総仕上げ問題

■試験番号　SAA-C02

■問題数　65問

■試験時間　130分

問題

1. **ある企業では、企業内で共有するファイルサーバーとしてWindowsサーバーを使用しています。SMBプロトコルを使用してWindowsフォルダ共有や、複数のWindowsサーバー間での複製（DFSレプリケーション）を実現しています。**
ソリューションアーキテクトであるあなたは、このファイル共有の仕組みをAWSに移行することで、構築・運用のコストを削減したいと考えています。移行先として適切なAWSサービスはどれですか。

A. Amazon EFS
B. Amazon S3
C. Amazon FSx for Windows
D. Amazon EBS
E. Amazon FSx for Lustre

➡ P33

2. **あなたの会社では、社内向けWebアプリケーションを運用しています。フロントエンド処理とバックエンド処理の2つのバッチモジュールで構成されており、フロントエンドで処理を受け付けたあとに、バックエンド処理に連携しています。**
このWebアプリケーションのユーザー数が増加し、バックエンド処理に時間がかかっています。そこでAmazon ECSに移行し、マイクロサービス化を行い、ユーザー数の増加に耐えるアーキテクチャにすることを検討しています。次のうちどのソリューションが適切ですか。

A. フロントエンド処理とバックエンド処理の連携にAmazon SQSを使用し、SQSキューからデータを取り出す
B. フロントエンド処理とバックエンド処理の連携にAmazon SNSを使用し、データをトピック通知する
C. フロントエンド処理とバックエンド処理の連携にAmazon S3を使用し、S3バケットに登録されたデータをトリガーとする
D. フロントエンド処理とバックエンド処理の連携にAmazon EFSを使用し、データを共有する

➡ P33

3. 現在開発を進めているアプリケーションはグローバルサービスであるため、データベースに対して常に多数の読み取りと書き込みが発生することがわかっています。このアプリケーションにおいて、データベースがボトルネックにならないようにしたいと考えています。
データベース側の処理によるボトルネックの発生を抑え、アプリケーションのパフォーマンスを最大限に引き出すことができるEBSストレージタイプは次のうちどれですか。

A. プロビジョンドIOPS SSD
B. スループット最適化HDD
C. コールドHDD
D. 汎用SSD

➡ P33

4. ソリューションアーキテクトであるあなたは、EC2インスタンス間で低いネットワークレイテンシーと高いネットワークスループットを必要とする新しいアプリケーションのアーキテクチャを設計しています。
これを実現するために選択するソリューションとして、適切なものはどれですか。

A. AWS Auto Scaling
B. クラスタープレイスメントグループ（クラスター配置グループ）
C. パーティションプレイスメントグループ(パーティション配置グループ)
D. スプレッドプレイスメントグループ（スプレッド配置グループ）

➡ P34

5. Amazon S3を利用した特定の会員向けの画像共有サイトがあります。会員以外の不特定多数の人がこのサイトにアクセスし、画像をダウンロードしているとの報告がありました。この状況を解決するには、どのような方法をとればよいでしょうか（2つ選択）。

A. 有効期限付きの署名付きURLを使用する
B. Amazon S3では会員だけに画像を共有するといったことができないため、WebサーバーのEBSボリュームに写真を保存する
C. セキュリティグループを利用して会員のIPアドレスのみアクセスを許可する
D. Amazon S3の一般公開用のアクセス権を削除する

➡ P34

6. VPC内のアプリケーションから、Amazon DynamoDBに接続するシステムをAWS上で構築したいと考えています。ただし、アプリケーションとDynamoDBへはインターネット経由での接続が許可されていないため、同じリージョン内でプライベート接続しなければいけません。
この状況で利用するサービスとして、適切なものはどれですか。

A. VPCピアリング
B. AWS Direct Connect
C. NATゲートウェイ
D. VPCエンドポイント

➡ P35

7. ある企業では現在、業務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のデータを格納するデータベースは、多くの業務データを頻繁に登録・更新・削除することに耐えられる性能が求められています。
また、格納されたデータからレポートを生成するために、複数のテーブルを結合してデータを取得することを想定しています。さらに、今後のデータの増加量に備えて、データベースのストレージを自動拡張する機能も求められています。
これらの要求を満たすことができる、最も適切なサービスはどれですか。

A. Amazon DynamoDB
B. Amazon Glacier
C. Amazon Aurora
D. Amazon Redshift
E. Amazon S3

➡ P35

8. **ある企業では、アプリケーションのユーザー数が1年間で5倍になると予想しています。このアプリケーションはひとつのリージョンでホストされ、Amazon RDSのMySQLデータベース、Application Load Balancer、およびEC2を使用して静的コンテンツと動的コンテンツをホストするWebサイトとそのマイクロサービスをホストします。**
この企業の成長をサポートするためには、どのような設計変更を推奨する必要がありますか（2つ選択）。

A. EC2からS3に静的ファイルを移動する
B. Amazon Route 53の位置情報ルーティングポリシーを使用する
C. リアルタイムのCloudTrailログに基づいて環境をスケーリングする
D. マイクロサービスごとに専用のElastic Load Balancingを作成する
E. RDSリードレプリカを作成し、これらのレプリカを使用するようにアプリケーションを変更する

➡ P35

9. **ある企業がcompany.comというZone Apexを使用して静的なWebサイトを公開しています。このWebサイトではDNSにAmazon Route 53を使用したいと考えています。スケーラブルで費用対効果の高い構成は、次のうちどれですか（2つ選択）。**

A. EC2インスタンス上にWebサイトを構築し、Amazon Route 53のエイリアスとしてEC2インスタンスのパブリックIPアドレスを紐付ける
B. AWS CloudFormationを使用してWebサイトを構築し、Amazon Route 53のエイリアスとしてCloudFormationスタックを紐付ける
C. Amazon S3上のコンテンツを静的Webサイトホスティングで公開し、Amazon Route 53のエイリアスとしてS3のエンドポイントを紐付ける
D. Elastic Load BalancingとAuto Scalingを使用してEC2上にWebサイトを構築し、Amazon Route 53のエイリアスとしてElastic Load Balancingのエンドポイントを紐付ける

➡ P36

10. ある企業では、パブリックサブネットとプライベートサブネットで実行されている2層Webアプリケーションが稼働しています。アプリケーション層はパブリックサブネットで、データベース層はプライベートサブネットで稼働しており、いずれも単一のアベイラビリティーゾーン（AZ）のEC2インスタンス上で実行されています。
このアーキテクチャで高可用性を実現するには、次のうちどの方法を組み合わせる必要がありますか（2つ選択）。

A. 同じAZに新しいパブリックサブネットとプライベートサブネットを作成する
B. 複数のAZにまたがるEC2のAuto Scalingグループと Application Load Balancerを作成する
C. 既存のWebアプリケーションインスタンスをApplication Load BalancerのAuto Scalingグループに追加する
D. 別のAZに新しいパブリックサブネットとプライベートサブネットを作成し、ひとつのAZでEC2インスタンスにデータベース層を構築する
E. 別のAZに新しいパブリックサブネットとプライベートサブネットを作成し、データベースをAmazon RDSのマルチAZ配置に移行する

➡ P36

11. あなたの会社では、顧客企業向けのアプリケーションをAWS上に構築しています。アプリケーションで利用する画像をRDSのMySQLデータベースに格納していますが、画像は日々増加しており、画像へのアクセスも非常に多いため、コスト削減とパフォーマンス向上の対策を行うよう依頼されました。次のうち、適切な対応方法はどれですか。

A. Amazon RDSのMySQLデータベースのリードレプリカを利用する
B. 画像ファイルのうち、特に頻繁に使用される1割の画像ファイルのみAmazon RDSのMySQLデータベースに格納し、残りをAmazon S3 Glacierに移行する
C. 画像ファイルをすべてAmazon EBSに移行し、顧客からはAmazon CloudFrontを介して画像にアクセスできるようにする
D. 画像ファイルをすべてAmazon S3に移行し、顧客からはAmazon CloudFrontを介して画像にアクセスできるようにする

➡ P37

12. **あなたの会社のシステムは、ハードウェア保守期限切れに伴い、1カ月以内に複数のアプリケーションをAWSクラウドへ移行する必要があります。各アプリケーションは約50TBのデータを転送する必要があり、移行完了後は自社とAWSの間で安全かつ安定したスループットを持つネットワーク接続が必要です。**
あなたは、初回のデータ移行と移行後の安定したネットワークをどのように用意しますか。

A. 初回のデータ移行および継続的なネットワークにAWS Direct Connectを利用する
B. 初回のデータ移行および継続的なネットワークにSite to Site VPNを利用する
C. 初回のデータ移行にAWS Snowball、継続的なネットワークにAWS Direct Connectを利用する
D. 初回のデータ移行にAWS Snowball、継続的なネットワークにSite to Site VPNを利用する

➡ P37

13. **ある企業では、Application Load Balancerに登録されたEC2インスタンスでWebサービスを実行しています。**
EC2インスタンスは、2つのアベイラビリティーゾーン（AZ）にまたがるAuto Scalingグループで実行されます。このアプリケーションは、必要なSLAを満たすために最低4台のEC2インスタンスを必要としています。
ひとつのAZに障害が発生した場合、この企業がより低コストでSLAを維持し続けるためには、次のうちどの戦略を採用すればよいでしょうか。

A. クールダウン期間が短いスケーリングポリシーを追加する
B. Auto Scalingグループの起動設定を変更して、より大きなインスタンスタイプを使用する
C. Auto Scalingグループを変更して、3つのAZで合計6台のEC2インスタンスを使用する
D. Auto Scalingグループを変更して、2つのAZで合計8台のEC2インスタンスを使用する

➡ P37

14. あなたはEC2インスタンス上で動作するアプリケーションを構築し、データベースとしてAmazon DynamoDBを使用することを考えています。このアプリケーションでは、EC2インスタンスからDynamoDBのデータを書き込みできなければいけません。
キーペア（アクセスキーIDとシークレットアクセスキー）のEC2インスタンスへの格納が許可されていない場合の説明として、適切なものはどれですか（2つ選択）。

A. Amazon DynamoDBへの書き込みを可能にするIAMロールを作成する
B. Amazon DynamoDBへの書き込みはIAMロールの権限がなくても可能である
C. 実行中のEC2インスタンスにIAMユーザーを追加する
D. Auto Scalingの起動設定にIAMロールが含まれているEC2インスタンスを起動する

➡ P38

15. あなたの会社ではWebマーケティングを目的に、各ユーザーのWebサイト上での動きを追跡し、リコメンデーションを発信しています。EC2インスタンス上でユーザーのアクセスログをほぼリアルタイムで収集し、Amazon RDSに保存しています。保存されたログを別のEC2インスタンスがリアルタイムでチェックし、SQLクエリによりリコメンデーションを作成しています。ソリューションアーキテクトであるあなたは、現在のアーキテクチャを疎結合にし、SQLでリアルタイムデータを分析したいと考えています。適切なソリューションを選びなさい。

A. Amazon SNSを使用し、Webサイトからのアクセスログを受信したあとに、AWS Lambdaに連携してLambdaからSQLクエリを実行する
B. Amazon SQSを使用し、Webサイトからのアクセスログを受信したあとに、現在のEC2インスタンスにデータを連携する
C. Amazon Kinesis Data Streamsを使用し、Webサイトからのアクセスログを受信したあとに、Amazon Kinesis FirehoseでS3にデータを保存する。保存されたデータをAmazon AthenaでSQL分析する
D. Amazon Kinesis Data Streamsを使用し、Webサイトからのアクセスログを受信したあとに、Amazon Kinesis Data AnalyticsでSQL分析する。Amazon Kinesis FirehoseでS3にデータを保存する

