間利用する予定でリザーブドインスタンスのスタンダードを前払いして購入してWEBアプリケーションを構築しました。しかしながら、このアプリケーションには不具合が多くなったため、急遽利用を取りやめることが決定されました。リザーブドインスタンスの利用期間はまだ2年以上残っています。あなたはソリューションアーキテクトとして、リザーブドインスタンスの料金の発生をできるだけ早く停止する必要があります。

この状況でどのような費用削減が実行できますか？

- 1) Amazonマーケットプレイスにおいて、リザーブドインスタンスを販売する。
- 2) リザーブドインスタンスマーケットプレイスにおいて、リザーブドインスタンスを販売する。
- 3) リザーブドインスタンスは3年契約で前払い購入しているため、料金は既に発生しており、このまま利用するしかない。
- 4) AWSに連絡してAWSサブスクリプションをキャンセルする。

リザーブドインスタンスの特徴

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	

[Q]スポットインスタンスの特徴

B社ではWEBアプリケーションをAWSサービスを利用して構築しました。このWEBアプリケーションでは最近になって負荷が高まっており、処理が滞るトラブルが発生しています。あなたはソリューションアーキテクトとして、一時的な負荷向上に対応するためAuto Scalingを設定して、スポットインスタンスを利用する構成を行いました。

スポットインスタンスの機能に関して、正しいと説明は次のうちどれですか？（2つ選択してください）

- 1) スポットリクエストが永続的である場合は、スポットインスタンスが中断された後に再びスポットインスタンスを起動する。
- 2) アクティブなスポットリクエストをキャンセルすると、関連するインスタンスも終了する。
- 3) スポットリクエストが永続的である場合は、スポットインスタンスを停止した後に再びスポットインスタンスを起動する。
- 4) スポットブロックはスポットインスタンスと同じように、中断される可能性がある。
- 5) アクティブなスポットリクエストをキャンセルしても、関連付けられたインスタンスは終了しない。

スポットインスタンスの特徴

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

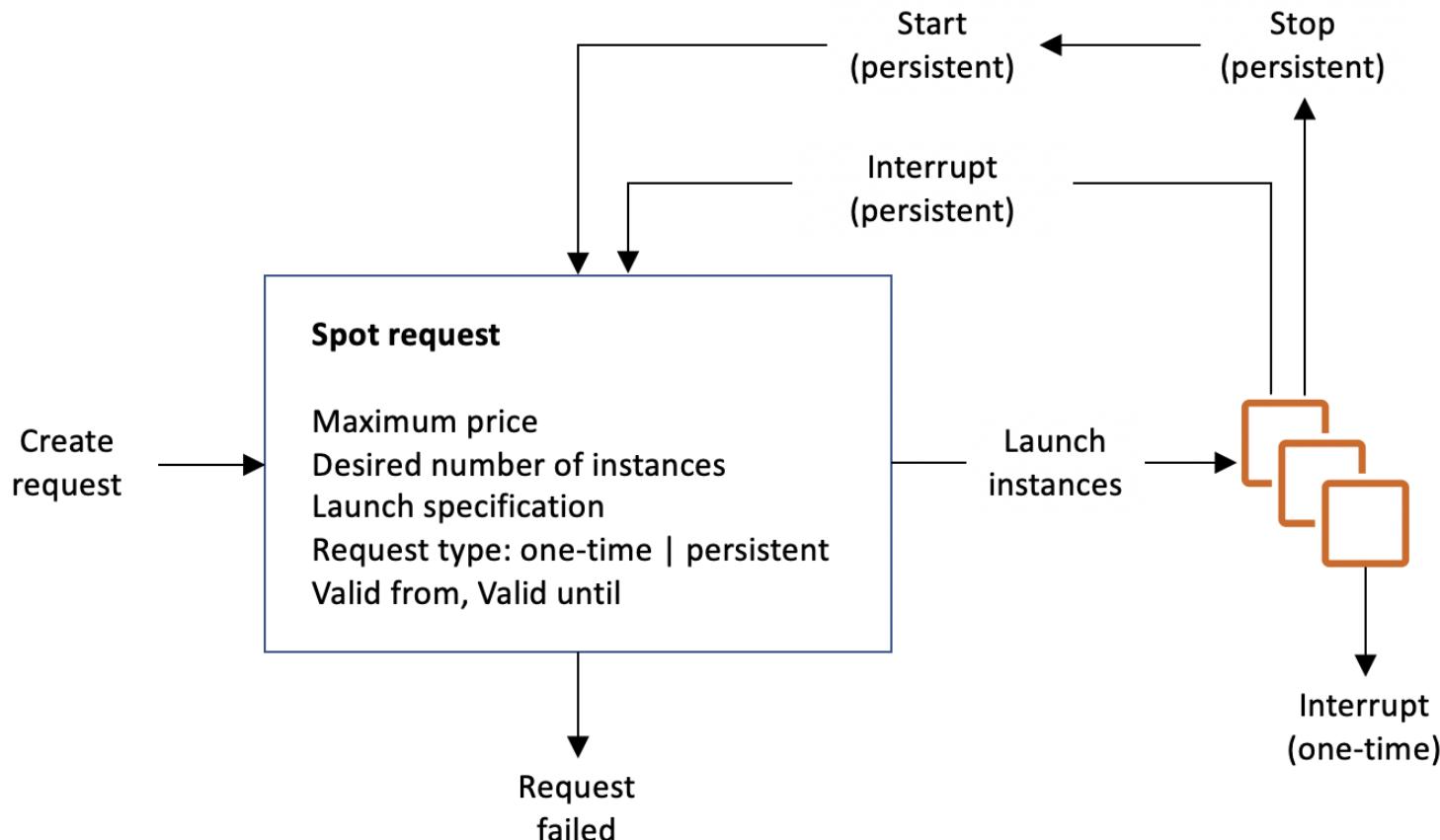
- 予備用を入札式で利用するためとても安い（最大90%引き）
- 起動に通常よりも少し時間がかかる
- 予備用のため途中で削除される可能性がある
⇒一時的な拡張などの用途で利用

【リクエストの中斷などの挙動】

- スポットリクエストが永続的である場合は、スポットインスタンスが中斷された後に再びスポットインスタンスを起動する
- スポットブロックは中斷されないように設計されている。

スポットインスタンスの特徴

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



[Q]スポットフリートの利用

あなたの会社には毎週実行されるバッチ処理のワークロードがあり、約2時間実行されます。このワークロードの処理はコスト効率を高めるために、インスタンスタイプや入札価格や価格上限などの容量ターゲットを指定することで、自動で最安値のインスタンスを選択して起動することが必要です。

この要件を満たすことができる最もコストが最適なソリューションはどれですか？

- 1) スポットインスタンスでワークロードを実行する
- 2) リザーブドインスタンスでワークロードを実行する
- 3) スケジュールドリザーブドインスタンスでワークロードを実行する
- 4) スポットフリートでワークロードを実行する

スポットフリートの利用

インスタンスタイプや入札価格を指定することで、自動で最安値のインスタンスを選択してスポットインスタンス数を調整して、リクエストを処理する。

【スポットフリートの設定例】

- ✓ インスタンス数： 10台
- ✓ 入札価格： 1ドル
- ✓ インスタンスタイプ： c4.16xlarge, c3.8xlarge



c4.16xlargeとc3.8xlargeのインスタンスタイプから
10インスタンスを自動で入札・起動する。

[Q]スポットブロックの利用

あなたの会社には毎週実行されるバッチ処理のワークフロードがあり、約2時間実行されます。このワークフロードの処理はコスト効率を高めるために、スポットインスタンスを利用する必要ですが、2時間のワークフロードは途中で停止することが許されません。あなたはソリューションアーキテクトとして、最適なインスタンスを検討しています。

次のオプションのうち、最も費用効果の高いソリューションはどれでしょうか？

- 1) スポットフリートを使用してスポットインスタンスを実行する
- 2) スポットブロックを使用してスポットインスタンスを実行する
- 3) EC2フリートを使用してスポットインスタンスを実行する
- 4) EC2ブロックフリートを使用してスポットインスタンスを実行する

スポットブロックの利用

スポットインスタンスを1時間から6時間の間中断することなく
継続利用が可能になる機能

メリット

- ✓ 最大6時間まで中断することがない。
- ✓ 途中で中断する可能性があるスポットインスタンスの利用を安定させる。
- ✓ スポットフリートのオプションとして設定することが可能

デメリット

- ✓ 通常のスポットインスタンスよりは値段が若干高くなるため、最安ではなくなる。

[Q]EC2フリートの利用

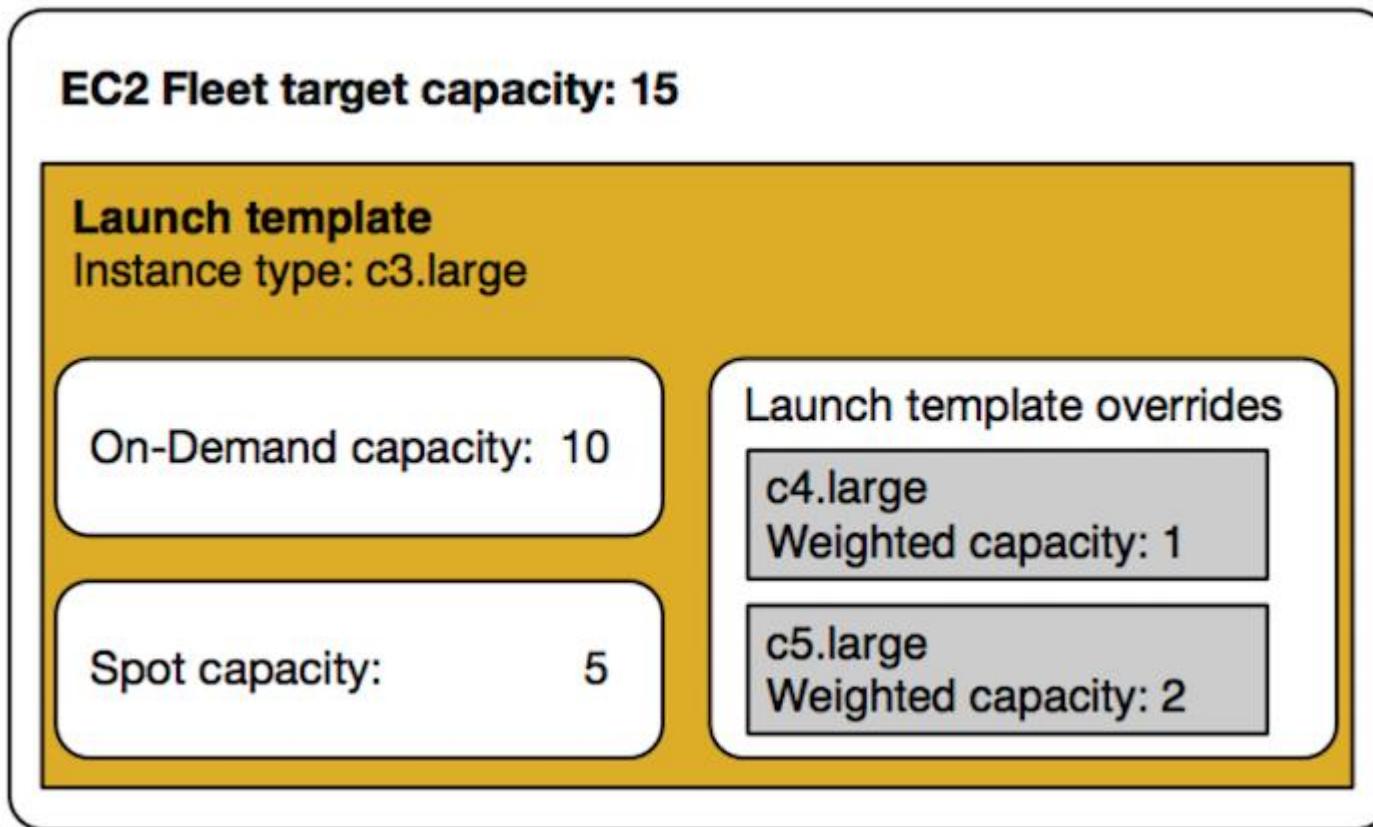
大手ECマース企業はECマースアプリケーションを構築しています。このアプリケーションはグローバルから沢山のユーザーからアクセスされる予定です。パフォーマンス要件を試算したところ、中長期的に20個のインスタンスが必要であり、不定期に実施されるバッチジョブなどのバックグラウンドジョブ用に追加で5個のインスタンスを利用することが必要となります。このバッチジョブは30分から2時間ほどで完了し、実行に失敗すると再処理を実行します。

インスタンス購入オプションの最適な組み合わせを選択してください。

- 1) リザーブドインスタンス20個とスケジュールドインスタンス5個でスポットフリートを構成する。
- 2) オンデマンドインスタンス20個とスケジュールドリザーブドインスタンス5個でEC2フリートを構成する。
- 3) リザーブドインスタンス20個とスポットインスタンス5個でEC2フリートを構成する。
- 4) オンデマンドインスタンス20個とスケジュールドリザーブドインスタンス5個でスポットフリートを構成する。

EC2フリートの利用

オンデマンドインスタンスとスポットインスタンスで構成されるインスタンスグループとして設定を定義する仕組み



- どのインスタンスタイプを利用するか？
- オンデマンドとスポットの組合せ数をどうするか？
- 利用料金の上限をいくらにするか？

[Q]プレイスメントグループの利用

大学ではゲノムデータの分析をAWS上で実行することになりました。ゲノム解析には高性能なサーバー処理が求められており、パフォーマンスコンピューティングに対応した複数のEC2インスタンスを利用した高パフォーマンスなネットワーク処理も不可欠となっています。

このアプリケーションを実行する際に利用するべきEC2インスタンスの構成はどれでしょうか？

- 1) EC2インスタンスでパーティションプレイスメントグループを構成する。
- 2) EC2インスタンスでEC2フリートを構成する。
- 3) EC2インスタンスでスポットフリートを構成する。
- 4) EC2インスタンスでスプレッドプレイスメントグループを構成する。
- 5) EC2インスタンスでクラスタープレイスメントグループを構成する。

プレイスメントグループの利用

単一のアベイラビリティーゾーン内のインスタンスのパフォーマンスを向上させるために論理的にグループ化する機能

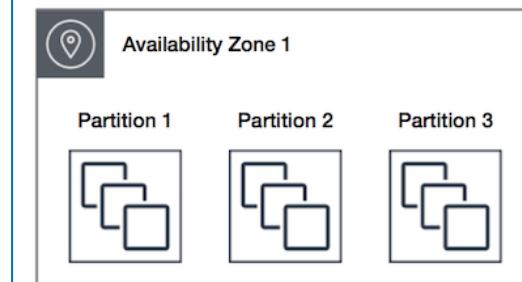
クラスター プレイスメント グループ

- ✓ 単一AZ内のインスタンスを論理的にグループ化した構成
- ✓ 同じリージョン内の複数のピア VPC にまたがることも可能
- ✓ グループ内のインスタンスは、TCP/IP トラフィックのフローあたりのスループット上限が高くなり、ネットワークの二分帯域幅の広い同じセグメントに配置されインスタンス間通信が向上する
- ✓ 低いネットワークレイテンシー、高いネットワークスループットを実現するアプリケーション向けの構成



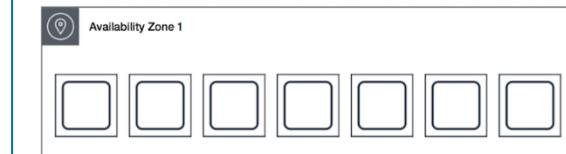
パーティション プレイスメント グループ

- ✓ Amazon EC2 は各グループをパーティションと呼ばれる論理的なセグメントに分割した構成
- ✓ プレイスマントグループ内の各パーティションにそれぞれ一連のラックがあり、プレイスメントグループ内のパーティションどうしが同じラックを共有しない。
- ✓ ラックを分離することで、アプリケーション内でのハードウェア障害による影響を隔離して、軽減する。



スプレッド プレイスメント グループ

- ✓ それぞれに独自のネットワークおよび電源がある異なるラックに別々に配置できるインスタンスのグループ
- ✓ 1 つのAZ内の、スプレッドプレイスメントグループに配置された 7 つのインスタンスは、7 つの異なるラックに配置される。
- ✓ 少数の重要なインスタンスが互いに分離して保持できる。インスタンスが同じラックを共有するときに発生する可能性のある同時障害のリスクを軽減する。



[Q]拡張ネットワーキング

大学ではゲノムデータの分析をAWS上で実行することになりました。ゲノム解析には高性能なサーバー処理が求められており、パフォーマンスコンピューティングに対応した複数のEC2インスタンスを利用した高パフォーマンスなネットワーク処理も不可欠となっています。あなたはソリューションアーキテクトとして、EC2インスタンスの最適な構成により高ネットワークスループットを確保する必要があります。

この要件を達成するのに必要な構成はどれでしょうか？（3つ選択してください）

- 1) EC2インスタンスの拡張ネットワーキングを使用する。
- 2) EBSのプロビジョンドIOPSボリュームを使用する。
- 3) EC2インスタンスのコンピューティング最適化インスタンスを利用する。
- 4) クラスター・プレイスメント・グループを使用する。
- 5) Dedicated Hostを使用する。

拡張ネットワーキング

高い帯域幅、1秒あたりのパケット(PPS)の高いパフォーマンス、常に低いインスタンス間レイテンシーを実現する。3つのタイプを利用する。

アダプター	インスタンスタイプの例	カーネルモジュール	Windows ドライバ	パフォーマンス
VIF	すべて	xen-netfront	Citrix または AWS PV	低～中
Intel 82599 VF	C3、C4、D2、I2、R3、M4 (m4.16xlarge は除く)	ixgbevf	Intel 82599 VF	最大 10 Gbps
Elastic Network Adapter	C5、C5d、F1、G3、H1、I3、m4.16xlarge、M5、M5a、M5d、P2、P3、R4、R5、R5a、R5d、T3、u-6tb1.metal、u-9tb1.metal、u-12tb1.metal、X1、X1e、および z1d	ena	ena	最大 25 Gbps

Reference: <https://aws.amazon.com/jp/premiumsupport/knowledge-center/enable-configure-enhanced-networking/>

[Q] Elastic Fabric Adapterの利用

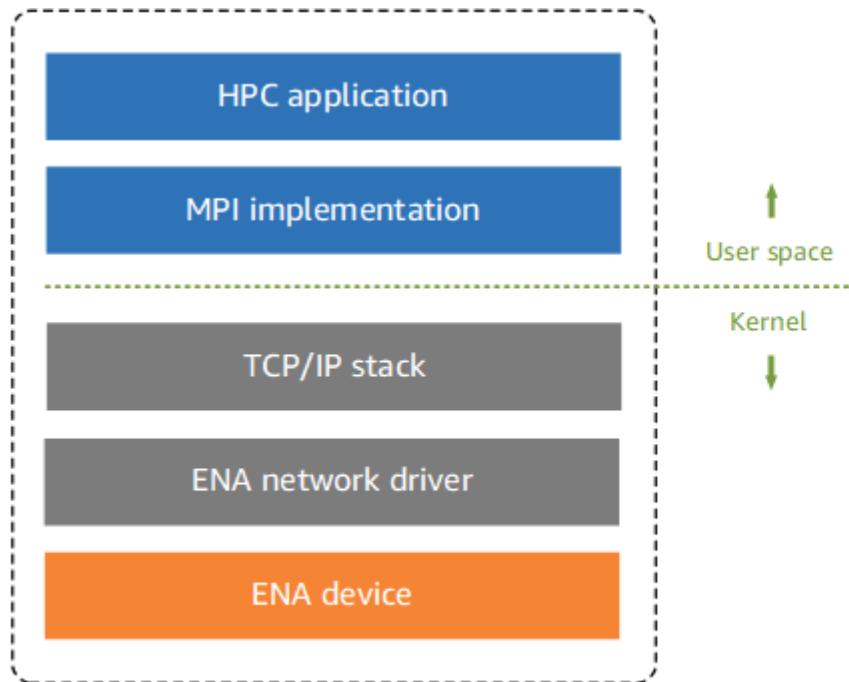
大学ではゲノムデータの分析をオンプレミス環境で実行しています。ゲノム解析には高性能なサーバー処理が求められており、パフォーマンスコンピューティング(HPC)を利用しています。あなたはソリューションアーキテクトとして、これらのワークフローをオンプレミスインフラストラクチャからAWSクラウドに移行することを検討しています。

HPCワークフローを実行するEC2インスタンスで利用されるネットワークコンポーネントはどれでしょうか？

- 1) Elastic Network Interface
- 2) Elastic Fabric Adapter
- 3) Elastic Network Adapter
- 4) Elastic IP Address

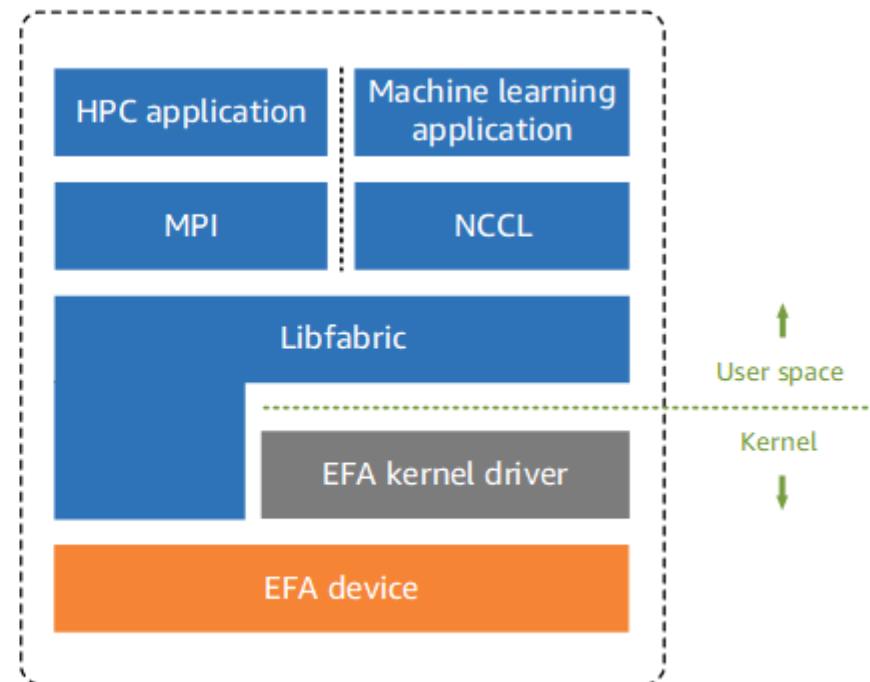
Elastic Fabric Adapterの利用

ハイパフォーマンスコンピューティング (HPC) と機械学習アプリケーションを高速化するためのEC2用ネットワークデバイス



Traditional HPC software stack in EC2

ENAは、VPC のサポートに必要な従来の IP ネットワーキング機能を提供



HPC software stack in EC2 with EFA

EFAはENAsの機能に加えてOSバイパス機能がある。
Libfabric APIを利用してHPCと機械学習アプリケーションはオペレーティングシステムのカーネルをバイパスしてEFAデバイスと直接通信できる

[Q] Run Command

あなたは社内でAWSでの運用を担当しているエンジニアです。EC2インスタンスを起動して、Windows サーバーのセットアップを実施しています。このWindows サーバーのPowerShellスクリプトを実行する必要がありますが、AWSマネジメントコンソールから実行することが必要です。

AWSマネジメントコンソールからターゲットEC2インスタンスでスクリプトを実行するための方法を選択してください。

- 1) AWS Trusted Advisor
- 2) AWS CLI
- 3) Run Command
- 4) AWS OpsWorks

Run Command

マネージメントコンソール上からPowerScript、Windows Updateの設定などのコマンド各種コマンドを実行できる機能

コマンドの実行

コマンドのドキュメントには、実行するコマンドに関する情報が含まれています。次のリストからコマンドを選択して実行できます。

コマンドのドキュメント*	Description
AWS-ConfigureCloudWatch	CLOUDWATCH インスタンスに CloudWatch Metrics を登録する
AWS-ConfigureWindowsUpdate	WINDOWSUPDATE インスタンスに Windows Update の構成を登録する
AWS-InstallApplication	APPLICATION インスタンスに新しいアプリケーションをインストールする
AWS-InstallPowerShellModule	POWERSHELLMODULE インスタンスに PowerShell モジュールをインストールする
AWS-JoinDirectoryServiceDomain	DOMAIN インスタンスに Active Directory ドメインに接続する
AWS-RunPowerShellScript	SCRIPT インスタンスに PowerShell スクリプトを実行する
AWS-UpdateEC2Config	EC2CONFIG インスタンスに EC2 Config ルールを登録する

ターゲットインスタンス* インスタンス 個を選択済み ⓘ

インスタンスの選択 ▾

Status Enabled ⓘ

Properties

[Q]EC2の自動リカバリー

あなたの会社は30台以上のEC2インスタンスを利用して大規模なWEBアプリケーションを運用しています。このアプリケーションはなるべく自動的に運用をする必要があります。あなたはソリューションアーキテクトとして、Amazon CloudWatchアラームを使用して、EC2インスタンスが障害になった場合に自動的に回復されます。

この自動回復されたインスタンスのステータスとして正しい説明はどれでしょうか？

- 1) インスタンスに設定されたパブリックIPv4アドレスは、インスタンスが復元時には別のアドレスに変更される。
- 2) インスタンスに設定されたパブリックIPv4アドレスは、リカバリ後も維持される。
- 3) 復元されたインスタンスは、インスタンスID、プライベートIPアドレス、Elastic IPアドレス、全てのメタデータは保持される。
- 4) インスタンス復元前のメモリ内にあるデータはすべて保持される。

EC2のリカバリー

EC2インスタンスは定期的にバックアップすることが重要

- 定期的にバックアップ（AMI／スナップショット）をとる
- 定期的にリカバリプロセスを確認する
- 複数のAZに重要なアプリケーションをデプロイする
- CloudWatchによりインスタンスのステータスをモニタリングする
 - チェック結果が失敗になった場合、CloudWatch アラームアクションを使用してインスタンスを自動的に復旧させる
 - 自動復旧後のステータスとIPアドレスは元のインスタンスと同じ
- インスタンス起動時に動的IPアドレス処理の設定を行う

[Q]インスタンスの停止と起動

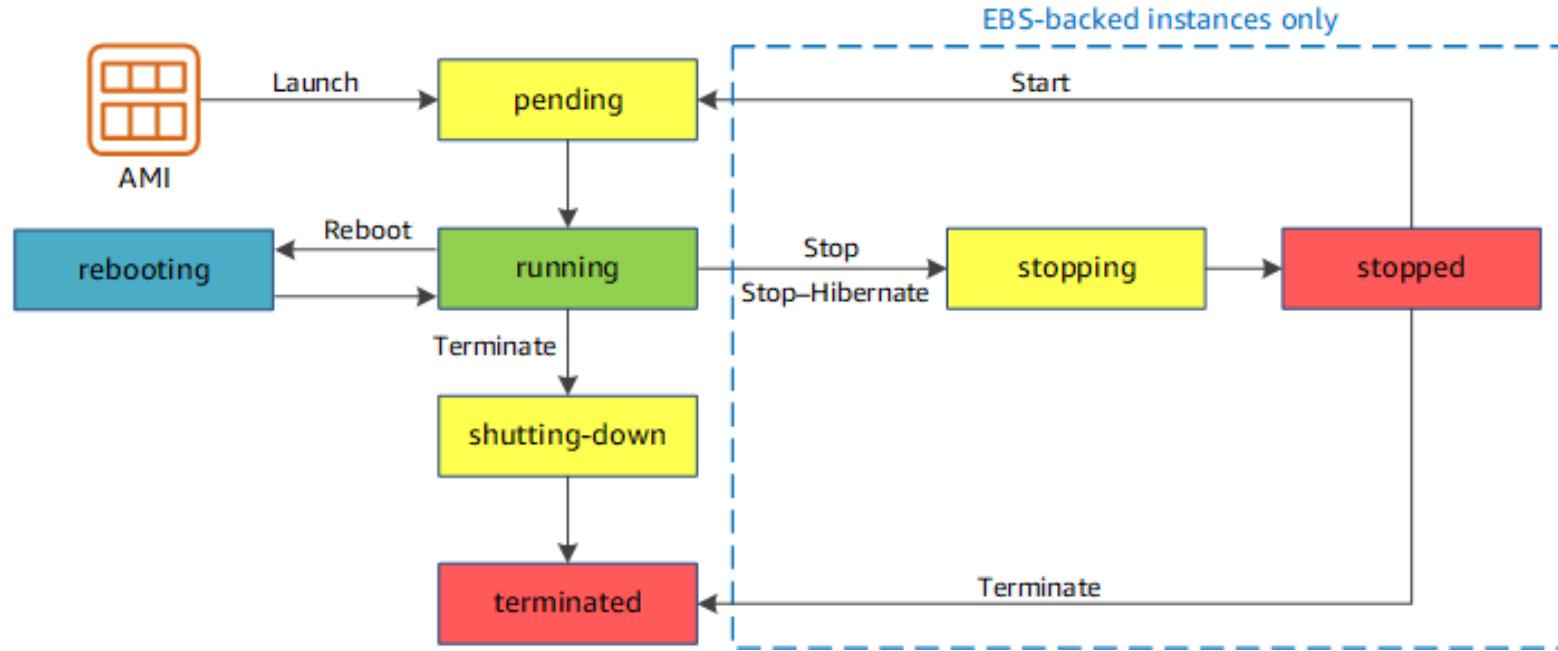
あなたはソリューションアーキテクトとしてEC2インスタンスのメンテナンスを実施しています。停止したEC2インスタンスを再起動しようとしましたが、すぐに保留状態から終了状態に変わりました。

最も可能性の高い原因はどれでしょうか？（2つ選択してください）

- 1) EBSボリューム制限を超過した。
- 2) EBSのスナップショットが壊れている。
- 3) EBSのスナップショットが暗号化されている。
- 4) EBSのスナップショットがコピーされたものである。
- 5) EBSボリュームが不足している。

インスタンスの再起動

インスタンスのステータスは以下のように遷移



Reference: https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html

- ✓ 再起動時にはデータが消失され、ホストが変更される可能性あり
- ✓ 以下のような場合は起動に失敗する。
 1. スナップショットが壊れている
 2. EBSボリューム制限を超過している
 3. 暗号化されたスナップショットのキーを有していない。
 4. インスタンスストア型のAMIが必要なパートが失っている。

インスタンスの再起動

インスタンスのステータスは以下のような内容を示している。

pending	インスタンスは running 状態への移行準備中です。 初めて起動する場合、または pending 状態になってから起動する場合、インスタンスは stopped 状態になります。	課金されない
running	インスタンスは実行中で、使用できる状態です。	課金される
stopping	インスタンスは停止または停止休止の準備中です。	停止準備中は無課金 休止準備中は課金
stopped	インスタンスは停止されているため、使用できません。 インスタンスはいつでも起動できます。	課金されない
shutting-down	インスタンスは削除準備中です。	課金されない
terminated	インスタンスは完全に削除されているため、起動することはできません。	課金されない

[Q]ハイバネーションの利用

あなたのEC2インスタンスを起動しました。このEC2インスタンスはメンテナンス時に一時的に停止させる必要がありますが、その際にメモリ内のデータなどを維持することが求められています。

この要件を満たすためにEC2インスタンスで設定するべき機能はどれでしょうか？

- 1) AMIを使用する。
- 2) EC2インスタンスのリブート設定を利用する。
- 3) EC2インスタンスの再起動を実施する。
- 4) ハイバネーションを使用する

ハイバネーションの利用

ハイバネーションにより、再起動時に停止前の状態を維持することが可能

ハイバネーションの機能

シャットダウン前にメインメモリの内容をハードディスク等に退避することで、次回起動時にまたメインメモリに読み込んで、シャットダウンする前と同じ状態で起動する。
再起動時に停止前の状態を維持することで再起動後のセッティングを容易にする。

インスタンスタイプ に応じて設定

インスタンスタイプに応じてハイバネーションの実施可否が決まる。
初期ではAmazon Linux 1を実行しているM3、M4、M5、C3、C4、C5、R3、R4、R5のみで可能であったが、現在はAmazon Linux 2やWindowsなども対応

ハイバネーションの利用

インスタンスの詳細設定時に有効化する必要がある。

ステップ 3: インスタンスの詳細の設定

ドメイン結合ディレクトリ	<input type="text" value="ディレクトリなし"/>	新しいディレクトリの作成
IAM ロール	<input type="text" value="なし"/>	新しい IAM ロールの作成
CPU オプション	<input type="checkbox"/> CPU オプションを指定	
シャットダウン動作	<input type="text" value="停止"/>	
停止 - 休止動作	<input checked="" type="checkbox"/> 停止動作に休止動作を追加する	
休止動作を有効にする際、インスタンスマемリ (RAM) を格納するための容量がルートボリュームが RAM の内容を保存し、予想される使用量 (OS、アプリケーションなど) に対応ください。休止状態を使用するには、ルートボリュームが暗号化された EBS ボリューム		
タグ付けのための URL		

[Q]メタデータの取得

ソリューションアーキテクトはAWSアカウントに新規にITインフラストラクチャーを構成しています。Amazon VPCに新しいサブネットを作成し、そのサブネットにAmazonEC2インスタンスを起動しました。あなたはインスタンスにSSHで接続しており、インスタンスのコマンドラインで実行されているシェルスクリプト内からインスタンスのパブリックIPを取得する必要があります。

インスタンスのパブリックIPを取得するための正しいURLパスを選択してください。

- 1) `http://169.254.169.254/latest/meta-data/public-ipv4`
- 2) `http://169.254.169.254/latest/user-data/public-ipv4`
- 3) `http://254.169.254.169/latest/meta-data/public-ipv4`
- 4) `http://254.169.254.169/latest/user-data/public-ipv4`

メタデータの取得

インスタンスのメタデータを取得する場合は、次のURIを利用

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

IP アドレスの169.254.169.254 は、リンクローカルアドレスで、インスタンスからのみ有効なもの

VPCの出題範囲

VPCとは何か？

VPCはAWSクラウドのネットワークからユーザー専用の領域を切り出すことができる仮想ネットワークのサービス

AWSクラウドのネットワーク空間

VPCとは何か？

VPCはAWSクラウドのネットワークからユーザー専用の領域を切り出すことができる仮想ネットワークのサービス

AWSクラウドのネットワーク空間



VPCの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

VPCの設定 (デフォルトVPC)	✓ デフォルトVPCの構成状況を問う質問が出題される。
VPCの設定 (VPCウィザード)	✓ VPCを設定する際に利用するVPCウィザードを利用した構成方式が問われる。
サブネットマスク の設定	✓ サブネットマスクを利用したCIDRの設定内容に関する質問が出題される。
ゲートウェイの設定	✓ VPCとサブネットに設置する各種ゲートウェイの使い分けに関する質問が問われる。
インターネット ゲートウェイ	✓ インターネットゲートウェイの設定方法や活用に関する質問が問われる。

VPCの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

NATゲートウェイ	<ul style="list-style-type: none">✓ NATゲートウェイの設定方法に関する質問が問われる。✓ NATインスタンスとNATゲートウェイとの違いや特徴について問われる。
VPCエンドポイント	<ul style="list-style-type: none">✓ VPCエンドポイントを利用したAWSサービスとの連携方法が問われる。
VPCピアリング	<ul style="list-style-type: none">✓ VPCとVPCとを接続するVPCピアリングの活用や設定方法が問われる。
ネットワークACL	<ul style="list-style-type: none">✓ ネットワークACLとセキュリティゲートウェイの違いなど、その特徴が問われる。✓ ネットワークACLの設定内容を確認する質問が出題される。
VPC内サービスへの接続	<ul style="list-style-type: none">✓ VPCに設置したAWSサービスへとアクセスする接続方式が問われる。✓ また、接続方式の設定方法が問われる。

VPCの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

サブネットによる構成	<ul style="list-style-type: none">✓ サブネットの構成方法が問われる。✓ パブリックサブネットとプライベートサブネットを利用した最適なAWSリソースの配置構成が問われる。
踏み台サーバー	<ul style="list-style-type: none">✓ 踏み台サーバーを設置した、プライベートサブネット内のリソースへのアクセス構成が問われる。
VPCフローログ	<ul style="list-style-type: none">✓ VPCフローログの役割に関する質問が出題される。
VPCにおけるDNSの使用	<ul style="list-style-type: none">✓ VPCにおいてDNSの名前解決が適用されるための設定が問われる。
Elastic IP	<ul style="list-style-type: none">✓ Elastic IPの役割や課金方式が問われる。

VPCの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

IPフローティング	✓ EC2インスタンスを切り替える際にダウンタイムを抑える仕組みとしてIPフローティングの利用方法が問われる。
ENI	✓ ENIの役割とアタッチ方式について問われる。

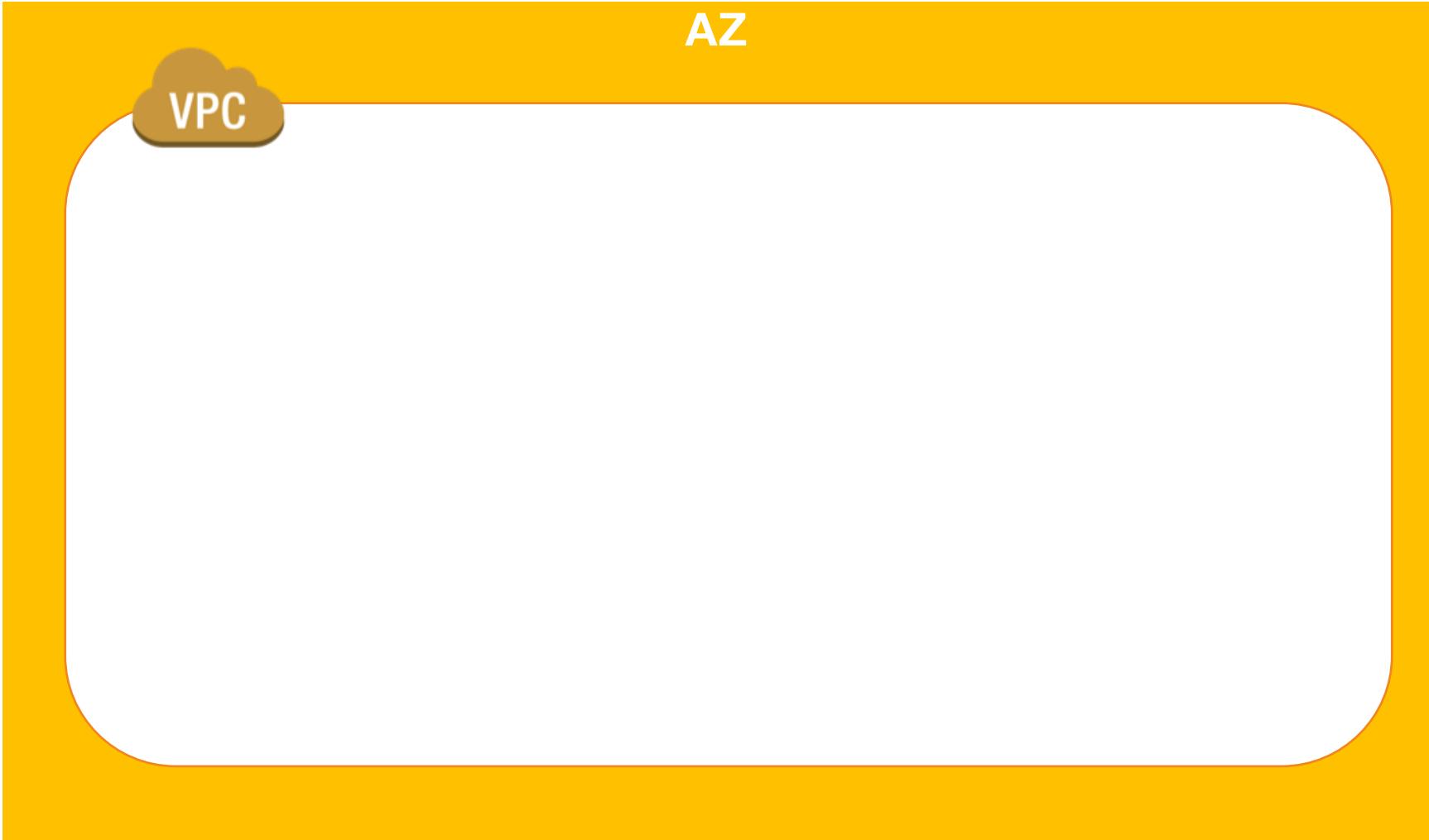
Virtual Private Cloud (VPC)

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 アドレス範囲を選択して仮想ネットワークを構築する
- ✓ 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により、仮想ネットワーキング環境を完全に制御できる。
- ✓ 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)

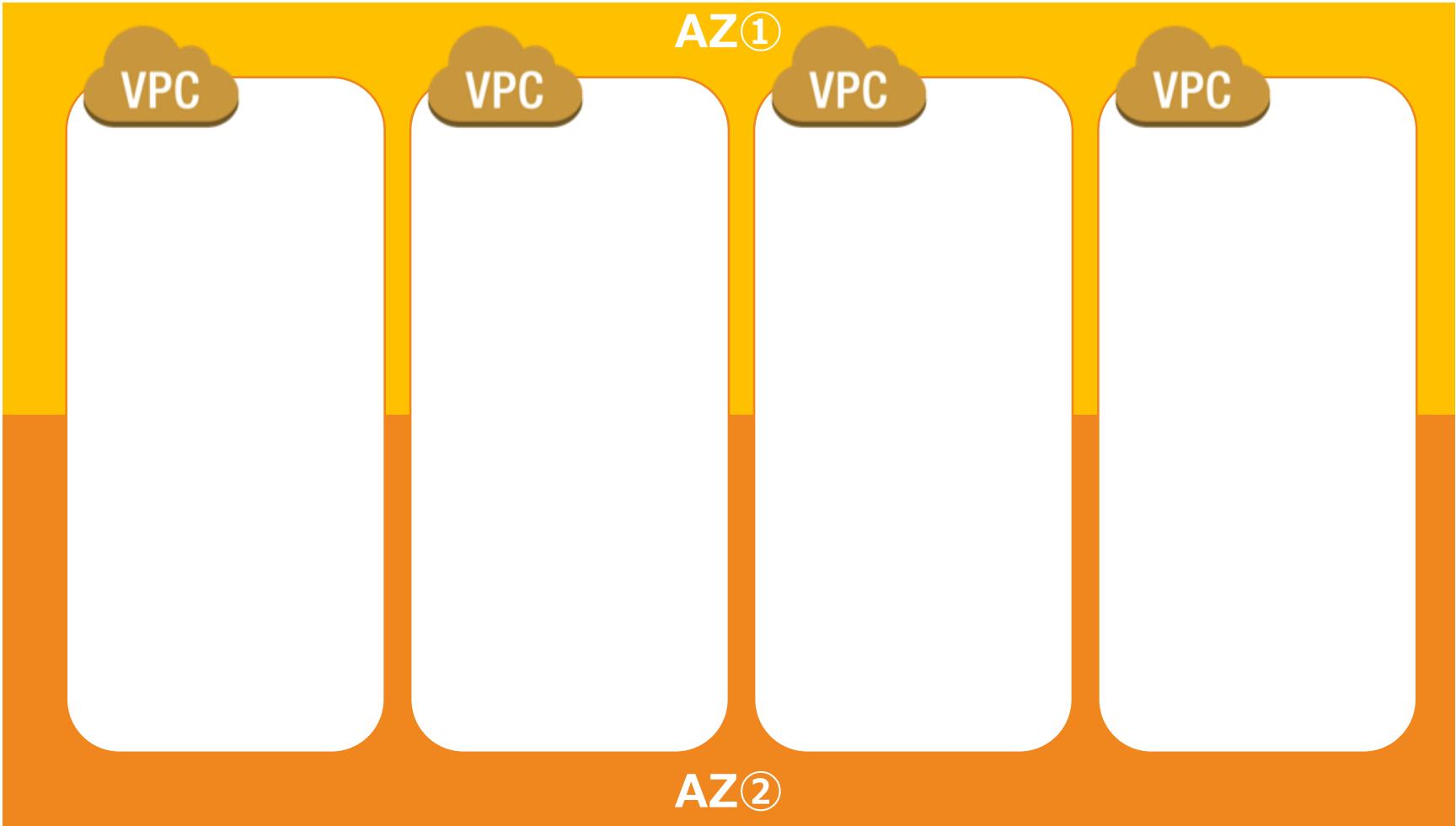
Virtual Private Cloud (VPC)

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



[Q] VPCの設定（デフォルトVPC）

あなたはAWSアカウントを新規に開設して、まずはEC2インスタンスを起動させました。VPCの構成をしていなかったため、このEC2インスタンスにはデフォルトVPCが設定されています。インスタンスにプライベートDNSホスト名とパブリックDNSホスト名の両方があることを確認する必要があります。

デフォルトVPCを利用した場合にDNSホスト名はどのように割り当てられますか？
(2つ選択してください)

- 1) デフォルト以外のVPCでは、初期設定ではプライベートDNSホスト名が割り当てられるが、パブリックDNSホスト名は割り当てられない。
- 2) デフォルト以外のVPCでは、パブリックDNSホスト名とプライベートDNSホスト名が割り当てられる。
- 3) デフォルト以外のVPCでは、必ずプライベートDNSホスト名が割り当てられるが、パブリックDNSホスト名は割り当てられない。
- 4) デフォルトVPCではパブリックDNSホスト名とプライベートDNSホスト名が割り当てられる。
- 5) デフォルトVPCではパブリックDNSホスト名とプライベートDNSホスト名が割り当てられない。

VPCの設定（デフォルトVPC）

AWSアカウントを作成すると、自動的に各リージョンに1つずつデフォルトVPCとデフォルトサブネットが生成される

- ✓ サイズ /16 の IPv4 CIDR ブロック (172.31.0.0/16) の VPC を作成する。これは、最大 65,536 個のプライベート IPv4 アドレスを提供する。
- ✓ 各アベイラビリティーゾーンに、サイズ /20 のデフォルトサブネットを作成する。この場合は、サブネットあたり最大 4,096 個のアドレスが作成され、その中のいくつかは Amazon が使用するように予約されている。
- ✓ インターネットゲートウェイを作成して、デフォルトVPCに接続する。
- ✓ デフォルトのセキュリティグループを作成し、デフォルトVPCに関連付ける。
- ✓ デフォルトのネットワークアクセスコントロールリスト (ACL) を作成し、デフォルトVPCに関連付ける。
- ✓ デフォルトVPC を備えた AWS アカウントにはデフォルトDHCPオプションセットを関連付ける
- ✓ パブリックとプライベートのDNSホスト名が付与される。

[Q] VPCの設定（VPC ウィザード）

あなたはAWSアカウントを新規に開設して、まずはVPCを構成することにしました。VPC ウィザードを使用することでよく利用される構成を迅速に設定することが可能です。パブリックなアクセスが必要なWebサーバー、セキュリティを高めるためにプライベートなアクセスに限定したデータベースサーバーを設置するためのネットワーク構成が必要です。あなたはVPC ウィザードを利用して目的の構成に一番近い構成を選択することにしました。

次の中で、VPC ウィザードでは選択できない構成はどれでしょうか？

- 1) 単一のパブリックサブネットを備えたVPC
- 2) 1つのパブリックサブネットと1つのプライベートサブネットを備えたVPC
- 3) 1つのパブリックサブネットと1つのプライベートサブネットにハードウェアVPNアクセスを備えたVPC
- 4) 1つのパブリックサブネットとハードウェアVPNアクセスを備えたVPC
- 5) 単一のプライベートサブネットにハードウェアVPNアクセスを備えたVPC

VPCの設定 (VPC ウィザード)

VPC ウィザードを利用することで、頻繁に利用される VPC 構成を瞬時に構成することができる。

ステップ 1: VPC 設定の選択

1 個のパブリックサブネットを持つ VPC

パブリックとプライベートサブネットを持つ VPC

パブリックとプライベートサブネットおよびハードウェア VPN アクセスを持つ VPC

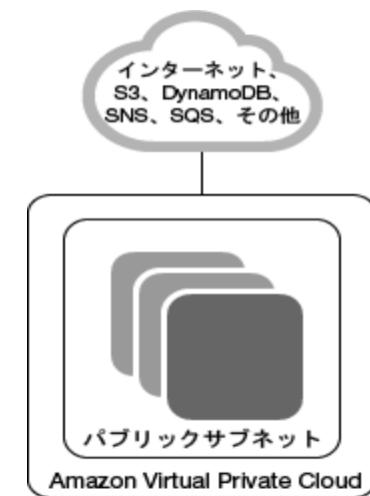
プライベートのサブネットのみで、ハードウェア VPN アクセスを持つ VPC

インターネットに直接アクセスできる AWS クラウドの分離されたプライベート空間でインスタンスは実行されます。インスタンスのインバウンドおよびアウトバウンドのネットワークトラフィックを厳重に管理するには、ネットワークアクセス ACL とセキュリティグループを使用します。

作成:

/24 サブネットを持つ /16 ネットワークです。パブリックサブネットインスタンスは Elastic IP またはパブリック IP を使用してインターネットにアクセスします。

選択



VPCの設定：通常の設定

VPCウィザードを利用しない場合は、VPCを作成、サブネットを作成と1つずつ作成する。

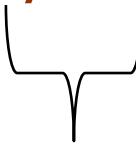


CIDR (Classless Inter-Domain Routing)

サブネットマスクの値を設定し、同じネットワーク範囲として扱う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桁目までのIPアドレスを固定

[Q]サブネットマスクの設定

あなたは新しくVPCを設定して、パブリックサブネットを2つ、プライベートサブネットを2つ設定してITインフラを設置しようと考えています。単一のVPC内でのIPv4アドレス指定およびサブネット作成に対して、CIDRを設定する必要があります。CIDRの設定として200個のIPアドレスを利用できるようにする必要があります。

CIDRのサブネットマスク指定として、多すぎず最適なIPアドレス数となる設定を選択してください。

- 1) /21
- 2) /22
- 3) /23
- 4) /24

CIDR

VPCは/16 ~ /28のCIDR範囲を使用できる

/16 ~ /28

CIDR

CIDRに/16を設定した際に設定可能となるサブネット数とIPアドレス数の組合せ（AWS管理IPの5つを引いたもの）

サブネットマスク	サブネット数	サブネット当たりのIPアドレス数 (AWSで利用可能な)
/18	4	16379
/20	16	4091
/22	64	1019
/24	256	251
/26	1024	59
/28	4096	11

CIDR

既にAWS側で利用されており、設定できないアドレスもある
(/24の例)

ホストアドレス	用途
.0	ネットワークアドレス
.1	VPCルータ
.2	Amazonが提供するDNSサービス
.3	AWSで予約されているアドレス
.255	ブロードキャストアドレス

[Q]サブネットの作成

あなたはAWSアカウントを新規に開設して、まずはVPCを構成することにしました。VPCウィザードを使用することでよく利用される構成を迅速に設定することが可能です。パブリックなアクセスが必要なWebサーバー、セキュリティを高めるためにプライベートなアクセスに限定したデータベースサーバーを設置するためのネットワーク構成が必要です。

Amazon VPCのサブネットに関して正しい説明は次のうちどれですか？（2つ選択してください。）

- 1) 各サブネットは単一のアベイラビリティーゾーンに設定される。
- 2) 各サブネットは複数のアベイラビリティーゾーンに設定可能である。
- 3) 各サブネットは、VPCのメインルートテーブルに自動的に関連付けられる。
- 4) 各サブネットは、サブネットのメインルートテーブルが設定され、そのルートテーブルがVPCに自動的に関連付けられる。
- 5) 各サブネットはインターネットゲートウェイがデフォルトで構成される。

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

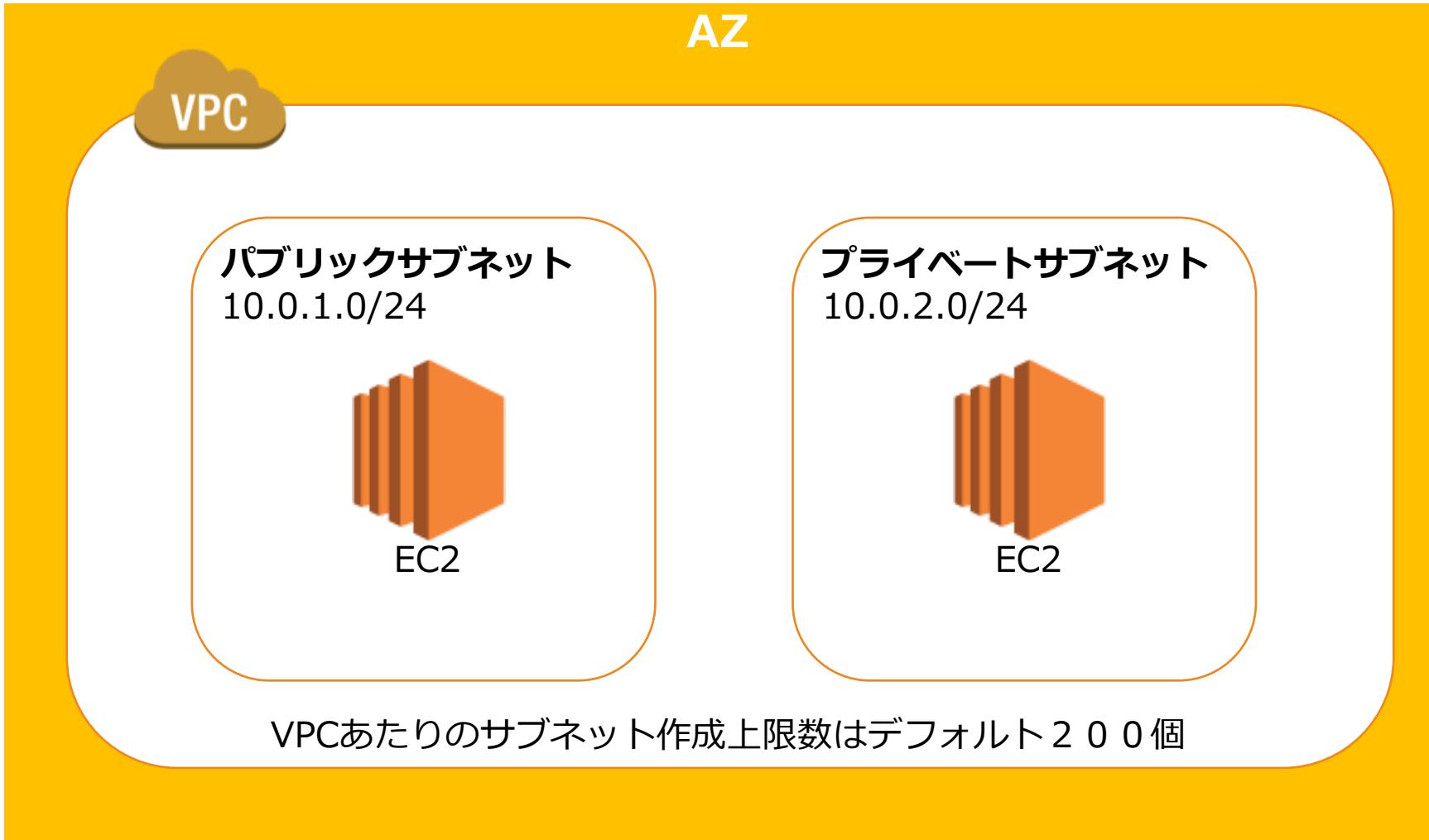
プライベートサブネット
10.0.2.0/24



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

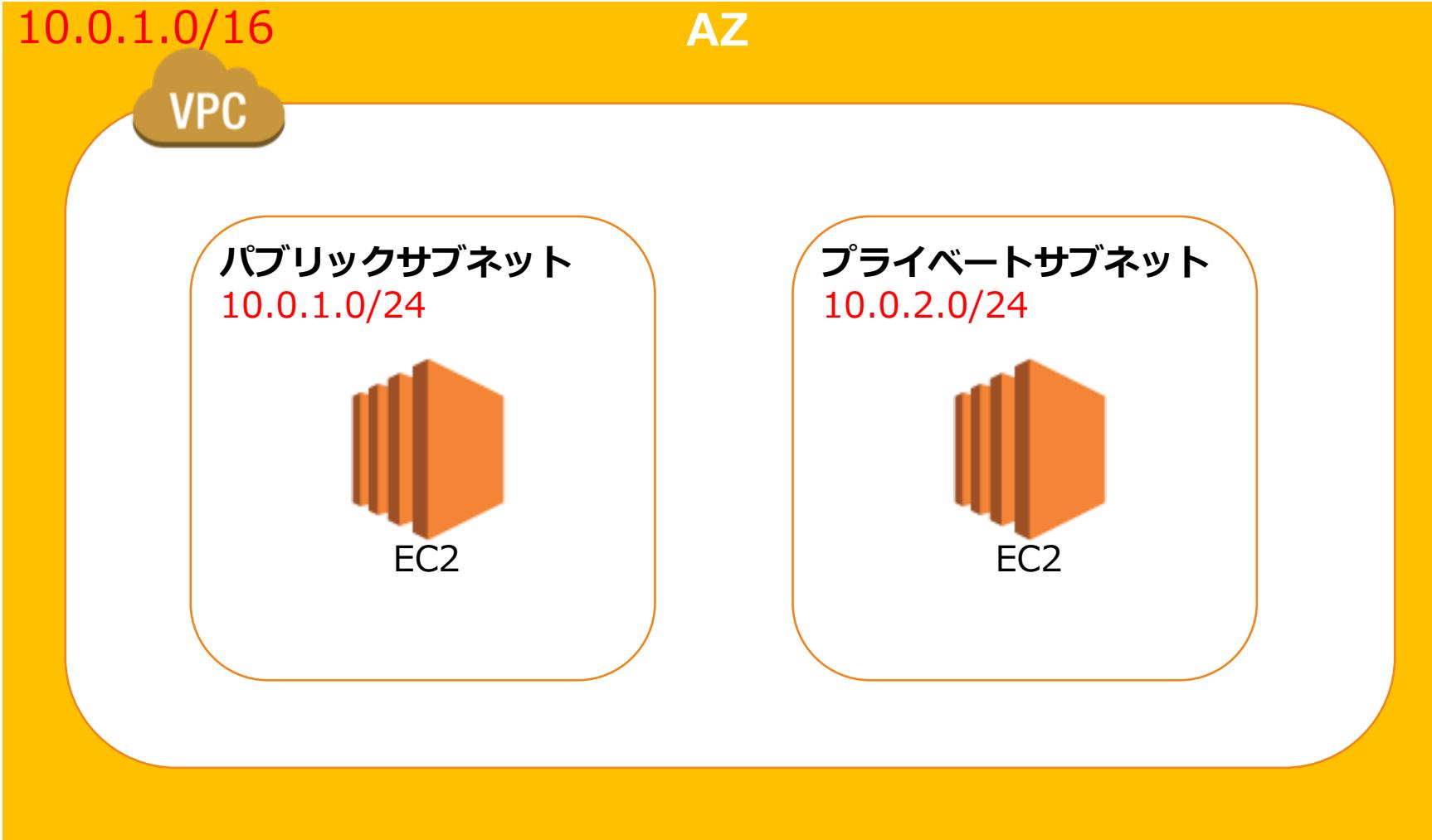
サブネット

サブネットはVPC内の複数設置でき、1つのAZを指定して配置される。パブリックとプライベートがある。



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、ネットワークレンジが決まる。



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

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

ルートテーブル > ルートの編集

ルートの編集

送信先	ターゲット	ステータス	伝播済み
172.31.0.0/16	local	active	いいえ
0.0.0.0/0	igw-80b29de4	active	いいえ

[ルートの追加](#)

* 必須

[キャンセル](#) [ルートの保存](#)

[Q] ゲートウェイの設定

あなたは新しくVPCを設定して、パブリックサブネットを2つ、プライベートサブネットを2つ設定してインフラを設置しようと考えています。構成したプライベートサブネットにあるインスタンスはIPv6プロトコルを使用してインターネットからホストに接続する必要があります。その際に、インターネットからのアクセスは拒否しつつ、インターネット側へのトラフィックは通せるようにします。

この接続を有効にするには、どの仕組みを設定することが必要ですか？（2つ選択してください。）

- 1) Egress-Onlyインターネットゲートウェイ
- 2) インターネットゲートウェイ
- 3) NATゲートウェイ
- 4) カスタマーゲートウェイ

ゲートウェイの設定

VPCコンソールで作成・管理できるゲートウェイは以下の通り

インターネット ゲートウェイ	✓ インターネットへの出入り口となるゲートウェイで、デフォルトゲートウェイとして利用されることが多い
NATゲートウェイ	✓ プライベートサブネットのリソースからインターネットへのトラフィックを可能にするためのゲートウェイ
Egress-Only Internet Gateway	✓ IPv6向けのインターネットゲートウェイ ✓ IPv6 経由での VPC からインターネットへの送信を可能にし、インターネットからのインスタンスへの接続は防ぐ
カスタマーゲートウェイ	✓ オンプレミス環境と接続する際に利用するゲートウェイ ✓ カスタマーゲートウェイデバイスまたはソフトウェアアプリケーションに関する情報を AWS に提供する
仮想プライベート ゲートウェイ	✓ 仮想プライベートゲートウェイは、VPN トンネルの Amazon 側にあるルーター ✓ VPN接続時に利用する

[Q]インターネットゲートウェイ

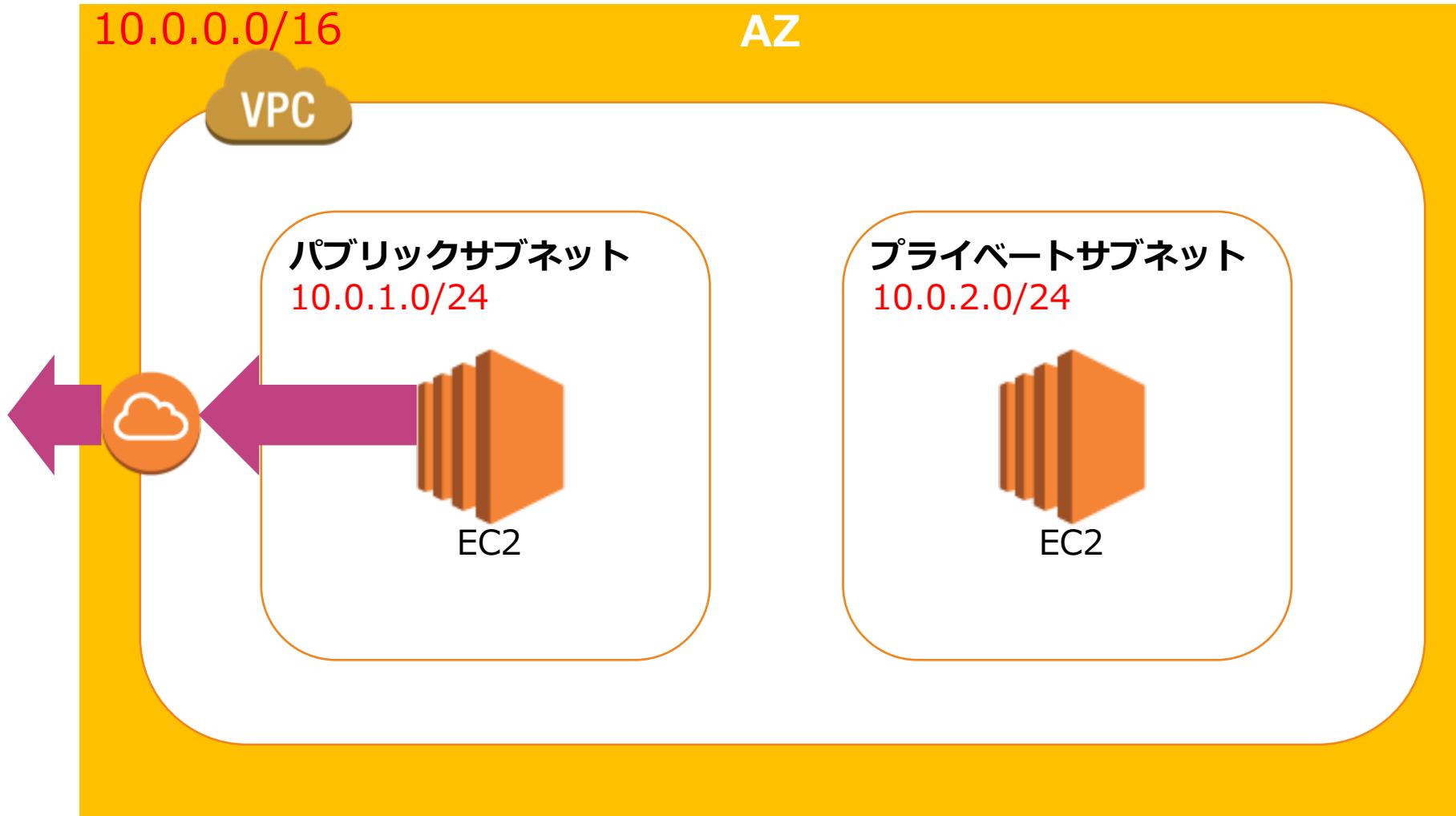
あなたは新しくVPCを設定して、パブリックサブネットを1つ、プライベートサブネットを1つ設定してインフラを設置しようと考えています。IPv4アドレスを利用してインターネットへのアクセスを許可するためには、サブネットにパブリックサブネットとして機能させる設定が必要です。

パブリックサブネットに必要な設定はどれでしょうか？

- 1) Egress-Onlyインターネットゲートウェイへのルートを設定する。
- 2) インターネットゲートウェイへのルートを設定する。
- 3) NATゲートウェイへのルートを設定する。
- 4) カスタマーゲートウェイへのルートを設定する。

インターネットゲートウェイ

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



インターネットゲートウェイ

ルートテーブルによりインターネットゲートウェイへのルートを確立する。

- インターネットゲートウェイをVPCに設置する。
- パブリックサブネットのルートテーブルにインターネットゲートウェイへの経路を設定する。

[Q] NATゲートウェイ

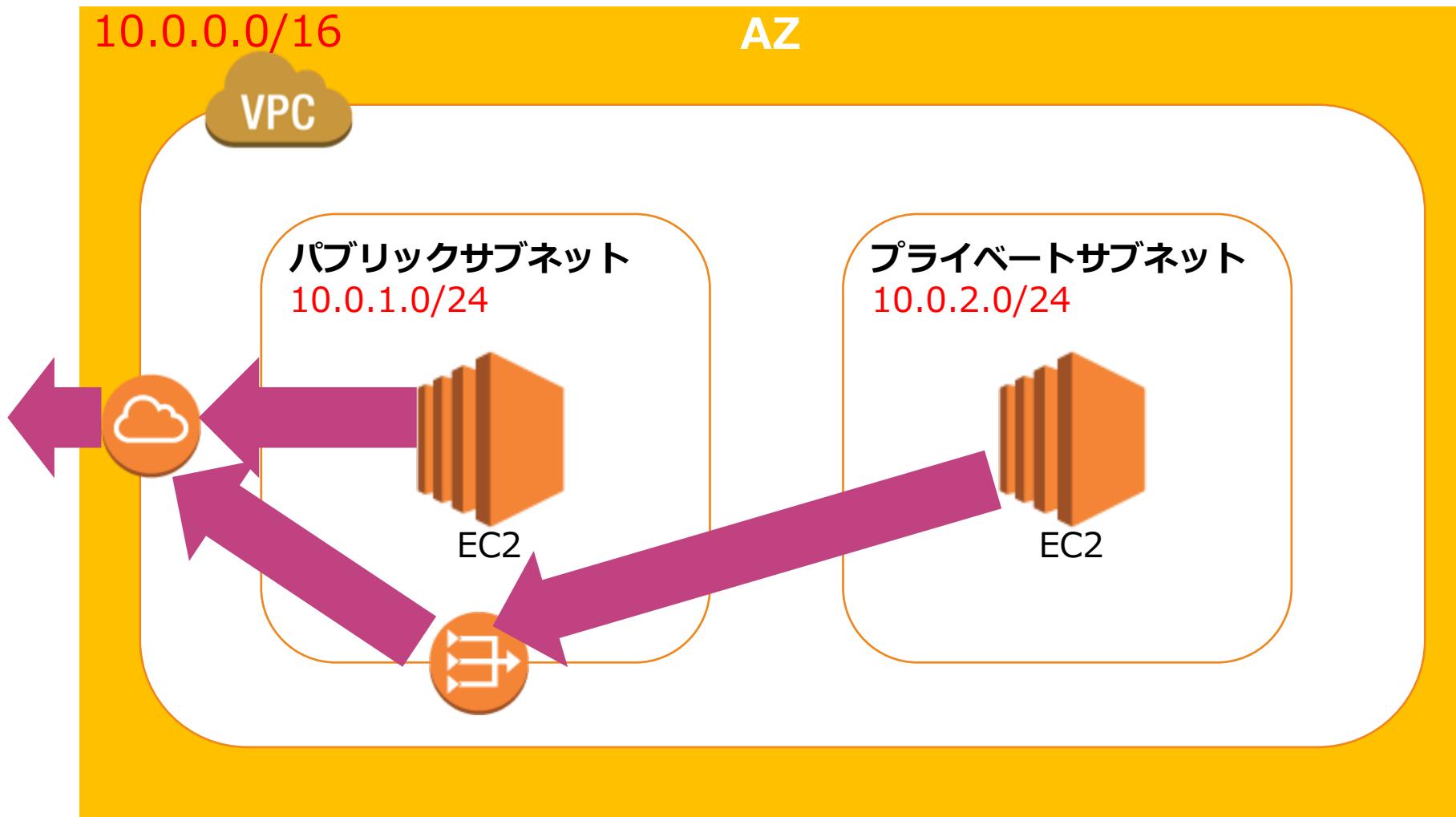
あなたの会社はニュースメディア配信アプリケーションをAWSにホストしています。このアプリケーションはバックエンドサーバーが1つのAZで利用されていることや、NATゲートウェイも同じAZのみに展開されていることが問題となっています。

