2026年版 | SAA-C03対応 | PDF版 EXAMPLE

65問サンプル / 詳解付き

AWS認定
SAA-C03

ソリューションアーキテクト - アソシエイト

実践問題集

非公式学習教材

Q. 001

SAA-C03

ある企業は、複数の大陸にある都市で気温、湿度、大気圧のデータを収集している。各サイトから毎日収集するデータ量の平均は500 GBである。各サイトには高速インターネット接続がある。企業は、これらのグローバルサイトからのデータを単一のAmazon S3バケットにできるだけ速く集約したい。ソリューションは運用上の複雑さを最小限に抑える必要がある。どのソリューションがこれらの要件を満たすか。

A. 宛先のS3バケットでS3 Transfer Accelerationを有効にする。マルチパートアップロードを使用して、各サイトのデータを宛先のS3バケットに直接アップロードする。

B. 各サイトのデータを最も近いリージョンのS3バケットにアップロードする。S3クロスリージョンレプリケーションを使用してオブジェクトを宛先のS3バケットにコピーする。その後、元のS3バケットからデータを削除する。

C. AWS Snowball Edge Storage Optimizedデバイスのジョブを毎日スケジュールし、各サイトから最も近いリージョンにデータを転送する。S3クロスリージョンレプリケーションを使用してオブジェクトを宛先のS3バケットにコピーする。

D. 各サイトのデータを最も近いリージョンのAmazon EC2インスタンスにアップロードする。Amazon Elastic Block Store（Amazon EBS）ボリュームにデータを保存する。定期的にEBSスナップショットを取得し、宛先S3バケットがあるリージョンにコピーする。そのリージョンでEBSボリュームを復元する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- グローバルサイトから1日あたり約500 GBのデータを集約する
- 可能な限り速やかに単一のAmazon S3バケットに集約する
- 各サイトは高速インターネット接続を持つ
- 運用上の複雑さを最小限に抑える

正解はAである。

S3 Transfer Accelerationはエッジロケーションを経由した最適化されたネットワーク経路により、地理的に分散したサイトからのアップロードを高速化できる。マルチパートアップロードは大容量データを並列に送信できるため、500 GB規模のデータを効率よくアップロードでき、追加の中間基盤を管理する必要も少ない。

不正解の理由

B. 各サイトのデータを最も近いリージョンのS3バケットにアップロードする。S3クロスリージョンレプリケーションを使用してオブジェクトを宛先のS3バケットにコピーする。その後、元のS3バケットからデータを削除する。

S3クロスリージョンレプリケーションは非同期であり、宛先バケットへの反映に遅延が発生する。リージョンごとの中間バケット管理も必要になるため、最速の集約と運用上の複雑さの最小化には適さない。

C. AWS Snowball Edge Storage Optimizedデバイスのジョブを毎日スケジュールし、各サイトから最も近いリージョンにデータを転送する。S3クロスリージョンレプリケーションを使用してオブジェクトを宛先のS3バケットにコピーする。

Snowball Edgeはオフラインの物理デバイスベースで毎日使用するには非現実的であり、運用負担と遅延が非常に大きい。

D. 各サイトのデータを最も近いリージョンのAmazon EC2インスタンスにアップロードする。Amazon Elastic Block Store（Amazon EBS）ボリュームにデータを保存する。定期的にEBSスナップショットを取得し、宛先S3バケットがあるリージョンにコピーする。そのリージョンでEBSボリュームを復元する。

EC2/EBSスナップショットを用いる方法は複雑で多くの運用作業（スナップショット管理、復元など）と時間を要し、迅速かつ簡単な集約要件を満たさない。

Q. 002

SAA-C03

企業は独自アプリケーションのログファイルを分析する必要がある。ログはJSON形式でAmazon S3バケットに保存されている。クエリは単純でオンデマンドで実行される。ソリューションアーキテクトは既存のアーキテクチャに最小限の変更で分析を行う必要がある。運用上の負担を最小限に抑えてこれらの要件を満たすにはどうすべきか？

A. Amazon Redshiftを使用してすべてのコンテンツを一箇所にロードし、必要に応じてSQLクエリを実行する。

B. Amazon CloudWatch Logsを使用してログを保存し、Amazon CloudWatchコンソールから必要に応じてSQLクエリを実行する。

C. Amazon AthenaをAmazon S3と直接使用して、必要に応じてクエリを実行する。

D. AWS Glueでログをカタログ化し、Amazon EMRの一時的なApache Sparkクラスターを使用して必要に応じてSQLクエリを実行する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- ログはJSON形式でAmazon S3に保存すること
- クエリは単純でオンデマンドで実行すること
- 既存アーキテクチャの変更を最小限に抑えること
- 運用上の負担を最小限に抑えること

正解はCである。

Amazon AthenaはS3に保存されたJSONを別途ロードせずに直接クエリ可能であり、既存アーキテクチャの変更がほとんどなく、サーバーレスで運用負担とコストを最小限に抑える。

不正解の理由

A. Amazon Redshiftを使用してすべてのコンテンツを一箇所にロードし、必要に応じてSQLクエリを実行する。

Redshiftはデータのロードや ETLが必要で、クラスターの運用と管理が求められ、変更と運用負担が大きい。

B. Amazon CloudWatch Logsを使用してログを保存し、Amazon CloudWatchコンソールから必要に応じてSQLクエリを実行する。

CloudWatch Logsに移行するにはS3からログを転送または再収集する必要があり、アーキテクチャ変更と追加の運用負担が発生する。

D. AWS Glueでログをカタログ化し、Amazon EMRの一時的なApache Sparkクラスターを使用して必要に応じてSQLクエリを実行する。

GlueとEMRはカタログとクラスター管理が必要で、運用負担と複雑性が増し、単純なオンデマンドクエリには過剰である。

Q. 003

SAA-C03

ある企業は、AWS Organizationsを使用して複数のAWSアカウントを異なる部門ごとに管理している。管理アカウントにはプロジェクトレポートを格納したAmazon S3バケットがある。この企業は、S3バケットへのアクセスをAWS Organizations内のアカウントのユーザーのみに制限したい。運用上の負担を最小限に抑えつつ、これらの要件を満たすソリューションはどれか。

A. S3バケットポリシーに組織IDを参照するaws:PrincipalOrgIDグローバル条件キーを追加する。

B. 各部門ごとに組織単位（OU）を作成し、S3バケットポリシーにaws:PrincipalOrgPathsグローバル条件キーを追加する。

C. AWS CloudTrailを使用してCreateAccount、InviteAccountToOrganization、LeaveOrganization、RemoveAccountFromOrganizationイベントを監視し、S3バケットポリシーを適宜更新する。

D. S3バケットへのアクセスが必要な各ユーザーにタグを付け、S3バケットポリシーにaws:PrincipalTagグローバル条件キーを追加する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- S3バケットへのアクセスをAWS Organizationsに属するアカウントのユーザーのみに制限すること
- 運用上の負担を最小限に抑えること
- 管理アカウントが所有するS3バケットに適用すること

正解はAである。

aws:PrincipalOrgID条件キーをバケットポリシーに使用すると、該当組織IDに属するすべてのアカウントのプリンシパルのみを許可し、アカウント変更時のポリシー更新が不要となり運用負担を最小化する。S3でサポートされる標準的な方法で要件を直接満たす。

不正解の理由

B. 各部門ごとに組織単位（OU）を作成し、S3バケットポリシーにaws:PrincipalOrgPathsグローバル条件キーを追加する。

各部門ごとにOUを作成しパスを管理する必要があり、追加設定と維持管理が必要なため運用負担が増加する。

C. AWS CloudTrailを使用してCreateAccount、InviteAccountToOrganization、LeaveOrganization、RemoveAccountFromOrganizationイベントを監視し、S3バケットポリシーを適宜更新する。

CloudTrailで監視後にポリシーを手動更新する必要があり、運用負担が大きくリアルタイム制約がある。

D. S3バケットへのアクセスが必要な各ユーザーにタグを付け、S3バケットポリシーにaws:PrincipalTagグローバル条件キーを追加する。

すべてのアカウントのユーザーに一貫してタグを付与・管理する必要があり、実装と維持管理が煩雑で誤りが発生しやすい。

Q. 004

SAA-C03

アプリケーションはVPC内のAmazon EC2インスタンス上で稼働している。このアプリケーションはAmazon S3バケットに保存されたログを処理する。EC2インスタンスはインターネット接続なしでS3バケットにアクセスする必要がある。どのソリューションがAmazon S3へのプライベートネットワーク接続を提供するか？

A. S3バケットへのゲートウェイVPCエンドポイントを作成する。

B. ログをAmazon CloudWatch Logsにストリーミングし、ログをS3バケットにエクスポートする。

C. S3アクセスを許可するためにAmazon EC2にインスタンスプロファイルを作成する。

D. S3エンドポイントにアクセスするためにプライベートリンクを持つAmazon API Gateway APIを作成する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- EC2インスタンスがインターネット経由で外部に出ることなくS3にアクセスすること
- VPC内でプライベートネットワーク経路を提供すること
- アプリケーションはVPC内のAmazon EC2インスタンス上で実行されること
- アプリケーションはAmazon S3バケットに保存されたログを処理すること

正解はAである。

ゲートウェイVPCエンドポイントはルーティングテーブルを介してVPCからAmazon S3へのプライベート経路を提供するため、インターネットやNATを経由せずにS3にアクセス可能である。S3に対する推奨されるプライベートアクセス方法である。

不正解の理由

B. ログをAmazon CloudWatch Logsにストリーミングし、ログをS3バケットにエクスポートする。
CloudWatch Logsにストリーミング後S3にエクスポートする方法はアーキテクチャの変更であり、EC2が直接インターネットなしでS3にアクセスする要件を満たさない。

C. S3アクセスを許可するためにAmazon EC2にインスタンスプロファイルを作成する。
インスタンスプロファイル（IAMロール）は権限を付与するが、ネットワーク経路を作成しないためインターネットなしでS3に到達できない（VPCエンドポイントまたはNATが別途必要）。

D. S3エンドポイントにアクセスするためにプライベートリンクを持つAmazon API Gateway APIを作成する。
API Gatewayとプライベートリンクの組み合わせはS3への標準的かつ効率的なプライベートアクセス方法ではなく、不要な複雑さと管理負担を招く。

Q. 005

SAA-C03

ある企業は、単一のAmazon EC2インスタンス上でウェブアプリケーションをホストし、ユーザーがアップロードしたドキュメントをAmazon EBSボリュームに保存している。より高いスケーラビリティと可用性を実現するために、同じ構成を複製し、別のアベイラビリティーゾーンに2つ目のEC2インスタンスとEBSボリュームを作成し、両方をApplication Load Balancerの背後に配置した。この変更後、ユーザーはウェブサイトを更新するたびに、ドキュメントの一部しか表示されず、すべてのドキュメントを同時に見ることができないと報告した。ユーザーがすべてのドキュメントを一度に閲覧できるようにするために、ソリューションアーキテクトは何を提案すべきか？

A. 両方のEBSボリュームにすべてのドキュメントが含まれるようにデータをコピーする

B. Application Load Balancerを設定し、ユーザーをドキュメントがあるサーバーに誘導する

C. 両方のEBSボリュームのデータをAmazon EFSにコピーし、アプリケーションを修正して新しいドキュメントをAmazon EFSに保存する

D. Application Load Balancerを設定し、リクエストを両方のサーバーに送信し、各ドキュメントを正しいサーバーから返すようにする。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- すべてのインスタンスで同一のドキュメントセットを即時に閲覧可能であること
- 複数のアベイラビリティーゾーンにまたがるアクセスをサポートすること
- 新規アップロードもすべてのインスタンスで即時に一貫してアクセス可能であること

正解はCである。

Amazon EFSは複数のアベイラビリティーゾーンにまたがる複数のEC2インスタンスから同時にマウント可能なファイルストレージを提供し、すべてのインスタンスが同一のファイルセットに即時アクセス可能とする。アプリケーションをEFSに書き換えることで、一貫性と高可用性のファイルアクセスを保証する。

不正解の理由

A. 両方のEBSボリュームにすべてのドキュメントが含まれるようにデータをコピーする

EBSはアベイラビリティーゾーン単位のブロックストレージであり、手動でコピーや同期を行う必要があるため、一貫性の維持が困難で運用負担が大きく、リアルタイム同期を保証できない。

B. Application Load Balancerを設定し、ユーザーをドキュメントがあるサーバーに誘導する

ロードバランサーでユーザーを常に同一サーバーにルーティングするとセッション固定問題や単一障害点が発生し、分散インスタンス間のデータ不整合は解決できない。

D. Application Load Balancerを設定し、リクエストを両方のサーバーに送信し、各ドキュメントを正しいサーバーから返すようにする。

アプリケーションロードバランサーはリクエストを同時に複数サーバーに送信する方式ではなく、複数サーバーの応答を統合する複雑なロジックと非効率を招き、実用的でない。

Q. 006

SAA-C03

ある企業はオンプレミスのネットワーク接続ストレージにNFSを使用して大容量の動画ファイルを保存している。各動画ファイルのサイズは1MBから500GBまでである。総ストレージ容量は70TBであり、これ以上増加しない。企業は動画ファイルをAmazon S3に移行することを決定した。可能な限り速やかに、かつネットワーク帯域幅の使用を最小限に抑えて動画ファイルを移行しなければならない。どのソリューションがこれらの要件を満たすか？

A. S3バケットを作成する。S3バケットへの書き込み権限を持つIAMロールを作成する。AWS CLIを使用してすべてのファイルをローカルからS3バケットにコピーする。

B. AWS Snowball Edgeジョブを作成する。オンプレミスでSnowball Edgeデバイスを受け取る。Snowball Edgeクライアントを使用してデバイスにデータを転送する。デバイスを返送し、AWSがデータをAmazon S3にインポートする。

C. オンプレミスにS3ファイルゲートウェイを展開する。S3ファイルゲートウェイに接続するためのパブリックサービスエンドポイントを作成する。S3バケットを作成する。S3ファイルゲートウェイ上に新しいNFSファイル共有を作成し、そのファイル共有をS3バケットにポイントする。既存のNFSファイル共有からS3ファイルゲートウェイにデータを転送する。

D. オンプレミスネットワークとAWS間にAWS Direct Connect接続を設定する。オンプレミスにS3ファイルゲートウェイを展開する。S3ファイルゲートウェイに接続するためのパブリック仮想インターフェイス（VIF）を作成する。S3バケットを作成する。S3ファイルゲートウェイ上に新しいNFSファイル共有を作成し、そのファイル共有をS3バケットにポイントする。既存のNFSファイル共有からS3ファイルゲートウェイにデータを転送する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 可能な限り迅速なマイグレーション
- ネットワーク帯域幅の使用を最小限に抑える
- 総データ量は70 TB（増加しない）
- ファイルサイズ範囲は1 MBから500 GB

正解はBである。

AWS Snowball Edgeは物理デバイスを用いて大量データをオフラインで転送するため、ネットワーク帯域幅の消費を最小限に抑えつつ70 TBの大量データを迅速にマイグレーションできる。ネットワーク転送に依存しないため、「可能な限り迅速に」の要件を満たす。

不正解の理由

A. S3バケットを作成する。S3バケットへの書き込み権限を持つIAMロールを作成する。AWS CLIを使用してすべてのファイルをローカルからS3バケットにコピーする。

AWS CLIによるコピーはオンプレミスからネットワーク経由で直接転送するため、70 TBの転送に多くのネットワーク帯域幅と時間を要し、要件を満たさない。

C. オンプレミスにS3ファイルゲートウェイを展開する。S3ファイルゲートウェイに接続するためのパブリックサービスエンドポイントを作成する。S3バケットを作成する。S3ファイルゲートウェイ上に新しいNFSファイル共有を作成し、そのファイル共有をS3バケットにポイントする。既存のNFSファイル共有からS3ファイルゲートウェイにデータを転送する。

S3ファイルゲートウェイ経由の転送はオンプレミスからS3へのネットワーク転送を行うため、70 TBの移動時にネットワーク帯域幅を多く使用し、要件に不適合である。

D. オンプレミスネットワークとAWS間にAWS Direct Connect接続を設定する。オンプレミスにS3ファイルゲートウェイを展開する。S3ファイルゲートウェイに接続するためのパブリック仮想インターフェイス（VIF）を作成する。S3バケットを作成する。S3ファイルゲートウェイ上に新しいNFSファイル共有を作成し、そのファイル共有をS3バケットにポイントする。既存のNFSファイル共有からS3ファイルゲートウェイにデータを転送する。

Direct Connectの設定にかかる時間と準備作業により「可能な限り迅速に」の要件を満たしにくく、さらに大量データをネットワークで転送する必要がある。

Q. 007

SAA-C03

ある企業は、受信メッセージを取り込むアプリケーションを持つ。数十の他のアプリケーションやマイクロサービスがこれらのメッセージを迅速に消費する。メッセージ数は大きく変動し、時には1秒あたり10万件に急増することもある。企業はソリューションの疎結合化とスケーラビリティの向上を望んでいる。これらの要件を満たすソリューションはどれか。

A. メッセージをAmazon Kinesis Data Analyticsに永続化する。コンシューマーアプリケーションを設定してメッセージを読み取り処理する。

B. 取り込みアプリケーションをAuto Scalingグループ内のAmazon EC2インスタンスにデプロイし、CPUメトリクスに基づいてEC2インスタンス数をスケールする。

C. メッセージを単一シャードのAmazon Kinesis Data Streamsに書き込む。AWS Lambda 関数を使用してメッセージを前処理し、Amazon DynamoDBに保存する。コンシューマーアプリケーションを設定してDynamoDBから読み取りメッセージを処理する。

D. メッセージを複数のAmazon Simple Queue Service (Amazon SQS)サブスクリプションを持つAmazon Simple Notification Service (Amazon SNS)トピックに公開する。コンシューマーアプリケーションを設定してキューからメッセージを処理する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 大量（最大秒間100,000件）かつ変動の大きいメッセージ処理
- 数十の独立したアプリケーションおよびマイクロサービスがメッセージを消費
- 生産者と消費者の分離（デカップリング）が必要
- メッセージが迅速に消費される

正解はDである。

SNSにパブリッシュし、各消費者ごとにSQSキューをサブスクライブするファンアウトアーキテクチャは、生産者と消費者の分離を提供し、各消費者が独立してスケールおよび処理可能で高い拡張性と分離性を実現する。

不正解の理由

A. メッセージをAmazon Kinesis Data Analyticsに永続化する。コンシューマーアプリケーションを設定してメッセージを読み取り処理する。

Kinesis Data Analyticsはリアルタイム分析用であり、メッセージの保存や多数の独立消費者への自然なパブリッシュ-サブスクライブ分離を提供せず、要件に合致しない。

B. 取り込みアプリケーションをAuto Scalingグループ内のAmazon EC2インスタンスにデプロイし、CPUメトリクスに基づいてEC2インスタンス数をスケールする。

EC2の自動スケーリングはアプリケーションレベルのスケーリングのみで、多数の消費者の分離や消費者ごとの速度制御を提供せず、デカップリング要件を満たさない。

C. メッセージを単一シャードのAmazon Kinesis Data Streamsに書き込む。AWS Lambda 関数を使用してメッセージを前処理し、Amazon DynamoDBに保存する。コンシューマーアプリケーションを設定してDynamoDBから読み取りメッセージを処理する。

単一シャードでは秒間100,000件の処理能力が不足し、DynamoDBへの前処理後に消費者がDBを読み取る方式はパブリッシュ-サブスクライブの分離が弱く、拡張性や処理遅延の問題が生じる。

Q. 008

SAA-C03

企業が分散アプリケーションをAWSに移行している。このアプリケーションは可変のワークロードに対応している。レガシープラットフォームは、複数のコンピュートノードにジョブを調整するプライマリサーバーで構成されている。企業は、回復力とスケーラビリティを最大化するソリューションでアプリケーションをモダナイズしたい。これらの要件を満たすために、ソリューションアーキテクトはどのようにアーキテクチャを設計すべきか？

A. ジョブの送信先としてAmazon Simple Queue Service（Amazon SQS）キューを構成する。コンピュートノードはAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。EC2 Auto Scalingをスケジュールスケーリングで構成する。

B. ジョブの送信先としてAmazon Simple Queue Service（Amazon SQS）キューを構成する。コンピュートノードはAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。EC2 Auto Scalingをキューのサイズに基づいて構成する。

C. プライマリサーバーとコンピュートノードをAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。ジョブの送信先としてAWS CloudTrailを構成する。プライマリサーバーの負荷に基づいてEC2 Auto Scalingを構成する。

D. プライマリサーバーとコンピュートノードをAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。ジョブの送信先としてAmazon EventBridge（Amazon CloudWatch Events）を構成する。コンピュートノードの負荷に基づいてEC2 Auto Scalingを構成する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 可変的なワークロードを処理する必要がある
- 復元力（障害許容）を最大化する必要がある
- スケーラビリティを最大化する必要がある
- アプリケーションをモダナイズする必要がある

正解はBである。

Amazon SQSで作業をデカップリングし、メインサーバーのボトルネックと単一障害点を排除する。キューの長さに基づくEC2の自動スケーリングは、可変的なワークロードに対して即時かつ弾力的なインスタンス調整を提供し、復元力とスケーラビリティを最大化する。

不正解の理由

A. ジョブの送信先としてAmazon Simple Queue Service（Amazon SQS）キューを構成する。コンピュートノードはAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。EC2 Auto Scalingをスケジュールスケーリングで構成する。

予約ベースの自動スケーリングは予測可能なパターンにのみ適しており、可変的かつ予測不可能なワークロードに対して即時のスケーラビリティや復元力を保証しない。

C. プライマリサーバーとコンピュートノードをAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。ジョブの送信先としてAWS CloudTrailを構成する。プライマリサーバーの負荷に基づいてEC2 Auto Scalingを構成する。

CloudTrailは監査およびログ記録サービスであり、作業対象のキューとして不適切である。メインサーバーに依存する設計は単一障害点を排除できない。

D. プライマリサーバーとコンピュートノードをAuto Scalingグループで管理されるAmazon EC2インスタンスで実装する。ジョブの送信先としてAmazon EventBridge（Amazon CloudWatch Events）を構成する。コンピュートノードの負荷に基づいてEC2 Auto Scalingを構成する。

EventBridgeはイベントバスであるが、作業キューのようにインスタンス数を直接駆動するスケール指標として適切でない。メインサーバーおよびイベントベースの設計はメインサーバーのボトルネックを完全に排除しない可能性がある。

Q. 009

SAA-C03

ある企業はデータセンターでSMBファイルサーバーを運用している。このファイルサーバーは、大きなファイルを保存しており、ファイル作成後の最初の数日間は頻繁にアクセスされる。7日経過後はファイルへのアクセスはほとんどない。総データサイズは増加しており、企業の総ストレージ容量に近づいている。ソリューションアーキテクトは、最近アクセスされたファイルへの低遅延アクセスを失うことなく、利用可能なストレージ容量を増やす必要がある。また、将来のストレージ問題を回避するためにファイルのライフサイクル管理も提供しなければならない。どのソリューションがこれらの要件を満たすか？