➡ P38

16. 世界中の会員に動画を配信するサービスで、一部の国や地域の会員より、アクセスしてから再生されるまでに時間がかかるという指摘が寄せられています。
アクセスする地域に関係なく、アクセスから再生までの時間を短縮する方法として適切なものはどれですか。

A. Amazon S3に動画ファイルを格納し、URLに直接アクセスさせる
B. Amazon S3に動画ファイルを格納し、署名付きURLを利用する
C. EC2インスタンス上でWebサーバーを起動し、動画ファイルをEBSボリュームに格納する
D. Amazon CloudFrontの署名付きURLを利用する

➡ P38

17. あなたの会社では、多くの顧客が利用するWebアプリケーションを運営しています。あなたは、このシステムのデータが格納されているAmazon RDSのMySQLデータベースがボトルネックにならないように対応を依頼されました。
MySQLデータベースがボトルネックになるのを防ぐのに効果的な方法はどれですか（2つ選択）。

A. ELBのClassic Load BalancerをWebアプリケーション層の前に配置する
B. Amazon RDSのリードレプリカを利用する
C. RDSのMySQLデータベースの前にAmazon ElastiCacheを配置する
D. Amazon RDSのMySQLデータベースのマルチAZ機能を利用する

➡ P39

18. Amazon Auroraの特徴として、誤っているものはどれですか。

A. マネージド型のサービスである
B. MySQLやPostgreSQLよりもスループットが高い
C. 3つのアベイラビリティーゾーン（AZ）にデータが格納されるため耐久性が高い
D. 列指向のアーキテクチャで、大量データの集計・分析に向いている
E. リレーショナルデータベースサービスである

➡ P39

19. **Amazon Redshiftのクラスターの冗長性を高めるための方法として、適切なものはどれですか。**

A. より性能の高いインスタンスタイプに変更する
B. クロスリージョンスナップショットを設定する
C. マルチAZを有効化する
D. ノード数を増やす

➡ P39

20. **Webサーバーが、ある特定のIPアドレスから不正アクセスを受けていることが判明しました。このIPアドレスからの接続を拒否したい場合、どのサービスあるいは機能で対応すればよいでしょうか。**

A. インターネットゲートウェイ
B. ネットワークACL
C. AWS Direct Connect
D. Amazon API Gateway

➡ P39

21. **あなたの会社では、多くの会員が利用する画像ファイル共有のためのWebアプリケーションを設計しています。画像ファイルの格納にはAmazon S3を利用する予定ですが、画像ファイルをアップロードする際に経由するWebサーバーのトラフィックが大きくなるのを避けたいと考えています。このWebアプリケーションから画像を保存するのに最も適切な方法はどれですか。**

A. Elastic IPを利用してWebサーバーのIPアドレスを固定化する
B. 画像を一時的に格納するS3バケットを複数用意する。S3バケットに画像がアップロードされたら、Lambda関数で画像格納用のS3バケットにファイルを移動させる
C. ELBのClassic Load Balancerを利用してAuto Scalingグループにアップロードすることで、S3バケットに書き込みができるように設定する
D. 画像処理用のリソースを提供するために、スポットインスタンスを使用してWebサーバーの機能を拡張する
E. 署名付きURLを使用してS3に直接アップロードする

➡ P40

22. ある企業には、Webサーバーをパブリックサブネットに、データベースサーバーをプライベートサブネットに構築している2層のWebサイトシステムがあります。
このシステムでは、インターネットからアクセスできるのはWebサーバーだけですが、データベースサーバーはソフトウェア更新のためにインターネットにアクセスする必要があります。
このシステムの要件を満たすサービスの利用方法は次のうちどれですか。

A. パブリックサブネットにNATゲートウェイを構築する
B. プレイスメントグループを設定する
C. データベースサーバーにElastic IPを割り当てる
D. プライベートサブネットのネットワークACLで、インターネットからの通信トラフィックを「許可」に設定する

➡ P40

23. EC2インスタンス上で毎日7時間だけ稼働が要求されるWebアプリケーションを設計しています。このEC2インスタンスは、r4.8xlargeのインスタンスタイプを使用すると安定して動作します。このシステムは高可用性が求められておらず、1年後に廃止されます。このシステムを動作させるEC2の購入オプションとして、最もコスト効果の高いのはどれですか。

A. Standardタイプのリザーブドインスタンス
B. Convertibleタイプのリザーブドインスタンス
C. スケジュールされたリザーブドインスタンス
D. スポットインスタンス

➡ P40

24. あなたの会社では、リレーショナルデータベースを実行しているオンプレミスサーバーがあります。現在のデータベースは、さまざまな場所にいるユーザーから高い読み取りトラフィックが発生しています。
あなたは、データベースサーバーを最小限の変更でAWSに移行したいと考えています。データベースに障害が発生しても業務を継続でき、現在のトラフィックでも影響が出ないようにする必要があります。
これらの要件を満たすソリューションはどれですか。

A. 異なるアベイラビリティーゾーン（AZ）のApplication Load Balancerに登録されたEC2インスタンスでホストされているデータベースを構築する
B. 異なるリージョンに複数のEC2インスタンスでホストされているデータベースを構築する
C. Amazon RDSを使用し、マルチAZ配置およびひとつ以上のリードレプリカで構成する
D. Amazon RDSを使用し、マルチAZ配置およびひとつ以上のスタンバイデータベースで構成する

➡ P40

25. ある会社では、バッチ処理を行うシステムを2つに区分けしています。ひとつはミッションクリティカルな基幹システムで実行するバッチ処理で、もうひとつは業務に直接影響のない非基幹システムで実行するバッチ処理です。これらのバッチ処理は、不定期に実行されます。このシステムをできるだけ低コストで構築するための構成として、適切なものはどれですか。

A. 基幹システムをリザーブドインスタンス、非基幹システムをオンデマンドインスタンスで構成する
B. 基幹システムをリザーブドインスタンス、非基幹システムをスポットインスタンスで構成する
C. 基幹システム、非基幹システムとも、オンデマンドインスタンスで構成する
D. 基幹システムをスポットインスタンス、非基幹システムをリザーブドインスタンスで構成する

➡ P41

26. **あなたの会社では、システムの更改に伴い、20TBのデータを30日以内にデータセンターからAWSクラウドに移行する必要があります。ネットワーク帯域幅は15Mbpsに制限されており、使用率が70%を超えることはできません。これらの要件を満たすためには、次のうちどのサービスを利用すべきですか。**

A. AWS Snowballを利用し、データを移行する
B. AWS DataSyncを利用し、データを移行する
C. AWS Storage Gatewayのファイルゲートウェイを利用し、データを移行する
D. Amazon S3 Transfer Accelerationを利用し、Amazon S3へデータを移行する

➡ P41

27. **Amazon API Gateway上に構築されたAPIレイヤーを保護する一環として、既存のIDプロバイダーによって認証されているユーザーを承認する必要があります。ユーザーが認証に3回失敗した場合、1時間、アクセスを拒否されるようにしなければなりません。**
これらの要件を満たす方法として適切なものはどれですか。

A. IAMの認証を使用して、IAMロールに最小のアクセス許可を追加する
B. Amazon API Gatewayカスタム認証を使用してLambda関数を呼び出し、各ユーザーのIDを検証する
C. Cognitoユーザープールを使用し、組み込みのユーザー管理を提供する
D. Cognitoユーザープールを使用し、外部IDプロバイダーと統合する

➡ P41

28. あなたは、B to C向けのサービス提供を検討している企業からシステム構築の相談を受けました。
このサービスは常にサイトへのアクセスがあるわけではなく、1日の中で夕方から夜にかけてのみ利用者が急増することが予想されています。あなたは、この一時的な高負荷に対応するためにEC2のAuto Scalingグループを使用することにしました。
ほかにもサービス内容について調査を進めていると、サービス利用者のデータ蓄積には非リレーショナルデータベースが適しており、また、負荷の増減に自動で対応できる仕組みが望まれていることもわかりました。
この企業に提案するソリューションとして、最も適切なものはどれですか。

A. トラフィック分散にはAmazon Route 53を使用し、データ蓄積にはAmazon Auroraを使用する
B. トラフィック分散にはAmazon Route53を使用し、データ蓄積にはAmazon DynamoDBを使用する
C. トラフィック分散にはNetwork Load Balancerを使用し、データ蓄積には Amazon Auroraを使用する
D. トラフィック分散にはNetwork Load Balancerを使用し、データ蓄積には Amazon DynamoDBを使用する

➡ P42

29. 情報システム部門でデータベース管理者をしているあなたのもとに、AWSクラウドへのデータ移行の要望がありました。調査したところ、ボリュームあたりのIOPSは50000 IOPSが必要になることがわかりました。
データ格納先をEBSにする場合のソリューションとして適切なものはどれですか。

A. ボリュームタイプにスループット最適化HDD（st1）を選択する
B. ボリュームタイプに汎用SSD（gp2）を選択する
C. ボリュームタイプにプロビジョンドIOPS SSD（io1）を選択し、このEBSと接続するNitro SystemのEC2インスタンスを作成する
D. ボリュームタイプにプロビジョンドIOPS SSD（io1）を選択し、このEBSと接続するNitro System以外のEC2インスタンスを作成する

➡ P42

30. 大量のストリーミングデータを分析するために、Amazon S3やAmazon Redshiftに格納するのに適しているサービスは次のうちどれですか。

A. Amazon Kinesis Data Streams
B. Amazon Kinesis Data Firehose
C. Amazon Kinesis Data Analytics
D. Amazon SQS
E. Amazon SNS

➡ P42

31. あなたの会社には、バックエンドでAPIサービスへのリクエストを行うWebアプリケーションがあります。APIサービスは、ELBに登録されたEC2インスタンスで実行されます。
ほとんどのAPIサービスの呼び出しはごく短時間で終了しますが、外部サービスでオブジェクトを作成するエンドポイントの呼び出しには時間がかかっています。これにより、クライアントサイドではタイムアウトが起こり、システム全体のレイテンシーが増加しています。
低速なエンドポイントの影響を最小限に抑えるために行うべきことはどれですか。

A. EC2インスタンスのサイズを変更し、メモリ容量を増やす
B. Amazon SQSを使用し、別々のワーカーによる非同期処理で長時間実行されるリクエストをオフロードする
C. ELBのアイドルタイムアウト時間を増やし、長時間実行されるリクエストを完了できるようにする
D. Amazon ElastiCache（Redis）を使用し、外部サービスからの応答をキャッシュする

➡ P43

32. 最近、あなたの会社ではグローバルユーザー向けにコンテンツを提供するためのWebサイトを立ち上げました。このWebサイトで、EC2インスタンスをオリジンとして接続したAmazon CloudFrontを利用して、静的コンテンツをユーザーへ高速に配信したいと考えています。
アプリケーションの高可用性を実現するソリューションとして、適切なものはどれですか。

A. Amazon CloudFrontにLambda@Edgeを使用する
B. Amazon CloudFrontにAmazon S3 Transfer Accelerationを有効化する
C. オリジンの一部として、別のアベイラビリティーゾーンに別のEC2インスタンスを設定する
D. 同じアベイラビリティーゾーンのオリジンサーバークラスターの一部として別のEC2インスタンスを設定する

➡ P43

33. アメリカ、ヨーロッパ、日本での利用を想定した大規模なグローバルアプリケーションの構築が進められており、ソリューションアーキテクトであるあなたは、データベースについて相談されました。会社からの要望は以下のとおりです。

・それぞれの国でアプリケーションを利用しても高速で処理できるように、データベースが複数地域に分散していること
・各地域でデータの書き込みをした場合に、その変更がその他地域の分散したテーブルに反映されること。また、その変更は概ね1秒以内に反映されること
・各地域でテーブルの同じ項目を同時に更新し競合が発生した場合には、最終更新者の内容を反映すること