この問題を解決する最適なAWSアーキテクチャ構成を選択してください。（2つ選択してください）

- 1) 1つのAZにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネットに設置する。
- 2) 2つのAZにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネット設置する。
- 3) 2つのAZにおいてパブリックサブネットとプライベートサブネットを構成して、NATインスタンスを各パブリックサブネットに設置する。
- 4) 各AZにおいてプライベートサブネットからNATゲートウェイ（またはNATインスタンス）にルートを設定する。
- 5) 1つのプライベートサブネットと1つのNATゲートウェイ（またはNATインスタンス）をセットにして、ルートを設定する。

NATゲートウェイ

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



NATゲートウェイ

ルートテーブルによりインターネットゲートウェイへのルートを確立する。

- NATゲートウェイをパブリックサブネットに設置する。
- プライベートサブネットのルートテーブルにNATゲートウェイへの経路を設定する。

[Q] NATインスタンス

あなたは新しくVPCを設定して、パブリックサブネットを2つ、プライベートサブネットを2つ設定してインフラを設置しようと考えています。現在、プライベートサブネットのインスタンスがインターネットへのアウトバウンドIPv4トラフィックを開始できる構成を設定しているところです。そのためにNATインスタンスを構成することが必要です。

NATインスタンスの特徴として正しい説明はどれでしょうか？（3つ選択してください）

- 1) セキュリティグループによりNATインスタンスのトラフィックを制御できる。
- 2) ネットワークACLによりNATインスタンスのトラフィックを制御できる。
- 3) NATインスタンスはポート転送が利用できる。
- 4) NATインスタンスはAWS側で管理されている。
- 5) NATインスタンスはインスタンスタイプは選択できない。

NATインスタンス

NATゲートウェイはAWS側でマネージド型で提供されており、NATインスタンスに比較して冗長性も高く、管理が楽である

ポイント	NATゲートウェイ	NATインスタンス
現在利用できるリージョン	高可用性。各アベイラビリティーゾーンの NAT ゲートウェイは冗長性を持たせて実装されます。アベイラビリティーゾーンごとに NAT ゲートウェイを作成し、ゾーンに依存しないアーキテクチャにします。	スクリプトを使用してインスタンス間のフェイルオーバーを管理します。
帯域幅	45 Gbps まで拡張できます。	インスタンスタイプの帯域幅に依存します。
メンテナンス	AWS によって管理されます。	ユーザーが管理します
パフォーマンス	ソフトウェアは NAT トラフィックを処理するように最適化されます。	一般的な Amazon Linux AMI が NAT を実行するように設定されます。
Cost	NAT ゲートウェイの使用数、使用期間、NAT ゲートウェイを通じて送信するデータの量に応じて課金されます。	NATインスタンスの使用数、使用期間、インスタンスタイプとサイズに応じて課金されます。
タイプおよびサイズ	一律提供で、タイプやサイズを決める必要はありません。	予測されるワークロードに応じて適切なインスタンスタイプとサイズを選択
パブリック IP アドレス	作成時に NAT ゲートウェイに関連付ける Elastic IP アドレスを選択します。	NAT インスタンスで Elastic IP アドレスまたはパブリック IP アドレスを使用します。
プライベート IP アドレス	ゲートウェイの作成時にサブネットの IP アドレス範囲から自動的に選択	インスタンスの起動時にサブネットの IP アドレス範囲から特定のプライベート IP アドレスを割り当てます。
セキュリティグループ	NAT ゲートウェイに関連付けることはできません。	セキュリティグループでトラフィックをコントロール可能
ネットワーク ACL	ネットワーク ACL を使用して、設置されたサブネットに出入りするトラフィックをコントロールします。	
フローログ	フローログを使用してトラフィックをキャプチャします。	
ポート転送	サポート外。	設定を手動でカスタマイズしてポート転送をサポートします。
踏み台サーバー	サポート外。	踏み台サーバーとして使用します。
タイムアウト動作	接続がタイムアウトになると、NAT ゲートウェイは、NAT ゲートウェイの背後で接続を継続しようとするリソースすべてに RST パケットを返します (FIN パケットは送信しません)。	接続がタイムアウトになると、NAT インスタンスは、接続を閉じるために、NAT インスタンスの背後にあるリソースに FIN パケットを送信します。
IP フラグメント化	UDP プロトコルの IP フラグメント化されたパケットの転送をサポートします。	TCP、UDP、ICMP プロトコルの IP フラグメント化されたパケットの再アセンブルをサポートします。

[Q] VPCエンドポイント

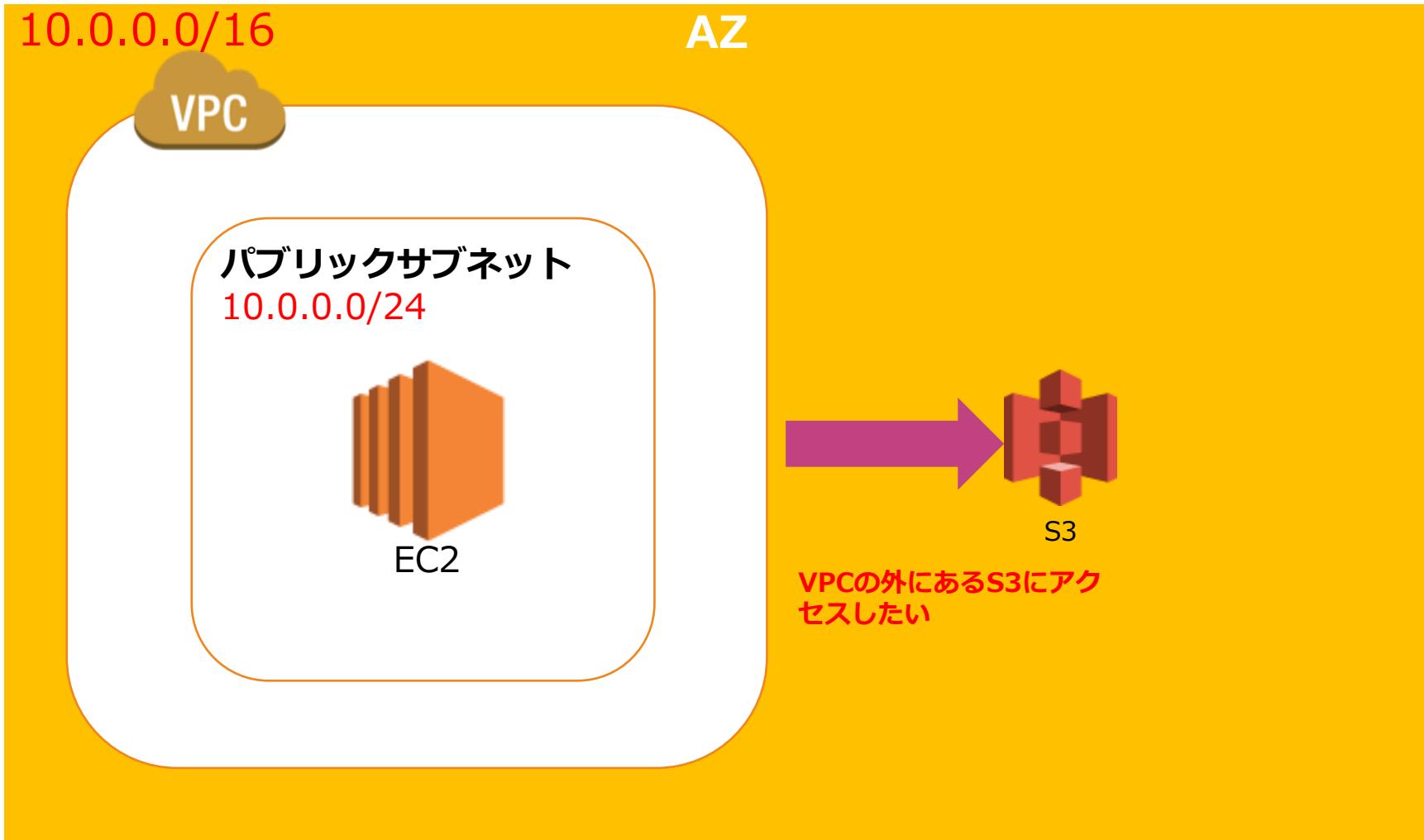
あなたはソリューションアーキテクトとして、VPC内のEC2インスタンスからVPC外に構成されているDynamoDBへとアクセスする設定をしています。インスタンスは、DynamoDBへのAPI呼び出しを行う必要があり、セキュリティポリシーに従ってAPI呼び出しがインターネットを通過しないようにする必要があります。

この要件を達成する設定方法として正しい設定はどれでしょうか？

- 1) ゲートウェイエンドポイントを作成して、エンドポイントのルートテーブルエントリを設定する。
- 2) インターフェースエンドポイントを作成して、エンドポイントのルートテーブルエントリを設定する。
- 3) プライベート型エンドポイントを作成して、エンドポイントのルートテーブルエントリを設定する。
- 4) VPCの各サブネットにエンドポイントのENIを作成する。
- 5) VPCとDynamoDBの間にVPCピアリング接続を作成する。

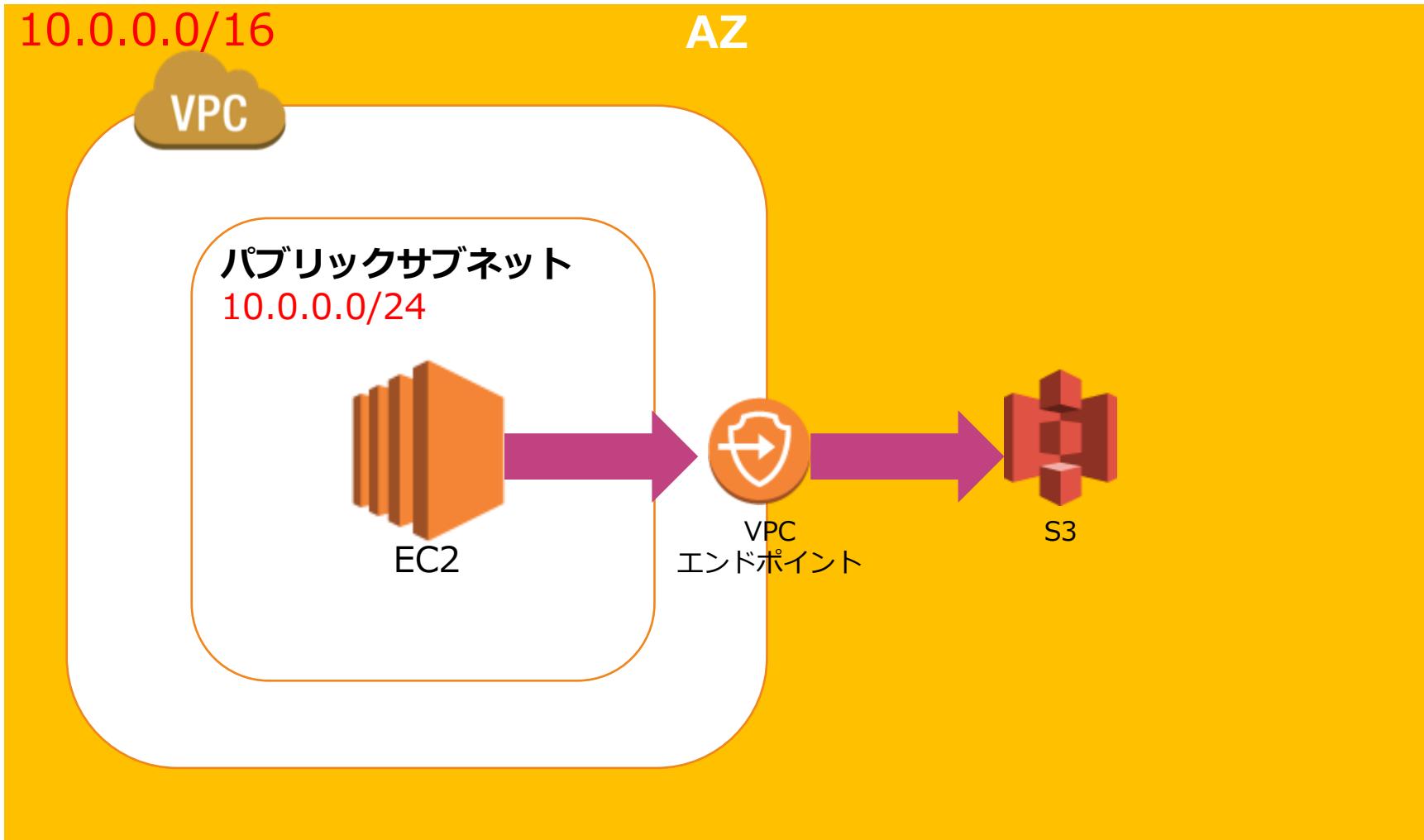
VPCエンドポイント

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

ゲートウェイ型はS3とDynamoDBのみに適用され、多くのサービスはプライベートリンク（インターフェース）を利用

ゲートウェイ型 エンドポイント

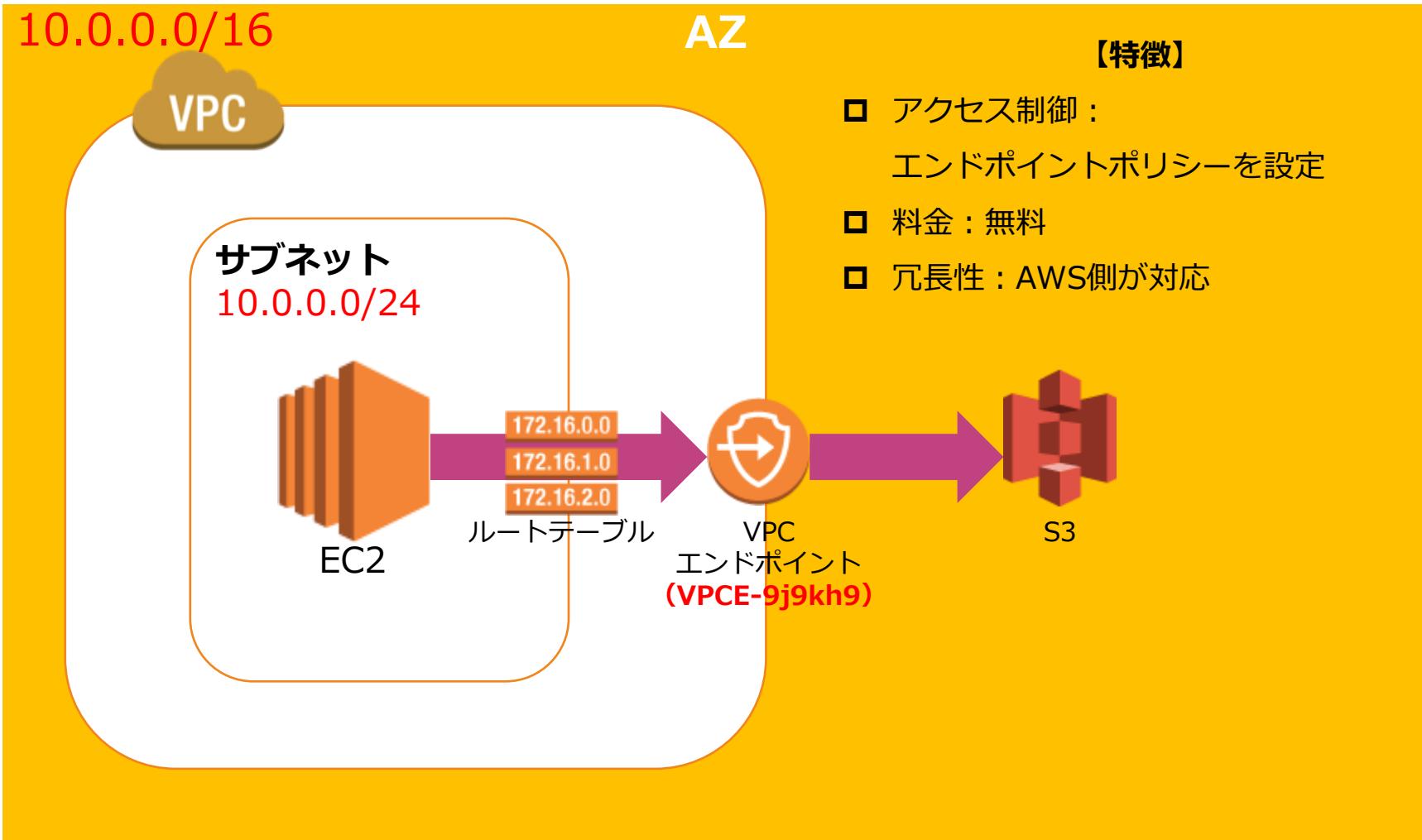
- ✓ サポートされる AWSサービスを宛先とするトラフィックのルートテーブルの宛先として指定できるゲートウェイ
- ✓ DynamoDBとS3のみに適用可能

プライベートリンク型 エンドポイント (インターフェース型)

- ✓ サポートされるサービスを宛先とするトラフィックのエントリーポイントとして機能するサブネットの IP アドレス範囲のプライベート IP アドレスを持つ Elastic Network Interface
- ✓ プライベート IP アドレスを使用してサービスにプライベートにアクセスする。
- ✓ AWS PrivateLink は、VPC とサービス間のすべてのネットワークトラフィックを Amazon ネットワークに制限
- ✓ RDS、EC2などの多くのAWSサービスに適用可能

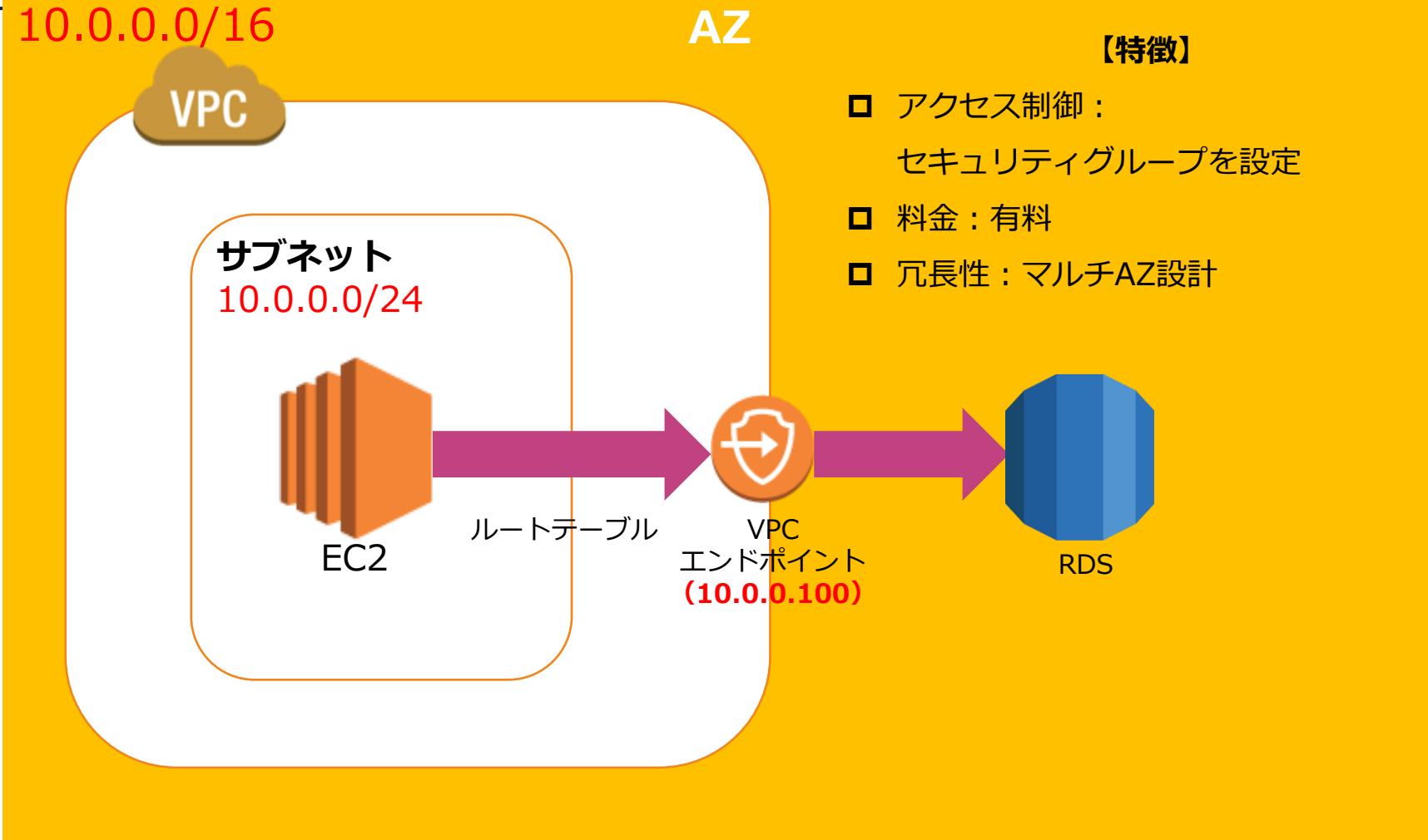
VPCエンドポイント

ゲートウェイ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

プライベートリンク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



[Q] VPCピアリング

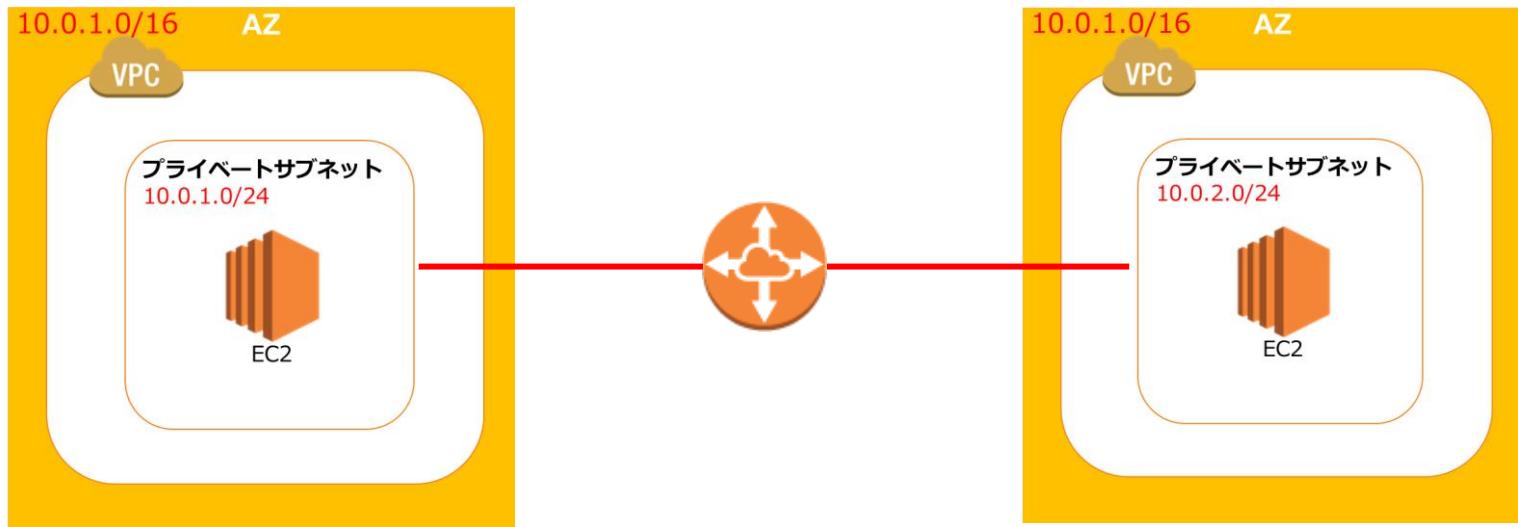
あなたの会社は複数のリージョンに複数のアプリケーションを展開しています。それぞれ別々のVPCを利用していますが、アプリケーション同士を連携することが必要となっています。VPCが異なるアプリケーションが相互に通信できるように、これらのVPCを接続する必要があります。

このユースケースで最も費用効果の高いソリューションは次のうちどれですか？

- 1) VPCピアリング接続を使用する
- 2) インターネットゲートウェイを使用する
- 3) VPN接続を使用する
- 4) Direct Connectを使用する

VPC Peering

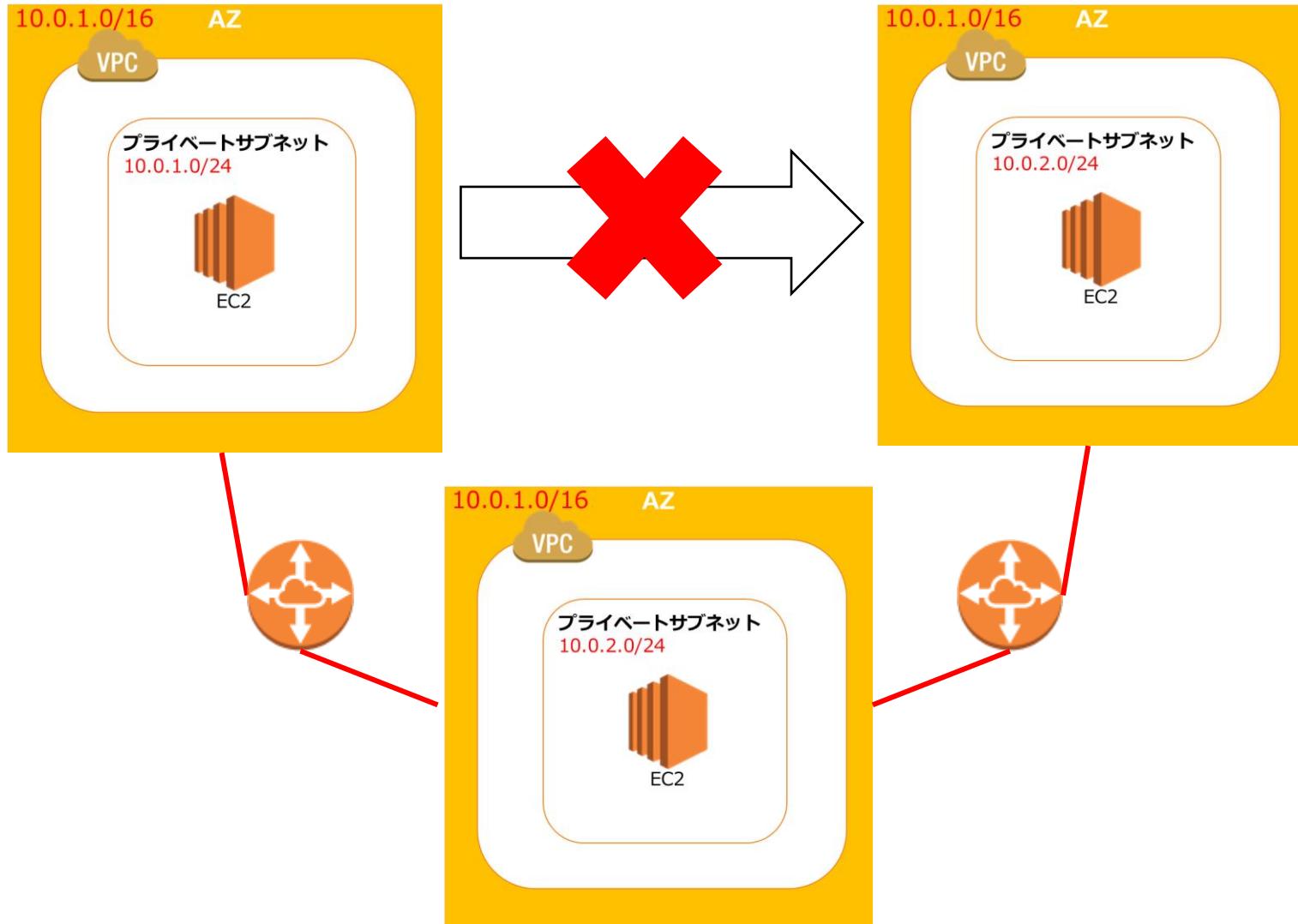
VPC peeringにより2つのVPC間でのトラフィックルーティングが可能



- 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

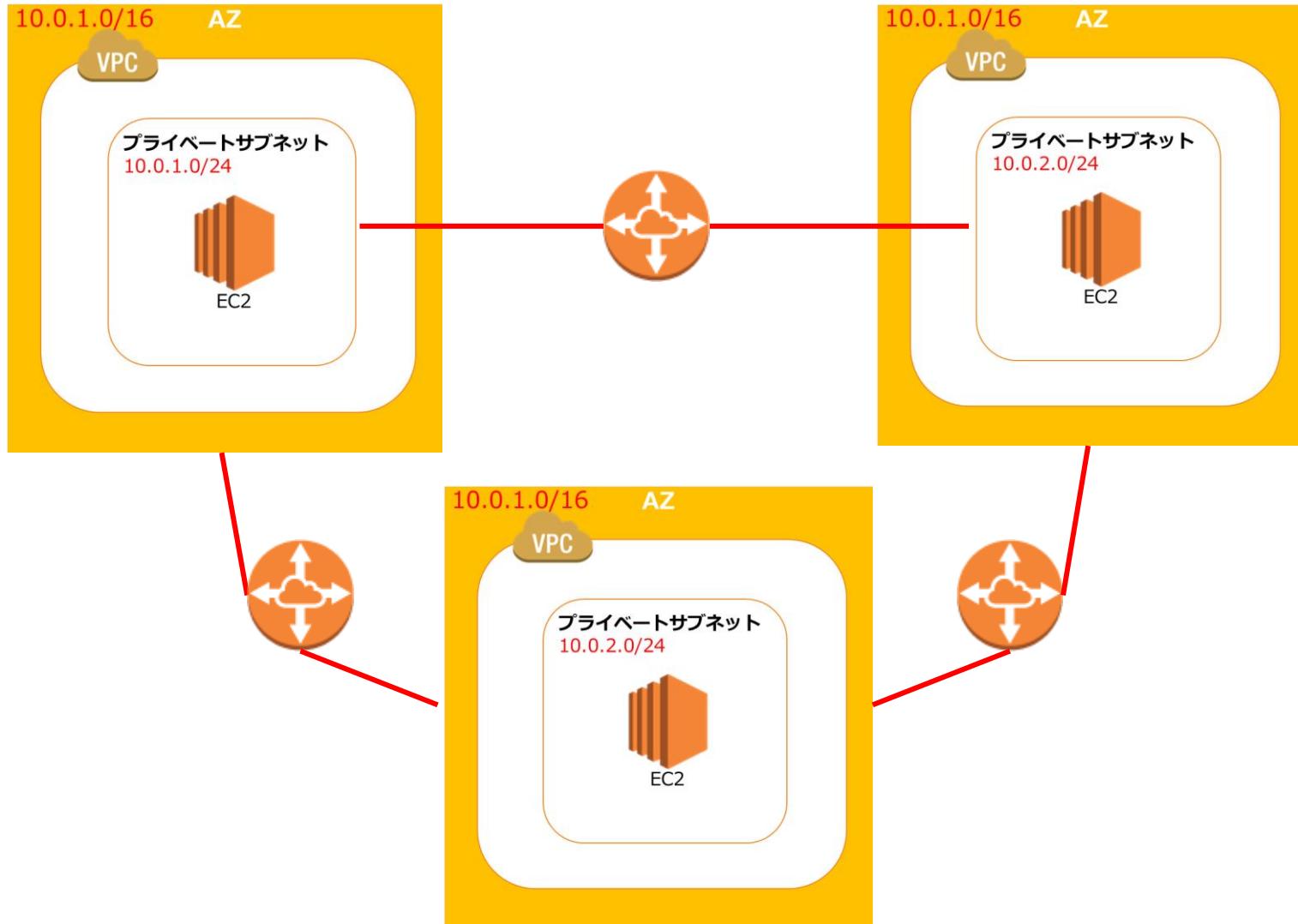
VPC Peering

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



[Q]ネットワークACL

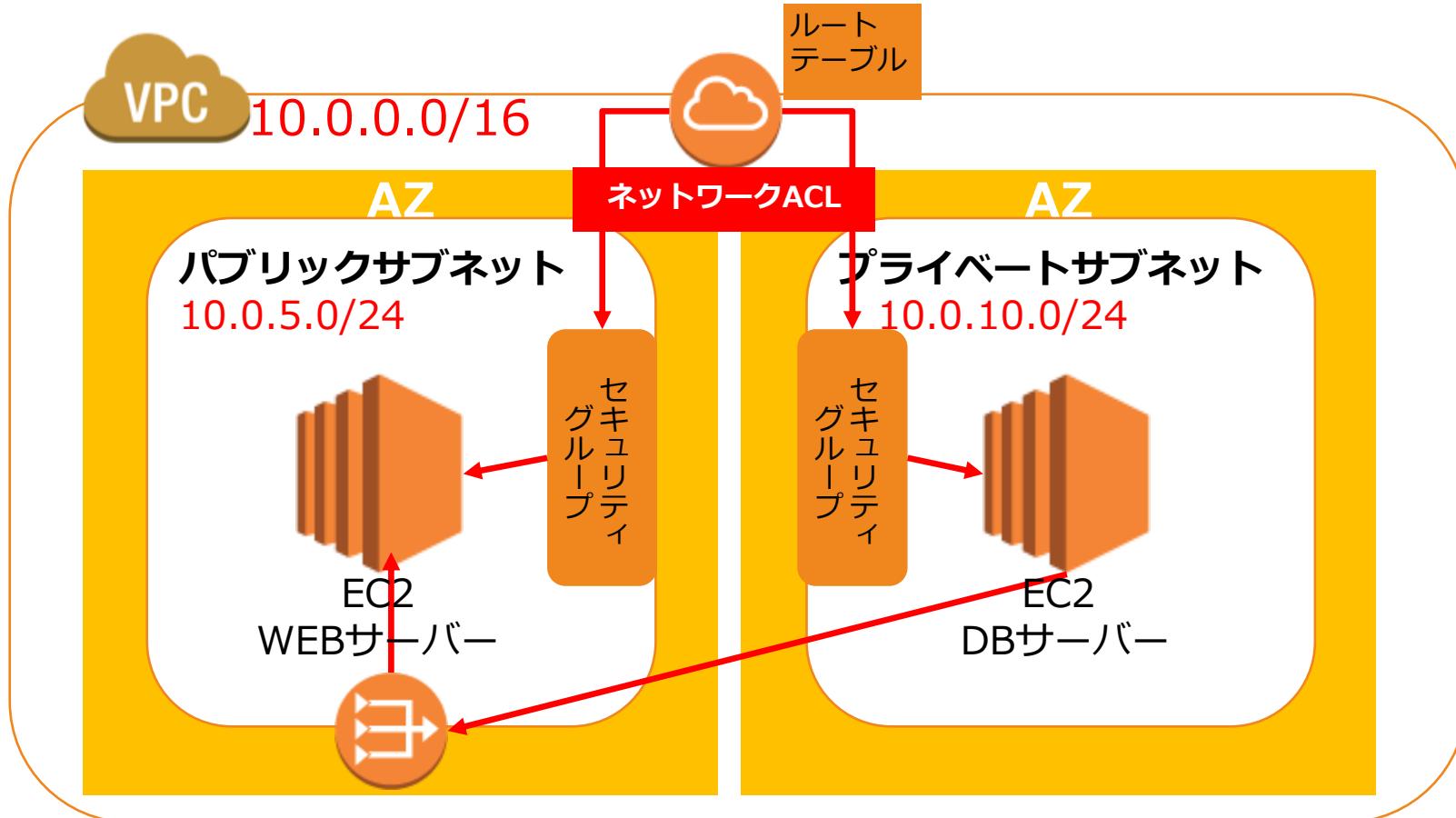
あなたの会社はAWSを利用したWEBアプリケーションを運用しています。最近になって不正アクセスを試みるようなトラフィックが急増しています。いくつかの固定されたIPアドレスから不正アクセスが試みられているようです。このリクエストは同じCIDR範囲内の異なるIPアドレスからの実施されているようです。

このアクセスに対して直接効果がある保護策を選択してください。

- 1) ネットワークACLのインバウンドテーブルにおいて、他のルールよりも小さいルール番号で該当するCIDRを拒否する。
- 2) ネットワークACLのアウトバウンドテーブルにおいて、他のルールよりも小さいルール番号で該当するCIDRを拒否する。
- 3) セキュリティグループのインバウンドテーブルにおいて、他のルールよりも小さいルール番号で該当するCIDRを拒否する。
- 4) セキュリティグループのアウトバウンドテーブルにおいて、他のルールよりも小さいルール番号で該当するCIDRを拒否する。

ネットワークACL

ネットワークACLによるアクセス制御を追加する



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

[Q]ネットワークACL

あなたはVPCを構築して、2つのサブネットを作成しました。現在は、ネットワークACLの設定を行っているところです。その際には、VPCを設置した際に設定されるデフォルトのネットワークACLを利用する予定です。

ネットワークACLのデフォルト設定に関する正しい説明は次のうちどれですか。（2つ選択してください）

- 1) すべてのトラフィックを拒否するデフォルトのインバウンドルールが設定されている。
- 2) すべてのトラフィックを拒否するデフォルトのアウトバウンドルールが設定されている。
- 3) すべてのトラフィックを許可するデフォルトのインバウンドルールが設定されている。
- 4) すべてのトラフィックを許可するデフォルトのアウトバウンドルールが設定されている。
- 5) インターネットゲートウェイへのトラフィックを許可するデフォルトのアウトバウンドルールがある。

ネットワークACL

ネットワークのデフォルトの構成はデフォルトとカスタムで異なる

VPCに最初に設定される
デフォルトNACL

- ✓ 全てのインバウンドトラフィックを許可する設定がされている。
- ✓ 全てのアウトバウンドトラフィックを許可する設定がされている。

カスタムで作成する
NACLのデフォルト設定

- ✓ 全てのインバウンドトラフィックを拒否する設定がされている。
- ✓ 全てのアウトバウンドトラフィックを拒否する設定がされている。

[Q]ネットワークACLの設定

あなたはVPCを構築して、2つのサブネットを作成しました。現在は、ネットワークACLの設定を行っているところです。

The screenshot shows the AWS Network ACL inbound rules editor. The title bar says "ネットワーク ACL > インバウンドのルールの編集". The main heading is "インバウンドのルールの編集". Below it, it says "ネットワーク ACL acl-326cbd54". A table lists three rules:

ルール #	タイプ	プロトコル	ポート範囲	送信元	許可 / 拒否
98	HTTP (80)	TCP (6)	80	121.103.215.159/32	DENY
99	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW

At the bottom left is a "ルールの追加" button, and at the bottom center is a note "* 必須".

このネットワークACLが適用されたサブネットにあるWEBサーバーに121.103.215.159からアクセスがあった場合にどのようにになりますか？

- 1) 121.103. 215.159からのSSH接続が許可される。
- 2) 121.103. 215.159からのSSH接続が拒否される。
- 3) 121.103. 215.159からHTTP経由でのWEBサイトにアクセスできる。
- 4) 121.103. 215.159からHTTP経由でのWEBサイトにアクセスできない。
- 5) 121.103. 215.159からHTTPS経由でのWEBサイトにアクセスできる。

ネットワークACLの設定

トライ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

ネットワーク ACL > インバウンドのルールの編集

インバウンドのルールの編集

ネットワーク ACL acl-326cbd54

ルール #	タイプ	プロトコル	ポート範囲 <small>i</small>	送信元 <small>i</small>	許可 / 拒否
98	HTTP (80)	TCP (6)	80	121.103.215.159/32	DENY
99	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW

[ルールの追加](#)

* 必須

[Q]サブネットによる構成

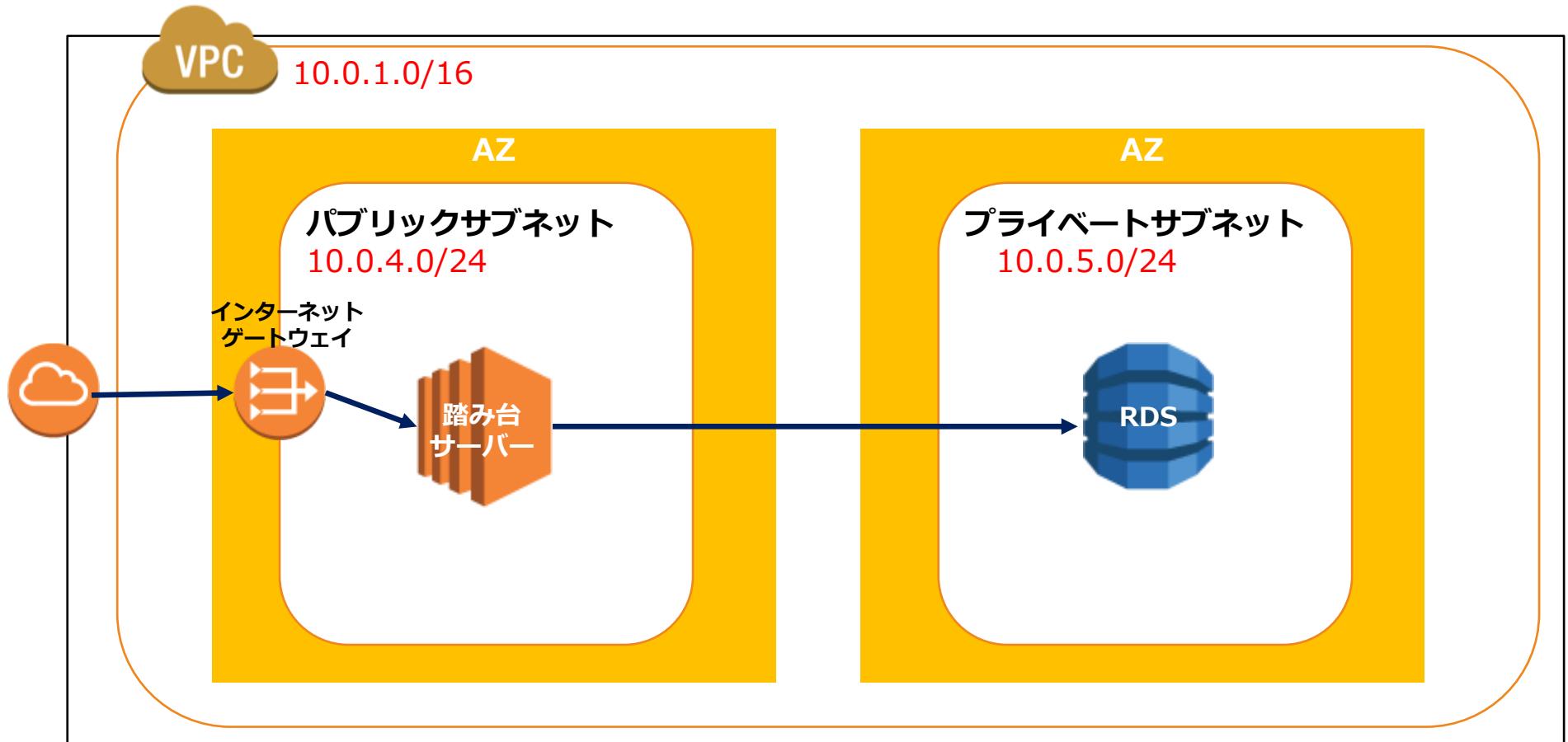
あなたはAWSにWEBアプリケーションをホストすることを計画しています。まずはVPCを作成して、パブリックサブネットにWEBサーバーとなるEC2インスタンスを起動しました。さらにMySQLデータベースをホストする別のEC2インスタンスを別のサブネットに設置して、WEBサーバーから接続します。

安全性を考慮すると、どのようにデータベースをセットアップするべきでしょうか。
(2つ選択してください。)

- 1) データベースサーバーをプライベートサブネットに配置する。
- 2) データベースサーバーをパブリックサブネットに配置する。
- 3) セキュリティグループでWEBサーバーのIPアドレスを指定して、MySQLからのポート番号のみを許可する設定をDB側のインスタンスに設定する。
- 4) セキュリティグループでWEBサーバーのIPアドレスを指定して、MySQLからのポート番号のみを許可する設定をWEBサーバー側のインスタンスに設定する。
- 5) IAMデータベース認証でWEBサーバーのIPアドレスを指定して、MySQLからのポート番号のみを許可する設定をWEBサーバー側のインスタンスに設定する。

サブネットによる構成

セキュリティを高めたいサービスはプライベートサブネットに設置する



[Q] VPC内サービスへの接続：SSH

あなたはAWSアカウントを新規に開設して、まずはVPCを構成することにしました。VPCウィザードを使用することでよく利用されるVPC構成を迅速に設定することが可能です。セキュリティを高めるためにプライベートなアクセスに限定したデータベースサーバーを設置するためのネットワーク構成が必要です。パブリックサブネットに踏み台サーバーを設定して、SSH経由で企業データセンターからのみアクセスする必要があります。

これを達成するための最適な方法はどれでしょうか？（2つ選択してください。）

- 1) パブリックサブネットにEC2インスタンスを起動する。
- 2) プライベートサブネットにEC2インスタンスを起動する。
- 3) 企業データセンターのIPアドレスを介したポート22でのアクセスのみを許可するセキュリティグループをインスタンスに付与して、Pemキーでアクセスを実施する。
- 4) 企業データセンターのIPアドレスを介したポート22でのアクセスのみを許可するセキュリティグループをインスタンスに付与して、アクセスキーでアクセスを実施する。
- 5) 企業データセンターのIPアドレスを介したポート22でのアクセスのみを許可するセキュリティグループをインスタンスに付与して、ユーザーIDとパスワードでアクセスを実施する。

[Q] VPC内サービスへの接続：RDP

あなたはAWSアカウントを新規に開設して、まずはVPCを構成することにしました。セキュリティを高めるためにプライベートなアクセスに限定したWEBサーバーを設置する予定です。Microsoftリモートデスクトッププロトコル（RDP）アクセスを備えた踏み台サーバーを利用して、すべてのインスタンスへの管理アクセスを制限したいと考えています。

次の踏み台サーバーの設定をどのように実施するべきでしょうか？（2つ選択してください。）

- 1) パブリックサブネットにElasticIPアドレスを設定したEC2インスタンスを起動する。
- 2) プライベートサブネットにElasticIPアドレスを設定したEC2インスタンスを起動する。
- 3) パブリックサブネットにパブリックIPアドレスを設定したEC2インスタンスを起動する。
- 4) プライベートサブネットにプライベートIPアドレスを設定したEC2インスタンスを起動する。
- 5) セキュリティグループで企業IPアドレスからのみEC2インスタンスへとRDPアクセスを22ポートで許可する設定を付与する。
- 6) セキュリティグループで企業IPアドレスからのみEC2インスタンスへとRDPアクセスを3389ポートで許可する設定を付与する。

VPC内サービスへの接続

VPC内のサービスに接続する際はネットワークACLとセキュリティグループでの許可が必要

SSH接続

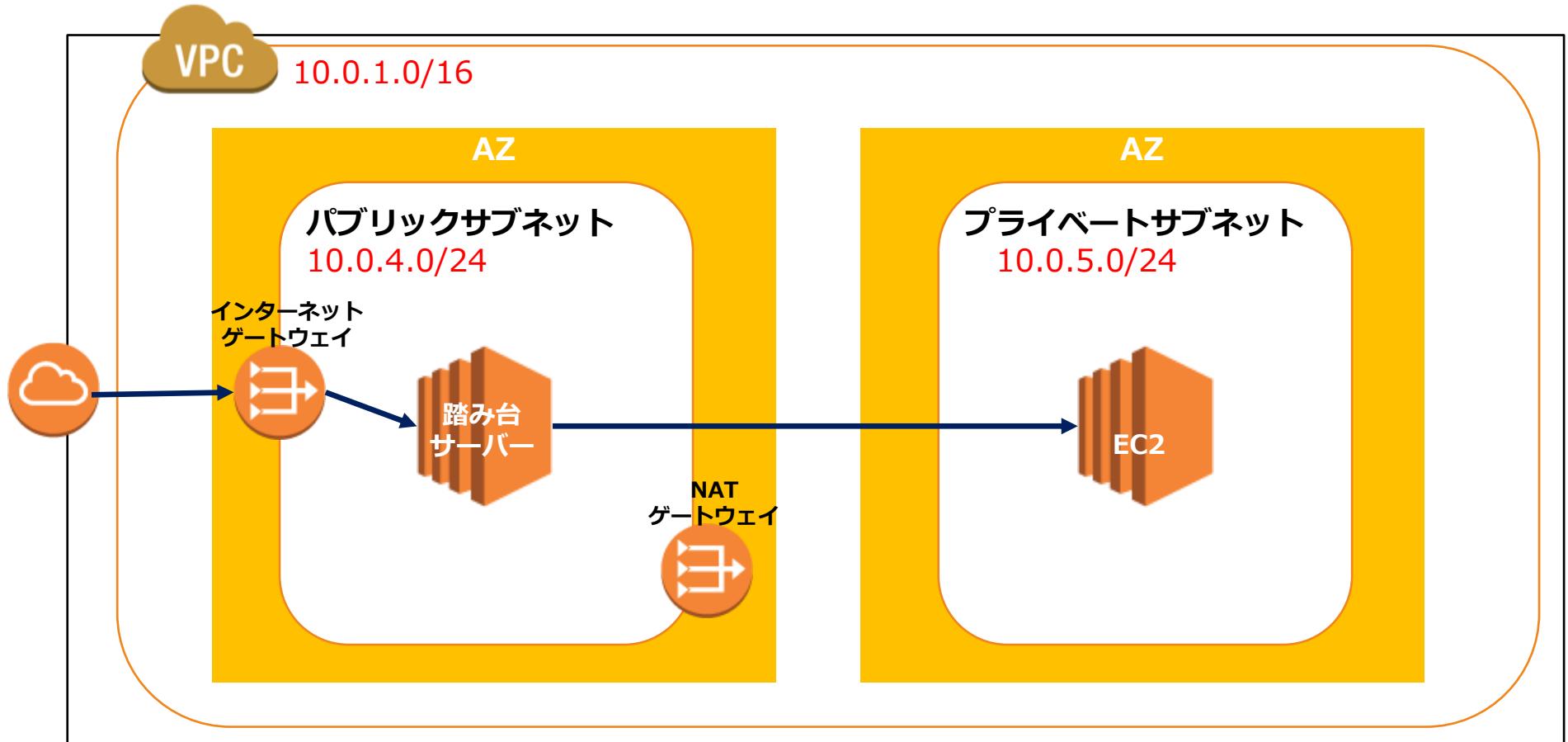
- ✓ SSHはインスタンスへの標準的な接続に利用するプロトコル
- ✓ セキュリティグループ／ネットワークACLで接続するIPアドレスを指定してポート22番のSSHを許可する。
- ✓ パブリックIPアドレス／EIPを指定してPEMキーを利用してインスタンスにアクセスを実施する。

RDP接続

- ✓ リモートデスクトップによる接続方式
- ✓ RDPはリモートデスクトップ用の接続プロトコル
- ✓ パブリックサブネットに踏み台サーバー（Bastionサーバー）を設置して、Elastic IPを付与する。
- ✓ セキュリティグループ／ネットワークACLで接続するIPアドレスを指定してポート3389番のRDPを許可する。

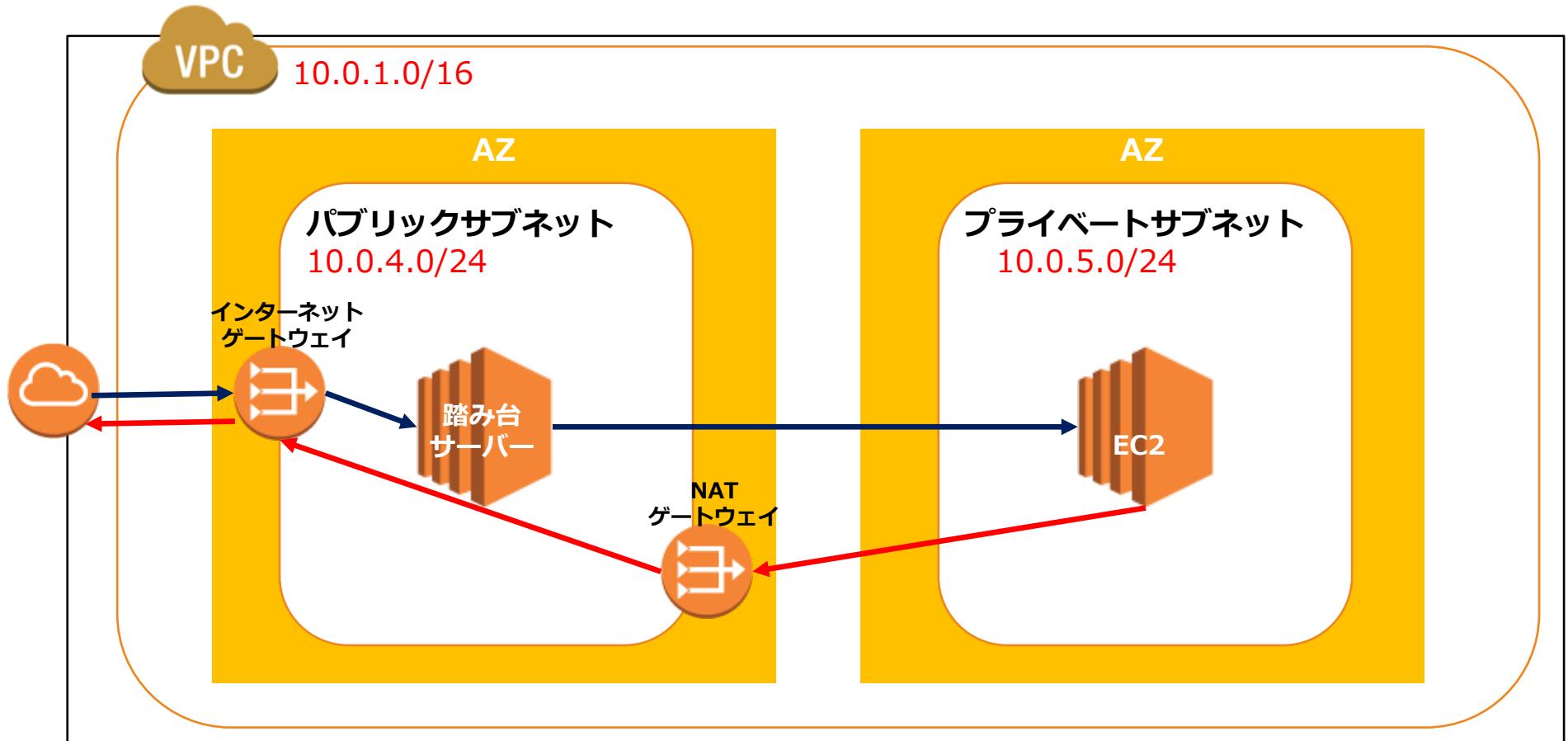
踏み台サーバー

プライベートサブネット内のインスタンスに接続するには踏み台サーバーが必要。戻りトラフィックにはNATゲートウェイが必要



踏み台サーバー

プライベートサブネット内のインスタンスに接続するには踏み台サーバーが必要。戻りトラフィックにはNATゲートウェイが必要



[Q] VPCフロー-ログ

あなたはVPCをセッティングしてAWSリソースを利用してます。WEBアプリケーション用にVPC内に複数のEC2インスタンスを起動しており、ELBによるトラフィック分散を実行しています。モニタリングの一環として、ELBに到達するトラフィックに関する情報をキャプチャする必要があります。

このデータを収集するための最適な方法を選択してください。

- 1) ELBが関連付けられたEC2インスタンスのVPCフロー-ログを有効化する。
- 2) Amazon CloudWatch Logsを使用して、ELBからのログを確認する。
- 3) ELBに関連付けられたネットワークインターフェイスにVPCフロー-ログを有効化する。
- 4) ELBが実行されているサブネットに対してVPCフロー-ログを有効化する。

VPCフロー・ログ

VPCフロー・ログ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となる。
- 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を取得する
- 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できる。
- 追加料金はなし

[Q]VPCにおけるDNSの使用

あなたはAWSアカウントを新規に開設して、EC2インスタンスを起動させました。このEC2インスタンスにはカスタムVPCが設定されています。このEC2インスタンスをWEBサーバーとして利用してPintor.comというカスタムドメインを設定したいと考えています。あなたはソリューションアーキテクトとして、これを実現するためRoute53のプライベートホストゾーン機能を使用したいと考えています。

次のVPC設定のどれを有効にする必要がありますか？（2つ選択してください）

- 1) enableDnsHostnames
- 2) enableDnsSupport
- 3) enableVpcSupport
- 4) enableVpcHostnames
- 5) enableDnsDomain

VPCにおけるDNSの使用

VPC 内で起動したインスタンスがパブリック IP アドレスに対応するパブリック DNS ホスト名を受け取るための設定が必要

enableDnsHostname S

- ✓ パブリック IP アドレスを持つインスタンスが、対応するパブリック DNS ホスト名を取得するかどうか示す。
- ✓ この属性が true で enableDnsSupport 属性も true 場合、VPC 内のインスタンスは DNS ホスト名を取得する

enableDnsSupport

- ✓ DNS 解決がサポートされているかどうかを示す。
- ✓ この属性が false の場合、パブリック DNS ホスト名を IP アドレスに解決するAmazon Route 53 Resolverサーバーが機能しない
- ✓ この属性が true の場合、Amazon が提供する DNS サーバー (IP アドレス 169.254.169.253) へのクエリ、またはリザーブド IP アドレス (VPC IPv4 ネットワークの範囲に 2 をプラスしたアドレス) へのクエリは成功する。

[Q] Elastic IP

あなたはソリューションアーキテクトとして、AWSのコスト削減を検討しています。Cost Explorerを利用してコスト内容を確認すると、無料で利用できるはずのElastic IPアドレスに課金されていることが判明しました。

Elastic IPアドレスに課金されてしまった理由は何でしょうか？

- 1) Elastic IPを解放していないが、Elastic IPがEC2インスタンスにアタッチしていない。
- 2) Elastic IPを解放せずにElastic IPがEC2インスタンスにアタッチしている。
- 3) Elastic IPの無料利用時間を超過している。
- 4) Elastic IPの無料利用数を超過している。

Elastic IP

Elastic IPは静的に利用できる追加のIPアドレス。インスタンスがインターネットへとアクセスするためには、パブリックIPかElastic IPを利用する。

パブリックIP

- ✓ 動的なパブリック IPv4 アドレス
- ✓ インスタンスが停止した場合はIPアドレスが変更される。
- ✓ VPCでパブリックIPアドレスの割当が有効化されれば自動的にVPC内リソースに割り当てられる。
- ✓ 無料

Elastic IP

- ✓ 静的なパブリック IPv4 アドレス
- ✓ インスタンスが停止してもIPアドレスは変更されない。
- ✓ VPCコンソールにおいてElastic IPを作成してから、必要なサービスにアタッチする。
- ✓ 利用時は無料。解放せずに利用しないと有料になる。

[Q] IPフローディング

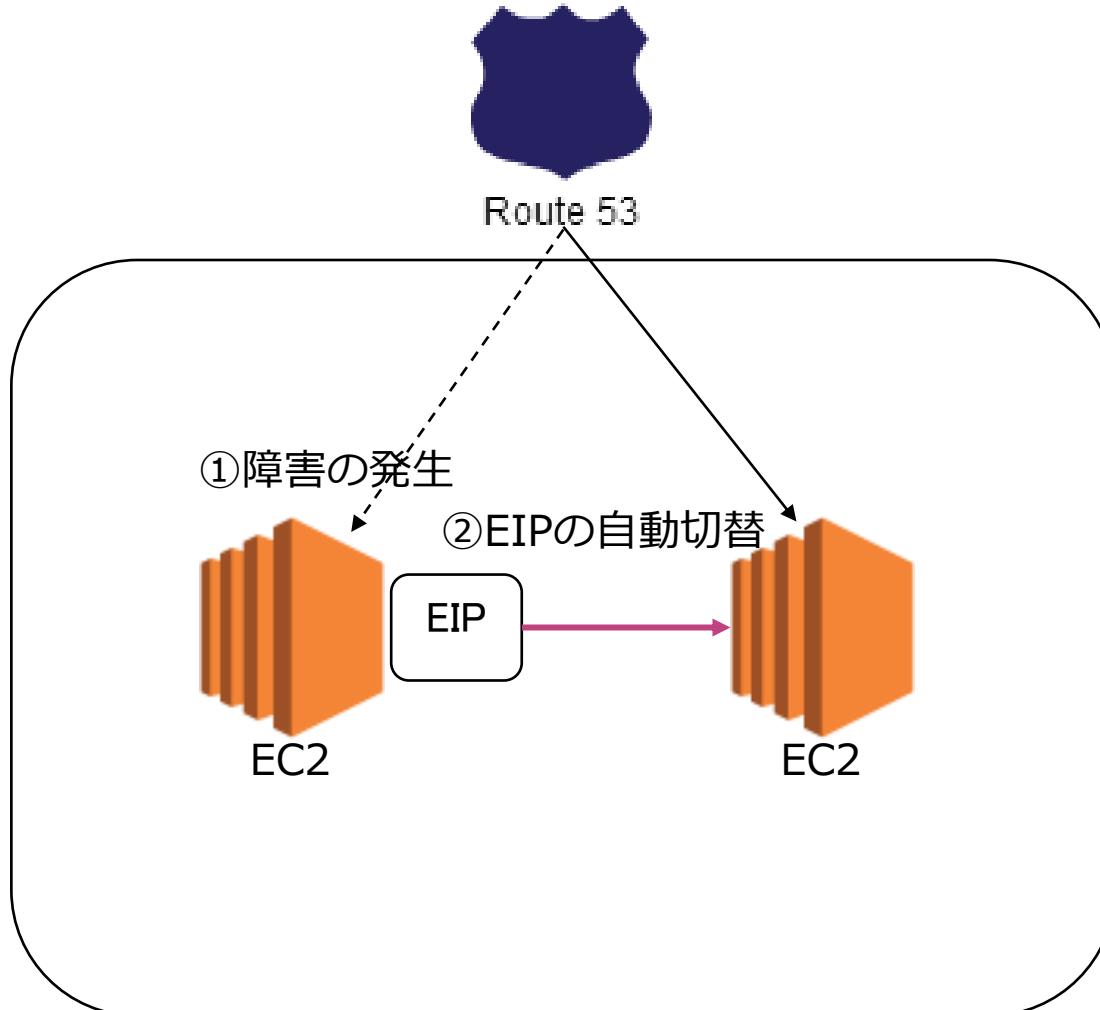
あなたはEC2インスタンスにホストされたアプリケーションを構築しています。このアプリケーションの非機能要件として、EC2インスタンスに障害が発生した場合に別のEC2インスタンスへとトラフィックを変更することで処理を継続させる必要があります。アプリケーションの運用が開始されるとEC2インスタンスに障害が発生し、トラフィックを別インスタンスに切り替えることができましたが、ダウントIMEが発生してしまいます。

この問題を解決するために実施するべき方法を選択してください。

- 1) ENIを利用してIPフローディングを利用する。
- 2) EFAを利用してIPフローディングを利用する。
- 3) ELBを利用してIPフローディングを利用する。
- 4) Elastic IPを利用してIPフローディングを利用する。

IPフローティング

障害発生時にダウンタイムをなくすため、Elastic IPを自動で付け替える機能



[Q] ENI

あなたはEC2インスタンスにホストされたアプリケーションを構築しています。このインスタンスにはプライベートIPアドレスとMACアドレスを利用した構成を実施しており、プライマリインスタンスが終了した場合は、ENIをスタンバイセカンダリインスタンスに接することが必要です。これにより、トラフィックフローを数秒以内に再開できます。その際に、EC2インスタンスへのENIアタッチメントで「ウォームアタッチ」を利用します。

ウォームアタッチの正しい説明を選択してください。

- 1) 停止中のインスタンスにENIをアタッチする
- 2) 起動プロセス中のインスタンスにENIをアタッチする
- 3) 実行中のインスタンスにENIをアタッチする
- 4) インスタンスがアイドル状態のときにENIをアタッチする

ENI

Elastic Network Interface は、仮想ネットワークカードを表す VPC 内の論理ネットワーキングコンポーネント。インスタンスへのIPアドレスの割り当て時に利用

【ENIが保持するネットワークの属性情報】

- ✓ VPC の IPv4 アドレス範囲からのプライマリプライベート IPv4 アドレス
- ✓ VPC の IPv4 アドレス範囲からの 1 つ以上のセカンダリプライベート IPv4 アドレス
- ✓ プライベート IPv4 アドレスごとに 1 つの Elastic IP アドレス (IPv4)
- ✓ 1 つのパブリック IPv4 アドレス
- ✓ 1 つ以上の IPv6 アドレス
- ✓ 1 つ以上のセキュリティグループ
- ✓ MAC アドレス
- ✓ 送信元/送信先チェックフラグ

ENI

ENIはインスタンスにアタッチして利用する。以下の3つのアタッチ方法がある。

ホットアタッチ

- ✓ ENI をインスタンスの実行中にアタッチすること

ウォームアタッチ

- ✓ ENI をインスタンスの停止中にアタッチすること

コールドアタッチ

- ✓ ENI をインスタンスの起動中にアタッチすること

セクションの内容

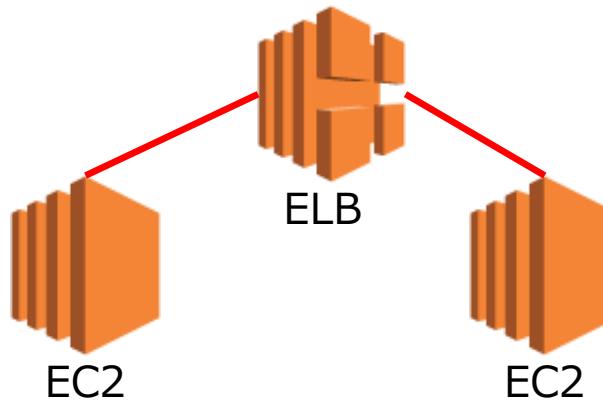
レクチャー	レクチャーで学ぶ内容
Auto Scalingの出題範囲	AWSのアーキテクチャ構成では欠かせないAuto Scalingにおける出題問題を確認して、その範囲の知識を詳細に学習します。
RDSの出題範囲	AWSの代表的なリレーショナルデータベースサービスであるRDSにおける出題問題を確認して、その範囲の知識を詳細に学習します。
EBSの出題範囲	EC2インスタンスと併に利用するストレージであるEBSにおける出題問題を確認して、その範囲の知識を詳細に学習します。
ELBの出題範囲	AWSのアーキテクチャ構成では欠かせないELBにおける出題問題を確認して、その範囲の知識を詳細に学習します。

Auto Scalingの出題範囲

Auto Scalingとは何か？

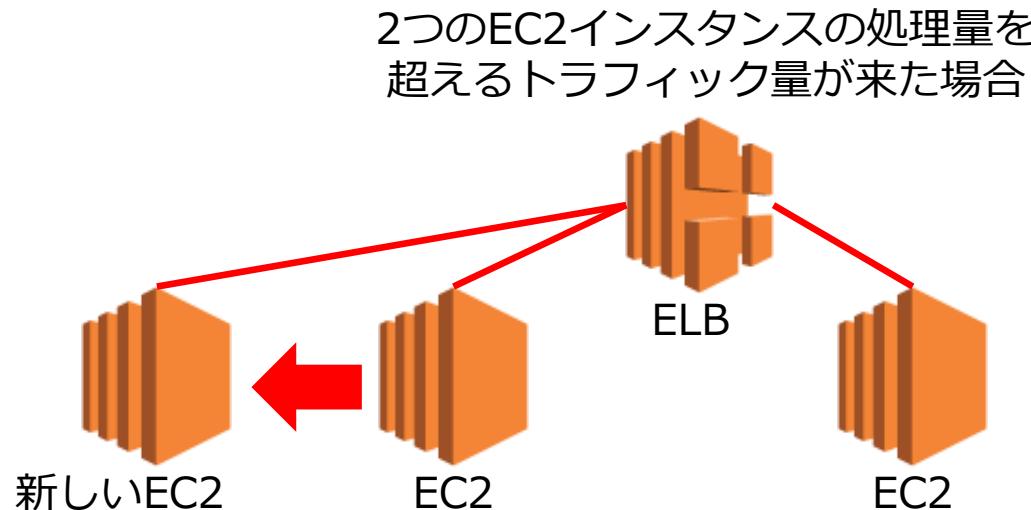
インスタンスへのアクセスが高まったときに、新しいインスタンスを増設して、パフォーマンスを向上させる機能