A. AWS DataSyncを使用して、SMBファイルサーバーから7日より古いデータをAWSにコピーする。

B. Amazon S3 File Gatewayを作成して企業のストレージ容量を拡張する。7日後にデータをS3 Glacier Deep Archiveに移行するS3ライフサイクルポリシーを作成する。

C. Amazon FSx for Windows File Serverのファイルシステムを作成して企業のストレージ容量を拡張する。

D. 各ユーザーのコンピュータにユーティリティをインストールしてAmazon S3にアクセスする。7日後にデータをS3 Glacier Flexible Retrievalに移行するS3ライフサイクルポリシーを作成する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 最近（最初の数日間）頻繁にアクセスされるファイルに対し低遅延アクセスを維持すること
- 利用可能な総ストレージ容量を拡張すること
- ファイルのライフサイクル管理により7日以降にアクセス頻度の低いデータを長期保存に移行すること
- データ総量が増加し会社の総ストレージ容量に近づくこと

正解はBである。

S3 File GatewayはSMBインターフェースを通じてオンプレミスからS3をファイルストレージのように拡張可能であり、ローカルキャッシュにより最近アクセスされたファイルに低遅延アクセスを提供する。S3に保存されたオブジェクトにライフサイクルポリシーを適用し、7日後に低コストの長期保存（S3 Glacier Deep Archive）に移行できるため、要件を満たす。

不正解の理由

A. AWS DataSyncを使用して、SMBファイルサーバーから7日より古いデータをAWSにコピーする。

DataSyncはデータをコピーして移動するのみで、オンプレミスのSMBインターフェースを透過的に拡張したりローカルキャッシュを提供せず、低遅延アクセスを保証できない。

C. Amazon FSx for Windows File Serverのファイルシステムを作成して企業のストレージ容量を拡張する。

FSxは管理されたSMBファイルストレージを提供するが、オンプレミス拡張時にネットワーク遅延やコストが発生し、自動ライフサイクル移行機能がなく要件を完全に満たさない。

D. 各ユーザーのコンピュータにユーティリティをインストールしてAmazon S3にアクセスする。7日後にデータをS3 Glacier Flexible Retrievalに移行するS3ライフサイクルポリシーを作成する。

各クライアントにユーティリティをインストールすることは運用負担が大きく、S3は基本的にオブジェクトストレージでありSMBのような透過的なファイルアクセスを提供しない。

Q. 010

SAA-C03

企業がAWS上にeコマースのウェブアプリケーションを構築している。このアプリケーションは新しい注文に関する情報を処理するためにAmazon API GatewayのREST APIに送信する。企業は注文が受信された順序で処理されることを保証したい。どのソリューションがこれらの要件を満たすか？

A. アプリケーションが注文を受信したときに、API Gatewayの統合を使用してAmazon Simple Notification Service（Amazon SNS）トピックにメッセージを公開する。トピックにAWS Lambda 関数をサブスクライブして処理を実行する。

B. アプリケーションが注文を受信したときに、API Gatewayの統合を使用してAmazon Simple Queue Service（Amazon SQS）FIFOキューにメッセージを送信する。SQS FIFOキューを設定して処理のためにAWS Lambda 関数を呼び出す。

C. アプリケーションが注文を処理している間、API Gatewayのオーソライザーを使用してリクエストをブロックする。

D. アプリケーションが注文を受信したときに、API Gatewayの統合を使用してAmazon Simple Queue Service（Amazon SQS）標準キューにメッセージを送信する。SQS標準キューを設定して処理のためにAWS Lambda 関数を呼び出す。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 注文は受信した順序で処理する必要がある
- API Gatewayを通じて注文が送信される
- AWSで電子商取引ウェブアプリケーションを構築している
- 処理対象は新規注文情報である

正解はBである。

SQS FIFOキューはメッセージグループIDに基づいて順序を保証し、SQSイベントソースとしてLambdaを構成すると順次処理が可能であり、受信順序の保証要件を満たす。

不正解の理由

A. アプリケーションが注文を受信したときに、API Gatewayの統合を使用してAmazon Simple Notification Service（Amazon SNS）トピックにメッセージを公開する。トピックにAWS Lambda 関数をサブスクライブして処理を実行する。

SNSはパブリッシュ/サブスクライブサービスであり、送信順序を保証しないため受信順序保証要件を満たさない。

C. アプリケーションが注文を処理している間、API Gatewayのオーソライザーを使用してリクエストをブロックする。

認証機能でリクエストをブロックすることは順序保証のメカニズムではなく、拡張性と可用性を損なう。

D. アプリケーションが注文を受信したときに、API Gatewayの統合を使用してAmazon Simple Queue Service（Amazon SQS）標準キューにメッセージを送信する。SQS標準キューを設定して処理のためにAWS Lambda 関数を呼び出す。

SQSスタンダードキューは高スループットを提供するが、メッセージの順序を保証しない。

Q. 011

SAA-C03

ある企業がAmazon EC2インスタンス上で動作するアプリケーションを持ち、Amazon Auroraデータベースを使用している。EC2インスタンスは、ローカルのファイルに保存されたユーザー名とパスワードを使ってデータベースに接続している。企業は認証情報管理の運用上の負担を最小限に抑えたい。ソリューションアーキテクトはこの目標を達成するために何をすべきか？

A. AWS Secrets Managerを使用し、自動ローテーションを有効にする。

B. AWS Systems Manager Parameter Storeを使用し、自動ローテーションを有効にする。

C. AWS KMS暗号化キーで暗号化されたオブジェクトを保存するためのAmazon S3バケットを作成し、認証情報ファイルをS3バケットに移行し、アプリケーションをS3バケットに向ける。

D. 各EC2インスタンス用に暗号化されたAmazon EBSボリュームを作成し、新しいEBSボリュームを各EC2インスタンスにアタッチし、認証情報ファイルを新しいEBSボリュームに移行し、アプリケーションを新しいEBSボリュームに向ける。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- EC2インスタンスがローカルファイルに保存されたユーザー名およびパスワード認証情報でデータベースに接続する
- 認証情報管理の運用負担を最小限に抑える
- Amazon Auroraデータベースを使用する
- アプリケーションはAmazon EC2インスタンス上で実行される

正解はAである。

AWS Secrets Managerは管理された認証情報サービスであり、AWS KMSで保存時に暗号化され、AuroraなどのRDSとの自動ローテーション機能を提供するため、手動管理を減らし運用負担を最小限に抑える。EC2はSDK/APIで容易にシークレットを取得でき、アプリケーションの変更も最小限で済む。

不正解の理由

B. AWS Systems Manager Parameter Storeを使用し、自動ローテーションを有効にする。

AWS Systems Managerパラメーターストアはシークレット保存が可能だが、Secrets Managerのようなネイティブの自動ローテーション機能を提供せず、運用負担を完全に軽減できない。

C. AWS KMS暗号化キーで暗号化されたオブジェクトを保存するためのAmazon S3バケットを作成し、認証情報ファイルをS3バケットに移行し、アプリケーションをS3バケットに向ける。

S3にファイルを保存する方法は保存時の暗号化は可能だが、自動ローテーションやアクセス制御・監査・安全なシークレット取得の管理機能が不足し、運用負担が増加する可能性がある。

D. 各EC2インスタンス用に暗号化されたAmazon EBSボリュームを作成し、新しいEBSボリュームを各EC2インスタンスにアタッチし、認証情報ファイルを新しいEBSボリュームに移行し、アプリケーション

を新しいEBSボリュームに向ける。

各EC2に暗号化されたEBSボリュームを使用する方法は認証情報の集中管理や自動ローテーションを提供せず、インスタンスごとの管理負担が増加し要件を満たさない。

Q. 012

SAA-C03

グローバル企業が、Application Load Balancer（ALB）配下のAmazon EC2インスタンスでウェブアプリケーションをホストしている。このウェブアプリケーションは静的データと動的データを持つ。企業は静的データをAmazon S3バケットに保存している。静的データと動的データのパフォーマンスを向上させ、レイテンシーを低減したい。企業はAmazon Route 53に登録された独自ドメイン名を使用している。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. S3バケットとALBをオリジンとするAmazon CloudFrontディストリビューションを作成する。Route 53を設定してトラフィックをCloudFrontディストリビューションにルーティングする。

B. ALBをオリジンとするAmazon CloudFrontディストリビューションを作成する。S3バケットをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。Route 53を設定してトラフィックをCloudFrontディストリビューションにルーティングする。

C. S3バケットをオリジンとするAmazon CloudFrontディストリビューションを作成する。ALBとCloudFrontディストリビューションをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。アクセラレータのDNS名を指すカスタムドメイン名を作成し、そのカスタムドメイン名をウェブアプリケーションのエンドポイントとして使用する。

D. ALBをオリジンとするAmazon CloudFrontディストリビューションを作成する。S3バケットをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。2つのドメイン名を作成し、1つは動的コンテンツ用にCloudFrontのDNS名を指し、もう1つは静的コンテンツ用にアクセラレータのDNS名を指す。これらのドメイン名をウェブアプリケーションのエンドポイントとして使用する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 世界中のユーザーに対し、静的（S3）および動的（ALB/EC2）コンテンツのレイテンシーを低減し性能を向上させる
- Amazon Route 53に登録された既存ドメインを使用し、そのドメイン経由でトラフィックをルーティングする
- ウェブアプリケーションはALBの背後にあるAmazon EC2インスタンスでホストされている
- 静的データはAmazon S3バケットに保存されている

正解はAである。

Amazon CloudFrontはS3とALBの両方をオリジンとしてサポートし、静的オブジェクトをエッジでキャッシュし動的リクエストをエッジで高速化できる。Route 53でCloudFrontにユーザードメインをルーティングすることで世界中のレイテンシーが低減される。単一のディストリビューションで静的・動的コンテンツの両方を効果的に高速化する。

不正解の理由

B. ALBをオリジンとするAmazon CloudFrontディストリビューションを作成する。S3バケットをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。Route 53を設定してトラフィックをCloudFrontディストリビューションにルーティングする。

AWS Global AcceleratorはS3バケットを直接エンドポイントとしてサポートせず、S3の静的コンテンツ高速化にはCloudFrontが適切である。

C. S3バケットをオリジンとするAmazon CloudFrontディストリビューションを作成する。ALBとCloudFrontディストリビューションをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。アクセラレータのDNS名を指すカスタムドメイン名を作成し、そのカスタムドメイン名をウェブアプリケーションのエンドポイントとして使用する。

Global AcceleratorのエンドポイントにCloudFrontを設定する構成はサポートされていないか、不要な重複経路で非効率的である。

D. ALBをオリジンとするAmazon CloudFrontディストリビューションを作成する。S3バケットをエンドポイントとするAWS Global Accelerator標準アクセラレータを作成する。2つのドメイン名を作成し、1つは動的コンテンツ用にCloudFrontのDNS名を指し、もう1つは静的コンテンツ用にアクセラレータのDNS名を指す。これらのドメイン名をウェブアプリケーションのエンドポイントとして使用する。

Global AcceleratorはS3を直接エンドポイントとしてサポートせず、静的・動的でドメインを分けることは不要な複雑さを招く。

Q. 013

SAA-C03

ある企業はAWSインフラストラクチャの月次メンテナンスを実施している。これらのメンテナンス作業中に、複数のAWSリージョンにまたがるAmazon RDS for MySQLデータベースの認証情報をローテーションする必要がある。運用上の負担を最小限に抑えつつ、これらの要件を満たすソリューションはどれか。

A. 認証情報をAWS Secrets Managerのシークレットとして保存する。必要なリージョンに対してマルチリージョンシークレットレプリケーションを使用する。Secrets Managerでスケジュールに基づくシークレットのローテーションを設定する。

B. 認証情報をAWS Systems Managerのセキュアストリングパラメータとして保存する。必要なリージョンに対してマルチリージョンシークレットレプリケーションを使用する。Systems Managerでスケジュールに基づくシークレットのローテーションを設定する。

C. 認証情報をサーバーサイド暗号化（SSE）を有効にしたAmazon S3バケットに保存する。Amazon EventBridge（Amazon CloudWatch Events）を使用してAWS Lambda 関数を呼び出し、認証情報をローテーションする。

D. 認証情報をAWS KMSのマルチリージョンカスタマーマネージドキーで暗号化したシークレットとして保存する。Amazon DynamoDBグローバルテーブルにシークレットを保存する。AWS Lambda 関数を使用してDynamoDBからシークレットを取得し、RDS APIを使用してシークレットをローテーションする。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 複数のAWSリージョンにわたりAmazon RDS for MySQLの認証情報をローテーションする必要がある
- 認証情報は毎月のメンテナンスサイクルに合わせて定期的にローテーションする必要がある
- 会社はAWSインフラに対して毎月メンテナンスを実施している
- 認証情報のローテーションは月次メンテナンス作業の一部である

正解はAである。

AWS Secrets Managerは管理型サービスであり、RDSとの統合された自動ローテーション機能と複数リージョンにわたるシークレットのレプリケーション機能を提供するため、カスタム実装なしで要件を満たし運用負荷を最小限に抑える。

不正解の理由

B. 認証情報をAWS Systems Managerのセキュアストリングパラメータとして保存する。必要なリージョンに対してマルチリージョンシークレットレプリケーションを使用する。Systems Managerでスケジュールに基づくシークレットのローテーションを設定する。

AWS Systems Manager Parameter StoreはSecrets ManagerほどRDS統合の自動ローテーション機能や標準的な複数リージョンシークレットレプリケーション機能を提供しないため、追加の開発・運用が必要となる。

C. 認証情報をサーバーサイド暗号化（SSE）を有効にしたAmazon S3バケットに保存する。Amazon EventBridge（Amazon CloudWatch Events）を使用してAWS Lambda 関数を呼び出し、認証情報をローテーションする。

S3とEventBridgeおよびLambdaの組み合わせは独自のカスタムローテーションロジックと権限・セキュリティ設計が必要であり、運用負荷が大きくエラーの可能性が高い。

D. 認証情報をAWS KMSのマルチリージョンカスタマーマネージドキーで暗号化したシークレットとして保存する。Amazon DynamoDBグローバルテーブルにシークレットを保存する。AWS Lambda 関数を使用してDynamoDBからシークレットを取得し、RDS APIを使用してシークレットをローテーションする。

KMSの複数リージョンキーとDynamoDBおよびLambdaの組み合わせは完全なカスタムソリューションであり、複雑かつ運用負荷が高く、Secrets Managerと比較して自動ローテーション統合が不足している。

Q. 014

SAA-C03

企業は、Application Load Balancerの背後にあるAmazon EC2インスタンス上でeコマースアプリケーションを運用している。インスタンスは複数のアベイラビリティーゾーンにまたがるAmazon EC2 Auto Scalingグループで稼働している。Auto ScalingグループはCPU使用率のメトリクスに基づいてスケールする。eコマースアプリケーションは、トランザクションデータを大規模なEC2インスタンス上でホストされているMySQL 8.0データベースに保存している。データベースのパフォーマンスはアプリケーションの負荷が増加すると急速に低下する。アプリケーションは書き込みトランザクションよりも読み取りリクエストを多く処理している。企業は、高可用性を維持しつつ予測不可能な読み取りワークロードの需要に自動的にスケールするデータベースソリューションを求めている。どのソリューションがこれらの要件を満たすか？

A. リーダーおよびコンピュート機能を単一ノードで提供するAmazon Redshiftを使用する。

B. 単一アベイラビリティーゾーン展開のAmazon RDSを使用する。異なるアベイラビリティーゾーンにリーダーインスタンスを追加するようAmazon RDSを構成する。

C. マルチアベイラビリティーゾーン展開のAmazon Auroraを使用する。Auroraレプリカで Aurora Auto Scalingを構成する。

D. EC2スポットインスタンスとともにMemcached用のAmazon ElastiCacheを使用する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- 読み取り性能を自動的に拡張する
- 予測不可能な読み取りワークロードに対応する
- 可用性を維持する（複数アベイラビリティーゾーン）
- トランザクションデータは大規模なEC2インスタンス上のMySQL 8.0データベースに保存する

正解はCである。

Amazon Auroraは複数アベイラビリティーゾーンにまたがる高可用性アーキテクチャと高速なレプリケーション性能を提供し、Aurora読み取りレプリカを用いたAurora自動スケーリングは読み取り容量を自動的に拡張して予測不可能な読み取りワークロードに対応する。

不正解の理由

A. リーダーおよびコンピュート機能を単一ノードで提供するAmazon Redshiftを使用する。

Redshiftはデータウェアハウジングサービスであり、OLTP特性の読み取り遅延が短いトランザクション処理や高可用性要件を満たす設計ではない。

B. 単一アベイラビリティーゾーン展開のAmazon RDSを使用する。異なるアベイラビリティーゾーンにリーダーインスタンスを追加するようAmazon RDSを構成する。

単一AZのRDSは可用性保証が弱く、提案された構成（単一AZ＋別AZにリーダー追加）は一貫した複数AZ高可用性を保証しない。

D. EC2スポットインスタンスとともにMemcached用のAmazon ElastiCacheを使用する。

ElastiCacheはキャッシュとして読み取り応答を高速化できるが、MemcachedとEC2スポットの組み合わせは耐久性・可用性・一貫性要件を自動的に満たすデータベーススケーリングソリューションではない。

Q. 015

SAA-C03

ある企業が最近AWSに移行し、本番VPCの入出力トラフィックを保護するソリューションを実装したいと考えている。同社はオンプレミスのデータセンターに検査サーバーを設置していた。この検査サーバーはトラフィックフローの検査やトラフィックフィルタリングなどの特定の操作を実行していた。同様の機能をAWSクラウドで実現したい。どのソリューションがこれらの要件を満たすか？

A. 本番VPCのトラフィック検査とトラフィックフィルタリングにAmazon GuardDutyを使用する。

B. 本番VPCのトラフィックをミラーリングしてトラフィック検査とフィルタリングを行うためにTraffic Mirroringを使用する。

C. 本番VPCのトラフィック検査とトラフィックフィルタリングのために必要なルールを作成するためにAWS Network Firewallを使用する。

D. 本番VPCのトラフィック検査とトラフィックフィルタリングのために必要なルールを作成するためにAWS Firewall Managerを使用する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- プロダクションVPCの入出力トラフィックを検査すること
- トラフィックをフィルタリング（許可/拒否）する機能を提供すること
- オンプレミスデータセンターの検査サーバーと同等の機能をAWSクラウドで提供すること

正解はCである。

AWS Network FirewallはVPCに統合され、ステートフルおよびステートレスルールでトラフィックを検査・フィルタリング可能なマネージドファイアウォールサービスである。インラインのネットワークレベル検査およびブロックポリシーを直接適用でき、要件を満たす。

不正解の理由

A. 本番VPCのトラフィック検査とトラフィックフィルタリングにAmazon GuardDutyを使用する。
GuardDutyは脅威検出（侵害の兆候分析）サービスであり、トラフィックの直接フィルタリングやインラインブロック機能を提供しない。

B. 本番VPCのトラフィックをミラーリングしてトラフィック検査とフィルタリングを行うためにTraffic Mirroringを使用する。
Traffic Mirroringはトラフィックを複製して外部分析に送信する機能であり、インラインフィルタリングやトラフィックブロックは行わない。

D. 本番VPCのトラフィック検査とトラフィックフィルタリングのために必要なルールを作成するためにAWS Firewall Managerを使用する。

Firewall Managerは複数アカウントやリージョンのセキュリティポリシー管理サービスであり、独自にトラフィック検査やインラインフィルタリングを実施しない。

Q. 016

SAA-C03

ある企業がAWS上にデータレイクをホストしている。データレイクはAmazon S3とAmazon RDS for PostgreSQLのデータで構成されている。企業は、データレイク内のすべてのデータソースを含み、データの可視化を提供するレポーティングソリューションを必要としている。企業の経営陣のみがすべての可視化に完全アクセスでき、その他の社員は限定的なアクセスのみを許可する必要がある。これらの要件を満たすソリューションはどれか。

A. Amazon QuickSightで分析を作成する。すべてのデータソースに接続し、新しいデータセットを作成する。ダッシュボードを公開してデータを可視化する。適切なIAMロールとダッシュボードを共有する。

B. Amazon QuickSightで分析を作成する。すべてのデータソースに接続し、新しいデータセットを作成する。ダッシュボードを公開してデータを可視化する。適切なユーザーおよびグループとダッシュボードを共有する。

C. Amazon S3のデータに対してAWS Glueテーブルとクローラーを作成する。AWS GlueのETLジョブを作成してレポートを生成する。レポートをAmazon S3に公開する。S3バケットポリシーでレポートへのアクセスを制限する。

D. Amazon S3のデータに対してAWS Glueテーブルとクローラーを作成する。Amazon Athena Federated Queryを使用してAmazon RDS for PostgreSQL内のデータにアクセスする。Amazon Athenaでレポートを生成する。レポートをAmazon S3に公開する。S3バケットポリシーでレポートへのアクセスを制限する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- データレイクのすべてのデータソース（S3およびRDS for PostgreSQL）を含む可視化を提供すること
- 経営陣のみがすべての可視化に対して完全なアクセス権を持つこと
- その他の従業員は制限されたアクセスのみを持つこと
- 経営陣とその他の従業員で異なるアクセス権レベルがあること

正解はBである。

Amazon QuickSightは複数のデータソース（S3およびRDS）を接続し、統合ダッシュボードと可視化を作成可能である。ユーザーおよびグループベースの共有により、経営陣に完全な権限を付与し、他のユーザーには制限されたアクセスを適用できるため、要件を満たす。

不正解の理由

A. Amazon QuickSightで分析を作成する。すべてのデータソースに接続し、新しいデータセットを作成する。ダッシュボードを公開してデータを可視化する。適切なIAMロールとダッシュボードを共有する。

QuickSightのダッシュボード共有は主にユーザー／グループベースで管理され、IAMロールによる共有は一般的な方法ではないため、要件を正確に満たさない。

C. Amazon S3のデータに対してAWS Glueテーブルとクローラーを作成する。AWS GlueのETLジョブを作成してレポートを生成する。レポートをAmazon S3に公開する。S3バケットポリシーでレポートへのアクセスを制限する。

Glue ETLとS3に公開されたレポートは可視化プラットフォーム（ダッシュボード）を提供せず、ユーザー／グループレベルの対話的アクセス制御を容易に提供できない。

D. Amazon S3のデータに対してAWS Glueテーブルとクローラーを作成する。Amazon Athena Federated Queryを使用してAmazon RDS for PostgreSQL内のデータにアクセスする。Amazon Athenaでレポートを生成する。レポートをAmazon S3に公開する。S3バケットポリシーでレポートへのアクセスを制限する。

Athenaフェデレーテッドクエリで統合クエリは可能だが、結果をS3に公開する方法はダッシュボード型の可視化およびユーザー／グループ単位の細分化された共有機能を提供しない。

Q. 017

SAA-C03

ある企業が新しい業務アプリケーションを導入している。このアプリケーションは2台のAmazon EC2インスタンス上で稼働し、ドキュメントの保存にAmazon S3バケットを使用している。ソリューションアーキテクトは、EC2インスタンスがS3バケットにアクセスできるようにする必要がある。要件を満たすためにソリューションアーキテクトは何をすべきか？