これらの要望を満たすことができるソシューションはどれですか。

A. データベースにAmazon ElastiCacheを選択し、データストアにRedisを選択する
B. データベースにAmazon Redshiftを選択し、コンピュータノード数が3つ以上となるようにクラスターを構築する
C. データベースにAmazon Auroraを選択し、リードレプリカを使用する
D. データベースにAmazon DynamoDBを選択し、グローバルテーブルを使用する

➡ P43

34. ある会社では、企業のアプリケーションを単一リージョンのEC2インスタンス上で実行しています。ソリューションアーキテクトは、広域災害に備えてアプリケーションを別のリージョンでもデプロイできるようにする必要があると考えています。
これを実現するためには、以下のどの方法を組み合わせる必要がありますか（2つ選択）。

A. EC2インスタンスのEBSボリュームをデタッチし、デタッチされたEBSボリュームをAmazon S3にコピーする
B. 別のリージョンのAmazon Machine Imageから新しいEC2インスタンスを起動する
C. 別のリージョンでEC2インスタンスを新たに起動し、Amazon S3に保管されているEBSにボリュームをコピーする
D. EC2インスタンスのAmazon Machine Imageをコピーし、別のリージョンをコピー先に指定する
E. Amazon S3からEBSボリュームをコピーし、そのEBSボリュームを使用してコピー先のリージョンでEC2インスタンスを起動する

➡ P44

35. あるゲーム会社は、単一のアベイラビリティーゾーン（AZ）に複数のEC2インスタンスを構築し、レイヤー4でユーザーと通信するマルチプレーヤーゲームを運営しています。このゲーム会社は、アーキテクチャの可用性と費用対効果を高くしたいと考えています。
ソリューションアーキテクトであるあなたは、この要件を満たすためにどのような設計変更を推奨する必要がありますか（2つ選択）。

A. EC2インスタンスの数を増やす
B. EC2インスタンスの数を減らす
C. EC2インスタンスの前にNetwork Load Balancerを構成する
D. EC2インスタンスの前にApplication Load Balancerを構成する
E. Auto Scalingグループを設定して、複数のAZのEC2インスタンスを自動的に追加または削除する

➡ P44

36. **あるWebアプリケーションは、パブリックサブネットにELBのClassic Load Balancerが配置されており、その配下にコンテンツベースの振り分けが可能なリバースプロキシサーバーが配置されています。アプリケーションを動作させるWebサーバーは、プライベートサブネットに配置されています。あるとき、このリバースプロキシへのトラフィックが増大していることがわかり、あなたは改善策を求められています。スケーラブルでかつ費用対効果が高い方法は次のうちどれですか（2つ選択）。**

A. リバースプロキシをClassic Load Balancerに置き換える
B. WebサーバーにAuto Scalingを追加する
C. リバースプロキシにAuto Scalingを追加する
D. Webサーバーをバースト可能（突発的なアクセス増加に対応可能）なt2のインスタンスタイプに変更する
E. Classic Load BalancerをApplication Load Balancerに変更する

➡ P45

37. **ある企業は3階層のWebアプリケーションで構成されたキャンペーンサイトを開設しています。キャンペーンサイトはEC2で配信し、データベースはAmazon RDS（Aurora）を利用しています。週末にトラフィックの急増が予想されていますが、RDSが過負荷にならず、コストを最小限に抑える設計はどれですか。**

A. EC2でAuto Scalingグループを設定する
B. Amazon DynamoDB Accelerator（DAX）を設定し、データベース読み込み時のキャッシュを行う
C. Amazon DynamoDBを設定し、トラフィックの急増に対応する
D. RDSデータベースインスタンスでAuto Scalingを設定する
E. あらかじめ複数のRDSデータベースインスタンスを構成する

➡ P45

38. **あなたの会社では、Windowsの共有ファイルストレージを必要とする大規模なMicrosoft SharePointをオンプレミスで運用しています。**
あなたはこのワークロードをAWSへ移行したいと考えており、さまざまなストレージを検討しています。ストレージは、可用性が高くアクセス制御のためにActive Directoryと統合する必要があります。これらの要件を満たす方法として適切なものはどれですか。

A. Amazon EFSストレージを利用し、認証用のActive Directoryドメインを設定する
B. 2つのアベイラビリティーゾーン（AZ）にSMBファイル共有が可能なAWS Storage Gatewayのファイルゲートウェイを作成する
C. S3バケットを作成し、Windows Serverのボリュームとしてマウントする
D. AWS上にファイルサーバーとしてAmazon FSx for Windowsを作成し、認証用にActive Directoryドメインを設定する

➡ P45

39. **ソリューションアーキテクトであるあなたは、組織内に新しいAWSアカウントを作成しようとしています。作成直後に、AWSアカウントのルートユーザーに対して、アカウント乗っ取りなどによる脅威からセキュリティを保護するため、いくつかの対策を予定しています。適切な対策はどれですか（2つ選択）。**

A. ルートユーザーに多要素認証（MFA）を有効化する
B. ルートユーザーのアクセスキーIDとシークレットアクセスキーを暗号化し、ローカルに保管する
C. ルートユーザーのパスワードを複雑なものに変更する
D. ルートユーザーに対してIP制限をかける
E. ルートユーザーから管理者権限を取り除く

➡ P46

40. ある会社ではオンプレミスでWebアプリケーションを実行しています。Webアプリケーションはコンテナ化されており、ユーザーレコードを含むPostgreSQLデータベースに接続された複数台のLinuxホストで実行されています。
同社では、インフラストラクチャのメンテナンスにかかる運用コストと将来的なキャパシティの計画が自社の成長を阻害していることがわかりました。この問題を解決するために、ソリューションアーキテクトが実施するべき対策はどれですか。

A. PostgreSQLデータベースをAmazon Auroraに移行する
B. WebアプリケーションをEC2インスタンスでホストする
C. Webアプリケーションのコンテンツを Amazon CloudFrontを利用して配信する
D. WebアプリケーションとPostgreSQLデータベースの間にAmazon ElastiCacheを配置する

➡ P46

41. ソリューションアーキテクトであるあなたは、企業が所有する秘匿情報を含んだ業務データの保存先としてAmazon S3の導入を検討しています。セキュリティ要件は厳しく、保存するデータの暗号化や、暗号化鍵の自動的なローテーション、暗号化鍵の使用状況の可視化・証跡管理や暗号化鍵の権限管理などが求められています。
S3でこれらの要件を実現する方法として適切なものはどれですか。

A. AWS KMSサービスで暗号化鍵を管理し、サーバーサイド暗号化（SSE－KMS）を使用するようS3バケットを作成する
B. Amazon S3が管理する暗号化鍵により、サーバーサイド暗号化（SSE-S3）を使用するようS3バケットを作成する。また、S3バケット内のファイルのバージョニング機能を有効化しておく
C. Amazon S3が管理する暗号化鍵により、サーバーサイド暗号化（SSE-S3）を使用するようS3バケットを作成する
D. 会社が発行・管理している暗号化鍵により、サーバーサイド暗号化（SSE-C）を使用するようS3バケットを作成する

➡ P46

42. **ある会社のWebアプリケーションは複数のLinuxインスタンスを使用しており、EBSボリュームにデータを保存しています。同社では、障害が発生した場合にアプリケーションの回復力を高め、原子性、一貫性、独立性、耐久性（ACID）に準拠したストレージを提供するソリューションを探しています。これらの要件を満たすために、次のうちどのソリューションが最も適切ですか。**

A. 各アベイラビリティーゾーン（AZ）のEC2インスタンスでアプリケーションを起動し、EBSボリュームを各EC2インスタンスに接続する
B. 複数のAZにAuto Scalingグループを構成して、Application Load Balancerを作成する。各EC2インスタンスでインスタンスストアをマウントする
C. 複数のAZにAuto Scalingグループを構成して、Application Load Balancerを作成する。Amazon EFSにデータを格納し、各EC2インスタンスにターゲットをマウントする
D. 複数のAZにAuto Scalingグループを構成して、Application Load Balancerを作成する。Amazon S3の1ゾーン低頻度アクセス（One Zone-Infrequent Access）を使用してデータを保存する

➡ P47

43. **ある会社では、Webアプリケーションを構築し、そのアプリケーションから読み書きされるストレージとしてAmazon S3を利用しています。アプリケーションを利用する顧客から、古いデータが表示されることがあるという報告を受けていますが、Webアプリケーションの機能は正しく動作していることを確認しています。原因として考えられるものはどれですか。**

A. Webアプリケーションから、マルチパートアップロードでAmazon S3へ書き込みしている
B. WebアプリケーションからAmazon S3への書き込みの際に、S3上の既存のファイルを同じオブジェクトキーで上書きして更新している
C. WebアプリケーションからAmazon S3への書き込みの際に、毎回新しいオブジェクトキーでファイルを新規作成している
D. Amazon S3の暗号化機能を有効にしている

➡ P47

44. ソリューションアーキテクトであるあなたは、モバイル端末のアプリケーションから社内の業務システムにアクセスできるようAWSのアーキテクチャを設計しています。要件として、モバイル端末のアプリケーションからS3への業務データのアップロードがあります。
しかし、モバイル端末のアプリケーションが、AWS上に構築しているWebアプリケーションサーバーを中継してデータをアップロードすると、大量のトラフィックが発生することが懸念されています。
モバイル端末のアプリケーションからAmazon S3にデータをアップロードする方法として、コスト面で最も効率的かつ適切なものはどれですか。

A. Amazon S3のクロスリージョンレプリケーション機能を利用する
B. Amazon S3上の一時的な別のバケットにデータをアップロードし、完了後にAWS Lambdaの機能で適切なS3バケットにコピーする
C. 大量のトラフィックを処理できるよう、Webサーバーのインスタンスサイズを増やす
D. Amazon S3の署名付きURLを発行し、モバイル端末のアプリケーションからデータを直接アップロードする

➡ P47

45. あなたの会社にはEC2インスタンスで動作するアプリケーションがあり、IAMロールをアタッチしてAmazon DynamoDBへのアクセス制御を設定しようとしています。
アクセスするDynamoDBのテーブル名はusersで、EC2からusersテーブル内のレコード削除のみを許可したいと考えています。
最小権限の法則に従ったIAMポリシーは次のうちどれですか。

A.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "dynamodb:DeleteItem",
      "Resource": "arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/*",
    }
  ]
}
```

B.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "dynamodb:DeleteItem",
      "Resource": "arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/users",
    }
  ]
}
```

C.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/*",
    }
  ]
}
```

D.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "arn:aws:dynamodb:ap-northeast-1:xxxxxxxxxxxx:table/users",
    }
  ]
}
```

➡ P48

46. **あなたの会社では、社内に100TBの業務データを保存しているファイルサーバーを運用しています。バックアップ先としてAmazon S3 Glacierへのデータ移行を検討しています。社内のネットワーク回線への負担を軽減しつつ、コスト効果の高い移行方法として適切なものを選びなさい。**

A. S3へインターネット経由でブラウザからファイルアップロードを行う。S3上に移行されたデータをGlacierにアーカイブするライフサイクルポリシーを設定する
B. 会社とAWSのVPC間にサイト間VPNを設定し、VPN経由でブラウザからGlacierにファイルをアップロードする
C. 会社とAWSのVPC間にサイト間VPNを設定し、VPN経由でブラウザからS3にファイルをアップロードする。S3上に移行されたデータをGlacierにアーカイブするライフサイクルポリシーを設定する
D. AWS Snowballを使用し、S3バケットを移行先として設定する。S3上に移行されたデータをGlacierにアーカイブするライフサイクルポリシーを設定する

➡ P48

47. **ある企業では、古いニュース映像のビデオアーカイブをAWSに保存できるソリューションを探しています。映像データを復元する必要はほとんどありませんが、データが必要となった場合は最大でも5分以内で使用可能になることが求められ、コストは最小限に抑える必要があります。**
最も費用対効果の高いソリューションは次のうちどれですか。