2つのEC2インスタンスの処理量を
超えるトラフィック量が来た場合



Auto Scalingとは何か？

インスタンスへのアクセスが高まったときに、新しいインスタンスを増設して、パフォーマンスを向上させる機能



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

Auto Scalingの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

起動設定の作成	✓ Auto Scalingグループを設定する際に利用するインスタンスの構成内容を決める設定方式が問われる。
起動テンプレートの作成	✓ Auto Scalingグループを設定する際に利用するインスタンスの構成内容を決める設定方式が問われる。 ✓ 起動設定との違いが問われる。
Auto Scalingの構成	✓ シナリオに基づいて、Auto Scalingを利用したアーキテクチャの構成が問われる。
Auto Scaling構成の設定	✓ シナリオに基づいてAuto Scalingを利用した設定上のトラブルや確認が問われる。
グループサイズの設定	✓ Auto Scalingグループを設定する際のグループサイズの設定方法が問われる。

Auto Scalingの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

スケーリングポリシーの設定	<ul style="list-style-type: none">✓ Auto Scalingグループを設定する際に選択するスケーリングポリシーの設定方法が問われる。✓ スケーリングポリシーのタイプの選択方法が問われる。
ヘルスチェック	<ul style="list-style-type: none">✓ Auto Scalingグループ上のヘルスチェック方式の選択と、その効果に関する質問が出題される。
終了ポリシー	<ul style="list-style-type: none">✓ Auto Scalingのスケールイン時にインスタンス削除順序を決定する終了ポリシーの選択方法が問われる。✓ デフォルトの削除順序やAZの選択順序が問われる。
クールダウン期間	<ul style="list-style-type: none">✓ スケールイン時に設定できるクールダウン期間の設定方法や用途が問われる。
Auto Scalingの挙動	<ul style="list-style-type: none">✓ Auto Scaling実行時に不均衡が発生した場合や、インスタンスが終了したり異常が発生した場合の挙動が問われる。

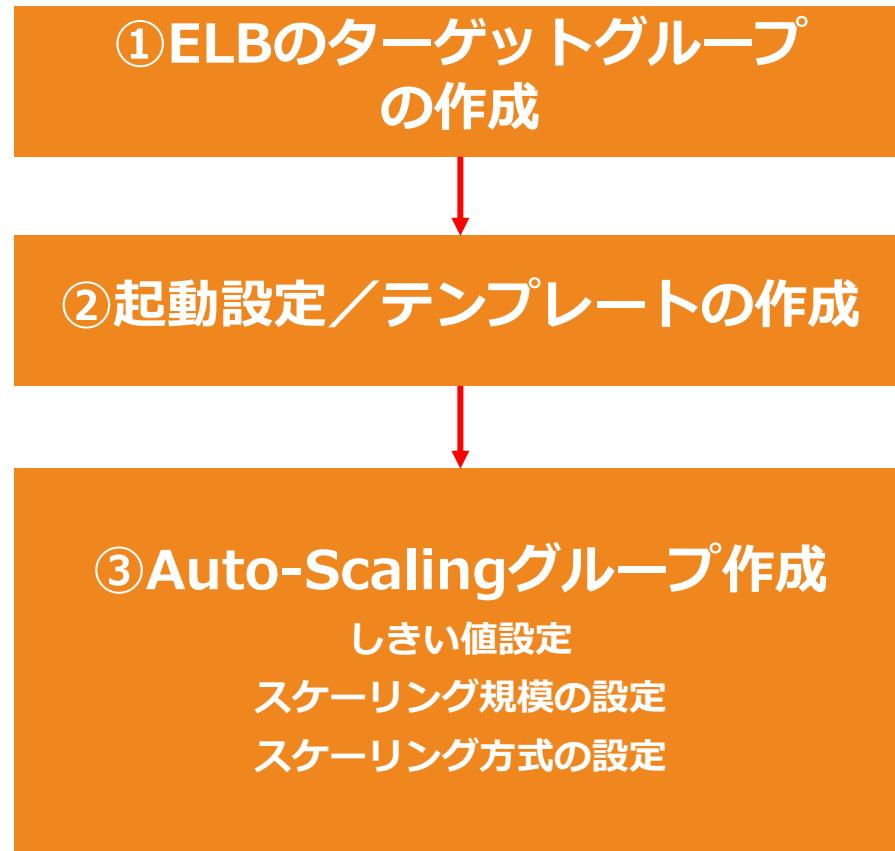
Auto Scalingの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

ライフサイクルフック	✓ Auto Scalingグループによるインスタンス起動または削除時に実行されるカスタムアクションであるライフサイクルフックの用途や挙動に関する質問が出題される。
トラブルシューティング	✓ Auto Scaling実行時にトラブルが発生した場合の適切なトラブルシューティングの実行方法が問われる。

Auto-Scalingの設定プロセス

Auto Scaling設定にはELBと起動テンプレートを事前に準備する必要がある



ELBとの連携

Auto-Scalingで起動するインスタンスをELBのターゲットグループ内に配置することが可能

ロードバランシング - 省略可能 [Info](#)

ロードバランシングの有効化

Application Load Balancer または Network Load Balancer

Classic Load Balancer

ロードバランサーのターゲットグループを選択

ターゲットグループの選択 [▼](#) [C](#)

udemy-elb-target [X](#)

[ターゲットグループを作成する](#)

ヘルスチェック - 省略可能

ヘルスチェックのタイプ [Info](#)

EC2 Auto Scaling は、ヘルスチェックに合格しなかったインスタンスを自動的に置き換えます。ロードバランシングを有効にした場合、常に有効になっている EC2 ヘルスチェックに加えて、ELB ヘルスチェックを有効にすることができます。

EC2 ELB

ヘルスチェックの猶予期間

新しいインスタンスの運用が開始されてから、EC2 Auto Scaling が最初のインスタンスのヘルスチェックを実行するまでの時間です。

300 秒

Auto-Scalingの要素

起動設定や起動テンプレートを準備した後、Auto Scalingグループを設定する。

起動設定または 起動テンプレート

- ✓ Auto Scalingによって起動するインスタンスタイプなどの起動設定
- ✓ 起動設定または起動テンプレートを利用する。
- ✓ 起動設定はAuto Scaling専用
- ✓ 起動テンプレートはインスタンス起動全般で利用可能であり、バージョニングなどの機能が充実

Auto Scaling グループ

- ✓ Auto Scalingのグループサイズ（起動するインスタンス数）の設定
- ✓ 実行時のしきい値の設定
- ✓ スケーリングポリシーを選択して、スケールアウトとスケールインの方法を設定
- ✓ ターミネーションポリシーを設定

[Q]起動設定の作成

あなたはソリューションアーキテクトとして、AWS上でWEBアプリケーションを構築しています。このアプリケーションは冗長構成を高めるためにELBの背後に複数のEC2インスタンスを利用しています。さらにAuto Scalingグループを設定して負荷が高まった際にスケールアウトできるように構成しました。しばらくして、あなたはAuto Scalingグループにおいてインスタンスタイプを変更する必要性が発生していました。

Auto Scalingグループに構成されたインスタンスタイプを変更するには、どうしたら良いでしょうか？

- 1) 新しいインスタンスタイプを利用した新しい起動設定を作成して、その起動設定を利用するようにAuto Scalingグループを新しく構成します。
- 2) 新しいインスタンスタイプを利用した新しい起動設定を作成して、その起動設定を利用するようにAuto Scalingグループを変更します。
- 3) Auto Scalingグループのインスタンスタイプの修正画面で新しいインスタンスタイプを選択して、Auto Scalingグループを修正します。
- 4) Auto Scalingグループで利用している起動設定の編集を実行して、新しいインスタンスタイプに変更します。

[Q]起動テンプレートの作成

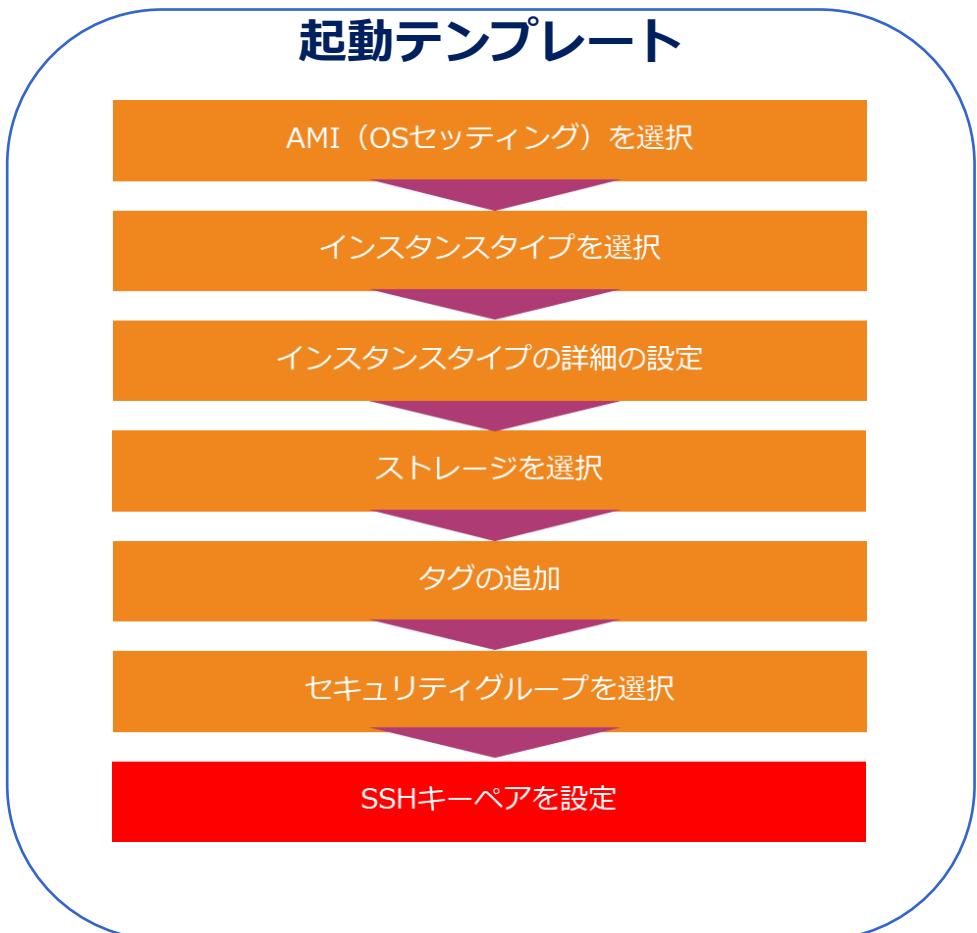
ある会社はWEBアプリケーションをAWS上で構築しています。需要増などによって一時的にアプリケーションの負荷が高まることに備えるためにAuto Scalingの仕組みをEC2インスタンスに導入することになりました。ソリューションアーキテクトはインスタンス構成を適切に管理する仕組みを選択して、Auto Scalingグループを設定することが求められています。

インスタンスを管理するために利用するべき機能はどれでしょうか？

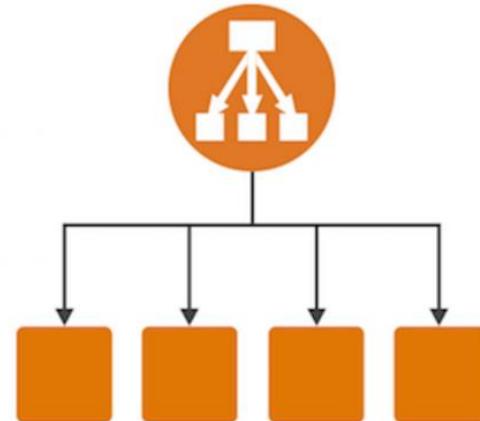
- 1) 起動テンプレートを使用してAuto Scalingグループを作成する
- 2) ゴールデンイメージを使用してAuto Scalingグループを作成する
- 3) スポットフリートリクエストを使用して、Auto Scalingグループを作成する
- 4) 起動構成を使用してAuto Scalingグループを作成する

起動テンプレートの作成

起動テンプレートはEC2で説明した起動設定をテンプレート化して、自動で起動する際に利用する仕組み



Auto Scaling



- ✓ 現在は起動設定ではなく起動テンプレートの利用が推奨されている。
- ✓ AMIを更新した場合は作成しなおす必要がある。
- ✓ 起動テンプレートの構成通りにインスタンスを選択して起動する。
- ✓ 起動設定はAuto Scaling専用
- ✓ 起動テンプレートは広くE2インスタンスの起動時に利用

[Q] Auto Scalingの構成

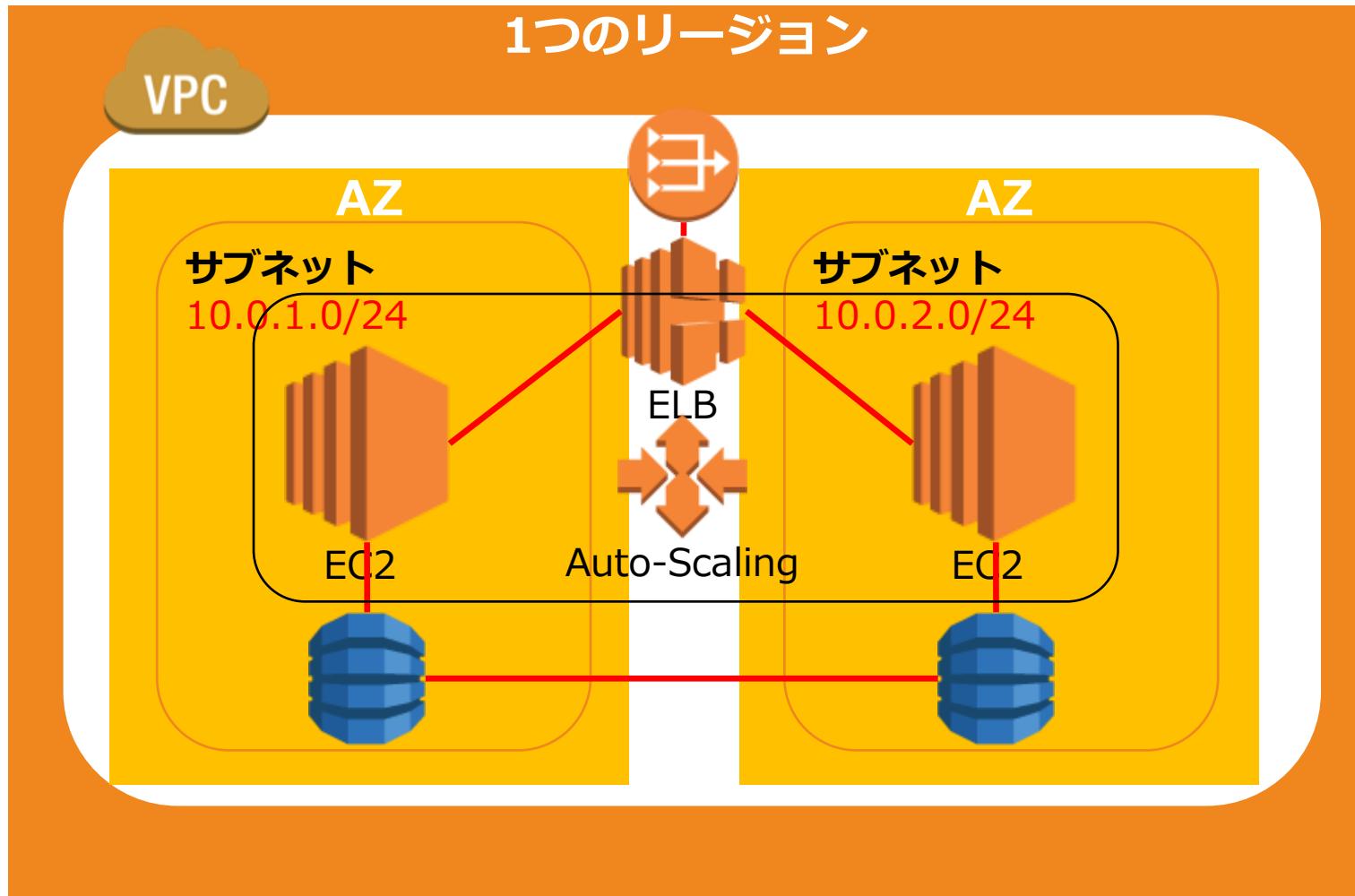
B社ではAWS上にWEBアプリケーションを構築して、コンテンツを配信する仕組みを構築しています。データ層では、オンライントランザクション処理（OLTP）データベースを利用しています。WEB層では柔軟でスケーラブルなアーキテクチャ構成を実現する必要があり、負荷分散や一時的な負荷に対する対策が必要不可欠です。

この要件を満たすための最適な方法を選択してください。

- 1) EC2インスタンスに対してAuto ScalingとELBを設定する
- 2) RDSのマルチAZ構成を構成する。
- 3) EC2インスタンスをマルチAZに展開してRoute53によるフェイルオーバーティングを実施する
- 4) EC2インスタンスを予測キャパシティよりも多く設置する

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



[Q] Auto Scaling構成の設定

あなたはWebアプリケーションをAWS上に実装しました。このアプリケーションは、Amazon EC2インスタンス、Amazon ELB、および2つのサブネットにわたるAutoScalingとRoute53により構成されています。しかしながら、デプロイされたアプリケーションは2つのサブネットではなく、1つのサブネットのみでEC2インスタンスを実行しているようです。

この問題の最も可能性が高い原因は何でしょうか？

- 1) 起動設定のAMIが存在していない。
- 2) Route53のターゲットグループが複数サブネットで構成されてない。
- 3) ELBでクロスゾーンロードバランシングが有効になっていない。
- 4) AutoScalingグループが複数サブネットで構成されてない。

[Q] Auto Scaling構成の設定

あなたはWebアプリケーションをAWS上に実装しました。 このアプリケーションは、Amazon EC2インスタンスとAmazon ELBによりマルチAZ構成となっています。 さらにAuto Scalingを追加して、EC2インスタンスを自動的に追加し、着信リクエストの一時的な負荷増加に対応する設定が必要です。

既存のEC2インスタンスをAuto Scalingグループに追加するための対応を選択してください。 (2つ選択してください。)

- 1) 既存インスタンスを起動したAMIが存在する。
- 2) Auto Scalingグループに追加するインスタンスを休止状態とする。
- 3) Auto Scalingグループに追加するインスタンスは別のAuto Scalingグループのメンバーではない。
- 4) Auto Scalingグループで定義されたVPCの1つで既存のインスタンスが起動されている。
- 5) Auto Scalingグループで定義されたアベイラビリティーゾーンの1つで既存のインスタンスが起動されている。

Auto Scalingの構成

Auto Scalingグループは特定のVPCのサブネットを指定して、サブネットが利用されるAZにインスタンスを起動する。

設定の構成 [Info](#)

以下の設定を行います。起動テンプレートを選択したかどうかに応じて、これらの設定には EC2 リソースを最適に使用するために役立つオプションが含まれる場合があります。

ネットワーク [Info](#)

ほとんどのアプリケーションでは、マルチアベイラビリティーゾーンを使用して、Amazon EC2 Auto Scaling でゾーン間のインスタンスのバランスを取ることができます。デフォルトの VPC とデフォルトのサブネットは、迅速な使用の開始に適しています。

VPC

vpc-01c20188c52590827 (test)
10.0.0.0/16

[C](#)

[VPCを作成する](#)

サブネット

サブネットを選択する

ap-northeast-1d | subnet-026a59c8d727b13f3 (Blue)
10.0.1.0/24

[X](#)

[C](#)

[サブネットを作成する](#)

[Q] グループサイズの設定

あなたはWebアプリケーションをAWS上に構築しています。このアプリケーションは、このWEBアプリケーションは単一のEC2インスタンスで構成されています。コスト面とWEBアプリケーションの重要度の低さから複数のインスタンスを利用しないことが決まっていますが、インスタンス障害に対してAuto scalingを実行していても单一インスタンスを維持する設定が必要です。

この要件を満たすことができる最も費用対効果の高いスケーリング方法はどれですか？

- 1) min = 1、max = 1、desired = 1の1つのAZにまたがる自動スケーリンググループを作成する
- 2) min = 1、max = 1、desired = 1の2つのAZにまたがる自動スケーリンググループを作成する
- 3) min = 1、max = 2、desired = 1の1つのAZにまたがる自動スケーリンググループを作成する
- 4) min = 1、max = 2、desired = 1の2つのAZにまたがる自動スケーリンググループを作成する

グループサイズの設定

グループサイズの設定において、インスタンスの増減値を設定することができる。

希望する容量

- ✓ Auto Scaling が実行されない状態でのインスタンス数を設定する。
- ✓ この数値を変更することで、手動でスケーリングさせることも可能

最小キャパシティ

- ✓ スケールイン時にインスタンスを削減する際の下限のインスタンス数を設定する。
- ✓ 希望する容量より大きい数値は設定できない。

最大キャパシティ

- ✓ 最大キャパシティはスケールアウト時に起動するインスタンスの最大数を設定する。
- ✓ 希望する容量より少ない数値は設定できない。

[Q]スケーリングポリシーの設定

あなたは2層WebアプリケーションをAWS上に実装しました。 このアプリケーションは、Amazon EC2インスタンスとAmazon ELBによりマルチAZ構成となっています。 さらにAuto Scalingを追加して、EC2インスタンスを自動的に追加し、着信リクエストの一時的な負荷増加に対応する設定が必要です。 EC2インスタンスは60%のCPU使用率までが正常に処理を実行できますが、それ以上の使用率になるとパフォーマンスが低下するようです。

どのようなスケーリングポリシーを設定するべきでしょうか？

- 1) Auto Scalingグループで平均合計CPU使用率を60%をしきい値としたターゲット追跡スケーリングポリシーを設定する。
- 2) Auto Scalingグループで平均合計CPU使用率を60%をしきい値としたステップスケーリングポリシーを設定する。
- 3) Auto Scalingグループで平均合計CPU使用率を60%をしきい値としたスケジュールドケーリングポリシーを設定する。
- 4) Auto Scalingグループで平均合計CPU使用率を60%をしきい値とした手動スケーリングポリシーを設定する。

ターゲット追跡スケーリングポリシー

CloudWatchのモニタリングメトリクスを利用したスケーリングを実施する。

スケーリングポリシー - 省略可能

需要の変化に対応するために、スケーリングポリシーを使用して Auto Scaling グループのサイズを動的に変更するかどうかを選択します。 [Info](#)

ターゲット追跡スケーリングポリシー
希望する結果を選択して、スケーリングポリシーが結果を達成するために必要に応じてキャパシティを追加および削除するようにします。

なし

スケーリングポリシー名

メトリクスタイプ

ターゲット値

インスタンスには以下のものが必要です
 メトリクスに含める前にウォームアップする秒数

スケールインを無効にしてスケールアウトポリシーのみを作成する

[Q] スケーリングポリシーの設定

あなたは2層WebアプリケーションをAWS上に実装しました。 このアプリケーションは、Amazon EC2インスタンスとAmazon ELBによるマルチAZ構成となっています。 さらにAuto Scalingを追加して、EC2インスタンスを自動的に追加し、着信リクエストの一時的な負荷増加に対応する設定が必要です。 このアプリケーションは定期的に週末の一定時間に負荷が増加する見込みです。

この要件を満たすためにAuto Scalingをどのように設定するべきでしょうか？

- 1) ライフサイクルフックを利用する。
- 2) スケジュールドスポットインスタンスを利用する。
- 3) スケジュールされたスケーリングポリシーを利用する。
- 4) ステップスケーリングポリシーを利用する。

スケーリングポリシーの設定

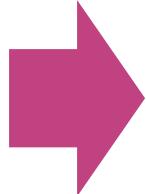
スケーリングポリシーを設定して、スケーリングを実施する。

動的 スケーリング	簡易 スケーリング ポリシー	ターゲット追跡スケーリングポリシーの通常の設定 アラーム設定に基づいて1段階のスケーリングを実施
	ステップ スケーリング ポリシー	アラーム超過のサイズに基づいてインスタンス数を動的にスケーリングする1つ以上のステップ調整値を指定して複数回の段階的なスケーリングを実施
	手動スケーリング	希望する容量を調整して、手動でスケーリングを実施する。
スケジュールされた スケーリング		スケーリングを実施する日時を指定して、スケーリングを実行する。

スケーリングポリシーの設定

スケーリングポリシーの設定は複数組み合わせて利用することができる

スケーリングを
スケジュールで設定



スケジュール設定
を超過したら
動的スケーリング

[Q]ヘルスチェック

現在WEBアプリケーションはAWS上で実行されています。このWEBアプリケーションはELBの背後にあるAmazonEC2インスタンスにAuto Scalingグループが構成されています。本日、1つのEC2インスタンスに異常が発生し、ELBがそれをターゲットからはずしましたが、インスタンスがまだ実行中となっています。

このような挙動の最も可能性が高い原因はどれでしょうか？

- 1) ELBヘルスチェックタイプがAuto Scalingで利用されていない。
- 2) EC2ヘルスチェックタイプがAuto Scalingで利用されていない。
- 3) Auto Scalingグループにクールダウン期間が設定されている。
- 4) Auto Scalingグループにタイムアウト猶予時間が設定されている。

ヘルスチェック

Auto-Scaling配下のEC2のヘルスチェックにはEC2のステータス情報またはELBのヘルスチェックのどちらかを利用する

EC2ステータス

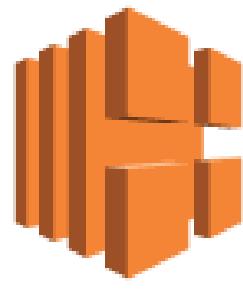
インスタンスのステータスがrunning以外の状態を異常と判断

ELB

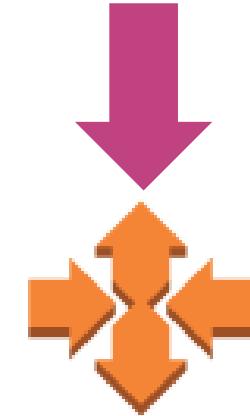
ELBのヘルスチェック機能を活用する

ヘルスチェック

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



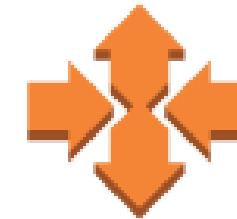
ELB



Auto-Scaling



CloudWatch



Auto-Scaling

[Q]終了ポリシー

現在WEBアプリケーションはAWS上で実行されています。このWEBアプリケーションはELBの背後にあるAmazonEC2インスタンスにAuto Scalingグループが構成されています。負荷が高まるとAuto Scalingグループによって新規インスタンスが2つのアベイラビリティーゾーン (AZ) にまたがって生成されます。スケーリングが実行されると、ap-northeast-1aには3つのEC2インスタンスが配置され、ap-northeast-1cには4つのEC2インスタンスが配置されています。

スケーリング時に、どのようにインスタンスが削除されますか？

- 1) 最も古い起動構成のインスタンスがap-northeast-1cで終了する。
- 2) 最も古い起動構成のインスタンスがap-northeast-1aで終了する。
- 3) ap-northeast-1aでランダムにインスタンスを終了する。
- 4) ap-northeast-1cでランダムにインスタンスを終了する。
- 5) 均衡を保つためにap-northeast-1aのインスタンスが1つ作成される。

終了ポリシー

需要減に基づくスケールインの際に、どのインスタンスから終了するかを設定

デフォルト	AZの選択	<ul style="list-style-type: none">✓ 複数AZにインスタンスがあるか確認し、一番多いインスタンスが配置されているAZのインスタンスを削除する。✓ 全AZで同数のインスタンスが配置されている場合は、ランダムでAZを選択してインスタンスを削除する。
	インスタンスの選択	<ul style="list-style-type: none">✓ 起動時間が一番古いインスタンスを削除✓ 古いインスタンスが複数ある場合は、次の課金発生が短いインスタンスを削除する。✓ 次の課金時間に近いインスタンスが複数ある場合は、ランダムで削除する。
カスタム	AZの選択	<ul style="list-style-type: none">✓ 複数AZにインスタンスがあるか確認し、一番多いインスタンスが配置されているAZのインスタンスを削除する。✓ 全AZで同数のインスタンスが配置されている場合は、ランダムでAZを選択してインスタンスを削除する。
	インスタンスの選択	<ul style="list-style-type: none">✓ 選択したAZのカスタムポリシーに従い削除する。

終了ポリシー

需要減に基づくスケールインの際にどのインスタンスから終了するかを設定

OldestInstance

最も古いインスタンスから順番に終了

NewestInstance

最も新しい起動時刻のインスタンスから終了

OldestLaunch Configuration

最も古い起動設定により起動しているインスタンスから終了

ClosestTo NextInstanceHour

次の課金が始まるタイミングが最も近いインスタンスから終了

[Q]クールダウン期間

現在WEBアプリケーションはAWS上で実行されています。このWEBアプリケーションはELBの背後にあるAmazonEC2インスタンスにAuto Scalingグループが構成されています。最近、Auto Scalingが同じ時間にインスタンスを増やしたり、削除したりと短期間に実行しており、スケーリングイベントの発生が多くなっています。

このようなスケーリング状況を改善するために、何をするべきでしょうか？（3つ選択してください）

- 1) Auto Scalingグループサイズを変更して、希望する容量を増加させる。
- 2) スケジュールされたスケーリングアクションを使用してスケーリングを設定する。
- 3) Auto ScalingスケールダウンポリシーをトリガーするCloudWatchアラーム期間を変更する。
- 4) Auto ScalingスケールダウンポリシーをトリガーするCloudWatchアラームのしきい値を変更する。
- 5) Auto Scalingグループのクールダウン期間を変更する

クールダウン期間

スケールイン時のインスタンスの終了においてクールダウン時間を設定することが可能

クールダウン期間

- ✓ 終了するインスタンスの前のアクティビティの影響前に、Auto Scaling グループが追加のインスタンスを起動または終了するのを防ぐ
- ✓ クールダウン期間はデフォルトで設定されている
- ✓ クールダウン期間は変更可能

クールダウン期間 の例外

- ✓ クールダウン期間中、スケジュールされたアクションがスケジュールされた時間に開始されるか、ターゲット追跡またはステップスケーリングポリシーによりスケーリングアクティビティが開始されると、クールダウン期間が終了するのを待たずに、それらのスケーリングアクティビティを実行する。
- ✓ インスタンスが正常でなくなった場合、Amazon EC2 Auto Scaling はクールダウン期間の完了を待つことなく、異常のあるインスタンスを置き換る。

[Q] Auto Scalingの挙動

現在WEBアプリケーションはAWS上で実行されています。このWEBアプリケーションはELBの背後にあるAmazonEC2インスタンスにAuto Scalingグループが構成されています。このAuto Scaling Groupは2つのAZを使用しており、現在、グループ内で6つのAmazonEC2インスタンスが実行されています。

EC2インスタンスの1つの不具合が発生した場合に、Auto Scalingはどのようなアクションを実行しますか？（2つ選択してください。）

- 1) 不均衡を是正するため、3つのEC2インスタンスが実行されているAZ内のインスタンスを終了する。
- 2) 障害が発生したインスタンスがあるAZ内において新規に1つインスタンスを起動する。
- 3) 障害が発生したインスタンスがないAZ内において新規に1つインスタンスを起動する。
- 4) 最初に障害が発生したインスタンスを削除してから、同じAZ内に新しいインスタンスを起動する。
- 5) 新しいインスタンスを起動した後に、障害が発生したインスタンスを終了する。
- 6) 2つのAZの1つをランダムに選択し、そのAZのインスタンスを終了する。

Auto Scalingの挙動

Auto Scalingが実行されるとAZに適切に分散されるようにインスタンス数が調整される。

基本的な挙動

- ✓ インスタンスが最も少ないAZでインスタンスを起動する
- ✓ インスタンス起動が失敗した場合は、起動が成功するまで別AZで起動する

AZ間にアンバランスが発生した場合の挙動

再分散の実施

- ✓ AZ間でインスタンス数の不均衡があると調整する。
- ✓ グループが不均等になった原因のインスタンスを停止して、リソースが不足していたAZに新規インスタンスを起動する。

再分散時に挙動

- ✓ 古いインスタンスを終了する前に新しいインスタンスを起動することで、パフォーマンス低下を防ぐ。
- ✓ Auto Scalingの最大容量に近づくと、再分散処理が遅くなったり、完全に停止する可能性がある。これを回避するために、一時的に最大容量を増やす（最大容量の10%または+1の容量を追加する。）

[Q]ライフサイクルフック

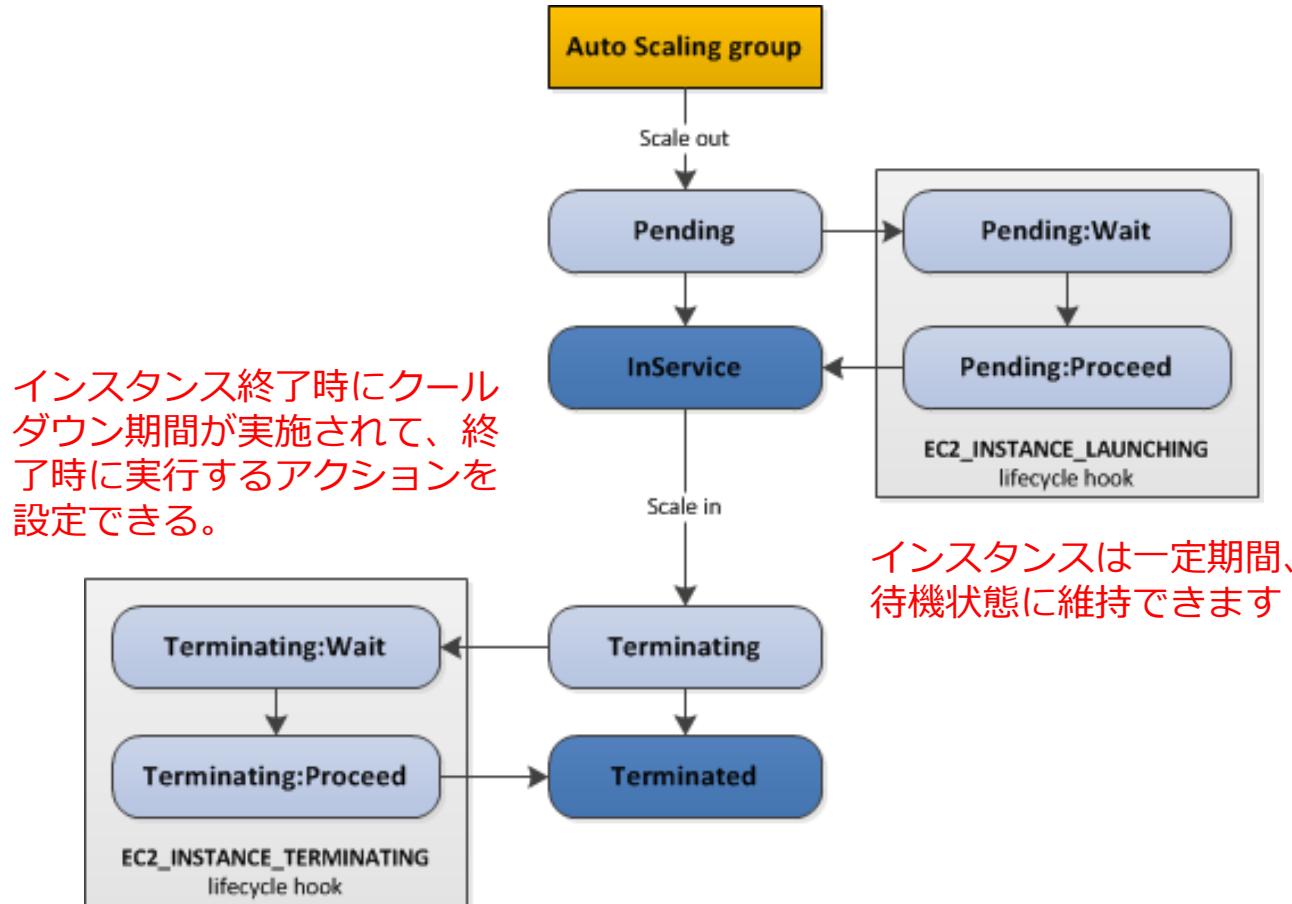
現在WEBアプリケーションはAWS上で実行されています。このWEBアプリケーションはELBの背後にあるAmazonEC2インスタンスにAuto Scalingグループが構成されています。スケールインを実行する際に、インスタンス停止の影響を調べるために、停止されるインスタンスのログファイルをダウンロードできるようにしたいと考えています。

このカスタムアクションを有効にするために使用できる機能は次のうちどれですか？

- 1) Auto ScalingグループのEC2フリート構成
- 2) Auto Scalingグループの終了ポリシー
- 3) Auto Scalingグループのスケジュールされたスケーリングポリシー
- 4) Auto Scalingグループのライフサイクルフック

ライフサイクルフック

Auto Scaling グループによるインスタンスの起動時または削除時にインスタンスを一時停止してカスタムアクションを実行。
Lambdaと連携した処理も可能



[Q] トラブルシューティング

あなたの会社はEC2インスタンスにELBを設定してトラフィック分散した上で、Auto Scalingグループを設定しました。負荷が向上した際の挙動を確かめるため、負荷テストツールを利用してAuto Scalingグループを実行させます。しかしながら、Auto Scalingによって起動された EC2インスタンスのステータスチェックにおいて、Impairedと表示されているようです。

Auto Scalingはどのようなアクションを実行しますか？

- 1) インスタンスが回復するまで数分待機し、回復しない場合はインスタンスを終了してから、別のインスタンスへと置換する。
- 2) 即時にインスタンスを終了してから、別のインスタンスへと置換する。
- 3) ELBが別のインスタンスへとターゲットを切り替える。
- 4) Auto Scalingは障害が発生していないAZ間でのリバランスを実行する。

トラブルシューティング

インスタンスのメンテナンスや調査時にはAuto Scalingを一時中斷して、対応することが必要

インスタンスの起動失敗

- ✓ Auto Scalingはインスタンスの起動を繰り返し実施し、24時間失敗し続けるとAmazon側で停止される可能性がある。

インスタンスの障害

- ✓ インスタンスの状態が“Impaired”となると、数分間リカバリーされるかチェックする
- ✓ リカバリーされない場合は新しいインスタンスを起動して、Impairedのインスタンスを終了する。

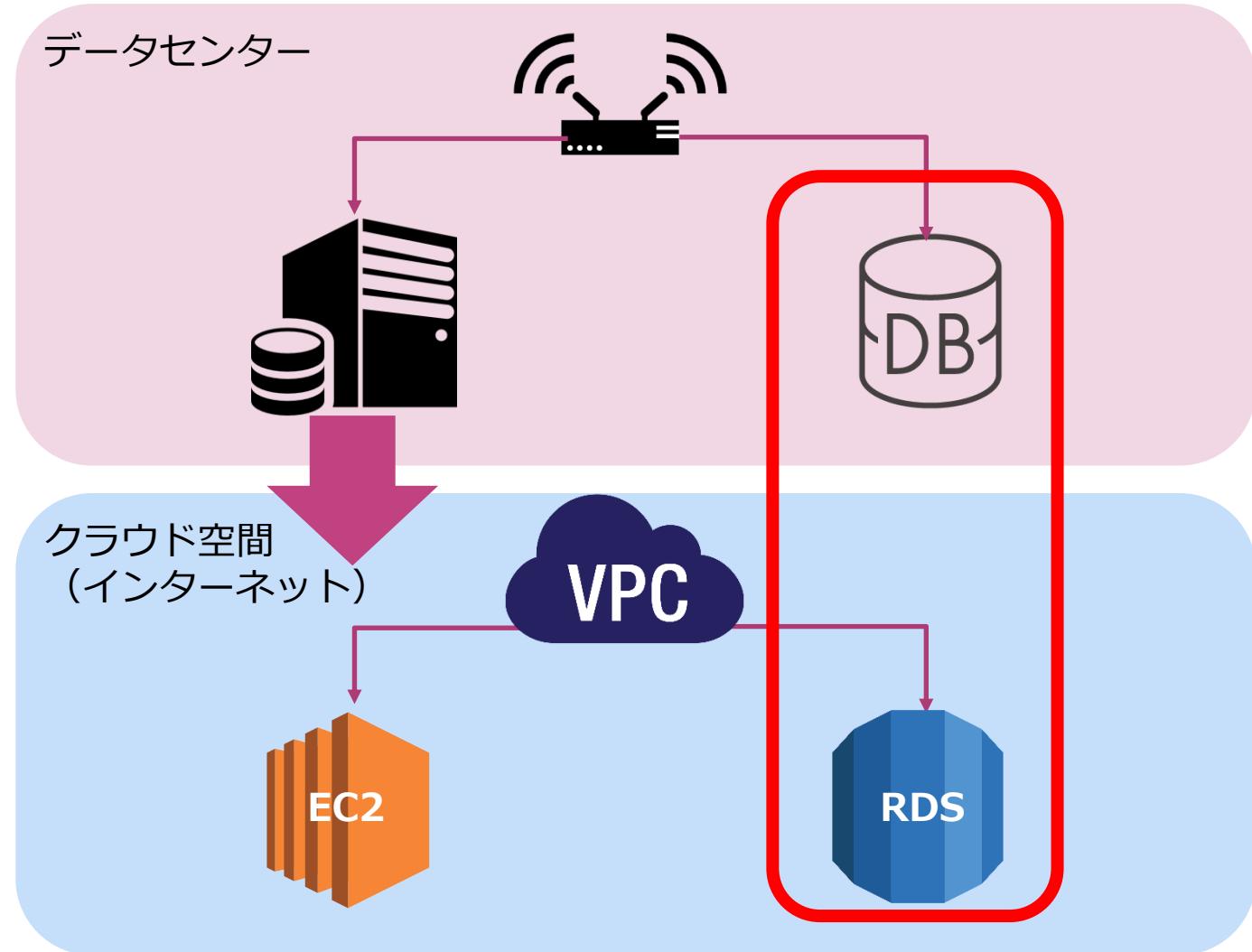
トラブルシューティングのステップ

- ✓ Auto Scalingグループを一時的に停止しないでインスタンスを停止すると新規インスタンスが起動してしまう。
- ✓ Auto Scalingを停止して、調査・復旧し、Auto Scalingを再開することが基本的な実施方法

RDSの出題範囲

RDSとは何か？

RDSはリレーショナルデータベースをクラウド上で即時に起動して、利用することができるサービス



RDSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

RDSの選択	✓ AWSが提供するデータベースサービスの中で、最適なデータベースとしてRDSを選択する質問
RDSの特徴	✓ RDSの特徴やMySQLやPostgreSQLなどのデータベースエンジンに関する特徴が出題される。
ストレージタイプの選択	✓ DBインスタンスを利用するストレージタイプの特徴とユースケースに関する質問が出題される。
パブリックアクセス構成	✓ RDSのDBインスタンスに対してインターネットから直接アクセスする構成が質問される。
リードレプリカ	✓ RDSを利用したスケーリング方式であるリードレプリカの特徴が出題される。 ✓ Auroraとの違いが出題される。

RDSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

クロスリージョン レプリカ	✓ RDSを利用してクロスリージョンでリードレプリカを構成する際のユースケースが出題される。
RDSのスケーリング	✓ RDSのスケーリング方法としてスケールアップの方式とスケールアウトの方式が問われる。 ✓ コスト最適やパフォーマンス向上などの要件に応じて最適なスケーリング方式を選択する質問が出題される。
RDSの暗号化	✓ RDSの暗号化の実施方法が問われる。 ✓ 暗号化されていないRDSのDBインスタンスを途中から暗号化する方法が問われる。
メンテナンス	✓ RDSのメンテナンス方法が問われる。 ✓ RDSのメンテナンスウィンドウの設定方法や、その影響が問われる。
バックアップ	✓ RDSのバックアップ方法とその復元方法が問われる。

[Q]RDSの選択

B社はAWSを利用したデータベースを構築するための要件を確認しています。あなたはソリューションアーキテクトとして、データベース要件から最適なAWSサービスを選択することになりました。この会社ではデータベース環境を自社内で管理することが要件となっています。

この要件を満たすデータベース構築方法を選択してください。

- 1) EC2
- 2) RDS
- 3) Aurora
- 4) DynamoDB

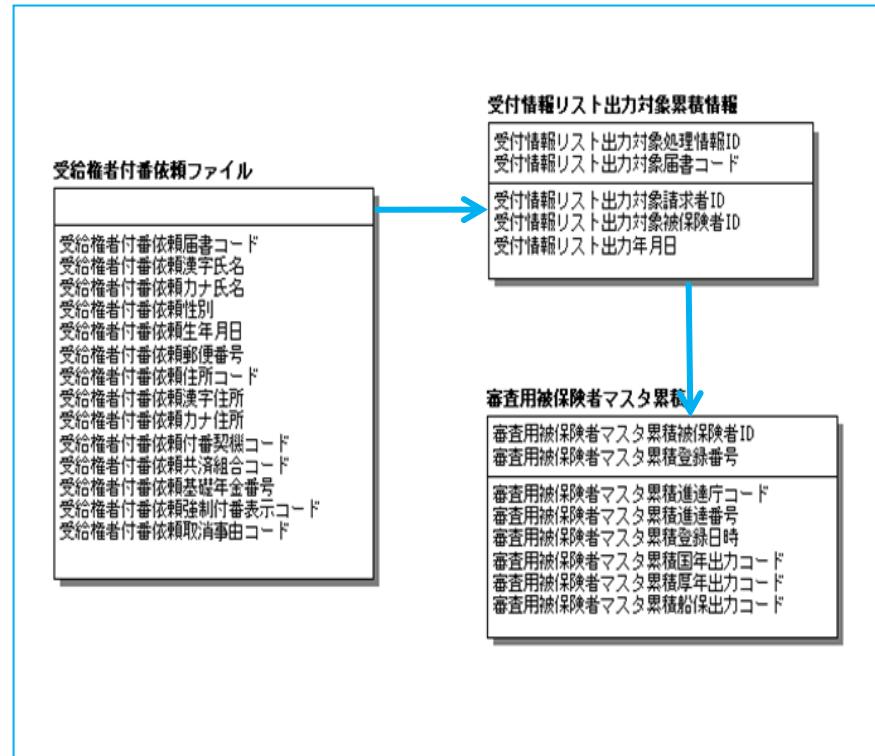
データモデル

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

リレーションナルモデル

データベースはリレーションナルモデルが基本的なデータモデルとなっている。



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

[Q] RDSの特徴

あなたはソリューションアーキテクトとして、AWS上にデータベースを構築しています。現在、オンプレミスではMySQLを利用しているため、RDSのMySQLを利用すれば容易に移行ができると判断しました。RDSを利用する場合はその特徴を踏まえて移行する必要があります。

次のうちでRDSに推奨されていない方法を選択してください。

- 1) 自動バックアップを有効化する
- 2) MySQLのストレージエンジンとしてMyISAMを利用する。
- 3) MySQLのストレージエンジンとしてInnoDBを利用する。
- 4) 大きなテーブルのパーティションは16TBを超えないようにする。

RDSの特徴

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

RDSのベストプラクティス

RDSは主だったベストプラクティスとして以下のような内容が推奨されている。

- メモリ内に保持できるように十分な RAM を割り当てる
- 拡張モニタリングを使用したオペレーティングシステムの問題の特定
- 特定のメトリクスしきい値に対して Amazon CloudWatch アラームを設定
- MySQLのストレージエンジンにはInnoDBを利用する。
- 大きなテーブルのパーティションは16TBを超えないようにする。

RDSの制約事項

RDSはマネージド型であり管理が楽であるものの、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
- ・ 一部の機能が使えない
- ・ 個別パッチは適用できない

[Q]ストレージタイプの選択

あなたはリレーショナルデータベースをAWS上で構築しています。このデータベースソリューションでは多数のトランザクション処理が発生することが予想されており、ランダムI/O遅延が発生することが懸念されています。あなたはソリューションアーキテクトとして、データベース設定によって性能を向上させるように依頼を受けました。容易に運用負荷をかけないで実行することが求められます。

次のうちどのデータベースを使った方式を選択するべきでしょうか。

- 1) ElastiCacheによるキャッシュ処理により高速処理を実現する
- 2) EC2インスタンスにプロビジョンドIOPSを設定して、データベースをインストールして利用する
- 3) RDSを利用してストレージタイプをプロビジョンドIOPSに変更する
- 4) RDSを利用してインスタンスタイプを最適なものに変更する。

ストレージタイプの選択

ストレージタイプは汎用とプロビジョンドIOPSから選択する。
マグネティックは古いタイプであり、あまり利用しない

汎用	<ul style="list-style-type: none">✓ SSDタイプ✓ GBあたりの容量課金を実施✓ 通常のパフォーマンスに加えてバーストを実施し、100～10,000IOPSを実現可能（サイズによって変わる）
プロビジョンドIOPS	<ul style="list-style-type: none">✓ SSDタイプ✓ GBあたりの容量課金を実施+プロビジョンド済みIOPS単位の課金✓ 通常のパフォーマンスに加えてバーストを実施し、1,000～30,000IOPSを実現可能（サイズによって変わる）
マグネットイック	<ul style="list-style-type: none">✓ ハードディスクタイプ✓ GBあたりの容量課金を実施+IOリクエスト課金✓ 平均100～最大数百のIOPS

[Q] パブリックアクセス構成

顧客管理部門ではCRMソリューションとしてAWSでデータベースソリューションを運用しています。部門では機能追加に伴って、新規にRDS MySQLを利用してデータベースを構築する予定です。非機能要件に対応するため、そのデータベースはインターネットから直接にアクセスできるようにすることが必要です。

インターネット経由でRDS MySQLに接続する正しい設定方法はどれでしょうか？
(3つ選択してください)

- 1) RDSインスタンスのパブリックアクセスを有効化する。
- 2) RDSインスタンスをパブリックサブネットに配置する。
- 3) RDSインスタンスをプライベートサブネットに配置する。
- 4) インターネットからRDSインスタンスへのアクセスを許可するセキュリティグループを作成し、RDSインスタンスに割り当てる。
- 5) NATゲートウェイを構成して、RDSデータベースがあるサブネットにルートを設定する。
- 6) RDSインスタンスにおいてインターネットアクセスを有効化する。

パブリックアクセス構成

パブリックアクセスを有効化して、セキュリティグループでアクセスを許可する必要がある。

The screenshot shows the AWS RDS console interface for configuring public access. It includes sections for Security Groups, Authentication, and Public Accessibility.

セキュリティグループ
この DB インスタンスに関連付ける DB セキュリティグループの一覧。

セキュリティグループの選択 ▾

default (sg-a418d7d8) (vpc-940724f3) X

認証機関
この DB インスタンスの認証機関。

rds-ca-2019 ▾

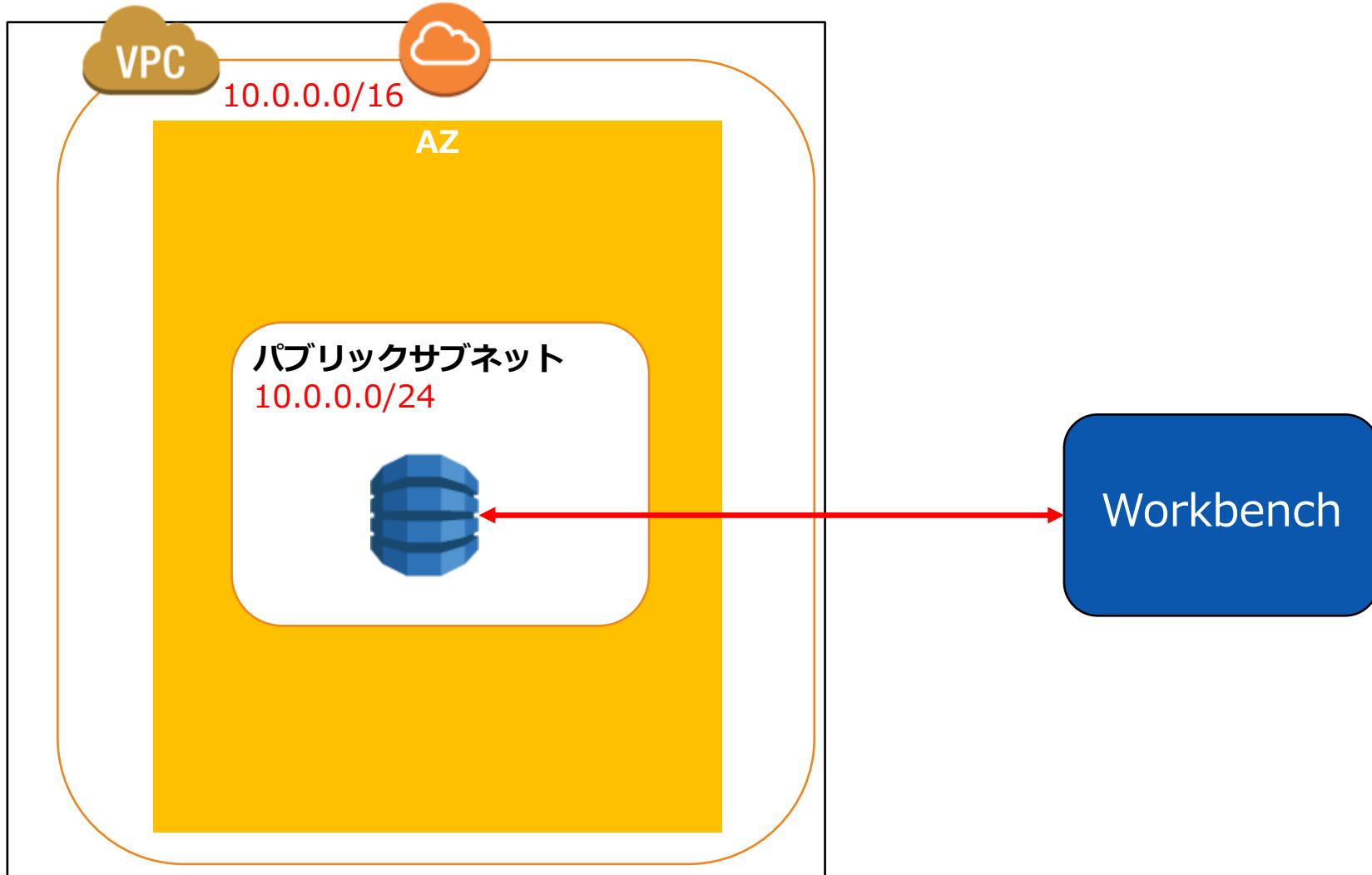
パブリックアクセシビリティ [info](#)

はい
DB インスタンスをホストしている VPC 外部の EC2 インスタンスとデバイスは、DB インスタンスに接続します。DB インスタンスに接続できる EC2 インスタンスおよびデバイスを指定する 1 つ以上の VPC セキュリティグループも選択する必要があります。

いいえ
DB インスタンスにはパブリック IP アドレスが割り当てられていません。VPC 外部のいずれの EC2 インスタンスあるいはデバイスも接続できません。

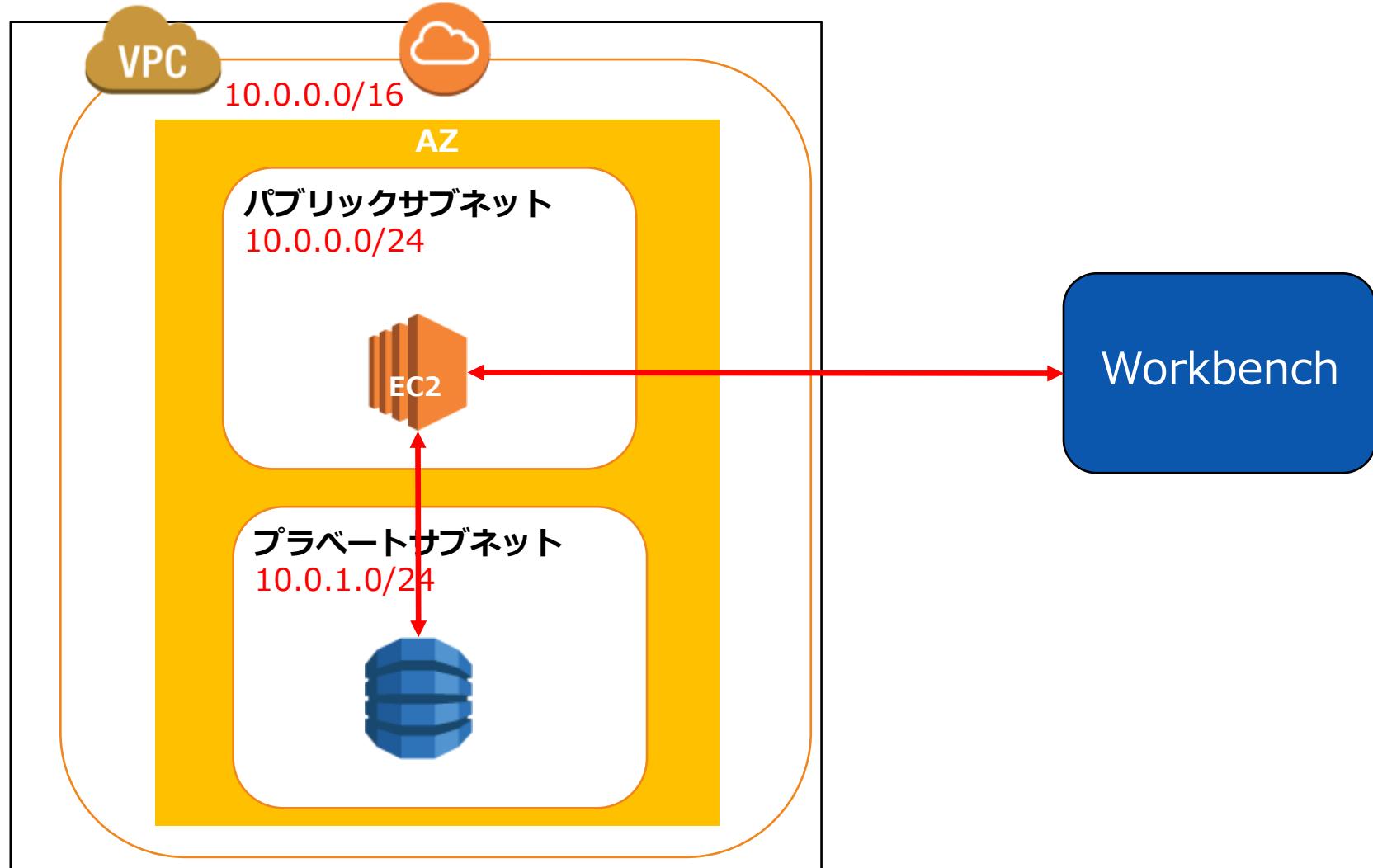
パブリックアクセス構成

パブリックサブネットにRDSを設置し、直接にSQLソフトウェアで接続して操作する。



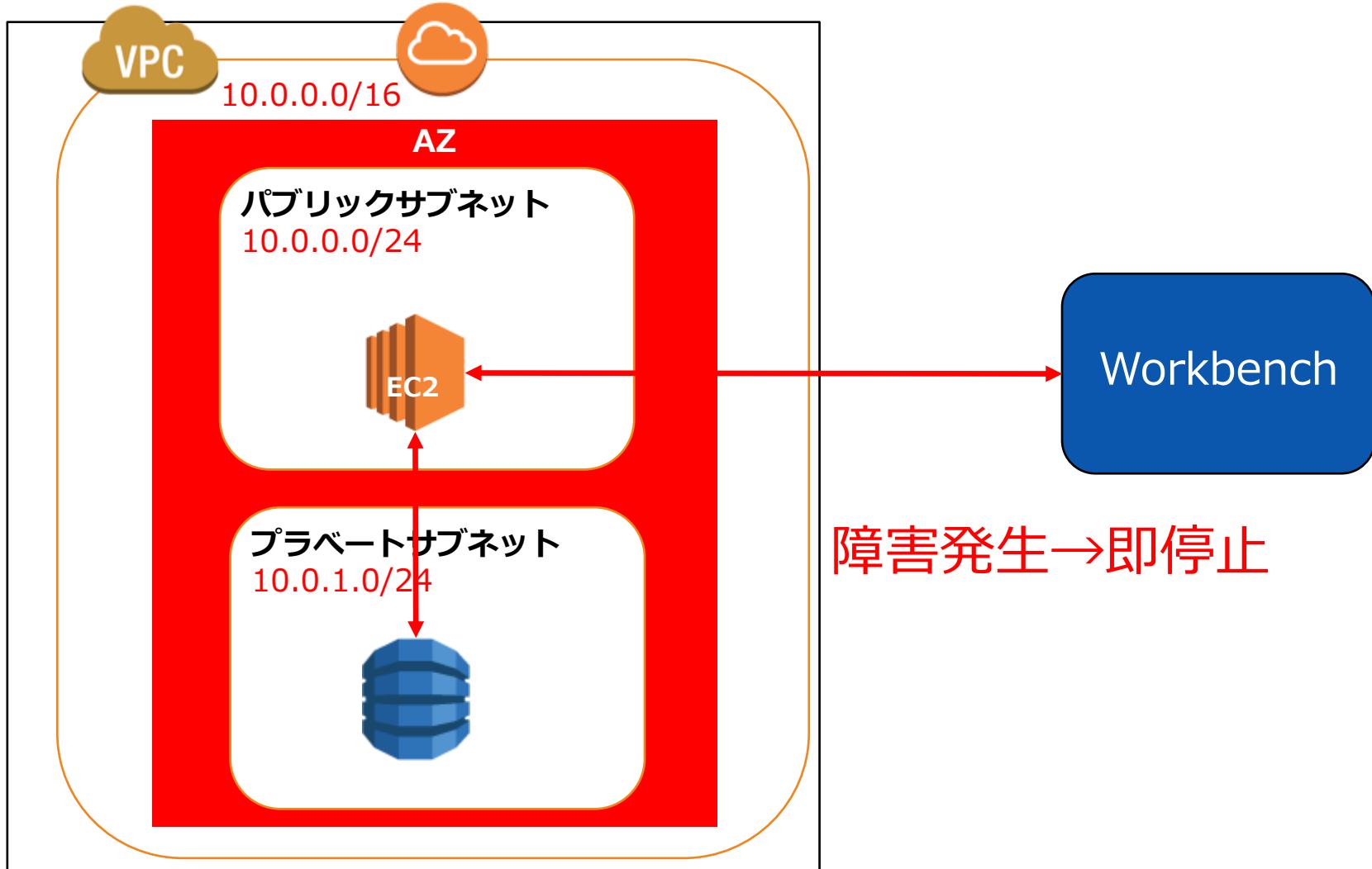
一般的な構成

RDSをプライベートサブネットに設置して、EC2インスタンスを踏み台にしてアクセスする。



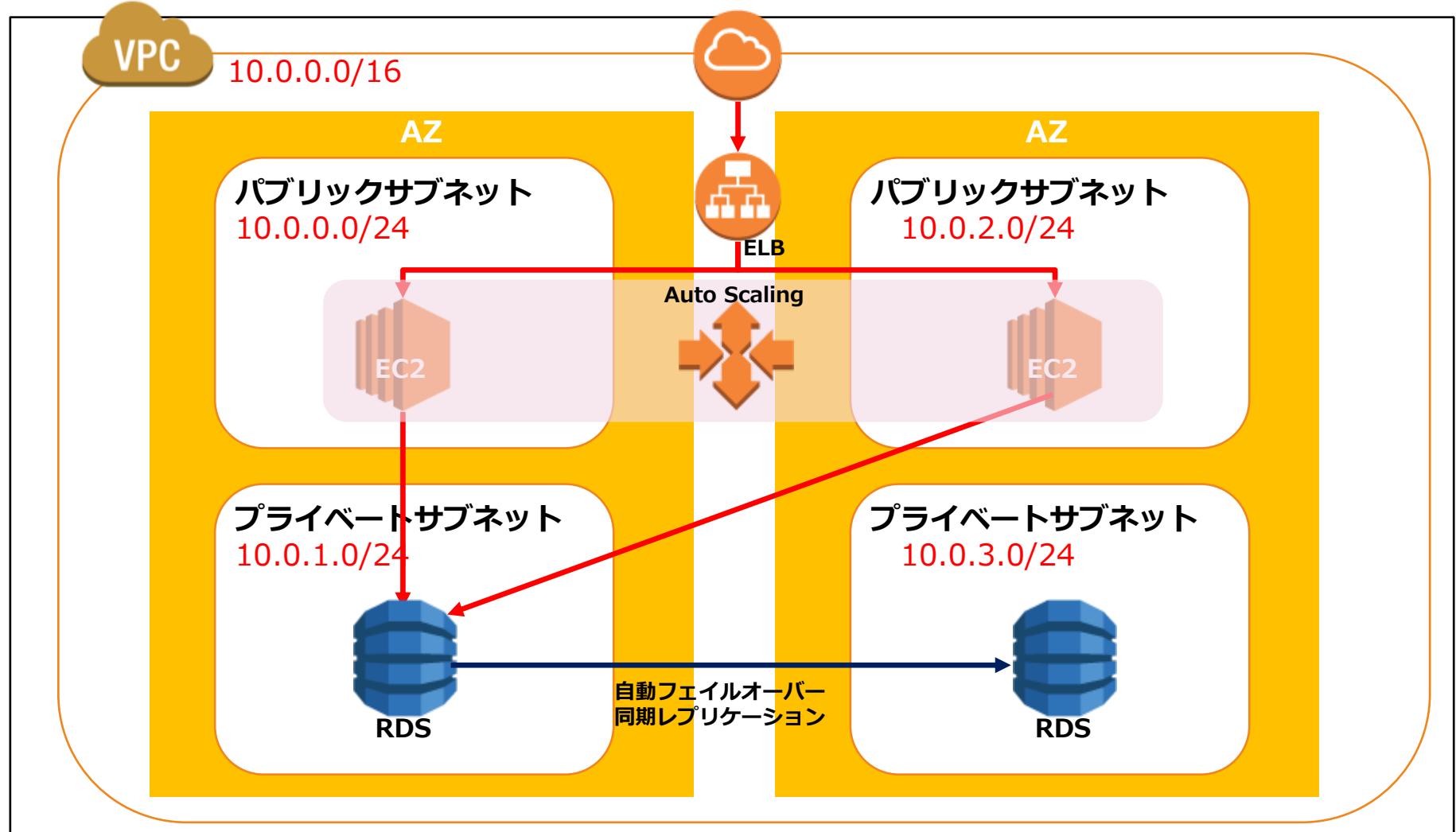
一般的な構成

この構成は1つのAZに依存しているため、AZ障害が発生するとダウンタイムが発生するリスクが高い。



マルチAZ構成

マルチAZ構成にすることで、AZ障害が発生しても停止しない構成をとる必要がある。



[Q]マルチAZ構成による効果

ある会社は自社のエンタープライズシステムの可用性を向上させるためにマルチAZ配置で構成されたRDSデータベースを利用しています。このRDSのプライマリーデータベースに障害が発生しました。

障害後にRDS上で自動でどのような対応がなされているのか選択してください。

- 1) CNAMEレコードがプライマリーからセカンダリーに移行する。
- 2) プライマリーデータベースがリブートする
- 3) RDSのセカンダリーデータベースが構成される。
- 4) スケーリングが実行される。

マルチAZ構成による効果

フェールオーバー設定を有効化するだけで、非常に簡単にフェールオーバーが利用可能となる。

- ✓ プライマリーデータベースとセカンダリーデータベースの構成
- ✓ 2つのデータベースは同期レプリケーションを実施し、常に同じデータ内容を維持
- ✓ プライマリー側に障害が発生した場合、自動でフェールオーバーが実行されセカンダリーデータベースがプライマリーに昇格する。
- ✓ フェールオーバー時にCNAMEレコードがプライマリーからセカンダリーに移行する。
- ✓ スタンバイ状態のDBはアクセス不可