A. S3バケットへのアクセスを許可するIAMロールを作成し、そのロールをEC2インスタンスにアタッチする。

B. S3バケットへのアクセスを許可するIAMポリシーを作成し、そのポリシーをEC2インスタンスにアタッチする。

C. S3バケットへのアクセスを許可するIAMグループを作成し、そのグループをEC2インスタンスにアタッチする。

D. S3バケットへのアクセスを許可するIAMユーザーを作成し、そのユーザーアカウントをEC2インスタンスにアタッチする。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- EC2インスタンスがAmazon S3バケットにアクセスする必要がある
- アプリケーションは2台のAmazon EC2インスタンスで実行される
- ドキュメント保存にAmazon S3バケットを使用する
- EC2インスタンスがS3バケットにアクセスできることを保証する必要がある

正解はAである。

IAMロールをEC2インスタンスに割り当てることで、インスタンスはインスタンスプロファイルを通じて自動的に一時的な認証情報を取得しS3にアクセス可能となる。これにより長期認証情報をインスタンスに保存する必要がなく、最小権限の適用が可能である。AWS推奨のパターンに合致する。

不正解の理由

B. S3バケットへのアクセスを許可するIAMポリシーを作成し、そのポリシーをEC2インスタンスにアタッチする。

IAMポリシーはポリシー単体でインスタンスに直接割り当てられず、ユーザー・ロール・グループなどの主体に紐付ける必要がある。EC2に直接ポリシーを付与することは不可能である。

C. S3バケットへのアクセスを許可するIAMグループを作成し、そのグループをEC2インスタンスにアタッチする。

IAMグループはユーザー管理用であり、EC2インスタンスに割り当てられないため要件を満たさない。

D. S3バケットへのアクセスを許可するIAMユーザーを作成し、そのユーザーアカウントをEC2インスタンスにアタッチする。

IAMユーザーは長期認証情報（アクセスキー/シークレットキー）を必要とし、インスタンスにキーをハードコーディングする必要があるためセキュリティ上不適切である。

Q. 018

SAA-C03

アプリケーション開発チームは、大きな画像を小さく圧縮された画像に変換するマイクロサービスを設計している。ユーザーがウェブインターフェイスから画像をアップロードすると、マイクロサービスは画像をAmazon S3バケットに保存し、AWS Lambda 関数で画像を処理および圧縮し、圧縮後の画像を別のS3バケットに保存する必要がある。ソリューションアーキテクトは、耐久性がありステートレスなコンポーネントを使用して画像を自動的に処理するソリューションを設計する必要がある。どのアクションの組み合わせがこれらの要件を満たすか。**（2つ選べ）**

A. Amazon Simple Queue Service（Amazon SQS）キューを作成する。S3バケットに画像がアップロードされたときにSQSキューに通知を送信するようにS3バケットを設定する。

B. Amazon Simple Queue Service（Amazon SQS）キューをLambda 関数のイベントソースとして設定する。SQSメッセージが正常に処理されたら、キュー内のメッセージを削除する。

C. Lambda 関数をS3バケットの新しいアップロードを監視するように設定する。アップロードされた画像が検出されたら、ファイル名をメモリ内のテキストファイルに書き込み、処理済みの画像を追跡するためにそのテキストファイルを使用する。

D. Amazon Simple Queue Service（Amazon SQS）キューを監視するAmazon EC2インスタンスを起動する。キューにアイテムが追加されたときに、EC2インスタンス上のテキストファイルにファイル名を記録し、Lambda 関数を呼び出す。

E. Amazon EventBridge（Amazon CloudWatch Events）イベントを設定してS3バケットを監視する。画像がアップロードされたときに、アプリケーション所有者のメールアドレスを含むAmazon Simple Notification Service（Amazon SNS）トピックにアラートを送信し、さらなる処理を行う。

✅ 正解: A、B / 解説

ソリューションは、次の要件を満たす必要がある。

- アップロードされた画像を自動で処理すること
- 処理パイプラインは耐久性を提供すること
- 構成要素はステートレスに設計すること
- 処理済み画像は別のS3バケットに圧縮形式で保存すること

正解はA、Bである。

S3、SQS、Lambdaを組み合わせることで、画像アップロードイベントを耐久性のあるSQSキューに保持し、Lambda 関数で非同期に処理できる。SQSにより一時的な処理失敗時にもメッセージを保持でき、Lambdaはステートレスに画像変換を実行できるため、自動処理、耐久性、ステートレス性の要件を満たす。

不正解の理由

C. Lambda 関数をS3バケットの新しいアップロードを監視するように設定する。アップロードされた画像が検出されたら、ファイル名をメモリ内のテキストファイルに書き込み、処理済みの画像を追跡するためにそのテキストファイルを使用する。

誤り：メモリ内のテキストファイルに処理状態を記録すると、ステートレス要件と耐久性を満たさず、信頼できない追跡方法となる。

D. Amazon Simple Queue Service（Amazon SQS）キューを監視するAmazon EC2インスタンスを起動する。キューにアイテムが追加されたときに、EC2インスタンス上のテキストファイルにファイル名を記録し、Lambda 関数を呼び出す。

誤り：EC2インスタンスとローカルテキストファイルはステートフルで運用負担が増大し、ステートレスかつ耐久性の要件を満たさない。

E. Amazon EventBridge（Amazon CloudWatch Events）イベントを設定してS3バケットを監視する。画像がアップロードされたときに、アプリケーション所有者のメールアドレスを含むAmazon Simple Notification Service（Amazon SNS）トピックにアラートを送信し、さらなる処理を行う。

誤り：SNSによるメール通知は自動画像処理ワークフローを実行せず、手動介入が必要なため要件を満たさない。

Q. 019

SAA-C03

ある企業はAWS上に3層のウェブアプリケーションを展開している。ウェブサーバーはVPCのパブリックサブネットに、アプリケーションサーバーとデータベースサーバーは同じVPCのプライベートサブネットに展開されている。企業はAWS Marketplaceからサードパーティの仮想ファイアウォールアプライアンスをインスペクションVPCに展開している。このアプライアンスはIPパケットを受け入れることができるIPインターフェイスで構成されている。ソリューションアーキテクトは、ウェブアプリケーションのすべてのトラフィックがウェブサーバーに到達する前にアプライアンスで検査されるように統合する必要がある。運用上の負担を最小限に抑えつつ、これらの要件を満たすソリューションはどれか。

A. アプリケーションのVPCのパブリックサブネットにNetwork Load Balancerを作成し、トラフィックをアプライアンスにルーティングしてパケット検査を行う。

B. アプリケーションのVPCのパブリックサブネットにApplication Load Balancerを作成し、トラフィックをアプライアンスにルーティングしてパケット検査を行う。

C. インスペクションVPCにトランジットゲートウェイを展開し、ルートテーブルを設定して受信パケットをトランジットゲートウェイ経由でルーティングする。

D. インスペクションVPCにGateway Load Balancerを展開し、Gateway Load Balancerエンドポイントを作成して受信パケットを受け取り、アプライアンスに転送する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- アプリケーショントラフィックのすべてのパケットをウェブサーバーに到達する前に検査すること
- サードパーティの仮想ファイアウォールアプライアンス（検査用VPC）にトラフィックを転送すること
- 運用上の負担を可能な限り最小限に抑えて実装すること
- ウェブサーバーはVPCのパブリックサブネットに配置すること
- アプリケーションサーバーとデータベースサーバーは同一VPCのプライベートサブネットに配置すること

正解はDである。

Gateway Load Balancer（GWLB）とGWLBエンドポイントは、ネットワークトラフィックを透過的にサードパーティのネットワーキングアプライアンスに送信可能に設計されており、スケーリングとヘルスチェックが統合されているため、パケット検査チェーンを運用上の負担を最小限に抑えて実装できる。

不正解の理由

A. アプリケーションのVPCのパブリックサブネットにNetwork Load Balancerを作成し、トラフィックをアプライアンスにルーティングしてパケット検査を行う。

Network Load BalancerはL4ロードバランシングに適するが、GWLBが提供する透過的なパケットチェイニングや自動スケーリング・連携機能を提供せず、運用負担が大きい。

B. アプリケーションのVPCのパブリックサブネットにApplication Load Balancerを作成し、トラフィックをアプライアンスにルーティングしてパケット検査を行う。

Application Load BalancerはL7サービスであり、生のIPパケット検査や透過的なパケットチェイニングには適さない。

C. インスペクションVPCにトランジットゲートウェイを展開し、ルートテーブルを設定して受信パケットをトランジットゲートウェイ経由でルーティングする。

Transit Gatewayはルーティングを提供するが、パケット検査用アプライアンスへの透過的なトラフィックチェイニングや自動スケーリングを提供せず、構成および運用負担が増加する。

Q. 020

SAA-C03

ある企業は、同一のAWSリージョン内で大量の本番データをテスト環境にクローンする能力を向上させたいと考えている。データはAmazon EC2インスタンスのAmazon Elastic Block Store（Amazon EBS）ボリュームに保存されている。クローンしたデータへの変更は本番環境に影響を与えてはならない。このデータにアクセスするソフトウェアは一貫して高いI/Oパフォーマンスを必要とする。ソリューションアーキテクトは、本番データをテスト環境にクローンするのに必要な時間を最小限に抑える必要がある。どのソリューションがこれらの要件を満たすか？

A. 本番のEBSボリュームのEBSスナップショットを取得する。テスト環境のEC2インスタンスストアボリュームにスナップショットを復元する。

B. 本番のEBSボリュームにEBSマルチアタッチ機能を設定する。本番のEBSボリュームのEBSスナップショットを取得する。本番のEBSボリュームをテスト環境のEC2インスタンスにアタッチする。

C. 本番のEBSボリュームのEBSスナップショットを取得する。新しいEBSボリュームを作成して初期化する。新しいEBSボリュームをテスト環境のEC2インスタンスにアタッチしてから、本番のEBSスナップショットからボリュームを復元する。

D. 本番のEBSボリュームのEBSスナップショットを取得する。EBSスナップショットでEBS高速スナップショット復元機能を有効にする。スナップショットを新しいEBSボリュームに復元する。新しいEBSボリュームをテスト環境のEC2インスタンスにアタッチする。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 同一AWSリージョン内で大量のEBSベースブロックストレージデータをテスト用に複製すること
- 複製データの変更が本番環境に影響を与えない（分離されていること）
- 複製データは一貫して高いI/O性能を提供すること
- 複製にかかる時間を最小限に抑えること

正解はDである。

EBS Fast Snapshot Restore(FSR)を有効化すると、スナップショットから復元された新しいEBSボリュームは即座に初期化され、初期化遅延なしで一貫した高いI/O性能を提供するため、複製時間と性能要件を満たし、新しいボリュームは本番環境と分離されており変更が本番に影響しない。

不正解の理由

A. 本番のEBSボリュームのEBSスナップショットを取得する。テスト環境のEC2インスタンスストアボリュームにスナップショットを復元する。
インスタンスストアはスナップショットから直接復元する標準的な対象ではなく、耐久性および管理面で要件を満たさない。

B. 本番のEBSボリュームにEBSマルチアタッチ機能を設定する。本番のEBSボリュームのEBSスナップショットを取得する。本番のEBSボリュームをテスト環境のEC2インスタンスにアタッチする。

Multi-Attachで同一ボリュームを共有するとテスト環境の変更が本番に影響し、分離要件に違反する。

C. 本番のEBSボリュームのEBSスナップショットを取得する。新しいEBSボリュームを作成して初期化する。新しいEBSボリュームをテスト環境のEC2インスタンスにアタッチしてから、本番のEBSスナップショットからボリュームを復元する。

スナップショットから作成した新しいEBSボリュームは初回アクセス時に遅延（遅延ブロック初期化）が発生し、即時に一貫した高いI/O性能を保証できない。

Q. 021

SAA-C03

あるEC企業が、AWS上で1日1商品限定のセールサイトを立ち上げたいと考えている。毎日24時間限定で1つの商品を特集する。ピーク時には毎時数百万のリクエストをミリ秒単位のレイテンシで処理できることが求められる。これらの要件を最も運用負荷を抑えて満たすソリューションはどれか。

A. Amazon S3を使用して、異なるS3バケットにフルサイトをホストする。Amazon CloudFrontディストリビューションを追加し、S3バケットをオリジンに設定する。注文データはAmazon S3に保存する。

B. Amazon EC2インスタンスを複数のアベイラビリティーゾーンにまたがるAuto Scalingグループで展開し、フルサイトをホストする。Application Load Balancer（ALB）を追加してサイトトラフィックを分散し、バックエンドAPI用に別のALBを追加する。データはAmazon RDS for MySQLに保存する。

C. フルアプリケーションをコンテナに移行し、Amazon Elastic Kubernetes Service（Amazon EKS）でホストする。Kubernetes Cluster Autoscalerを使用してトラフィックの急増に応じてPod数を増減させる。データはAmazon RDS for MySQLに保存する。

D. Amazon S3バケットを使用してウェブサイトの静的コンテンツをホストし、Amazon CloudFrontディストリビューションを展開する。S3バケットをオリジンに設定する。バックエンドAPIにはAmazon API GatewayとAWS Lambda 関数を使用し、データはAmazon DynamoDBに保存する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 1日に1つの商品を24時間特徴的に表示する
- ピーク時に1時間あたり数百万件のリクエストを処理する
- 応答遅延がミリ秒単位である
- 運用上の負担を最小限に抑える

正解はDである。

CloudFrontとS3で静的コンテンツをグローバルにキャッシュしミリ秒単位の遅延を実現、API GatewayとLambda（サーバーレス）、およびAmazon DynamoDB（マネージドNoSQL）が自動スケーリングと高スループットを提供し運用負荷を最小化する。

不正解の理由

A. Amazon S3を使用して、異なるS3バケットにフルサイトをホストする。Amazon CloudFrontディストリビューションを追加し、S3バケットをオリジンに設定する。注文データはAmazon S3に保存する。

S3とCloudFrontで静的ホスティングは可能だが、注文データや高い同時処理のトランザクションをS3（オブジェクトストレージ）に保存するのは適切でなく、一貫性や性能要件を満たさない。

B. Amazon EC2インスタンスを複数のアベイラビリティーゾーンにまたがるAuto Scalingグループで展開し、フルサイトをホストする。Application Load Balancer（ALB）を追加してサイトトラフィックを分散し、バックエンドAPI用に別のALBを追加する。データはAmazon RDS for MySQLに保存する。

EC2、ALB、RDSの組み合わせは実現可能だが、インフラとデータベースの水平スケーリングや管理が複雑であり、運用負荷最小化の要件を満たさない。

C. フルアプリケーションをコンテナに移行し、Amazon Elastic Kubernetes Service（Amazon EKS）でホストする。Kubernetes Cluster Autoscalerを使用してトラフィックの急増に応じてPod数を増減させる。データはAmazon RDS for MySQLに保存する。

EKSはコンテナオーケストレーションの柔軟性を提供するが、クラスター管理やチューニングの運用負荷が大きく、自動化されたサーバーレスより複雑である。

Q. 022

SAA-C03

ソリューションアーキテクトは、Amazon S3を使用して新しいデジタルメディアアプリケーションのストレージアーキテクチャを設計している。メディアファイルはアベイラビリティーゾーンの喪失に耐えられなければならない。ファイルの中には頻繁にアクセスされるものもあれば、予測不可能なパターンでまれにアクセスされるものもある。ソリューションアーキテクトは、メディアファイルの保存および取得のコストを最小限に抑えなければならない。これらの要件を満たすストレージオプションはどれか。

A. S3 Standard

B. S3 Intelligent-Tiering

C. S3 Standard-Infrequent Access (S3 Standard-IA)

D. S3 One Zone-Infrequent Access（S3 One Zone-IA）

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- アベイラビリティーゾーンの損失に対する復元力を保証すること
- 頻繁にアクセスされるオブジェクトと稀にアクセスされるオブジェクトが混在し、アクセスパターンが予測できないこと
- 保存コストおよび取得コストを最小化すること

正解はBである。

S3 Intelligent-Tieringはオブジェクトのアクセスパターンを自動的に検出し、適切なストレージ階層に移動させることで、予測不可能なアクセスパターンに対して保存コストを最適化する。また、すべての階層がマルチアベイラビリティーゾーンで耐久性と可用性を提供するため、要件を満たす。

不正解の理由

A. S3 Standard

S3 Standardは頻繁にアクセスされるオブジェクトに適しているが、稀なアクセスに対してコスト最適化されておらず、予測不可能なパターンではコストが高くなる可能性がある。

C. S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IAはマルチAZ耐久性を提供するが、頻繁にアクセスされるオブジェクトに対して取得コストとレイテンシーが増加し、予測不可能な混合パターンではコストと性能の面で非効率的となる可能性がある。

D. S3 One Zone-Infrequent Access（S3 One Zone-IA）

S3 One Zone-IAは単一アベイラビリティーゾーンにのみ保存されるため、アベイラビリティーゾーンの損失に対する復元力の要件を満たさない。

Q. 023

SAA-C03

ある企業はバックアップファイルをAmazon S3 Standardストレージを使用して保存している。ファイルは1か月間頻繁にアクセスされるが、その後はアクセスされない。企業はファイルを無期限に保持しなければならない。これらの要件を最もコスト効率よく満たすストレージソリューションはどれか。

A. S3 Intelligent-Tieringを設定してオブジェクトを自動的に移行する。

B. S3 Lifecycle設定を作成し、1か月後にオブジェクトをS3 StandardからS3 Glacier Deep Archiveに移行する。

C. S3 Lifecycle設定を作成し、1か月後にオブジェクトをS3 StandardからS3 Standard-Infrequent Access (S3 Standard-IA)に移行する。

D. S3 Lifecycle設定を作成し、1か月後にオブジェクトをS3 StandardからS3 One Zone-Infrequent Access (S3 One Zone-IA)に移行する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- ファイルは最初の1か月間頻繁にアクセスされる
- 1か月以降はアクセスされない（無期限保管が必要）
- 長期保管に最もコスト効率が良いこと
- 会社はAmazon S3 Standardストレージにバックアップファイルを保存している

正解はBである。

S3 Glacier Deep Archiveは長期保管向けで、S3ストレージクラスの中で最も低い保存コストを提供し、1か月後にアクセスがなくなるパターンに対してコスト効率が良い。ライフサイクルで1か月後に移行することで、初期の頻繁なアクセス期間を確保しつつ、その後の長期保管コストを最小化する。またGlacier Deep ArchiveはS3の高い耐久性を維持する。

不正解の理由

A. S3 Intelligent-Tieringを設定してオブジェクトを自動的に移行する。

S3 Intelligent-Tieringはアクセスパターンが不確実な場合に有用だが、アーカイブ層は最低保存期間や監視・管理コストがあり、この特定の（1か月後に全くアクセスしない）シナリオでは最もコスト効率が良いとは限らない。

C. S3 Lifecycle設定を作成し、1か月後にオブジェクトをS3 StandardからS3 Standard-Infrequent Access (S3 Standard-IA)に移行する。

S3 Standard-IAは頻繁にアクセスされないオブジェクトに適しているが、Glacier Deep Archiveより保存コストが高いため無期限の長期保管ではコスト効率が低い。

D. S3 Lifecycle設定を作成し、1か月後にオブジェクトをS3 StandardからS3 One Zone-Infrequent Access (S3 One Zone-IA)に移行する。

S3 One Zone-IAは単一アベイラビリティーゾーンにのみ保存されるため耐久性・可用性リスクがあり、「無期限保管」の要件には適さない。

Q. 024

SAA-C03

ある企業が最新の請求書でAmazon EC2のコスト増加を観察した。請求チームは数台のEC2インスタンスで望ましくない垂直スケーリングが発生していることに気付いた。ソリューションアーキテクトは、過去2か月のEC2コストを比較するグラフを作成し、垂直スケーリングの根本原因を特定するために詳細な分析を行う必要がある。運用上の負担を最小限に抑えて情報を生成するにはどうすべきか？

A. AWS Budgetsを使用して予算レポートを作成し、インスタンスタイプに基づくEC2コストを比較する。

B. Cost Explorerの詳細なフィルタリング機能を使用して、インスタンスタイプに基づくEC2コストの詳細な分析を行う。

C. AWS Billing and Cost Managementダッシュボードのグラフを使用して、過去2か月のインスタンスタイプに基づくEC2コストを比較する。

D. AWS Cost and Usage Reportsを使用してレポートを作成し、Amazon S3バケットに送信する。Amazon S3をソースとするAmazon QuickSightでインスタンスタイプに基づくインタラクティブなグラフを生成する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 過去2か月間のEC2コストをインスタンスタイプ別に比較するグラフを作成すること
- インスタンスタイプ変更（垂直スケーリング）の根本原因を特定するための詳細分析を行うこと
- 運用上の負担を可能な限り最小限に抑えること

正解はBである。

Cost Explorerはインスタンスタイプ別にコストを細分化し、過去期間の比較やフィルタリングを即座に提供するため、別途レポートパイプラインを構築せずに迅速な詳細分析が可能であり、運用負担が最も低い。

不正解の理由

A. AWS Budgetsを使用して予算レポートを作成し、インスタンスタイプに基づくEC2コストを比較する。

AWS Budgetsは予算超過通知などの用途には適しているが、インスタンスタイプレベルの詳細なコスト分析やインタラクティブな探索機能が限定的である。

C. AWS Billing and Cost Managementダッシュボードのグラフを使用して、過去2か月のインスタンスタイプに基づくEC2コストを比較する。

請求およびコスト管理ダッシュボードの基本グラフはインスタンスタイプレベルの詳細なフィルタリングや分析機能が不足しており、根本原因の特定には不適切である。

D. AWS Cost and Usage Reportsを使用してレポートを作成し、Amazon S3バケットに送信する。Amazon S3をソースとするAmazon QuickSightでインスタンスタイプに基づくインタラクティブなグラフを生成する。

AWS Cost and Usage ReportsとQuickSightは非常に詳細な分析が可能であるが、S3やQuickSightの設定およびデータ処理が必要なため初期設定および運用負担が大きく、最小限の運用負担という要件を満たさない。

Q. 025

SAA-C03

ある企業がアプリケーションを設計している。このアプリケーションは、Amazon API Gatewayを通じて情報を受信し、その情報をAmazon Aurora PostgreSQLデータベースに保存するためにAWS Lambda 関数を使用している。概念実証段階では、企業がデータベースにロードする必要がある大量のデータを処理するために、Lambdaのクォータを大幅に増やす必要があった。ソリューションアーキテクトは、スケーラビリティを向上させ、設定作業を最小限に抑える新しい設計を推奨しなければならない。どのソリューションがこれらの要件を満たすか？

A. Lambda 関数のコードをApache Tomcatコードにリファクタリングし、Amazon EC2インスタンス上で実行する。ネイティブのJava Database Connectivity（JDBC）ドライバーを使用してデータベースに接続する。