A. ビデオアーカイブをAmazon S3 Glacierに保存し、Expeditedオプションを使用する
B. ビデオアーカイブをAmazon S3 Glacierに保存し、Standardオプションを使用する
C. ビデオアーカイブをAmazon S3の標準低頻度アクセス（Standard-Infrequent Access）で保存する
D. ビデオアーカイブをAmazon S3の1ゾーン低頻度アクセス（One Zone-Infrequent Access）で保存する

➡ P48

48. **あるアプリケーションは、開発環境（DEV）と本番環境（PROD）で構成されています。DEV環境のEC2インスタンスは、営業時間に毎日10時間実行されます。一方、PROD環境のEC2インスタンスは、毎日24時間実行されています。**
ソリューションアーキテクトであるあなたは、コストを最小限に抑えるためにコンピューティングインスタンスの購入戦略を決定する必要があります。次のうち、最も費用対効果の高いものはどれですか。

A. DEV環境にはスポットインスタンス、PROD環境にはオンデマンドインスタンスを使用する
B. DEV環境にはオンデマンドインスタンス、PROD環境にはスポットインスタンスを使用する
C. DEV環境にはスケジュールされたリザーブドインスタンス、PROD環境にはリザーブドインスタンスを使用する
D. DEV環境にはオンデマンドインスタンス、PROD環境にはスケジュールされたリザーブドインスタンスを使用する

➡ P49

49. **あなたの会社では、Application Load Balancerに登録されたEC2インスタンスでWebサイトを運用しており、DNSにはAmazon Route 53を使用しています。**
同社は、メインのWebサイトがダウンした場合に、ユーザーがアクセス可能なバックアップサイトを構築したいと考えています。
これらの要件を満たすソリューションは、次のうちどれが最も適切ですか。

A. バックアップサイトにAmazon S3のWebサイトホスティングを利用し、Amazon Route 53のフェイルオーバールーティングポリシーを設定する
B. バックアップサイトにAmazon S3のWebサイトホスティングを利用し、Amazon Route 53のレイテンシールーティングポリシーを設定する
C. アプリケーションを別のリージョンにデプロイし、ELBのヘルスチェックを使用してフェイルオーバールーティングを行う
D. アプリケーションを別のリージョンにデプロイし、メインサイトのサーバーサイドでリダイレクトを設定する

➡ P49

50. 米国からアクセスしているユーザーにだけ画像を配信したいと考えています。次のうち、適切な方法はどれですか。

A. NATインスタンスでIPアドレスを制限する
B. セキュリティグループを利用する
C. Amazon S3に画像ファイルを格納し、バケットポリシーを設定する
D. Amazon CloudFrontの地域制限配信を利用する
E. Amazon API Gatewayを利用する

➡ P49

51. ある会社では、インターネット向けにWebアプリケーションを構築し、サービスを運営しています。このWebアプリケーションは、Amazon Cloud Front、Application Load Balancer、EC2で構成されており、CloudFrontのオリジンサーバーとしてApplication Load Balancerを設定しています。アクセスログから、最近ある特定のIPアドレスからの悪意ある攻撃が検知されています。今後のセキュリティ対策のために、特定のIPアドレスをブロックするのはどのソリューションですか。

A. Application Load Balancer配下にあるEC2のセキュリティグループで、特定のIPアドレスからのアクセスをブロックする
B. AWS WAFをAmazon CloudFrontに設定し、WAFのIPアドレスマッチ条件を使用して特定のIPアドレスからのアクセスを遮断する
C. Application Load Balancer配下にあるEC2のネットワークACLで、特定のIPアドレスからのアクセスをブロックする
D. Amazon CloudFrontの設定で、特定のIPアドレスからのアクセスをブロックする

➡ P49

52. Auto Scalingを設定したアプリケーションAとアプリケーションBが同じサブネットで動作しています。アプリケーションAからアプリケーションBへの通信は許可しますが、アプリケーションBからアプリケーションAへの通信は拒否したい場合の設定として、正しいものはどれですか（2つ選択）。

A. アプリケーションAのセキュリティグループの設定で、アプリケーションBのIPアドレスからのインバウンド通信設定を行わない
B. アプリケーションAのセキュリティグループの設定で、アプリケーションBのIPアドレスからのインバウンド通信を拒否する
C. アプリケーションBのセキュリティグループの設定で、アプリケーションAのIPアドレス以外のアウトバウンド通信を許可する
D. サブネットに設定されたネットワークACLで、アプリケーションAのIPアドレスからのインバウンド通信を許可する
E. サブネットに設定されたネットワークACLで、アプリケーションBのIPアドレスのインバウンド通信を拒否する

➡ P50

53. ある会社では、レガシーなシステムで利用しているレガシーサーバーにおいて、独自のファイルシステムを使用したアプリケーションを運用しています。レガシーサーバーをAWSに移行する際に使用すべきストレージサービスはどれですか。

A. Amazon EBS
B. Amazon EFS
C. Amazon S3
D. Amazon S3 Glacier
E. Amazon DynamoDB

➡ P50

54. ある会社では、工場からリアルタイムでIoTデータを収集し、ディスクストレージに保存しています。収集対象のデータ量が増加し、スループットに問題が発生しています。
ソリューションアーキテクトであるあなたは、インメモリデータベースに移行することでスループットの改善を検討しています。可用性が高く、スループット向上が見込めるソリューションは次のうちどれですか。

A. Amazon RDS for PostgreSQL
B. Amazon Aurora
C. Amazon ElastiCache for Redis
D. Amazon ElastiCache for Memcached

➡ P50

55. **Amazon DynamoDB Accelerator（DAX）の説明として、適切なものはどれですか（2つ選択）。**

A. Amazon DynamoDBよりもパフォーマンスは劣るが、コスト効率のよいNoSQL型のデータベースサービスである
B. Amazon S3に格納した半構造データを一定時間ごとにAmazon DynamoDBに読み込み、S3にアクセスすることなくS3内のデータを扱うことができるサービスである
C. Amazon DynamoDBのインメモリキャッシュサービスである
D. 1秒あたり100万回単位のリクエスト処理でも、数ミリ秒のレイテンシーを実現できる
E. フルマネージド型のサービスであるAmazon DynamoDBのスケーリングルールを設定できる機能である

➡ P51

56. **セキュリティチームに属しているあなたは、会社が所有しているすべてのAWSアカウントで特定のサービスまたはアクションへのアクセスを制限することを検討しています。すべてのAWSアカウントは、AWS Organizationsの組織で構成されています。アクセス許可を設定する箇所は単一である必要があり、かつスケーラブルである必要があります。これらの要件を満たす方法として適切なものはどれですか。**

A. ACLを作成し、サービスまたはアクションへのアクセスを制限する
B. アカウントを許可するセキュリティグループを作成し、ユーザーグループにアタッチする
C. 各アカウントにクロスアカウントロールを作成して、サービスまたはアクションへのアクセスを拒否する
D. サービスまたはアクションへのアクセスを拒否するために、ルート組織単位でサービスコントロールポリシーを作成する

➡ P51

57. **AWSをセキュアに利用するためのサービスや利用方法に関する説明として、誤っているものはどれですか。**

A. すでにS3に保存しているオブジェクトをAWS KMSのキーを利用して暗号化することができる
B. AWS KMSでは作成した鍵の管理は可能だが、鍵の無効化や削除はできない
C. AWS CloudHSMは、AWSのデータセンター内に配置されるユーザー占有のハードウェアアプライアンスである
D. AWS CloudHSMは、セキュリティコンプライアンス要件が厳しい場合に適用する

➡ P51

58. **ある会社では、月次の出勤管理簿データをPDFファイルでS3バケットに保存しています。総務部は、前月分の出勤管理簿データに頻繁にアクセスします。前月分より過去の出勤管理簿データにはあまりアクセスしませんが、必要に応じてすぐにデータを取得する必要があります。**
この会社には多くの従業員がいるため、S3バケットのデータ保存にかかるコストの削減を検討しています。
出勤管理簿データをS3バケットに保存する方法として、費用対効果が高く耐久性も損なわないものはどれですか。

A. 過去の出勤管理簿データを定期的にAmazon S3 Glacierに手動でアーカイブする
B. Amazon S3のライフサイクルルールの設定により、前月分より過去のデータを標準低頻度アクセス（Standard-Infrequent Access）に移行する
C. Amazon S3のライフサイクルルールの設定により、前月分より過去のデータを1ゾーン低頻度アクセス（One Zone-Infrequent Access）に移行する
D. 出勤管理簿データをバイナリ変換してAmazon RDSに保存する

➡ P52

59. あなたの会社は、Webサービスを運用しています。Webアプリケーションサーバーは、VPC内のプライベートサブネットに配置されたデータベースへ接続しています。
ソリューションアーキテクトであるあなたは、セキュリティ強化のために、以下のセキュリティ要件に従い設計を行う必要があります。

・Webアプリケーションサーバーは、インターネットからのSSL（HTTPS接続）を受け付ける
・データベースサーバーは、Webアプリケーションサーバーからの接続のみ受け付ける

運用中のサービスへの影響を最小限にするセキュリティ設定はどれですか。（2つ選択）

A. ネットワークACLで、Webアプリケーションサーバーのサブネットに対し、HTTPS接続のインバウンド通信をすべて許可、アウトバウンド通信をすべて拒否する
B. セキュリティグループで、データベースサーバーの接続ポートを開放し、Webアプリケーションサーバーのセキュリティグループからの接続のみ許可する
C. データベースサーバーを、Webアプリケーションサーバーと同じサブネットに再配置する
D. ネットワークACLで、プライベートサブネットに対し、データベースサーバーの接続ポートへのインバウンド通信をすべて許可、アウトバウンド通信をすべて拒否する
E. セキュリティグループで、WebアプリケーションサーバーのHTTPSポートを開放し、インターネット（0.0.0.0/0）からの接続を許可する

➡ P52

60. EC2インスタンスとAmazon DynamoDBを利用してアプリケーションを開発し、利用者にサービス提供している企業があります。
あるとき、このアプリケーションを利用している複数のユーザーから、削除したはずのデータが表示されてしまうことがあると相談を受けました。
あなたが行うべき対策として適切なものはどれですか。

A. Amazon DynamoDBグローバルテーブルを利用する
B. Amazon DynamoDBストリームを利用する
C. キャパシティモードはオンデマンドを選択する
D. Consistent Readの設定を有効にする

➡ P52

61. プライベートサブネット内のEC2インスタンスから、インターネットへのIPv6トラフィックを確立する必要があります。また、自動的にスケールされ、かつ追加費用が発生しないようにしなければなりません。
次のうち、この要件を満たすサービスはどれですか。

A. Egress-Onlyインターネットゲートウェイ
B. NATゲートウェイ
C. カスタムNATインスタンス
D. VPCエンドポイント

➡ P53

62. プライベートサブネット内のEC2インスタンスからインターネットを経由せずにAmazon S3を利用する適切な方法は、次のうちどれですか。

A. EC2インスタンス用のVPCエンドポイントを作成し、ルートテーブルにAmazon S3のターゲットを設定する
B. EC2インスタンス用のVPCエンドポイントインターフェイスを作成する
C. Amazon S3用のVPCエンドポイントを作成し、ルートテーブルにAmazon S3のターゲットを設定する
D. Amazon S3用のVPCエンドポイントインターフェイスを作成する

➡ P53

63. ある企業が全国テレビキャンペーンを実施しています。同社では、このキャンペーンによって、毎分5件のリクエストから毎分5,000件以上のリクエストにトラフィックが増加すると予想しています。システムは、Node.jsで動作するアプリケーションです。トラフィック急増を確実に処理するための適切なサービスもしくは方法は、次のうちどれですか。