[Q]リードレプリカ

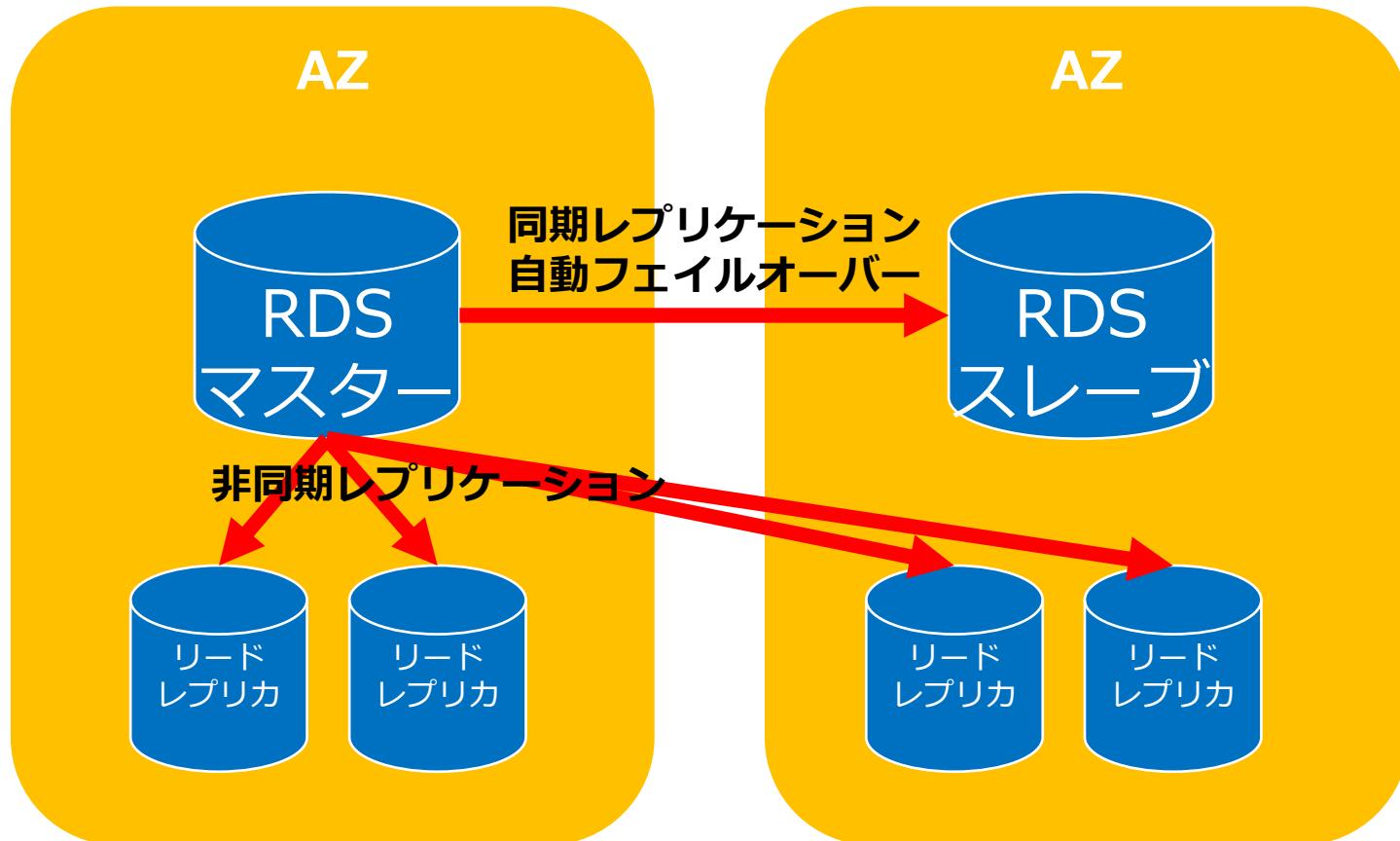
大手ECマース企業は自社のECサイトにRDS PostgreSQLデータベースを使用してます。顧客の購買データを分析して、レコメンデーションなどの機能を実装することが必要です。このような新規機能の分析処理も同じデータベースで実行することになるため、ECサイトの処理速度が低下するなどの悪影響を与えてしまいます。

この問題を解決するための最もコスト最適なソリューションは次のうちどれですか？

- 1) マスターデータベースと同じAZにリードレプリカを作成する。
- 2) マスターデータベースと別のAZにリードレプリカを作成する。
- 3) マスターデータベースと別リージョンにリードレプリカを作成する。
- 4) RDSデータベースでマルチAZを有効にし、スタンバイデータベースで分析ワークロードを実行する。

リードレプリカ

読み取り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



[Q]クロスリージョンの構成

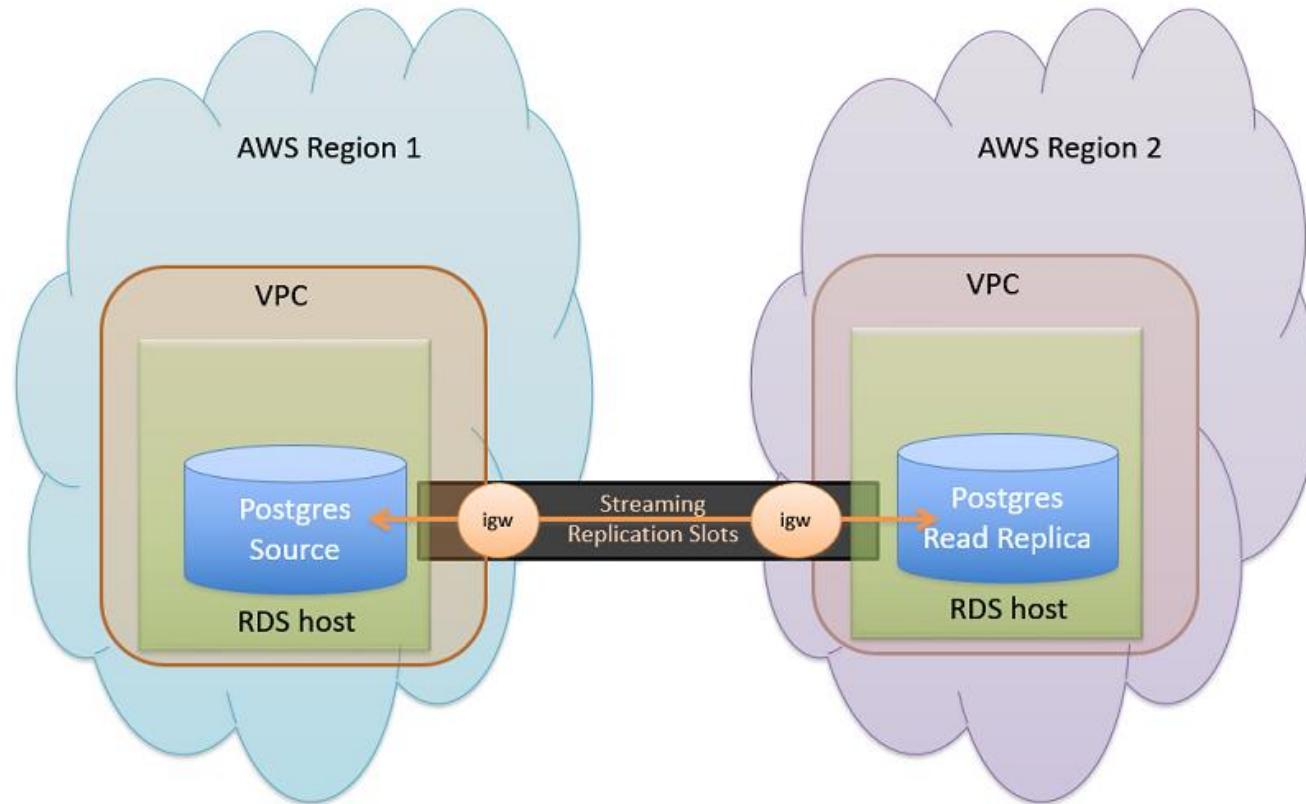
大手ECマース企業は自社のECサイトにRDS PostgreSQLデータベースを使用してます。このECサイトはアジア各国で展開されており、マスターデータベースはシンガポールリージョンに配置されていますが、データベースはローカルの読み取りトランザクション効果的に提供するために増設する必要があります。

この要件を満たすことができる最もコスト最適なソリューションを選択してください。

- 1) RDSのフェールオーバー構成
- 2) クロスリージョン構成のRDS
- 3) マルチマスター構成のRDS
- 4) クロスリージョンリードレプリカを使用したRDS

クロスリージョンの構成

クロスリージョンでリードレプリカを構成することも可能



Reference: <https://aws.amazon.com/jp/blogs/news/best-practices-for-amazon-rds-for-postgresql-cross-region-read-replicas/>

[Q]RDSのスケーリング

あなたはEC2インスタンスとRDSを利用して、2層アプリケーションを構築しています。現段階ではアプリケーションに必要となるワークロード要件は明確ですが、データベース処理に必要な予想されるリクエスト数などのパフォーマンス要件が不明です。したがって、データベースを起動後にスケーリングすることが必要です。

この要件に対してRDSデータベースをデプロイ後に実施するべきスケーリング方法はどれでしょうか？（2つ選択してください）

- 1) リードレプリカを追加する。
- 2) マルチAZ構成を有効化する。
- 3) より最適なインスタンスタイプを選択する。
- 4) より大きなインスタンスサイズを選択する。
- 5) 拡張ネットワーキングを有効化する。

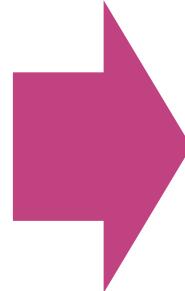
RDSのスケーリング

データベースのパフォーマンス低下に対してスケーリング対応を実施することが求められる

RDSのパフォーマンス低下



- ✓ 読み込み処理が遅い
- ✓ 書き込みが止まる etc



- ✓ スケーリングによってパフォーマンスを向上させる

RDSのスケールアップ

インスタンスタイプやサイズを変更することでスケールアップによるパフォーマンス向上を実施

インスタンスサイズの変更

現在のDBインスタンスタイプに対してサイズを高性能なものに変更することで、パフォーマンスを向上させる。

インスタンスタイプの変更

現在のDB利用方式に適したDBインスタンスタイプがある場合は、そのタイプに変更する。

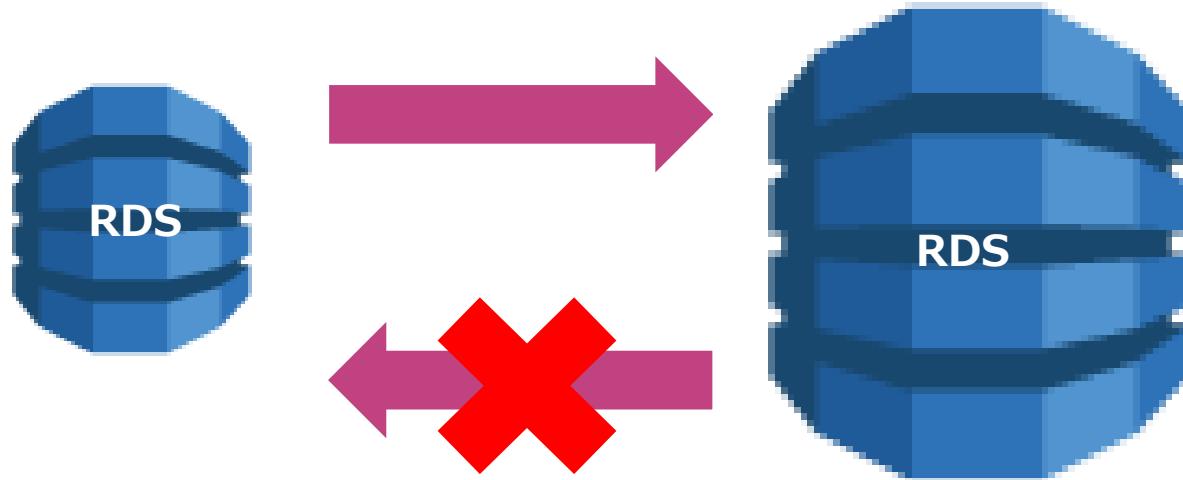
ストレージタイプの変更

ストレージタイプを高性能なタイプ（I/O処理が多い場合はIOPS）に変更する。

ストレージの容量変更

ストレージ容量は設定変更で増加させることはできるが、減少させることはできない。

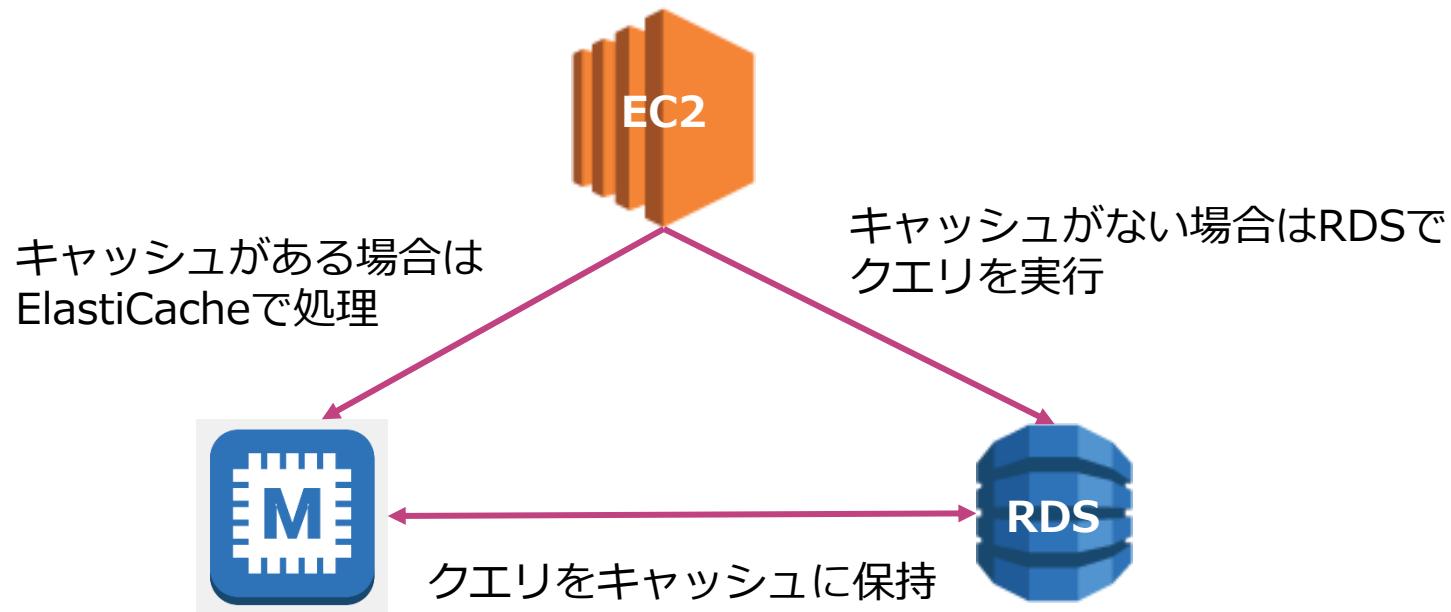
- ✓ ストレージ容量の増加は可能



- ✓ ストレージ容量の減少変更はできない

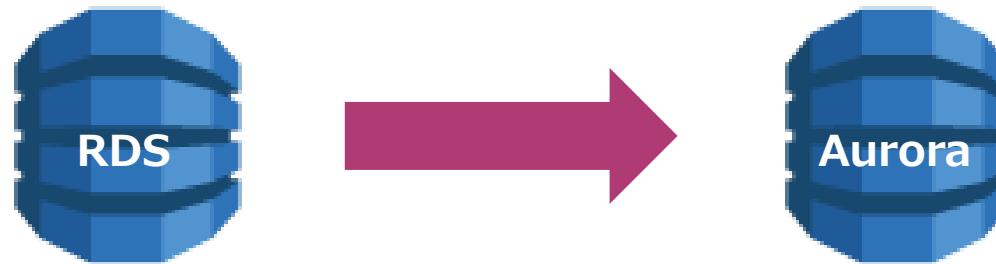
ElastiCacheの利用

読み込み処理の一部をキャッシュに保持して、高速クエリ処理を実現する構成が可能



Auroraへの移行

RDSのMySQLとPostgreSQLはAuroraと互換性があるバージョンは
容易に移行が可能で、パフォーマンスを向上させることができる



[Q] RDSの暗号化

大手ECマース企業は自社のECサイトにRDS PostgreSQLデータベースを使用してます。最近になってIT監査が実施されたところ、RDSデータベースが暗号化されていないことを指摘されました。

このRDSデータベースを暗号化する手順として正しい説明を選択してください。（2つ選択してください。）

- 1) 既存のRDSデータベースのアクション操作において、暗号化オプションの有効化を実施する。
- 2) RDSデータベースのスナップショットを作成し、暗号化されたスナップショットをコピーし、暗号化されたスナップショットからデータベースを復元する。
- 3) 既存のRDSデータベースは暗号化できないので終了する。
- 4) 既存のRDSデータベースの設定変更画面において、暗号化オプションの有効化を実施する。
- 5) RDSデータベースの暗号化されたリードレプリカを作成し、これをマスターデータベースに昇格させる。

RDSの暗号化

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

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。

DB RDS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暗号化を設定可能
- スナップショットのコピーの暗号化／リストア可能

[Q]メンテナンス

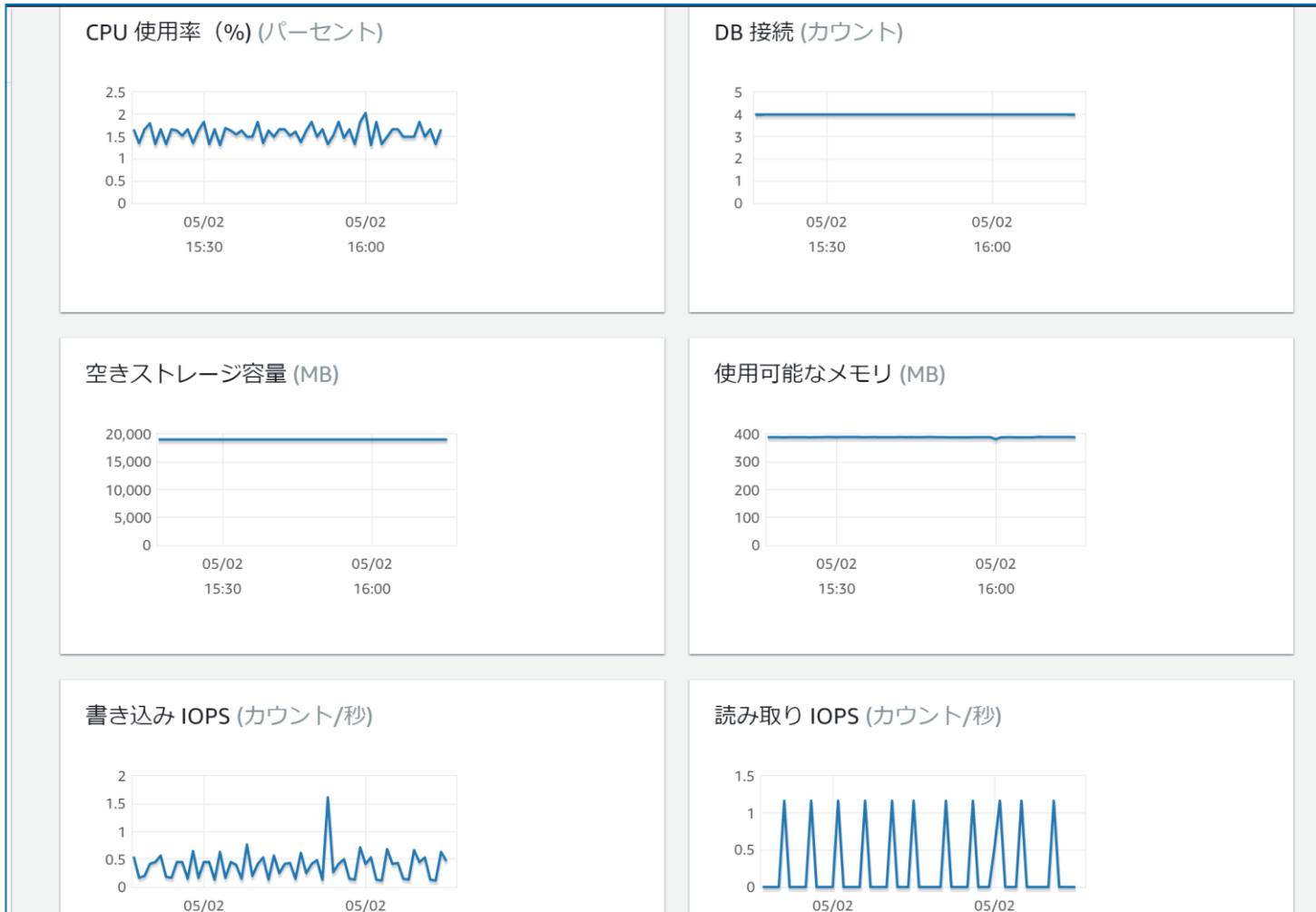
B社はAWS上にデータベース環境を整備しようと計画しています。RDSを利用するこ
とを検討していますが、メンテナンスの多くがマネージド型サービスで提供されるた
め、その内容を把握することが必要です。特に、メンテナンスウィンドウ中にDBが
強制的にオフラインになると影響が大きいため、その期間を回避することが必要です。

次のメンテナンスイベントの中で、データベースのダウンタイムが発生する内容を選
択してください。（2つ選択してください。）

- 1) セキュリティパッチの適用
- 2) マルチAZ機能の適用
- 3) データベースのアップデート
- 4) DBパラメーターグループの更新
- 5) オプショングループの更新

AWSコンソールダッシュボード

RDSのコンソールダッシュボードには、RDSインスタンスの状態が一目でわかるビューが表示される。



ログの確認

ダッシュボードでログの確認・ダウンロードを実施可能

DBエンジン	ログのタイプ	ログの保持期間 (デフォルト)
MySQL/MariaDB	<ul style="list-style-type: none">一般クエリログエラーログスロークエリ	<ul style="list-style-type: none">24時間
Oracle	<ul style="list-style-type: none">アラートログ監査ログトレースログ	<ul style="list-style-type: none">アラートログは30日監査ログとトレースログは7日
SQL Server	<ul style="list-style-type: none">エラーログエージェントログトレースログ・ダンプログ	<ul style="list-style-type: none">7日
PostgreSQL	<ul style="list-style-type: none">クエリログエラーログ	<ul style="list-style-type: none">3日

CloudWatchとの連携

CloudWatchと連携して、集中的にRDSのメトリクスに基づいた運用管理を実行することが可能となる。

CloudWatch メトリクス	Amazon RDS のアクティブな各データベースのメトリクスを 5 分間隔の取得して、ダッシュボードに表示する。
拡張モニタリング	送信間隔を秒単位でメトリクスが取得され、ほぼリアルタイムでのモニタリングが可能となる。 モニタリングコストが有料になる。
CloudWatchアラーム	特定の期間にわたって単一の Amazon RDS メトリクスを監視し、指定したしきい値に関連するメトリクス値に基づいて 1 つ以上のアクションを実行できる
CloudWatch Logs	CloudWatch Logs のデータベースログファイルの監視、保存、およびアクセスが可能になる。
CloudWatchイベント	CloudWatchイベントでは、イベントパターンを使用して受信イベントをフィルタリングし、ターゲットをトリガーするルールを作成することができる。

AWS コンソールダッシュボード

メンテナンスとバックアップではメンテナスウィンドウとバックアップウィンドウの設定が確認できる

The screenshot shows the AWS RDS maintenance and backup configuration interface. It includes sections for maintenance windows, reserved maintenance, and backup windows.

メンテナンス (Maintenance)

マイナーバージョン自動アップグレード 有効	メンテナスウィンドウ mon:19:55-mon:20:25 UTC (GMT)	メンテナスの保留中	保留中の変更
--------------------------	---------------------------------------------	-----------	--------

保留中のメンテナンス (0) (Reserved Maintenance (0))

C	今すぐ適用	次のメンテナスウィンドウで適用					
保留中のメンテナンス のフィルタリング							
説明	▼	タイプ	▼	ステータス	▼	日付の適用	▲
保留中のメンテナンスはありません							

バックアップ (Backups)

自動バックアップ 有効 (10 日) スナップショットにタグをコピー ー 有効	復元可能な最も早い時刻 May 2nd 2020, 4:10:00 pm UTC--9 (local)	バックアップウィンドウ 13:50-14:20 UTC (GMT)
-----------------------------------------------------	--------------------------------------------------------	--------------------------------------

必要なオペレーティングシステムやデータベースのパッチの適用時にはDBインスタンスを一時的にオフラインにするので注意が必要

[Q] バックアップ

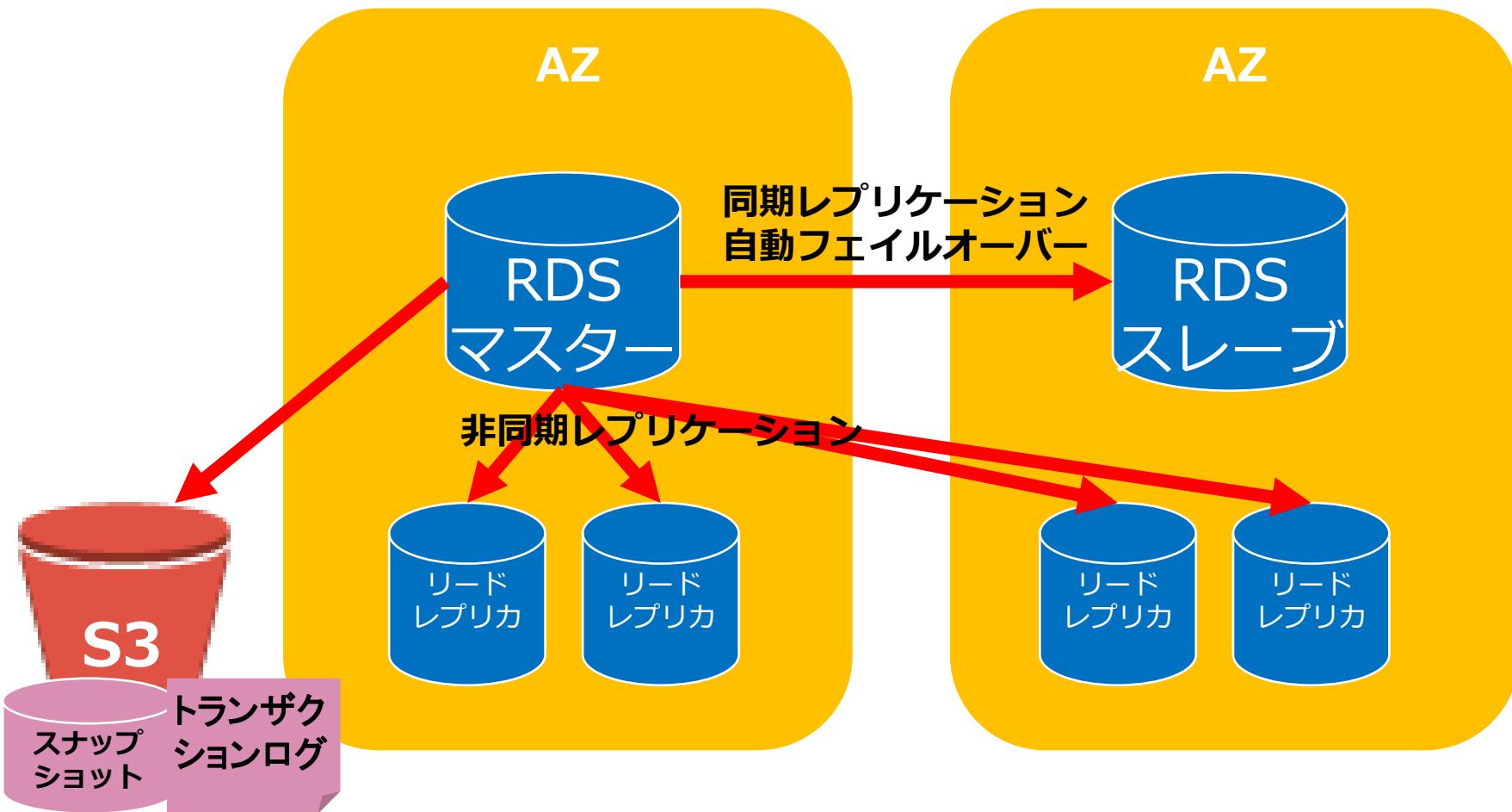
B社はAWS上にRDSを利用してデータベース環境を利用しています。しかしながら、データベースが障害によって破損したため、復元が必要となりました。あなたはソリューションアーキテクトとして、ポイントインタイムリカバリを使用して、データの最新な構成にリカバリすることになりました。

RDSデータベースを特定の時点に復元する正しい方法はどれでしょうか？（2つ選択してください）

- 1) スナップショットとトランザクションログがDBを5分前の状態に復元できる。
- 2) スナップショットのみがDBを5分前の状態に復元できる。
- 3) トランザクションログのみがDBを5分前の状態に復元できる。
- 4) スナップショットとトランザクションログがDBを10分前の状態に復元できる
- 5) スナップショットのみがDBを10分前の状態に復元できる。
- 6) トランザクションログのみがDBを10分前の状態に復元できる。

バックアップ

スナップショットを取得することでデータを保存し、耐障害性を確保することができる。



バックアップ

RDSのバックアップはスナップショットで取得され、2つの方法が提供されている。

自動バックアップ

自動バックアップ有効化されると、Amazon RDS は毎日、データのスナップショットを自動的に作成するポイントタイムリカバリが可能

スナップショットの取得

ユーザーによって指定された頻度でスナップショットを取得することが可能

自動バックアップ

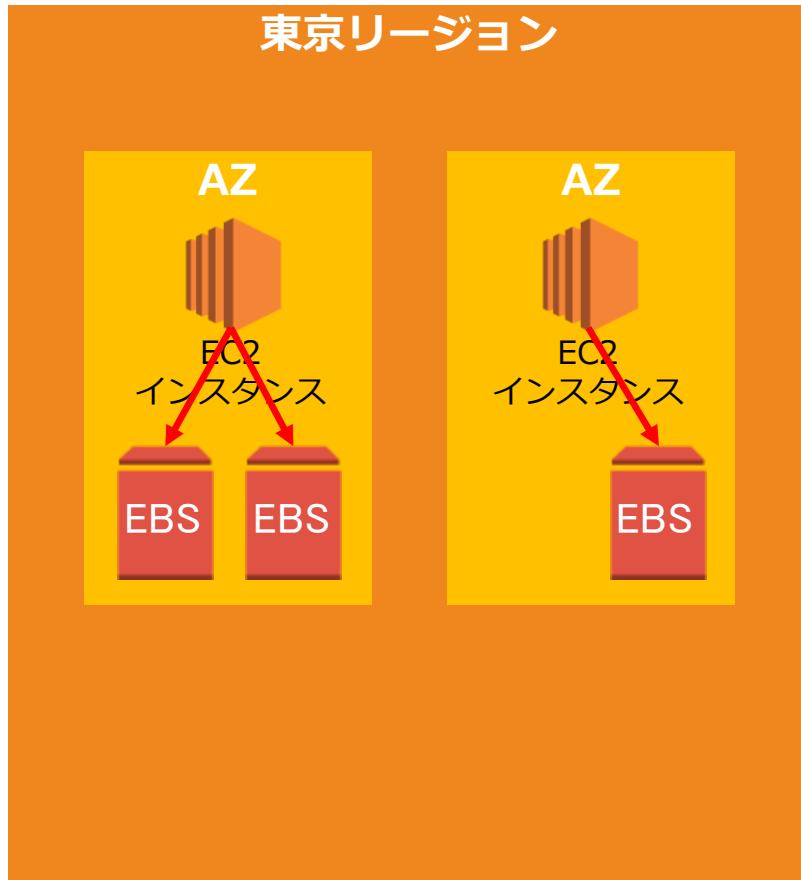
自動バックアップはRDS側で管理された定期的スナップショット取得を自動で実施する。

- ✓ 自動でのスナップショット取得とトランザクションログを取得
- ✓ 最も適切なデイリーバックアップとトランザクションログを利用して、DB インスタンスを特定の時刻の状態に復元することができる。
- ✓ バックアップサイクルは「1日1回」で固定されている。
- ✓ 5分毎にトランザクションログのアーカイブを自動で行っており、これにより、ポイントインタイムリカバリが可能となる。
- ✓ バックアップの保存期間はデフォルト7日で最大35日まで設定できる。
- ✓ 増分バックアップを実施する。
- ✓ RDSのバックアップはAWSが管理するS3ストレージに保存される。
- ✓ DBインスタンスを削除した場合や自動バックアップを無効にした場合に、スナップショットは削除される。

EBSの出題範囲

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の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

EBSの選択	✓ シナリオのストレージ要件を満たすストレージを選択する質問
EBSの特徴	✓ EBSの特徴を回答させる質問 ✓ EC2インスタンスにEBSのアタッチ方式やインターネットからのアクセスの有無などに関する質問
EBSボリュームタイプの選択	✓ シナリオに基づいてワークロードの要件が提示され、EBSボリュームタイプを選択する質問が出題される。
スナップショットの特徴	✓ EBSのスナップショットの機能や特徴に関する質問が出題される。
スナップショットの管理	✓ スナップショットを利用して定期的なバックアップ取得などの設定方法が出題される。

EBSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

スナップショットの共有	<ul style="list-style-type: none">✓ スナップショットを別アカウントと共有する方法が問われる。✓ スナップショットを別リージョンと共有する方法が問われる。
EBSボリュームの削除	<ul style="list-style-type: none">✓ EBSボリュームが削除される設定状況が問われる。✓ EC2インスタンスが削除された際のEBSの挙動が問われる。
EBSの暗号化	<ul style="list-style-type: none">✓ EBSの暗号化設定の方法が問われる。✓ EBSの暗号化対象範囲が問われる。✓ 暗号化されたスナップショットの利用上の制約などが問われる。
EBSのステータス	<ul style="list-style-type: none">✓ EBSのステータスに応じた特徴が問われる。
EBSのRAID構成	<ul style="list-style-type: none">✓ EBSを利用したRAID0とRAID1の構成と利用方法が問われる。

[Q] EBSの選択

大手金融機関はAWSを利用してFintech事業用のアプリケーションを開発しています。このアプリケーションでは、EC2インスタンスを利用してアプリケーションのデータ処理を実施する必要があり、データへの最小遅延アクセスを提供できるストレージサービスが必要です。データ容量は10TBまで増大することが予想されています。

この要件を満たす最も適切なストレージサービスは次のうちどれですか？

- 1) EFS
- 2) インスタンスストア
- 3) EBS
- 4) S3
- 5) Amazon FS x

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

[Q] EBSの特徴

B社ではWEBアプリケーションをAWS上に構築しています。あなたはソリューションアーキテクトとして、WEBサーバー用のストレージとしてEBSボリュームの汎用SSDを利用することにしました。複数のEC2インスタンスと複数のEBSボリュームを連携して利用するつもりですが、どのような設定が可能か調べています。

EBSボリュームの正しい説明は次のうちどれですか？

- 1) EBSボリュームは複数インスタンスにアタッチできる。
- 2) EBSボリュームは同じリージョンのインスタンスであればアタッチできる。
- 3) EBSボリュームは同じVPCのインスタンスにのみアタッチできる。
- 4) EBSボリュームは同じAZ内のインスタンスにのみアタッチできる。

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】

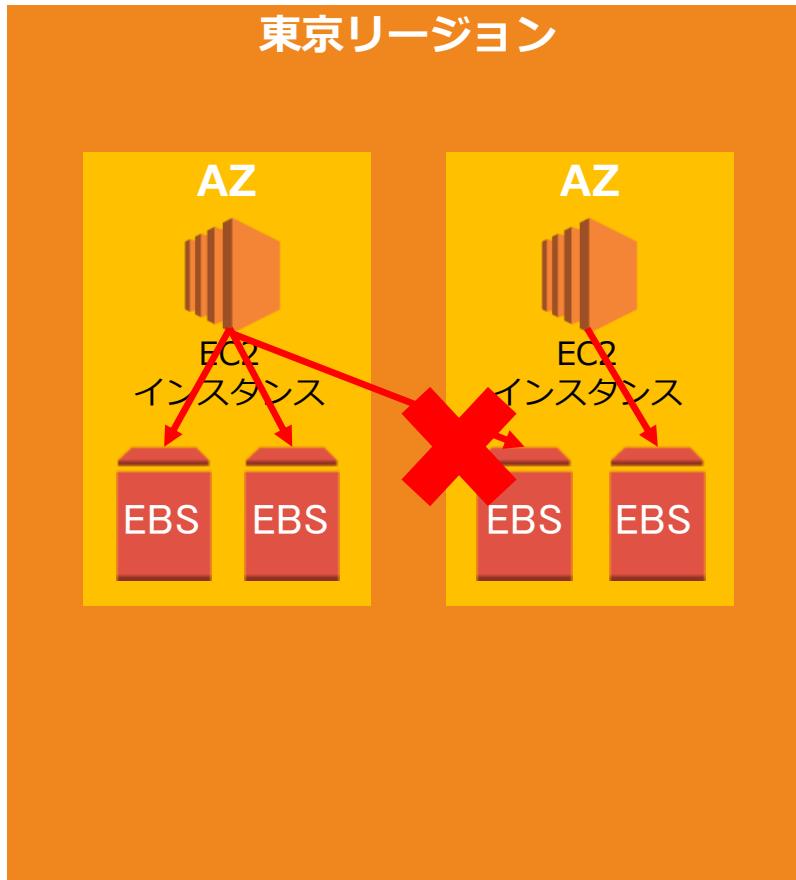
- ✓ OSやアプリケーション、データの置き場所など様々な用途で利用される
- ✓ 実体はネットワーク接続型ストレージ
- ✓ 99.999%の可用性
- ✓ サイズは1 GB～16TB
- ✓ サイズと利用期間で課金

【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。

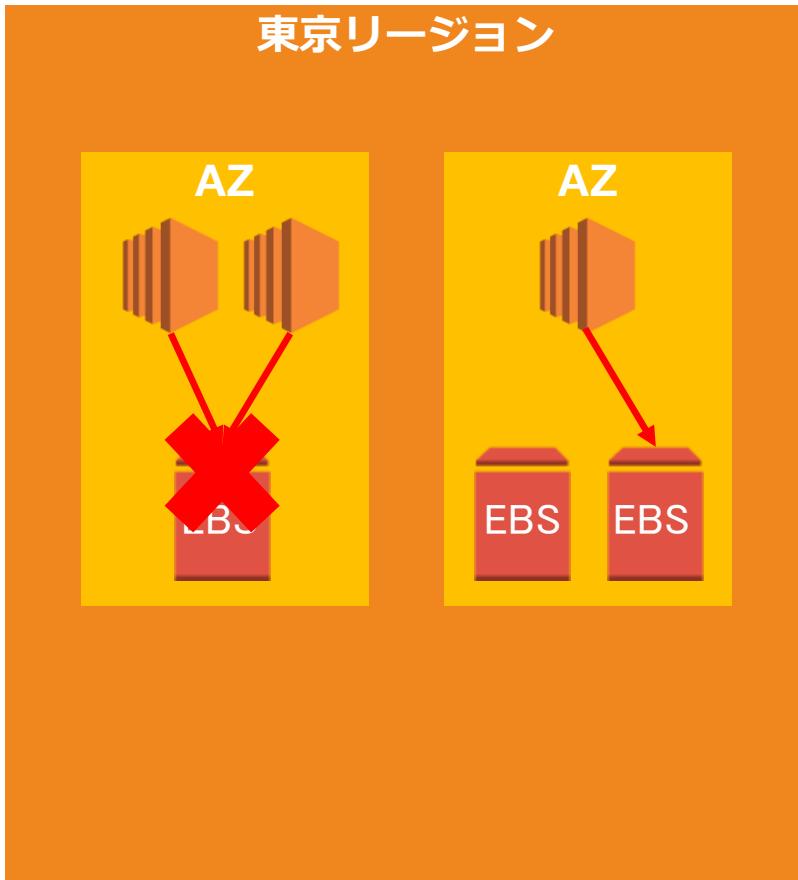


【特徴】

- ✓ 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。

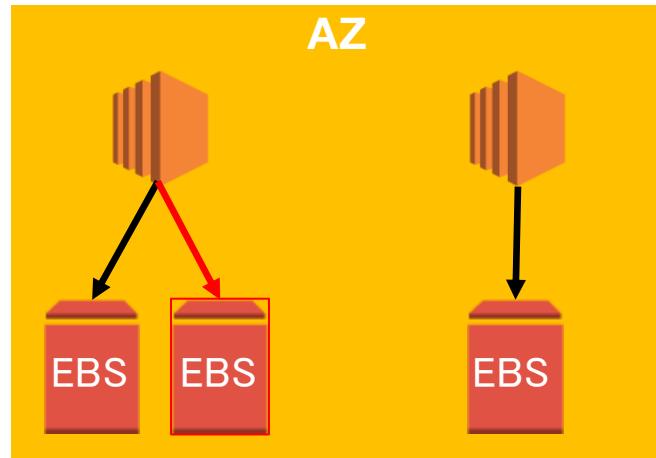


【特徴】

- ✓ 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

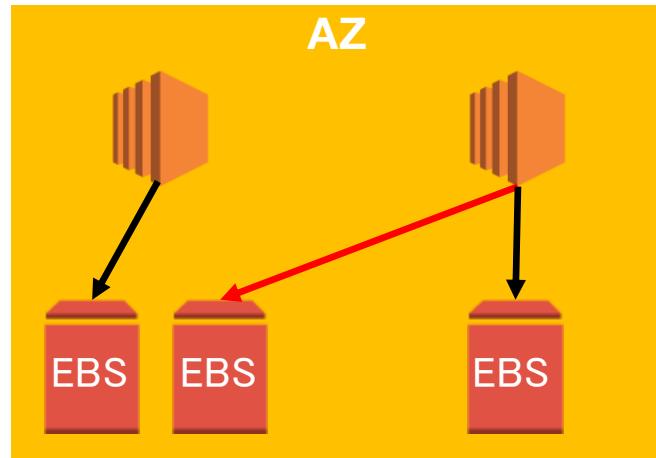


【特徴】

- ✓ 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

[Q] EBSボリュームタイプの選択

あなたはソリューションアーキテクトとして、新しいECアプリケーションをモバイル用に構築しています。現在はEC2 APIを介してEC2インスタンスをプロビジョニングする対応を行っています。これらのインスタンスは、顧客データに応じて顧客に最適な画面を表示させます。ストレージの非機能要件として、ブートボリュームに使用できないボリュームタイプをすることが必要です。

EC2インスタンスのブートボリュームとして使用できないストレージボリュームタイプはどれでしょうか？（2つ選択してください）

- 1) 汎用SSD
- 2) プロビジョンドIOPSSSD
- 3) インスタンスストア
- 4) スループット最適化HDD
- 5) コールドHDD

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

[Q]スナップショットの特徴

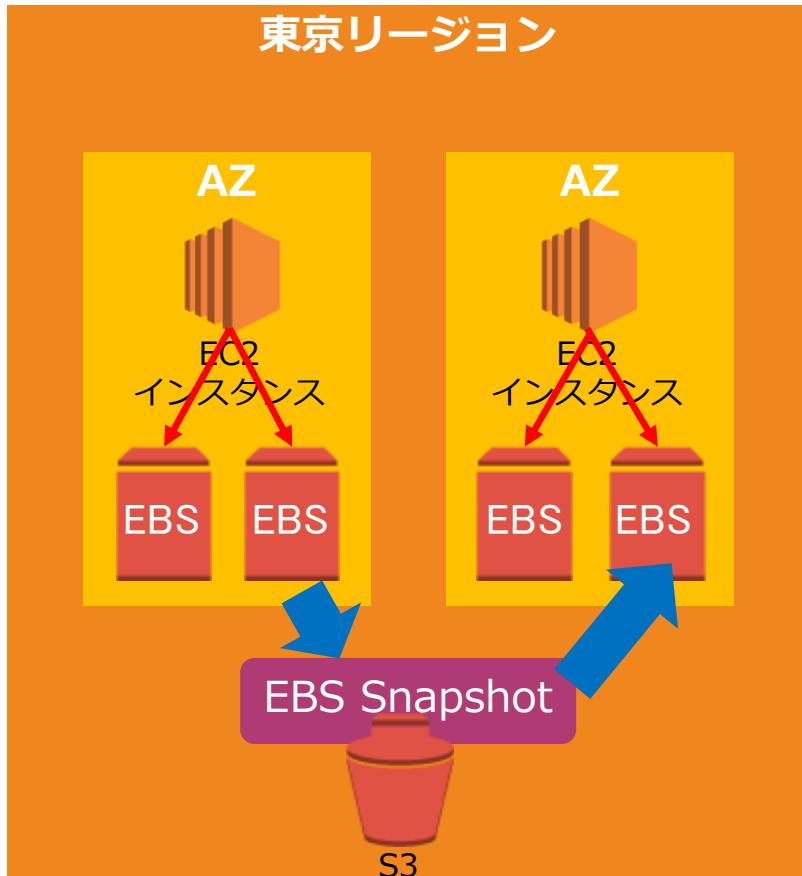
あなたはソリューションアーキテクトとして、会社内でAWSの管理を任せています。この会社ではAWSの利用コストが増大しており、 AWS Trusted Advisorを利用してコスト最適の余地を検証しました。 AWS Trusted Advisorによるとスペースとコストを節約するために、未使用のEBSボリュームとスナップショットをクリーンアップすることによってコストを削減できるようです。

スナップショットを削減する際の注意点として正しい説明はどれでしょうか？

- 1) 増分スナップショットであるため一連のスナップショットのいづれかを削除すると他のスナップショットが利用できなくなる。
- 2) 増分スナップショットであるが、最新のスナップショット以外を削除しても最新のスナップショットだけでEBSを復元できる。
- 3) 増分スナップショットであるため最初のスナップショットと最新のスナップショットだけは保持する必要がある。
- 4) 増分スナップショットであるため最初のスナップショット以外は削除できる。

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。

[Q]スナップショットの管理

会社ではEBSを複数利用したWEBアプリケーションを利用しています。セキュリティ規定によるバックアップを定期的に実行することが必要ですが、現在は手動で行っており非常に手間がかかります。そのため、EBSボリュームのバックアップの作成、保持、および削除を自動化する方法を実装したいと考えています。

EBSのこれらのタスクを自動化する最も簡単な方法は何ですか？

- 1) S3でバックアップを作成するようにEBSボリュームレプリケーションを構成する
- 2) AWS CLIコマンドでスナップショットの実行スクリプトを定義する。
- 3) データライフサイクルマネージャー（DLM）を使用して、ボリュームのスナップショットを管理する。
- 4) EBSコンソール画面で自動バックアップを有効化する。

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。

[Q]スナップショットの共有

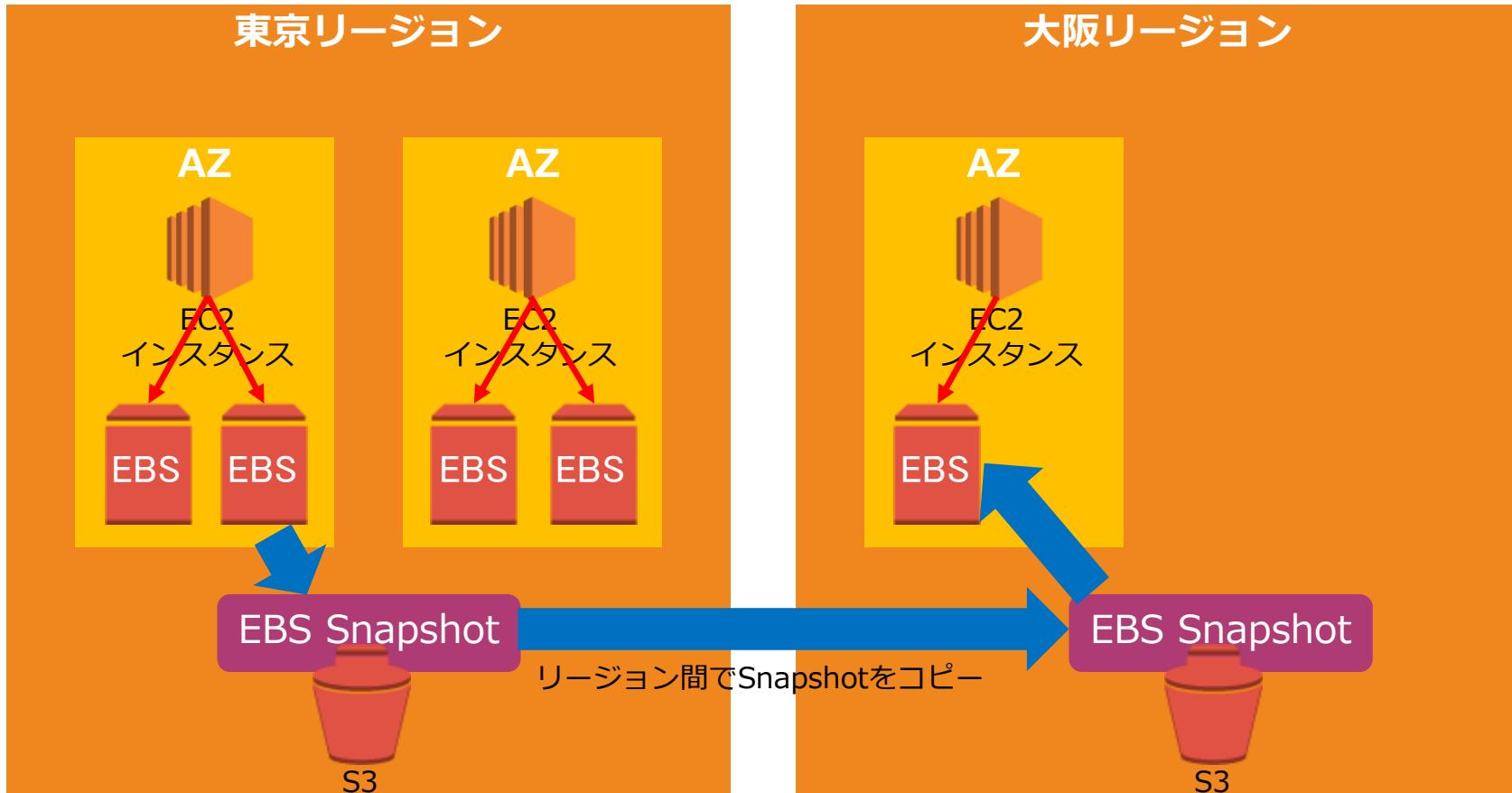
会社は複数部門でAWSアカウントを有してAWSリソースを様々な用途に利用しています。A部門のAアカウントにあるEBSをB部門のBアカウントでも利用することが必要となっており、あなたはソリューションアーキテクトとして、対応を求められています。このスナップショットは、カスタムキーで暗号化されたEBSボリュームから取得されました。

暗号化されたEBSスナップショットを共有する手順の正しい組合せはどれでしょうか？（2つ選択してください）

- 1) EBSボリュームのコピーを別アカウントにコピーする設定を行う。
- 2) EBSスナップショットの暗号化を非有効化する。
- 3) EC2コンソール画面でBアカウントIDを指定したスナップショットの共有設定を行う。
- 4) ボリュームの暗号化に使用されるカスタマーキーを共有する
- 5) EC2コンソール画面で暗号化されたスナップショットの権限を変更して、Bアカウントに設定する。

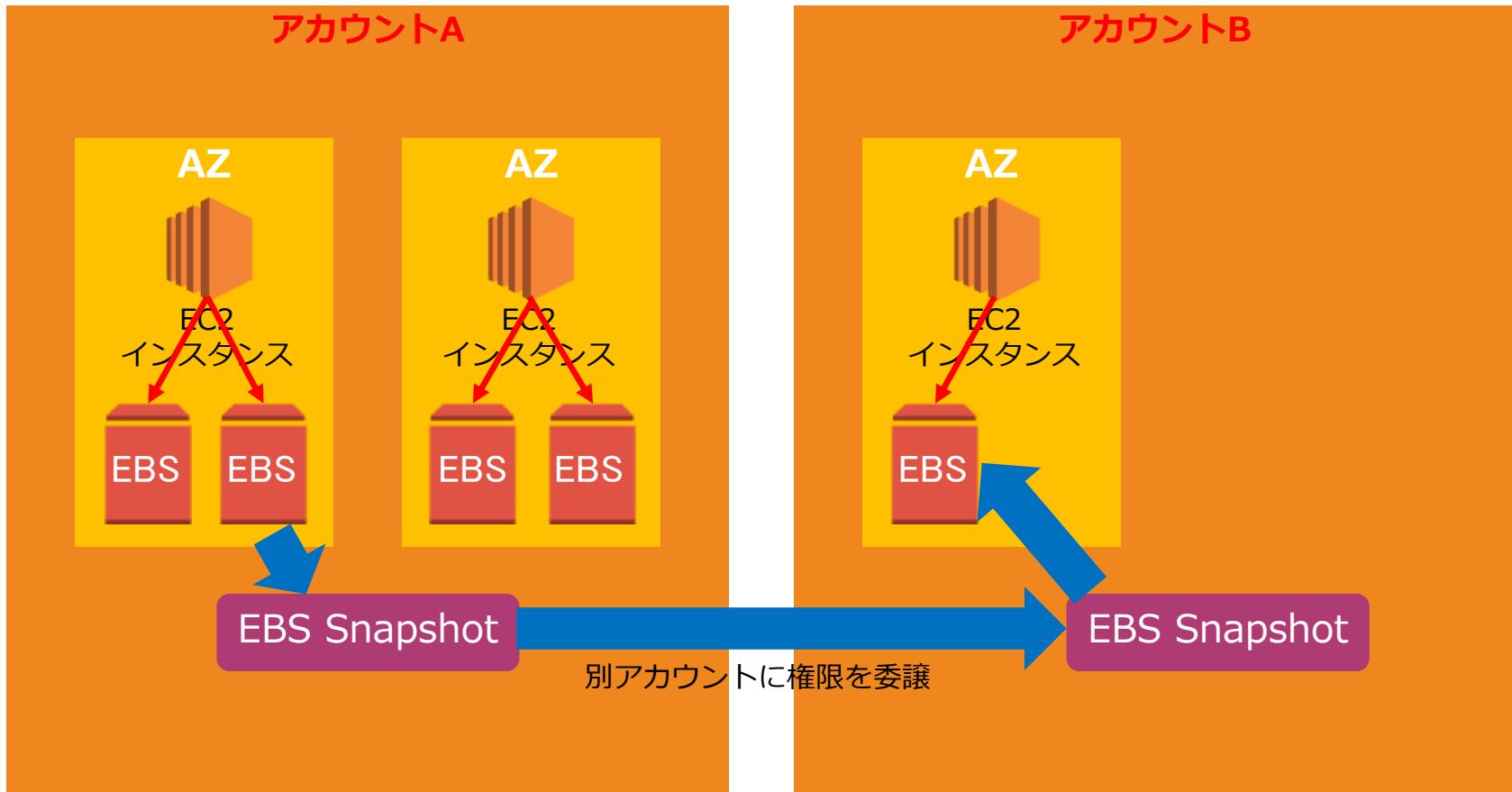
スナップショットの共有

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

[Q] EBSボリュームの削除

研究チームではデータ解析にEC2インスタンスを利用しています。日々収集されるデータをEBSボリュームがアタッチされたEC2インスタンスでバッチジョブとして分析ワークフローを実施します。分析の実行中に、チームはEC2インスタンスを終了すると、接続されているEBSボリュームも失われることを発見しました。

この問題に関する最も可能性が高い原因は何でしょうか？

- 1) EC2インスタンスがインスタンスストアベースAMIで作成されているため、ルートボリュームがデータを一時的にしか保存できない。
- 2) EBSボリュームのスナップショット取得を実施していないため、終了時にデータを保持できなかった。
- 3) EC2インスタンスの終了時に、EBSボリュームの保護をチェック入れていないため、EBSボリュームを同時に削除してしまった。
- 4) EBSボリュームがEC2インスタンスのルートボリュームとして設定されているとインスタンスの終了時のデフォルトの動作では、接続されているルートボリュームも終了する。

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

[Q] EBSの暗号化

研究機関ではデータ解析にEC2インスタンスを利用しています。日々収集されるデータをEBSボリュームがアタッチされたEC2インスタンスでバッチジョブとして実施します。これらのデータは非常に機密性が高いため、EBSに保存されている機密データはHIPAAコンプライアンス基準を満たす必要があります。

暗号化されたEBSボリュームの正しい説明はどれでしょうか？（3つ選択してください）

- 1) ボリューム内に保存されるデータは暗号化される
- 2) ボリュームのスナップショットは暗号化される
- 3) ボリュームとインスタンス間を移動するデータは暗号化されていない。
- 4) ボリュームとインスタンス間を移動するデータ暗号化にはSSL証明書が必要である。
- 5) ボリュームのスナップショットは別途スナップショットの暗号化を実施する必要がある。

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

[Q] EBSのステータス

あなたはAWSアカウントを作成して、新規にEC2インスタンスを起動しました。起動したEC2インスタンスを確認すると、EC2のステータスチェックが不十分なデータ（Insufficient Data）と表示されています。

このようなステータスとなった最も可能性の高い説明は何ですか？

- 1) ボリュームのチェックが進行中である。
- 2) EBSがボリューム制限を超過している。
- 3) ボリュームのチェックに失敗した。
- 4) ボリュームには十分なデータがない。

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

[Q]EBSのRAID構成

あなたはソリューションアーキテクトとして、EC2インスタンスのWebサーバーとデータベースを利用して業務アプリケーションを構築しました。リレーショナルデータベースをホストするために、1つの500 GB EBSボリュームを持つ大規模なEC2インスタンスを使用しています。パフォーマンスを確認すると、データベースへの書き込みスループットを向上させる必要があることが判明しました。

この要件を満たすための方法を選択してください（2つ選択してください。）

- 1) EC2インスタンスのサイズを増やす。
- 2) 2つ以上のEBSボリュームを利用したRAID0構成を設定する
- 3) 2つ以上のEBSボリュームを利用したRAID1構成を設定する
- 4) EC2インスタンスをクラスター・プレイスメント・グループに設置する。
- 5) PV AMIを利用してECインスタンスを再起動して、拡張ネットワークを有効化する。

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。

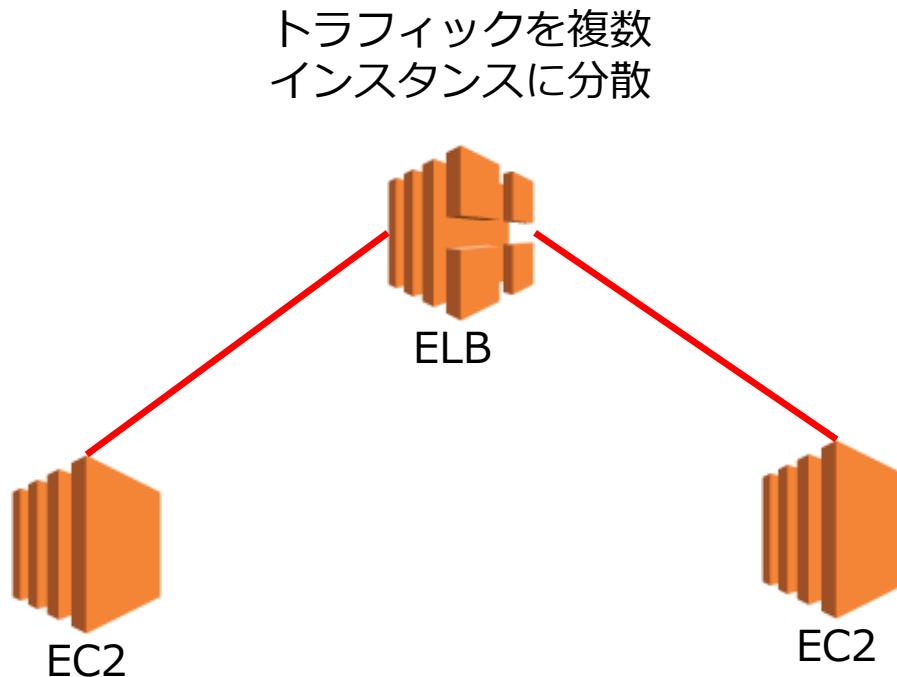
RAID 1

- ✓ 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。

ELBの出題範囲

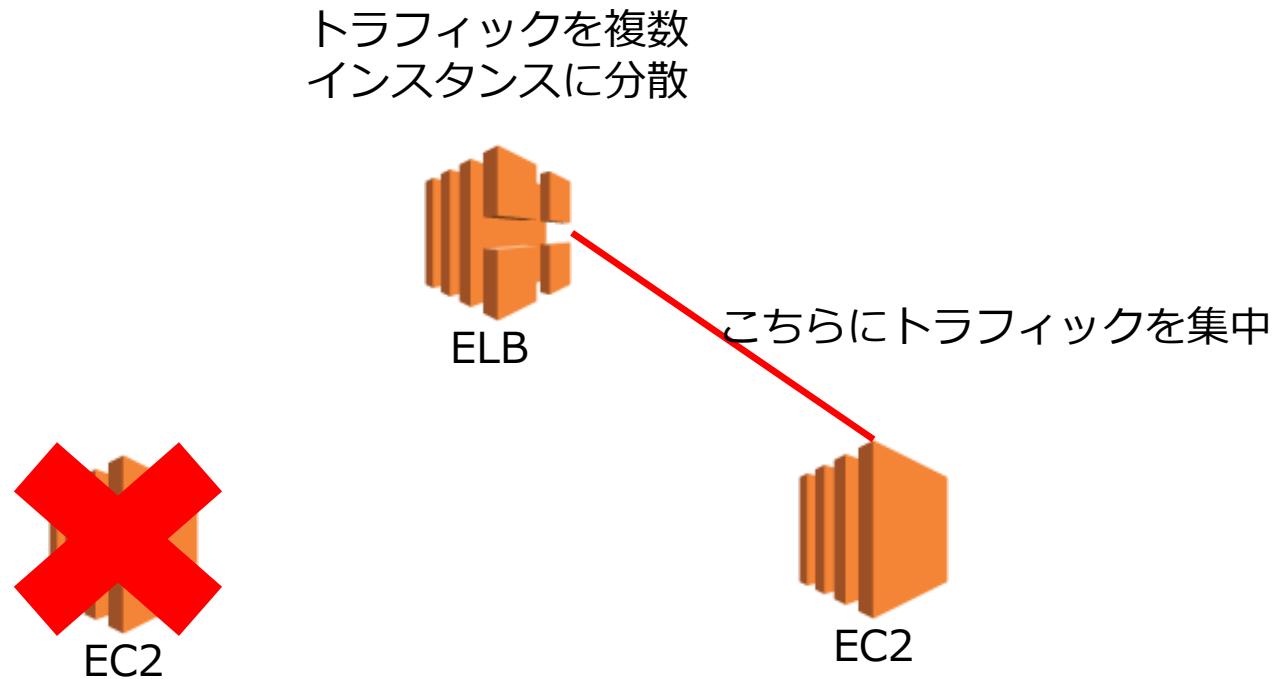
ELBとは何か？

ELBは複数のEC2インスタンスで処理を可能にするロードバランサーを提供するサービス



ELBとは何か？

EC2インスタンスのヘルスチェックを行い、正常なインスタンスのみを利用することも



ELBの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

ELBの特徴	✓ Route53との違いも含めて、 ELBの利用方法や特徴に関する質問が問われる
ELBの構成	✓ ELBを利用した基本的なアーキテクチャ構成に関する質問が出題される。 ✓ セキュリティ要件に基づいてインターナルELBを利用した構成方法が問われる。
ELBタイプの選択	✓ シナリオに基づいてELBを利用するべき要件が説明されて、 どのELBタイプを利用するべきかが問われる。
ALBの特徴	✓ ALBの機能や他のELBタイプとの違いに関する質問が出題される。
NLBの特徴	✓ NLBの機能や他のELBタイプとの違いに関する質問が出題される。

ELBの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

クロスゾーン負荷分散	✓ ELBのクロスゾーン負荷分散に関する特徴やユースケースに関する質問が出題される。
暗号化	✓ ELBの暗号化の設定方法に関する質問が出題される。
ステイッキーセッション	✓ ELBのステイッキーセッションに関する特徴やユースケースに関する質問が出題される。
Connection Draining	✓ ELBのConnection Drainingに関する特徴やユースケースに関する質問が出題される。
ログ取得	✓ ELBのログ取得方法に関する質問が出題される。

[Q] ELBの特徴

あなたの会社は複数部門でAWSを利用しておあり、アプリケーション毎にVPCを設定しています。あなたはソリューションアーキテクトとして、アプリケーション間連携機能を実装しています。その実装には、それぞれのVPCをピアリング接続を構成しまして単一のELBを使用して、同じリージョン内のピアリングされたVPC内の複数のEC2インスタンスにトラフィックをルーティングしたいと考えています。

このようなELBの構成をどのように達成することができますか？

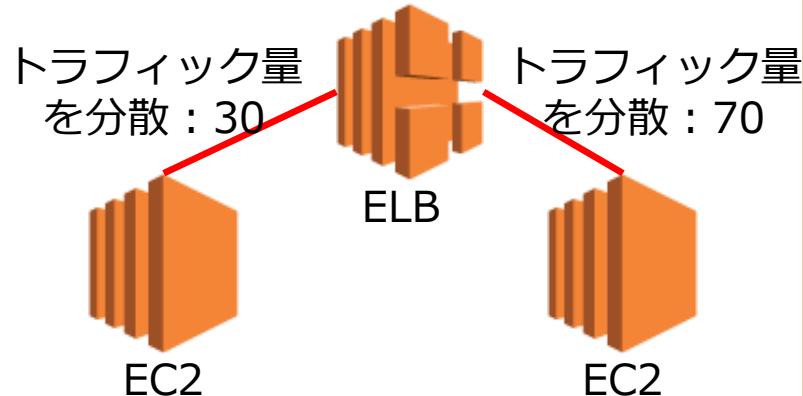
- 1) NLBまたはALB によりIPアドレスをターゲットとして利用する。
- 2) どのELBでもVPCを跨いだ構成を実現可能である。
- 3) この要件にはELBではなくRoute53を使用する必要がある。
- 4) ELBではVPC間を跨いだ構成ができない。

ELBの特徴

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

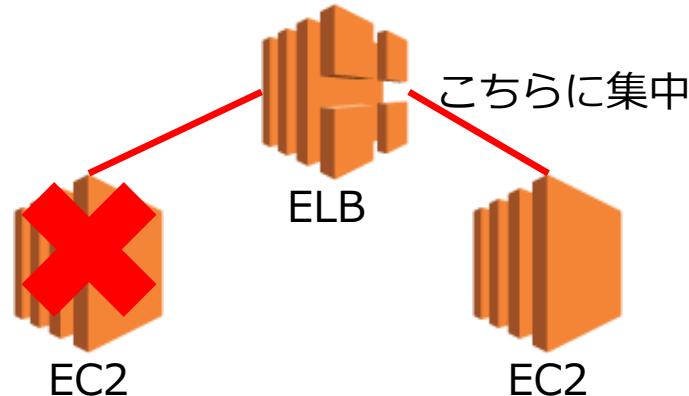
スケーラビリティの確保

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の特徴

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マネージド型のロードバランシングサービス

- インスタンス間の負荷を分散するサービス。インスタンスに限らずIPアドレスをターゲットにした負荷分散も可能である。
- ヘルスチェックにより異常なインスタンスを認識してトラフィックを正常なインスタンスのみに分散させる。
- パブリックサブネット／プライベートサブネットのどちらでも使用可能
- 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するが、これはAWS側でマネージドサービスとして実施される。
- 時間に応じたロードバランサー・キャパシティ・ユニット (LCU) 使用量で課金 (CLBのみ転送データ単位)
- Auto Scaling, Route 53, Cloud Formationなどと連携

[Q] ELBの構成

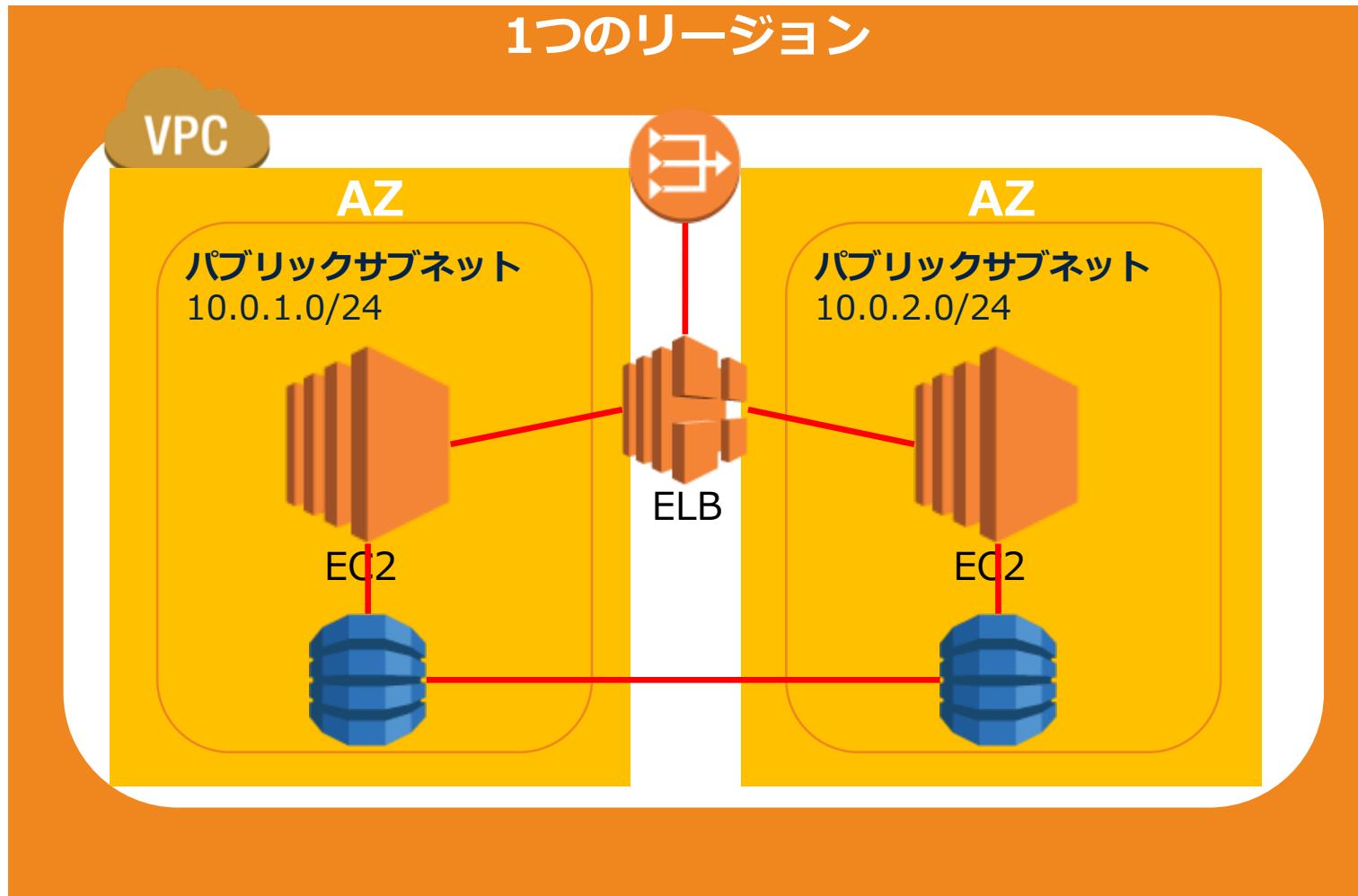
シンガポールにあるベンチャー企業はAWSを利用して新サービス用のアプリケーションを構築しています。このアプリケーションはWEBサーバーに4つのEC2インスタンスを設置して、さらにELBのターゲットグループを構成することが必要です。