B. プラットフォームをAuroraからAmazon DynamoDBに変更する。DynamoDB Accelerator（DAX）クラスターをプロビジョニングし、既存のDynamoDB API呼び出しをDAXクラスターに向けるためにDAXクライアントSDKを使用する。

C. 2つのLambda 関数を設定する。1つの関数を情報の受信に、もう1つの関数をデータベースへの情報のロードに設定する。Amazon Simple Notification Service（Amazon SNS）を使用してLambda 関数を統合する。

D. 2つのLambda 関数を設定する。1つの関数を情報の受信に、もう1つの関数をデータベースへの情報のロードに設定する。Amazon Simple Queue Service（Amazon SQS）キューを使用してLambda 関数を統合する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 大量データロードを処理可能なスケーラビリティ向上
- 構成作業を最小限に抑える
- Lambdaの割り当てを大幅に増やさずにスループットを吸収またはバッファリング
- Aurora PostgreSQLへのデータロードを維持

正解はDである。

SQSを用いて受信関数とロード関数を非同期に分離することで、メッセージバッファリングによりバックプレッシャーを吸収し、Lambdaの同時実行数増加要求を緩和する。SQSとLambdaの統合はマネージドサービスであり構成作業が少ない。Auroraへのロードロジックは別のコンシューマLambdaで維持可能であり、最小限のリファクタリングでスケーラビリティを保証する。

不正解の理由

A. Lambda 関数のコードをApache Tomcatコードにリファクタリングし、Amazon EC2インスタンス上で実行する。ネイティブのJava Database Connectivity（JDBC）ドライバーを使用してデータベースに接続する。

EC2/Tomcatに切り替えるとマネージドサーバーでの実行が必要となり、運用負担と構成作業が増加し、「構成最小化」の要件を満たさない。

B. プラットフォームをAuroraからAmazon DynamoDBに変更する。DynamoDB Accelerator（DAX）クラスターをプロビジョニングし、既存のDynamoDB API呼び出しをDAXクラスターに向けるためにDAXクライアントSDKを使用する。

AuroraをDynamoDBに変更するとデータモデルとアプリケーションロジックの大規模なリファクタリングが必要で構成作業が増え、RDBの特性維持要件を満たさない。DAXはRDBの問題解決策ではない。

C. 2つのLambda 関数を設定する。1つの関数を情報の受信に、もう1つの関数をデータベースへの情報のロードに設定する。Amazon Simple Notification Service（Amazon SNS）を使用してLambda 関数を統合する。

SNSはPub/Subメッセージングに適するが、メッセージバッファリングや順序保証、コンシューマ側のバックプレッシャー制御が弱く、大量データロードのバッファリング役としてSQSより不適切である。

Q. 026

SAA-C03

企業は、Amazon S3バケットに不正な設定変更がないことを確認するためにAWSクラウドの展開を見直す必要がある。ソリューションアーキテクトはこの目的を達成するために何をすべきか？

A. 適切なルールを設定してAWS Configを有効にする。

B. 適切なチェックを設定してAWS Trusted Advisorを有効にする。

C. 適切な評価テンプレートを設定してAmazon Inspectorを有効にする。

D. Amazon S3サーバーアクセスログを有効にし、Amazon EventBridge（Amazon CloudWatch Events）を設定する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- Amazon S3バケットの不正な構成変更を防止するために監査する
- AWSクラウドの展開を監査する
- 不正な構成変更が発生しないようにする

正解はAである。

AWS Configはリソースの構成履歴と変更を記録し、ルールを通じてS3バケット設定の準拠状況を継続的に評価し、違反時には通知や自動修正（即時修正ルール）と連携可能であり、要件を満たす。

不正解の理由

B. 適切なチェックを設定してAWS Trusted Advisorを有効にする。

AWS Trusted Advisorはコスト・セキュリティ・推奨事項のチェックに重点を置き、S3の不正な構成変更を継続的に記録・評価する機能を提供しない。

C. 適切な評価テンプレートを設定してAmazon Inspectorを有効にする。

Amazon InspectorはEC2インスタンスのセキュリティ脆弱性評価サービスであり、S3構成変更の検出とは目的が異なる。

D. Amazon S3サーバーアクセスログを有効にし、Amazon EventBridge（Amazon CloudWatch Events）を設定する。

S3サーバーアクセスログとEventBridgeはアクセスログやイベントベースの処理に有用であるが、S3構成の変更履歴やルールベースの準拠評価を提供しない。

Q. 027

SAA-C03

ある企業が新しいアプリケーションを立ち上げ、Amazon CloudWatch ダッシュボードにアプリケーションのメトリクスを表示する予定である。プロダクトマネージャーはこのダッシュボードに定期的にアクセスする必要があるが、AWSアカウントを持っていない。ソリューションアーキテクトは最小権限の原則に従い、プロダクトマネージャーにアクセスを提供しなければならない。これらの要件を満たすソリューションはどれか。

A. CloudWatch コンソールからダッシュボードを共有する。プロダクトマネージャーのメールアドレスを入力し、共有手順を完了する。ダッシュボードの共有可能なリンクをプロダクトマネージャーに提供する。

B. プロダクトマネージャー専用の IAM ユーザーを作成する。CloudWatchReadOnlyAccess AWS 管理ポリシーをユーザーにアタッチする。新しいログイン認証情報をプロダクトマネージャーと共有する。正しいダッシュボードのブラウザ URL をプロダクトマネージャーに共有する。

C. 企業の従業員用の IAM ユーザーを作成する。ViewOnlyAccess AWS 管理ポリシーを IAM ユーザーにアタッチする。新しいログイン認証情報をプロダクトマネージャーと共有する。プロダクトマネージャーに CloudWatch コンソールに移動し、ダッシュボードセクションで名前からダッシュボードを探すよう依頼する。

D. パブリックサブネットに踏み台サーバーを展開する。プロダクトマネージャーがダッシュボードにアクセスする必要があるときにサーバーを起動し、RDP 認証情報を共有する。踏み台サーバー上で、適切な権限を持つキャッシュされた AWS 認証情報でダッシュボード URL を開くようブラウザを設定する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- AWSアカウントを持たないユーザーである
- ダッシュボードに定期的にアクセスする必要がある
- 最小権限の原則を遵守する

正解はAである。

CloudWatchダッシュボードはAWSアカウントを持たない外部ユーザーにも読み取り専用の共有リンクを提供可能である。コンソールのメールベース共有を利用すればIAMユーザーを作成せずに特定のダッシュボードのみアクセス可能であり、最小権限の原則を正確に満たす。運用およびセキュリティの負担も最も低い。

不正解の理由

B. プロダクトマネージャー専用の IAM ユーザーを作成する。CloudWatchReadOnlyAccess AWS 管理ポリシーをユーザーにアタッチする。新しいログイン認証情報をプロダクトマネージャーと共有する。正しいダッシュボードのブラウザ URL をプロダクトマネージャーに共有する。

IAMユーザーを新規作成しCloudWatchReadOnlyAccessを付与する方法は、AWSアカウントを持たないユーザーに不必要なアカウントアクセス権を与えるため最小権限の原則に反する。

C. 企業の従業員用の IAM ユーザーを作成する。ViewOnlyAccess AWS 管理ポリシーを IAM ユーザーにアタッチする。新しいログイン認証情報をプロダクトマネージャーと共有する。プロダクトマネージャーに CloudWatch コンソールに移動し、ダッシュボードセクションで名前からダッシュボードを探すよう依頼する。

ViewOnlyAccessはCloudWatchダッシュボードだけでなく多数のAWSサービスリソースの閲覧を許可するため権限範囲が過剰である。またアカウント作成自体が不要なセキュリティおよび運用負担となる。

D. パブリックサブネットに踏み台サーバーを展開する。プロダクトマネージャーがダッシュボードにアクセスする必要があるときにサーバーを起動し、RDP 認証情報を共有する。踏み台サーバー上で、適切な権限を持つキャッシュされた AWS 認証情報でダッシュボード URL を開くようブラウザを設定する。

バスチョンサーバー経由のアクセスはダッシュボード閲覧という単純な要件に対して構成が過剰に複雑であり、認証情報管理・サーバー運用・セキュリティリスクも発生し、最小権限および運用効率の条件を両方満たさない。

Q. 028

SAA-C03

ある企業がアプリケーションをAWSに移行している。アプリケーションは異なるアカウントにデプロイされている。企業はAWS Organizationsを使用してアカウントを集中管理している。企業のセキュリティチームは、全アカウントにわたるシングルサインオン（SSO）ソリューションを必要としている。企業はオンプレミスの自己管理型Microsoft Active Directoryでユーザーとグループの管理を継続しなければならない。これらの要件を満たすソリューションはどれか。

A. AWS SSOコンソールからAWS Single Sign-On（AWS SSO）を有効化する。AWS Directory Service for Microsoft Active Directoryを使用して、企業の自己管理型Microsoft Active DirectoryとAWS SSOを接続するために、一方向のフォレストトラストまたは一方向のドメイントラストを作成する。

B. AWS SSOコンソールからAWS Single Sign-On（AWS SSO）を有効化する。AWS Directory Service for Microsoft Active Directoryを使用して、企業の自己管理型Microsoft Active DirectoryとAWS SSOを接続するために、双方向のフォレストトラストを作成する。

C. AWS Directory Serviceを使用する。企業の自己管理型Microsoft Active Directoryと双方向のトラスト関係を作成する。

D. オンプレミスにIDプロバイダー（IdP）をデプロイする。AWS SSOコンソールからAWS Single Sign-On（AWS SSO）を有効化する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- すべてのAWSアカウントにわたる集中型シングルサインオン(SSO)を提供すること
- ユーザーおよびグループ管理はオンプレミスの自己管理Microsoft Active Directoryで継続すること
- AWS Organizationsで管理される複数アカウント環境と統合すること
- アプリケーションは異なるAWSアカウントに展開されていること

正解はAである。

AWS Organizations環境で複数アカウントに対して単一のSSOを提供するには、AWS Single Sign-On（AWS SSO、現IAM Identity Center）を使用する必要がある。オンプレミスの自己管理Microsoft Active Directoryを継続使用するため、AWS Directory Service for Microsoft ADとの一方向トラストを介してAWS SSOと連携する方法が要件を正確に満たす。

不正解の理由

B. AWS SSOコンソールからAWS Single Sign-On（AWS SSO）を有効化する。AWS Directory Service for Microsoft Active Directoryを使用して、企業の自己管理型Microsoft Active DirectoryとAWS SSOを接続するために、双方向のフォレストトラストを作成する。

双方向フォレストトラストは過剰な権限と信頼範囲を生み出す。AWS SSO連携には一方向トラストで十分であり、セキュリティ原則上過剰なトラストは推奨されない。

C. AWS Directory Serviceを使用する。企業の自己管理型Microsoft Active Directoryと双方向のトラスト関係を作成する。

AWS Directory Service単体では複数AWSアカウントに対する集中SSOを提供できない。またAWS SSO（IAM Identity Center）を使用しないため要件を満たさない。

D. オンプレミスにIDプロバイダー（IdP）をデプロイする。AWS SSOコンソールからAWS Single Sign-On（AWS SSO）を有効化する。

オンプレミスIdPを直接構築する方法は可能だが、AWS SSOによる基本統合経路より運用負担が大きく不必要に複雑である。要件上は管理された統合を優先する。

Q. 029

SAA-C03

ある企業はUDP接続を使用するVoice over Internet Protocol（VoIP）サービスを提供している。このサービスはAuto Scalingグループで稼働するAmazon EC2インスタンスで構成されている。企業は複数のAWSリージョンに展開している。ユーザーを最も低遅延のリージョンにルーティングし、リージョン間での自動フェイルオーバーも必要である。これらの要件を満たすソリューションはどれか。

A. Network Load Balancer（NLB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各リージョンでNLBをAWS Global Acceleratorのエンドポイントとして使用する。

B. Application Load Balancer（ALB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各リージョンでALBをAWS Global Acceleratorのエンドポイントとして使用する。

C. Network Load Balancer（NLB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各NLBのエイリアスを指すAmazon Route 53のレイテンシーレコードを作成する。レイテンシーレコードをオリジンとして使用するAmazon CloudFrontディストリビューションを作成する。

D. Application Load Balancer（ALB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各ALBのエイリアスを指すAmazon Route 53の加重レコードを作成する。加重レコードをオリジンとして使用するAmazon CloudFrontディストリビューションをデプロイする。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- UDPベースのトラフィック（VoIP）をサポートすること
- ユーザーを最も低遅延のリージョンにルーティングすること
- リージョン間の自動フェイルオーバーを実現すること
- Auto Scalingグループで実行されるEC2インスタンスと統合すること

正解はAである。

AWS Global AcceleratorはAnycastを用いてユーザーを最も低遅延のエンドポイントにルーティングし、リージョン障害時に自動フェイルオーバーをサポートする。NLBはUDPトラフィックを処理可能でVoIP要件に適合し、Auto Scalingグループと直接連携できる。

不正解の理由

B. Application Load Balancer（ALB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各リージョンでALBをAWS Global Acceleratorのエンドポイントとして使用する。

ALBは主にHTTP/HTTPS（L7）トラフィック向けのロードバランサーであり、UDPをサポートしないためVoIP要件を満たさない。

C. Network Load Balancer（NLB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各NLBのエイリアスを指すAmazon Route 53のレイテンシーレコードを作成する。レイテンシーレコードをオリジンとして使用するAmazon CloudFrontディストリビューションを作成する。

Route 53の遅延ルーティングとNLBは一部の遅延最適化を提供するが、Route 53とCloudFrontの組み合わせはUDPリアルタイムトラフィック（CloudFrontはUDP非対応）やGlobal Acceleratorの提供するグローバルAnycastベースの自動フェイルオーバー機能を代替できない。

D. Application Load Balancer（ALB）と関連するターゲットグループをデプロイする。ターゲットグループをAuto Scalingグループに関連付ける。各ALBのエイリアスを指すAmazon Route 53の加重レコードを作成する。加重レコードをオリジンとして使用するAmazon CloudFrontディストリビューションをデプロイする。

ALBとCloudFrontはUDPをサポートせず、重み付けベースのRoute 53は自動的に最も低遅延のリージョンにルーティングしたり迅速なリージョン障害対応を保証しない。

Q. 030

SAA-C03

開発チームは、Performance Insightsを有効にした汎用のAmazon RDS for MySQLインスタンスで、毎月48時間にわたるリソース集約型のテストを実行している。このテストは月に1回のみ実行され、データベースを使用する唯一のプロセスである。チームはDBインスタンスのコンピューティングおよびメモリ属性を減らすことなく、テスト実行のコストを削減したい。これらの要件を最もコスト効率よく満たすソリューションはどれか。

A. テスト完了後にDBインスタンスを停止し、必要時にDBインスタンスを再起動する。

B. DBインスタンスにAuto Scalingポリシーを使用して、テスト完了後に自動的にスケールするようにする。

C. テスト完了後にスナップショットを作成し、DBインスタンスを終了して必要時にスナップショットから復元する。

D. テスト完了後にDBインスタンスを低容量インスタンスに変更し、必要時に再度DBインスタンスを変更する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 月に1回、48時間DBインスタンスを使用する
- DBインスタンスのコンピューティングおよびメモリ属性を削減できない
- テスト実行コストを削減したい
- Performance Insightsが有効な汎用Amazon RDS for MySQL DBインスタンスでテストを実施する

正解はAである。

テストは毎月48時間のみ実施され、それ以外の期間はDBを使用しないため、DBインスタンスを停止して不要なインスタンス稼働コストを削減する方法が最もコスト効率的である。インスタンスのサイズ（コンピューティング/メモリ）を変更せず、必要なときに再起動して同じ性能でテストを実行できる。

不正解の理由

B. DBインスタンスにAuto Scalingポリシーを使用して、テスト完了後に自動的にスケールするようにする。

「自動スケーリング」はRDS単一インスタンスのコンピューティング/メモリをテスト後に自動で削減する概念ではない。通常はストレージの自動拡張（容量）であり、問題の要件（コンピューティング/メモリ維持＋コスト削減）とは異なる。

C. テスト完了後にスナップショットを作成し、DBインスタンスを終了して必要時にスナップショットから復元する。

スナップショット→終了→復元はコスト削減になるが、運用負担や復元時間（RTO）、エンドポイント変更の可能性など変数が多く、毎月の繰り返しテストには過度に複雑である。「コンピューティング/メモリ

属性を削減しない」条件で毎回再構築するアプローチは要件上は選びにくい。

D. テスト完了後にDBインスタンスを低容量インスタンスに変更し、必要時に再度DBインスタンスを変更する。

テスト後に低容量に変更することは「コンピューティング/メモリ属性を削減しない」という条件と正面から矛盾する。また、変更作業自体が繰り返しの運用負担を生む。

Q. 031

SAA-C03

AWS上でウェブアプリケーションをホストする企業が、すべてのAmazon EC2インスタンス、Amazon RDS DBインスタンス、およびAmazon Redshiftクラスターにタグが設定されていることを保証したい。企業はこのチェックの設定および運用の労力を最小限に抑えたい。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か？

A. AWS Configルールを使用して、適切にタグ付けされていないリソースを定義および検出する。

B. Cost Explorerを使用して適切にタグ付けされていないリソースを表示し、それらのリソースに手動でタグを付ける。

C. すべてのリソースのタグ割り当てを確認するAPIコールを作成し、EC2インスタンス上で定期的にコードを実行する。

D. すべてのリソースのタグ割り当てを確認するAPIコールを作成し、Amazon CloudWatchを通じてAWS Lambda 関数をスケジュールし、定期的にコードを実行する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- すべてのEC2インスタンス、RDS DBインスタンス、およびRedshiftクラスターにタグが付与されていること
- 検査の構成および運用上の負担を最小限に抑えること
- すべてのAmazon EC2インスタンス、Amazon RDS DBインスタンス、およびAmazon Redshiftクラスターのタグの存在を確認すること

正解はAである。

AWS Configは管理されたコンプライアンスサービスであり、タグに関するルールを定義し継続的に評価することで、適切にタグ付けされていないリソースを自動的に検出し報告する。これにより、別途インフラを運用することなく検査と継続的な監視を実施でき、運用負荷を最小限に抑える。

不正解の理由

B. Cost Explorerを使用して適切にタグ付けされていないリソースを表示し、それらのリソースに手動でタグを付ける。

Cost Explorerはコスト分析用であり、タグの準拠を継続的に自動監視および自動修正する機能を提供しないため、手動でのタグ付けが必要となり運用負荷が増大する。

C. すべてのリソースのタグ割り当てを確認するAPIコールを作成し、EC2インスタンス上で定期的にコードを実行する。

EC2上で定期的に実行されるカスタムスクリプトはインスタンスの運用および保守が必要であり、運用負荷が増加する。

D. すべてのリソースのタグ割り当てを確認するAPIコールを作成し、Amazon CloudWatchを通じてAWS Lambda 関数をスケジュールし、定期的にコードを実行する。

Lambdaの予約実行方式は自動化可能であるが、カスタムコードの保守および準拠報告・評価機能を自ら実装する必要があり、AWS Configより運用負荷が大きい。

Q. 032

SAA-C03

開発チームは、他のチームがアクセスするウェブサイトをホストする必要がある。ウェブサイトの内容はHTML、CSS、クライアントサイドJavaScript、および画像で構成されている。ウェブサイトをホストするための最もコスト効率の高い方法はどれか。

A. ウェブサイトをコンテナ化し、AWS Fargateでホストする。

B. Amazon S3バケットを作成し、そこでウェブサイトをホストする。

C. Amazon EC2インスタンスにウェブサーバーをデプロイしてウェブサイトをホストする。

D. Express.jsフレームワークを使用するAWS Lambdaターゲットを持つアプリケーションロードバランサーを構成する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 他チームがアクセス可能であること
- コスト効率が良いこと
- 開発チームがウェブサイトをホスティングすること
- ウェブサイトのコンテンツがHTML、CSS、クライアント側JavaScriptおよび画像で構成されていること

正解はBである。

Amazon S3はオブジェクトストレージであり、静的コンテンツのホスティングに最適で、コスト効率が高く自動的にスケールし、運用上の負担がほとんどない。追加のサーバー管理やコンテナのオーバーヘッドが不要であり、要件に最も適合する。

不正解の理由

A. ウェブサイトをコンテナ化し、AWS Fargateでホストする。

Fargateはコンテナ管理を簡素化するが、静的サイトには不要なコストと設定の複雑さをもたらし、コスト効率が悪い。

C. Amazon EC2インスタンスにウェブサーバーをデプロイしてウェブサイトをホストする。

EC2はウェブサーバーやOSの管理、容量計画および保守が必要であり、運用負担と総コストが増加する。

D. Express.jsフレームワークを使用するAWS Lambdaターゲットを持つアプリケーションロードバランサーを構成する。

ALBとLambda（Express）は不要なアーキテクチャの複雑さとコストを引き起こし、静的ファイルの配信には過剰である。

Q. 033

SAA-C03

ある企業はAWS上でオンラインマーケットプレイスのウェブアプリケーションを運用している。このアプリケーションはピーク時に数十万人のユーザーにサービスを提供する。企業は数百万件の金融取引の詳細を複数の内部アプリケーションとスケーラブルかつほぼリアルタイムで共有するソリューションを必要としている。取引はまた、低レイテンシーでの取得のためにドキュメントデータベースに保存する前に機密データを除去して処理する必要がある。これらの要件を満たすためにソリューションアーキテクトは何を推奨すべきか？

A. 取引データをAmazon DynamoDBに保存する。DynamoDBでルールを設定し、書き込み時にすべての取引から機密データを除去する。DynamoDB Streamsを使用して取引データを他のアプリケーションと共有する。

B. 取引データをAmazon Kinesis Data Firehoseにストリーミングし、Amazon DynamoDBとAmazon S3にデータを保存する。Kinesis Data Firehoseと連携したAWS Lambdaを使用して機密データを除去する。他のアプリケーションはAmazon S3に保存されたデータを利用できる。

C. 取引データをAmazon Kinesis Data Streamsにストリーミングする。AWS Lambdaとの統合を使用して各取引から機密データを除去し、その後、取引データをAmazon DynamoDBに保存する。他のアプリケーションはKinesisデータストリームから取引データを取得できる。

D. バッチ処理された取引データをファイルとしてAmazon S3に保存する。AWS Lambdaを使用して各ファイルを処理し、機密データを除去してからAmazon S3のファイルを更新する。Lambda 関数はその後データをAmazon DynamoDBに保存する。他のアプリケーションはAmazon S3に保存された取引ファイルを利用できる。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- 数百万件の取引をスケーラブルに処理すること
- 複数の内部アプリケーションとほぼリアルタイムで取引詳細を共有すること
- ドキュメントデータベースに保存する前に機密データを除去すること
- 保存データを低レイテンシーで取得できること

正解はCである。

Kinesis Data Streamsは、複数のコンシューマーがほぼリアルタイムで同じストリームのデータを処理できる。Lambdaをストリームコンシューマーとして使用して各レコードから機密データを除去し、処理後のデータをDynamoDBに保存することで、ほぼリアルタイム共有、保存前の機密データ除去、低レイテンシー取得の要件を満たす。