A. AWS Lambda
B. Amazon ElastiCache
C. 想定の負荷を処理できる数のEC2インスタンスを用意する
D. Auto Scalingグループを作成し、EC2インスタンスをスケールアウトする

➡ P53

64. あなたは、常時アクセス可能な社内の共有ファイルシステムを設計しています。チームごとにそれぞれ独立したディレクトリを持ち、ユーザーは自分のチームが所有するファイルだけにアクセスできるようにファイルを保護したいと考えています。
次のうち適切な設計方針はどれですか。

A. Amazon EFSを利用し、ファイル単位でアクセス制御を行う
B. Amazon S3を利用し、ACLによるアクセス制御を行う
C. Amazon S3を利用し、IAMによるアクセス制御を行う
D. Amazon EFSを利用し、セキュリティグループによるアクセス制御を行う

➡ P54

65. あなたは、アジア各国に支社がある企業の本社で情報システム部門に所属しています。
同社の経営会議では、毎日Redshiftに蓄積される業務データを用いて打ち合わせが行われるため、あなたは前日分データの分析結果を準備しています。この分析には多くのクエリを実行する必要がありますが、通常は各支社がデータを格納し、そのデータを分析するには十分な時間があります。また、時差があるので、Redshiftのクエリ処理も問題なく実行できています。しかし、支社の状況によっては、まれにAmazon Redshiftへのデータ格納が遅くなることがあります。
このような場合でも確実に分析結果を提供する必要があるため、Redshiftのクエリ数が多くなった場合に、その処理数に応じてスケールして処理されるよう対応したいと考えています。
次のうち、適切なソリューションはどれですか。

A. 処理待ちのクエリをSQSに格納する
B. クロスリージョンスナップショットを利用する
C. ノード数を増やす
D. Redshift concurrency scalingを有効にする

➡ P54

解答

1. C

➡ P2

この問題では、Windowsサーバーによるファイル共有の仕組みを移行する場合に適切なAWSサービスの選択が求められています。

Amazon FSx for Windowsは、Windowsファイル共有で標準的に用いられる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サービスです。Windows Server上に構築されており、クォータ機能やMicrosoft Active Directory統合など、Windows Server標準の幅広い管理機能を提供します。したがって、**C**が正解です。

A. Amazon EFSはNFSの機能を提供しており、複数のEC2インスタンスから利用できますが、設問の要件には合いません。
B. Amazon S3は、オブジェクトストレージサービスです。
D. Amazon EBSは永続可能なブロックストレージサービスで、EC2インスタンスにアタッチすることで利用できます。
E. Amazon FSx for Lustreは、高性能ファイルシステムであるLustreファイルシステムをフルマネージド型で利用できるサービスです。

2. A

➡ P2

設問では、フロントエンド処理とバックエンド処理の連携方法が問われています。Amazon SQSを利用することで、大量の処理や時間がかかる処理を行う必要がある場合でも、フロントエンド処理からの依頼をSQSでキューイングし、バックエンドへ処理を連携かつ並列化することができます。したがって、**A**が正解です。

B. Amazon SNSはメッセージ通知サービスですが、マイクロサービス間での処理連携としては適切な用途ではありません。
C. Amazon S3はオブジェクトストレージサービスです。
D. Amazon EFSは、EC2インスタンス間でファイル共有を提供するサービスですが、処理の連携という観点では適切ではありません。

3. A

➡ P3

多数の読み取りや書き込み性能が求められるデータベースには、一般的に低レイテンシーかつ高スループットな性能を実現できるストレージタイプを選択する必要があります。

プロビジョンドIOPS SSDは最もパフォーマンスが高く、ミッションクリティカルなデータベースなどで利用されるケースが多いです（**A**）。
スループット最適化HDDは、スループットが高く低コストなHDDです。ビッグデータの格納やログ処理など、アクセス頻度が高いデータの格納に適しています（B）。
コールドHDDは、アクセス頻度の低い大量のデータを格納するのに適しています（C）。コスト効果を高めたい場合にも適しています。
汎用SSDは、価格とパフォーマンスのバランスのよいEBSストレージタイプです（D）。

4. B

➡ P3

プレイスメントグループとは、EC2インスタンスを論理的にグループ化したものです。
プレイスメントグループの機能を利用してグループ化すると、そのグループ化したEC2インスタンス間での通信は、通常のEC2インスタンス間通信よりもさらに高速になります。
クラスタープレイスメントグループは、EC2インスタンスを同じラックに配置することで、インスタンス間の通信を高速に行えるため、低レイテンシーかつ高スループットなネットワークが求められるアプリケーションに適しています。したがって、**B**が正解です。

A. AWS Auto Scalingは、自動スケーリングと予測スケーリングの機能を持つサービスです。
C. パーティションプレイスメントグループは、EC2インスタンスをパーティション単位で異なるラックに配置します。分散処理に適しています。
D. スプレッドプレイスメントグループは、すべてのEC2インスタンスを異なるラックに配置します。障害発生時の影響を低減したいシステムに適しています。

5. A、D

➡ P3

Amazon S3を利用することで、外部へのファイルの公開が簡単に行えますが、適切に設定しなければ想定していないユーザーからのアクセスを許してしまうことになります。
S3には、パブリックアクセスというアクセス制御機能があります。不特定多数のユーザーへのファイル公開が不要な場合は、この権限を設定しないようにします（**D**）。S3で適切な権限を設定することで、セキュアに特定のユーザーにファイルへのアクセスを許可することが可能です。
また、有効期限付きの署名付きURLを使用することで、このURLを通知したユーザーにだけ一定時間ファイルのダウンロードを許可することができます（**A**）。
会員の増減に合わせてアクセス元IPアドレスを管理することは運用上難しく、現実的な対応ではありません（C）。

6. D

➡ P4

VPCエンドポイントは、Amazon S3やAmazon DynamoDBへアクセスする際にインターネットを経由せず、AWS内のプライベート接続を実現するサービスです。指定されたルートへのターゲットをルートテーブルに設定することで利用できます。したがって、**D**が正解です。

A. VPCピアリングは、異なるVPC間をプライベート接続するサービスで、AWSサービスへの接続経路を作るものではありません。
B. AWS Direct Connectは、オンプレミス環境とAWSの間を専用線で接続するサービスなので、AWSサービスへの接続経路を作るものではありません。
C. NATゲートウェイは、プライベートサブネットのEC2インスタンスからインターネットへ接続するためのNATサービスです。AWSサービスへの経路を作ることはできますが、インターネット経由となってしまいます。

7. C

➡ P4

Amazon Auroraは、マネージド型のリレーショナルデータベースサービスであるAmazon RDSがサポートしているデータベースエンジンのひとつです。頻繁にデータの更新・削除が行われるデータベースに向いており、SQLを発行して複数のテーブルを結合し、結合したテーブルから対象のデータを取得することもできます。また、Auroraはフルマネージド型のデータベースサービスであるため、データ量に応じてストレージを自動拡張する機能も備えています（**C**）。
RDSでは、AuroraのほかにMySQLやPostgreSQLなどのデータベースもサポートしています。
Amazon DynamoDBはNoSQLデータベースサービスで、キーとなるIDを指定することでデータベースに格納されているバリューを取得します。一般的なリレーショナルデータベースのようにSQLを利用したデータの取り出しはできません（A）。
Amazon S3 Glacierは、長期的にアーカイブを格納するのに優れたオブジェクトストレージです（B）。
Amazon Redshiftは列指向のアーキテクチャを持ち、大量データの集計・分析に適したデータウェアハウスサービスです（D）。
Amazon S3は、大容量のデータを格納できる耐久性の高いオブジェクトストレージサービスです（E）。

8. A、E

➡ P5

この問題では、今後、アクセス増加が見込まれているアプリケーションのパフォーマンスをどのように向上させるかを考える必要があります。
EC2はインスタンスタイプが決まっており、アクセス負荷に応じて都度調整する

必要があります。このため、S3を利用したほうがアクセス増加にも適切に対応できると考えられます（**A**）。
このアプリケーションはひとつのリージョンにしかホストされていないため、Amazon Route 53の位置情報ルーティングを利用する効果はないと考えられます（B）。
AWS CloudTrailはAWSアカウントで利用された操作（APIコール）のログを取得するため、アプリケーションのアクセス負荷をモニタリングすることはできません（C）。
Elastic Load Balancer（ELB）は、通信トラフィックの負荷に応じて自動でスケーリングする機能を備えており、ELB自体にも冗長性が確保されているため、マイクロサービス専用のELBを用意する必要はありません（D）。
RDSのリードレプリカを用意することで、読み取りスループットを増やし、パフォーマンスを向上させることができます（**E**）。

9. C、D

➡ P5

Amazon Route 53のエイリアスは、Elastic Load Balancing（ELB）やAmazon CloudFrontに対してZone Apexレコードを設定することが可能です。Amazon Route 53、Amazon S3、ELB、CloudFrontはいずれもAWSのマネージドサービスであり、これらを組み合わせて静的Webサイトを構成することで負荷に応じた費用対効果の高いスケーラビリティが実現できます（**C**、**D**）。
EC2インスタンスのパブリックIPアドレス（A）やCloudFormationスタック（B）に対して紐付けすることはできません。

10 B、E

➡ P6

設問の2層Webアプリケーションは、アプリケーション層、データベース層とも単一のアベイラビリティーゾーン（AZ）で動作するEC2インスタンス上で実行されています。設問で問われている「高可用性を実現する」ためには、地理的に離れた冗長化を行うことがポイントです。

複数のAZにまたがるEC2インスタンスのAuto Scalingを実行することで、地理的に離れた冗長化を実現できます。また、Application Load Balancer（ALB）を組み合わせることで、EC2インスタンスに障害が発生しても通信を適切に振り分けることができます（**B**）。
また、データベース層をAmazon RDSのマルチAZ配置にすることで、AZをまたぐ地理的に離れた冗長化を実現でき、障害が発生しても自動で切り替わるため、高可用性を実現することができます（**E**）。

A. 同じAZにサブネットを作成しても、AZをまたぐ地理的に離れた冗長化を行う

ことができません。

C. 既存のWebアプリケーションは単一のAZで実行されているため、ALBを組み合わせても、AZをまたいでの冗長化を行うことはできません。

D. 別のAZに新しいサブネットを作ったとしても、EC2インスタンスが単一のAZで稼働しているのでは高可用性を実現することはできません。

11. D

➡ P6

AWSには、CloudFrontというCDN（Content Delivery Network、コンテンツ配信ネットワーク）サービスがあります。このサービスを利用することで、画像・動画などのコンテンツを安全かつ高速に配信することが可能となります。

CloudFrontは、設問にあるような静的コンテンツである画像ファイルだけでなく、動画ファイルなどのWebコンテンツもキャッシュすることができます。また、画像ファイルをAmazon S3に格納することでコストを抑えることができます（**D**）。

12. C

➡ P7

複数のアプリケーションの総データ量が非常に多いため、AWS Direct Connectでは初回のデータ移行が1カ月以内に間に合わない可能性があります（A）。

Site to Site VPNでも同様に、初回のデータ移行が1か月以内に間に合わない可能性があるうえ、移行後も安定したスループットを維持することは難しいと考えられます（B）。

一度に大量のデータをAWSへ転送する手段として、AWS Snowballは非常に有効です。移行後も、Direct Connectであれば安全かつ安定したスループットを維持することが期待できますが（**C**）、Site to Site VPNでは安定したスループットを維持することは難しいと考えられます（D）。

13. C

➡ P7

クールダウンを設定することで、コストを適切に管理することができるかもしれませんが、EC2インスタンスを最低4台維持し続けるための機能ではないため、SLAを維持することはできません（A）。