アジアにあるリージョンを利用して、どのように構成することが可能でしょうか？

- 1) 4つのインスタンスを全てシンガポールリージョンの2つのアベイラビリティゾーンにデプロイする。
- 2) 4つのインスタンスをシンガポールリージョンのAZ-aにデプロイする。
- 3) 4つのインスタンスは全てシドニーリージョンのAZ-bにデプロイする。
- 4) 2つのインスタンスをシンガポールリージョンのAZ-aにデプロイし、他の2つのインスタンスは、シドニーリージョンのAZ-bにデプロイする。

ELBの構成

ELBを利用したマルチAZにインスタンスへのトラフィックを分散する構成が利用される。ELBはリージョンを跨げない



[Q] ELBの構成

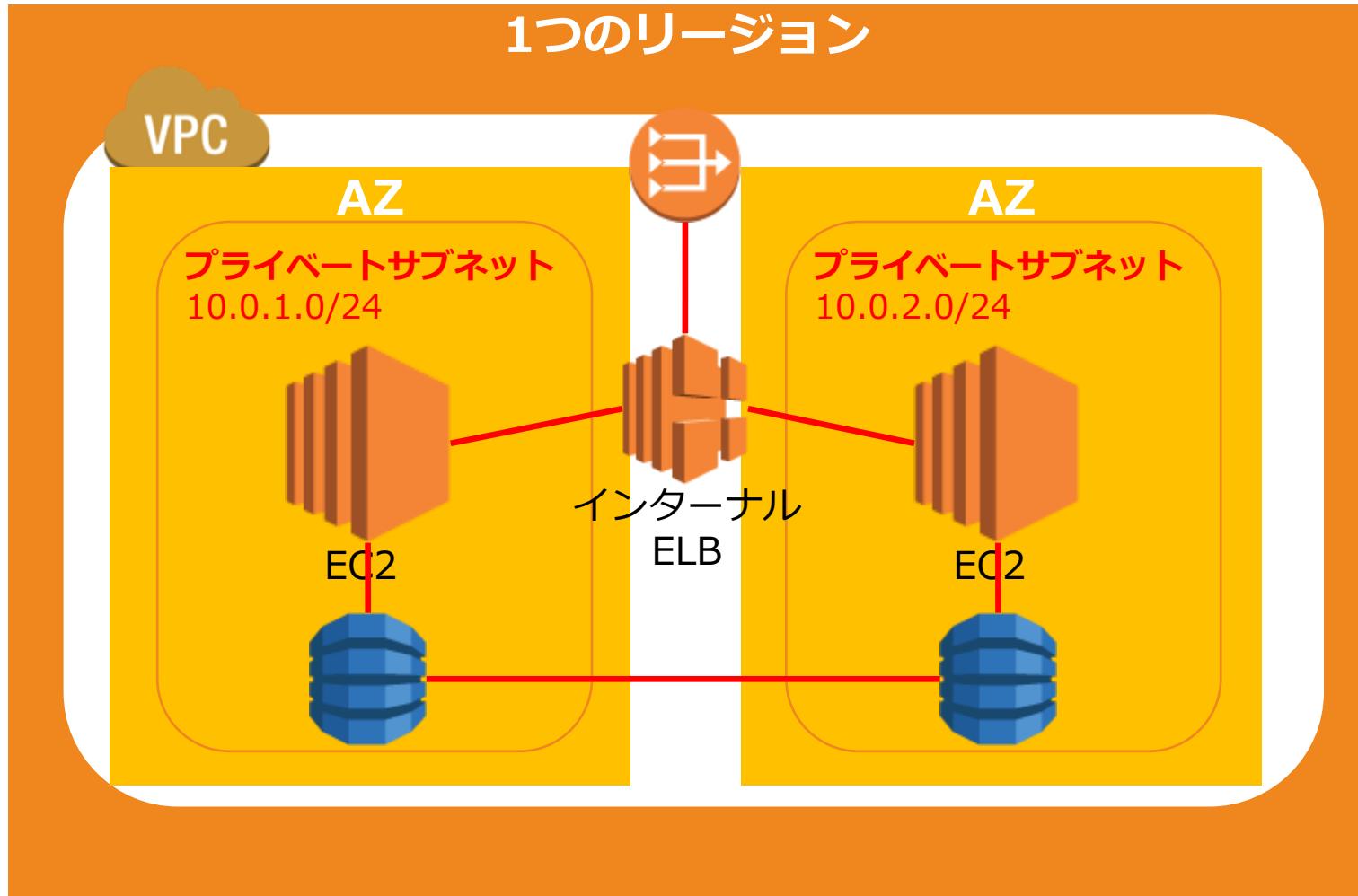
医療企業はAWSを利用して新サービス用の医療データ共有アプリケーションを構築しています。このアプリケーションはWEBサーバーにEC2インスタンスを利用して、データレイヤーにはS3とRDSを利用しています。負荷を分散するには、インターネット向けのALBを構成する必要があります。医療データを取り扱うためパブリックなアクセスを制限することが必要です。

この構成を機能させるために必要な構成を選択して下さい。 (2つ選択してください)

- 1) 同じAZに対応するパブリックサブネットを作成してALBに関連付ける。
- 2) インターネットゲートウェイをプライベートサブネットに接続する
- 3) プライベートサブネット内の各EC2インスタンスにElastic IPアドレスを追加する。
- 4) プライベートサブネットにNATゲートウェイを設置する。
- 5) プライベートサブネットにRDSとEC2インスタンスを設置してアプリケーション用のサーバーとする。

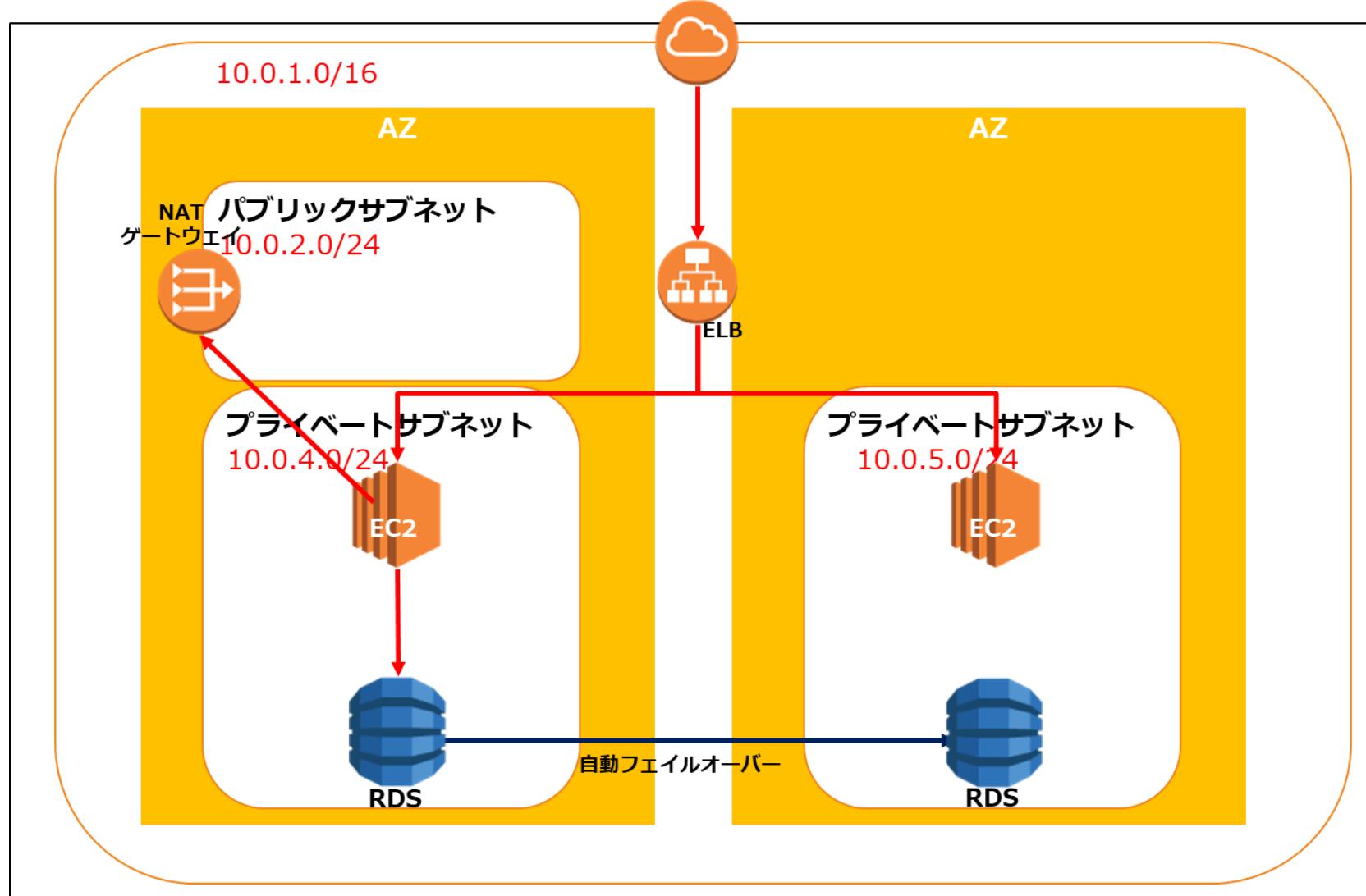
ELBの構成

プライベートサブネット空間にもELBを利用することが可能



ELBの構成

プライベートサブネットに対してパブリックネットワークとつながったELBを構成してトラフィック分散させることも可能



[Q] ELBタイプの選択

動画配信サイトを展開しているA社は、コンテンツを世界中のユーザーに配信するためにAWSクラウドを利用することを検討しています。この動画配信サイトは世界中にユーザーを抱えており、毎秒少なくとも100万件のリクエストをサポートすることが要件となっています。

この要件を満たすためにどのELBタイプを利用するべきでしょうか？

- 1) Application Load Balancer
- 2) Classic Load Balancer
- 3) Basic Load Balancer
- 4) Network Load Balancer

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

CLB

レイヤー4と7に対応しており、TCP,SSL,HTTP,HTTPSリスナーを利用
古いタイプなのでALB/NLBの利用を優先する。
データ転送（GB単位）に応じて課金される。
IPアドレスが可変であるため、指定時にDNSのみ利用可能

ALB

レイヤー7に対応しHTTP／HTTPSリスナーに対応
パスルーティングが利用可能
時間に応じたロードバランサーキャパシティーユニット (LCU) の使用量で
課金される。
IPアドレスが可変であるため、指定時にDNSのみ利用可能
デフォルトでクロスゾーン負荷分散が有効

NLB

- L4 NATロードバランサでTCPリスナーに対応（戻りトラフィックがNLBを
経由しない）

時間に応じたLCU の使用量で課金される。
NLB のサブネット拡張サポート（サブネットを追加できる）
固定IPのためDNSとIPのどちらも利用可能
ALBよりも高パフォーマンス処理が可能
デフォルトでクロスゾーン負荷分散が無効

[Q] ALBの特徴

ベンチャー企業はAWSを利用して新サービス用のアプリケーションを構築しています。このアプリケーションはWEBサーバーに4つのEC2インスタンスを利用して、ALBのターゲットグループを構成することが必要です。さらに開発チームは、HTTPヘッダーのURLパスに基づいて、トラフィックを複数のバックエンドサービスにルーティングして次のルーティングを設定します。

https://www.pintor.com/indexのリクエストをマイクロサービスAへ

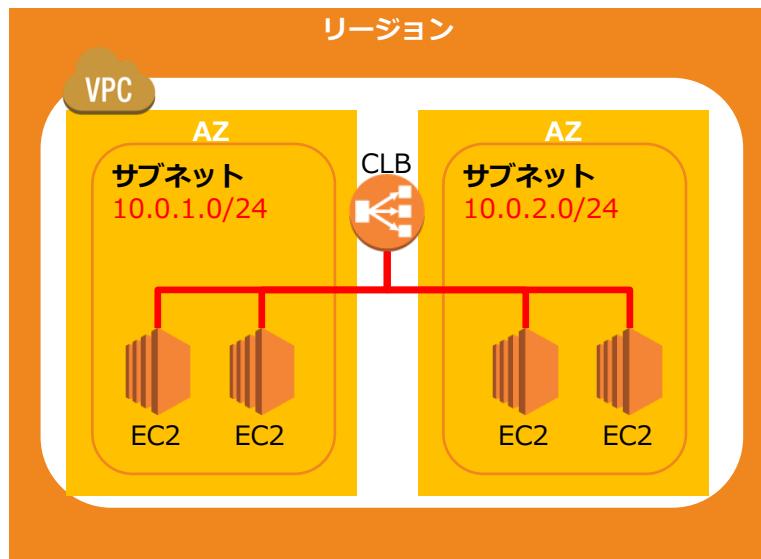
https://www.example.com/headのリクエストをマイクロサービスBへ

このような要件を満たす設定方法を選択してください。

- 1) NLBのクエリ文字列パラメータベースのルーティングを利用する
- 2) ALBのHTTPヘッダーベースのルーティングを利用する
- 3) Route53の加重ルーティングを利用する。
- 4) ALBのパスベースルーティングを使用する。

CLB (Classic Load Balancer)

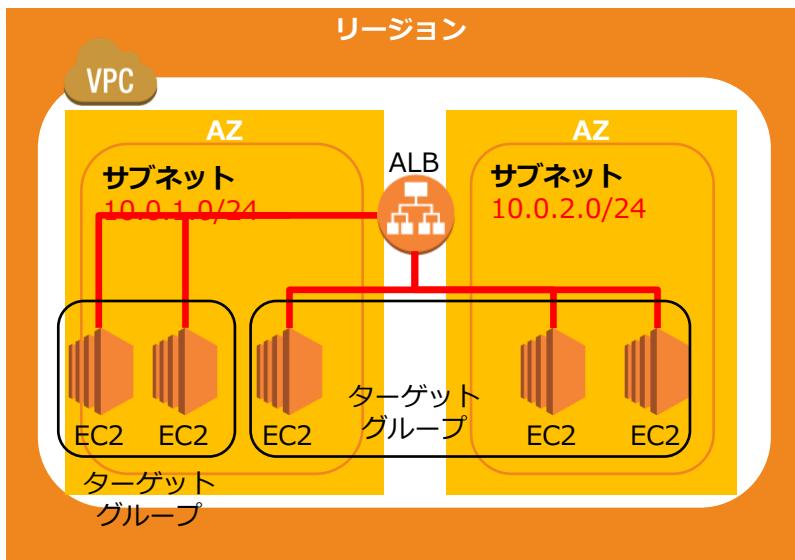
初期のELBタイプであり、標準的なL4／L7におけるロードバランシングが可能だが、複雑な設定はできない



- HTTP/HTTPSとTCP/SSLプロトコルのL4とL7に対応
- Proxyプロトコルによる発信元IPアドレス識別
- ELBとバックエンドのEC2インスタンス間でHTTPS/SSL使用時にサーバ証明書認証を実施
- CLB配下のインスタンスは、全て同一の機能を持ったインスタンスである必要がある。
- リクエスト内容を確認して分散先を振り分ける
コンテンツベースルーティングは出来ない

ALB (Application Load Balancer)

レイヤー7の対応が強化された単一ロードバランサーで、異なるアプリケーションへリクエストをルーティングが可能

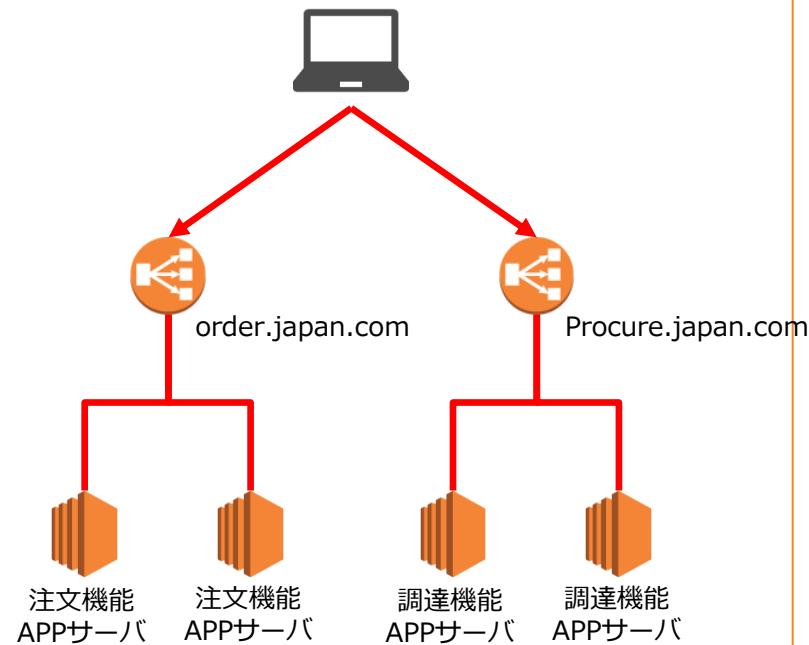


- レイヤー7に対応しHTTP／HTTPSリスナー対応
- WebSocketとHTTP/2のリクエストを受付
- 1インスタンスに複数ポートを登録可能
- 複数ポートを個別のターゲットとして登録するこ
とが可能なため、ポートを利用するECSなどのコ
ンテナをロードバランシング可能
- ターゲットグループでのヘルスチェックが可能
- EC2と同様に削除保護が可能
- 加重ロードバランシングが利用可能
- リクエスト内容を確認して分散先を振り分けるコ
ンテントベースルーティングが可能
- URLのパスに基いてルーティングが可能なパス
ベースルーティングが可能

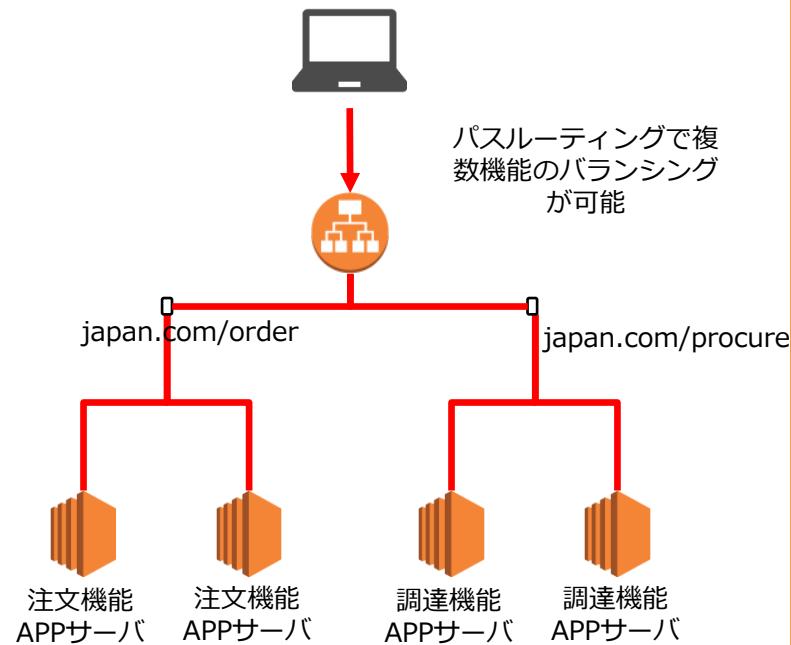
CLBとALB

ALBはパスベースルーティングによりリクエスト内容に応じて機能毎にバランスシングすることが可能

CLBの複数機能バランスシング



ALBの複数機能バランスシング



[Q] NLBの特徴

動画配信サイトを展開しているA社は、コンテンツを世界中のユーザーに配信するためにAWSクラウドを利用することを検討しています。この動画配信サイトは世界中にユーザーを抱えており、毎秒少なくとも100万件のリクエストをサポートすることが要件となっています。エンジニアリングチームは、パブリックサブネットに複数のインスタンスをプロビジョニングし、これらのインスタンスIDをNLBのターゲットとして指定しました。

NLBに設定したターゲットインスタンスの正しいルーティング方式を説明して下さい。

- 1) トラフィックはプライマリプライベートIPアドレスを使用してインスタンスをルーティングされる
- 2) トラフィックはプライマリパブリックIPアドレスを使用してインスタンスにルーティングされる
- 3) トラフィックはDNS名を使用してインスタンスにルーティングされる
- 4) トラフィックはElastic IPアドレスを使用してインスタンスにルーティングされる
- 5) トラフィックはインスタンスIDを使用してインスタンスにルーティングされる。

NLB (Network Load Balancer)

NLBは超低遅延で高スループットを維持しながら秒間何百万リクエストを捌けるように設計された高性能ロードバランサー

- L4 NATロードバランサでTCPリスナーに対応（戻りトラフィックがNLBを経由しない）
- 振発性ワークロードを処理し、毎秒数百万のリクエストに対応できる能力
- VPC外のターゲットを含めたIP アドレスや静的IPアドレスでの登録可能
- 複数のポートで各インスタンスまたは IP アドレスを同ターゲットグループに登録可能
- 大規模アクセスが予測される際にCLBやALBでは必要な事前申請が不要
- ALBやCLBはX-Forwarded-Forでアクセス元IPアドレスを判断するが、NLBは送信元IPアドレスと送信元ポートを書き換えないため、パケットからアクセス元を判断可能
- NLBはフルトトレランス機能を内蔵したコネクション処理を持ち、数カ月から数年のオープンなコネクションを処理できる
- ECSなどによりコンテナ化されたアプリケーションのサポート
- 各サービスの個別のヘルステータスのモニタリングのサポート
- NLB のサブネット拡張サポート（サブネットを追加できる）

[Q]クロスゾーン負荷分散

大手スーパー・マーケットチェーンはECアプリケーションを運用しています。冗長構成をするために4つのEC2インスタンスをAZ-aに1つのインスタンスをAZ-bに3つのインスタンスを展開して、ELBを利用したトラフィック制御を行っています。

この構成でクロスゾーン負荷分散を実施している場合と、実施していない場合のラフィック分散の結果はどうなりますか？

- 1) クロスゾーン負荷分散を有効にすると、AZ-aの1つのインスタンスが50%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ17%のトラフィックを受信します。クロスゾーン負荷分散を無効にすると、AZ-aの1つのインスタンスが25%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ25%のトラフィックを受信します。
- 2) クロスゾーン負荷分散を有効にすると、AZ-aの1つのインスタンスが25%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ17%のトラフィックを受信します。クロスゾーン負荷分散を無効にすると、AZ-aの1つのインスタンスが25%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ25%のトラフィックを受信します。
- 3) クロスゾーン負荷分散を有効にすると、AZ-aの1つのインスタンスが25%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ25%のトラフィックを受信します。クロスゾーン負荷分散を無効にすると、AZ-aの1つのインスタンスが50%のトラフィックを受信し、AZ-bの4つのインスタンスがそれぞれ約17%のトラフィックを受信します。
- 4) クロスゾーン負荷分散を有効にすると、AZ-aの1つのインスタンスが90%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ10%のトラフィックを受信します。クロスゾーン負荷分散を無効にすると、AZ-aの1つのインスタンスが10%のトラフィックを受信し、AZ-bの3つのインスタンスがそれぞれ30%のトラフィックを受信します。

[Q]暗号化通信

大手スーパー・マーケットチェーンはECアプリケーションを運用しています。冗長構成のために複数のEC2インスタンスに対してELBを利用したトラフィック制御とAuto Scalingを利用したスケーリングを設定しています。ELBを介した転送中のすべてのデータは暗号化する必要があります。

どのように暗号化要件を実現することができますか？（2つ選択してください）

- 1) NLBでTLSリスナーを構成してEC2インスタンスでSSLを終了する。
- 2) ALBでHTTPSリスナーを構成してALBにSSL証明書をインストールする。
- 3) NLBでHTTPSリスナーを構成してALBにSSL証明書をインストールする。
- 4) ALBでパススルーモードを使用して、EC2インスタンスでSSLを終了する。
- 5) ALBでTLSリスナーを構成してALBにSSL証明書をインストールする。

[Q]ステイッキーセッション

大手スーパー・マーケット・チェーンはECアプリケーションを運用しています。冗長構成するために複数のEC2インスタンスに対してELBを利用したトラフィック制御とAuto Scalingを利用したスケーリングを設定しています。このシステムでは同じユーザーから断続的にシステム処理が発生することが多いため、同じユーザーには同じEC2インスタンスからのトラフィックを継続することが要件となっています。

この要件を満たすためのELBの設定方法を選択してください。

- 1) 負荷分散機能を利用して、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
- 2) Connection Drainingを利用して、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
- 3) スティッキーセッションを利用して、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
- 4) SSL Terminationを利用して、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

[Q]Connection Draining

大手スーパー・マーケットチェーンはALBを設定したEC2インスタンスをマルチAZに構成したEC2アプリケーションを運用しています。開発チームは、インスタンスが異常になったときにELBからEC2インスタンスへの処理中のリクエストがドロップされるという問題を繰り返し発生しており、対応に追われています。

この問題に対処するために利用するべき機能はどれでしょうか？

- 1) コネクションドレイニング
- 2) クロスゾーン負荷分散
- 3) スティックィセッション
- 4) ヘルスチェックの有効化

[Q]ログ取得

会社はEC2インスタンスにALBを設定してマルチAZにクロスゾーン負荷分散を実施しているWEBアプリケーションを運用しています。あなたはソリューションアーキテクトとして、このアプリケーションの解析を担当しています。ALBによって処理されるすべてのHTTPリクエストに関する詳細情報を取得して、トラフィック状況を解析することが求められています。

この要件を満たすための対応を選択してください。

- 1) CloudWatchでALBのメトリクスを取得する。
- 2) ELBのアクセスログを有効にして、S3にログデータを保存する
- 3) EC2の詳細モニタリングを有効にする。
- 4) CloudTrailをELBに設定してアクセスログを取得する。

ELBの主要機能

ELBのロードバランシングの際に様々な機能を利用

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
クロスゾーン 負荷分散	配下のEC2の負荷に応じて、複数のAZに跨るEC2インスタンスに均等に負荷分散を行う
暗号化通信	SSL/TSL証明書をELBに設定することでHTTPSまたはTLS通信を実施することができる。
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継続して同じ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
ログ取得	ELBのログ取得を有効化するとS3バケットにログを収集

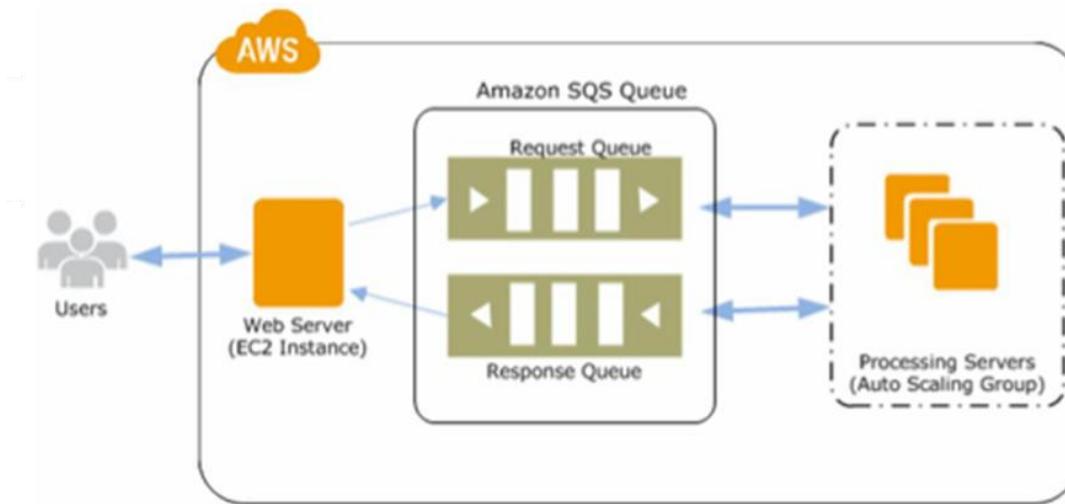
セクションの内容

レクチャー	レクチャーで学ぶ内容
SQSの出題範囲	キューイングによるタスク管理を実施するSQSにおける出題問題を確認して、その範囲の知識を詳細に学習します。
CloudFrontの出題範囲	AWSのCDNサービスであるCloudFrontにおける出題問題を確認して、その範囲の知識を詳細に学習します。
DynamoDBの出題範囲	代表的なNoSQL型のデータベースであるDynamoDBにおける出題問題を確認して、その範囲の知識を詳細に学習します。
Lambdaの出題範囲	代表的なサーバレスコンピューティングであるLambdaにおける出題問題を確認して、その範囲の知識を詳細に学習します。
Route53の出題範囲	AWSにDNSサーバー機能を提供するRoute53における出題問題を確認して、その範囲の知識を詳細に学習します。

SQSの出題範囲

SQSとは何か？

タスクのトリガーとなるキューを複数管理することで、ワークロードの並列実行を実現するキューイングサービス



Reference: <https://aws.amazon.com/jp/blogs/developer/using-python-and-amazon-sqs-fifo-queues-to-preserve-message-sequencing/>

SQSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

SQSの選択	✓ シナリオに基づいて、Amazon SNSやSESなどと比較して、SQSを選択する出題が問われる。
SQSの特徴	✓ SQSキューのポーリング処理などの特徴および制約に関する問題が出題される。 ✓ SQSの挙動や設定内容に関する問題が出題される。
SQSキュータイプ	✓ SQSで選択できる標準キューとFIFOキューの特徴とユースケースに関する質問が問われる。
SQSの識別子	✓ SQSの識別子として利用されるIDの特徴や使い方についての問題が出題される。
SQSの構成	✓ SQSをEC2インスタンスやECSなどと構成する際の基本的な構成方法が問われる。

SQSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

SQSとAuto Scaling	✓ SQSをAuto Scalingと連動して利用する際のスケーリング設定などが問われる。
可視性タイムアウト	✓ 可視性タイムアウトの特徴とユースケースなどが問われる。
ポーリング方式	✓ ショートポーリングとロングポーリングの違い方とユースケースが問われる。
遅延キュー	✓ 遅延キューの特徴とユースケースなどが問われる。
優先度付キュー	✓ 優先度付キューの特徴とユースケースなどが問われる。

SQSの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

メッセージタイマー	✓ メッセージタイマーの特徴とユースケースなどが問われる。
メッセージ重複排除ID	✓ メッセージ重複排除IDの特徴とユースケースなどが問われる。
デッドレターキュー	✓ デッドレターキューの特徴とユースケースなどが問われる。
SQSのバッチアクション	✓ SQSキューでまとめてメッセージを送付する際の設定方式が問われる。

[Q]SQSの選択

あなたの会社はユーザーが投稿したビデオのアップロード・処理・公開用の動画管理アプリケーションを運用しています。このアプリケーションは、ユーザーによってアップロードされたビデオを処理するために複数のEC2インスタンスを利用しています。ビデオを処理し公開するEC2ベースのワーカープロセスを有しており、Auto Scalingグループが設定されています。

ワーカープロセスの信頼性を高めるため利用すべきサービスを選択してください。

- 1) Amazon SQS
- 2) Amazon SNS
- 3) Amazon SES
- 4) Amazon MQ

SQSの選択

SQSはポーリング処理型のキューイングサービスで、タスクの並行実施などに利用される。

Amazon SNS	完全マネージド型 pub/sub メッセージングを実施するサービス。メール通知やプッシュ通知による連携処理に利用する。
Amazon SQS	完全マネージド型のキューイングサービス ポーリング処理によるタスクの並列実施に利用する。
Amazon SES	Eメール機能を可能にするサービス。アプリケーション上にEメール送受信機能を実装する際に利用する。安全、グローバル、大規模に E メールを送信が可能になる。
Amazon MQ	JMS、NMS、AMQP、STOMP、MQTT、WebSocket などの業界標準 API やメッセージング用プロトコルを使用するApache ActiveMQ 向けのマネージド型メッセージブローカーサービス

[Q] SQSの特徴

あなたはソリューションアーキテクトとして、EC2インスタンスにホストされているEコマースサイトを構築しています。このサイトの注文はSQSキューからのメッセージによって処理サーバーが処理する構成となっています。SQSキューの可視性タイムアウトは30分に設定しています。注文が完了すると注文担当者にメッセージが通知される構成となっていますが、注文に対してメッセージ通知のいくつかが配信されないトラブルが発生しています。

この問題の最も可能性が高い原因はどれでしょうか？

- 1) 注文を処理するサーバーがメッセージを処理後に、SQSキュー内のメッセージを削除していない。
- 2) 標準キューを利用しているためメッセージに重複が発生している。
- 3) キューはショートポーリングに設定されているため、空のメッセージ取得が増加している。
- 4) いくつかの注文メッセージがデットレターキューへと移行している。

SQSの特徴

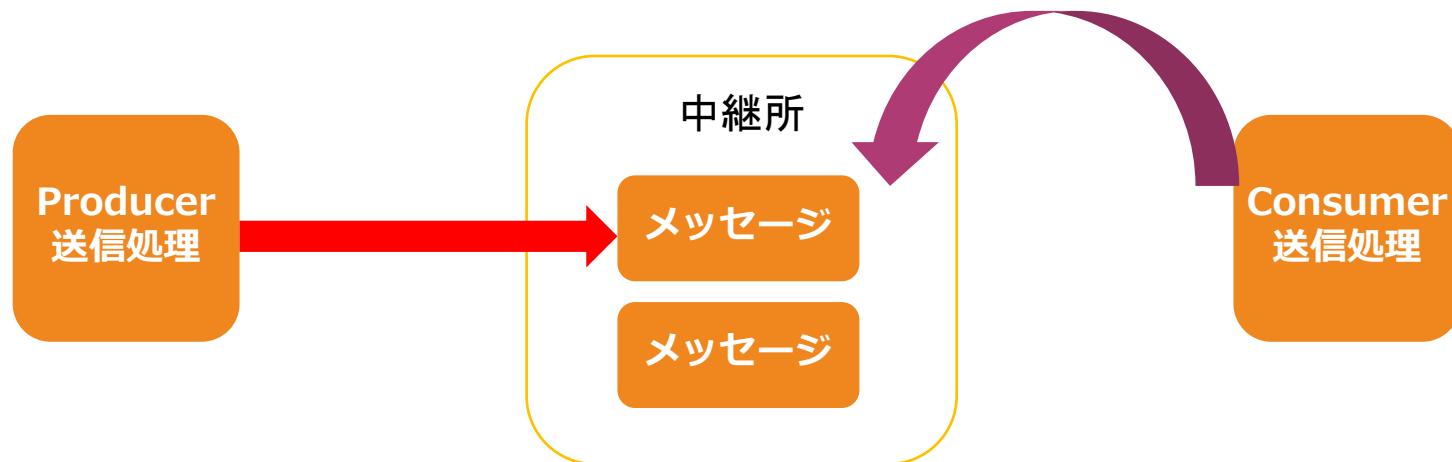
AWSの様々なサービスと連携して通知可能で、疎結合アーキテクチャに実現する。

【基本的な機能】

- 単一発行メッセージをキューとして利用
- ポーリング処理型のキューイングサービス
- 標準キューはメッセージ通信順番は保証されないが、FIFO
キューは順番を保証する。
- 優先キューは他のキューよりも優先的に処理させることが可能
- メッセージ保持期間の間はメッセージを保持するが、超過するとメッセージを削除する。
- 発行したメッセージは取り消し不可
- 配信ポリシーによるキューの再試行を実施する

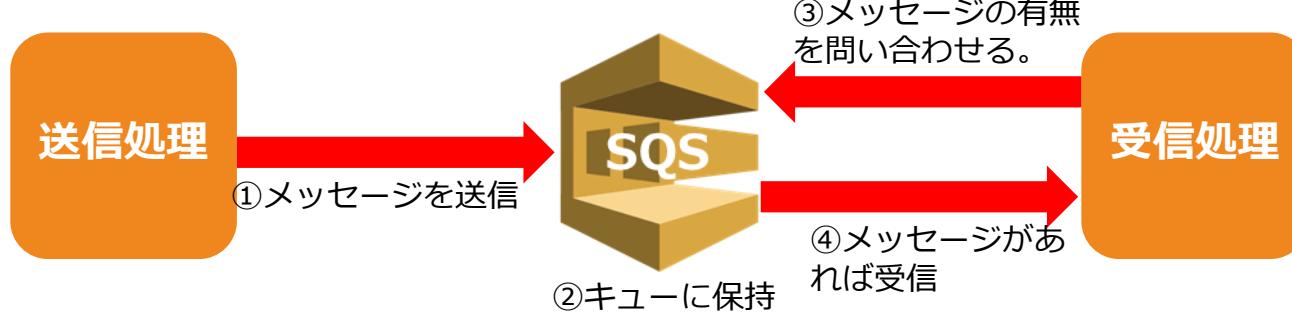
SQSの特徴

キューとはProducerが送信したメッセージをキュー内に蓄積して、Consumerがプルすることで処理が始まるメッセージ方式



SQSの特徴

SQSはキューを発行・蓄積して、ポーリング処理を管理する。



SQSキューの特徴

無制限にメッセージを利用可能だが、メッセージ保持期間をうまく設定することが必要

メッセージの制約

メッセージ数は無制限に利用可能

メッセージサイズは最大256KB

ただし、拡張クライアントライブラリーを利用すると2GBまでのメッセージのやり取りが可能となる。

メッセージの保持期間

SQSのキューメッセージは保持期間の間は保存される。

デフォルト4日間（最小60秒～最大14日で設定可能）

APPLICATION上でメッセージを削除する処理を実施しないと、期間を超過するまでキューが滞留してしまう。

[Q] SQSのキュータイプ

グローバルコンサルティングファームではコンサルティングの知見をグローバルで共有するための情報共有システムをAWS上に構築しています。このシステムはストレージレイヤーにS3を利用していますが、S3にデータがアップロードされるたびに、イベントをトリガーによってSQSキューを配信する処理を追加します。

この機能に関して正しい説明は次のうちどれですか？

- 1) S3イベントにはAmazon SQSの標準キューを設定できるが、FIFOキューを設定できない。
- 2) S3イベントにはAmazon SQSのFIFOキューを設定できるが、標準キューを設定できない。
- 3) S3イベントにはAmazon SQSの標準キューとFIFOキューの両方を設定できる。
- 4) S3イベントにはAmazon SQSを設定できないため、SNSを利用する必要がある。

SQSのキュータイプ

SQSでは標準キューとFIFOキューのどちらかを選択して、SQSを初期設定することになる。

標準キュー

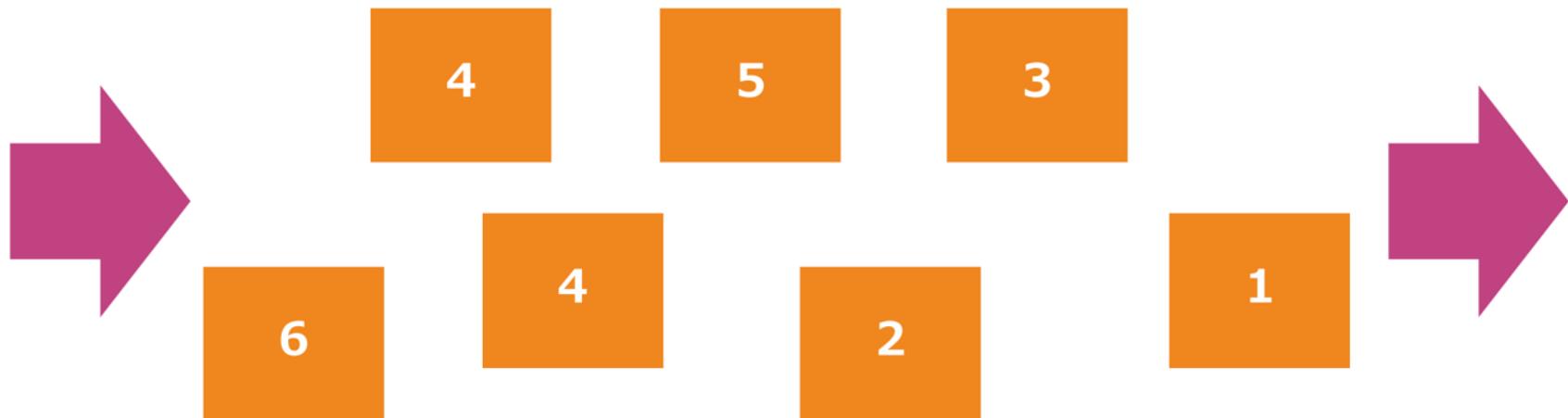
- ✓ メッセージの1つ以上のコピーが順序どおりに配信できないことがある。
- ✓ メッセージが少なくとも1回配信される方式であり、キューには重複が発生する可能性がある。
- ✓ 1秒あたりのトランザクション数はほぼ無制限
- ✓ 標準キューは、アプリケーションが1回以上に順序が正確ではなくても配信されれば良いケースで利用する。

FIFOキュー

- ✓ 先入れ先出し方式 (FIFO) により配信順番を守る。
- ✓ メッセージが1回だけ配信され、コンシューマがプロセスを処理して削除するまで使用可能なキューの状態を保つため、キューに重複がない。
- ✓ 1秒あたり300トランザクションに制限
- ✓ FIFO キューは、操作やイベントの順序が重要である場合や、重複を許容できないユースケースに利用する。

標準キュー

標準キューは「順番通りの処理」と「1回だけのメッセージング」を“なるべく”実施するキュー方式



FIFOキュー

その名の通り、最初に入ったキューを最初に処理する順番を守るキュー方式



[Q] SQSの識別子

あなたはソリューションアーキテクトとして、IoTデバイスからのストリーミングデータを分析するワークフローを構築しています。このストリーミング処理では、データは1分ごとにAWSに送信されます。各IoTデバイスのデータは順番に個別に処理する求められます。また、IoTデバイスは同じ場所に設置された2～5個のグループ単位になっており、グループでまとめてデータを解析することも必要です。

この要件を満たすことができるソリューションを選択してください。

- 1) SQSのFIFOキューを使用し、IoTデータのデバイスIDの値を表すグループID属性を付与してメッセージを送信する。
- 2) SQSの標準キューを使用し、IoTデータのデバイスIDの値を表すグループID属性を付与してメッセージを送信する。
- 3) Kinesis Data Streamsを使用し、IoTデータのデバイスIDの値を表すグループID属性を付与してメッセージを送信する。
- 4) Kinesis Data Streamsを使用し、IoTデータのデバイスIDの値を表すグループID属性を付与してシャードごとに分離してデータを処理する。

SQSの識別子

SQSではキューを利用する際に様々な機能を利用することが可能。ユースケースに応じて使い分ける必要がある。

キューURL

- キューに割り当てられるURL

メッセージID

- メッセージに対して割り当てられたID

メッセージグループID

- メッセージグループ ID は 特定のメッセージグループに属するメッセージを指定するタグ
- 同じメッセージグループに属するメッセージは、メッセージグループに相対的な厳密な順序で 1 つずつ処理される、
- 単一の FIFO キュー内で複数の順序付きメッセージグループをインターリーブするには、メッセージグループ ID 値を使用する。

[Q] SQSの構成

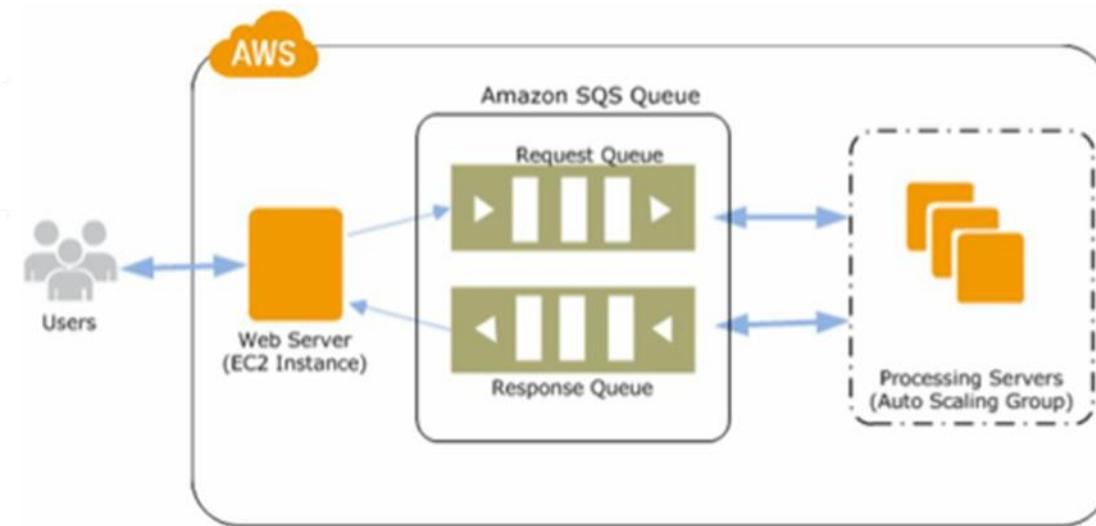
マーケティング会社はAmazon ECSを利用してデータ分析アプリケーションを構築しています。このアプリケーションは複数のAmazon ECSタスクで実行されます。フロントエンドアプリケーションがデータの前処理を実施し、そのデータをバックエンドのECSタスクに渡してデータ解析を実行します。これらの分析処理が並列で実行されることで高パフォーマンスを達成しつつ、障害が他のコンポーネントに影響を与えないように、相互依存性を減らす必要があります。

この要件を満たすことができる最もコスト最適なAWSアーキテクチャ構成の組合せはどれでしょうか？

- 1) Amazon SQSキューを作成し、キューにメッセージを追加するようにフロントエンドを設定し、メッセージについてキューをポーリングするようにバックエンドを設定する。
- 2) Amazon SQSキューを作成し、キューにメッセージを追加するようにバックエンドを設定し、メッセージについてキューをポーリングするようにフロントエンドを設定する。
- 3) Amazon SNSを作成し、キューにメッセージを追加するようにフロントエンドを設定し、メッセージについてキューをポーリングするようにバックエンドを設定する。
- 4) Amazon SNSを作成し、キューにメッセージを追加するようにバックエンドを設定し、メッセージについてキューをポーリングするようにフロントエンドを設定する。

SQSの構成

フロントのサーバーからキューがトリガーされて、バックエンドの処理サーバーが並列処理するのがSQSの基本構成



Reference: <https://aws.amazon.com/jp/blogs/developer/using-python-and-amazon-sqs-fifo-queues-to-preserve-message-sequencing/>

[Q] SQSとAuto Scaling

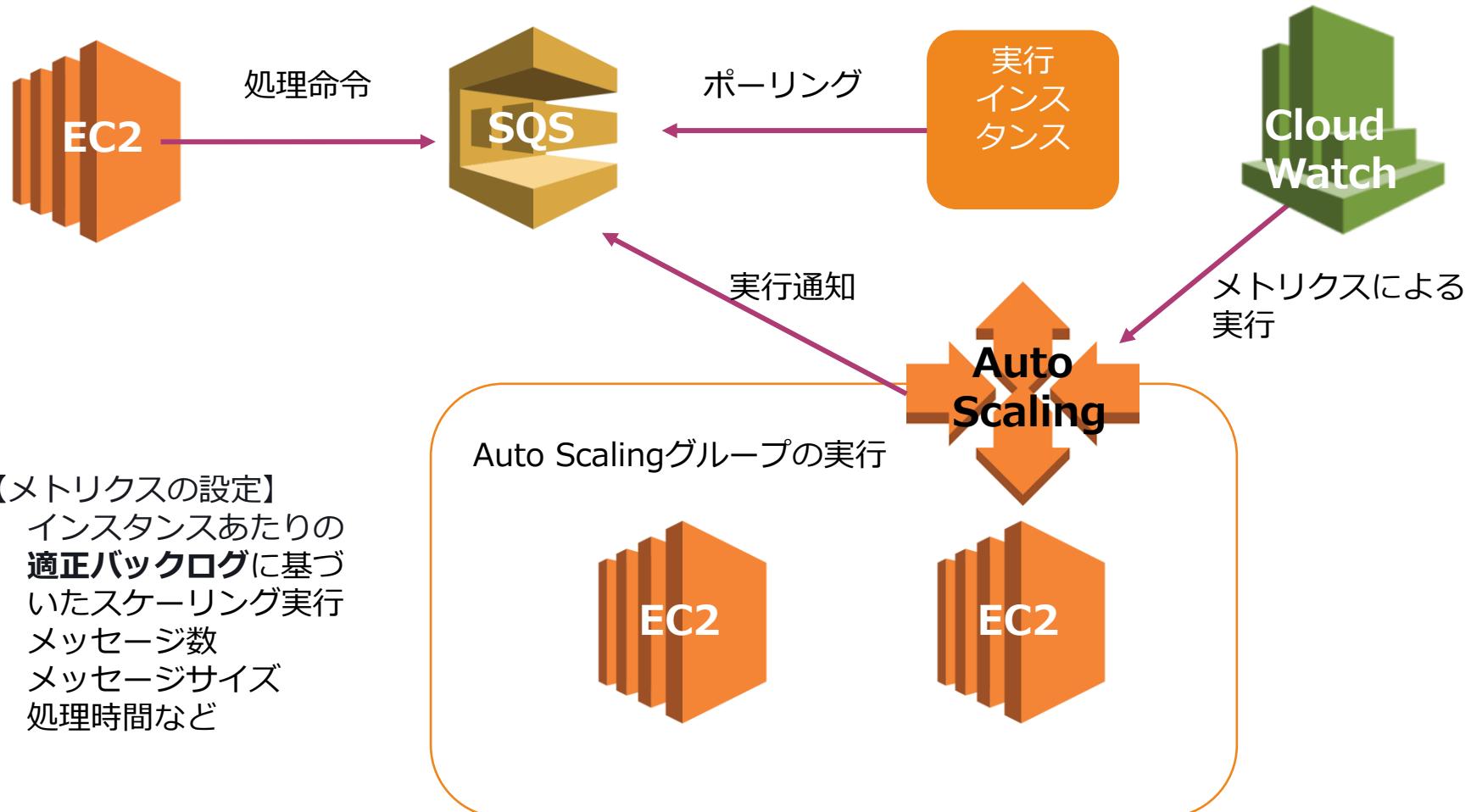
B社ではAWS上に動画処理を実行するワークフローを構築しました。このシステムはデータ処理を並列処理するためのキューを利用した分散構成が必要となります。このジョブは不定期に実行され、処理変更も多いため実行期間が不明確です。また負荷の増減も多いようです。この動画処理システムは中長期稼働させる予定であり、1つ1つの編集処理は1分から30分ほどで完了します。

この要件を満たすことができる最もコスト最適なAWSアーキテクチャ構成の組合せはどれでしょうか？（2つ選択してください。）

- 1) 動画処理サーバーにリザーブドインスタンスを利用して、SQSによる並列処理を設定する。
- 2) 動画処理サーバーにスポットインスタンスを利用して、SQSによる並列処理を設定する。
- 3) 動画処理サーバーにスポットインスタンスを利用して、Lambdaによる並列処理を設定する。
- 4) Auto Scalingにスポットインスタンスを利用したスケーリングを構成して、SQSの適正バックログをしきい値に設定してスケーリングを実行する。
- 5) Auto Scalingにスポットインスタンスを利用したスケーリングを構成して、SQSのメッセージ数をしきい値に設定してスケーリングを実行する。

SQSとAuto Scaling

SQSとAuto Scalingを構成する際は、CloudWatchメトリクスに基づいてキューの処理量に応じたスケーリングを設定する。



[Q]可視性タイムアウト

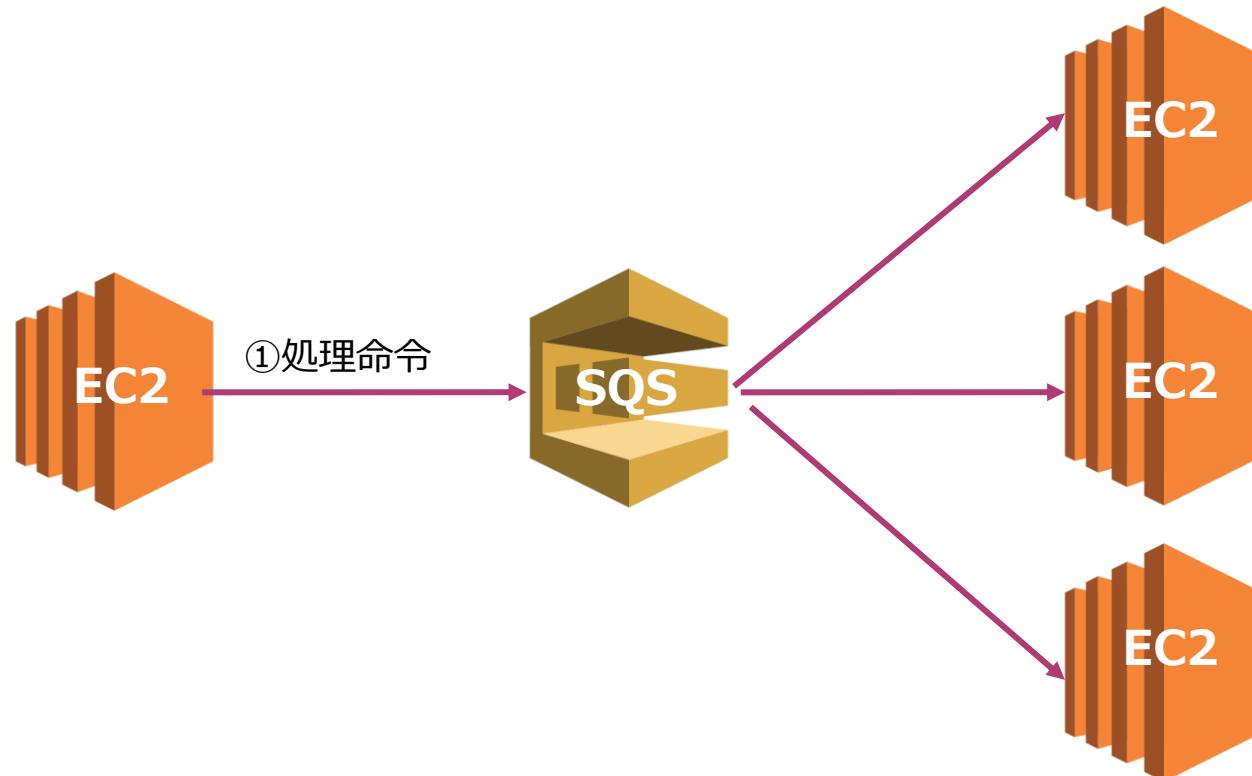
B社ではAWS上に動画処理を実行するワークフローを構築しました。この動画処理システムでは、EC2インスタンスから送信されたAmazon SQSキューからのメッセージに基づいて動画編集プロセスが実行されます。処理後の動画はS3に保存します。プロセス処理にはスポットインスタンスが利用されていますが、キューからメッセージを取得した直後に、いくつかのスポットインスタンスが終了してしまいました。これらのスポットインスタンスはメッセージの処理を完了していません。SQSはFIFOキューを利用しておらず、可視性タイムアウトが設定されています。

このシナリオの要件に基づくと、終了していないメッセージはどうなりますか？

- 1) 可視性のタイムアウトが経過すると、メッセージは再び処理できる。
- 2) メッセージは処理時にキューから削除されたため、失われる。
- 3) メッセージは処理されずにデッドレターキューに移行する。
- 4) メッセージはキューに残り、すぐに別のインスタンスによって取得される。

可視性タイムアウト

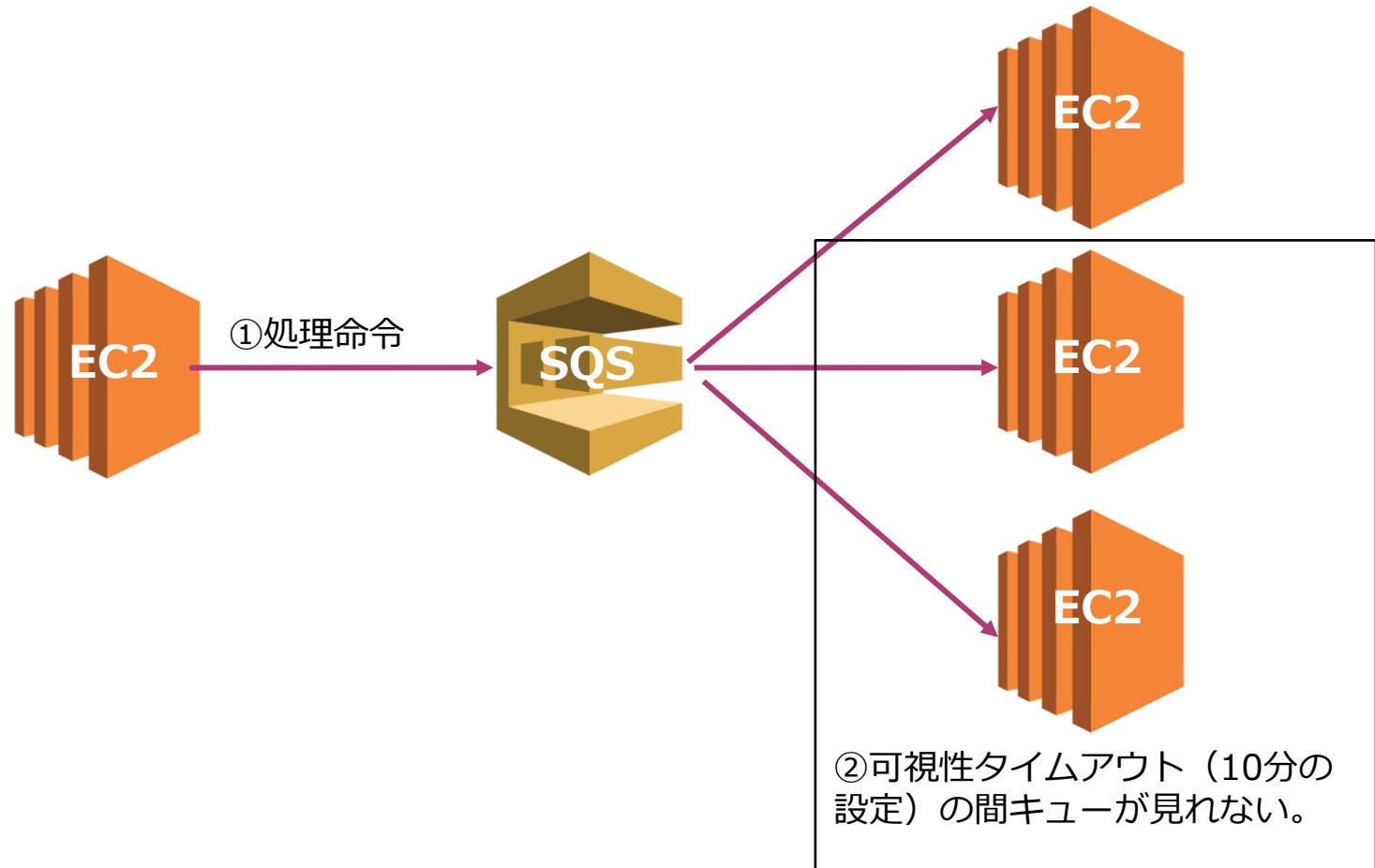
可視性タイムアウトは処理担当のインスタンス以外からは一定時間（30秒～12時間）キューが見えなくなる機能



メッセージが受信された直後は、メッセージはキューに残ったままとなる。他のコンシューマーが同じメッセージを再処理しないように、Amazon SQSは可視性タイムアウトを設定することで、重複処理を防ぐことができる。

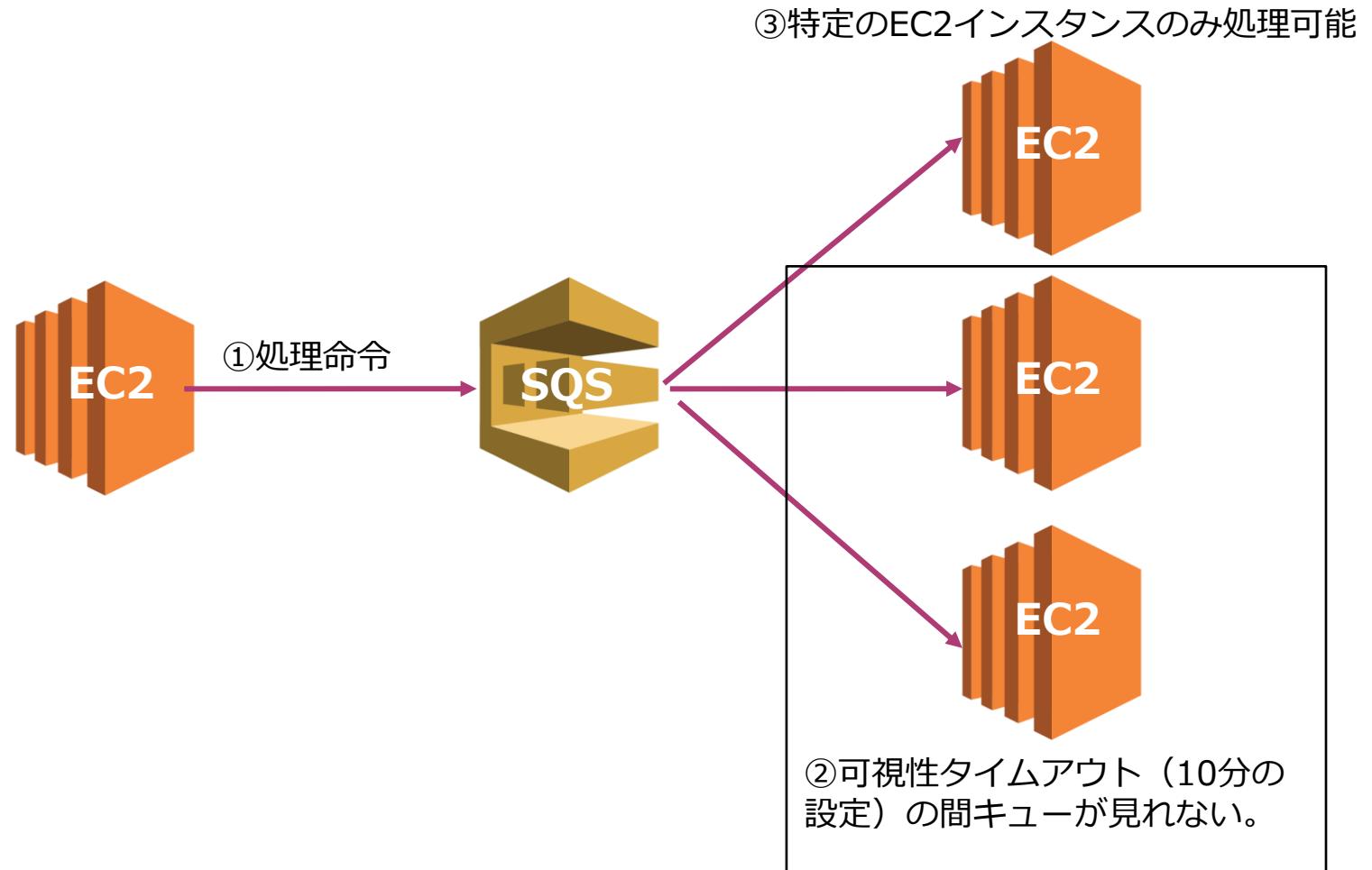
可視性タイムアウト

可視性タイムアウトは処理担当のインスタンス以外からは一定時間（30秒～12時間）キューが見えなくなる機能



可視性タイムアウト

可視性タイムアウトは処理担当のインスタンス以外からは一定時間（30秒～12時間）キューが見えなくなる機能



[Q]ポーリングの方式

B社はAWS上に動画処理を実行するワークフローを構築しました。このアプリケーションでは、EC2インスタンスによる動画編集処理をAmazon SQSキューを使用してを分離して実行できる構成としています。開発チームは、動画編集中に動画リストが更新されると動画リストが未処理となり、メッセージ処理が失敗する事象を発見しました。

メッセージ処理が失敗するケースで利用するべき機能はどれでしょうか？

- 1) 遅延キューを使用して、メッセージ処理の失敗を処理する。
- 2) ショートポーリングを使用して、メッセージ処理の失敗を処理する。
- 3) ロングポーリングを使用して、メッセージ処理の失敗を処理する。
- 4) デッドレターキューを使用して、メッセージ処理の失敗を処理する。

ポーリングの方式

ポーリング処理の方式でショートポーリングとロングポーリングの2通りがある。

ロングポーリング

問い合わせの結果が空であった場合に、指定したメッセージ受信待機時間はSQSは待機してから応答を返す。メッセージ受信待機時間は0秒から20秒で設定
空のレスポンス数を削減することができる。

ショートポーリング

キューが空の場合にすぐに空のメッセージが返される

[Q]遅延キュー

あなたはソリューションアーキテクトとして、マイクロサービスを利用したアプリケーションを構築しています。マイクロサービス間のコンポーネントを分離するためにSQSキューを使用しています。各コンポーネントはSQSメッセージを処理するためには一定の時間を必要とするため、新しいメッセージのキューへの配信を10秒間停止してから、処理を開始することがキュー設定として必要不可欠です。

この要件を満たすことができるキューの設定方法を選択してください。

- 1) 遅延キューを使用して、キューへの新しいメッセージの配信を10秒間延期する。
- 2) ショートポーリングを使用して、キューへの新しいメッセージの配信を10秒間延期する。
- 3) メッセージタイマーを使用して、キューへの新しいメッセージの配信を10秒間延期する。
- 4) 可視性タイムアウトを使用して、キューへの新しいメッセージの配信を10秒間延期する。

[Q]メッセージタイマー

あなたはソリューションアーキテクトとして、マイクロサービスを利用したアプリケーションを構築しています。マイクロサービス間のコンポーネントを分離するためにSQSキューを使用しています。現在、あなたは特定のメッセージのキューへの配信を10秒延期し、他のすべてのメッセージはすぐにキューに配信する設定を実施しているところです。

この要件を満たすことができるキューの設定方法を選択してください。

- 1) 遅延キューを使用して、キューへの特定のメッセージの配信を10秒間延期する。
- 2) ショートポーリングを使用して、キューへの特定のメッセージの配信を10秒間延期する。
- 3) メッセージタイマーを使用して、キューへの特定のメッセージの配信を10秒間延期する。
- 4) 可視性タイムアウトを使用して、キューへの特定のメッセージの配信を10秒間延期する。

[Q]優先度付キュー

B社ではAWS上に動画編集アプリケーションを構築しました。この動画処理アプリケーションはEC2インスタンスから送信されたAmazon SQSキューからのメッセージにより動画編集を実行して、処理後の動画をS3に保存します。ユーザーは無料ユーザーと有料ユーザーとに分かれます。有料ユーザーから提出されたファイルは優先的に処理される必要があります。

このような要件は満たす実装方法を選択してください。

- 1) SQSを利用して、有料ユーザーには優先的に処理するメッセージを設定し、無料ユーザーにはデフォルトメッセージを利用する。
- 2) Lambdaファンクションを利用して有料ユーザーのメッセージ処理を優先的に処理するポーリング処理を設定し、無料ユーザーにはデフォルトメッセージを利用する。
- 3) SNSを利用して有料ユーザーのメッセージ処理を優先的に処理するポーリング処理を設定し、無料ユーザーにはデフォルトメッセージを利用する。
- 4) Amazon MQを利用して、有料ユーザーには優先的に処理するメッセージを設定し、無料ユーザーにはデフォルトメッセージを利用する。