不正解の理由

A. 取引データをAmazon DynamoDBに保存する。DynamoDBでルールを設定し、書き込み時にすべての取引から機密データを除去する。DynamoDB Streamsを使用して取引データを他のアプリケーションと共有する。

DynamoDB自体には、書き込み時に各取引から機密データを自動的に除去するルール機能はない。DynamoDB Streamsは変更イベントの配信には使用できるが、複数アプリケーションへのスケーラブルなほぼリアルタイム共有と保存前変換の要件を十分に満たさない。

B. 取引データをAmazon Kinesis Data Firehoseにストリーミングし、Amazon DynamoDBとAmazon S3にデータを保存する。Kinesis Data Firehoseと連携したAWS Lambdaを使用して機密データを除去する。他のアプリケーションはAmazon S3に保存されたデータを利用できる。

Kinesis Data FirehoseはLambda変換後にS3などに配信する用途に適するが、FirehoseはDynamoDBへの直接配信をサポートせず、ドキュメント型DBへの低遅延書き込みを保証できない。

D. バッチ処理された取引データをファイルとしてAmazon S3に保存する。AWS Lambdaを使用して各ファイルを処理し、機密データを除去してからAmazon S3のファイルを更新する。Lambda 関数はその後データをAmazon DynamoDBに保存する。他のアプリケーションはAmazon S3に保存された取引ファイルを利用できる。

S3にバッチファイルとして保存しLambdaで処理する方式はバッチベースであり、準リアルタイム要件を満たさず遅延が大きい。

Q. 034

SAA-C03

ある企業がAWS上でマルチティアアプリケーションをホストしている。コンプライアンス、ガバナンス、監査、およびセキュリティのために、同社はAWSリソースの構成変更を追跡し、これらのリソースに対して行われたAPIコールの履歴を記録しなければならない。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. AWS CloudTrailを使用して構成変更を追跡し、AWS Configを使用してAPIコールを記録する。

B. AWS Configを使用して構成変更を追跡し、AWS CloudTrailを使用してAPIコールを記録する。

C. AWS Configを使用して構成変更を追跡し、Amazon CloudWatchを使用してAPIコールを記録する。

D. AWS CloudTrailを使用して構成変更を追跡し、Amazon CloudWatchを使用してAPIコールを記録する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- AWSリソースの構成変更履歴を追跡すること
- リソースに対して実行されたAPIコールの記録（監査ログ）を残すこと
- コンプライアンス、ガバナンス、監査およびセキュリティを満たすこと

正解はBである。

AWS Configはリソースの構成変更を追跡し構成履歴を記録し、AWS CloudTrailはアカウント全体のAPIコール（監査ログ）をキャプチャするため、両サービスを組み合わせることで要件を満たす。

不正解の理由

A. AWS CloudTrailを使用して構成変更を追跡し、AWS Configを使用してAPIコールを記録する。

役割が逆である。CloudTrailはAPIコールを記録し、AWS Configが構成変更を追跡する。

C. AWS Configを使用して構成変更を追跡し、Amazon CloudWatchを使用してAPIコールを記録する。

CloudWatchはAPIコールの監査ログを代替できず、CloudTrailが必要である。

D. AWS CloudTrailを使用して構成変更を追跡し、Amazon CloudWatchを使用してAPIコールを記録する。

CloudTrailは構成変更の追跡手段ではなく、CloudWatchもAPIコール監査ログを代替できない。

Q. 035

SAA-C03

企業はAWSクラウドでパブリック向けのウェブアプリケーションを立ち上げる準備をしている。アーキテクチャはVPC内のAmazon EC2インスタンスがElastic Load Balancer（ELB）の背後に配置されている。DNSにはサードパーティのサービスを使用している。企業のソリューションアーキテクトは、大規模なDDoS攻撃を検出し防御するためのソリューションを推奨しなければならない。どのソリューションがこれらの要件を満たすか？

A. アカウントでAmazon GuardDutyを有効にする。

B. EC2インスタンスでAmazon Inspectorを有効にする。

C. AWS Shieldを有効にし、Amazon Route 53を割り当てる。

D. AWS Shield Advancedを有効にし、ELBに割り当てる。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- パブリックに公開されたウェブアプリケーションを保護する
- 大規模なDDoS攻撃を検出し保護できるソリューションが必要
- Amazon EC2インスタンスはELBの背後に配置されている
- DNSはサードパーティサービスを使用している

正解はDである。

AWS Shield AdvancedはELBに対する大規模なDDoS攻撃の検出と高度な緩和機能を提供し、DDoS対応チーム（DFRT）によるサポートとコスト保護機能を含むため、大規模攻撃に適している。サードパーティDNSを使用していてもELBに直接Shield Advancedを適用して保護可能である。

不正解の理由

A. アカウントでAmazon GuardDutyを有効にする。

Amazon GuardDutyは侵入検知および異常検知サービスであり、DDoSトラフィックに対するリアルタイム緩和機能を提供しない。

B. EC2インスタンスでAmazon Inspectorを有効にする。

Amazon Inspectorは脆弱性およびベストプラクティス検査ツールであり、DDoS防御機能とは無関係である。

C. AWS Shieldを有効にし、Amazon Route 53を割り当てる。

AWS Shield(Standard)は基本的な保護を提供するが、大規模攻撃の緩和やDFRTサポートが必要な場合はShield Advancedが必要である。また、問題の環境はサードパーティDNSであるためRoute 53連携に依存できない。

Q. 036

SAA-C03

ある企業がAWSクラウドでアプリケーションを構築している。このアプリケーションは2つのAWSリージョンにあるAmazon S3バケットにデータを保存する。企業は、S3バケットに保存されるすべてのデータを暗号化するために、AWS Key Management Service（AWS KMS）のカスタマー管理キーを使用しなければならない。両方のS3バケットのデータは同じKMSキーで暗号化および復号されなければならず、データとキーはそれぞれの2つのリージョンに保存されなければならない。これらの要件を最小限の運用上の負担で満たすソリューションはどれか？

A. 各リージョンにS3バケットを作成する。S3バケットをAmazon S3管理の暗号化キー（SSE-S3）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

B. カスタマー管理のマルチリージョンKMSキーを作成する。各リージョンにS3バケットを作成する。S3バケット間でレプリケーションを設定する。アプリケーションをクライアントサイド暗号化でKMSキーを使用するように設定する。

C. カスタマー管理のKMSキーとS3バケットを各リージョンに作成する。S3バケットをAmazon S3管理の暗号化キー（SSE-S3）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

D. カスタマー管理のKMSキーとS3バケットを各リージョンに作成する。S3バケットをAWS KMSキー（SSE-KMS）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 2つのリージョンのS3バケットに保存されるすべてのデータは顧客管理のKMSキーで暗号化すること。
- 2つのバケットのデータは同一のKMSキーで暗号化および復号化されること。
- データと該当KMSキーは各リージョンに保存されること。
- 要件を満たすソリューションは運用上の負担を最小限に抑えること。

正解はBである。

Bは顧客管理のマルチリージョンKMSキーを使用するため、論理的に「同一キー」を2つのリージョンに複製し、両方で暗号化および復号化が可能である。また、S3バケットをリージョンごとに設置しレプリケーションを構成するため、「データとキーが各リージョンに保存される」条件も満たす。運用負担の観点では本来SSE-KMSが軽いが、「同一キー＋リージョンごとのキー存在」を満たす選択肢は実質Bのみである。

不正解の理由

A. 各リージョンにS3バケットを作成する。S3バケットをAmazon S3管理の暗号化キー（SSE-S3）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

SSE-S3（S3管理キー）であるため、「顧客管理のKMSキーを使用する」という要件に正面から違反している。つまり、最初から規定条件を満たさない。

C. カスタマー管理のKMSキーとS3バケットを各リージョンに作成する。S3バケットをAmazon S3管理の暗号化キー（SSE-S3）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

リージョンごとにKMSキーを別々に作成しながら暗号化はSSE-S3を使用するとしており、顧客管理のKMSキー使用要件を満たさず、さらに「2つのバケットのデータが同一KMSキーで暗号化および復号化される」ことも不可能である（キーが別なら同一キーではない）。

D. カスタマー管理のKMSキーとS3バケットを各リージョンに作成する。S3バケットをAWS KMSキー（SSE-KMS）を使用するサーバーサイド暗号化に設定する。S3バケット間でレプリケーションを設定する。

リージョンごとに顧客管理のKMSキーとSSE-KMSを使用する点は良いが、リージョンごとにキーが「異なるキー」となる。問題は「2つのリージョンのデータが同一のKMSキーで暗号化および復号化される」必要があるため、Dはこの重要な条件を満たさない。

Q. 037

SAA-C03

ある企業が最近、AWSアカウント内のAmazon EC2インスタンスでさまざまな新しいワークロードを開始した。この企業は、インスタンスにリモートで安全にアクセスし管理するための戦略を策定する必要がある。企業は、ネイティブなAWSサービスを使用し、AWS Well-Architected Frameworkに準拠した繰り返し可能なプロセスを実装する必要がある。これらの要件を最小限の運用上の負担で満たすソリューションはどれか。

A. EC2シリアルコンソールを使用して、各インスタンスのターミナルインターフェイスに直接アクセスし管理する。

B. 既存および新規の各インスタンスに適切なIAMロールをアタッチする。AWS Systems Manager Session Managerを使用して、インスタンスへの安全なリモートセッションを開始する。

C. 管理用のSSHキーペアを作成する。公開鍵を各EC2インスタンスにロードする。パブリックサブネットに踏み台ホストを展開し、各インスタンスの管理用トンネルを提供する。

D. AWS Site-to-Site VPN接続を確立する。管理者に対して、オンプレミスのローカルマシンを使用してVPNトンネル経由でSSHキーを使いインスタンスに直接接続するよう指示する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- ネイティブAWSサービスを利用すること
- 繰り返し可能な標準化されたリモート管理プロセスであること
- リモートで安全にアクセスし管理すること
- 運用上の負担を最小限に抑えるソリューションであること

正解はBである。

AWS Systems Manager Session ManagerはIAMロールベースのアクセス制御、SSHキー配布不要の接続、集中監査ログ、AWSネイティブサービスとの統合を提供する。踏み台ホストやVPNと比較して運用負担が少なく、繰り返し可能で安全なリモート管理プロセスを実現できる。

不正解の理由

A. EC2シリアルコンソールを使用して、各インスタンスのターミナルインターフェイスに直接アクセスし管理する。

EC2シリアルコンソールは主にデバッグや緊急復旧用であり、一般的な運用管理に拡張・標準化が困難で、必要な繰り返しプロセスや監査機能が限定的である。

C. 管理用のSSHキーペアを作成する。公開鍵を各EC2インスタンスにロードする。パブリックサブネットに踏み台ホストを展開し、各インスタンスの管理用トンネルを提供する。

パブリックサブネットのバスチョンホストとSSHキー管理は、キー配布・ローテーション・パッチ適用・単一障害点など追加の運用負担とセキュリティ管理作業を生じる。

D. AWS Site-to-Site VPN接続を確立する。管理者に対して、オンプレミスのローカルマシンを使用してVPNトンネル経由でSSHキーを使いインスタンスに直接接続するよう指示する。

サイト間VPNはオンプレミスインフラ依存が必要で、ネットワーク管理・運用負担が増大し、完全なネイティブAWSベースの繰り返しプロセスではない。

Q. 038

SAA-C03

ある企業はAmazon S3で静的ウェブサイトをホスティングし、DNSにAmazon Route 53を使用している。ウェブサイトへの世界中からの需要が増加している。企業はウェブサイトにアクセスするユーザーのレイテンシーを低減しなければならない。これらの要件を最もコスト効率よく満たすソリューションはどれか。

A. ウェブサイトを含むS3バケットをすべてのAWSリージョンにレプリケートする。Route 53のジオロケーションルーティングエントリを追加する。

B. AWS Global Acceleratorでアクセラレータをプロビジョニングする。提供されたIPアドレスをS3バケットに関連付ける。Route 53のエントリをアクセラレータのIPアドレスに変更する。

C. S3バケットの前にAmazon CloudFrontディストリビューションを追加する。Route 53のエントリをCloudFrontディストリビューションに変更する。

D. バケットでS3 Transfer Accelerationを有効にする。Route 53のエントリを新しいエンドポイントに変更する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- 全世界のユーザーに対する遅延時間の短縮
- コスト効率の良いソリューション
- Amazon S3で静的ウェブサイトをホスティングしている
- Amazon Route 53をDNSとして使用している

正解はCである。

CloudFrontはグローバルエッジネットワークでコンテンツをキャッシュし、全世界のユーザーの遅延時間を短縮する。S3をオリジンとして自然に統合され、多リージョン複製よりもコスト効率が良い。

不正解の理由

A. ウェブサイトを含むS3バケットをすべてのAWSリージョンにレプリケートする。Route 53のジオロケーションルーティングエントリを追加する。

すべてのリージョンにS3バケットを複製すると、データ複製コストと運用負担および管理の複雑さが大幅に増加し、コスト効率が悪い。

B. AWS Global Acceleratorでアクセラレータをプロビジョニングする。提供されたIPアドレスをS3バケットに関連付ける。Route 53のエントリをアクセラレータのIPアドレスに変更する。

AWS Global Acceleratorは主にアプリケーションやロードバランサー向けであり、S3静的ホスティングの直接的な加速には適さず、コストも高い。

D. バケットでS3 Transfer Accelerationを有効にする。Route 53のエントリを新しいエンドポイントに変更する。

S3 Transfer Accelerationは主にアップロード（クライアント→S3）の性能を改善し、全世界のダウンロード遅延を減らすキャッシュソリューションではないため、要件に合致しない。

Q. 039

SAA-C03

ある企業は、自社ウェブサイト上のアイテムの検索可能なリポジトリを維持している。データは1,000万行を超えるAmazon RDS for MySQLのデータベーステーブルに格納されている。データベースは2 TBのGeneral Purpose SSDストレージを使用している。毎日、同社のウェブサイトを通じてこのデータに対して数百万件の更新が行われている。
同社は、一部の挿入操作に10秒以上かかることに気づいた。データベースのストレージ性能が問題であると判断している。
この性能問題に対処するソリューションはどれか。

A. ストレージタイプをProvisioned IOPS SSDに変更する。

B. DBインスタンスをメモリ最適化インスタンスクラスに変更する。

C. DBインスタンスをバースト可能なパフォーマンスインスタンスクラスに変更する。

D. MySQLネイティブの非同期レプリケーションを使用してMulti-AZ RDSリードレプリカを有効にする。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 挿入遅延を削減する必要がある（一部の挿入に10秒以上かかる）
- 毎日数百万件の更新を処理できる書き込みスループットが必要
- 問題の根本原因がストレージI/O性能であることが確認されている
- データは1,000万行を超えるAmazon RDS for MySQLテーブルに保存されており、データベースには2TBのGeneral Purpose SSDストレージがある

正解はAである。

Provisioned IOPS SSDはプロビジョニングされたIOPSにより一貫して高いI/O性能と書き込みスループットを提供するため、ストレージI/Oがボトルネックの書き込み集約型ワークロードの挿入遅延を削減する。

不正解の理由

B. DBインスタンスをメモリ最適化インスタンスクラスに変更する。

メモリ最適化インスタンスはメモリやCPUのボトルネックを解消するが、問題の原因がストレージI/Oである場合、挿入遅延を解決できない。

C. DBインスタンスをバースト可能なパフォーマンスインスタンスクラスに変更する。

バースト性能インスタンスはCPUやネットワークのバーストに有利であるが、一貫した高いディスクI/O要求を満たせず、書き込み遅延を解決できない。

D. MySQLネイティブの非同期レプリケーションを使用してMulti-AZ RDSリードレプリカを有効にする。

リードレプリカと非同期レプリケーションは読み取りスケーリングに役立つが、書き込みスループットやストレージI/O遅延を減少させず、Multi-AZは主に可用性と耐久性の目的である。

Q. 040

SAA-C03

ある企業は数千台のエッジデバイスを所有しており、これらが毎日合計1 TBのステータスアラートを生成している。各アラートのサイズは約2 KBである。ソリューションアーキテクトは、これらのアラートを取り込み、将来の分析のために保存するソリューションを実装する必要がある。企業は高可用性のソリューションを望んでいるが、コストを最小限に抑え、追加のインフラストラクチャを管理したくない。また、14日間のデータを即時分析のために利用可能にし、14日を超えるデータはアーカイブしたい。これらの要件を満たす最も運用上効率的なソリューションはどれか。

A. Amazon Kinesis Data Firehose配信ストリームを作成してアラートを取り込む。Kinesis Data Firehoseストリームを設定し、アラートをAmazon S3バケットに配信する。S3ライフサイクル設定を構成して、14日後にデータをAmazon S3 Glacierに移行する。

B. 2つのアベイラビリティーゾーンにまたがってAmazon EC2インスタンスを起動し、Elastic Load Balancerの背後に配置してアラートを取り込む。EC2インスタンス上にスクリプトを作成し、アラートをAmazon S3バケットに保存する。S3ライフサイクル設定を構成して、14日後にデータをAmazon S3 Glacierに移行する。

C. Amazon Kinesis Data Firehose配信ストリームを作成してアラートを取り込む。Kinesis Data Firehoseストリームを設定し、アラートをAmazon OpenSearch Service（Amazon Elasticsearch Service）クラスターに配信する。Amazon OpenSearch Serviceクラスターで毎日手動スナップショットを取得し、14日より古いデータをクラスターから削除するよう設定する。

D. Amazon Simple Queue Service（Amazon SQS）標準キューを作成してアラートを取り込み、メッセージ保持期間を14日に設定する。コンシューマーを設定してSQSキューをポーリングし、メッセージの経過時間を確認して必要に応じてメッセージデータを分析する。メッセージが14日経過した場合、コンシューマーはメッセージをAmazon S3バケットにコピーし、SQSキューからメッセージを削除する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 高可用性で通知を安定的に収集すること
- 運用負担を最小限に抑えること（管理型サービスを優先）
- 14日間は即時分析可能なデータを保持すること
- 14日を超えるデータは低コストストレージにアーカイブすること

正解はAである。

Kinesis Data Firehoseは管理型かつ高可用性のサービスであり、大規模データを安定的に転送し、直接Amazon S3に配信して運用負担を最小限に抑える。S3のライフサイクルルールにより14日後にAmazon S3 Glacierへ自動移行し、コスト削減と要求された保持・アーカイブポリシーを満たす。

不正解の理由

B. 2つのアベイラビリティーゾーンにまたがってAmazon EC2インスタンスを起動し、Elastic Load Balancerの背後に配置してアラートを取り込む。EC2インスタンス上にスクリプトを作成し、アラートをAmazon S3バケットに保存する。S3ライフサイクル設定を構成して、14日後にデータをAmazon S3 Glacierに移行する。

EC2ベースのソリューションは追加のインフラ管理と運用負担が大きく、コスト効率が悪く管理型の要件を満たさない。

C. Amazon Kinesis Data Firehose配信ストリームを作成してアラートを取り込む。Kinesis Data Firehoseストリームを設定し、アラートをAmazon OpenSearch Service（Amazon Elasticsearch Service）クラスターに配信する。Amazon OpenSearch Serviceクラスターで毎日手動スナップショットを取得し、14日より古いデータをクラスターから削除するよう設定する。

OpenSearchはリアルタイム分析には有用だが、大規模長期保存ではコストが高く、手動スナップショットや削除は運用負担を増加させ要件に合わない。

D. Amazon Simple Queue Service（Amazon SQS）標準キューを作成してアラートを取り込み、メッセージ保持期間を14日に設定する。コンシューマーを設定してSQSキューをポーリングし、メッセージの経過時間を確認して必要に応じてメッセージデータを分析する。メッセージが14日経過した場合、コンシューマーはメッセージをAmazon S3バケットにコピーし、SQSキューからメッセージを削除する。

SQSはメッセージ配信用であり、大規模長期保存・分析のストレージとして不適切で、コンシューマーベースのコピー処理は複雑さと運用負担を増やしコスト効率が悪い。

Q. 041

SAA-C03

ある企業のアプリケーションは、複数のソフトウェア・アズ・ア・サービス（SaaS）ソースと統合してデータ収集を行っている。同社はAmazon EC2インスタンスを使用してデータを受信し、分析のためにAmazon S3バケットにデータをアップロードしている。データの受信とアップロードを行う同じEC2インスタンスが、アップロード完了時にユーザーへ通知も送信している。同社はアプリケーションのパフォーマンスが遅いことに気づき、可能な限りパフォーマンスを改善したいと考えている。これらの要件を最小限の運用上の負担で満たすソリューションはどれか。

A. Auto Scalingグループを作成し、EC2インスタンスのスケールアウトを可能にする。S3イベント通知を設定し、S3バケットへのアップロード完了時にAmazon Simple Notification Service（Amazon SNS）トピックへイベントを送信する。

B. Amazon AppFlowフローを作成し、各SaaSソースとS3バケット間でデータを転送する。S3イベント通知を設定し、S3バケットへのアップロード完了時にAmazon Simple Notification Service（Amazon SNS）トピックへイベントを送信する。

C. 各SaaSソースの出力データを送信するためにAmazon EventBridge（Amazon CloudWatch Events）ルールを作成する。S3バケットをルールのターゲットに設定する。S3バケットへのアップロード完了時にイベントを送信するための2つ目のEventBridge（CloudWatch Events）ルールを作成し、Amazon Simple Notification Service（Amazon SNS）トピックを2つ目のルールのターゲットに設定する。

D. EC2インスタンスの代わりに使用するDockerコンテナを作成する。コンテナ化されたアプリケーションをAmazon Elastic Container Service（Amazon ECS）でホストする。Amazon CloudWatch Container Insightsを設定し、S3バケットへのアップロード完了時にAmazon Simple Notification Service（Amazon SNS）トピックへイベントを送信する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 複数のSaaSソースからのデータ収集処理を自動化する
- S3にデータをアップロードし、アップロード完了時に通知を送信する
- 可能な限り性能を最大化する
- 運用上の負担を最小限に抑える

正解はBである。

Amazon AppFlowは複数のSaaSソースから直接S3へデータを転送可能なマネージドサービスであるため、従来EC2が担っていた「受信→アップロード」処理をサービスに置き換え、性能のボトルネック（EC2のCPU/ネットワーク/同時処理）を大幅に削減できる。またアップロード完了通知はS3イベントからSNSへ分離し、アプリケーション処理と通知を疎結合にする。結果としてEC2の運用・スケーリング・障害対応の負担を排除しつつ処理性能を最大化する選択肢である。

不正解の理由

A. Auto Scalingグループを作成し、EC2インスタンスのスケールアウトを可能にする。S3イベント通知を設定し、S3バケットへのアップロード完了時にAmazon Simple Notification Service（Amazon SNS）トピックへイベントを送信する。

Auto Scalingを導入し通知をS3イベントで分離しても、データ受信・アップロードの主要経路が依然としてEC2に残る。つまりSaaS連携・受信・変換・アップロードをEC2が行う構造がボトルネックなら性能問題は完全に解消されない。またスケーリング・パッチ適用・監視など運用負担も継続するため、運用負担最小化の最適解としてBより劣る。