インスタンスタイプを変更することはパフォーマンスを最適化するための方法であり、SLAを維持することとは関係ありません（B）。

3つのアベイラビリティーゾーン（AZ）で合計6台EC2インスタンスが稼働していることから、ひとつのAZあたり2台稼働していることがわかります。ひとつのAZに障害が発生しても、残りの2つのAZで最低4台で稼働することができます（**C**）。

2つのAZで合計8台EC2インスタンスが稼働していることから、ひとつのAZあたり4台稼働していることがわかります。ひとつのAZに障害が発生しても残りのAZで最低4台で稼働することができますが、通常稼動時は8台稼働することになり、C

の6台よりもコストが高くなってしまうため、適切ではありません（D）。

14. A、D

➡ P8

EC2インスタンスからAmazon DynamoDBを利用するには、利用する機能に応じた権限が必要です。
設問の場合は、EC2インスタンスからDynamoDBに書き込みを行うため、EC2インスタンスに対してDynamoDBへの書き込みを可能にするIAMロールを作成します（**A**）。
Auto Scalingを使用する場合は、起動設定で上記のIAMロールを設定します（**D**）。

15. D

➡ P8

Amazon Kinesisは、リアルタイムに流れてくる大量のデータを処理するサービスです。
KinesisのサービスのひとつであるAmazon Kinesis Data Streamsでは、ストリーミングデータをほぼリアルタイムで収集でき、収集されたデータはAmazon Kinesis Data FirehoseによってAmazon S3やAmazon RDSなどに保存ができます。加えて、Amazon Kinesis Data Analyticsと連携すると、ストリーミングデータに対してSQLクエリを実行し、リアルタイム分析が行えます。したがって、**D**が正解です。
Amazon SQSやAmazon SNSで疎結合なアーキテクチャに構成することはできますが、リアルタイム処理やSQL分析についてはKinesisが向いています（A、B）。
Amazon Athenaに保存したあとに分析を行うこともできますが、リアルタイム性の要件を加味するとKinesisが向いています（C）。

16. D

➡ P9

Amazon CloudFrontは、「エッジロケーション」と呼ばれるグローバルに点在する拠点からコンテンツを配信するCDNサービスです。高可用性、高パフォーマンス、低レイテンシーなネットワークを備えています。
CloudFrontの署名付きURLを利用すると、ユーザーはコンテンツのダウンロードやストリーミング配信ができます。
その他の方法でも動画配信は可能ですが、設問の「アクセスする地域に関係なく、アクセスから再生までの時間を短縮する」ことに最も適した方法は**D**となります。

17. B、C

➡ P9

Amazon RDSのリードレプリカとは、マスターデータベースと同じデータベースを複製し、読み取り専用として構築したものです。リードレプリカを利用することで、読み取り頻度の高いデータベースを増設できるため、読み取りスループットを増やし、パフォーマンスを向上させることができます（**B**）。
Amazon ElastiCacheはマネージド型のインメモリデータベースです。メモリ上で処理を実行するため、データをキャッシュすることで、データベースの負荷軽減を実現します（**C**）。

18. D

➡ P9

Amazon Auroraはマネージド型のリレーショナルデータベース（RDB）サービスです（A、E）。
MySQLの5倍、PostgreSQLの3倍のスループットを実現しているといわれています（B）。データは3カ所のアベイラビリティーゾーン（AZ）に格納されます（C）。
Auroraは、一般的なRDBと同様の行指向のリレーショナルデータベースサービスです。列指向のアーキテクチャを持ち、大量データの集計・分析に向いているサービスはAmazon Redshiftです（**D**）。

19. D

➡ P10

ノード数を増やすと複数のデータベースがクラスター化され、耐障害性が高まります（**D**）。
より性能の高いインスタンスタイプに変更すると処理性能は向上しますが、冗長性を高めることにはなりません（A）。
クロスリージョンスナップショットにより別のリージョンへのバックアップができますが、冗長性を高めることにはなりません（B）。
マルチAZは、Amazon Redshiftでは設定することができません（C）。

20. B

➡ P10

インターネットゲートウェイはVPC内のリソースからインターネットへアクセスするためのゲートウェイで、アクセス制御を行うためのものではありません（A）。
ネットワークACLはVPC内に構成されたサブネットに対するファイアウォール機能で、特定のIPアドレスからのアクセスを制御することができます（**B**）。
AWS Direct Connectは、オンプレミス環境とAWSの間を専用線で接続するサービスです（C）。
Amazon API Gatewayは、APIの作成、配布、保守、監視、保護を簡単に行えるサービスで、アクセス制御を行うためのものではありません（D）。

21. E ➡ P10

Amazon S3の署名付きURLとは、S3上のデータに対して一定時間だけアクセスを許可するためのURLを発行する機能です。この機能を利用することで、Webサーバーを経由せずに直接S3にファイルを格納することができます（**E**）。

22. A ➡ P11

NATゲートウェイには、プライベートサブネットからインターネットへ接続するためのNAT機能があります。この機能を使うことにより、設問のケースに対応できます（**A**）。
プレイスメントグループは単一のアベイラビリティーゾーン（AZ）内のEC2インスタンスを論理的にグルーピングしたものです。同じAZ内に配置されたEC2インスタンスをグループ化できるため、異なるAZ間や異なるリージョン間の通信よりも高速な処理が可能となりますが、設問のシステム要件は満たしません（B）。
Elastic IPは、固定のグローバルIPアドレスを提供するサービスです。固定のパブリックIPを割り当てるだけではインターネットへ接続できません（C）。
ネットワークACLでインターネットからの通信トラフィックを許可するのはインバウンドのルールであるため、データベースサーバーから外部のインターネットへ接続するための要件ではありません。

23. C ➡ P11

設問のケースでは毎日7時間だけ稼働すればよいため、Standardタイプのリザーブドインスタンスと Convertibleタイプのリザーブドインスタンスは適切ではありません（A、B）。
また、高可用性は求められていないものの7時間は稼働を要求されているため、スポットインスタンスも適切ではありません（D）。
スケジュールされたリザーブドインスタンスは、予約した時間枠内で起動できる購入オプションで、インスタンスがスケジュールされた時間に対して課金されます（**C**）。非営業日に実行するバッチ処理など、継続的に行う必要がなく、定期的な処理を行う際に適しています。したがって、毎日7時間だけ稼働する設問のシステムでは適切な購入オプションといえます。

24. C ➡ P12

異なるアベイラビリティーゾーン（AZ）やリージョンにデータベースを配置することで業務継続性は向上しますが、EC2インスタンスでデータベースを冗長化構成する場合はクラスタリングの仕組みを導入する必要があり、構成を大きく見直す必要があると考えられます（A、B）。
設問のケースでは、Amazon RDSのマルチAZによる耐障害性の向上、およびリー

ドレプリカによる読み取りスループットの向上が見込めます（**C**）。
RDSではスタンバイデータベースを構成する機能がありません（D）。

25. B

➡ P12

基幹システムで実行するバッチ処理は、インスタンスを常時起動する必要があるため、リザーブドインスタンスが適切です。
一方、非基幹システムで実行するバッチ処理は、処理が中断したとしても業務に直接影響しないため、最もコストが低いスポットインスタンスが適切です。
したがって、**B**が正解です。

26. A

➡ P13

AWS Snowballでは、AWSから発送されたSnowball筐体に移行データを保存し、筐体をAWSへ返送すると、データの移行はAWSが行ってくれます。設問のようにネットワーク帯域が制限される場合、大量のデータを移行するのに最適です。したがって、**A**が正解です。

B. AWS DataSyncはネットワーク経由でデータを転送するため、制限されたネットワーク帯域で期限内にデータを移行することは困難と考えられます。
C. AWS Storage Gatewayでは、サーバーとAmazon S3がローカルで接続されているように見えますが、実際にはネットワークを経由してデータ転送を行っています。そのため、ネットワーク帯域が制限されている中、期限内にデータ転送することは困難と考えられます。
D. Amazon S3 Transfer Accelerationは、エッジロケーションを利用してS3へのデータ転送を最適化するサービスです。データ転送には、インターネットを経由する必要があり、ネットワーク帯域が制限されている中、期限内にデータを移行することは困難と考えられます。

27. B

➡ P13

IAMロールはホワイトリスト形式で権限を付与できますが、IAMのサービスだけで問題の要件に合致する仕組みを実装することはできません（A）。
Amazon API Gatewayのカスタム認証の中でLambdaと連携することができるため、条件に応じてアクセスを許可あるいは拒否するプログラムを実行できます（**B**）。
Cognitoユーザープールを利用した認証では、ユーザーアカウントをロックする機能はありますが、問題の要件に合致する仕組みを実装することはできません（C、D）。Cognitoユーザープールの詳細は、下記のWebページを参照してください。
https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/what-is-amazon-cognito.html

28. D

➡ P14

設問のケースでは、非リレーショナルデータベースによるデータ蓄積、負荷の増減に自動で対応が可能なことが求められています。
データ蓄積に関しては、マネージド型NoSQLデータベースサービス「Amazon DynamoDB」が適しています。負荷分散に関しては、低レイテンシーで高いスループットを実現するロードバランシングサービス「Network Load Balancer」が適しています。したがって、**D**が正解です。

Amazon Auroraは、リレーショナルデータベースサービスであるため、非リレーショナルデータベースが求められる設問のケースでは適していません（A、C）。
Amazon Route53では、DNSフェールオーバー機能で障害発生時にサーバーの切り替えができますが、設問のケースには適していません（B）。

29. C

➡ P14

EBSは、ボリュームタイプによってパフォーマンス特性が異なります。
設問のようにIOPSが50000を超えるボリュームタイプは、プロビジョンドIOPS SSDのio1またはio2のみとなります。ただし、Nitro Systemを選択した場合のみ、最大64000 IOPSとなります。プロビジョンドIOPS SSDを選択しても、Nitro System以外の場合は最大32000 IOPSとなります。
したがって、**C**が正解です。

30. B

➡ P15

Amazon Kinesisは、リアルタイムに流れてくる大量のデータを処理するサービスです。
Amazon Kinesis Data Streamsは、ストリーミングデータをほぼリアルタイムで保存することができ、登録されたデータはAmazon EMRやLambdaなどのサービス上に構築された独自アプリケーションで処理することが可能です（A）。
Amazon Kinesis Data Firehoseは、独自にアプリケーションを構築することなく、ストリームデータをAmazonの各サービス（S3やRedshift、Elasticsearch Service）に簡単に配信・保存できるサービスです（**B**）。
Amazon Kinesis Data Analyticsは、ストリーミングデータに対してSQLクエリを実行し、リアルタイム分析を行うサービスです（C）。
Amazon SQSは、メッセージキュー（MQ）のマネージドサービスです（D）。
Amazon SNSは、AWSで提供されるメッセージ通知サービスです（E）。

31. D

➡ P15

EC2インスタンスのメモリサイズを増やすことでEC2インスタンスの処理性能向上は見込めますが、外部サービスの呼び出しがボトルネックであると考えられ、EC2インスタンスの処理がボトルネックとなっているわけではないため適切ではありません（A）。

Amazon SQSによる非同期処理でワーカーを分割しても、外部サービスの呼び出しがボトルネックであると考えられるため適切ではありません（B）。

Elastic Load Balancer（ELB）のアイドルタイムアウト時間を増やしてもレイテンシーを抑えることはできません（C）。

事前にAmazon ElastiCacheへ外部サービスからの応答をキャッシュしておくことで、ボトルネックとなっている外部サービスへの呼び出しが不要となり、性能の向上が期待できます（**D**）。