キューの詳細設定

SQSではキューを利用する際に様々な機能を利用することが可能。ユースケースに応じて使い分ける必要がある。

遅延キュー

キューへの新しいメッセージの配信を数秒間遅延させることができる機能（0秒から15分で設定）

可視性タイムアウトとの違いは、キューが発行された直後から見えなくなるということ。またキュー全体に効果がある。

優先度付きキュー

キューの処理順序に優先度をつけることができる。

これにより、優先対応があるタスクを最初に処理するようにワークフローを設定できる。

デッドレターキュー

このキューは、正常に処理（消費）できないメッセージを別のキューへと移動させる。

処理不能なキューが蓄積されるのを防ぎつつ、処理できなかつた理由を後で解析できる。

キューの詳細設定

SQSではキューを利用する際に様々な機能を利用することが可能。ユースケースに応じて使い分ける必要がある。

メッセージ重複排除ID

- 送信されたメッセージの重複排除に使用するトークン
- 同一の重複排除IDが設定されたメッセージをキューへ送っても5分間の間は受け付けられないように設定できる。
- 個別のメッセージグループではなくキュー全体に適用される。
- FIFOのみで利用する

暗号化

- AWS Key Management Service (AWS KMS)を使用して、送信データを暗号化する。

メッセージタイマー

- メッセージタイマーはメッセージが発出された瞬間から、キューに追加されたメッセージが表示されないようにする機能。45秒のタイマーでメッセージを送信すると、キューの最初の45秒間は表示されない。
- 個々のメッセージではなくキュー全体に対して遅延の秒数を設定するには、遅延キューを使用する。
- 個々のメッセージのメッセージタイマー設定はキュー全体よりも優先される。

[Q] SQSのバッチアクション

あなたの会社はAWS上でワークフローを実行する業務システムを構築しています。あなたのソリューションアーキテクトとして、SQSを利用したキューイングによる高可用で高性能なフローを実装しています。SQSを介して処理される1秒あたり約1000メッセージのピークレートが期待されており、メッセージが順番に処理されることが重要です。

このSQSの実装の際に利用するべき機能はどれでしょうか？

- 1) 操作ごとに4メッセージのバッチモードでFIFOキューを使用する。
- 2) 操作ごとに2メッセージのバッチモードでFIFOキューを使用する。
- 3) 操作ごとに4メッセージのバッチモードで標準キューを使用する。
- 4) 操作ごとに2メッセージのバッチモードで標準キューを使用する。

SQSのバッチアクション

バッチアクションは1回のアクションで複数のメッセージを操作するなどのバッチ処理が設定可能

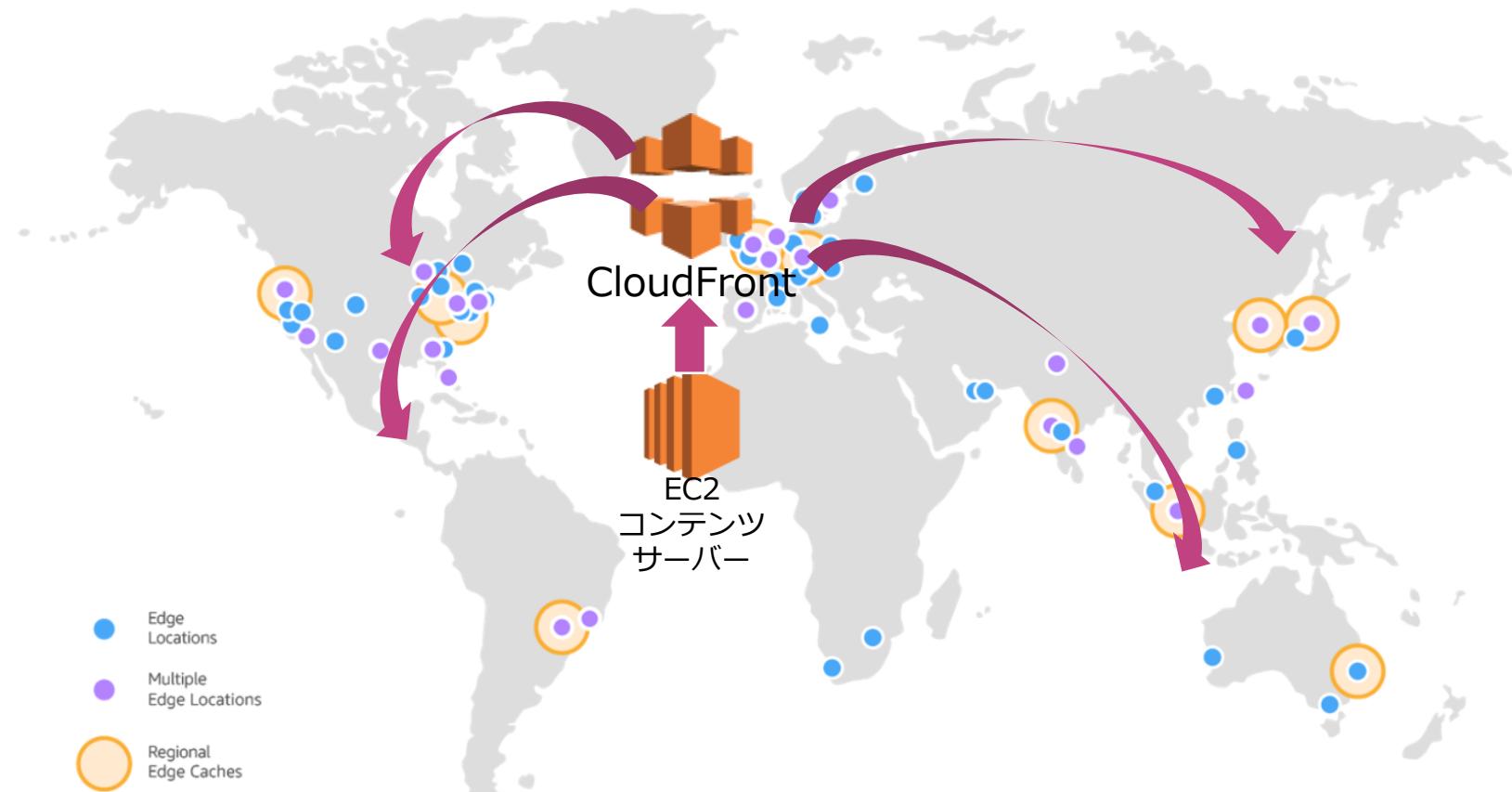
Amazon SQS バッチアクションをサポートする AWS SDK を使用して、バッチ機能を活用できる。

- SendMessageBatch
- DeleteMessageBatch
- ChangeMessageVisibilityBatch

CloudFrontの出題範囲

CloudFrontとは何か？

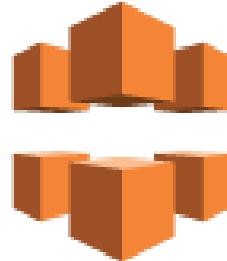
コンテンツ配信をグローバルロケーションを使って効率的に実施するサービス



参照 : <https://aws.amazon.com/jp/cloudfront/features/?nc=sn&loc=2>

CloudFrontとは何か？

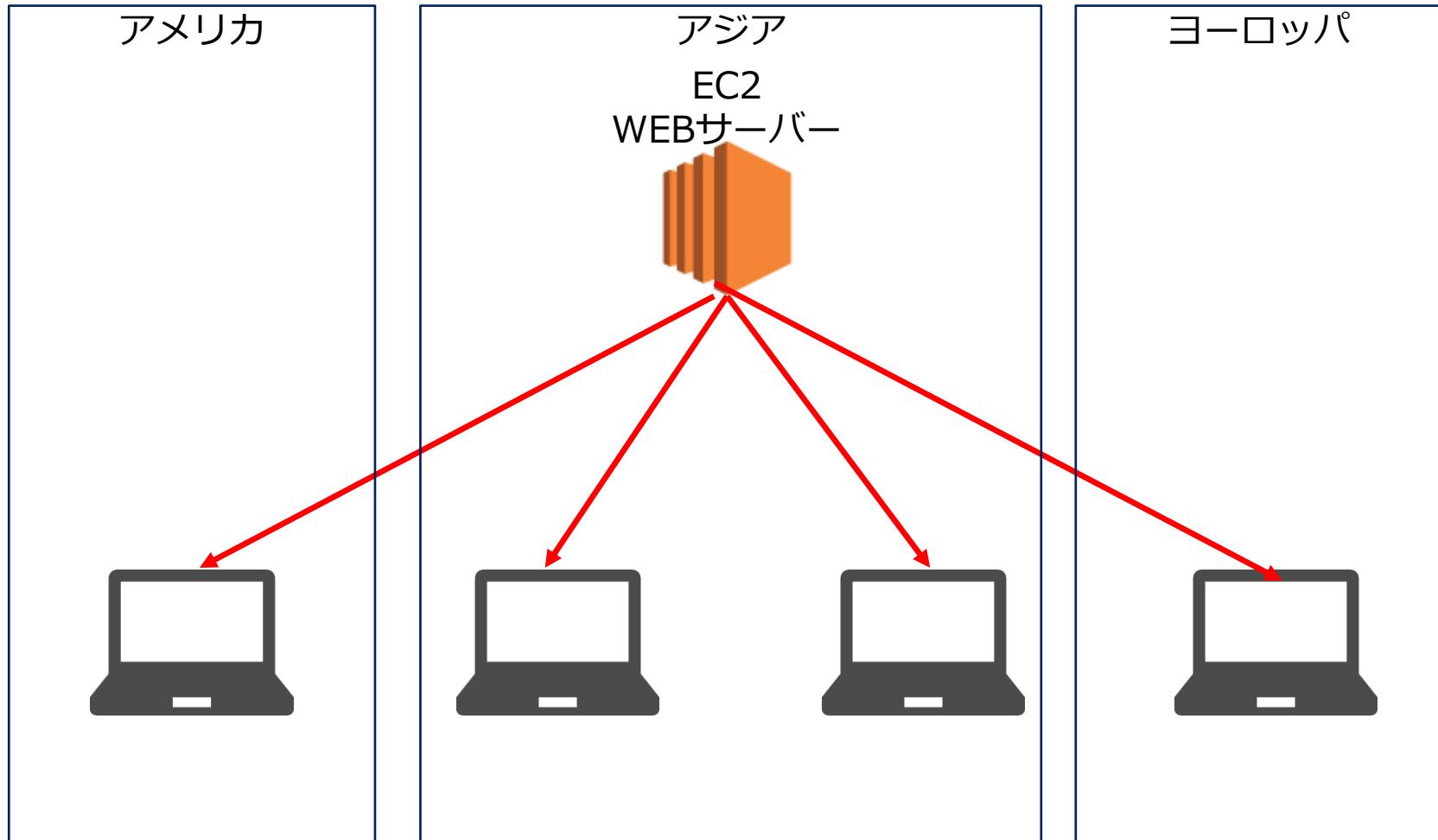
CloudFrontはAWSが提供するCDN（Content Delivery Network）サービス



CloudFront

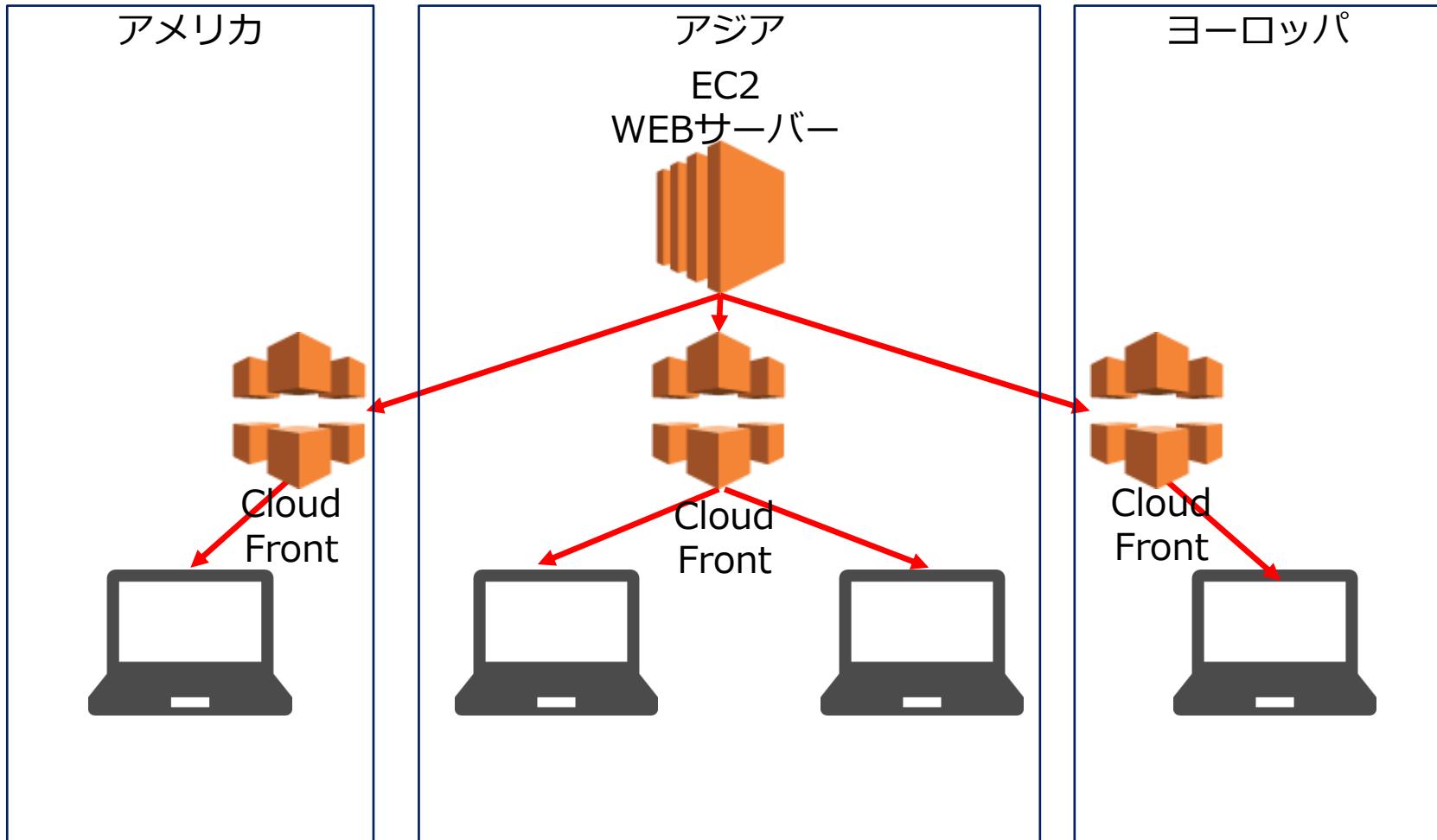
CloudFrontとは何か？

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



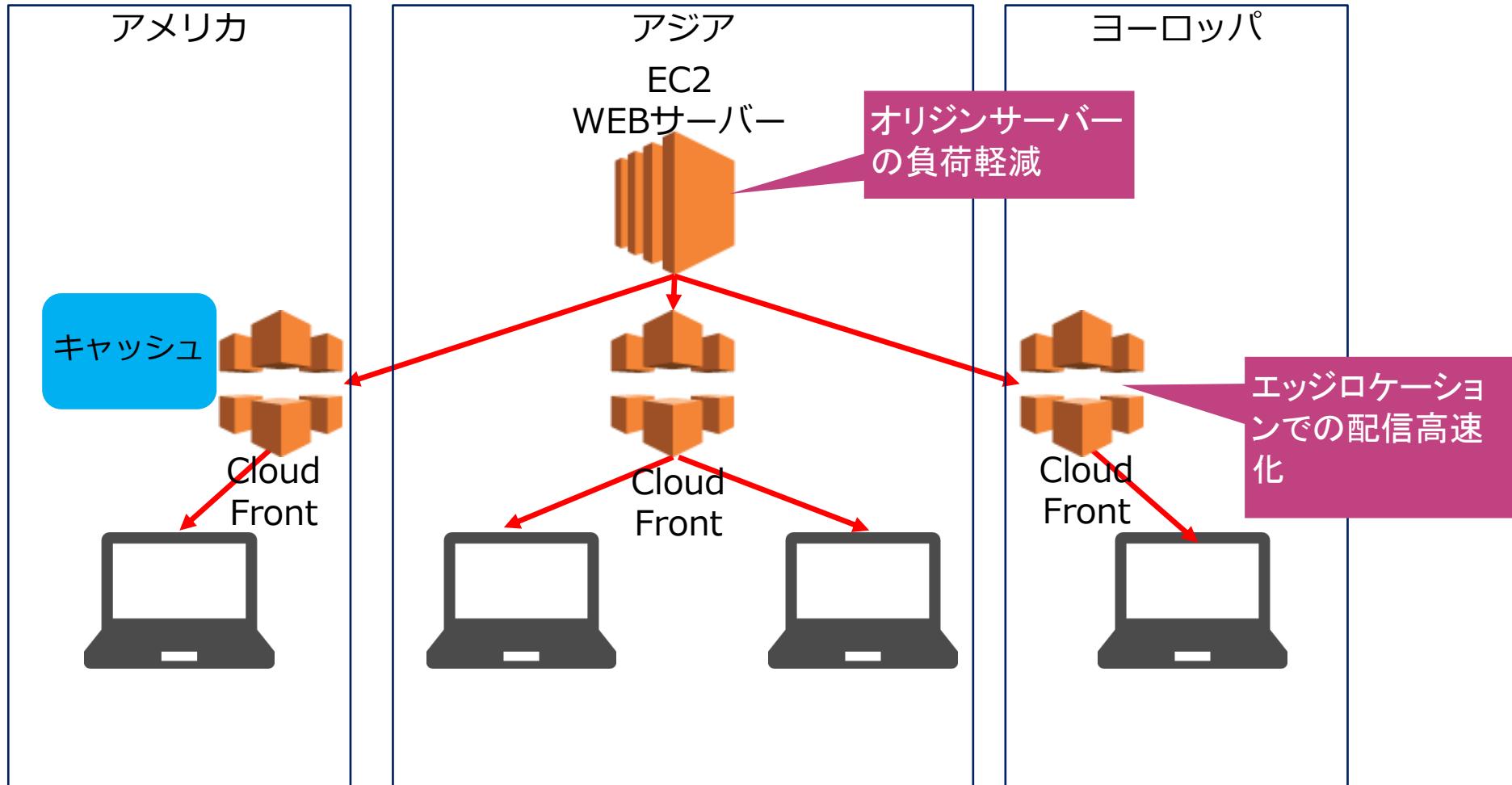
CloudFrontとは何か？

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とは何か？

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の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

CloudFrontのS3構成	✓ コンテンツ配信を高パフォーマンス化するなどのシナリオに基づいてCloudFrontを利用した構成が問われる。
CloudFrontのカスタムオリジン構成	✓ EC2やELBなどをカスタムオリジンとした場合のCloudFrontの構成が問われる。
オリジンの冗長化	✓ オリジンサーバーの冗長化が必要とされるシナリオに基づいて、CloudFrontの冗長化構成が問われる。
エッジロケーション	✓ CloudFrontが配信の際に利用するエッジロケーションの利用方法が問われる。
リージョナルエッジキャッシュ	✓ CloudFrontが配信の際に利用するリージョナルエッジキャッシュの利用方法が問われる。

CloudFrontの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

CloudFrontの挙動	✓ CloudFrontが最初にキャッシュを取得する挙動や、キャッシュデータが存在しない場合のCloudFrontの挙動が問われる。
キャッシュの保持期間の設定	✓ CloudFrontの配信設定時におけるキャッシュの保持期間の設定方法が問われる。 ✓ Cache-Control ヘッダーを利用した設定方法が問われる。
キャッシュの活用	✓ キャッシュを活用した配信処理設定や、細かい制御をする方法や効果が問われる。
CloudFrontの利用料	✓ CloudFrontにおいてコストが発生する要因が問われる。
Gzip圧縮機能	✓ Gzip圧縮機能の活用方法が問われる。

CloudFrontの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

オリジンへのアクセス制御	✓ CloudFrontを迂回してオリジンにアクセスすることを制限する設定方法が問われる。
キャッシュのアクセス制御	✓ ユーザーがキャッシュデータにアクセスする際の利用制限をする方法が問われる。
CloudFront地域制限	✓ 特定の国や地域からCloudFront配信へのアクセスを制限する設定が問われる。
暗号化	✓ CloudFrontにおける通信の暗号化の設定方法が問われる。 ✓ CloudFrontにおけるフィールドレベル暗号化の用途が問われる。
ログ取得	✓ CloudFrontにおけるログ取得方法とその使い方が問われる。

CloudFrontの特徴

大規模なアクセスも世界中にあるエッジロケーションを活用して効率的かつ高速にコンテンツ配信することができる。

- 210以上のエッジロケーションによる高性能な分散配信
- 高いパフォーマンス
- AWS WAF／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

[Q]CloudFrontのS3構成

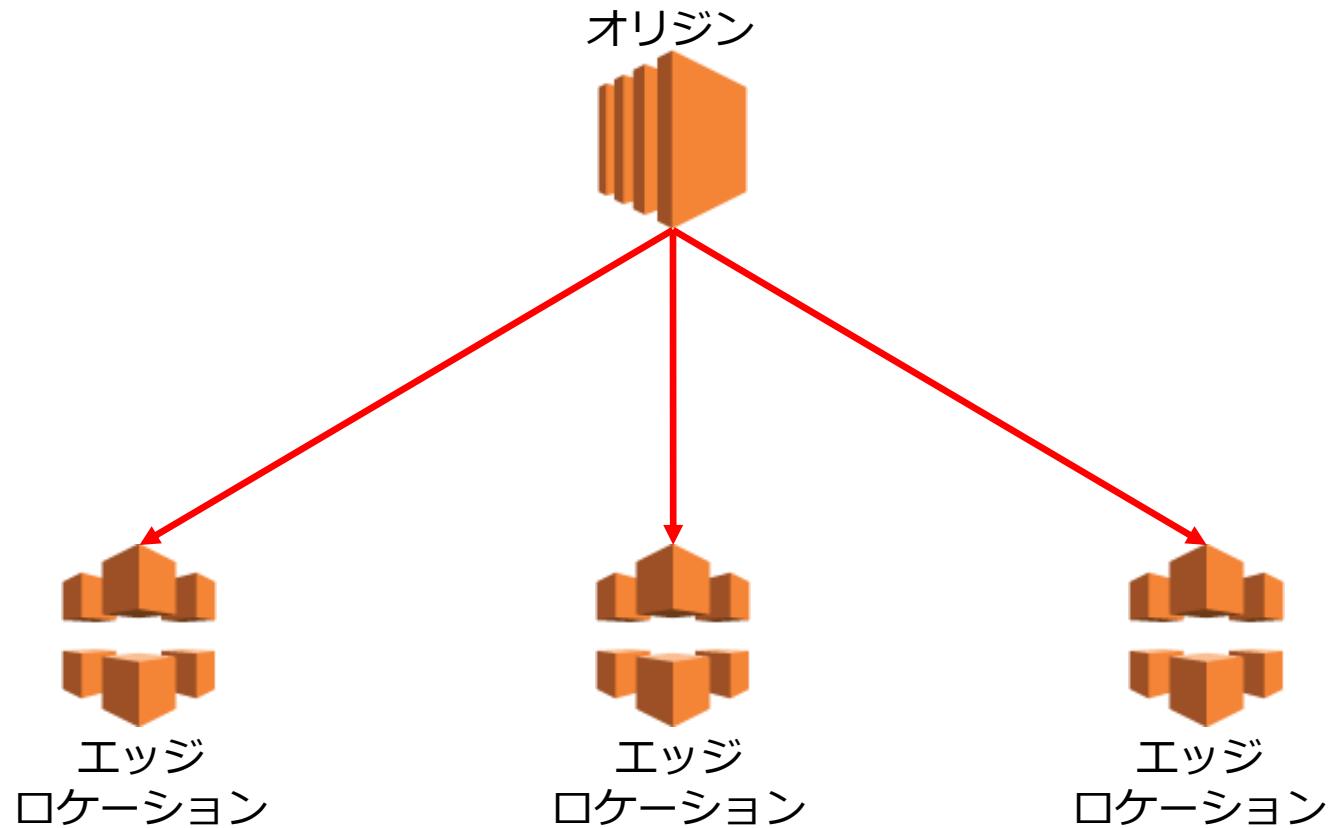
大手ニュースメディアは、AWSを利用したニュース配信アプリケーションを構築しています。アプリケーションはEC2インスタンスとS3を利用して構成されており、S3バケットに蓄積したビデオデータに基づいてストリーミング配信を実施します。ビデオデータのアップロードと配信リクエストが頻発されるため、あなたはソリューションアーキテクトとして、リクエスト処理のパフォーマンスを向上させたいと考えています。

この問題に対処するために実施すべきソリューションは次のうちどれですか？（2つ選択してください）

- 1) S3バケットをオリジンとしてCloudFrontディストリビューションを構成する。
- 2) Route53による地域制限設定を導入して、地域ごとの配信を最適化する。
- 3) S3バケットのS3 Transfer Accelerationを有効にする。
- 4) ELBを追加してクロスゾーン負荷分散を有効化する。
- 5) EC2インスタンスをストレージ最適化インスタンスに変更する。

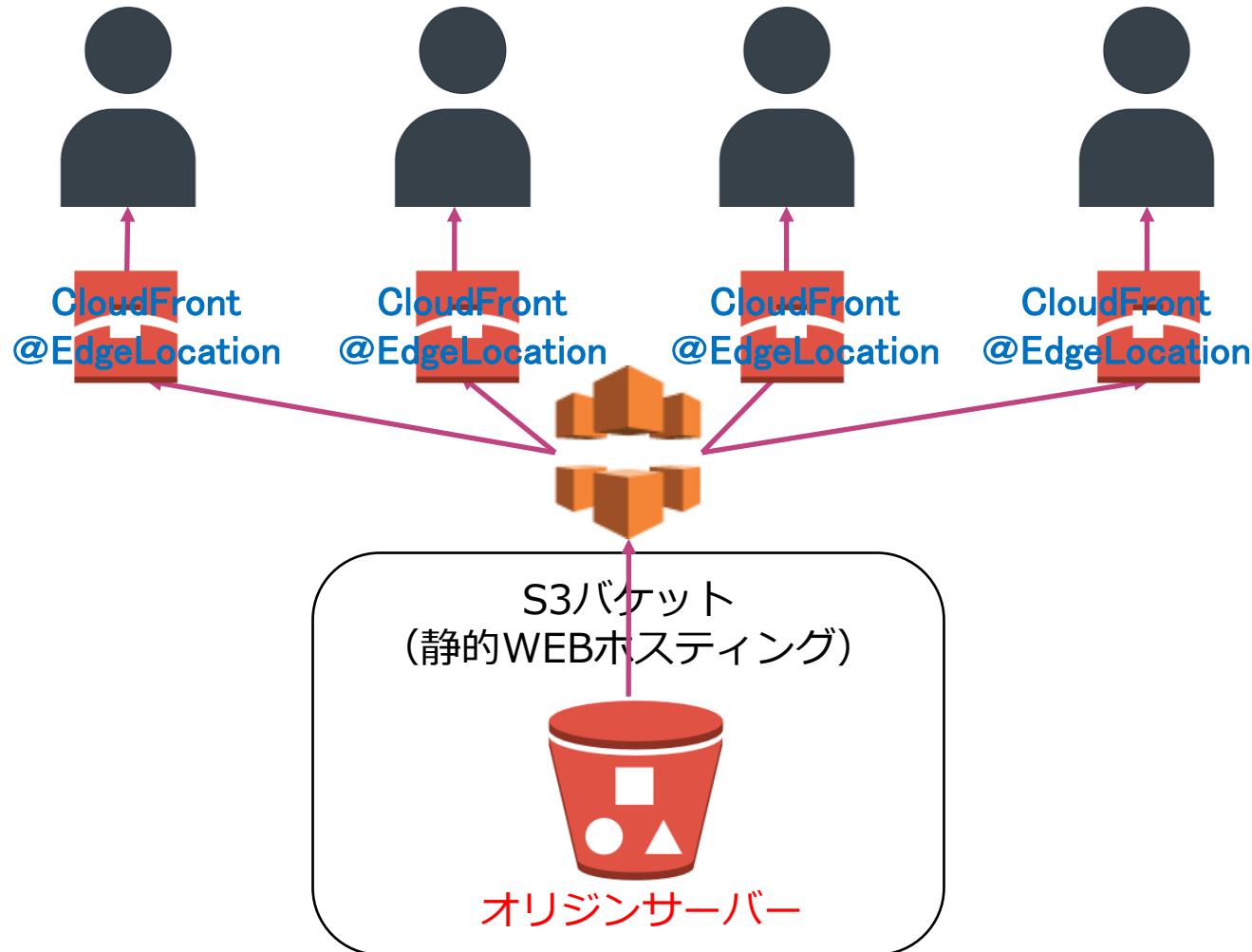
CloudFrontの構成

ユーザーに近い位置にあるエッジロケーションから配信する
シンプルなアーキテクチャ



CloudFrontの構成

S3の静的WEBホスティングなどに対してCloudFront配信を構成するのが基本構成の1つ



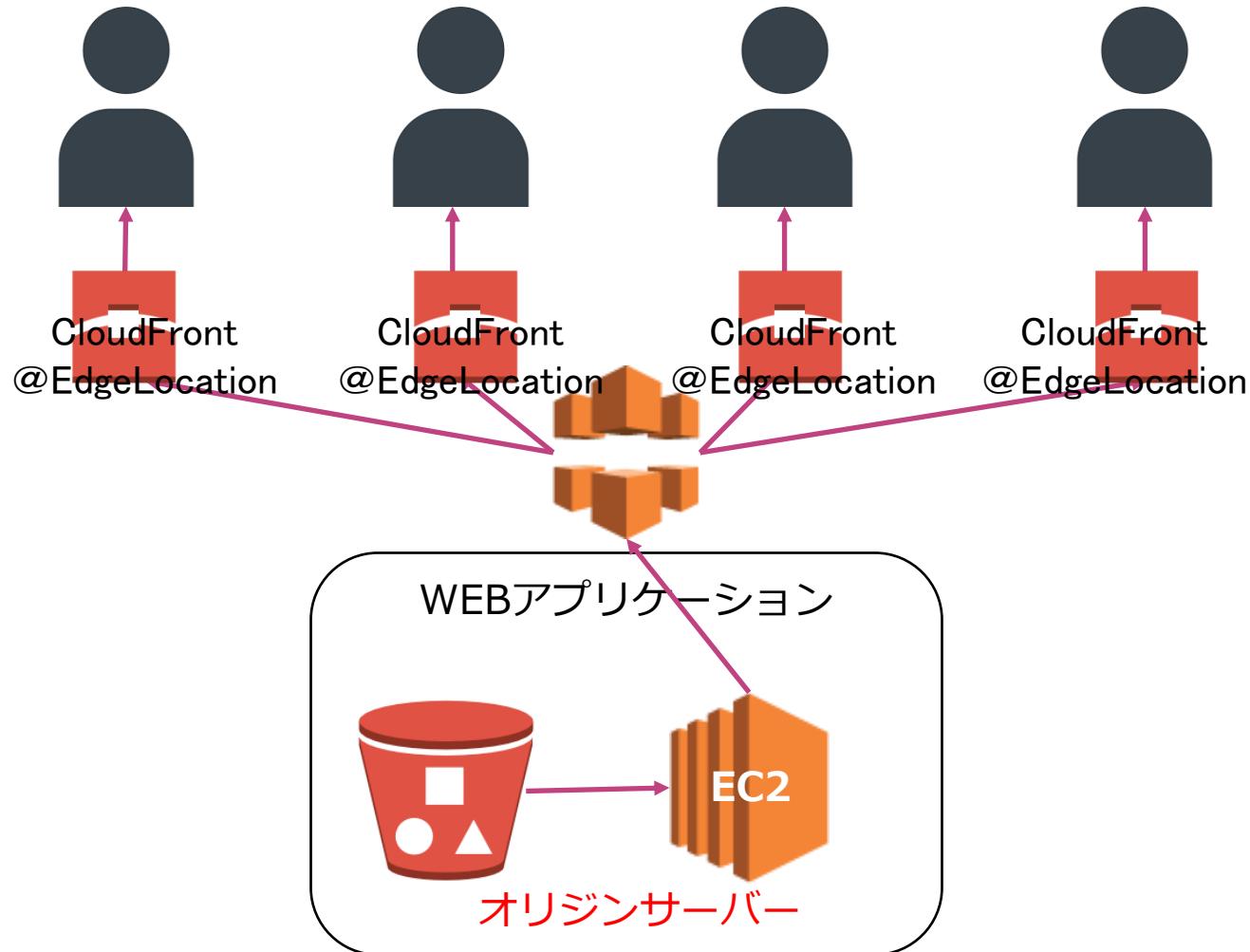
[Q] CloudFrontのカスタムオリジン構成

大手ニュースメディアは、AWSを利用した音楽配信アプリケーションを構築しています。アプリケーションは10個のEC2インスタンスとAuto scalingにより構成されており、各楽曲は、EC2インスタンスが簡単にアクセスできるFTP上に存在します。クリスマスシーズンなどの音楽配信が盛んに実施される時期になるとアクセスが急増し、Auto scaling がインスタンスを100個に拡張して、AWSの利用コストが増大します。特にネットワーク転送アウトが高いようです。あなたはソリューションアーキテクトとして、アプリケーションコードを変更せずに大幅にコストを削減するように依頼されました。

- 1) AWS Transit Gatewayを活用する
- 2) ELBのクロスゾーン負荷分散を利用する。
- 3) Route53の加重ルーティングを利用する。
- 4) CloudFrontディストリビューションを使用する

CloudFrontの構成

WEBアプリケーションのEC2インスタンスをオリジンサーバーとする構成も基本



[Q]オリジンの冗長化

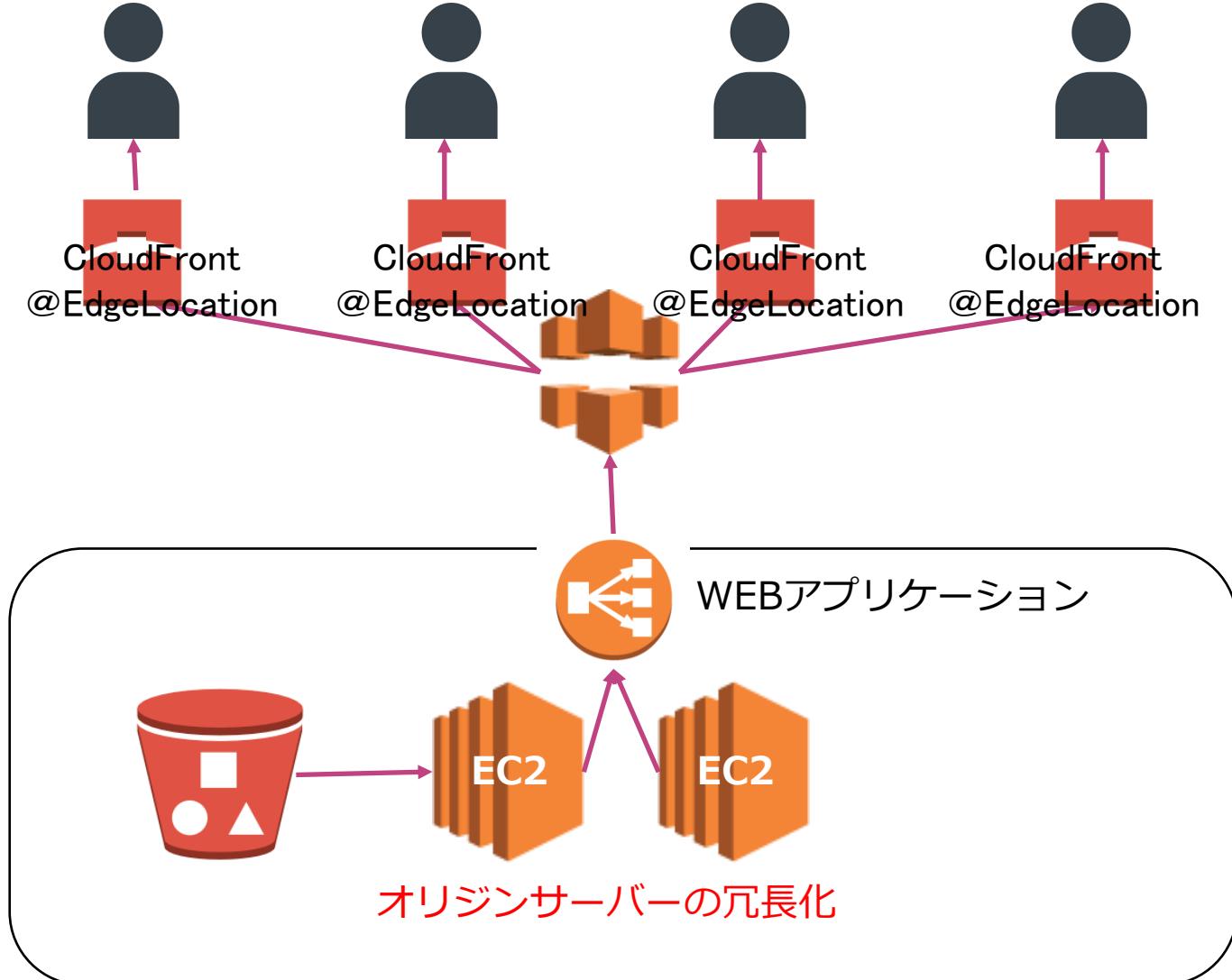
大手ニュースメディアは、AWSを利用した音楽配信アプリケーションを構築しています。アプリケーションは単一AZにある単一のEC2インスタンスを利用して構成されており、各楽曲は、EC2インスタンスをオリジンサーバーとして構成したCloudFrontを使用して配信されています。

このアプリケーションを高可用性にするための改善策を提案してください。

- 1) 既存のEC2インスタンスにELBを接続してELBをオリジンサーバーとして構成する。
- 2) Amazon S3を使用してWebアプリケーションの動的コンテンツを提供し、S3バケットをオリジンサーバーとして構成する。
- 3) 異なるアベイラビリティーゾーンにデプロイされた2つ以上のEC2インスタンスをオリジンサーバーとして構成する。
- 4) 既存のEC2インスタンスにAuto Scalingグループを追加して、Auto scaling をオリジンサーバーとして構成する。

CloudFrontの構成

オリジンサーバーを冗長化してELBを介してCloudFrontと連携する。



[Q]エッジロケーション

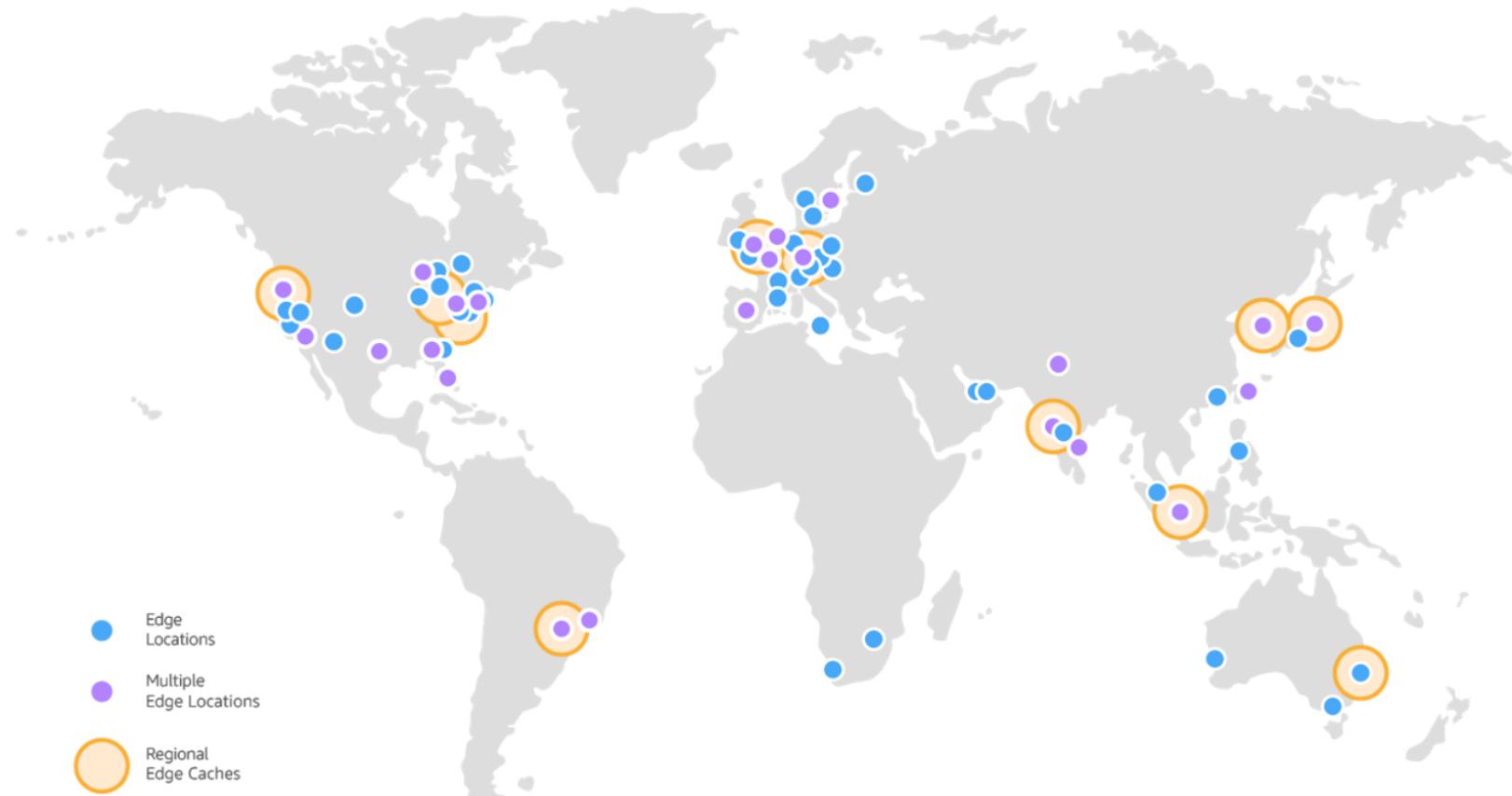
大手メディア企業は、Amazon S3 バケットにあるビデオデータにもとづいて顧客にニュースを提供しています。同社の顧客は世界中にあり、ピーク時には高い需要が発生します。欧州の各リージョンでは、ピーク時のダウンロード速度が遅く HTTP500 エラーが多発しているとのクレームが多発しており、あなたはソリューションアーキテクトとして、改善策を依頼されました。

この問題に対応するための最適なソリューションを選択してください。

- 1) Amazon Route 53 加重ルーティングポリシーを使用して、欧州地域へのルーティングの加重比率を高める。
- 2) DynamoDB の DAX クラスターを S3 バケットの前に配置して、高速な配信処理を可能にする。
- 3) ElastiCache クラスターを S3 バケットの前に配置して、高速な配信処理を可能にする。
- 4) CloudFront を使用してウェブコンテンツをキャッシュして、コンテンツ配信にすべてのエッジロケーションを使用する

エッジネットワーク

AWSはクローバルにコンテンツ配信ネットワークを利用できる



参照 : <https://aws.amazon.com/jp/cloudfront/features/?nc=sn&loc=2>

[Q]リージョナルエッジキャッシュ

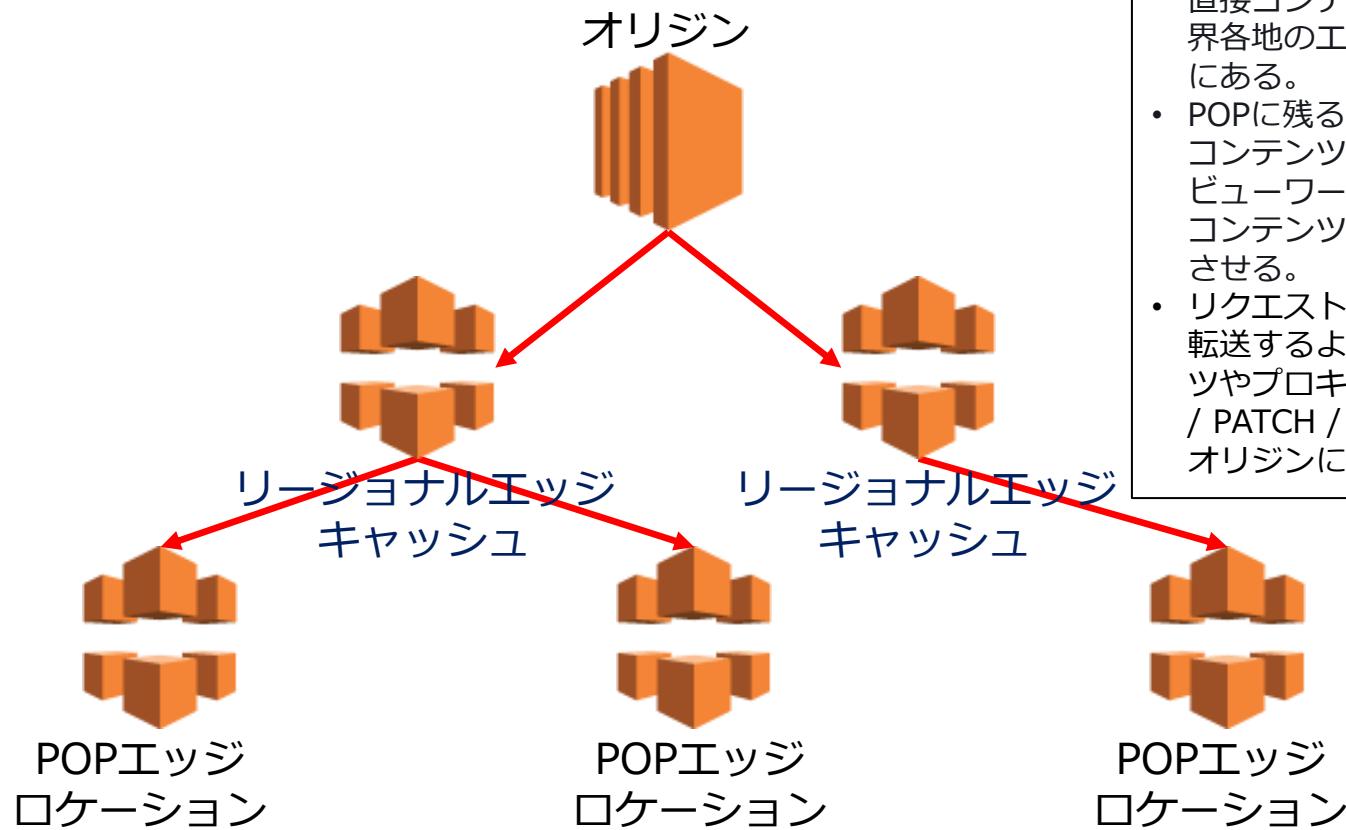
大手メディア企業は、Amazon S3 バケットにビデオデータを蓄積して、CloudFront 配信を構成して、顧客にニュースを提供しています。同社の顧客は世界中にあり、ピーク時には高い需要があります。AWS のコンテンツ配信ネットワーク（CDN）は、デフォルトで多層キャッシュを提供します。リージョナルエッジキャッシュは、オブジェクトがエッジにまだキャッシュされていない場合に、レイテンシーを改善し、オリジンサーバーの負荷を軽減してくれます。しかしながら、一部のコンテンツはリージョナルエッジキャッシュを利用していないようです。

リージョナルエッジキャッシュではなくオリジンに直接移動するコンテンツタイプはどれですか？（2つ選択してください）

- 1) 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
- 2) ユーザー側でオリジンへの直接アクセスリクエストが発せられたコンテンツ
- 3) カスタムヘッダーを利用したアクセス制御がされている全てのコンテンツ
- 4) 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。
- 5) 全てのTTLが0に設定されたコンテンツ

CloudFrontの構成

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）の中にある。
- 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

[Q] CloudFrontの挙動

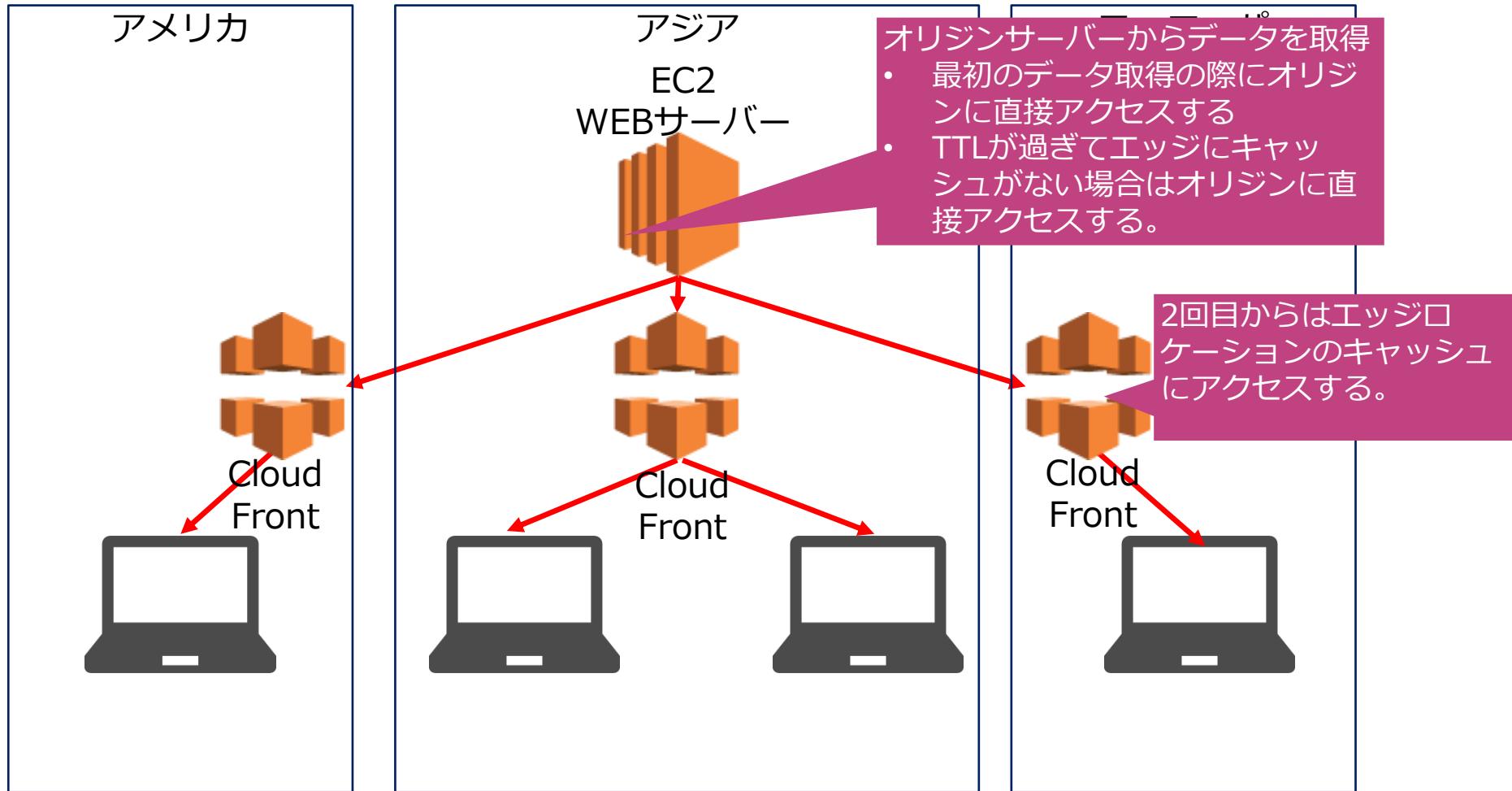
あなたの会社は、AmazonS3バケットとEC2インスタンスとCloudFrontで構成された画像配信サービスを提供しています。画像配信を最適にするためにCloudFrontを利用しています。コンテンツがエッジロケーションにない場合には、どのような処理が発生するかを確認することが必要です。

次の中でCloudFront処理として正しい説明を選択してください。

- 1) コンテンツが保存されている別のエッジロケーションを利用する。
- 2) CloudFrontがオリジンサーバーにアクセスしてエッジにデータを取得する
- 3) 適切なデータが配置されていないため404エラーが発生する
- 4) CloudFrontで要求をストックして、エッジにデータがくるまで待機する。

CloudFrontの挙動

キャッシュにデータを保持して配信を高速化する。



Distribution設定

CloudFrontは配信設定により要件に応じた最適な配信設定を実施することが必要

- 各配信先となるドメインに割り当てるCloudFrontを設定する
- マネジメントコンソールやAPIによりCloudFrontを構成する。
- WEB DistributionとRTMP Distributionのどちらかを選択する
- 使用量が最大40Gbps／10万RPS超は上限緩和申請を実施する
- 独自ドメインを指定可能

Distribution設定

Adobeメディアを利用する場合はRTMPディストリビューションを利用するが、通常はWEBディストリビューションを利用

WEB Distribution

- 通常のHTTPプロトコルを利用したWEB配信をする際に利用
- HTTP1.0/ HTTP1.1/ HTTP2に対応
- オリジンはS3バケット／MediaPackageチャネル／HTTP サーバーを設定
- HTTPやHTTPSを使用した静的および動的なダウンロードコンテンツ配信
- Apple HTTP Live Streaming (HLS)や Microsoft Smooth Streamingなど、さまざまな形式のビデオオンデマンド

RTMP Distribution

- RTMP形式配信の際に利用
- Adobe Media ServerとAdobe Real-Time Messaging Protocol (RTMP)を使用してメディアファイルをストリーミング
- S3バケットをオリジン設定
- クライアントはメディアファイル／メディアプレーヤー (JW Player、Flowplayer、Adobe Flash)を利用

[Q]キャッシュ保持期間の設定

あなたはソリューションアーキテクトとして、WEBアプリケーションの運用管理を行っています。このアプリケーションはグローバルに利用されているため、CloudFrontによる配信処理を行っています。現在、キャッシュされるべきオブジェクトがエッジロ케ーションにないため、オリジンサーバーへのアクセスが頻繁しています。この問題は、一般的に頻繁に利用されるオブジェクトに対しても発生します。

次のうち、この問題の最も可能性の高い原因を選択してください。

- 1) キャッシュすべきオブジェクト設定の指定範囲が狭い
- 2) Cache-Controlのmax-ageディレクティブが低い値に設定されている
- 3) キャッシュするべきファイルサイズがCloudFront標準を超過している。
- 4) SSL証明設定でキャッシュできていない。

キャッシュ保持期間の設定

キャッシュ対象を決定した上で、キャッシュの利用頻度を予測してキャッシュ保持期間を設定することが重要

Minimum TTL (最小 TTL)	<ul style="list-style-type: none">CloudFront がオリジンに別のリクエストを送るまでに、オブジェクトを CloudFront キャッシュに保持する最小期間 (秒) を指定デフォルト値は 0 (秒)
Maximum TTL (最大 TTL)	<ul style="list-style-type: none">オブジェクトが更新されたかどうかを CloudFront がオリジンにクエリするまでに、オブジェクトを CloudFront キャッシュに保持する最大期間 (秒) を指定する。デフォルト値は 31,536,000 (秒)つまり 1 年
Default TTL (デフォルト TTL)	<ul style="list-style-type: none">CloudFront がオリジンに別のリクエストを送るまでオブジェクトを CloudFront キャッシュに保持するデフォルト期間 (秒) を指定デフォルト値は 86,400 (秒)、つまり 1 日

キャッシュ保持期間の設定

TTLとCache-Control および Expires ヘッダーを使用して、オブジェクトをキャッシュに保持する期間を制御できます

キャッシュ対象設定		<ul style="list-style-type: none">□コンテンツ利用データ分析などを実施して、静的コンテンツ／動的コンテンツへのキャッシュ対象URLを設定する
キャッシュの有効期限	TTL	<ul style="list-style-type: none">□CloudFront配信時に設定されるキャッシュ保持期間
	Expires ヘッダー	<ul style="list-style-type: none">□Cache-Control ヘッダーのExpires ヘッダー□キャッシュの期限切れ日を設定する□【例】Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control max-age ヘッダー		<ul style="list-style-type: none">□CloudFront がオリジンサーバーからオブジェクトを再度取得するまでにオブジェクトをキャッシュに保持する期間(秒)を指定できる。□最小の有効期限切れ時間は、ウェブディストリビューションで 0 秒、RTMP ディストリビューションで 3600 秒。最大値は 100 (年)

キャッシュ保持期間の設定

キャッシュ期限を複数の要素で設定した場合に、複雑な結果となるため、矛盾する設定はなるべく避ける。

【設定が混在する場合の反映シナリオ】

- [Maximum TTL (最大 TTL)] に 5 分 (300 秒) を設定し、Cache-Control max-age ヘッダーに 1 時間 (3600 秒) を設定した場合、CloudFront は 1 時間ではなく 5 分間、オブジェクトをキャッシュする。
- Cache-Control max-age ヘッダーに 3 時間を設定し、Expires ヘッダーを 1 か月に設定した場合、CloudFront は 1 か月ではなく 3 時間オブジェクトをキャッシュする。
- [Default TTL (デフォルト TTL)]、[Minimum TTL (最小 TTL)]、および [Maximum TTL (最大 TTL)] に 0 秒を設定した場合、CloudFront は常にオリジンからの最新コンテンツがあることを確認する。

Reference: https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/Expiration.html#expiration-individual-objects

[Q]キャッシュの活用

A社はAWSで多言語ウェブサイトをホストしています。 WebサイトはCloudFrontを使用して提供されます。 言語はHTTPリクエストはhttp://pintor.cloudfrontで指定されて以下のように表示されます。

http://pintor.cloudfront.net/main.html?language=de
http://pintor.cloudfront.net/main.html?language=en
http://pintor.cloudfront.net/main.html?language=jp

net / main.html ? language = jp キャッシュデータは日本語表示サイトとして表示されるようにCloudFront側で設定する必要があります。

これを達成するための設定方法を選択してください。

- 1) クエリ文字列パラメータを設定する。
- 2) 動的コンテンツ設定を利用する。
- 3) キャッシュオリジン設定を利用する。
- 4) フォワードクッキーを利用する。

キャッシュの活用

キャッシュコントロールによりキャッシュヒット率を上昇させて効果的なキャッシュ活用を可能にする

パラメーター値の完全一致

- URLとフォワードオプション機能 (header/Cookie/Query Strings) のパラメーター値の完全一致でキャッシュが指定される仕組み
- 単一ファイルのキャッシュは最大20GB
- GET/HEAD/OPTIONリクエストを対象

キャッシュの無効化

- キャッシュが期限切れになる前に無効化することが可能
- 必要のないキャッシュを無効化することで効果的な利用を可能にする
- コンテンツ毎に最大3000個まで無効化パスを指定できる
- ワイルドカードを利用して最大15個まで無効化パスリクエストが指定可能

[Q] CloudFrontの利用料

大手画像配信サイトはAWS上に構築されています。サイトの運営会社は画像配信の仕組みを効率化するためにCDNの利用を検討しています。そこで、あなたはソリューションアーキテクトとして、CloudFrontを利用したコンテンツ配信に必要なコストを算出して報告することになりました。

次のうち、CloudFrontのコスト算出の要素を選択してください。（2つ選択してください。）

- 1) リージョン数
- 2) グローバルエッジロケーションの数
- 3) データ転送アウト
- 4) リクエスト数
- 5) 設定されたキャッシュ数

CloudFrontの利用コスト

主にリクエストとデータ転送アウトに対して料金が発生

リクエスト

- HTTP/HTTPS リクエスト
- ORIGIN SHIELD リクエスト
- 無効リクエスト
- フィールドレベル暗号化リクエスト
- リアルタイムログリクエスト

データ転送アウト

- インターネットへのリージョンデータ転送アウト (GB 単位)
- オリジンへのリージョン内データ転送アウト (GB 単位)

データ転送アウト

- CLOUDFRONT ディストリビューションに関する、専用 IP カスタム SSL 証明書

[Q] Gzip圧縮機能

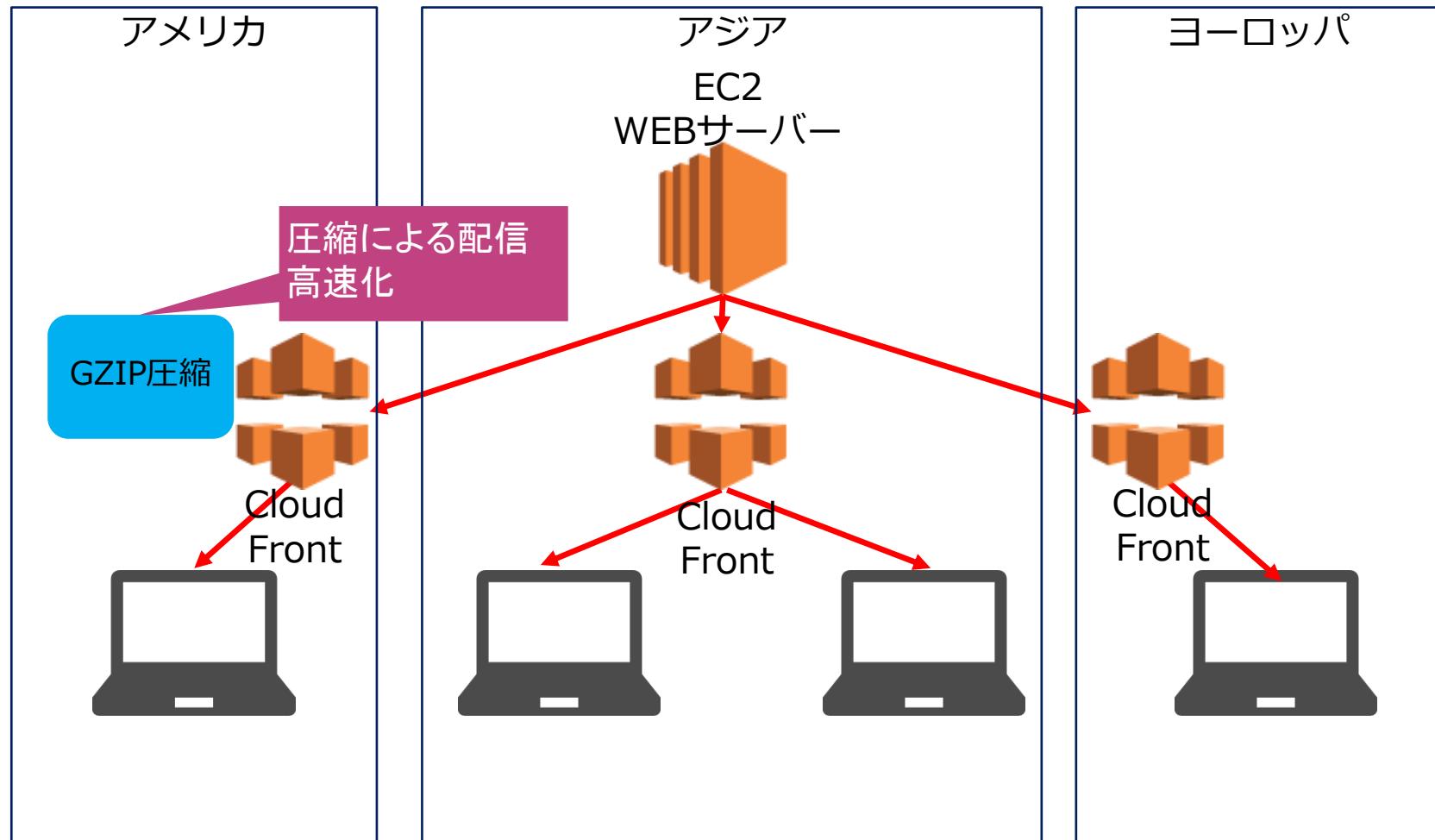
S3に静的コンテンツを保存した上で、CloudFrontを利用したグローバル配信を実施しています。CloudFrontは配信先が多いことで、利用料金が想定より高くなっています。これが問題となっています。

CloudFrontのコスト削減効果のある方法はどれでしょうか？

- 1) エッジロケーションによるファイル圧縮処理を実施する。
- 2) CloudFrontによるキャッシュ保持期間を短縮する。
- 3) Lambda@エッジによるファイル圧縮処理を実施する。
- 4) オリジンサーバーに設定したS3による配信コンテンツの圧縮処理を実施する。

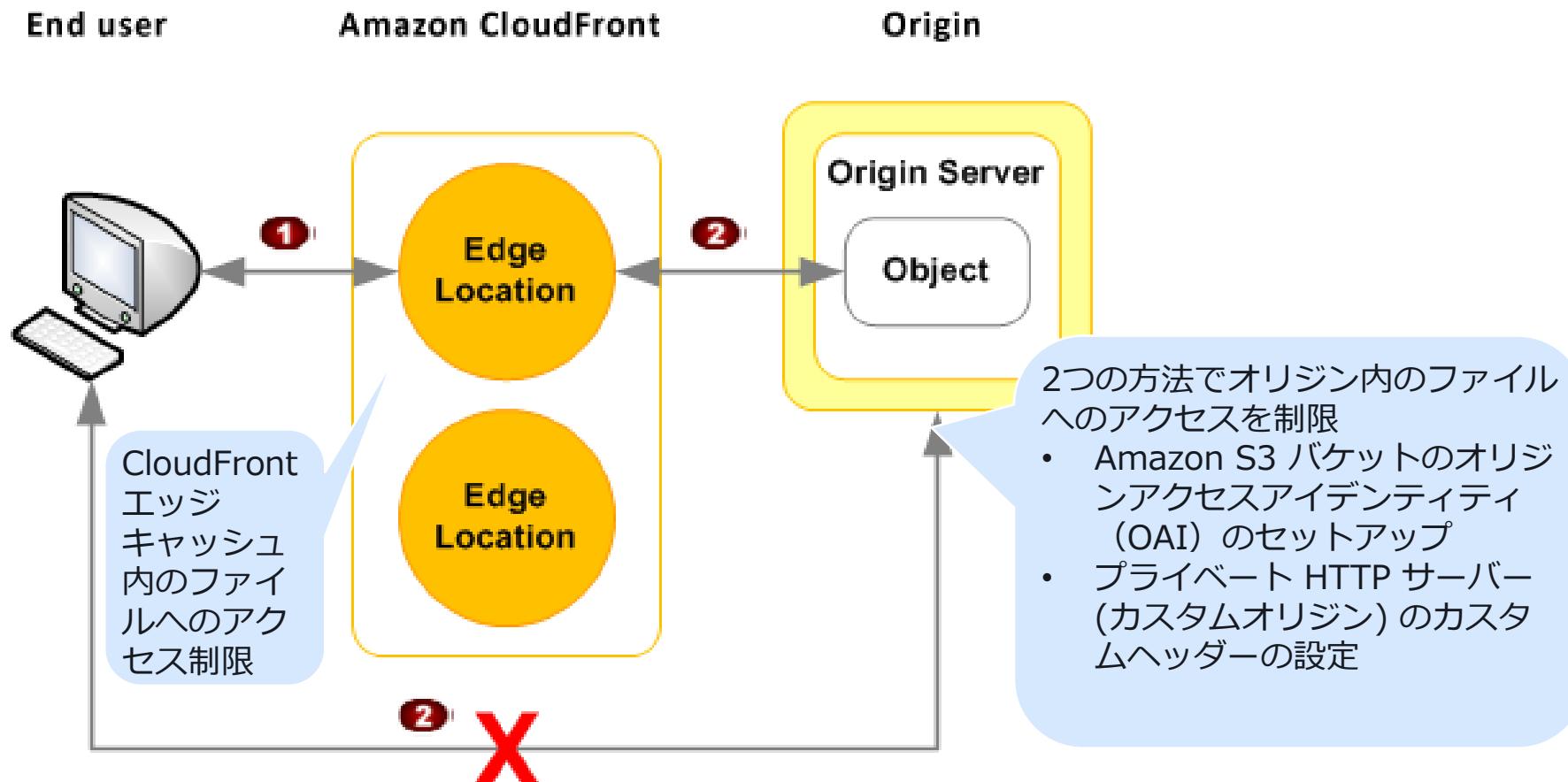
Gzip圧縮機能

エッジ側でコンテンツをGZIP圧縮してより高速に配信可能



アクセス制限

署名付きURLと署名付きCookieにより配信コンテンツへのアクセスを詳細に制御する。



[Q]オリジンへのアクセス宣言

あなたが構築したアプリケーションでは、S3に静的コンテンツを保存した上で、CloudFrontを利用したグローバル配信を実施しています。その際に、CloudFrontディストリビューションとWebサイトの静的ファイルを含むS3バケット間の通信を完全に保護したいと考えています。ユーザーはCloudFrontを介してのみS3バケットにアクセスでき、直接アクセスできないようにする必要があります。

この要件を満たすことができるソリューションを選択してください

- 1) オリジンアクセスID（OAI）を作成し、S3バケットポリシーに設定する。
- 2) CloudFrontセキュリティグループからのトラフィックのみを許可するようにS3バケットポリシーを設定する。
- 3) 署名付きURLを利用して、オリジンアクセスを制限する。
- 4) アクセスコントロールリストを作成し、オリジンアクセスを制限する。