C. 各SaaSソースの出力データを送信するためにAmazon EventBridge（Amazon CloudWatch Events）ルールを作成する。S3バケットをルールのターゲットに設定する。S3バケットへのアップロード完了時にイベントを送信するための2つ目のEventBridge（CloudWatch Events）ルールを作成し、Amazon Simple Notification Service（Amazon SNS）トピックを2つ目のルールのターゲットに設定する。

EventBridgeルールはイベントルーティングサービスであり、SaaSからの「データそのもの」をS3オブジェクトとして格納する転送パイプラインを直接提供しない。一般的にEventBridgeはイベントをLambda/SQS/SNSなどに渡す用途であり、「データファイルをS3にアップロード」する要件には適合しない。したがって問題文のデータ収集・アップロード経路を適切に代替できない。

D. EC2インスタンスの代わりに使用するDockerコンテナを作成する。コンテナ化されたアプリケーションをAmazon Elastic Container Service（Amazon ECS）でホストする。Amazon CloudWatch Container Insightsを設定し、S3バケットへのアップロード完了時にAmazon Simple Notification Service（Amazon SNS）トピックへイベントを送信する。

ECSに移行しても実行環境が変わるだけで、SaaS連携とアップロードロジックは依然アプリケーションが担う。さらにCloudWatch Container InsightsはS3アップロード完了イベントをSNSに送信する機能ではなく（監視用である）、通知トリガー設計が不正確であり、運用負担もEC2からECSへ単に移行したに過ぎず、運用負担最小化の観点で不利である。

Q. 042

SAA-C03

ある企業は、単一のVPC内の複数のアベイラビリティーゾーンにまたがる複数のサブネットでAmazon EC2インスタンス上に高可用性の画像処理アプリケーションを運用している。EC2インスタンス同士は通信しないが、単一のNAT GatewayをAmazon S3から画像をダウンロードし、Amazon S3に画像をアップロードしている。企業はデータ転送料金を懸念している。地域間データ転送料金を回避するために、最もコスト効率が高い方法は何か？

A. 各アベイラビリティーゾーンにNAT Gatewayを起動する。

B. NAT GatewayをNATインスタンスに置き換える。

C. Amazon S3用のゲートウェイVPCエンドポイントを展開する。

D. EC2インスタンスを実行するためにEC2 Dedicated Hostをプロビジョニングする。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- EC2インスタンスがS3からダウンロードおよびアップロードする
- 単一のNATゲートウェイを通じてS3と通信することによるリージョンまたはアベイラビリティーゾーン間のデータ転送料金を最小化する
- 最もコスト効率の良いソリューションであること
- EC2インスタンス同士は通信しない

正解はCである。

ゲートウェイVPCエンドポイントはS3トラフィックをAWSネットワーク内に直接ルーティングし、パブリックインターネットやNATを経由しないため、アベイラビリティーゾーン間やリージョン間のデータ転送料金を回避し、追加のゲートウェイやインスタンスコストなしでコスト効率が高い。

不正解の理由

A. 各アベイラビリティーゾーンにNAT Gatewayを起動する。
各アベイラビリティーゾーンにNATゲートウェイを配置するとアベイラビリティーゾーン間のデータ転送料金は削減できるが、各NATゲートウェイに対する時間およびGB単位の料金が発生しコスト効率が悪い。

B. NAT GatewayをNATインスタンスに置き換える。
NATインスタンスに置き換えると運用負担が増加し、S3へのトラフィックがパブリック経路を通る場合データ転送料金が発生する可能性がある。

D. EC2インスタンスを実行するためにEC2 Dedicated Hostをプロビジョニングする。
EC2専用ホストはデータ転送料金に関係なく非常にコストが高いため、要件に適合しない。

Q. 043

SAA-C03

ある企業はオンプレミスのアプリケーションを持ち、大量の時間に敏感なデータを生成し、それをAmazon S3にバックアップしている。アプリケーションの成長に伴い、ユーザーからインターネット帯域幅の制限に関する不満が出ている。ソリューションアーキテクトは、Amazon S3へのタイムリーなバックアップを可能にしつつ、社内ユーザーのインターネット接続への影響を最小限に抑える長期的なソリューションを設計する必要がある。どのソリューションがこれらの要件を満たすか？

A. AWS VPN接続を確立し、すべてのトラフィックをVPCゲートウェイエンドポイント経由でプロキシする。

B. 新しいAWS Direct Connect接続を確立し、バックアップトラフィックをこの新しい接続経由で送る。

C. 毎日AWS Snowballデバイスを注文し、データをSnowballデバイスにロードして毎日AWSに返却する。

D. AWSマネジメントコンソールからサポートチケットを提出し、アカウントからS3サービス制限の解除を依頼する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- Amazon S3へのタイムリーなバックアップを保証すること
- 社内ユーザーのインターネット接続への影響を最小限に抑えること
- 大量の時間に敏感なデータを処理可能であること
- 長期的なソリューションであること

正解はBである。

AWS Direct Connectは専用ネットワーク接続によりオンプレミスとAWS間の帯域幅を確保し、インターネットを迂回するため、継続的かつ遅延に敏感なバックアップを実行しつつ社内のインターネットトラフィックへの影響を最小限に抑える。

不正解の理由

A. AWS VPN接続を確立し、すべてのトラフィックをVPCゲートウェイエンドポイント経由でプロキシする。

サイト間VPNトラフィックは通常インターネット経由で送信され、オンプレミスのトラフィックをVPCゲートウェイエンドポイントに直接プロキシする方法は適切でなく、インターネット負荷を軽減できない。

C. 毎日AWS Snowballデバイスを注文し、データをSnowballデバイスにロードして毎日AWSに返却する。

Snowballはオフラインの大量データ転送に適しているが、毎日の配送・返送は時間的制約や遅延、高い運用負担をもたらし、リアルタイムかつ継続的なバックアップには不適切である。

D. AWSマネジメントコンソールからサポートチケットを提出し、アカウントからS3サービス制限の解除を依頼する。

S3サービスの制限解除はインターネット帯域幅の問題を解決せず、要件に関連しない。

Q. 044

SAA-C03

ある企業が重要なデータを含むAmazon S3バケットを所有している。このデータを誤って削除されることから保護しなければならない。これらの要件を満たすためにソリューションアーキテクトが取るべき手順の組み合わせはどれか。**(2つ選べ)**

A. S3バケットでバージョニングを有効にする。

B. S3バケットでMFA Deleteを有効にする。

C. S3バケットにバケットポリシーを作成する。

D. S3バケットでデフォルトの暗号化を有効にする。

E. S3バケット内のオブジェクトに対してライフサイクルポリシーを作成する。

✅ 正解: A、B / 解説

ソリューションは、次の要件を満たす必要がある。

- 重要なS3オブジェクトの誤削除を防止する
- 削除または上書きが発生した場合に以前のバージョンに復元可能である
- 削除操作に対して追加の認証（MFA）を要求する

正解はA、Bである。

バージョニングを有効化するとオブジェクトのすべてのバージョンが保存され、誤って削除または上書きされた場合に以前のバージョンへ復元可能である。MFA Deleteはバージョニングが有効な状態でオブジェクトバージョンの削除やバージョニングの一時停止に追加のMFA認証を要求し、誤操作や不正削除から保護する。

不正解の理由

C. S3バケットにバケットポリシーを作成する。

バケットポリシーは権限によって削除を制限できるが、アカウントルート権限や権限を持つユーザーの誤削除を完全に防止できず復旧手段を提供しない。

D. S3バケットでデフォルトの暗号化を有効にする。

保存時の暗号化はデータの機密性を保護するが、削除防止や削除復旧とは無関係である。

E. S3バケット内のオブジェクトに対してライフサイクルポリシーを作成する。

ライフサイクルポリシーはオブジェクトや以前のバージョンを自動削除する設定が可能であり、むしろデータ削除を招く可能性がある。

Q. 045

SAA-C03

ある企業は、以下のデータ取り込みワークフローを持つ。・新しいデータ配信に関する通知のためのAmazon Simple Notification Service（Amazon SNS）トピック・データを処理しメタデータを記録するAWS Lambda 関数企業は、ネットワーク接続の問題により取り込みワークフローが時折失敗することを観察している。このような失敗が発生すると、Lambda 関数は対応するデータを取り込まず、企業は手動でジョブを再実行しなければならない。将来的にLambda 関数がすべてのデータを取り込むことを保証するために、ソリューションアーキテクトはどの組み合わせの対策を取るべきか。**（2つ選べ）**

A. Lambda 関数を複数のアベイラビリティーゾーンにデプロイする。

B. Amazon Simple Queue Service（Amazon SQS）キューを作成し、それをSNSトピックにサブスクライブさせる。

C. Lambda 関数に割り当てるCPUとメモリを増やす。

D. Lambda 関数のプロビジョンドスループットを増やす。

E. Lambda 関数を修正してAmazon Simple Queue Service（Amazon SQS）キューから読み取るようにする。

✅ 正解: B、E / 解説

ソリューションは、次の要件を満たす必要がある。

- ネットワーク障害時にもデータ損失を防止
- 新規データ配信の通知用にAmazon SNSトピックが存在
- 手動再実行なしでワークフローを復旧可能
- データ処理とメタデータ記録にAWS Lambda 関数を使用

正解はB、Eである。

SNSからSQSへの構成によりメッセージを耐久的にバッファリングし、ネットワーク障害時の損失を防止する。LambdaがSQSから読み取るように変更すれば、メッセージの再試行、可視性タイムアウト、DLQを活用して自動復旧が可能である。

不正解の理由

A. Lambda 関数を複数のアベイラビリティーゾーンにデプロイする。

不適切 — AWS Lambdaはリージョンサービスであり、別アベイラビリティーゾーンに配置してもSNSトリガーの処理信頼性（メッセージ保持・再試行）は解決しない。

C. Lambda 関数に割り当てるCPUとメモリを増やす。

不適切 — CPUやメモリの増強は処理性能に影響するが、ネットワーク接続問題によるメッセージ損失は解決しない。

D. Lambda 関数のプロビジョンドスループットを増やす。

不適切 — プロビジョンドスループットはLambdaのネットワーク障害やメッセージ耐久性問題を解決する概念ではなく、本要件とは無関係である。

Q. 046

SAA-C03

ある企業は店舗向けにマーケティングサービスを提供するアプリケーションを持っている。このサービスは店舗の顧客の過去の購入履歴に基づいている。店舗はSFTPを通じて取引データを企業にアップロードし、そのデータは処理・分析されて新しいマーケティングオファーを生成する。ファイルの中には200GBを超えるものもある。最近、いくつかの店舗が個人を特定できる情報（PII）を含むファイルを誤ってアップロードしていたことが判明した。企業はPIIが再度共有された場合に管理者に通知し、かつ自動的に修復処理を行いたい。最小限の開発労力でこれらの要件を満たすには、ソリューションアーキテクトは何をすべきか？

A. Amazon S3バケットを安全な転送ポイントとして使用する。Amazon Inspectorを使ってバケット内のオブジェクトをスキャンする。オブジェクトにPIIが含まれている場合、S3ライフサイクルポリシーをトリガーしてPIIを含むオブジェクトを削除する。

B. Amazon S3バケットを安全な転送ポイントとして使用する。Amazon Macieを使ってバケット内のオブジェクトをスキャンする。オブジェクトにPIIが含まれている場合、Amazon Simple Notification Service（Amazon SNS）を使って管理者に通知をトリガーし、PIIを含むオブジェクトの削除を促す。

C. AWS Lambda 関数でカスタムスキャンアルゴリズムを実装する。オブジェクトがバケットにアップロードされたときに関数をトリガーする。オブジェクトにPIIが含まれている場合、Amazon Simple Notification Service（Amazon SNS）を使って管理者に通知をトリガーし、PIIを含むオブジェクトの削除を促す。

D. AWS Lambda 関数でカスタムスキャンアルゴリズムを実装する。オブジェクトがバケットにアップロードされたときに関数をトリガーする。オブジェクトにPIIが含まれている場合、Amazon Simple Email Service（Amazon SES）を使って管理者に通知をトリガーし、PIIを含むオブジェクトを削除するためにS3ライフサイクルポリシーをトリガーする。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- SFTP経由でアップロードされる大容量（200GB超を含む）オブジェクトを処理すること
- PIIを含む場合に管理者へ警告を送信すること
- PII露出時に自動修復を実行すること
- 最小限の開発労力で実装すること

正解はBである。

Amazon MacieはAmazon S3に保存されたオブジェクトを自動的にスキャンし、PIIなどの機密情報を検出する専用サービスである。独自のスキャンロジックを開発する必要がないため、開発労力を最小限に抑えられる。MacieはPII検出時にFindingを生成し、これをSNSやEventBridgeと連携して管理者への警告や自動修復のフローを容易に構築可能である。200GBを超える大容量オブジェクトもサービスレベルで処理可能な点で要件に最も適合する。

不正解の理由

A. Amazon S3バケットを安全な転送ポイントとして使用する。Amazon Inspectorを使ってバケット内のオブジェクトをスキャンする。オブジェクトにPIIが含まれている場合、S3ライフサイクルポリシーをトリガーしてPIIを含むオブジェクトを削除する。

Amazon InspectorはEC2、ECR、Lambdaなどのセキュリティ脆弱性分析に特化したサービスであり、S3オブジェクトのPII検出を目的としていない。また、S3 Lifecycleポリシーは時間ベースの移行や削除用であり、PII検出時の即時対応トリガーとして機能しない。したがって、PII検出と自動修復の要件を満たさない。

C. AWS Lambda 関数でカスタムスキャンアルゴリズムを実装する。オブジェクトがバケットにアップロードされたときに関数をトリガーする。オブジェクトにPIIが含まれている場合、Amazon Simple Notification Service（Amazon SNS）を使って管理者に通知をトリガーし、PIIを含むオブジェクトの削除を促す。

LambdaにカスタムPIIスキャンアルゴリズムを実装する方法は開発および保守の負担が非常に大きい。特に200GBを超えるファイルをLambdaで直接解析するのは時間制限やメモリ制限の観点から非効率であり、「最小限の開発労力」という要件に明確に反する。

D. AWS Lambda 関数でカスタムスキャンアルゴリズムを実装する。オブジェクトがバケットにアップロードされたときに関数をトリガーする。オブジェクトにPIIが含まれている場合、Amazon Simple Email Service（Amazon SES）を使って管理者に通知をトリガーし、PIIを含むオブジェクトを削除するためにS3ライフサイクルポリシーをトリガーする。

この選択肢もCと同様にカスタムスキャンロジックの実装が必要であり、自動化が一部含まれていても運用の複雑さが大きい。また、S3 Lifecycleポリシーはイベントベースの即時修復には適さず、PII検出後の自動対応要件を正確に満たさない。管理されたサービス活用という要件の意図から逸脱した過剰な設計である。

Q. 047

SAA-C03

ある企業が、特定のAWSリージョン内の3つの特定アベイラビリティーゾーンで、1週間続くイベントのためにAmazon EC2の容量を保証する必要がある。EC2の容量を保証するために企業は何をすべきか？

A. 必要なリージョンを指定したリザーブドインスタンスを購入する。

B. 必要なリージョンを指定したオンデマンド容量予約を作成する。

C. 必要なリージョンと3つのアベイラビリティーゾーンを指定したリザーブドインスタンスを購入する。

D. 必要なリージョンと3つのアベイラビリティーゾーンを指定したオンデマンド容量予約を作成する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 特定リージョン内の特定アベイラビリティーゾーン（3か所）での容量保証
- 保証は短期間（約1週間）必要
- 保証されたAmazon EC2容量が必要

正解はDである。

オンデマンド容量予約は特定のアベイラビリティーゾーンで即時にEC2容量を確保し、その期間中容量を保証する。要件が3つの特定アベイラビリティーゾーンを含むため、各アベイラビリティーゾーンで容量予約を作成すれば保証要件を満たす。

不正解の理由

A. 必要なリージョンを指定したリザーブドインスタンスを購入する。
リザーブドインスタンスは容量を保証せず料金割引のみ提供するため、特定アベイラビリティーゾーンでの容量確保要件を満たさない。

B. 必要なリージョンを指定したオンデマンド容量予約を作成する。
オンデマンド容量予約をリージョン単位で作成すると個別アベイラビリティーゾーンの容量保証にならず、Capacity Reservationはアベイラビリティーゾーン単位で作成する必要がある。

C. 必要なリージョンと3つのアベイラビリティーゾーンを指定したリザーブドインスタンスを購入する。
リザーブドインスタンスはリージョンやアベイラビリティーゾーンを指定しても実際に容量を予約しないため、保証された容量要件を満たさない。

Q. 048

SAA-C03

ある企業のウェブサイトは、商品カタログにAmazon EC2インスタンスストアを使用している。企業はカタログの高可用性を確保し、かつカタログを耐久性のある場所に保存したいと考えている。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. カタログをAmazon ElastiCache for Redisに移行する。

B. より大きなインスタンスストアを持つ大きなEC2インスタンスを展開する。

C. カタログをインスタンスストアからAmazon S3 Glacier Deep Archiveに移行する。

D. カタログをAmazon Elastic File System（Amazon EFS）ファイルシステムに移行する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- カタログデータはアベイラビリティーゾーン障害に対して高可用性を提供すること
- カタログデータは損失防止のため高い耐久性で保存すること
- 既存のEC2インスタンスストア（一時的ストレージ）のデータを永続的かつ共有可能な場所に移行すること

正解はDである。

Amazon EFSはマネージドファイルストレージであり、複数のアベイラビリティーゾーンからアクセス可能で、サービスレベルでのレプリケーションと耐久性を提供し、高可用性と耐久性の要件を満たす。POSIX互換のファイルシステムであり、EC2インスタンスと共有して運用に適する。

不正解の理由

A. カタログをAmazon ElastiCache for Redisに移行する。

ElastiCache for Redisは主にメモリベースのキャッシュであり、基本的に永続的な耐久性を提供しないため、アクティブカタログの耐久性要件を満たさない。

B. より大きなインスタンスストアを持つ大きなEC2インスタンスを展開する。

より大きなEC2インスタンスストアは依然として一時的（インスタンスの寿命に依存）であり、単一インスタンス障害時にデータ損失の可能性があるため、耐久性と高可用性の要件を満たさない。

C. カタログをインスタンスストアからAmazon S3 Glacier Deep Archiveに移行する。

Glacier Deep Archiveは非常に高い耐久性を提供するが、アーカイブ向けサービスであり、検索遅延が大きく、アクティブカタログの高可用性および即時アクセスの要件に適さない。

Q. 049

SAA-C03

ある企業は通話の文字起こしファイルを月単位で保存している。ユーザーは通話から1年以内のファイルをランダムにアクセスするが、1年を過ぎるとアクセス頻度は低くなる。企業は、1年未満のファイルをできるだけ迅速にクエリおよび取得できるようにし、古いファイルの取得に遅延があっても許容することで、ソリューションを最適化したい。これらの要件を最もコスト効率よく満たすソリューションはどれか。

A. 個々のファイルにタグを付けてAmazon S3 Glacier Instant Retrievalに保存する。タグをクエリしてS3 Glacier Instant Retrievalからファイルを取得する。

B. 個々のファイルをAmazon S3 Intelligent-Tieringに保存する。S3ライフサイクルポリシーを使用して1年後にファイルをS3 Glacier Flexible Retrievalに移行する。Amazon Athenaを使用してAmazon S3内のファイルをクエリおよび取得し、S3 Glacier内のファイルはS3 Glacier Selectを使用してクエリおよび取得する。

C. 個々のファイルにタグを付けてAmazon S3 Standardストレージに保存する。各アーカイブの検索メタデータもAmazon S3 Standardストレージに保存する。S3ライフサイクルポリシーを使用して1年後にファイルをS3 Glacier Instant Retrievalに移行する。Amazon S3からメタデータを検索してファイルをクエリおよび取得する。

D. 個々のファイルをAmazon S3 Standardストレージに保存する。S3ライフサイクルポリシーを使用して1年後にファイルをS3 Glacier Deep Archiveに移行する。検索メタデータをAmazon RDSに保存する。Amazon RDSからファイルをクエリし、S3 Glacier Deep Archiveからファイルを取得する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 1年未満のファイルは可能な限り迅速にクエリおよび即時検索可能であること
- 1年経過後のファイルは検索遅延が許容され、コストを最小化すること
- ユーザーは通話後1年以内にランダムにファイルへアクセスすること
- 全体のソリューションはコスト効率的であること

正解はBである。

BはAmazon S3に保存されたファイルをAmazon AthenaでSQLベースにクエリ可能であり、1年未満の通話記録ファイルを迅速に検索できる。また、Intelligent-Tieringとライフサイクルポリシーにより1年経過後のファイルをGlacierに自動移行し、コストを最適化しつつ要求されたアクセスパターンを満たす。AthenaとS3はサーバーレスであるため、運用負荷が最も少ない組み合わせである。

不正解の理由

A. 個々のファイルにタグを付けてAmazon S3 Glacier Instant Retrievalに保存する。タグをクエリしてS3 Glacier Instant Retrievalからファイルを取得する。

S3 Glacier Instant Retrievalは保存コストが高く、大量のアーカイブデータのコスト最適化要件に適さない。またタグベースの検索はファイル内容(SQLクエリ)の検索要件を満たさない。

C. 個々のファイルにタグを付けてAmazon S3 Standardストレージに保存する。各アーカイブの検索メタデータもAmazon S3 Standardストレージに保存する。S3ライフサイクルポリシーを使用して1年後にファイルをS3 Glacier Instant Retrievalに移行する。Amazon S3からメタデータを検索してファイルをクエリおよび取得する。

S3標準ストレージにメタデータを別管理する方法は追加の運用複雑性と管理コストが発生し、Athenaを用いた直接クエリより過剰な設計と評価される。

D. 個々のファイルをAmazon S3 Standardストレージに保存する。S3ライフサイクルポリシーを使用して1年後にファイルをS3 Glacier Deep Archiveに移行する。検索メタデータをAmazon RDSに保存する。Amazon RDSからファイルをクエリし、S3 Glacier Deep Archiveからファイルを取得する。

Amazon RDSを用いたメタデータ検索はサーバーレスでなく運用負荷が大きい。

Q. 050

SAA-C03

ある企業は、1,000台のAmazon EC2 Linuxインスタンスで稼働する本番ワークロードを持つ。このワークロードはサードパーティ製ソフトウェアによって動作している。企業は、重大なセキュリティ脆弱性を修正するために、すべてのEC2インスタンス上のサードパーティ製ソフトウェアにできるだけ早くパッチを適用する必要がある。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. すべてのEC2インスタンスにパッチを適用するためのAWS Lambda 関数を作成する。

B. すべてのEC2インスタンスにパッチを適用するようにAWS Systems Manager Patch Managerを設定する。

C. すべてのEC2インスタンスにパッチを適用するためにAWS Systems Managerのメンテナンスウィンドウをスケジュールする。

D. すべてのEC2インスタンスにパッチを適用するカスタムコマンドを実行するためにAWS Systems Manager Run Commandを使用する。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- 1,000台のEC2 Linuxインスタンスを対象とする
- サードパーティ製ソフトウェアに可能な限り迅速にパッチを適用する
- すべてのEC2インスタンスのサードパーティ製ソフトウェアにパッチを適用する
- パッチ適用の目的は重要なセキュリティ脆弱性の緩和である