32. C

➡ P16

A. Lambda@Edgeはエッジロケーションからコードを実行するサービスですが、EC2インスタンスをオリジンとした静的コンテンツ配信の高可用性には寄与しません。

B. CloudFrontでは、S3の機能であるTransfer Accelerationを利用することはできません。

C. オリジングループに対し、EC2インスタンスがオリジンとなっているものを複数設定することで、オリジングループ内でフェイルオーバーの設定を行うことが可能です。

D. 同じアベイラビリティーゾーン（AZ）にEC2インスタンスを配置しても、アベイラビリティーゾーン障害が発生した場合はオリジンであるEC2インスタンスへアクセスできないため、高可用性を実現する構成とはいえません。

したがって、**C**が正解です。

33. D

➡ P16

Amazon DynamoDBグローバルテーブルは、複数リージョンに配置しているデータベーステーブルでデータの整合性を取るフルマネージド型のソリューションです。

DynamoDBグローバルテーブルでは、リードレプリカのようにひとつがマスターテーブルで、そのデータをほかのレプリカテーブルに同期しているわけではありません。すべてのテーブルがマスターテーブルのため、どのリージョンのテーブルに対してデータ変更をしても、他リージョンのテーブルに対して同期が行われます。

通常、データの新規書き込みや更新処理は1秒以内に行われ、その他の分散されたテーブルに反映されます。ほぼ同時に更新処理が発生し競合が発生することもありますが、その場合は最後に更新された内容が反映されます。
したがって、**D**が正解です。A、B、Cともに、設問の要望を満たす機能はありません。

A. Amazon ElastiCacheは、キーバリュー型のNoSQLデータベースサービスです。一般的にRDSのパフォーマンス向上のために利用されるものです。
B. Amazon Redshiftは、ペタバイトクラスのデータを扱うことができるマネージド型のデータウェアハウスサービスです。コンピュータノードを増やすことでデータを分散するため、大量データの集計・分析に適しています。
C. Amazon Auroraのリードレプリカは、マスターデータベースと同じデータベースを複製し、読み取り専用として構築します。データ読み取り処理のパフォーマンスを上げるために利用されます。

34. B、D ➡ P17

本設問を解く上で、Amazon S3にEBSボリュームそのものを保管することができない点を押さえておく必要があります。EBSボリュームのデータをS3に保管するためには、EBSスナップショットを用います。

広域災害への対応として、EC2インスタンス上のアプリケーションを別リージョンで起動するためには、アプリケーション情報が保存されたAmazon Machine Image（AMI）が必要です（**B**）。情報を保存したAMIを別リージョンへコピーするためには、AMIをコピーする際に宛先リージョンを指定する必要があります（**D**）。

A. C.　前述のとおり、EBSボリュームはスナップショットとしてS3へ保管することはできますが、EBSボリューム自体をS3へコピーすることはできません。
E. EBSスナップショットをリージョン間でコピーすることは可能ですが、S3を介してEBSボリューム自体をコピーすることはできません。

35. C、E ➡ P17

このシステムは、すでに複数のEC2インスタンスで構成されており、単にEC2インスタンスを増やすだけでは可用性を向上させることはできないと考えられます（A）。
EC2インスタンスを減らすことで、費用は下がるかもしれませんが、可用性も下がる可能性があります（B）。
レイヤー4で通信を行うシステムであるため、Network Load Balancerを構成することで現在構築されている複数のEC2インスタンスの可用性を向上させることが見込めます（**C**）。

Application Load Balancerは、レイヤー7で通信を行うロードバランサーであるため、このシステムにおいて適切ではないと考えられます（D）。
複数のアベイラビリティーゾーンにEC2インスタンスを展開することで可用性の向上が見込まれ、かつAuto Scalingで費用対効果を高めることができます（**E**）。

36. B、C

➡ P18

Elastic Load Balancing（ELB）のClassic Load Balancerは、リクエストをバックエンドインスタンスへ振り分けますが、コンテンツベースで振り分けることはできません（A）。
リバースプロキシサーバーとWebサーバーにAuto Scalingを追加することで、負荷の状況に応じて自動でスケールアウト・スケールインを行うことができるため、最もスケーラブルで費用対効果が高い方法といえます（**B**、**C**）。
t2のインスタンスタイプはバーストすることで性能の向上が可能ですが、あくまでもスケールアップでしかないため、スケーラブルであるとはいいにくいと考えられます（D）。
ELBのApplication Load Balancerはコンテンツベースでの振り分けが可能ですが、振り分けを行っているのはリバースプロキシであるため、リバースプロキシに対して何かしら改善する必要があります（E）。

37. D

➡ P18

AuroraのAuto Scalingによって、リソースの使用状況をモニタリングし、その使用状況に応じてRDSデータベースインスタンスを自動で増減することができます（**D**）。
EC2でもAuto Scalingが可能ですが、RDSの負荷軽減にはなりません（A）。
Amazon DynamoDBはNoSQL型のデータベースであるため、リレーショナル型データベースであるRDSデータベースの置き換えにはなりません（B、C）。
あらかじめ複数のRDSインスタンスを作成しておいてもコスト的にメリットがありません（E）。

38. D

➡ P19

Amazon EFSは、NFSでアクセスを行うため、Windowsの共有ファイルストレージとして利用することはできません（A）。
AWS Storage Gatewayサービスの機能だけで、2つのアベイラビリティーゾーン（AZ）にインスタンスを構成することはできません（B）。
Amazon S3は、Windowsサーバーにマウントする機能を標準で備えていません（C）。
Amazon FSx for Windowsは、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で、オンプレミスのActive DirectoryやAWS Managed Microsoft ADと統合してアクセス制御を行うことができます（**D**）。

39. A、C

➡ P19

AWSアカウント作成直後に、すべての管理者権限を持つルートアカウントを保護するため、セキュリティ対策を行います。
通常は、パスワードを複雑なものに変更する（**C**）、あるいはログイン時の多要素認証（MFA：Multi-Factor Authentication）を有効化することで、なりすましなどによるアカウント乗っ取りのリスクを低減します。

40. C

➡ P20

データベースをAmazon Auroraに移行することで、運用コストやキャパシティ計画の問題は解決できますが、アプリケーションを実行しているコンテナ側も同様の対策を行う必要があります（A）。
WebアプリケーションをEC2インスタンスでホストしても、マネージドサービスを利用するわけではないので、メンテナンスやキャパシティ計画を行う必要はあるため、問題を解決することにはつながりません（B）。
Amazon CloudFrontを利用してコンテンツをエッジロケーションにキャッシュすることで、スケーラブルにコンテンツ配信ができます。また、CloudFrontはマネージドサービスであるため、コンテナのような運用コストもかかることはありません（**C**）。
データベースのクエリをAmazon ElastiCacheにキャッシュすることで、データベースアクセスに対するパフォーマンス向上は見込めますが、運用すべきリソースが増えてしまい、運用コストを下げることは難しいと考えられます（D）。

41. A

➡ P20

Amazon S3でバケットのオブジェクトを暗号化する方法には、以下の3種類があります。

- S3のデフォルトキーを使用したAES-256暗号化
- AWS Key Management Service（AWS KMS）で管理されている鍵によるAES-256暗号化
- ユーザーの任意の鍵によるAES-256暗号化

問題では暗号化鍵の自動ローテーションや、暗号化鍵の使用状況の可視化・証跡管理、鍵の権限管理が要件となっています。AWS KMSを利用した暗号化でこれらの機能を実現できるため、**A**が正解です。

S3が管理するデフォルトキーでは、自動ローテーションなどはAWS側で自動的に実施しますが、キーの証跡管理や権限管理はできません（B、C）。

ユーザーの任意の暗号化鍵を使用する場合は、ユーザー自身でローテーションなどの管理を行う必要があります（D）。

42. C

➡ P21

EBSはアベイラビリティーゾーン（AZ）をまたいでの共有ができないため、クラスタリングソフトウェアなどでレプリケーションする必要がありますが、障害が発生した場合はACIDに準拠することは難しいと考えられます（A）。
インスタンスストアは揮発性のディスクであるため、EC2インスタンス停止時にデータが消失するため不適切です（B）。
EFSは高可用のストレージサービスで、複数のEC2インスタンスから利用できます。また、強力な一貫性を持っているため適切なストレージと考えられます（**C**）。
Amazon S3は、データの結果整合性モデルを採用しているため、データの一貫性を担保することができません（D）。

43. B

➡ P21

Amazon S3では、更新時（PUT）または削除時（DELETE）に結果整合性モデルが採用されており、参照するタイミングによっては古いデータを参照する場合があります。したがって、**B**が正解です。

A. マルチパートアップロードは、大容量のオブジェクトを複数のパートに分割してアップロードすることで、効率よくS3へ転送する仕組みです。
C. 新規作成の場合は、結果整合性モデルではなく、データ保存後、S3から完了（HTTP200応答）が返されるとデータが参照できるようになり、データの一貫性が保証されます。
D. 暗号化機能の有効または無効は、原因にはなりません。

44. D

➡ P22

Amazon S3では、AWS CLIやAWS SDKを利用して、署名付きURLを発行することができます。
署名付きURLとは、S3に対して一定時間だけアクセスを許可するためのURLを発行する機能で、S3上のデータに対し、AWSにログインしていないユーザーやアプリケーションから、直接参照や書き込みなどのアクセスをさせることができます。アクセス可能な時間は自由に決めることができるため、セキュアなファイルの送受信が可能です。したがって、**D**が正解です。

A. S3に保存したデータはデフォルトで同一リージョン内の3カ所のAZへ自動的に複製されますが、クロスリージョンレプリケーションを有効化することで、別

のリージョンのS3バケットにオブジェクトを自動的に複製します。S3の耐障害性に関する機能のため、適切ではありません。

B. Webサーバーを中継して大量のトラフィックが発生する点が解決されないため、適切ではありません。

C. Webサーバーのインスタンスサイズを増やすことによりコスト増加が見込まれるため、このケースでは効率的な方法とはいえません。

45. B ➡ P22

Amazon S3 DynamoDBのusersテーブルのみに対するレコード削除権限をIAMポリシーで作成し、IAMロールに関連付けます。
DynamoDBテーブルのレコードのみ削除のActionを許可し、かつ対象のリソースとしてDynamoDBのusersテーブルのみを指定している**B**が正解です。

Aは、対象のテーブルが「*」となっており、範囲が広すぎます。Dは、DynamoDBのすべてのActionを許可しているため、最小権限の法則に反します。Cは、AとDの両方が合わさっています。

46. D ➡ P24

回線の逼迫を防ぎつつ大量のデータをGlacierにアーカイブするには、AWS Snowballを利用します。Snowballは、大容量データをAWS内ストレージへ転送するサービスです。Snowballで使用する筐体は、AWSが用意した物理耐久性が高いもので、AWSマネジメントコンソールからジョブを作成するだけで、登録した住所へ自動的に発送されます。
Snowballに保存したデータはS3に保存され、S3からGlacierへアーカイブする設定を行う必要があります。したがって、**D**が正解です。

設問では、会社の回線への負担を軽減するという要件がありますので、100TBのデータをインターネット経由やVPN経由で転送する方式は不適切です（A、B、C）。

47. A ➡ P24

Amazon S3 Glacierを使用することでAmazon S3よりもコストを抑えることができます。Expeditedオプションでは、1〜5分でのデータの取り出しが可能です（**A**）。
Standardオプションでは、データの取り出しに3〜5時間必要です（B）。
S3の標準低頻度アクセスでコストを抑えることができますが、取り出し頻度が不明なため、低頻度アクセスが適切かは判断できません（C）。1ゾーン低頻度アクセスでもコストを抑えることができますが、単一のゾーンでしかデータを保存していないため、データ損失の可能性が高くなります（D）。

48. C

➡ P25

DEV環境は営業時間に稼働することが要求されているため、スポットインスタンスを使用することは適切ではありません（A）。
PROD環境は24時間稼働するため、スポットインスタンスを使用することは適切ではありません（B）。
DEV環境は決まった時間にのみ起動していればよいため、スケジュールされたリザーブドインスタンスは有効であると考えられます。また、PROD環境は24時間稼働するため、リザーブドインスタンスは有効であると考えられます（**C**）。
PROD環境は24時間稼働するため、スケジュールされたリザーブドインスタンスよりもリザーブドインスタンスのほうが費用対効果は高いと考えられます（D）。