オリジンへのアクセス制限

OA1でS3バケットへの、カスタムヘッダーでカスタムオリジンへのアクセスを宣言する。

OA1

- OA1はS3 バケットへのアクセスを CloudFront からのリクエストに絞るための仕組み
- オリジンアクセスアイデンティティ (OA1) と呼ばれる特別な ユーザーを作成し、そのユーザーに限定してアクセスを許可
- CloudFrontはOA1 を使用してバケット内のファイルにアクセスする。

カスタムヘッダー

カスタムヘッダーをオプションで設定して、カスタムオリジンへのアクセスを制限する仕組み

ビューワープロトコル ポリシー

ビューワーが CloudFront にアクセスするのに HTTPS を使用しなければならないようにディストリビューションを設定

オリジンプロトコル ポリシー

CloudFront がビューワーと同じプロトコルを使用してリクエストをオリジンに転送するように、ディストリビューションを設定

[Q]キャッシュのアクセス制限

大手画像配信サイトはAWS上に構築されています。画像配信の仕組みを効率化するためにCDNの利用を検討しています。あなたはソリューションアーキテクトとして、CloudFrontを使用して、効率的にコンテンツを配信する計画をたてました。その際には会員登録されたエンドユーザーのみがコンテンツが利用できるようにする必要があります。

この要件を満たすことができるソリューションを選択してください。 (2つ選択してください)

- 1) CloudFrontの署名付きURLを使用する
- 2) CloudFrontで署名されたCookieを使用する
- 3) CloudFrontとカスタムオリジン間の通信にHTTPSが必要
- 4) CloudFrontとS3オリジン間の通信にHTTPSが必要
- 5) CloudFrontでOAIを使用する

キャッシュのアクセス制限

署名付きURLと署名付きCookieでキャッシュに保持したコンテンツにアクセスできるユーザーを制限する

署名付きURL

- ・コンテンツに直接アクセスするURLではなく、署名付きURLからのみアクセスさせる。
- ・署名付きCookieはRTMPディストリビューションではサポートされていないため署名付きURLを利用する。
- ・個別のファイル（アプリケーションのインストールダウンロード）へのアクセスを制限する場合に利用する。
- ・ユーザーがCookieをサポートしていないクライアント（カスタムHTTPクライアントなど）を使用している場合に利用する。

署名付きCookie

- ・コンテンツに直接アクセスするURLではなく、署名付きCookieからのみアクセスさせる。
- ・複数の制限されたファイル（HLS形式の動画のすべてのファイルやウェブサイトの購読者の領域にあるすべてのファイルなど）へのアクセスを提供する場合に利用する。
- ・現在のURLを変更したくない場合に利用する。

[Q] CloudFront地域制限

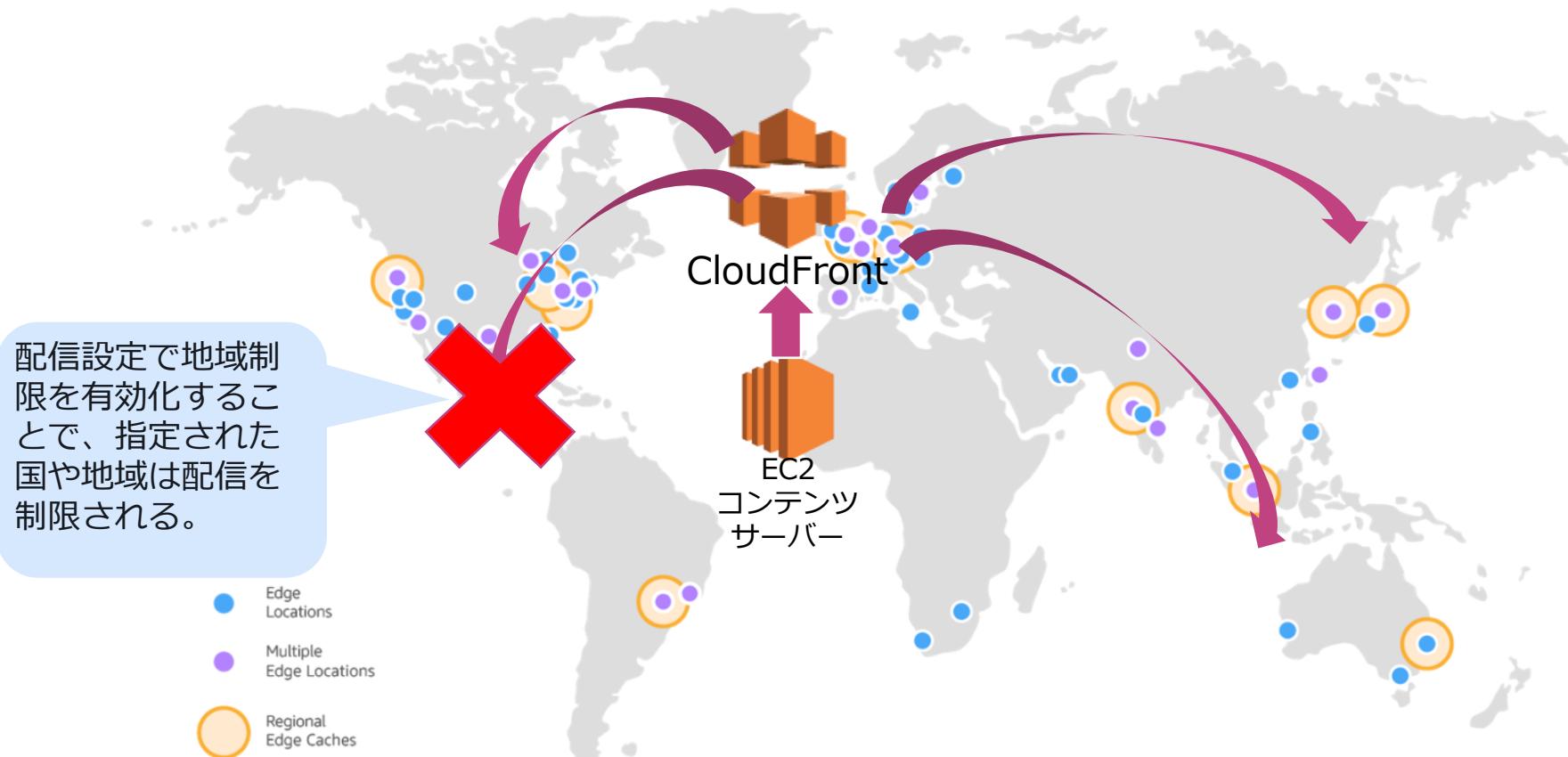
大手ニュース配信企業はニュース配信アプリケーションをAWS上に構築しています。ユーザーはグローバルに存在しており、グローバルにコンテンツを配信します。アプリケーションは、ALBの背後にあるプライベートサブネットに設置されたEC2インスタンスのフリートを使用しています。中国からの情報制限があり、中国からのアクセスをブロックする必要があります。

この要件を満たすための最も簡単な方法は何ですか？

- 1) ネットワークACLを使用して、特定の国に関連付けられたIPアドレス範囲をブロックする。
- 2) ELBのセキュリティグループを変更して、ブロックされた国からの着信トラフィックを拒否する。
- 3) CloudFrontを使用してコンテンツを提供し、特定の国からのアクセスをブロックする。
- 4) EC2インスタンスのセキュリティグループを変更して、ブロックされた国からの着信トラフィックを拒否する。

CloudFront地域制限

地域制限機能を利用して、特定の場所にいるユーザーからのアクセスを制限する。



参照 : <https://aws.amazon.com/jp/cloudfront/features/?nc=sn&loc=2>

[Q] ELBへのアクセス制限

ニュースメディアアプリケーションではCloudFrontを使用してWEBニュースを配信しています。このアプリケーションは、Elastic Load Balancer (ELB) の背後にあるEC2インスタンスで実行されています。ユーザーがCloudFrontを回避し、ELBを介してコンテンツに直接アクセスする機能を制限する必要があります。

この要件を満たすことができるソリューションを選択してください（2つ選択してください。）

- 1) ELBにVPCセキュリティグループを作成して、Lambda関数のアクセスを許可する。
- 2) ELBにIAMロールを設定して、Lambda関数のアクセスを許可する。
- 3) Lambda関数にIAMロールを設定して、ELBへのアクセスを許可する。
- 4) AWS Lambdaを使用して、CloudFront内部サービスのIPアドレスが変更されたときに自動的に更新する。
- 5) オリジンアクセスID (OAI) を作成し、それをディストリビューションに関連付ける。
- 6) ネットワークACLを使用してELBへのアクセスを制限する

ELBへのアクセス制限

CloudFrontではなくオリジンELBに直接アクセスするのを回避する設定も可能

CloudFrontのIPレンジを利用

- CloudFrontのIPアドレスを指定して、指定したIPのみELBへのアクセスを許可する設定を行う方式
- CloudFrontのIPレンジを取得し、IPアドレスに変更があった場合はセキュリティグループのインバウンドルールを更新するLambda関数がIPを作成して、Lambda関数によるIPアドレス設定を実施する。
- IPアドレス上限の緩和申請が必要

CloudFrontのカスタムヘッダーを利用

- 指定した文字列がカスタムヘッダに入ってない場合にELBへのアクセスを制限する方式
- CloudFrontのカスタムヘッダを利用して、任意のヘッダをELBオリジンに渡す

[Q]暗号化

Webメディア企業は、CloudFrontを使用してWebサーバーをオリジンとして設定して、読み取りパフォーマンスを改善することにしました。最近になって、IT監査を実施し、CloudFrontを利用した配信処理が安全ではないため、OriginサーバーとCloudFrontへのデータ通信をセキュアにすることを要求されました。このOriginサーバーはELBではないことに留意が必要です。

この要件に対応するための最適な方法を選択してください。

- 1) AWS Certificate Manager (ACM) をオリジンとCloudFront側に利用して、HTTPSによるデータ通信を可能にする。
- 2) サードパーティのCA証明書をビューアーとCloudFront側に利用して、HTTPSによるデータ通信を可能にする。
- 3) サードパーティのCA証明書をオリジンとCloudFront側の両方に利用して、HTTPSによるデータ通信を可能にする。
- 4) AWS Certificate Manager (ACM) をビューアーとCloudFront側に利用して、HTTPSによるデータ通信を可能にする。

[Q]暗号化

政府機関は個人のパーソナル番号に基づいて納税情報を配信するセキュリティ要求の高いアプリケーションをAWSを利用して構築しています。このアプリケーションは市民から個人を特定できる情報（PII）を送受信することが必要であり、その際の二重のデータ保護策が求められています。通信の暗号化を実施しつつ、CloudFront エッジロケーションで追加レベルの暗号化を適用して、PIIデータがエンドツーエンドで保護することが必要です。

ソリューションアーキテクトとして、最適な施策を選択してください。（2つ選択してください。）

- 1) 署名付きURLを利用してデータを配信する。
- 2) フィールドレベルの暗号化を設定する。
- 3) ACMを利用したHTTPS通信を実行する。
- 4) オリジンアクセスIDを付与したデータを配信する。
- 5) CloudHSMを利用したデータ暗号化を実施する。

暗号化

CloudFrontはSSL/TLS暗号化とフィールドレベル暗号化を利用

SSL/TLS

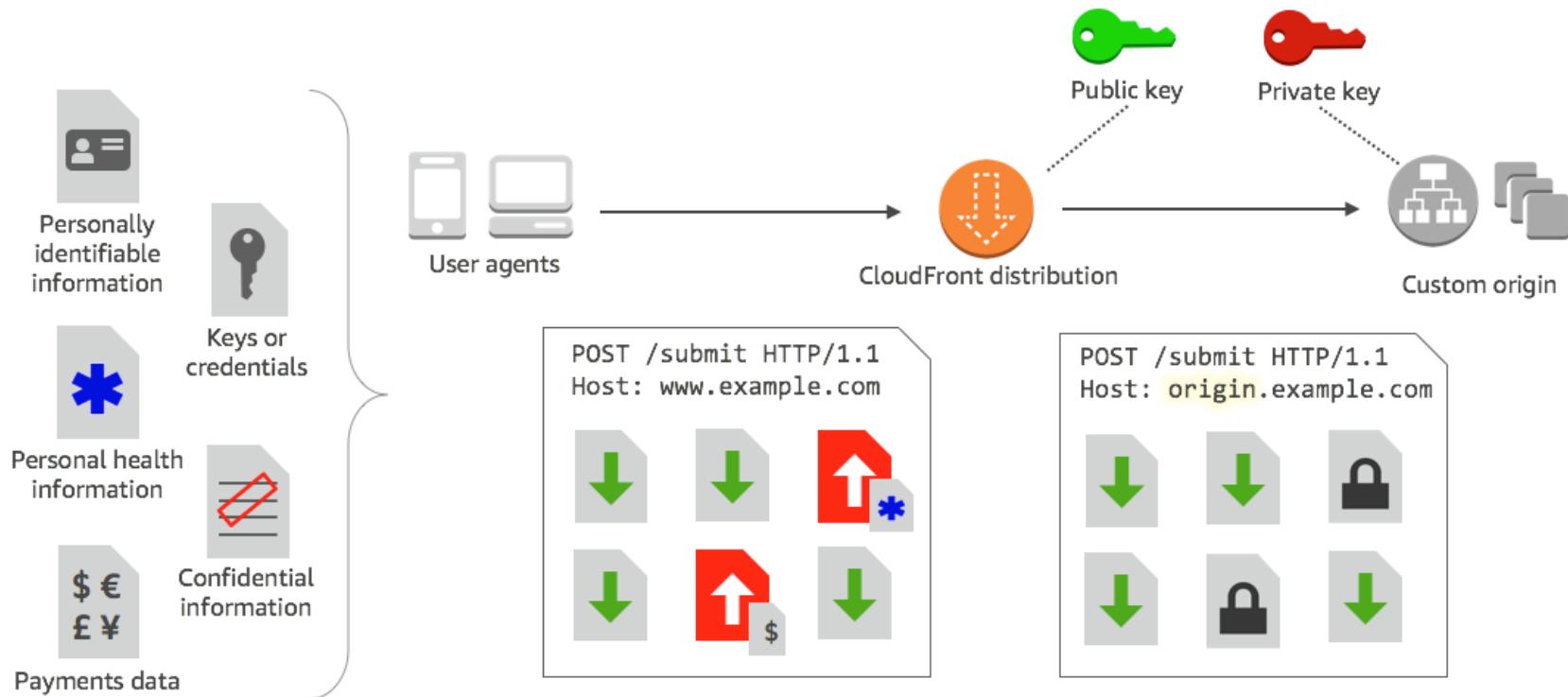
- AWS ACMと連携して証明を発行し、設定することが可能
- SSL証明書を設定してコンテンツ配信をHTTPSとする。
- CloudFront がビューアーと通信する際はビューアーが HTTPS を使用してファイルをリクエストするように Amazon CloudFront を設定
- オリジンからファイルを取得する際に CloudFront が HTTPS を使用するように設定して、CloudFront とオリジンとの通信を暗号化する
- SSLはPerfect Forward Secrecy (PFS) に対応

フィールドレベル 暗号化

- HTTPS と共にセキュリティのレイヤーが追加される。
- システムの処理中に特定のデータに特定のアプリケーションのみがアクセスできるようにエンドツーエンドでデータを保護
- CloudFront のフィールドレベル暗号化では、公開鍵認証方式を利用した暗号化を実施

フィールドレベル暗号化

CloudFront のフィールドレベル暗号化では、公開鍵認証方式を利用した暗号化を実施



Reference: https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

[Q]ログ取得

あなたの会社はCloudFrontを使用してホストされているWEB配信サービスを展開しています。ITセキュリティ部門はこのWeb配信を使用するアプリケーションのPCIコンプライアンスへの対応状況を監査しています。

コンプライアンス目標を確実に満たすための適切な対応を選択してください。（2つ選択してください。）

- 1) VPCフローログをCloudFrontに設定する。
- 2) CloudTrailをCloudFrontに設定する。
- 3) CloudFrontのキャッシュログを有効化する。
- 4) CloudFront APIに送信されるリクエストを取得する。
- 5) CloudFrontアクセスログを有効化する。

その他のセキュリティ機能

様々な外部サービスと連携することで、セキュアなコンテンツ配信やアクセス管理が可能

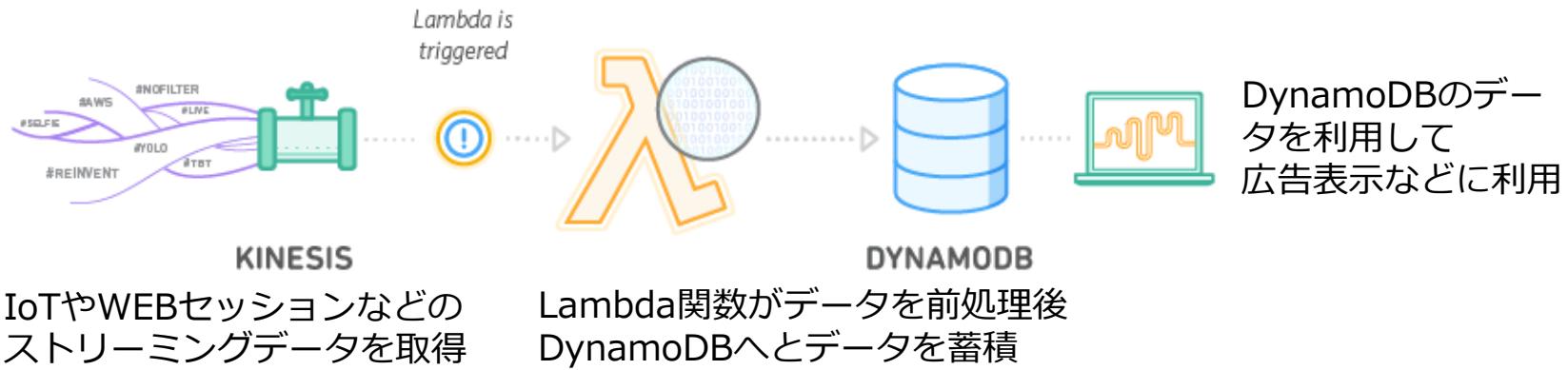
- AWS WAFによるファイアーウォールと連携し、ディストリビューションに対するウェブリクエストを許可、ブロックが可能。また、Referrer制限によるリンク参照禁止も可能
- AWS ShieldによるDDoS対応
- CloudTrailは、ユーザー、ロール、または AWS のサービスにより CloudFront で実行されたアクションレコードを提供
- CloudFront アクセスログは、ディストリビューションに対して行われたリクエストに関する詳細なレコードを提供

DynamoDBの出題範囲

DynamoDBとは何か？

ストリーミングデータを利用したリアルタイムデータ処理などに最適なデータベースとして利用するNoSQL型データベース

DynamoDBの活用例



Reference: <https://aws.amazon.com/jp/dynamodb/>

DynamoDBの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

DynamoDBの選択	✓ データベース要件が提示され、それに合った最適なデータベースとしてDynamoDBを選択する質問が出題される。
DynamoDBの特徴	✓ DynamoDBの性能や制約などを含めた特徴が問われる。 ✓ DynamoDBが利用できるユースケースが問われる。
整合性モデル	✓ DynamoDBの整合性モデルに基づく影響など、整合性モデルに関わる問題が出題される。
DynamoDBのインデックス	✓ DynamoDBで利用されるキーのタイプや設定方法が問われる。 ✓ DynamoDBの2つのセカンダリーアインデックスの用途と違いが問われる。
DynamoDBストリーム	✓ DynamoDBストリームの効果やユースケース、ストリームを利用したアーキテクチャ構成に関する問題が出題される。

DynamoDBの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

スケーリング	✓ DynamoDBのスケーリングの設定方法やその効果が問われる。
DAX	✓ DynamoDBを利用したスケーリング方法の1つとしてDAXの利用が問われる。
グローバルテーブル	✓ DynamoDBグローバルテーブルの設定方法や利用目的が問われる。
キャパシティモードの設定	✓ DynamoDBの2つのキャパシティモードの違いや目的に関する質問が出題される。

[Q] DynamoDBの選択

B社ではIoTソリューションを提供しています。この会社ではIoTデバイスから収集するストリーミングデータを利用して、リアルタイムのデータ処理を実行しています。このデータ処理には複雑なデータスキーマの設定などは必要なく、複雑なトランザクション処理も必要としませんが、リアルタイムでの高パフォーマンスな処理が求められています。

このデータベース処理に最適なAWSのデータベースサービスを選択してください。
(2つ選択してください)

- 1) Amazon Aurora
- 2) DynamoDB
- 3) Amazon EMR
- 4) ElastiCache
- 5) RedShift

NoSQL型データベース

データベースはリレーショナルDBかそうでないDBかの大きく2つの種類がある

これまでのDB

リレーショナル
DB

ビッグデータ向けDB

NoSQL

KVS : キーバリュー型

リレーションナルなしにバリュー一行にデータをまとめることで、高速処理を可能にする

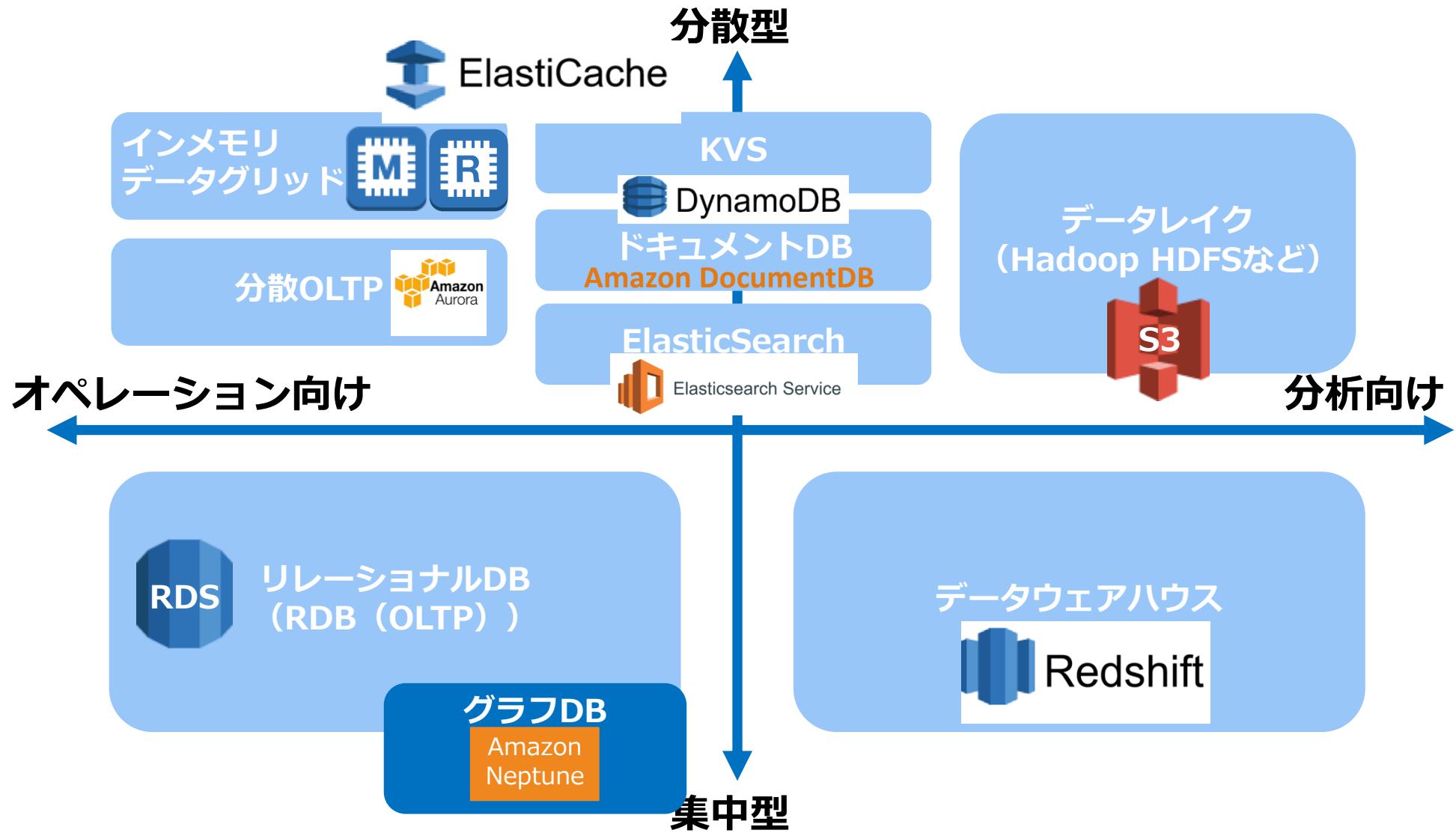
SQLのテーブル

ID	Data1	Data2	Data3
0001	XXXX	AAAA	BBBB
0002	XXXX	AAAA	BBBB

キーバルストア型DBのテーブル

Key	Value
0001	XXXX, AAAA, BBBB
0002	XXXX, AAAA, BBBB

AWSのデータベースサービス



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が得意

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

[Q] DynamoDBの特徴

B社ではAWS上に構築されたアプリケーションを利用してC to Cの売買ソリューションを提供しています。現在、WEBセッションデータ、顧客情報、商品情報を利用して、顧客への最適な商品を recommendationする機能を実装しているところです。様々なデータを利用する処理が必要となるため、どの領域でDynamoDBを使用するべきか要件を整理しています。

DynamoDBの最適な利用方法は次のうちどれですか？（2つ選択してください）

- 1) 商品画像などの400KBを超えるオブジェクトをS3に保存し、DynamoDBにはメタデータを格納する。
- 2) アイテムごとに個別のローカルセカンダリインデックスを使用して、高速処理を可能にする。
- 3) BLOBデータはDynamoDBに保存する。
- 4) アクセス頻度の高いデータとアクセス頻度の低いデータを別々のテーブルに保存する
- 5) レコメンデーションを高速処理するために顧客管理情報をDynamoDBに格納する。

DynamoDBのユースケース

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

- IoTデータなどKey Value型のシーケンシャルなデータを収集・蓄積・分析するのに最適
- Amazon EMRのHadoop処理と連携してビッグデータ処理が可能

アプリケーション

- セッションデータやメタデータなどのアプリケーション上でシンプルでデータを蓄積
- 高パフォーマンスな処理が必要なデータを保存

DynamoDBのユースケース

大量に発生しうるWEB行動データやログデータの保存には
DynamoDBを利用する。

ユーザー行動 データ管理

- ゲームのセッションデータやWEBサイトのユーザー行動データを保存・処理する。
- ユーザー毎の行動履歴管理などに利用する。

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

DynamoDBのユースケース

DynamoDBとElastiCacheはNoSQL型であるためユースケースが似ている。

比較項目	RDS	DynamonDB	ElastiCache	Redshift
リレーションナルデータベース	○	×	×	○
データベースキャッシュ	△	○	○	×
メタデータ検索	○	○	○	×
セッションなどの状態管理	△	○	△	×
大容量データ分析	△	×	×	○
リアルタイムデータ分析	△	○	○	×
低レイテンシー	△	○	○	×
モバイルバックエンドデータベース	△	○	△	×

参照 <https://qiita.com/leomaro7/items/e48d9941dab5b5f2a718>

DynamoDBの性能

完全マネージド型のNoSQLデータベースサービスであり、テーブルサイズは無制限だが、1つのデータは400KBに制限

【パフォーマンス】

- ハイスケーラブルで無制限に性能を拡張できる
- 負荷が高くなっ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

【データ容量の制限】

- **ストレージの容量制限がない**
テーブルのサイズには実用的な制限はない。
テーブルは項目数やバイト数について制限がない
- **データ項目には制限あり**
項目のサイズ制限は400 KBであり、大きなデータを格納できない。

DynamoDBの性能

1行台のミリ秒レイテンシーを安定して実現しつつ、DAXを利用すればマイクロセカンド単位でのリクエスト処理が可能

DynamoDBテーブル

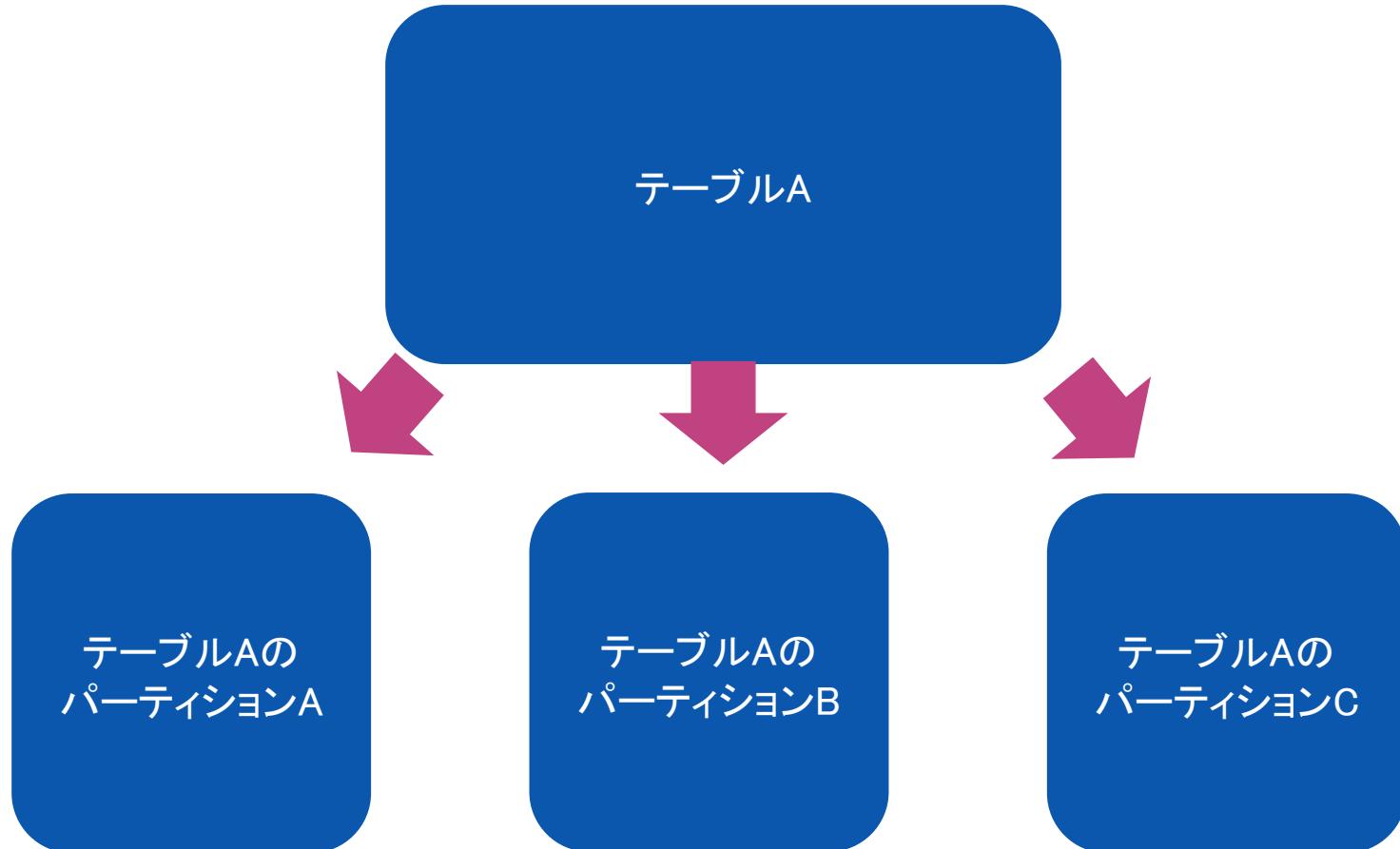
1 行のミリ秒レイテンシーを実現

DAX

1 秒あたりのリクエスト数が数百万件になる場合でも、ミリセカンドからマイクロセカンドへ向上

パーティショニング

大量データを高速処理するためにパーティショニングによる分散処理を実施している



[Q]整合性モデル

ある企業ではDynamoDBを利用して顧客のセッションデータを管理しています。ユーザーがデータベースにアクセスした際に陳腐化したデータが表示されるというクレームが届いています。

あなたは運用担当者として原因を確認した上で解決策を選択してください。

- 1) DynamoDBのレプリケーションの設定を有効化する。
- 2) DynamoDBのDAXを有効化する。
- 3) DynamoDBのデータ整合性モデルを変更する
- 4) DynamoDBのクラスターを増強する。

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

テーブル設計

DynamoDBはテーブル単位から利用が開始され、テーブル→項目→属性と設計する

テーブル

DynamoDBはテーブルはデータのコレクションのこと。他のDBと同様にテーブル単位にデータを保存する

項目（アイテム）

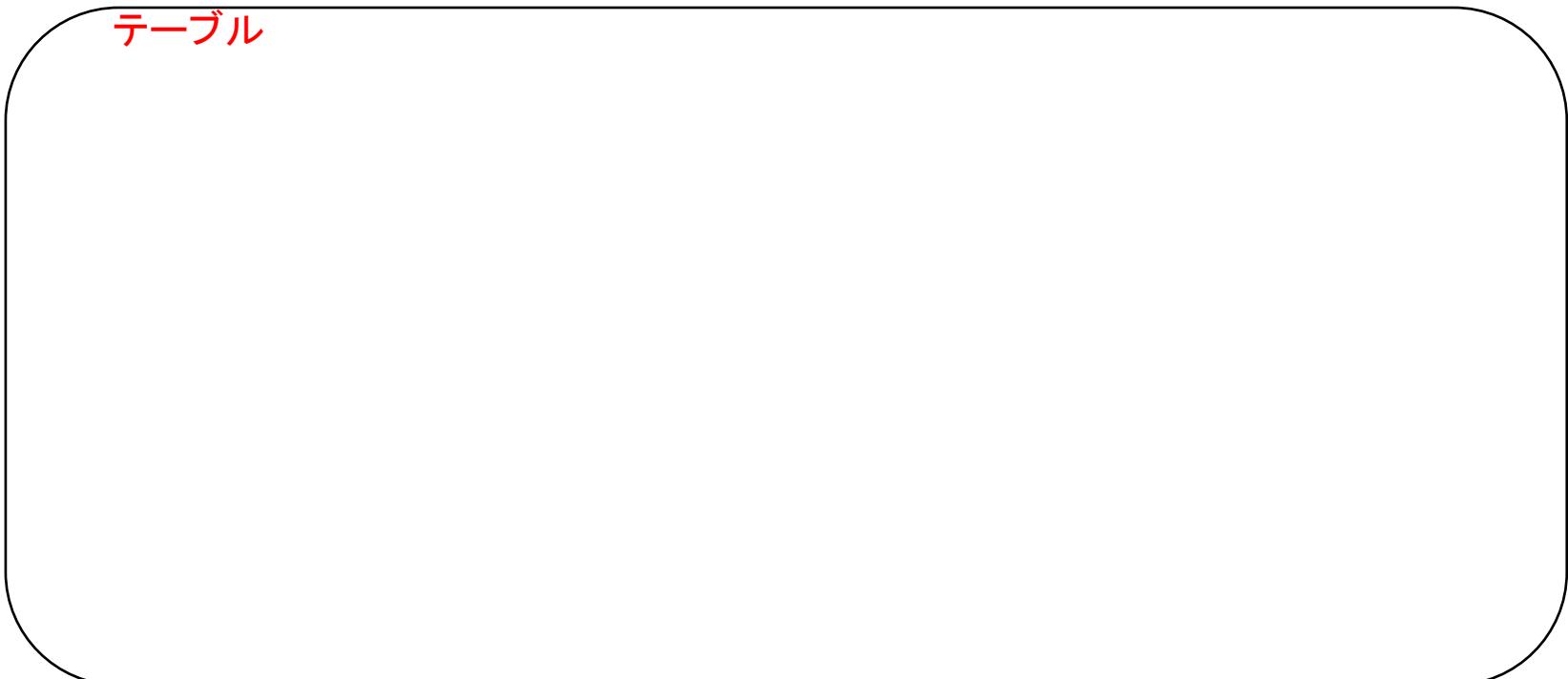
各テーブルの中に項目を作ってデータを作成する。項目間で一意に識別可能な属性グループとなる。Personalという項目を作成すれば、名前やIDなどが属性として付属する

属性

各項目は 1 つ以上の属性で構成される。属性はそれ以上分割する必要がない最小のデータ単位。例えばPersonal項目には、姓名といった名前の属性を設定する

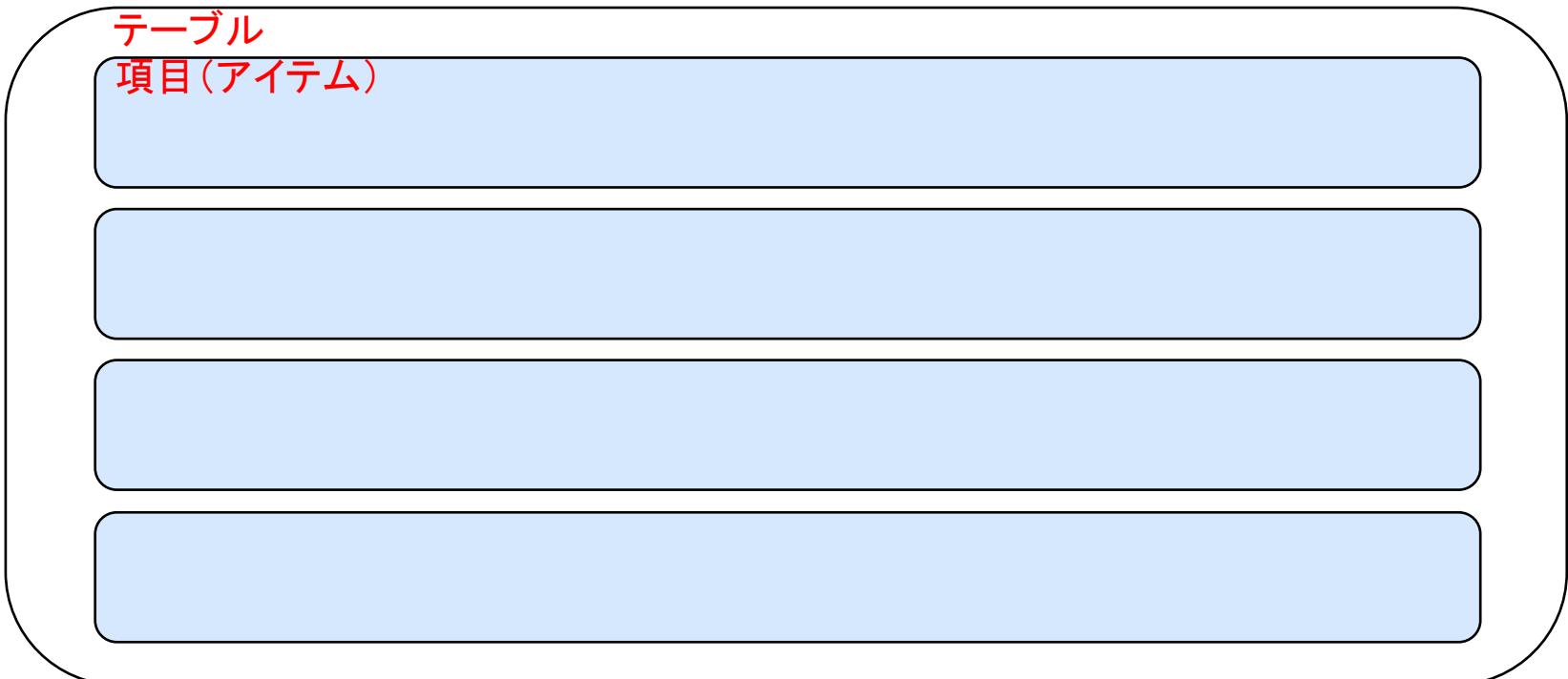
テーブル設計

テーブルと項目と属性の関係性を入れ子状にしてテーブルを設計する



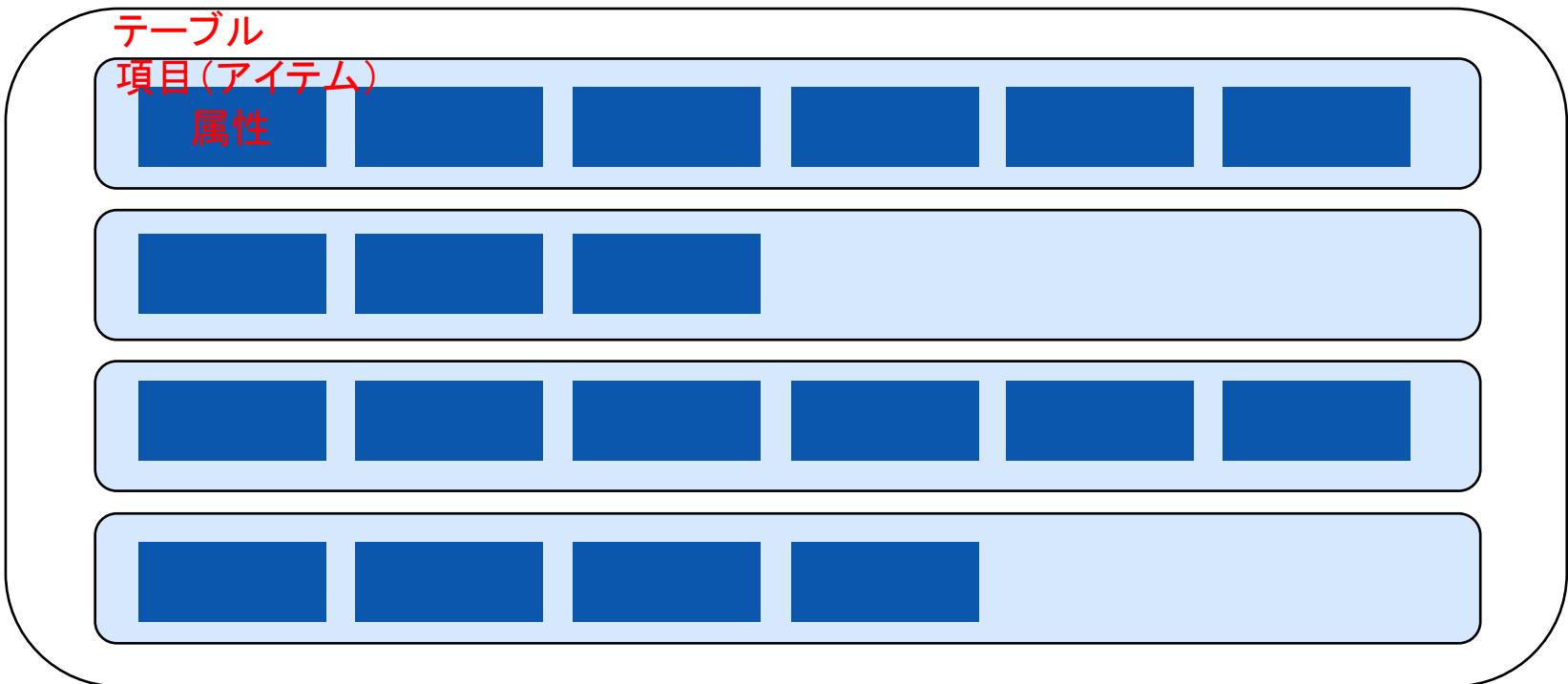
テーブル設計

テーブルと項目と属性の関係性を入れ子状にしてテーブルを設計する



テーブル設計

テーブルと項目と属性の関係性を入れ子状にしてテーブルを設計する



属性はVALUE型やJSON型など不ぞろいであっても構わない

[Q]キャパシティモードの設定

あなたの会社のアプリケーションはデータレイヤーにDynamoDBテーブルを構成して、CloudWatchアラームによってモニタリングを実施しています。このDynamoDBテーブルは、プロビジョニングキャパシティモードを使用して構成されています。本日、このDynamoDBテーブルの負荷が書き込みキャパシティに迫っているとのアラームが通知されました。

書き込みキャパシティが制限に達するとどうなりますか？

- 1) リクエストは抑制され、HTTP 503コードで失敗する。
- 2) リクエストは調整されて、HTTP 400コード（不正なリクエスト）と ProvisionedThroughputExceededExceptionで失敗します。
- 3) DynamoDBのキャパシティは自動的にスケーリングさえるため、リクエストは成功し、HTTP200ステータスコードが返される。
- 4) バーストループットモードとなり、リクエストは成功し、HTTP200ステータスコードが返される。

キャパシティモードの設定

利用するキャパシティが予測できるか否かでモードを選択

オンデマンドモード

- 利用するキャパシティが予測できないときに選択するモード
- トラフィック量の予測が困難な場合にリクエストの実績数に応じて課金
- オンデマンドでRead／Write処理に自動スケーリングを実施

プロビジョニング モード

- 利用するキャパシティが事前予測できるときに選択するモード
- 事前に予測した書き込みキャパシティユニット（WCU）と読み込みキャパシティユニット（RCU）を設定する。
- 設定したキャパシティに基づいて課金
- UpdateTable オペレーションを使用して、必要な回数だけ ReadCapacityUnits または WriteCapacityUnits を増やすことができる。
- キャパシティ容量に近づくとHTTP 400コード（不正なリクエスト）とProvisionedThroughputExceededExceptionが発せられる。

られる。

24時間ごとに1回、読み込み/書き込みキャパシティモードを切り替えることができる。

DynamoDBの料金

キャパシティ設定の方式と利用する機能に応じて課金される。

オンデマンド

- ストレージ容量（GB単位）
- 書き込み単位
- 読み込み単位

プロビジョンド

- ストレージ容量（GB単位）
- 読み込みキャパシティーユニット (RCU)
- 書き込みキャパシティーユニット (WCU)

その他

- グローバルテーブル：レプリケート書き込みキャパシティーユニット (rWCU)
- DynamoDB Accelerator (DAX)：ノード時間単位
- DynamoDB ストリーム：ストリーム読み込みリクエスト単位

インデックス

DynamoDBは暗黙的に設定するKVSにおけるKeyに値するものと、明示的に設定するキーがインデックスとして利用できる

暗黙的なキー

データを一意に特定するために暗黙的にキー（ハッシュキーやレンジキー）として宣言して検索に利用するインデックスで、1テーブルに1つ宣言する

明示的なキー

ローカル・セカンダリ・インデックス（LSI）はプライマリキーのタイプがハッシュキーやレンジキーの場合に追加で別のレンジキーを増やすように利用できる
1テーブルに5つ作成可能／テーブル作成時に作成

グローバル・セカンダリ・インデックス（GSI）は別のハッシュキーを設定することができる。全データに対してグローバルに検索を実施する。
1テーブルに5つ作成可能／テーブル作成後に作成

プライマリーキー

DynamoDBはハッシュキーとレンジキーという2種類のプライマリーキーを利用する

ハッシュキー

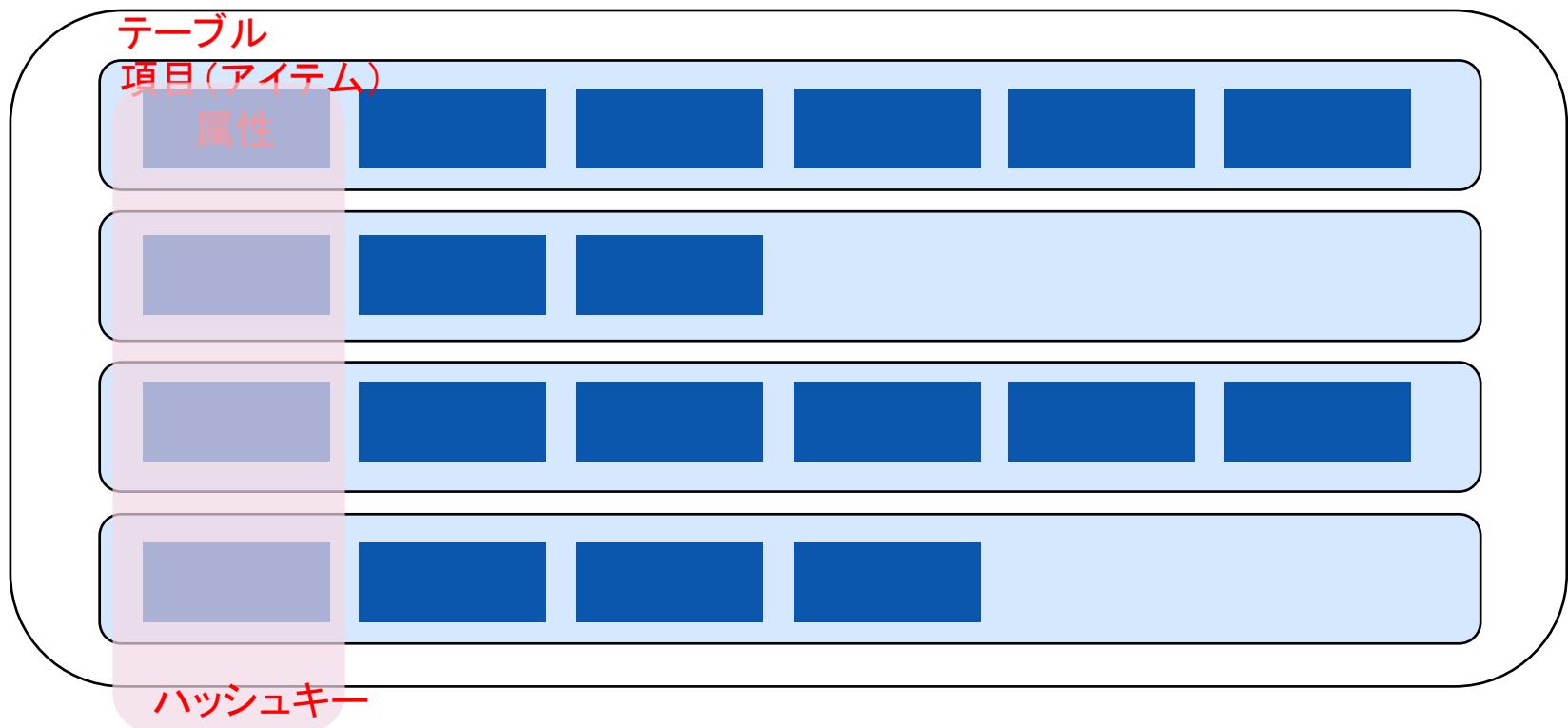
- KVSにおけるキーに相当するデータを一意に特定するためのIDなどのこと
- テーブル作成時に1つの属性を選び、ハッシュキーとして宣言
- ハッシュ関数によってパーティションを決定するためハッシュキーと呼ぶ
- ハッシュキーは単独での重複を許さない

レンジキー

- ハッシュキーにレンジを加えたものをレンジキーまたは複合キーと呼ぶ
- テーブル作成時に2つの属性を選び、1つをハッシュキーとして、もう一つをレンジキーと呼ばれるキーとして宣言
- 2つの値の組み合わせによって、1つの項目を特定
- 複合キーは、単独であれば重複が許される

プライマリーキー

テーブルと項目と属性の関係性を入れ子状にしてテーブルを設計する



プライマリーキー

テーブルと項目と属性の関係性を入れ子状にしてテーブルを設計する



セカンダリインデックス

ハッシュキーやレンジキーだけでは検索要件が満たせない場合にLSIとGSIを追加する。

Local Secondary Index (LSI)

- ソートキー以外にインデックスを作成できる検索方式。
- 複合キーテーブルにのみ設定可
- 複合キーによって整理されている項目に対して、パーティションキーを指定した上で、別の規則のインデックスとなりクエリ検索に利用できる。

Global Secondary Index (GSI)

- GSIはインデックス用に新たにパーティションキーとソートキーを指定する検索方式。
- ハッシュキーテーブル及び複合キーテーブルどちらにでも設定可能
- ハッシュキーの代わりになるため、ハッシュキーをまたいで物理パーティションに囚われない検索が可能

スループットやストレージ容量を追加で必要で書き込みも増大するため、多様すべきではない。

テーブル操作

テーブル操作としては以下のようなコマンドを利用する

.GetItem ハッシュキーを条件に一定の項目（アイテム）を取得	Query ハッシュキーとレンジキーにマッチする項目を取得（最大 1 MB）
PutItem 1件のアイテムを書き込む	Scan テーブルを全件検索する（最大 1 MB）
Update 1件のアイテムを更新	BatchGetitem 複数のプライマリーキーに対してマッチする項目を取得
Delete 1件のアイテムを削除	

[Q] DynamoDBストリーム

B社ではAWS上に構築されたアプリケーションを利用してC to Cの売買ソリューションを提供しています。現在、WEBセッションデータ、顧客情報、商品情報を利用して、顧客への最適な商品を recommendation する新機能を開発しています。顧客からの注文情報がテーブルの保存される度に、そのデータに対して前処理を実施して、recommendation用機能へとデータを引き渡す簡易なプログラム処理が必要です。

この要件を満たすことができる最適な組合せはどれでしょうか？

- 1) DynamoDB Streams + Lambda
- 2) DynamoDB DAX + API Gateway
- 3) Amazon SQS + Lambda
- 4) CloudWatch Events + Lambda

DynamoDBストリーム

DynamoDB テーブルに保存された項目の追加・変更・削除の発生時の履歴をキャプチャできる機能

データの保存

- 過去24時間以内のデータ変更の履歴を保存し、24時間を経過すると消去される
- データ容量はマネージド型で自動的に管理

データ保存の順番

- 操作が実施された順番に応じてデータはシリアル化される
- 特定のハッシュキーに基づいた変更は正しい順番で保存されるが、ハッシュキーが異なる場合は受信した順番が前後される可能性がある

DynamoDBストリームのユースケース

データ更新をトリガーとして処理を実行するアプリケーション機能や、DynamoDBテーブルのレプリケーションに活用できる

クロスリージョンレプリケーション

- ストリームによるキャプションをトリガーとしてクロスリージョンレプリケーションを実施することが可能

データ更新をトリガーとしたアプリケーション機能

- データ更新に応じた通知処理などのアプリケーション処理の実行 など

DynamoDBストリームのユースケース

DynamoDBの書き込み処理をトリガーにしてLambda関数によってさまざまな処理を自動化する



[Q]スケーリング

B社ではAWS上に構築されたアプリケーションを利用してC to Cの売買ソリューションを提供しており、セッションデータ処理にはプロビジョニングモードのAmazon DynamoDBテーブルを利用してます。Amazon DynamoDBテーブルの負荷変動が激しく、ある日は頻繁に使用されますが、ほとんど利用されない日もあります。プロビジョニングされたスループット容量は、スロットルが発生しないように、重い負荷を考慮して構成されており、コスト効率が悪いことが問題となっています。

コストを最適化するための最も効率的なソリューションは何でしょうか？

- 1) DynamoDBオートスケーリングポリシーを使用する。
- 2) プロビジョニングされたスループット数を削減する。
- 3) DynamoDBテーブルのキャパシティに基づいてCloudWatchアラームを作成し、アラームに基づいてLambda関数により、 WCUとRCUを自動調整する。
- 4) DynamoDB DAXを使用してデータベースのパフォーマンスを向上させる

DynamoDB Auto Scaling

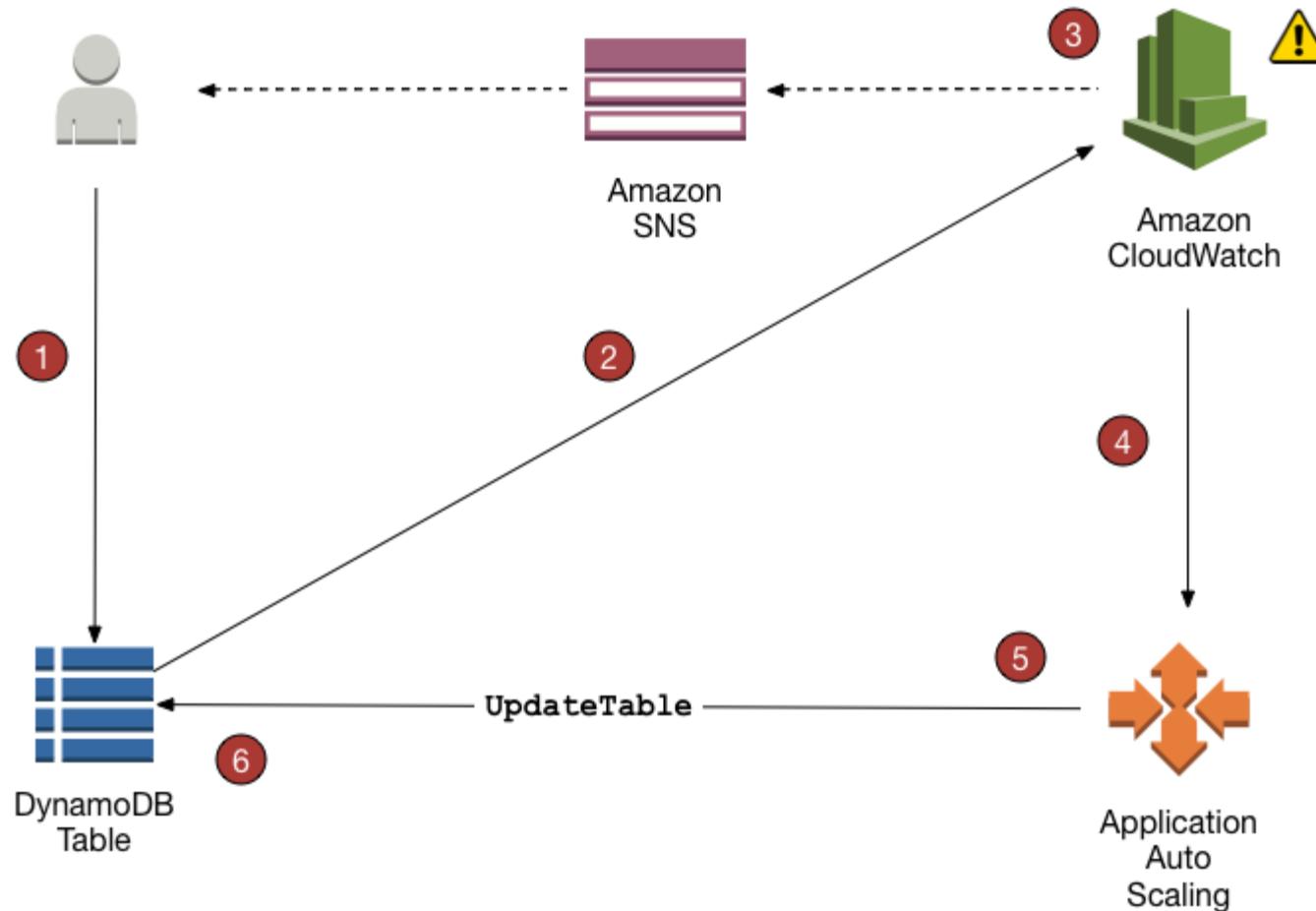
スケーリングポリシーに基づいてテーブルまたはGSIを自動でスケーリングする。

DynamoDB Auto Scaling

- AWS Application Auto Scaling サービスを使用して Application Auto Scaling ポリシーを設定する。
- CloudWatchのモニタリングに基づいてトラフィックパターンに応じてプロビジョンドスループット性能をユーザーに代わって動的に調節する。
- テーブルまたは グローバルセカンダリインデックスはプロビジョニングされた読み込みおよび書き込みキャパシティーを増やし、急激なトラフィック増加をスロットリングなしに処理できる。
- DynamoDB テーブルを作成すると、Auto Scaling がデフォルトで有効化されている。

DynamoDBのスケーリング

スケーリングポリシーに基づいてテーブルまたはGSIを自動でスケーリングする。



[Q] DAX

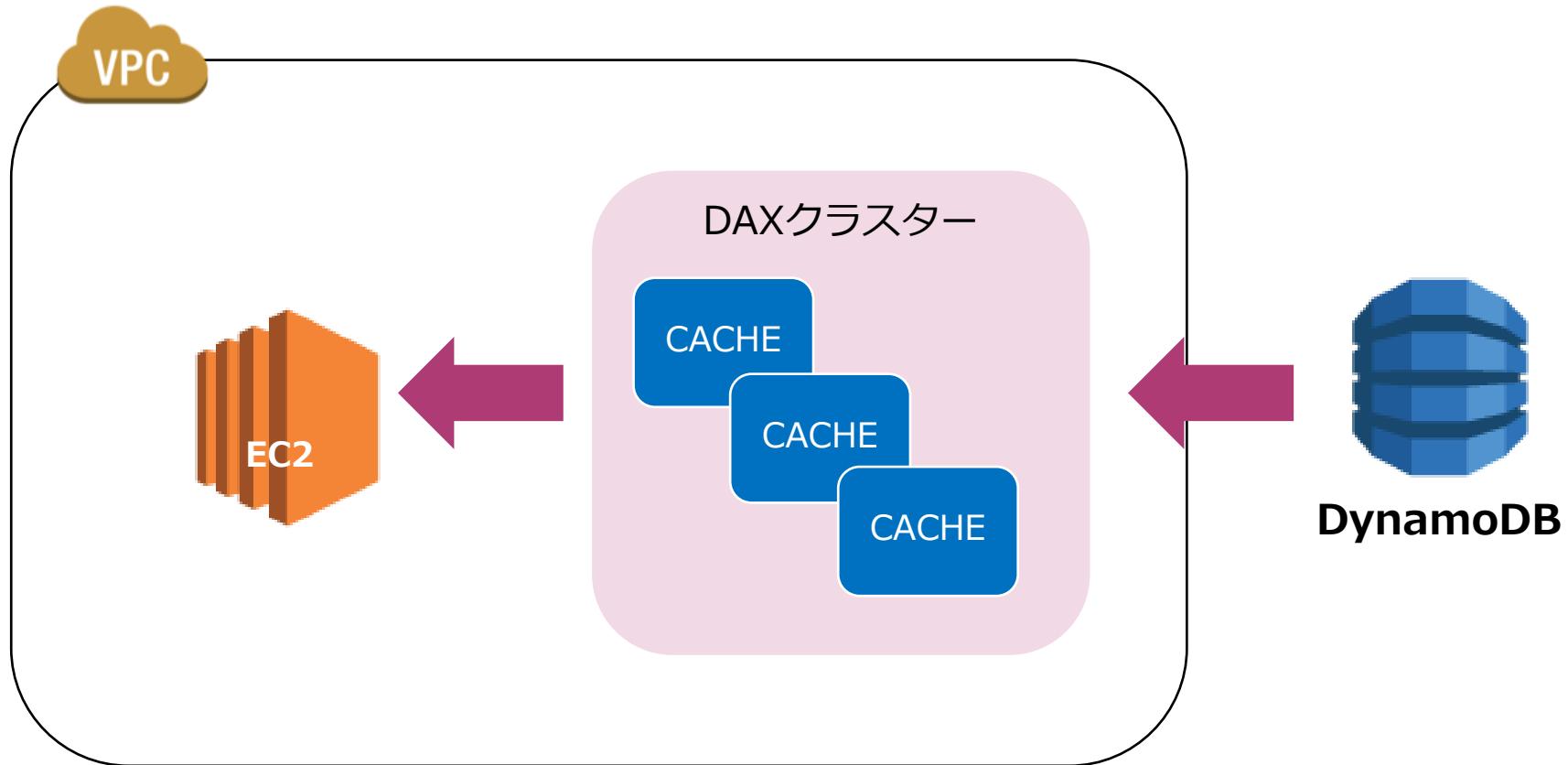
B社ではAWS上に構築されたアプリケーションを利用してC to Cの売買ソリューションを提供しており、セッションデータ処理にはプロビジョニングモードのDynamoDBテーブルを利用しています。最近になって、アプリケーションのリクエスト数が急増しており、あなたは担当のソリューションアーキテクトとして、DynamoDBのRCUを増やしました。それでも、ホットキーでホットパーティションの問題が発生しています。

このホットキーの問題を解消するにはどうすればよいですか？

- 1) DynamoDB グローバルテーブルを利用する。
- 2) DynamoDB Streamsを利用する。
- 3) DynamoDB Accelerator (DAX)を利用する。
- 4) DynamoDBのGSIを利用する。

DynamoDB Accelerator (DAX)

DAXはDynamoDBにインメモリキャッシュ型の機能を付加する



DynamoDB Accelerator (DAX)

DynamoDBにおいて高速なインメモリパフォーマンスを可能に

- インメモリキャッシュとして 1桁台のミリ秒単位からマイクロ秒単位まで結果整合性のある読み込みワークロードの応答時間を短縮。マルチAZ DAXクラスターは、1秒間に数百万件のリクエストを処理できる。
- DAXはDynamoDBを使用するAPIと互換性を持つマネージド型サービスであり、運用上そしてアプリケーションの複雑性を減少させて容易に導入可能
- 読み取りの多いワークロードや急激に増大するワークロードに対して、DAXはスループットを強化したり、読み込みキャパシティユニットを必要以上にプロビジョニングしないよう設計することで運用コストの節約できる

[Q]グローバルテーブル

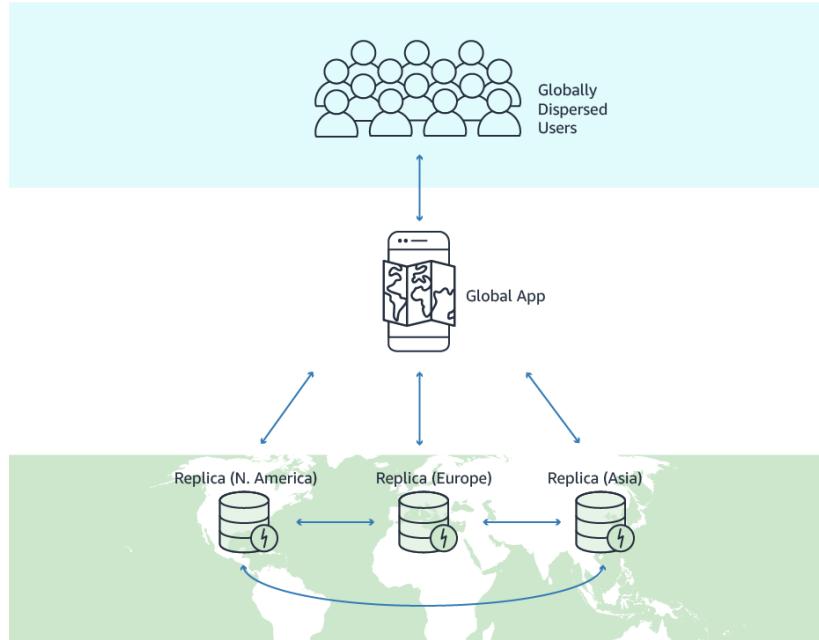
B社はAWS上に構築されたアプリケーションを利用してC to Cの売買ソリューションを提供しており、セッションデータ処理にはプロビジョニングモードのDynamoDBテーブルを利用しています。同社は、アクティブ-アクティブ構成の3つの異なるAWSリージョンにアプリケーションをデプロイしたいと考えています。情報の同期を維持するには、データベースを複製する必要があります。

これらの要件に最適なデータベースソリューションはどれですか？

- 1) グローバルテーブルを備えたAmazon DynamoDB
- 2) ElastiCacheのグローバルレイヤー
- 3) AmazonS3クロスリージョンレプリケーション
- 4) Amazon Auroraのグローバル構成されたマルチマスター構成

グローバルテーブル

リージョン間で同期されるマルチマスター作成可能



- DynamoDBの性能のまま、世界中で複数のリージョンにエンドポイントを持つことができる
- 読み書きのキャパシティに加えて、クロスリージョンレプリケーションのデータ転送料金に課金される。
- オプションで実施できた強い整合性は使用できない。

オンデマンドバックアップ

パフォーマンスに影響なく数百TBのバックアップを実行可能

- 任意のタイミングで利用可能な長期間データ保存用バックアップ
- 従来はデータパイプラインを利用して取得したバックアップを容易に実施できるようになった。

Lambdaの出題範囲

Lambdaとは何か？

サーバーを起動せずにプログラミングコードを実行する仕組み。
簡易なアプリケーション処理を構築することができる。



Lambdaとは何か？

サーバーを起動せずにプログラミングコードを実行する仕組み。簡易なアプリケーション処理を構築することができる。



Lambdaの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

Lambdaの特徴	✓ Lambdaが利用できるプログラミング言語など、その特徴に関する質問が出題される。
Lambdaの制限	✓ Lambdaの利用する上での制限設定に関する質問が出題される。
Lambdaの処理タイミング	✓ Lambdaが処理されるタイミングとして、同期処理と非同期処理の設定内容が問われる。
LambdaとVPC	✓ LambdaがVPC内のリソースにアクセスして処理を実行するための設定方法が問われる。
Lambdaレイヤー	✓ Lambdaレイヤーの利用目的が問われる。

Lambdaの出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

Lambdaの構成	✓ シナリオに基づいて要件が提示されて、それを実現するためのLambdaを利用したアーキテクチャの設計方法が問われる。
API Gatewayとの連携	✓ API Gatewayから、APIコールに基づいてLambda関数を動作させる場合のアーキテクチャ方式が問われる。
Lambdaエッジ	✓ CloudFrontと連携したLambda関数の実行方法が問われます。
RDSとの連携	✓ Lambdaを利用してRDSのデータベース処理を実施する際に、RDSプロキシを利用する構成が問われる。

[Q] Lambdaの特徴

B社はIoTソリューションを提供しているIT企業です。現在、サーバレスアプリケーションによってストリーミングデータを処理する仕組みを計画しています。Lambda関数を利用する予定ですが、Lambda関数の実装ができるプログラマーを選定しているところです。この選定のためにはLambda関数で利用可能なプログラミング言語を確認することが必要です。