正解はBである。

Patch Managerは、数百から数千台のEC2フリートに対してOSおよびアプリケーションのパッチを標準化された方法で配布するために設計されたサービスである。パッチ基準線、承認・拒否、再試行、結果報告など、脆弱性緩和に必要な運用および監査機能を備えている。また、「可能な限り迅速に」は単なる予約ではなく、大規模対象に対して自動化された一括パッチ適用を最も迅速かつ安全に実行する方法を意味する。つまり、「パッチ」「大規模」「セキュリティ脆弱性」が組み合わさった文脈ではPatch Managerが最適解の典型パターンである。

不正解の理由

A. すべてのEC2インスタンスにパッチを適用するためのAWS Lambda 関数を作成する。
Lambdaはサーバーパッチ専用サービスではなく、1,000台のインスタンスに対してパッチ適用を標準的かつ一貫して監査可能に管理する機能を持たない。パッチ適用にはインストール状態の追跡、失敗時の再試行、再起動や依存関係の処理など運用要素が必要であり、Lambdaでこれを実装すると不要なカスタムオーケストレーションとなる。要件適合性の観点では「セキュリティ脆弱性パッチ」に対しAWSが推奨する管理型アプローチ（SSM Patch Manager）が存在するため、Lambdaは意図された選択肢ではない。つまり「可能性」ではなく「正解パターン（サービスの意図）」で劣る。

C. すべてのEC2インスタンスにパッチを適用するためにAWS Systems Managerのメンテナンスウィンドウをスケジュールする。

メンテナンスウィンドウはパッチ作業を特定の時間帯に予約して繰り返し制御実行するのに適しているが、問題文の「可能な限り迅速に」が重要である。メンテナンスウィンドウは実行枠であり、パッチポリシーや承認、基準線などのパッチ管理自体はPatch Managerが担当する。緊急脆弱性対応では予約設計が本質ではなく、パッチ管理機能を通じて即時大規模適用が優先される。したがってこの条件下で「スケジューリング」が前面に出るCは正解としにくい。

D. すべてのEC2インスタンスにパッチを適用するカスタムコマンドを実行するためにAWS Systems Manager Run Commandを使用する。

Run Commandは大規模インスタンスに対してコマンドをリモート実行できるため緊急対応に見えるが、これは一時的な（ad-hoc）作業の性質が強い。パッチには基準線準拠、承認済みパッチ適用、結果報告・追跡など脆弱性緩和に必要な管理体制が重要であり、Run Commandはパッチ専用の管理機能を提供しない。つまり「今すぐ一度だけ実行」は可能でも、要件上は「セキュリティ脆弱性パッチ」という文言からPatch Managerという専用ソリューションを要求する。よってDは実務で一時的に使えるが最適解ではない。

Q. 051

SAA-C03

ある企業が、REST APIで取得可能な注文出荷統計を提供するアプリケーションを開発している。企業は出荷統計を抽出し、読みやすいHTML形式にデータを整理し、毎朝決まった時間に複数のメールアドレスにレポートを送信したい。これらの要件を満たすためにソリューションアーキテクトが取るべき手順の組み合わせはどれか。**（2つ選べ）**

A. アプリケーションを設定してデータをAmazon Kinesis Data Firehoseに送信させる。

B. Amazon Simple Email Service（Amazon SES）を使用してデータをフォーマットし、レポートをメールで送信する。

C. Amazon EventBridge（Amazon CloudWatch Events）のスケジュールイベントを作成し、AWS Glueジョブを呼び出してアプリケーションのAPIからデータをクエリする。

D. Amazon EventBridge（Amazon CloudWatch Events）のスケジュールイベントを作成し、AWS Lambda 関数を呼び出してアプリケーションのAPIからデータをクエリする。

E. アプリケーションデータをAmazon S3に保存する。Amazon Simple Notification Service（Amazon SNS）トピックをS3イベントの送信先として作成し、レポートをメールで送信する。

✅ 正解: B、D / 解説

ソリューションは、次の要件を満たす必要がある。

- アプリケーションのREST APIから毎日決まった時間に配送統計を抽出すること
- 抽出したデータを読みやすいHTML形式で整理すること
- 同じ時間に複数のメールアドレスにレポートを送信すること

正解はB、Dである。

EventBridgeのスケジュールイベントでLambdaを呼び出し、REST APIからデータを取得しLambdaでHTMLを生成した後、Amazon SESでメールを送信すれば、スケジュール呼び出し、HTMLフォーマット生成、複数受信者への送信の要件をすべて満たす。

不正解の理由

A. アプリケーションを設定してデータをAmazon Kinesis Data Firehoseに送信させる。

Kinesis Data Firehoseはストリーミングデータを送信先に配信するサービスであり、定期的にAPIを呼び出してHTMLレポートを生成しメール送信する要件には適さない。

C. Amazon EventBridge（Amazon CloudWatch Events）のスケジュールイベントを作成し、AWS Glueジョブを呼び出してアプリケーションのAPIからデータをクエリする。

AWS Glueは大規模ETLに適しているが、単純なREST API取得・HTML生成・メール送信には過剰であり、スケジュール利用時に不要な運用負担と複雑さがある。

E. アプリケーションデータをAmazon S3に保存する。Amazon Simple Notification Service（Amazon SNS）トピックをS3イベントの送信先として作成し、レポートをメールで送信する。

S3イベントはオブジェクト作成時にトリガーされるため、スケジュールベース（毎朝）の処理には合わず、SNSのメールはHTML形式の精緻なレポート送信や複数受信者の管理に制限がある。

Q. 052

SAA-C03

企業はオンプレミスのアプリケーションをAWSに移行したいと考えている。アプリケーションは数十ギガバイトから数百テラバイトまでのサイズの出力ファイルを生成する。アプリケーションデータは標準的なファイルシステム構造で保存する必要がある。企業は自動的にスケールし、高可用性があり、運用上の負担を最小限に抑えるソリューションを求めている。これらの要件を満たすソリューションはどれか。

A. アプリケーションをAmazon Elastic Container Service（Amazon ECS）上のコンテナとして移行する。ストレージにはAmazon S3を使用する。

B. アプリケーションをAmazon Elastic Kubernetes Service（Amazon EKS）上のコンテナとして移行する。ストレージにはAmazon Elastic Block Store（Amazon EBS）を使用する。

C. アプリケーションをマルチAZのAuto Scalingグループ内のAmazon EC2インスタンスに移行する。ストレージにはAmazon Elastic File System（Amazon EFS）を使用する。

D. アプリケーションをマルチAZのAuto Scalingグループ内のAmazon EC2インスタンスに移行する。ストレージにはAmazon Elastic Block Store（Amazon EBS）を使用する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- 出力ファイルサイズ：数十GB〜数百TB
- 標準的なファイルシステム構造が必要（ファイルシステムの意味論を維持）
- 自動スケール（スケールの自動化）および高可用性
- 運用負荷を最小限に抑える（マネージドサービスを優先）

正解はCである。

Amazon EFSは標準的なファイルシステムの意味論を提供するマネージドファイルストレージであり、容量を自動的に拡張し、リージョン内の複数アベイラビリティーゾーンで高可用性を提供するため、大容量ファイル保存と運用負荷の最小化の要件を満たす。

不正解の理由

A. アプリケーションをAmazon Elastic Container Service（Amazon ECS）上のコンテナとして移行する。ストレージにはAmazon S3を使用する。

Amazon S3はオブジェクトストレージであり、標準的なファイルシステムの意味論（ファイルロックやディレクトリ構造など）を提供しないため、要件を満たさない。

B. アプリケーションをAmazon Elastic Kubernetes Service（Amazon EKS）上のコンテナとして移行する。ストレージにはAmazon Elastic Block Store（Amazon EBS）を使用する。

Amazon EBSはブロックストレージで単一アベイラビリティーゾーンに依存し、複数ノード間での共有ファイルシステムとして不適切であり、自動スケールも制限される。

D. アプリケーションをマルチAZのAuto Scalingグループ内のAmazon EC2インスタンスに移行する。ストレージにはAmazon Elastic Block Store（Amazon EBS）を使用する。

EC2とEBSの構成は、EBSのアベイラビリティーゾーン依存性と共有ファイルシステムの欠如により、大規模ファイル共有、自動スケール、運用負荷の最小化の要件を満たさない。

Q. 053

SAA-C03

企業は会計記録をAmazon S3に保存する必要がある。記録は1年間即時アクセス可能でなければならず、その後さらに9年間アーカイブされなければならない。企業内の管理ユーザーやルートユーザーを含め、10年間の期間中に誰も記録を削除できてはならない。記録は最大の耐久性で保存されなければならない。これらの要件を満たすソリューションはどれか。

A. 記録を10年間S3 Glacierに保存する。アクセス制御ポリシーを使用して10年間記録の削除を拒否する。

B. S3 Intelligent-Tieringを使用して記録を保存する。IAMポリシーを使用して記録の削除を拒否する。10年後にIAMポリシーを変更して削除を許可する。

C. S3ライフサイクルポリシーを使用して、記録を1年後にS3 StandardからS3 Glacier Deep Archiveに移行する。S3 Object Lockのコンプライアンスモードを10年間使用する。

D. S3ライフサイクルポリシーを使用して、記録を1年後にS3 StandardからS3 One Zone-Infrequent Access (S3 One Zone-IA)に移行する。S3 Object Lockのガバナンスモードを10年間使用する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- 最初の1年間は即時アクセス可能
- その後9年間保管（合計10年間の保存期間）
- 管理者およびルートを含む誰も10年間削除不可
- 最大の耐久性（マルチAZ/耐久性保証）

正解はCである。

S3 Object Lockのコンプライアンスモードは保存期間中、管理者やルートを含むいかなるユーザーもオブジェクトを削除または上書きできない。また、ライフサイクルポリシーで1年後にS3 Glacier Deep Archiveに移行することで長期アーカイブと高い耐久性を提供する。

不正解の理由

A. 記録を10年間S3 Glacierに保存する。アクセス制御ポリシーを使用して10年間記録の削除を拒否する。

S3 Glacierに直接保存するだけでは、アカウントのルートや管理者がポリシーを変更して削除できるため、削除不可を保証できない。

B. S3 Intelligent-Tieringを使用して記録を保存する。IAMポリシーを使用して記録の削除を拒否する。10年後にIAMポリシーを変更して削除を許可する。

IAMポリシーは管理者やルートが変更または削除すれば回避可能であり、完全な削除防止にはならない。

D. S3ライフサイクルポリシーを使用して、記録を1年後にS3 StandardからS3 One Zone-Infrequent Access (S3 One Zone-IA)に移行する。S3 Object Lockのガバナンスモードを10年間使用する。

ガバナンスモードは特定の権限を持つユーザー（例：明示的権限を持つルートや管理者）が保存を無視できるため「誰も削除不可」の要件を満たさず、One Zone-IAはマルチAZ耐久性の要件を満たさない。

Q. 054

SAA-C03

ある企業はAWS上で複数のWindowsワークロードを運用している。同社の従業員は2台のAmazon EC2インスタンス上でホストされているWindowsファイル共有を使用している。これらのファイル共有は相互にデータを同期し、複製コピーを維持している。同社はユーザーが現在の方法でファイルにアクセスすることを維持しつつ、高可用性かつ耐久性のあるストレージソリューションを求めている。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. すべてのデータをAmazon S3に移行する。ユーザーがファイルにアクセスするためにIAM認証を設定する。

B. Amazon S3 File Gatewayを設定する。既存のEC2インスタンスにS3 File Gatewayをマウントする。

C. ファイル共有環境をマルチAZ構成のAmazon FSx for Windows File Serverに拡張する。すべてのデータをFSx for Windows File Serverに移行する。

D. ファイル共有環境をマルチAZ構成のAmazon Elastic File System（Amazon EFS）に拡張する。すべてのデータをAmazon EFSに移行する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- ユーザーの現在のファイルアクセス方法を維持する
- 高可用性を提供する
- データの耐久性を保証する
- Windowsファイル共有との互換性を維持する

正解はCである。

Amazon FSx for Windows File ServerはWindowsネイティブのSMBおよびActive Directory統合を提供するため、ユーザーはアクセス方法を変更する必要がなく、マルチAZ構成により高可用性と耐久性を備えた管理されたファイルストレージソリューションである。

不正解の理由

A. すべてのデータをAmazon S3に移行する。ユーザーがファイルにアクセスするためにIAM認証を設定する。

Amazon S3はオブジェクトストレージであり、SMB/Windowsファイルシステムのセマンティクス（ACL、ファイルロック、AD統合）を提供しないため、ユーザーの既存のアクセス方法を維持できない。

B. Amazon S3 File Gatewayを設定する。既存のEC2インスタンスにS3 File Gatewayをマウントする。

S3ファイルゲートウェイはS3のオブジェクトストレージを公開するため、Windowsネイティブのファイルサーバー機能（AD統合、ファイルロックなど）との完全な互換性を保証できない。

D. ファイル共有環境をマルチAZ構成のAmazon Elastic File System（Amazon EFS）に拡張する。すべてのデータをAmazon EFSに移行する。

Amazon EFSはNFSベースであり、Windows/SMBネイティブ機能をサポートしないため、Windowsファイル共有の要件を満たせない。

Q. 055

SAA-C03

ソリューションアーキテクトは複数のサブネットを含むVPCアーキテクチャを設計している。このアーキテクチャはAmazon EC2インスタンスとAmazon RDS DBインスタンスを使用するアプリケーションをホストする。アーキテクチャは2つのアベイラビリティーゾーンにまたがる6つのサブネットで構成されている。各アベイラビリティーゾーンにはパブリックサブネット、プライベートサブネット、およびデータベース専用のサブネットが含まれる。RDSデータベースにアクセスできるのはプライベートサブネットで実行されるEC2インスタンスのみである。これらの要件を満たすソリューションはどれか。

A. パブリックサブネットのCIDRブロックへのルートを除外した新しいルートテーブルを作成する。そのルートテーブルをデータベースサブネットに関連付ける。

B. パブリックサブネットのインスタンスに割り当てられたセキュリティグループからのインバウンドトラフィックを拒否するセキュリティグループを作成し、そのセキュリティグループをDBインスタンスにアタッチする。

C. プライベートサブネットのインスタンスに割り当てられたセキュリティグループからのインバウンドトラフィックを許可するセキュリティグループを作成し、そのセキュリティグループをDBインスタンスにアタッチする。

D. パブリックサブネットとプライベートサブネットの間に新しいピアリング接続を作成し、プライベートサブネットとデータベースサブネットの間に別のピアリング接続を作成する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- プライベートサブネットのEC2インスタンスのみがRDSにアクセス可能であること
- 各アベイラビリティーゾーンにパブリック、プライベート、DB専用サブネットが存在する（合計6サブネット）
- アプリケーションはAmazon EC2インスタンスとAmazon RDS DBインスタンスを使用する

正解はCである。

セキュリティグループでプライベートサブネットのインスタンスのセキュリティグループを送信元として許可すれば、これらのインスタンスのみがDBに接続可能となる詳細なインバウンド制御を提供する。セキュリティグループはステートフルであるため、応答トラフィックは自動的に許可される。VPC内部のアクセス制御はセキュリティグループで明確に実装される。

不正解の理由

A. パブリックサブネットのCIDRブロックへのルートを除外した新しいルートテーブルを作成する。そのルートテーブルをデータベースサブネットに関連付ける。

VPC内部のサブネット間通信は暗黙のlocalルートが存在し、ルーティングテーブルだけでパブリックサブネットへのアクセスを遮断できず、localルートは削除できない。

B. パブリックサブネットのインスタンスに割り当てられたセキュリティグループからのインバウンドトラフィックを拒否するセキュリティグループを作成し、そのセキュリティグループをDBインスタンスにアタッチする。

セキュリティグループは許可ルールのみをサポートし、明示的な拒否はサポートしないため、要件の実装に適さない。

D. パブリックサブネットとプライベートサブネットの間に新しいピアリング接続を作成し、プライベートサブネットとデータベースサブネットの間に別のピアリング接続を作成する。

VPCピアリングはVPC間の接続に使用され、同一VPC内のサブネット間制御のメカニズムではなく、不要に複雑である。

Q. 056

SAA-C03

ある企業はドメイン名をAmazon Route 53に登録している。同社はca-central-1リージョンでAmazon API Gatewayをバックエンドのマイクロサービスapiのパブリックインターフェースとして使用している。サードパーティのサービスはこれらのAPIを安全に利用している。同社はAPI GatewayのURLを自社のドメイン名と対応する証明書で設計し、サードパーティのサービスがHTTPSで利用できるようにしたい。どのソリューションがこれらの要件を満たすか？

A. API GatewayでName="Endpoint-URL"、Value="Company Domain Name"のステージ変数を作成し、デフォルトのURLを上書きする。会社のドメイン名に関連付けられた公開証明書をAWS Certificate Manager（ACM）にインポートする。

B. 会社のドメイン名でRoute 53のDNSレコードを作成する。エイリアスレコードをリージョナルAPI Gatewayステージエンドポイントにポイントする。会社のドメイン名に関連付けられた公開証明書をus-east-1リージョンのAWS Certificate Manager（ACM）にインポートする。

C. リージョナルAPI Gatewayエンドポイントを作成する。API Gatewayエンドポイントを会社のドメイン名に関連付ける。会社のドメイン名に関連付けられた公開証明書を同じリージョンのAWS Certificate Manager（ACM）にインポートし、証明書をAPI Gatewayエンドポイントにアタッチする。Route 53を設定してAPI Gatewayエンドポイントにトラフィックをルーティングする。

D. リージョナルAPI Gatewayエンドポイントを作成する。API Gatewayエンドポイントを会社のドメイン名に関連付ける。会社のドメイン名に関連付けられた公開証明書をus-east-1リージョンのAWS Certificate Manager（ACM）にインポートし、証明書をAPI GatewayのAPIにアタッチする。会社のドメイン名でRoute 53のDNSレコードを作成し、Aレコードを会社のドメイン名にポイントする。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- サードパーティクライアントがHTTPSでAPIにアクセスする必要がある
- 会社のドメイン名とその証明書を使用したAPI GatewayのURLを設計する必要がある

正解はCである。

Regional API Gatewayにカスタムドメインをマッピングするには、証明書がそのRegionalエンドポイントが存在する同一リージョンのACMに存在し、Route 53のエイリアスレコードでエンドポイントにルーティングする必要がある。選択肢Cはこの手順を正しく示している。

不正解の理由

A. API GatewayでName="Endpoint-URL"、Value="Company Domain Name"のステージ変数を作成し、デフォルトのURLを上書きする。会社のドメイン名に関連付けられた公開証明書をAWS Certificate Manager（ACM）にインポートする。

ステージ変数で基本URLを上書きしてもカスタムドメインとHTTPS証明書の適用は提供されず、正しい方法ではない。

B. 会社のドメイン名でRoute 53のDNSレコードを作成する。エイリアスレコードをリージョナルAPI Gatewayステージエンドポイントにポイントする。会社のドメイン名に関連付けられた公開証明書をus-east-1リージョンのAWS Certificate Manager（ACM）にインポートする。

Regionalエンドポイント用のカスタムドメイン証明書は該当Regionalリージョンの ACMに存在する必要があるが、us-east-1に証明書を配置すると誤って指定している。

D. リージョナルAPI Gatewayエンドポイントを作成する。API Gatewayエンドポイントを会社のドメイン名に関連付ける。会社のドメイン名に関連付けられた公開証明書をus-east-1リージョンのAWS Certificate Manager（ACM）にインポートし、証明書をAPI GatewayのAPIにアタッチする。会社のドメイン名でRoute 53のDNSレコードを作成し、Aレコードを会社のドメイン名にポイントする。

Regionalエンドポイントに対して証明書をus-east-1のACMに置くのは誤ったリージョンの使用であり、Aレコードの指示も不正確で正しくない。

Q. 057

SAA-C03

ある企業が人気のソーシャルメディアサイトを運営している。このサイトではユーザーが画像をアップロードして他のユーザーと共有できる。企業は画像に不適切なコンテンツが含まれていないことを確認したい。開発工数を最小限に抑えるソリューションが必要である。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. Amazon Comprehendを使用して不適切なコンテンツを検出する。信頼度の低い予測には人間によるレビューを行う。

B. Amazon Rekognitionを使用して不適切なコンテンツを検出する。信頼度の低い予測には人間によるレビューを行う。

C. Amazon SageMakerを使用して不適切なコンテンツを検出する。信頼度の低い予測にはGround Truthでラベル付けを行う。

D. AWS Fargateを使用してカスタム機械学習モデルをデプロイし、不適切なコンテンツを検出する。信頼度の低い予測にはGround Truthでラベル付けを行う。

✅ 正解: B / 解説

ソリューションは、次の要件を満たす必要がある。

- ユーザーがアップロードした画像の不適切なコンテンツを自動検出する
- 開発の労力を最小限に抑える
- 人気のソーシャルメディアウェブサイトを運営する
- ユーザーが他のユーザーと共有する画像をアップロード可能にする

正解はBである。

Amazon Rekognitionは画像の不適切なコンテンツ（Moderation）を検出するために設計されたマネージドサービスであり、すぐに利用可能なAPIを提供して開発の労力を最小限に抑える。信頼度スコアを提供するため、低い信頼度の結果に対して人によるレビューを容易に連携でき、要件を満たす。

不正解の理由

A. Amazon Comprehendを使用して不適切なコンテンツを検出する。信頼度の低い予測には人間によるレビューを行う。

Amazon Comprehendはテキスト分析用サービスであり、画像内容を直接分析するには適しておらず、要件を満たさない。

C. Amazon SageMakerを使用して不適切なコンテンツを検出する。信頼度の低い予測にはGround Truthでラベル付けを行う。

SageMakerはカスタムモデルの開発・トレーニングおよびGround Truthによるラベリングが必要であり、開発および運用の負担が大きくなり「開発の労力を最小限に抑える」要件を満たさない。

D. AWS Fargateを使用してカスタム機械学習モデルをデプロイし、不適切なコンテンツを検出する。信頼度の低い予測にはGround Truthでラベル付けを行う。

FargateにカスタムMLをデプロイするとモデルの開発・管理・デプロイによる相当な運用負担が発生し、要件を満たさない。

Q. 058

SAA-C03

企業は、スケーラビリティと可用性の要件を満たすために、重要なアプリケーションをコンテナで実行したいと考えている。企業は重要なアプリケーションの保守に注力したいと考えており、コンテナ化されたワークロードを実行する基盤となるインフラストラクチャのプロビジョニングおよび管理は担当したくない。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. Amazon EC2インスタンスを使用し、インスタンスにDockerをインストールする。