49. A

➡ P25

Amazon S3のWebサイトホスティングにAmazon Route53のフェイルオーバールーティングを設定することで、メインサイトの障害を検知した際に自動でバックアップサイトへ切り替えることが可能です（**A**）。Route 53のレイテンシールーティングを設定すると、レイテンシーが少ないサイトへ接続してしまうため、メインサイト稼働中でもバックアップサイトへ接続してしまう場合があります（B）。
ELBはアベイラビリティーゾーン（AZ）をまたいだ冗長化は可能ですが、リージョンをまたいだ冗長化を行うことはできません（C）。
メインサイトのサーバーがダウンするとサーバーはユーザーからのアクセスを受け付けないため、バックアップサイトへのリダイレクトを行うことができません（D）。

50. D

➡ P26

Amazon CloudFrontは、「エッジロケーション」と呼ばれるグローバルな拠点からコンテンツを配信するCDNサービスです。
CloudFrontには地域制限（地理的ブロッキング）の機能があり、これを使用すると特定地域のユーザーにコンテンツを配信したり、逆にブロックしたりすることができます（**D**）。

51. B

➡ P26

インターネットから特定のIPアドレスを通じた悪意ある攻撃を遮断するには、AWS WAFを使用するのが適切です。
AWS WAFは、Amazon CloudFrontなどに設定できるWebアプリケーションファイアウォールです。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の一般的な攻撃パターンをブロックするセキュリティルールや、IPアドレスなどの

事前定義した特定のトラフィックパターンを除外するルールを作成することができます。
設問では、インターネット向けにCloudFrontを利用しており、AWS WAFで特定のIPアドレスの遮断の設定をCloudFrontに対して行うことができます。したがって、**B**が正解です。

ネットワークACLやセキュリティグループなどで特定のIPアドレスからのアクセスをブロックすることは可能ですが、設問のケースのようにCloudFrontでアクセスを受け付ける場合、リクエストの入り口でセキュリティ対策を行う方法が適切です（A、C）。また、CloudFront自体に、特定のIPアドレスをブロックする機能はありません（D）。

52. A、C

➡ P27

セキュリティグループのインバウンド通信は、明示的にIPアドレスを指定しない場合、通信が許可されません（**A**）。また、特定のIPアドレスからの通信を拒否する設定を行うことはできません（B）。
セキュリティグループのアウトバウンド通信は、特定のIPアドレスへの通信を許可することができるため、設定していないIPアドレスへの通信は拒否されます（**C**）。
アプリケーションAとアプリケーションBは同じサブネットで動作しているため、ネットワークACLの設定を変更しても通信の許可または拒否の設定が適用されません（D、E）。

53. A

➡ P27

Amazon EBSは永続可能なブロックストレージサービスで、EC2インスタンスにアタッチすることで利用できます。ブロックストレージデバイスであるため、EC2にホストされているOSからどのようなファイルシステムでも作成が可能です（**A**）。
Amazon EFSは、スケーラブルな共有ストレージサービスです。EFSはNFSの機能を提供しており、現状ではLinuxのファイルシステムのみサポートしています。複数のEC2インスタンス（Linux）から利用できます（B）。
Amazon S3は、オブジェクトストレージサービスです（C）。
Glacierは、アーカイブを目的としたストレージサービスです（D）。
Amazon DynamoDBは、NoSQL型のマネージドデータベースです（E）。

54. C

➡ P27

インメモリデータベースとしては、Amazon ElastiCacheが利用できます。ElastiCacheは、MemcachedとRedisをエンジンとして利用することができますが、通常、高可用性の要件がある場合にはRedisを使用します。Redisは、マスター・スタンバイ型

の構成により可用性を高めることができるほか、データストアとしても利用可能であるため、IoTデータの保存用として適用が可能です。したがって、**C**が正解です。

インメモリデータベースのソリューションとして適切ではありません（A、B）。また、Memcachedの主な用途は一時的なデータキャッシュ用途で、高可用性やデータの永続性は担保できません（D）。

55. C、D

➡ P28

Amazon DynamoDB Accelerator（DAX）は、可用性が高くフルマネージドなDynamoDB用インメモリキャッシュです（**C**）。1秒あたり100万回単位のリクエストに数ミリ秒の応答時間で処理ができます（**D**）。
DAXを利用すると、DynamoDBに格納されたデータの読み込み回数を減らすことができるため、読み込みスループットが向上します。

56. D

➡ P28

ACLを用いてすべてのAWSアカウントのアクセス制限を行うための機能がありません（A）。
セキュリティグループは、AWSアカウントのアクセス制限を行うための機能ではありません（B）。
クロスアカウントロールによってアクセス制限を行うことはできますが、アカウントごとに設定する必要があるため、設問の要件を満たしません（C）。
AWS Organizationsのサービスコントロールポリシーを利用することで、組織単位に一括でアクセス制御を行うことができます（**D**）。

57. B

➡ P29

AWS KMSは、AWS上で鍵管理を提供するマネージドサービスで、主に暗号化鍵の作成や有効・無効の管理、ローテーション、削除などを行うことができます（**B**）。
AWS KMSを利用して、AWSに送信されたデータをサーバーサイド（AWS）で暗号化したり（A）、データ送信前にクライアントサイドで暗号化したりすることができます。
AWS CloudHSMは、AWSのデータセンター内に配置されるユーザー占有のハードウェアアプライアンスです（C）。CloudHSMはユーザーのVPC内に配置され、ほかのネットワークから隔離されることや、国際的なセキュリティ基準に準拠していることなどから、セキュリティコンプライアンス要件が厳しい場合に適用します（D）。

58. B ➡ P29

設問では、S3バケットに保管したデータを低頻度でアクセスする場合のコスト削減方法が問われています。

標準低頻度アクセス（Standard-Infrequent Access）は、スタンダードクラスと同等の耐久性があり、かつデータの格納コストはスタンダードクラスと比較して安価です。ただし、データの読み取りに対して課金されるため、データへのアクセス頻度が低い場合に適しています。したがって、**B**が正解です。

A. 過去のデータも必要に応じてすぐに取得しなければならないため、Amazon S3 Glacierのようなアーカイブストレージは適していません。
C. 1ゾーン低頻度アクセス（One Zone-Infrequent Access）は、ひとつのアベイラビリティーゾーン（AZ）のみにデータを保存します。複数のAZにデータを複製するスタンダードクラスと比較すると、コストを約20%削減できます。データへのアクセス頻度が低く、高い耐久性を必要とせず、かつ必要に応じてすぐに取り出したい場合に適していますが、耐久性が求められる場合は適していません。
D. バイナリ変換してAmazon RDSに保管する場合、RDSデータベースインスタンスなどの追加で必要なAWSリソースが増えてしまい、コスト面で適切ではありません。

59. B、E ➡ P30

セキュリティグループを利用することで、Webアプリケーションサーバー（**E**）とデータベースサーバー（**B**）の各々に対してファイアウォール機能を提供します。一方、ネットワークACLはサブネット単位で設定するファイアウォール機能です。セキュリティグループとは異なりステートレスであるため、インバウンドとアウトバウンドに対して明示的に通信制御を行う必要があります。Webアプリケーションサーバーとデータベースサーバーの各サブネットのアウトバウンド通信をネットワークACLですべて拒否した場合、戻りの通信ができません（A、D）。
Webアプリケーションサーバーとデータベースサーバーを同じサブネットに配置しただけでは、セキュリティ要件を満たしません（C）。

60. D ➡ P30

Amazon DynamoDBには、結果整合性モデルという特徴があります。これは、書き込んだデータは時間が経てば正しく反映される（時間が経てば整合性が保証される）というものですが、データ読み取りのタイミングによっては書き込んだデータが反映されていない状態になります。そのため、整合性が取れたデータへのア

クセスが必須となるアプリケーションには利用できません。
DynamoDBを利用して一貫性のあるデータへのアクセスを求める場合は、Consistent Read（読み取り一貫性）の設定を有効にします。したがって、**D**が正解です。

A. Amazon DynamoDBグローバルテーブルは、複数リージョンに配置しているデータベーステーブルでデータの整合性を取る機能です。
B. Amazon DynamoDBストリームは、DynamoDBのテーブルに対して行われたデータ変更（追加、更新、削除）の履歴情報をイベントとして検出し、24時間保持する機能です。
C. DynamoDBのキャパシティモードのオンデマンドは、データベースのテーブルに実行したデータの読み書きに対して課金が発生するモードです。

61. A ➡ P31

Egress-Onlyインターネットゲートウェイは、冗長化されたゲートウェイで、IPv6を利用してVPCからインターネットへ接続することができるサービスです（**A**）。
NATゲートウェイは、冗長化されたゲートウェイで、プライベートサブネットからインターネットへ接続するゲートウェイですが、利用時間に応じて料金が発生します（B）。
カスタムNATインスタンスは、EC2インスタンスをNATサーバーとして利用するため、自動でスケールすることはできません（C）。
VPCエンドポイントは、各種AWSサービスに対しプライベート接続する機能を持ち、インターネット接続はできません（D）。

62. C ➡ P31

プライベートサブネット内のEC2インスタンスからAmazon S3へプライベート接続するためには、ゲートウェイ型のVPCエンドポイントを作成し、ルートテーブルにS3のターゲットを設定します。
S3にはゲートウェイ型、EC2にはインターフェイス型のVPCエンドポイントが提供されています。したがって、選択肢**C**が正解です。

63. D ➡ P31

AWS Lambdaはサーバーレスのコンピューティングサービスで、コンテナ上で動いています。Lambdaのコンテナはコールドスタートするため、急増したトラフィックに対応できない可能性があります（A）。
Amazon ElastiCacheはインメモリデータベースサービスで、Node.jsのアプリケーションを実行することはできません（B）。

EC2で処理を行う場合、想定の負荷を処理できる数のインスタンスを用意したとしても、想定を超えた場合には処理が継続できなくなる可能性があります（C）。
Auto Scalingを設定してEC2インスタンスを自動的にスケールアウトさせることで、想定以上のトラフィック急増にも対応できると考えられます（**D**）。

64. A

➡ P32

Amazon EFSはEC2インスタンスへマウントして利用します。そのため、OS機能によるファイルのアクセス制御を行うことが可能です（**A**）。
Amazon S3はACLでアクセス制御を行うことが可能ですが、AWSアカウントやパブリックアクセスが対象となり、ユーザーグループなどで制御を行うことはできません（B）。また、IAMでアクセス制御を行う場合はAPIコールが対象となり、ディレクトリごとのアクセス制御を行うことはできません（C）。
セキュリティグループでディレクトリごとのアクセス制御を行うことはできません（D）。

65. D

➡ P32

Amazon Redshiftは同時実行クエリが多くなると、処理しきれないクエリはキューに格納され、Redshiftでの処理が可能となるリソースが確保されるまで待ち時間が発生してしまいます。
しかし、Redshift concurrency scalingを有効にすると、Redshiftでバースト性のあるユースケースが発生したときに、事前に設定した範囲で自動でスケーリングしてクエリの処理を行います。
したがって、**D**が正解です。

A. SQSを使用しなくても、Redshiftの処理待ちクエリはRedshiftのキューに格納されます。また、キューに格納しても複数クエリを高速に実行することはできません。
B. クロスリージョンスナップショットは、スナップショット取得時に、クラスターが配置されているのとは別のリージョンにスナップショットを複製することができる機能です。この機能はバックアップを目的とするため、設問のケースでは適切ではありません。
C. Redshiftのノード数を増やすと、データの格納、クエリの処理が早くなることがありますが、処理数に応じてスケールしてクエリを処理することはできません。