Lambdaランタイムでサポートされているプログラミング言語はどれでしょうか？
(2つ選択してください)

- 1) C#
- 2) .NET
- 3) Go
- 4) PHP
- 5) C++

Lambdaの特徴

Lambda関数は様々なコードを利用可能で、AWS側で実行環境が管理されている。

- 実行基盤は全てAWS側で管理されているマネージド型サービス
- AWSサービスと連携させることでLambda関数（ファンクション）と呼ばれる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
- **Java、Go、PowerShell、Node.js、C#、Python、Ruby** のランタイムをサポート

【関数の内容】

- コード

関数のコードと依存関係を作る。スクリプト言語の場合は、組み込みエディタで関数コードを編集が可能。ライブラリを追加するには、またはエディタでサポートされていない言語の場合は、デプロイパッケージをアップロードする。デプロイパッケージのサイズが 50 MB を超える場合はS3からアップロードする。
- ランタイム - 関数を実行する Lambda ランタイムのこと
- ハンドラー - 関数の呼び出し時にランタイムで実行されるメソッド

Lambdaの課金

Lambdaはリクエスト数とコードの実行期間で算出されて課金される。

- コード実行時間に対しての課金されるため、サーバーを保持して処理コードを実行するよりもコスト効率が非常に高い。
- リクエストの数とコードの実行時間に基づいて課金
- 実行時間はコードの実行が開始された瞬間から処理が返されるか、中止されるまでの時間で計算される。値は100 ミリ秒単位で切り上げられます。
- 1 か月ごとに 100 万件の無料リクエスト、および 40 万 GB-秒のコンピューティング時間が無料枠になっている。

[Q] Lambdaの制限

あなたはソリューションアーキテクトとして、AWS Lambdaを使用して、バッチジョブのワークロードを実装しています。このLambda関数は、Amazon S3からデータを取得して処理した上で、処理結果をDynamoDBに保存します。しかしながら、このLambda関数を実行すると、15分後にLambda関数にエラーが発生していました。

この問題の根本原因として最も可能性が高い要因はどれでしょうか？

- 1) Lambda関数には非同期処理が設定されている。
- 2) Lambda関数のメモリが不足している。
- 3) Lambda関数の同時実行数が上限に達している。
- 4) Lambda関数の実行時間を超過している。

Lambdaの制限

Lambda関数は効率的な処理を可能にするために、データ量や実行時間や同時実行数に制限がある。

- 関数のタイムアウト時間は**デフォルト値は3秒で、許容されている最大値は900秒（15分）**。タイムアウトに達すると、関数が停止される。
- 関数の最大同時実行数はデフォルトは100を最大は1000（申請によって数十万まで引き上げ可能）
- 関数の実行時に使用できるメモリの量。メモリの量を 128 MB ~ 3,008 MB の範囲
- /tmp ディレクトリのストレージの保存可能容量は512MB
- Lambdaレイヤーを最大5つまで設定可能

https://docs.aws.amazon.com/ja_jp/lambda/latest/dg/configuration-console.html
https://docs.aws.amazon.com/ja_jp/lambda/latest/dg/gettingstarted-limits.html

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)

Lambdaを呼び出す

Lambdaの実装：ブループリント

Lambdaファンクションをコーディングする際にサンプルコード集を利用することが可能

Lambdaを利用する
ユースケース
を設計

ブループリントに
てサンプルコード
を探す

サンプルコードを
修正してファンク
ションを作成する

[Q] Lambdaの処理タイミング

会社ではAWS Lambdaを使用して、データ処理アプリケーションのワークフローを実装しています。IoTデータをLambda関数が取得して、処理結果をAmazonS3に保存します。アプリケーションはデータ処理が成功したことをユーザーに通知するプロンプトを返します。通常、処理全体が完了するまでに約10分かかります。あなたはソリューションアーキテクトとして、このワークフローを非同期処理にするためにリファクタリングをするように依頼されました。

次のオプションの中で、Kinesis、S3に非同期で処理するために最適なソリューションを選択してください（2つ選択してください。）

- 1) Kinesisストリームを利用してLambda関数にデータを引き渡す。
- 2) Amazon SQSキューを利用してLambda関数にデータを引き渡す。
- 3) リクエストを非同期的に処理するLambda関数を作成する。
- 4) Lambda関数に実行スケジュールを設定して、非同期処理を行う。
- 5) DynamoDBストリームを利用してLambda関数にデータを引き渡す。

Lambdaの処理タイミング

他のAWSサービスやSDKを利用したアプリケーションからの呼び出して実行することが可能

非同期呼び出し

- 関数を非同期的に呼び出してイベントを処理する。
- 関数を非同期的に呼び出す場合は、関数コードからのレスポンスを待機しない。

同期呼び出し

- 関数を同期的に呼び出すと、Lambdaが関数を実行し、レスポンスを待つ。
- 実行完了時に、実行された関数のバージョンなどの追加データとともに、Lambda関数内でセットしたレスポンスが返ってくる

スケジュール機能

特定時刻をトリガーにしてLambdaファンクションを実行する

特定時刻に毎回ファンクション
を実行したい処理

Lambdaが定期的に実行

[Q] LambdaとVPC

ソリューションアーキテクトは、AWS Lambda関数を使用するコードを作成しています。Lambda関数は実行されるとElastiCacheクラスターにストリーミングデータを格納します。ElastiCacheは同じアカウントのVPC内に設置されているため、Lambda関数にはVPC内のリソースにアクセスする設定が必要です。

Lambda関数には必要なVPC固有の情報はどれでしょうか？（2つ選択してください）

- 1) VPCサブネットID
- 2) VPCセキュリティグループID
- 3) VPCのARN
- 4) VPC論理ID
- 5) VPCルートテーブルID

VPCアクセス

インターネットを経由せずにVPC内のAWSリソースへとアクセス可能になる

VPC内のリソースへのアクセス

- VPC内リソースにインターネットを経由せずにアクセスが可能
- VPCを指定する際にサブネットIDとVPCセキュリティグループIDを指定して、ENIを作成する。ENI経由で接続
- ENIには指定したサブネットのIPがDHCPで動的に割り当てられる

アクセス設定

- ファンクションに割り当てるIAM Roleに"AWSLambdaVPCAccessExecutionRole"というポリシーをアタッチしておくこと

[Q] Lambdaレイヤー

あなたはサーバレス構成を利用したアプリケーションでコスト最適化を目指しています。Lambda関数を利用したアプリケーションを複数実行していますが、その処理の一部分が重複していることがわかりました。

このLambda関数処理を改善するために必要な方法を選択してください。

- 1) Lambdaエッジ
- 2) Lambda Layer
- 3) Invocation
- 4) API Gatewayキャッシュ

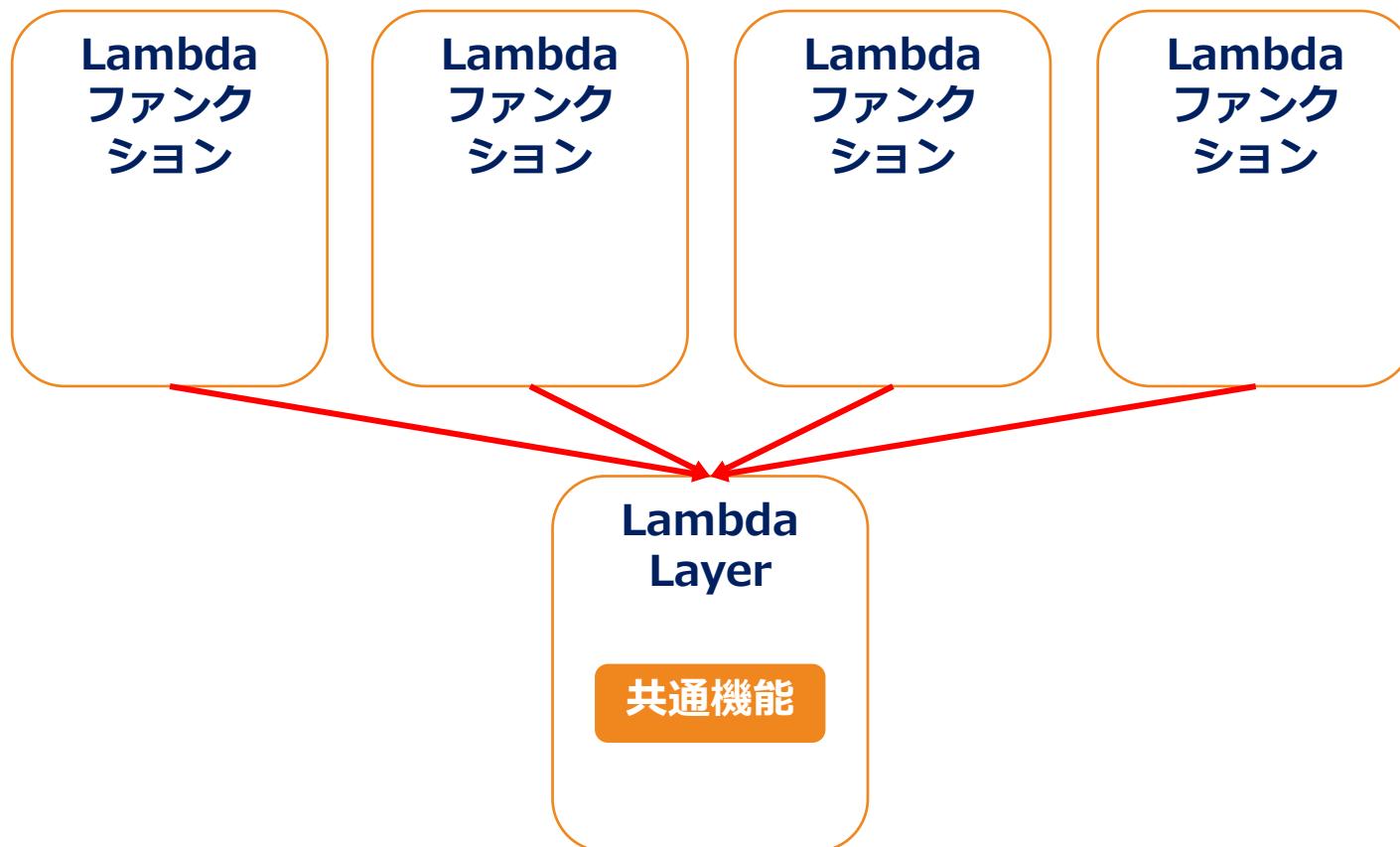
Lambdaレイヤー

Lambdaファンクション間で共通するコンポーネントをLambda Layerとして定義し参照できる（5つまで）



Lambdaレイヤー

Lambdaファンクション間で共通するコンポーネントをLambda Layerとして定義し参照できる（5つまで）



[Q] Lambdaの構成

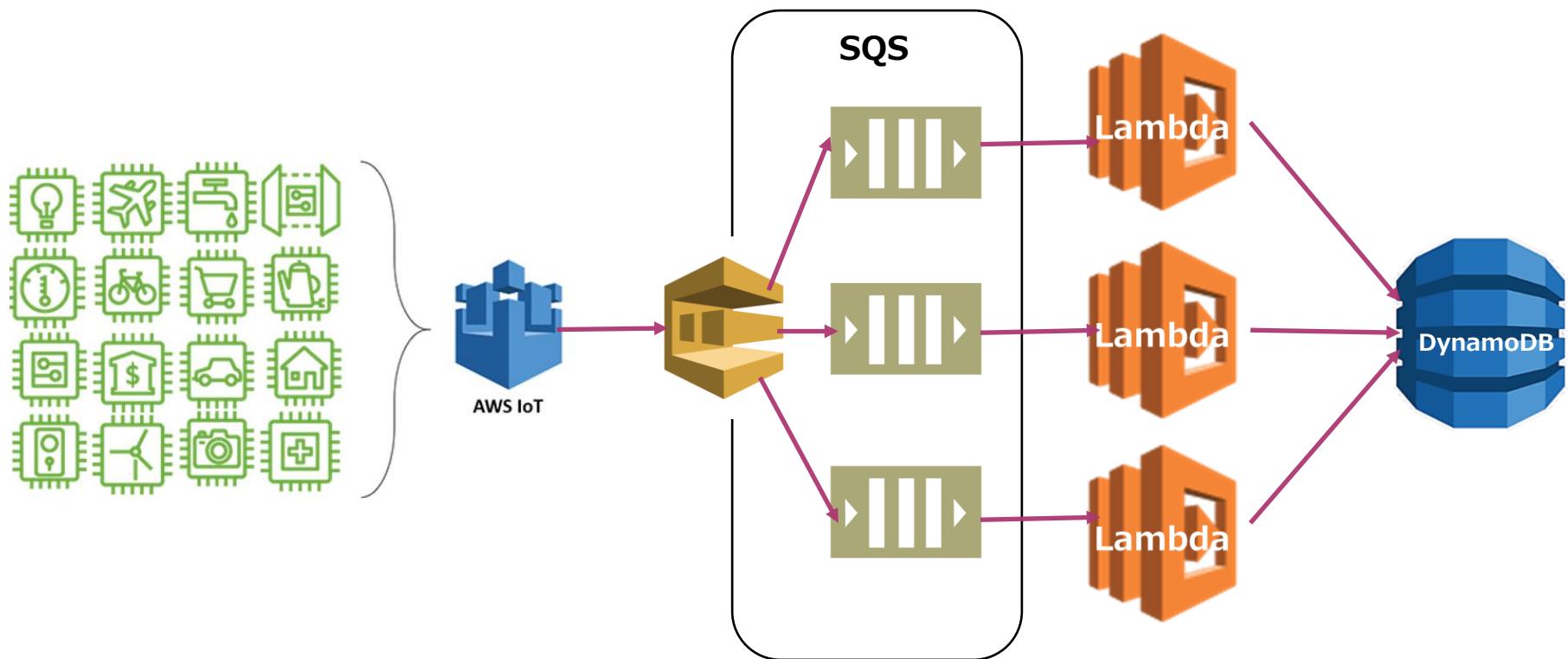
自動車メーカーはAWS上に自動車に設置されたセンサーデータを取得して、データを加工した上で、 DynamoDBに格納するデータ処理アプリケーションのワークフローを実装しています。アプリケーションはデータの保存が成功したことをユーザーに通知を返す必要があります。これらのイベント処理は自動で実行されることが必要です。

この要件を満たすことができるLambda関数の実装方法を選択してください（2つ選択してください。）

- 1) センサーデータをAmazon SQS FIFOキューに取り込み、 Lambda関数によって処理した上で、 DynamoDBテーブルに書き込む。
- 2) センサーデータをKinesis Data Streamsに取り込み、 Lambda関数によって処理した上で、 DynamoDBテーブルに書き込む。
- 3) センサーデータをAmazon SQS 標準キューに取り込み、 Lambda関数によって処理した上で、 DynamoDBテーブルに書き込む。
- 4) DynamoDBストリームによってデータ格納に基づいてSNS通知を実行する。
- 5) DynamoDBストリームによってデータ格納に基づいて別のLambda関数が通知を実行する。

Lambdaユースケース

SQSとLambdaを組み合わせてIoTセンサーデータを
DynamoDBに格納する処理プログラムを作ることが可能



Lambdaの連携

様々なAWSサービスをトリガーとして起動するなどの連携処理が可能

- Amazon S3
- Amazon Kinesis
- Amazon DynamoDB Streams
- Amazon Cognito(Sync)
- Amazon SNS
- Amazon SQS
- Alexa Skills Kit
- Amazon SWF

[Q] API Gatewayとの連携

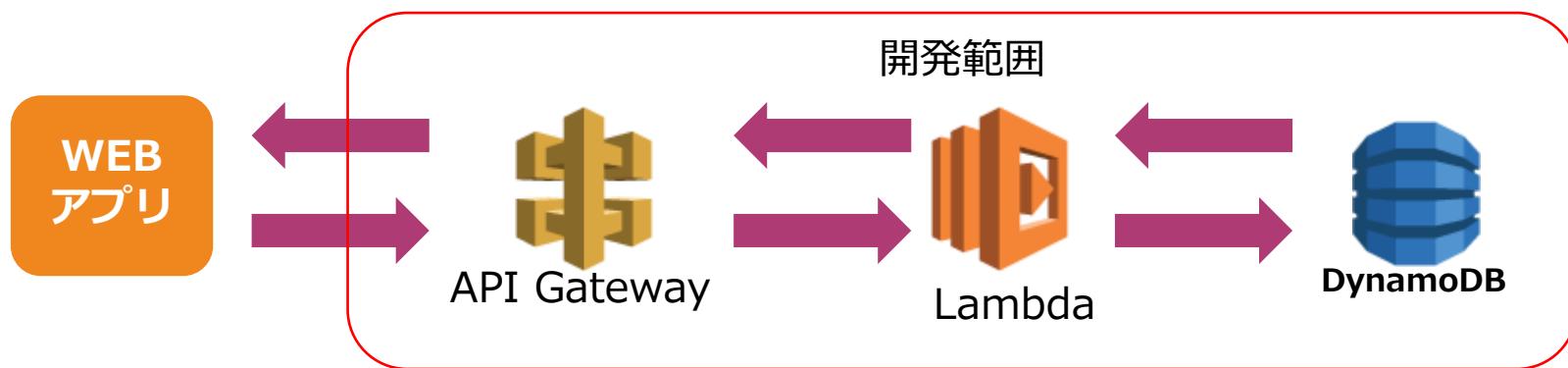
予測できないワークロードをサポートするために拡張性がある新しいWebアプリケーションを開発しています。このアプリケーションは、外部からのHTTPSコールに応じて実行されるシンプルなワークロードを実行します。

このユースケースに最も適したソリューションはどれですか？

- 1) API GatewayとLambda
- 2) Auto ScalingグループとEC2
- 3) CloudFrontとLambda
- 4) API GatewayとEC2

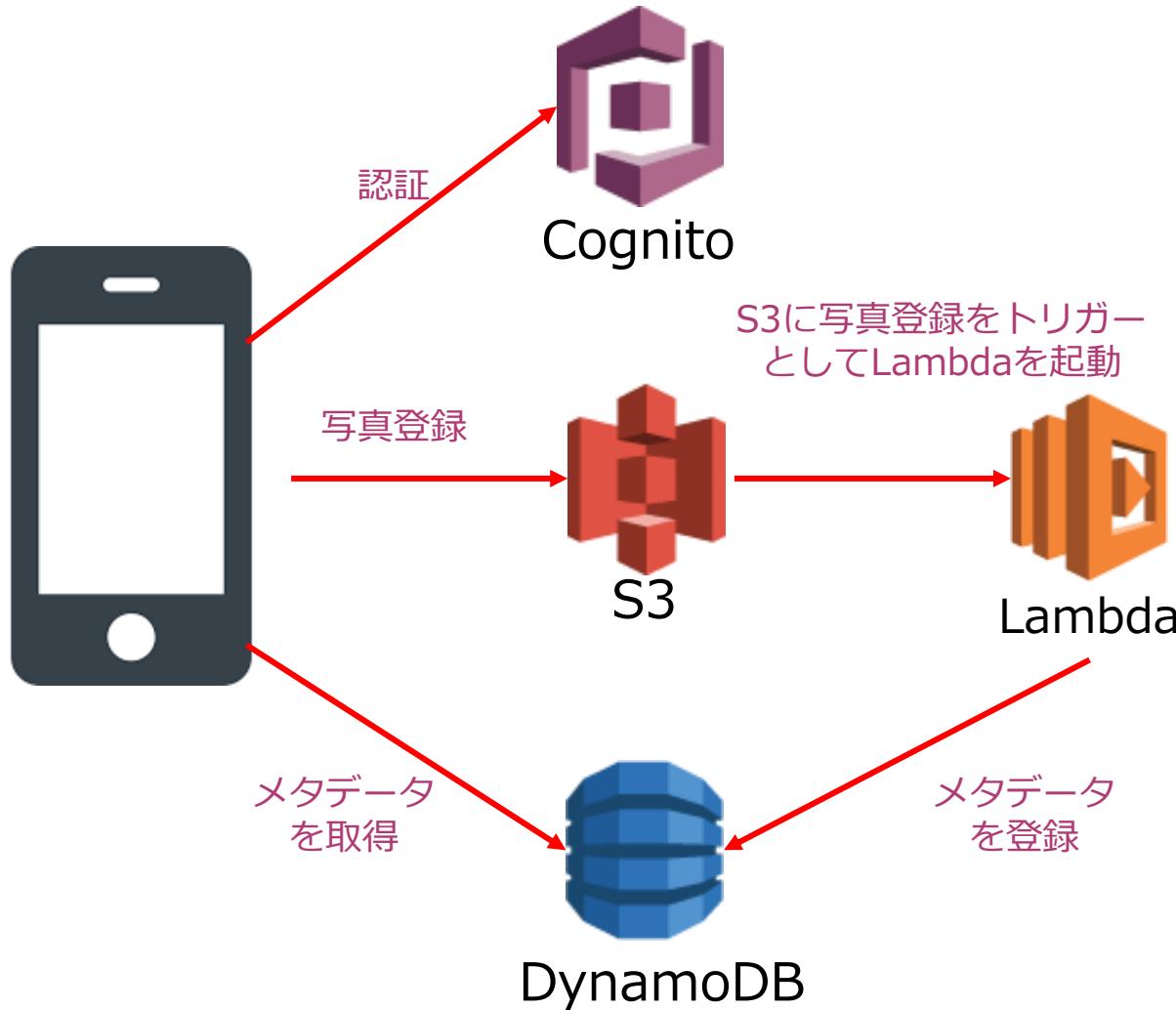
API Gatewayとの連携

API Gatewayと統合することで、Lambda関数をAPIから実行することができる。



Lambdaモバイルアプリ

モバイルからの写真管理をLambdaを通して実施するなどモバイル連携も容易



[Q] Lambdaエッジ

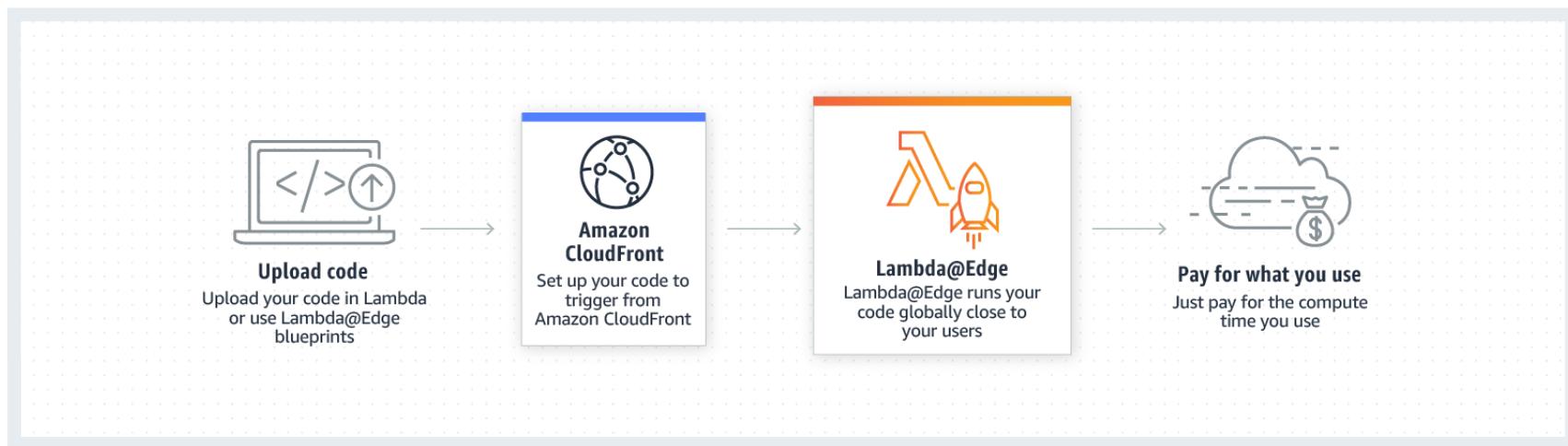
大手ニュースサイトはCloudFrontのWEBディストリビューションを使用して、静的コンテンツを世界中のユーザーに提供しています。URIに対応したHTMLファイルが存在しないため、ブラウザリロード時などのリクエストがエラーになってしまうことがあります。その際に、403／404などのエラーページをindex.htmlにリダイレクトすることでこの問題を回避する設定が必要です。

この要件を満たすことができるソリューションを選択してください。

- 1) リージョナルエッジキャッシュを利用して、レスポンスをリダイレクトする。
- 2) ローカリゼーションを利用して、レスポンスをリダイレクトする。
- 3) CloudFrontのリダイレクト設定を有効化する。
- 4) Lambda @ Edgeを使用して、CloudFront Webディストリビューションがユーザーに配信するコンテンツをカスタマイズする。

Lambdaエッジ

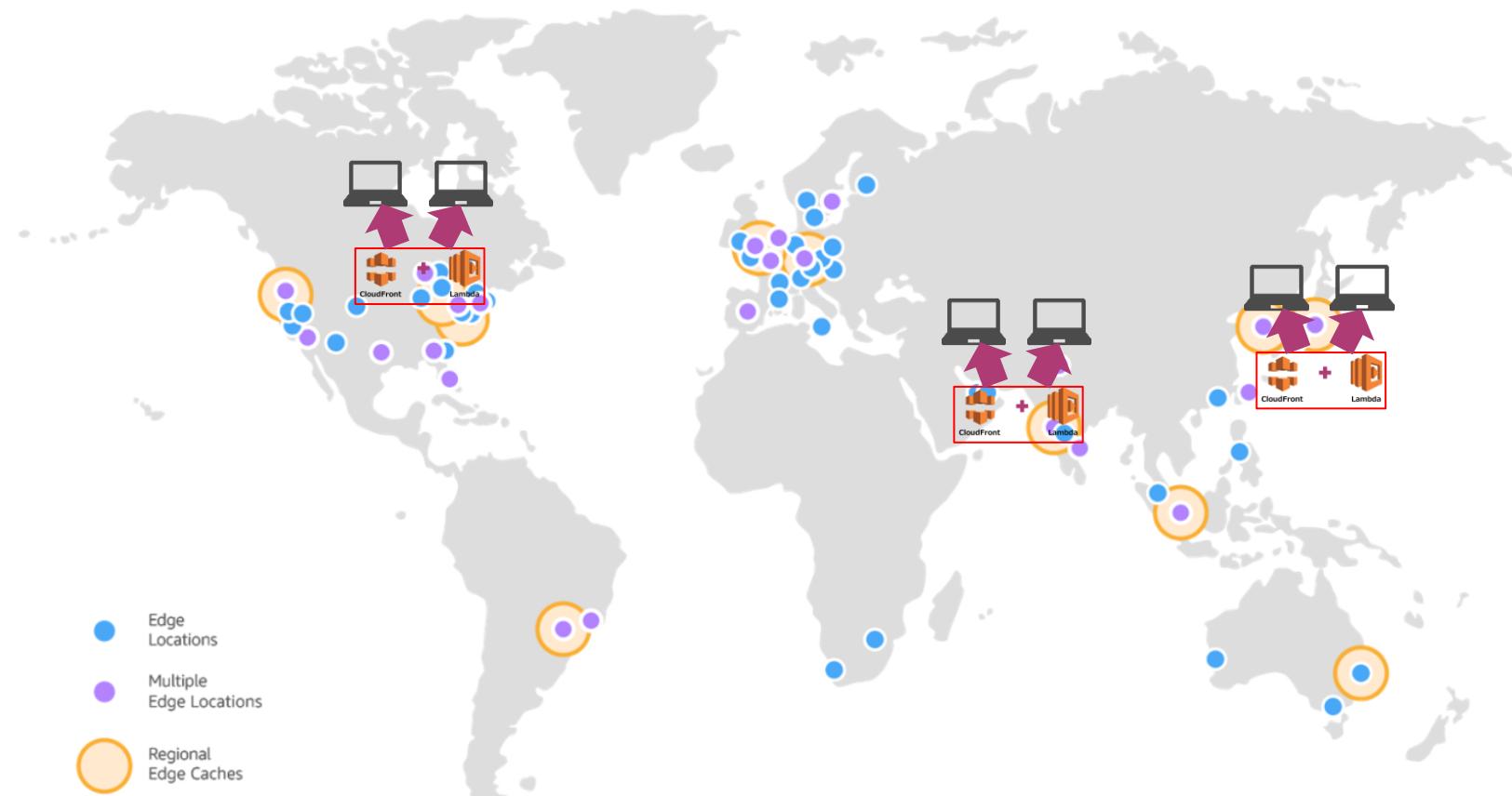
CloudFrontの配信コンテンツをLambda関数によってエッジロケーションで処理することが可能



Reference: <https://aws.amazon.com/jp/lambda/edge/>

Lambdaエッジ

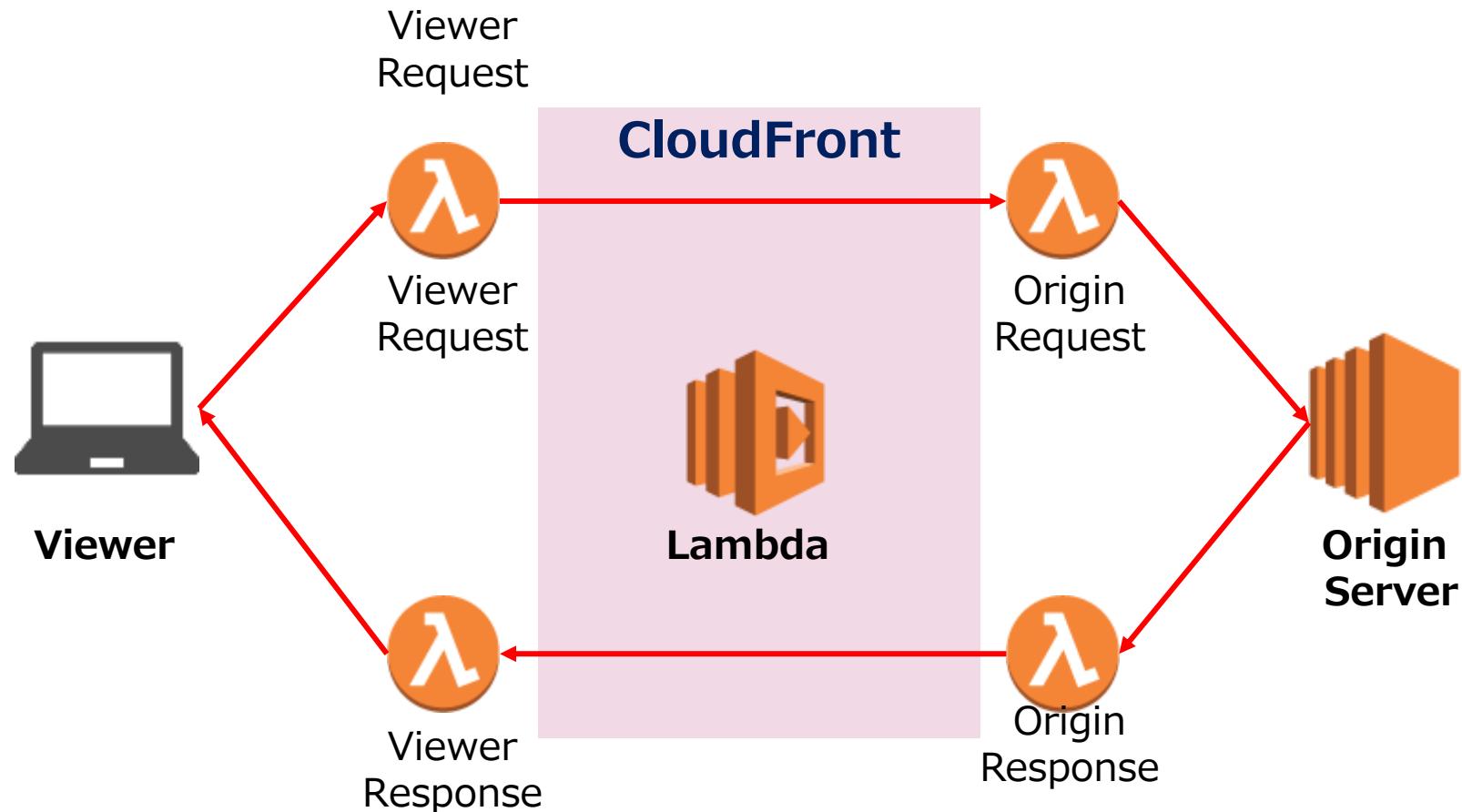
CloudFrontにLambda機能を連携することで、世界中でユーザーに近いロケーションにおいてコードを実行できる



参照 : <https://aws.amazon.com/jp/cloudfront/features/?nc=sn&loc=2>

Lambdaエッジ

イベントに関連付けられてLambdaファンクションがエッジロケーションで実行されて実行結果を返答する



[Q] RDSとの連携

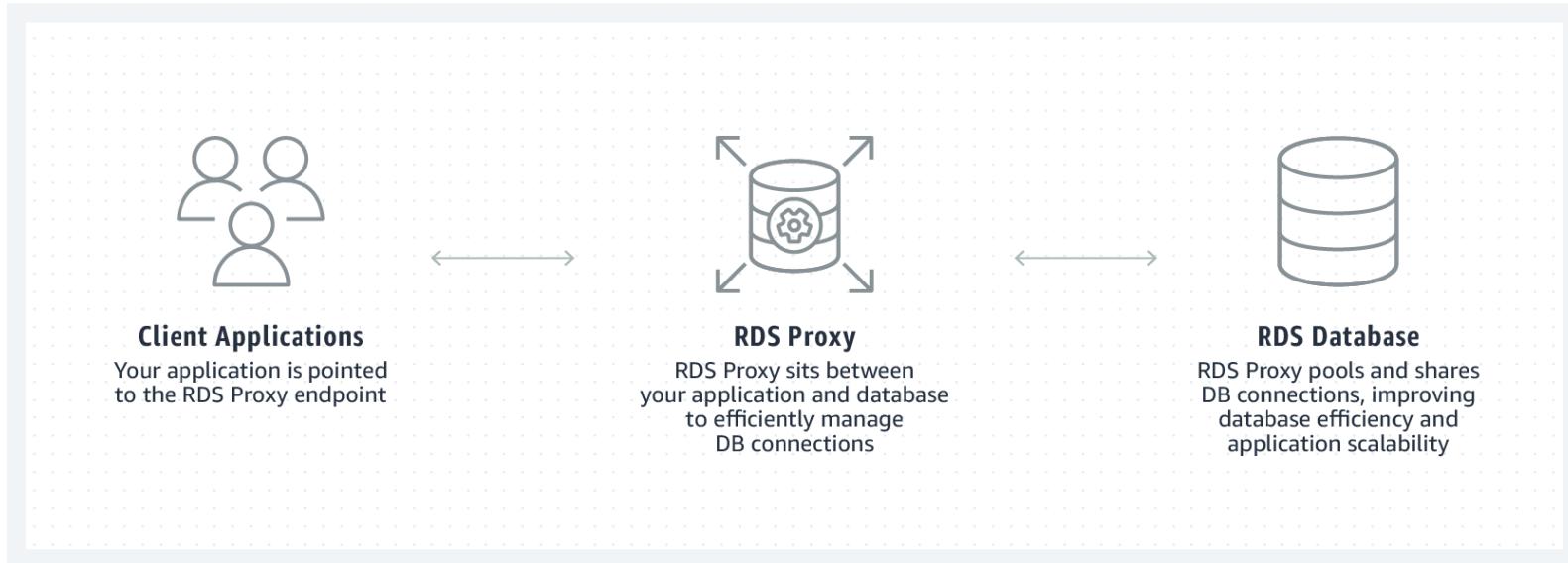
あなたはソリューションアーキテクトとして、RDSからデータを取得して、そのデータを加工した上でDynamoDBに処理結果を登録する仕組みを構築しています。Lambda関数を利用してデータベースにアクセスして、データを処理する仕組みを利用することにしました。

この要件を満たす方法を選択してください。 (2つ選択してください。)

- 1) Lambda関数でDynamoDBストリームを利用する。
- 2) Lambda関数でRDSプロキシを利用する。
- 3) Lambda関数でRDSエンドポイントを利用する。
- 4) RDSのパブリックアクセスを有効化することでLambda関数をRDSと接続する。

RDSプロキシ

Lambdaを利用してRDSのデータベースに接続する際は、RDSプロキシをエンドポイントの代わりに利用して、接続することでコネクションを効率的に実行することができる。



Route53の出題範囲

Route53とは何か？

IPアドレスを人が読みやすいURLに変換して、住所として利用できるようにしてくれるDNSサーバーの役割を提供



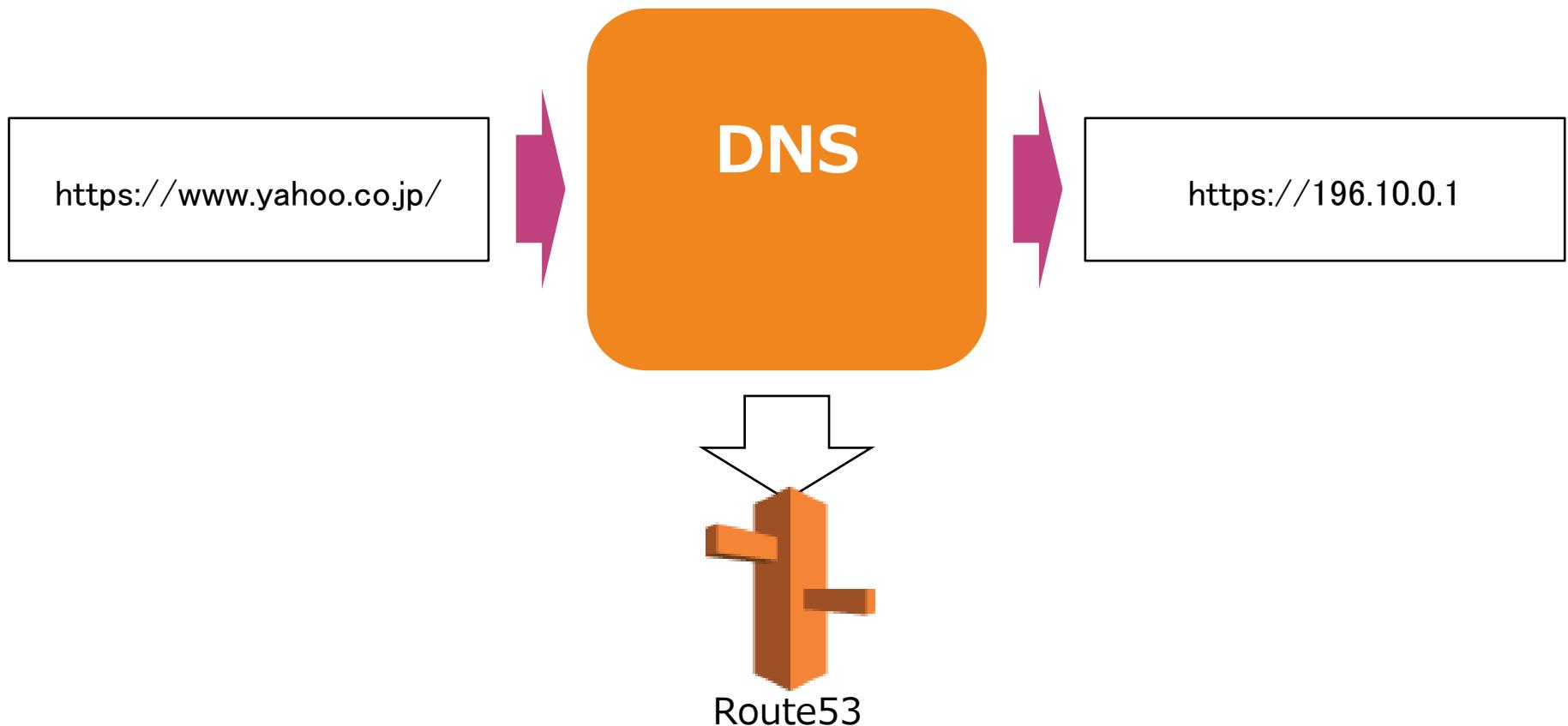
Route53とは何か？

DNSはインターネットにおける人向けのURLをシステム向けの住所となるIPアドレスに変換するための仕組み



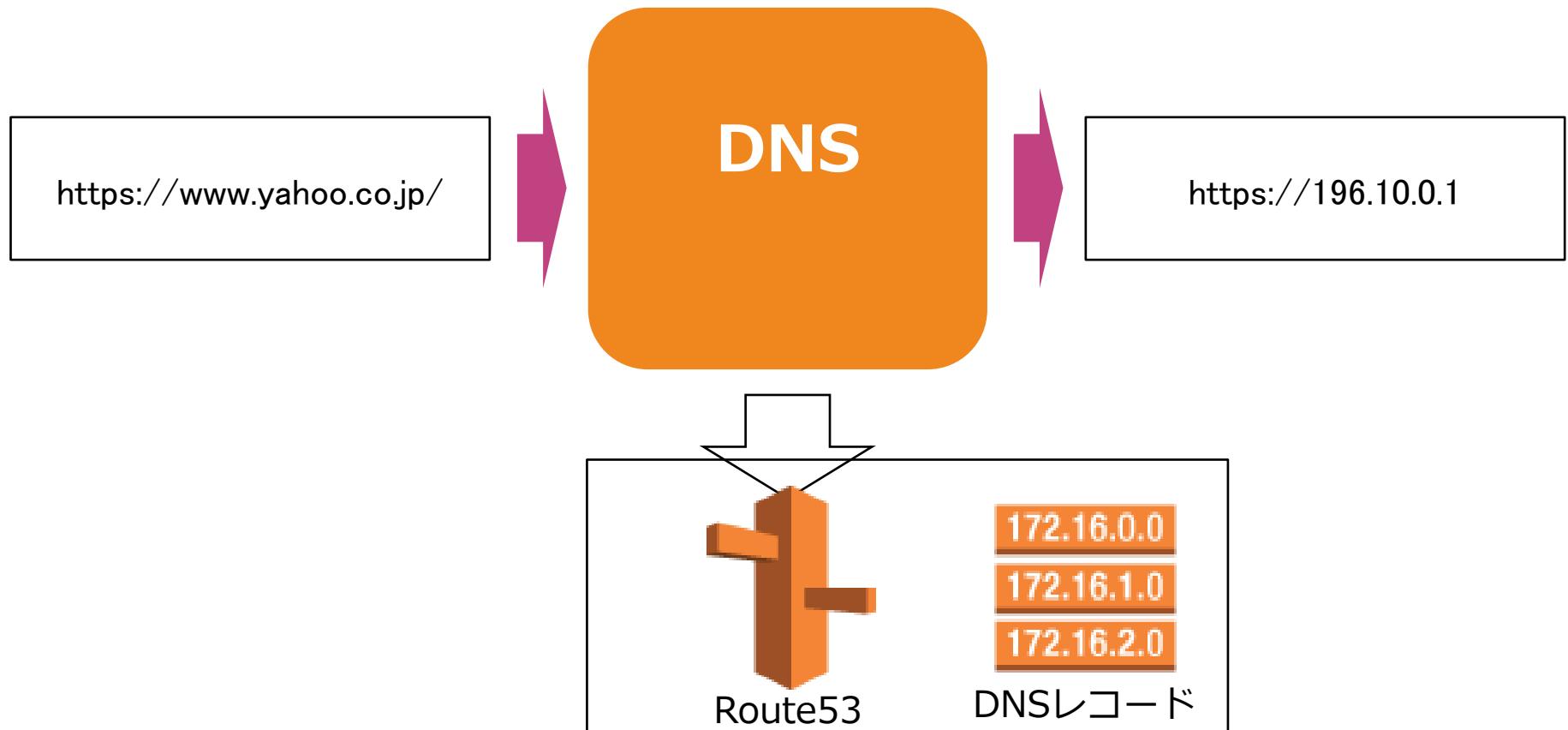
Route53とは何か？

Route53はAWSが提供する権威DNSサーバーで、ポート53で動作することからRoute53と呼ばれる



Route53とは何か？

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の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

ホストゾーン	<ul style="list-style-type: none">✓ Route53のドメイン設定の際に一番最初に実施するホストゾーンの作成について、プライベートホストゾーンとパブリックホストゾーンの使い分けなどの特徴に関する問題が出題
レコードタイプ	<ul style="list-style-type: none">✓ Route53の設定においてレコードタイプを選択する問題が出題される。✓ レコードタイプの違いに関する質問が出題される。
エイリアスレコード	<ul style="list-style-type: none">✓ Route53にCloudFrontなどのAWSリソースを設定する際に利用するエイリアスレコードの利用方法が出題される。
ルーティングポリシーの選択	<ul style="list-style-type: none">✓ Route53を設定するシナリオが提示されて、適切なルーティングポリシーを選択する問題が出題される。
フェールオーバー構成	<ul style="list-style-type: none">✓ Route53を利用してフェールオーバー構成を実現する際の設定方法が問われる。

Route53の出題範囲

1625問から質問出題範囲を抽出した頻出問題は以下の通り

Route53による 地域制限	✓ Route53を利用して配信先の地域を限定するための設定方法が 問われる。
トラフィックフロー	✓ Route53のルーティングポリシー設定におけるトラフィックフ ローの利用方法が問われる。
TTL	✓ Route53にDNS名前解決におけるTTL設定に関する質問が出題 される。
オンプレミス環境 への適用	✓ Route53を利用してオンプレミス環境への名前解決の適用方法 に関する質問が出題される。

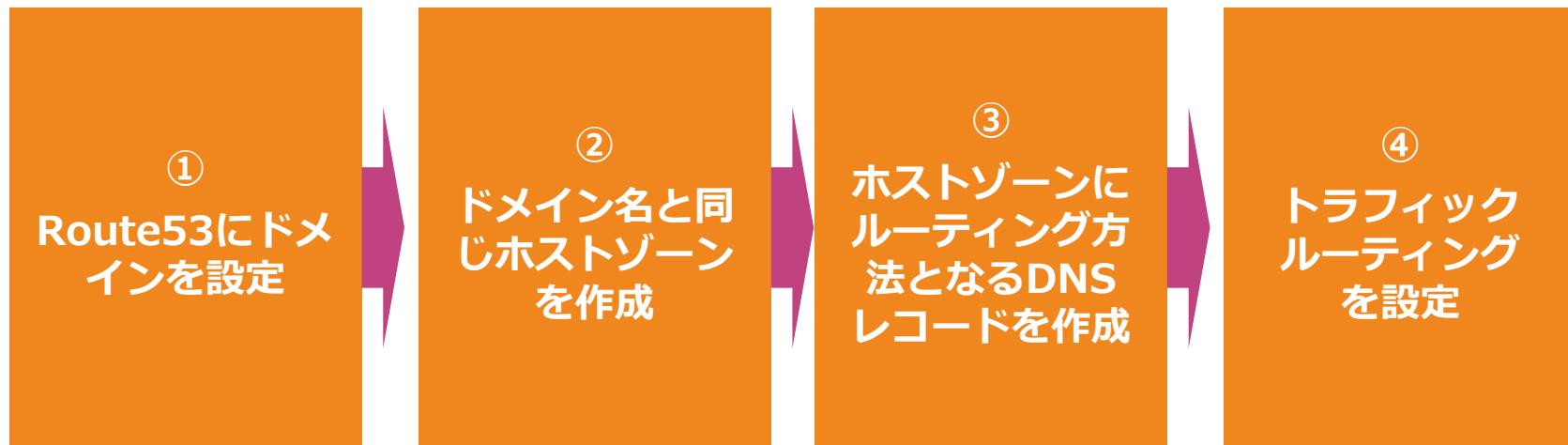
Route53

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

Route53の利用方法

Route53の利用を開始してドメインを登録すると自動でホストゾーンを自動生成し、そこにルーティングを設定する。



[Q]ホストゾーン

ある企業では2つのEC2インスタンスを利用してアプリケーションを構築しています。あなたはソリューションアーキテクトとして、EC2インスタンスをDNSルーティングによる冗長構成とすることで、異常が発生しているインスタンスへのトラフィックを回避できるように設定しようとしています。マルチリージョンにも対応できる構成とするため、Route53を利用したルーティングを利用するにしました。そのためにはパブリックホストゾーンを設定することが必要です。

パブリックホストゾーンの特徴として正しい内容を選択してください。（2つ選択してください。）

- 1) 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である
- 2) プライベートサブネット内にあるドメインをルーティングすることが可能である
- 3) 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である
- 4) 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する

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

[Q]レコードタイプ

あなたはソリューションアーキテクトとして、AWS上でWEBアプリケーションを構築しています。この構成に対して、example.comのドメイン名を利用したいと考えています。Route53のレコードへの設定が必要となります。

次のうち、Amazon Route 53でサポートされていないレコードタイプはどれでしょうか？

- 1) MX
- 2) AAAA
- 3) CNAME
- 4) DNSSEC

レコードタイプ

ルーティング方法を設定するためにDNSレコードを作成し、各種レコードを設定する

SOA	ドメインのDNSサーバー／ドメイン管理者のメール・アドレス／シリアル番号などを保持して、ゾーン転送時に情報が更新されているかの判断に利用する
A	ホスト名とIPv4アドレスの関連づけを定義するレコード
MX	メールの配送先（メールサーバ）のホスト名を定義するレコード
CNAME	正規ホスト名に対して別名を定義するレコード。特定のホスト名を別のドメイン名に転送する時などに利用する

他のレコードタイプは以下を参照

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/ResourceRecordTypes.html

[Q]エイリアスレコード

あなたはソリューションアーキテクトとして、AWS上でWEBアプリケーションを構築しています。このアプリケーションは、IPv4通信のみを利用しています。着信トラフィックを均等に分散するALBを設置して、EC2インスタンスのAuto Scalingグループにホストされたアプリケーションを展開しました。この構成に対して、example.comのドメイン名を利用したいと考えています。

Route 53にALBのDNS名を設定するために、どのレコードタイプを使用しますか？
(2つ選択してください。)

- 1) AAAAレコード
- 2) Aレコード
- 3) CNAMEレコード
- 4) エイリアスレコードのタイプ「AAAA」レコードセット
- 5) エイリアスレコードのタイプ「A」レコードセット

エイリアスレコード

CloudFrontやELBなどのAWSリソースをドメインと関連付ける際にはAWS専用のエイリアスレコードを利用する。

- エイリアスレコードはDNSクエリにAWSサービスのエンドポイントのIPアドレスを返答することで、AWSリソースにドメイン名を設定することができる。
- 以下のサービスに利用
 - 静的ウェブサイトとして設定されたS3バケット
 - CloudFront
 - ELB
 - AWS Elastic Beanstalk 環境
- IPアドレスバージョンに応じたタイプ
 - エイリアスターゲットの IP アドレスを伴う A レコード (IPv4 アドレス)
 - エイリアスターゲットの IP アドレスをAAAA レコード (IPv6 アドレス)

[Q]ルーティングポリシーの選択

あなたはソリューションアーキテクトとして、AWS上でWEBアプリケーションを構築しています。このアプリケーションは冗長構成を高めるためにELBの背後に複数のEC2インスタンスを利用しています。このアプリケーションに対して、Route53を利用して、通信の遅延発生を最小限に抑える構成が必要です。

このシナリオでAWS Route 53をどのように構成する必要がありますか？

- 1) フェイルオーバールーティングポリシーを使用する。
- 2) レイテンシールーティングを利用する。
- 3) 加重ルーティングポリシーを使用する。
- 4) シンプルルーティングを利用する。

[Q]ルーティングポリシーの選択

様々なルーティング方式を選択して設定することが可能

シンプルルーティング	<ul style="list-style-type: none">□ レコードセットにおいて事前に設定された値のみに基づいてDNSクエリに応答するルーティング方式□ 静的マッピングによりルーティングを決定する。
加重ルーティング	<ul style="list-style-type: none">□ 複数エンドポイントに重みを設定して、重みに応じてDNSクエリに応答するルーティング方式□ 重みづけの高いエンドポイントに多くルーティングする。
フェールオーバー ルーティング	<ul style="list-style-type: none">□ ヘルスチェックに基づいて、利用可能なリソースにDNSクエリを応答するルーティング方式□ 利用可能なリソースにルーティングされる。
複数値回答ルーティング	<ul style="list-style-type: none">□ ランダムに選ばれた最大8つの別々のレコードにIPアドレスを設定して、複数の値を返答するルーティング方式□ 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ことで、正常なリソースの値を返す。ELBに代わるものではないが、正常を確認して複数のIPアドレスを返す機能により、DNSを使用してアベイラビリティとロードバランシングを向上させることができる。

[Q]ルーティングポリシーの選択

様々なルーティング方式を選択して設定することが可能

レイテンシールーティング

- リージョンのレインテンシーに応じて、DNSクエリに応答するルーティング方式。ユーザーの最寄りのリージョンになることが多い。
- リージョン間のレインテンシーが低い方へルーティングされる。

位置情報ルーティング

- ユーザーのIPアドレスにより位置情報を特定して、地域ごとに異なるレコードを返すルーティング方式
- ネットワーク構成に依拠しない精度の高いレコード返答の区分けが可能となる。

地理的近接性ルーティング

- ユーザーとリソースの場所に基づいて地理的近接性ルールを作成して、トラフィックをルーティングする方式
-AWSリソースを使用している場合は、リソースを作成したAWSリージョンを場所とする。
-AWS以外のリソースを使用している場合は、リソースの緯度と経度で位置を場所とする。
- 必要に応じてバイアスを設定し、特定のリソースにルーティングするトラフィック量を変更できる。
- トラフィックフローを利用する必要がある。

[Q]フェールオーバー構成

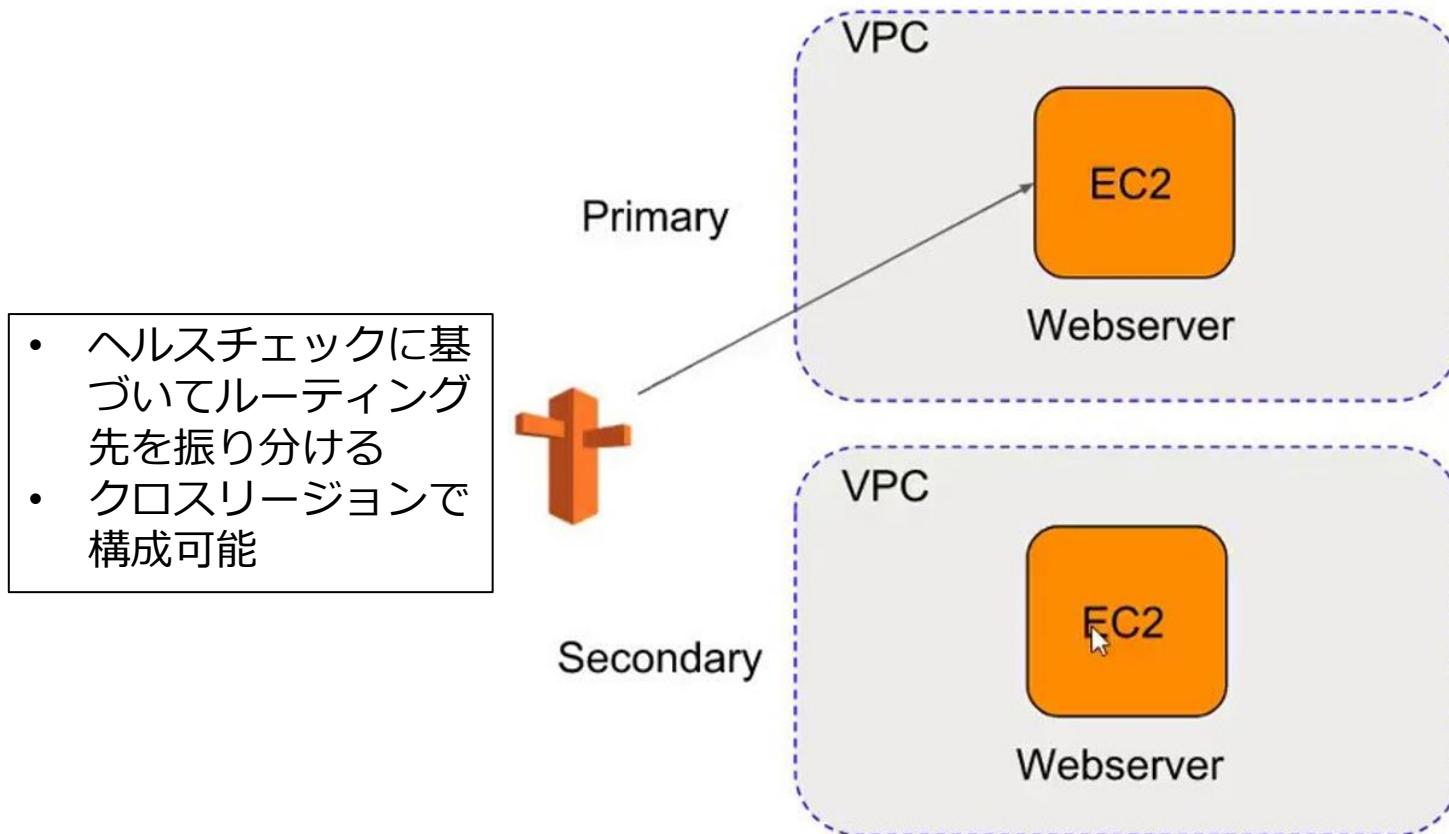
ある企業では2つのEC2インスタンスを利用してアプリケーションを構築しています。あなたはソリューションアーキテクトとして、EC2インスタンスに設定したALBに対してフェールオーバーを実行できるようにRoute53を設定することにしました。その際には、セカンダリALBを指すようにDNSエイリアスレコードを更新する必要があります。

フェイルオーバープロセスを自動化するために必要なRoute53の設定はどれでしょうか？

- 1) ELBヘルスチェックタイプを選択して、Route53を構成する。
- 2) EC2ヘルスチェックタイプを選択して、Route53を構成する。
- 3) ALBエンドポイントを指すCNAMEレコードをAmazon Route53に作成する
- 4) Amazon Route53ヘルスチェックを有効にして、ルーティングポリシーを設定する。

フェールオーバー構成

フェールオーバー構成はRoute53のヘルスチェック機能を利用したプライマリーとセカンダリーの冗長構成のこと



[Q]フェールオーバー構成

ある企業では2つのEC2インスタンスを利用してアプリケーションを構築しています。あなたはソリューションアーキテクトとして、EC2インスタンスをDNSルーティングして冗長構成とすることで、異常が発生しているインスタンスへのトラフィックを回避できるように設定しようとしています。異常が発生していない場合は、両方の構成をアクティブに利用する予定です。

この要件を満たす方法を選択してください。

- 1) フェールオーバールーティングでアクティブ／パッシブ構成
- 2) フェールオーバールーティングでアクティブ／アクティブ構成
- 3) レイテンシールーティングでアクティブ／パッシブ構成
- 4) レイテンシールーティングでアクティブ／アクティブ構成

フェールオーバー構成

フェールオーバー構成はRoute53のヘルスチェック機能を利用して正常なリソースを利用する構成のこと

フェールオーバー
(アクティブ/パッシブ)

- Route 53 はプライマリリソースをアクティブなリソースとしてルーティングする。障害が発生した場合、Route 53 はセカンダリーのリソースをルーティングする。
- フェールオーバーポリシーを使用して設定する。

フェールオーバー
(アクティブ/アクティブ)

- Route 53 は複数のリソースをアクティブとしてルーティングする。障害が発生した場合、Route 53 は正常なリソースにフェイルバックする。
- フェールオーバー以外のルーティングポリシーを使用して設定する。

[Q]Route53による地域制限

大手メディアはニュース配信アプリケーションをAWS上に構築しています。ユーザーはグローバルに存在しており、グローバルにコンテンツを配信します。アプリケーションは、ALBの背後にあるプライベートサブネットに設置されたEC2インスタンスのフリートを使用しています。中国からの情報制限があり、中国からのアクセスをロックする必要があります。

次のオプションのうち、地域制限を実施できるようにするのはどれですか？（2つ選択してください）

- 1) Route53の位置情報ルーティングポリシーを使用して、コンテンツ配信を、配信権を持っている場所に限定する。
- 2) Route53の地理的近接性ルーティングポリシーを使用して、コンテンツ配信を、配信権を持っている場所に限定する。
- 3) Route53の地域制限を有効化して、特定の地域への配信制限を設定する。
- 4) CloudFrontの地域制限を有効化して、特定の地域への配信制限を設定する。
- 5) CloudFrontの配信ポリシーにより、特定の地域への配信制限を設定する。

Route53による地域制限

位置情報ルーティングを利用して、コンテンツの配布を配信権限がある場所だけに制限することが可能

位置情報ルーティングによる地域制限

- 地域を指定して配信先としての制限設定し、コンテンツを権利がある場所のみに制限することが可能
- 地域に応じてコンテンツを変更するなど、コンテンツ配布のローカライズを実施することが可能
- 特定の地域からのエンドポイントを利用してローカルでのパフォーマンスを向上させる。

[Q] トラフィックフロー

ある企業では2つのEC2インスタンスを利用してアプリケーションを構築しています。あなたはソリューションアーキテクトとして、Route53を利用したルーティング設定を行っています。設計方針を整理したところ、組織構造やアプリユーザーが多数かつ複雑であることもあって、複雑なルーティングポリシーを設定することが必要となりました。

Route53を利用した複雑なルーティング設定を効率的に実施する方法を選定してください。

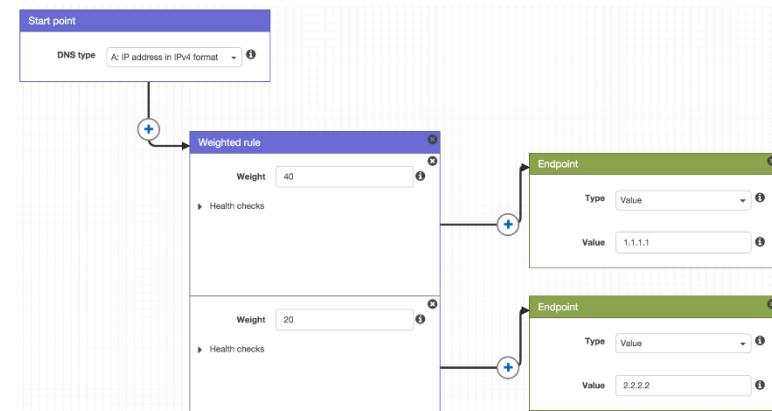
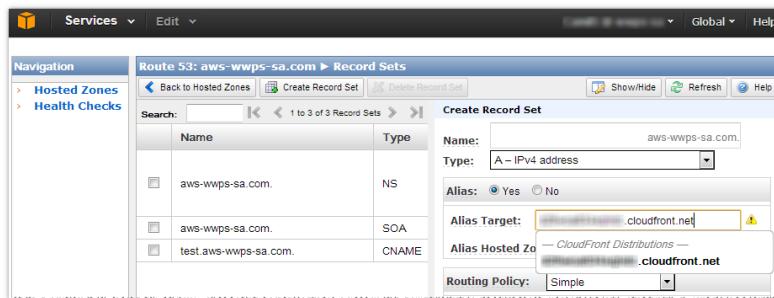
- 1) ALIASレコードを駆使して、フローを作成することでルーティングポリシーを設定する
- 2) ALIASレコードをトラフィックフローでフロー化することでルーティングポリシーを設定する
- 3) トラフィックフローを用いて、順序を設定することでルーティングポリシーを設定する
- 4) JSON/YAMLファイルにルーティングを設定することでルーティングポリシーを設定す

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



[Q]TTL

ある企業では2つのEC2インスタンスにELBとRoute53が設定されたアプリケーションを運用しています。このアプリケーションはexample.comというドメインを利用して公開されています。最近になって災害復旧計画を整備したため、あなたはソリューションアーキテクトとして、DNSルーティングにより冗長構成とするように構成を見直しています。そのために、Route53の既存のホストゾーンに対して新しいドメインに再設定しました。しかしながら、1時間たっても新しいドメインへのルーティングが実行されません。

この問題の最も可能性が高い要因はどれでしょうか？

- 1) TTLが有効期限となっている。
- 2) CNAMEレコードが正しく構成されていない。
- 3) ヘルスチェックエラーが発生している。
- 4) ドメインが取得されたばかりで、反映されていない。

TTL

再帰的な DNS リゾルバーでレコードに関する情報をキャッシュして保持しておく時間 (秒単位)を設定できる。

- DNSリゾルバーはリゾルバは自分の知っているDNSサーバへ問い合わせを行い、IPアドレスの割り出し（名前解決）を行う機能。つまりドメイン名の対応付けを確認してくれる。
- 再帰的な DNS リゾルバーはドメインに変更がないか再度問い合わせること。
- その情報をキャッシュに保持することで、毎回リゾルバが名前解決しなくともドメインの情報を把握することが可能となる。
- 再帰的な DNS リゾルバーで Route 53 に対して実行する必要がある呼び出しの数を減らすことが可能

[Q]オンプレミス環境への適用

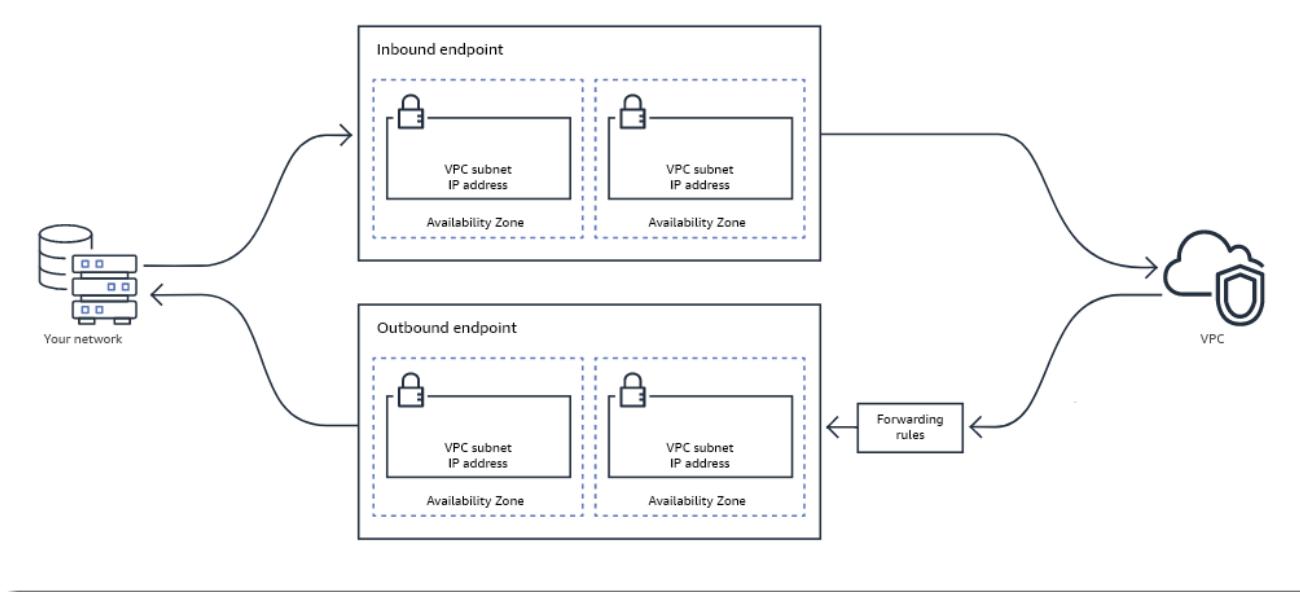
ある企業では2つのEC2インスタンスにELBとRoute53が設定されたアプリケーションを運用しています。このアプリケーションはexample.comというドメインを利用して公開されています。あなたはソリューションアーキテクトとして、Route53を利用してオンプレミス環境にも適用しようとしています。オンプレミスネットワーク内のリソースのDNSクエリをAWS VPCから解決することが必要です。

この要件を満たす、設定は次のうちどれですか？（2つ選択してください）

- 1) Route 53 リゾルバーでインバウンドエンドポイントを作成して、オンプレミスネットワーク上のDNSリゾルバーがDNSクエリをRoute 53リゾルバーに転送できるようにする。
- 2) Route 53 リゾルバーでアウトバウンドエンドポイントを作成して、Route 53 リゾルバーがオンプレミスネットワーク上のリゾルバーにクエリを転送できるようにする。
- 3) Route 53 リゾルバーでインバウンドエンドポイントを作成して、Route 53 リゾルバーがオンプレミスネットワーク上のリゾルバーにクエリを転送できるようにする。
- 4) Route 53 リゾルバーでアウトバウンドエンドポイントを作成して、オンプレミスネットワーク上のDNSリゾルバーがDNSクエリをRoute 53リゾルバーに転送できるようにする。
- 5) Route 53 リゾルバーからVPCエンドポイントを利用して、Route 53 リゾルバーとオンプレミスネットワーク上のリゾルバーがお互いに連携できるようにする。

オンプレミス環境への適用

Route53リゾルバを利用して、オンプレミスからVPC内の名前解決が可能となった。これにより、オンプレミス、AWS相互の名前解決を実現することができる。



- ✓ インバウンドエンドポイントを作成し、VPCへの接続を設定
- ✓ アутバウンドエンドポイントを作成し、アウトバウンドへの通信を設定