B. Amazon EC2ワーカーノード上のAmazon Elastic Container Service（Amazon ECS）を使用する。

C. AWS Fargate上のAmazon Elastic Container Service（Amazon ECS）を使用する。

D. Amazon Elastic Container Service（Amazon ECS）最適化Amazon Machine Image（AMI）からのAmazon EC2インスタンスを使用する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- コンテナベースの実行を提供すること
- アプリケーションの保守に集中できること
- 基盤インフラのプロビジョニングおよび管理を担当しないこと
- スケーラビリティと可用性の要件を満たすこと

正解はCである。

AWS Fargateはサーバーレスのコンテナ実行を提供し、EC2インスタンスのプロビジョニングおよび管理を不要にする。ECSと統合されており、スケーラビリティと可用性を提供するため、要件を最もよく満たす。

不正解の理由

A. Amazon EC2インスタンスを使用し、インスタンスにDockerをインストールする。
EC2にDockerを直接インストールすると、インフラのプロビジョニングおよび管理を自社で行う必要があり、要件に合致しない。

B. Amazon EC2ワーカーノード上のAmazon Elastic Container Service（Amazon ECS）を使用する。
ECSをEC2ワーカーノードで使用すると、ワーカーノード（EC2）の管理が必要であり、インフラ管理の責任が残る。

D. Amazon Elastic Container Service（Amazon ECS）最適化Amazon Machine Image（AMI）からのAmazon EC2インスタンスを使用する。

ECS最適化AMIを使用したEC2も依然としてEC2インスタンスのプロビジョニングおよび管理を要求するため、要件を満たさない。

Q. 059

SAA-C03

ある企業は300以上のグローバルなウェブサイトとアプリケーションをホストしている。同社は1日あたり30 TBを超えるクリックストリームデータを分析するプラットフォームを必要としている。クリックストリームデータを送信および処理するために、ソリューションアーキテクトは何をすべきか？

A. AWS Data Pipelineを設計してデータをAmazon S3バケットにアーカイブし、Amazon EMRクラスターを実行して分析を生成する。

B. Amazon EC2インスタンスのAuto Scalingグループを作成してデータを処理し、Amazon Redshiftが分析に使用するためにAmazon S3データレイクに送信する。

C. データをAmazon CloudFrontにキャッシュする。データをAmazon S3バケットに保存する。S3バケットにオブジェクトが追加されたときに、AWS Lambda 関数を実行して分析用にデータを処理する。

D. Amazon Kinesis Data Streamsからデータを収集する。Amazon Kinesis Data Firehoseを使用してデータをAmazon S3データレイクに送信する。分析のためにAmazon Redshiftにデータをロードする。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- 毎日30TB以上の処理が可能な拡張性
- 300以上のグローバルウェブサイトおよびアプリケーションから生成されるクリックストリームデータ
- クリックストリームデータの送信設計
- クリックストリームデータの処理設計
- クリックストリームデータを分析するプラットフォームが必要

正解はDである。

世界中のウェブおよびアプリで発生するクリックストリームを大規模（毎日30TB以上）かつ継続的に収集するため、ストリーミング収集層が必要である。Kinesis Data Streamsは大量のイベントをリアルタイムで受け取りバッファリングおよび拡張可能であり、Kinesis Data Firehoseは運用負荷を抑えてS3に自動的にデータを格納（バッチ処理、圧縮、変換も可能）する。その後、S3のデータレイクに蓄積されたデータをRedshiftにロードして大規模分析を行う流れが、「送信＋処理プラットフォーム」の要件に最も適合する。

不正解の理由

A. AWS Data Pipelineを設計してデータをAmazon S3バケットにアーカイブし、Amazon EMRクラスターを実行して分析を生成する。

AWS Data Pipelineは旧世代の性格が強く、リアルタイムのクリックストリーム収集や大規模ストリーミングパイプラインの代表的な解決策ではない。EMRも可能だが、毎日30TB以上を常に処理する場合、ク

ラスターの運用、チューニング、スケジューリングの負荷が大きくなり、管理型かつストリーミングの標準的設計という要件の意図から外れる。つまり可能だが効率的でなく現代的な選択肢ではない。

B. Amazon EC2インスタンスのAuto Scalingグループを作成してデータを処理し、Amazon Redshiftが分析に使用するためにAmazon S3データレイクに送信する。

EC2 Auto Scalingで直接パイプラインを構築すると、収集、バッファリング、再処理、重複排除、障害復旧などストリーミングパイプラインの核心をすべて自前で実装・運用する必要がある。毎日30TB以上の規模では運用負荷が非常に大きく、この種の要件では通常Kinesisやマネージドインジェストでの解決を推奨する。Redshiftでの分析は正しいが、前段の設計が非効率的である。

C. データをAmazon CloudFrontにキャッシュする。データをAmazon S3バケットに保存する。S3バケットにオブジェクトが追加されたときに、AWS Lambda 関数を実行して分析用にデータを処理する。

CloudFrontキャッシュはコンテンツ配信の高速化であり、クリックストリームの収集・送信層ではない。また、S3オブジェクトアップロードごとにLambdaで処理する方式は、30TB/日の規模でイベント数が爆発するとLambdaの呼び出し、同時実行、再試行、順序保証などの運用が複雑になる。クリックストリームの標準的な流れは「イベントストリーム収集→格納」であり、キャッシュとS3トリガーは性質が異なる。

Q. 060

SAA-C03

ある企業がAWS上にホストされたウェブサイトを運用している。このウェブサイトはHTTPとHTTPSを別々に処理するように設定されたApplication Load Balancer（ALB）の背後にある。企業はすべてのリクエストをHTTPSで処理するように転送したい。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. ALBのネットワークACLを更新してHTTPSトラフィックのみを許可する。

B. URL内のHTTPをHTTPSに置き換えるルールを作成する。

C. ALBにリスナールールを作成し、HTTPトラフィックをHTTPSにリダイレクトする。

D. ALBをServer Name Indication（SNI）を使用するように設定されたNetwork Load Balancerに置き換える。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- ウェブサイトはAWSでホスティングされている
- ウェブサイトはHTTPとHTTPSを別々に処理するように設定されたApplication Load Balancer(ALB)の背後にある
- 会社はウェブサイトへのすべてのリクエストがHTTPSを使用することを望んでいる
- すべてのクライアントリクエストがHTTPSで送信されることを望んでいる

正解はCである。

ALBはリスナールールを使用してHTTP(ポート80)で受信したリクエストをHTTPS(ポート443)にリダイレクトするよう設定でき、要件を直接満たす。これはユーザーに標準的な301/302リダイレクトを提供し、追加のインフラ変更を必要としない。

不正解の理由

A. ALBのネットワークACLを更新してHTTPSトラフィックのみを許可する。

NACLはステートレスで許可または拒否のみを行い、リダイレクト機能がないためHTTPリクエストをHTTPSに変換できない。拒否すると接続失敗を引き起こす。

B. URL内のHTTPをHTTPSに置き換えるルールを作成する。

URL文字列を単に置換すると表現しているが現実的でなく、プロトコルのアップグレードを保証するALBのリダイレクト機能を使う方が適切である。

D. ALBをServer Name Indication（SNI）を使用するように設定されたNetwork Load Balancerに置き換える。

Network Load BalancerはL4レベルのロードバランシングであり、HTTP→HTTPSのリダイレクトなどのHTTPレベルの操作は行わない。SNIはTLSの仮想ホスト用であり、プロトコルの強制切り替えとは無関係である。

Q. 061

SAA-C03

ある企業はAWS上で2層のウェブアプリケーションを開発している。同社の開発者は、バックエンドのAmazon RDSデータベースに直接接続するAmazon EC2インスタンス上にアプリケーションをデプロイした。同社はアプリケーションにデータベースの認証情報をハードコーディングしてはならない。また、データベースの認証情報を定期的に自動ローテーションするソリューションを実装しなければならない。これらの要件を運用上のオーバーヘッドを最小限に抑えて満たすソリューションはどれか。

A. データベースの認証情報をインスタンスメタデータに保存する。Amazon EventBridge（Amazon CloudWatch Events）ルールを使用して、スケジュールされたAWS Lambda 関数を実行し、RDSの認証情報とインスタンスメタデータを同時に更新する。

B. データベースの認証情報を暗号化されたAmazon S3バケット内の設定ファイルに保存する。Amazon EventBridge（Amazon CloudWatch Events）ルールを使用して、スケジュールされたAWS Lambda 関数を実行し、RDSの認証情報と設定ファイル内の認証情報を同時に更新する。S3バージョニングを使用して以前の値に戻せるようにする。

C. データベースの認証情報をAWS Secrets Managerのシークレットとして保存する。シークレットの自動ローテーションを有効にする。EC2ロールにシークレットへのアクセス権限を付与する。

D. データベースの認証情報をAWS Systems Manager Parameter Storeの暗号化されたパラメータとして保存する。暗号化パラメータの自動ローテーションを有効にする。EC2ロールに暗号化パラメータへのアクセス権限を付与する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- アプリケーションにデータベース認証情報をハードコーディングしないこと
- データベース認証情報を定期的に自動ローテーションすること
- 運用上のオーバーヘッドを最小限に抑えて実装すること

正解はCである。

AWS Secrets Managerはデータベース認証情報をシークレットとして安全に保存し、組み込みの自動ローテーション機能を提供する。EC2のIAMロールにシークレットへのアクセス権限を付与すれば、アプリケーションは認証情報を直接取得できるため、運用上のオーバーヘッドを最小限に抑えられる。

不正解の理由

A. データベースの認証情報をインスタンスメタデータに保存する。Amazon EventBridge（Amazon CloudWatch Events）ルールを使用して、スケジュールされたAWS Lambda 関数を実行し、RDSの認証情報とインスタンスメタデータを同時に更新する。

インスタンスメタデータに機密認証情報を保存するとセキュリティリスクが高く、自動ローテーションを自前で実装する必要があり運用上のオーバーヘッドが増加する。

B. データベースの認証情報を暗号化されたAmazon S3バケット内の設定ファイルに保存する。Amazon EventBridge（Amazon CloudWatch Events）ルールを使用して、スケジュールされたAWS Lambda関数を実行し、RDSの認証情報と設定ファイル内の認証情報を同時に更新する。S3バージョニングを使用して以前の値に戻せるようにする。

S3に設定ファイルを置きLambdaでローテーションすると手動でロジックを維持管理する必要があり、運用上のオーバーヘッドと複雑性が高まる。

D. データベースの認証情報をAWS Systems Manager Parameter Storeの暗号化されたパラメータとして保存する。暗号化パラメータの自動ローテーションを有効にする。EC2ロールに暗号化パラメータへのアクセス権限を付与する。

Parameter StoreはSecrets Managerほど完全なデータベース認証情報のローテーション機能を持たず（またはローテーションはユーザー実装が必要）、運用作業が増加する可能性がある。

Q. 062

SAA-C03

企業が新しいパブリックウェブアプリケーションをAWSに展開している。アプリケーションはApplication Load Balancer（ALB）の背後で動作する。アプリケーションは外部の証明書機関（CA）によって発行されたSSL/TLS証明書でエッジで暗号化する必要がある。証明書は有効期限が切れる前に毎年ローテーションしなければならない。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. AWS Certificate Manager（ACM）を使用してSSL/TLS証明書を発行する。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーションする。

B. AWS Certificate Manager（ACM）を使用してSSL/TLS証明書を発行する。証明書からキー素材をインポートする。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーションする。

C. AWS Certificate Manager（ACM）Private Certificate Authorityを使用してルートCAからSSL/TLS証明書を発行する。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーションする。

D. AWS Certificate Manager（ACM）を使用してSSL/TLS証明書をインポートする。証明書をALBに適用する。Amazon EventBridge（Amazon CloudWatch Events）を使用して証明書の有効期限が近づいたときに通知を送信する。証明書は手動でローテーションする。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- ALBでSSL/TLSによる転送中の暗号化を適用すること
- 証明書は外部認証機関(CA)が発行したものであること（ブラウザの信頼が必要）
- 証明書は毎年有効期限前に更新すること
- パブリックウェブアプリケーションに適用すること

正解はDである。

ACMは外部CAが発行した証明書をインポートしてALBに適用可能であり、インポートした証明書はACMの管理による自動更新対象外であるため、EventBridge通知と手動更新プロセスにより年間更新要件を実務的に満たす。

不正解の理由

A. AWS Certificate Manager（ACM）を使用してSSL/TLS証明書を発行する。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーションする。

ACMが発行する証明書はAWS管理のCAから発行されており、「外部認証機関(CA)が発行した」という条件を満たさない。

B. AWS Certificate Manager（ACM）を使用してSSL/TLS証明書を発行する。証明書からキー素材をインポートする。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーシ

ョンする。

発行済み証明書を再度キー素材としてインポートするのは矛盾であり、インポート証明書はACMの管理による自動更新をサポートしない。

C. AWS Certificate Manager（ACM）Private Certificate Authorityを使用してルートCAからSSL/TLS証明書を発行する。証明書をALBに適用する。管理された更新機能を使用して証明書を自動的にローテーションする。

ACM Private CAはプライベート証明書を発行するため、公開インターネット上のブラウザ信頼が必要なパブリックウェブアプリケーションの要件を満たさない。

Q. 063

SAA-C03

ある企業はAWS上でインフラを運用しており、ドキュメント管理アプリケーションの登録ユーザー数は70万人である。同社は大容量の.pdfファイルを.jpg画像ファイルに変換する製品を作成する予定である。.pdfファイルの平均サイズは5MBである。同社は元のファイルと変換後のファイルの両方を保存する必要がある。ソリューションアーキテクトは、需要が急速に増加することを見越してスケーラブルなソリューションを設計しなければならない。これらの要件を最もコスト効率よく満たすソリューションはどれか。

A. .pdfファイルをAmazon S3に保存する。S3のPUTイベントを設定してAWS Lambda 関数を呼び出し、ファイルを.jpg形式に変換してAmazon S3に保存する。

B. .pdfファイルをAmazon DynamoDBに保存する。DynamoDB Streams機能を使用してAWS Lambda 関数を呼び出し、ファイルを.jpg形式に変換してDynamoDBに保存する。

C. .pdfファイルをAWS Elastic Beanstalkアプリケーションにアップロードする。このアプリケーションはAmazon EC2インスタンス、Amazon Elastic Block Store（EBS）ストレージ、およびAuto Scalingグループを含む。EC2インスタンス内のプログラムでファイルを.jpg形式に変換し、.pdfファイルと.jpgファイルをEBSストアに保存する。

D. .pdfファイルをAWS Elastic Beanstalkアプリケーションにアップロードする。このアプリケーションはAmazon EC2インスタンス、Amazon Elastic File System（EFS）ストレージ、およびAuto Scalingグループを含む。EC2インスタンス内のプログラムでファイルを.jpg形式に変換し、.pdfファイルと.jpgファイルをEBSストアに保存する。

✅ 正解: A / 解説

ソリューションは、次の要件を満たす必要がある。

- 原本（.pdf）および変換後（.jpg）ファイルを保存する必要がある
- 平均ファイルサイズは5MBである
- ユーザー基盤が大きく需要が急速に増加している
- スケーラビリティの要件があり、コスト効率の良い設計が必要である
- 登録ユーザー数は700,000人である

正解はAである。

Amazon S3はオブジェクトストレージで大容量ファイルの保存にコスト効率が良くスケーラブルである。S3 PUTイベントとAWS Lambdaの組み合わせはサーバーレスで自動的にスケールし、使用量に応じた課金により運用負荷とコストを最小限に抑える。

不正解の理由

B. .pdfファイルをAmazon DynamoDBに保存する。DynamoDB Streams機能を使用してAWS Lambda 関数を呼び出し、ファイルを.jpg形式に変換してDynamoDBに保存する。

Amazon DynamoDBは大きなバイナリオブジェクトの保存に適さず、コストが高い。Streamsのペイロードやサイズ制限により不適切である。

C. .pdfファイルをAWS Elastic Beanstalkアプリケーションにアップロードする。このアプリケーションはAmazon EC2インスタンス、Amazon Elastic Block Store（EBS）ストレージ、およびAuto Scalingグループを含む。EC2インスタンス内のプログラムでファイルを.jpg形式に変換し、.pdfファイルと.jpgファイルをEBSストアに保存する。

Amazon EBSはインスタンスに依存するブロックストレージで共有やスケーラビリティに劣る。Elastic BeanstalkとEC2の組み合わせは運用負荷とコストがより大きい。

D. .pdfファイルをAWS Elastic Beanstalkアプリケーションにアップロードする。このアプリケーションはAmazon EC2インスタンス、Amazon Elastic File System（EFS）ストレージ、およびAuto Scalingグループを含む。EC2インスタンス内のプログラムでファイルを.jpg形式に変換し、.pdfファイルと.jpgファイルをEBSストアに保存する。

Amazon EFSは共有ファイルシステムであるが、S3よりコストと運用負荷が高い。提示された構成は不要な複雑さとコスト増加を招く。

Q. 064

SAA-C03

ある企業はオンプレミスで稼働するWindowsファイルサーバーに5TBを超えるファイルデータを保有している。ユーザーとアプリケーションは毎日そのデータにアクセスしている。企業はWindowsワークロードをAWSに移行している。移行を進める中で、AWSとオンプレミスのファイルストレージに対して最低限のレイテンシーでアクセスできることが求められている。既存のファイルアクセスパターンに大きな変更を加えず、運用上の負担を最小限に抑えるソリューションが必要である。企業はAWSへの接続にAWS Site-to-Site VPN接続を使用している。これらの要件を満たすためにソリューションアーキテクトは何をすべきか？

A. AWS上にAmazon FSx for Windows File Serverを展開および構成する。オンプレミスのファイルデータをFSx for Windows File Serverに移行する。ワークロードを再構成してAWS上のFSx for Windows File Serverを使用させる。

B. オンプレミスにAmazon S3 File Gatewayを展開および構成する。オンプレミスのファイルデータをS3 File Gatewayに移行する。オンプレミスのワークロードとクラウドのワークロードを再構成してS3 File Gatewayを使用させる。

C. オンプレミスにAmazon S3 File Gatewayを展開および構成する。オンプレミスのファイルデータをAmazon S3に移行する。ワークロードを再構成して、各ワークロードの場所に応じてAmazon S3またはS3 File Gatewayのいずれかを直接使用させる。

D. AWS上にAmazon FSx for Windows File Serverを展開および構成する。オンプレミスにAmazon FSx File Gatewayを展開および構成する。オンプレミスのファイルデータをFSx File Gatewayに移行する。クラウドのワークロードをAWS上のFSx for Windows File Serverを使用するように構成し、オンプレミスのワークロードをFSx File Gatewayを使用するように構成する。

✅ 正解: D / 解説

ソリューションは、次の要件を満たす必要がある。

- オンプレミスとAWSの両方から最小遅延でファイルにアクセスすること
- 運用上の負担を最小限に抑えること
- 既存のWindowsファイルアクセス（SMB）パターンに重要な変更を要求しないこと
- データ規模は5TBを超え、日次アクセスがあること
- 接続はAWS Site-to-Site VPNを使用すること

正解はDである。

FSx for Windows File ServerはWindowsネイティブのSMB機能を提供し、管理されたサービスで運用負担が少ない。オンプレミスにFSx File Gatewayを展開すればローカルキャッシュによりオンプレミスアクセスの遅延を最小化し、同じSMBインターフェースを維持してワークロードの変更を最小限に抑える。クラウドワークロードはAWSのFSxを直接利用して性能を確保する。

不正解の理由

A. AWS上にAmazon FSx for Windows File Serverを展開および構成する。オンプレミスのファイルデータをFSx for Windows File Serverに移行する。ワークロードを再構成してAWS上のFSx for Windows File Serverを使用させる。

オンプレミスのワークロードがVPN経由でAWSのFSxに直接アクセスすると遅延が大きくなり、「最小遅延」の要件を満たさない可能性がある。

B. オンプレミスにAmazon S3 File Gatewayを展開および構成する。オンプレミスのファイルデータをS3 File Gatewayに移行する。オンプレミスのワークロードとクラウドのワークロードを再構成してS3 File Gatewayを使用させる。

S3 File Gatewayはバックエンドがオブジェクトストレージ（Amazon S3）であるため、Windows固有のSMB/NTFS/ACL機能を完全に提供できず、既存のファイルアクセスパターンに変更を要求する可能性がある。

C. オンプレミスにAmazon S3 File Gatewayを展開および構成する。オンプレミスのファイルデータをAmazon S3に移行する。ワークロードを再構成して、各ワークロードの場所に応じてAmazon S3またはS3 File Gatewayのいずれかを直接使用させる。

Amazon S3（オブジェクトストレージ）への移行はWindowsファイルサーバー機能（SMB、NTFS ACLなど）と互換性がなく、ワークロードに重要な変更を要求し、遅延目標を保証できない。

Q. 065

SAA-C03

病院は最近、Amazon API Gateway と AWS Lambda を使用して RESTful API を展開した。病院は API Gateway と Lambda を使用して、PDF 形式および JPEG 形式のレポートをアップロードしている。病院は Lambda コードを修正して、レポート内の保護対象医療情報（PHI）を識別する必要がある。これらの要件を最小限の運用上の負担で満たすソリューションはどれか。

A. 既存の Python ライブラリを使用してレポートからテキストを抽出し、抽出したテキストから PHI を識別する。

B. Amazon Textract を使用してレポートからテキストを抽出し、Amazon SageMaker を使用して抽出したテキストから PHI を識別する。

C. Amazon Textract を使用してレポートからテキストを抽出し、Amazon Comprehend Medical を使用して抽出したテキストから PHI を識別する。

D. Amazon Rekognition を使用してレポートからテキストを抽出し、Amazon Comprehend Medical を使用して抽出したテキストから PHI を識別する。

✅ 正解: C / 解説

ソリューションは、次の要件を満たす必要がある。

- PDFおよびJPEG形式のレポートを処理すること
- 抽出したテキストから保護された健康情報（PHI）を識別すること
- Lambdaコードの変更で統合可能であること
- 運用上の負担を最小限に抑えること

正解はCである。

Amazon TextractはPDFおよび画像から文書レベルのOCRを正確に実行し、Amazon Comprehend MedicalはPHI（医療関連エンティティ）をマネージドAPIで識別するため、別途モデルの開発や保守が不要で要件を満たし運用負荷を軽減する。

不正解の理由

A. 既存の Python ライブラリを使用してレポートからテキストを抽出し、抽出したテキストから PHI を識別する。

既存のPythonライブラリではOCRや医療用エンティティ認識の精度を維持するためにモデル開発・チューニング・保守が必要であり、運用負荷が高い。

B. Amazon Textract を使用してレポートからテキストを抽出し、Amazon SageMaker を使用して抽出したテキストから PHI を識別する。

Textractは適切だが、SageMakerを使用するとPHI識別のためにモデルの開発・学習・デプロイ・保守が必要で運用負荷が大きい。

D. Amazon Rekognition を使用してレポートからテキストを抽出し、Amazon Comprehend Medical を使用して抽出したテキストから PHI を識別する。

Amazon Rekognitionは文書用OCRではなく画像分析に特化しており、PDF処理や文書テキスト抽出においてTextractより適しておらず、精度や運用面で不利である。