AWS Certified Security - Specialty (SCS-C02) 試験ガイド

はじめに

AWS Certified Security - Specialty (SCS-C02) 試験は、セキュリティ担当者を対象としています。この試験では、受験者が AWS の製品とサービスのセキュリティ保護に関する知識を効果的に示すことができるか試されます。

また、受験者が以下を身に付けているかどうかも確認します。

- 専門的なデータ分類と AWS のデータ保護メカニズムについて理解していること
- データ暗号化方式と、それを実装するための AWS のメカニズムを理解していること
- セキュアなインターネットプロトコルと、それを実装するための AWS のメカニズムを理解していること
- AWS のセキュリティサービスと、安全な本番環境の提供のために使用するサービスの機能について実践的な知識を備えていること
- AWS のセキュリティサービスと機能を使った本番環境をデプロイしてきた 2 年以上の経験から得られたコンピテンシーを身に付けていること
- 一連のアプリケーション要件を満たすために、コスト、セキュリティ、デプロイの複雑性に関してトレードオフを判断する能力があること
- セキュリティの運用とリスクについて理解していること

受験対象者について

受験対象者には、セキュリティソリューションの設計と実装の分野で 3〜5 年相当の経験が必要です。また、AWS ワークロードのセキュリティ保護の分野で 2 年以上の実務経験が必要です。

推奨される AWS の知識

受験対象者は、以下を理解している必要があります。

- AWS の責任共有モデルとそのアプリケーション
- AWS のサービスとクラウドソリューションのデプロイに関する一般的な知識
- AWS 環境とワークロードのセキュリティ管理
- ロギング戦略とモニタリング戦略

- 脆弱性管理とセキュリティの自動化
- AWS のセキュリティサービスをサードパーティーのツールと統合する方法
- バックアップ戦略を含む災害対策管理
- 暗号化とキー管理
- Identity Access Management
- データ保持とライフサイクル管理
- セキュリティ問題のトラブルシューティング方法
- マルチアカウントガバナンスと組織コンプライアンス
- 脅威検出とインシデント対応戦略

受験対象者にとって対象範囲外のジョブタスクとみなされるもの

受験対象者が実施できることが想定されていないジョブタスクは、以下のリストのとおりです。このリストはすべてを網羅しているわけではありません。以下のタスクは、本試験の範囲外です。

- 特定の言語 (Python、Java など) でソフトウェアを開発する。
- 規制コンプライアンスを確認する。
- ソフトウェア開発ライフサイクルを管理する。
- ネットワークトポロジーを設計する。
- クラウドデプロイ全体を設計する。
- データレジデンシー要件 (一般データ保護規則 [GDPR] など) に基づいてストレージサービスを構成する。

試験に出題される可能性のあるテクノロジーと概念のリスト、試験対象の AWS サービスと機能のリスト、および試験対象外の AWS サービスと機能のリストについては、付録を参照してください。

試験内容

解答タイプ

試験には次の 2 種類の設問があります。

- **択一選択問題:** 正しい選択肢が 1 つ、誤った選択肢 (不正解) が 3 つ提示される。
- **複数選択問題:** 5 つ以上の選択肢のうち、正解が 2 つ以上ある。

設問の記述に最もよく当てはまるもの、または正解となるものを 1 つ以上選択します。不正解の選択肢は、知識や技術が不十分な受験者が選択してしまいそうな、設問内容と一致するもっともらしい解答になっています。

未解答の設問は不正解とみなされます。推測による解答にペナルティはありません。試験には、スコアに影響する設問が 50 問含まれています。

採点対象外の設問

試験には、スコアに影響しない採点対象外の設問が 15 問含まれています。AWS ではこういった採点対象外の設問での成績情報を収集し、今後採点対象の設問として使用できるかどうかを評価します。試験では、どの設問が採点対象外かは受験者にわからないようになっています。

試験の結果

AWS Certified Security - Specialty (SCS-C02) 試験は、合否判定方式の試験です。試験の採点は、認定業界のベストプラクティスおよびガイドラインに基づいた、AWS の専門家によって定められる最低基準に照らして行われます。

試験の結果は、100～1,000 のスケールスコアとして報告されます。合格スコアは 750 です。このスコアにより、試験全体の成績と合否がわかります。複数の試験間で難易度がわずかに異なる可能性があるため、スコアを均等化するためにスケールスコアが使用されます。

スコアレポートには、各セクションの成績を示す分類表が含まれる場合があります。試験には補整スコアリングモデルが使用されるため、セクションごとに合否ラインは設定されておらず、試験全体のスコアで合否が判定されます。

試験の各セクションには特定の重みが設定されているため、各セクションに割り当てられる設問数が異なる場合があります。分類表には、受験者の得意な部分と弱点を示す全般的な情報が含まれます。セクションごとのフィードバックを解釈する際は注意してください。

試験内容の概要

この試験ガイドには、セクションに設定された重み、コンテンツドメイン、タスクステートメントについての説明が含まれています。本ガイドは、試験内容の包括的な

リストを提供するものではありません。ただし、各タスクステートメントの追加情報を使って、試験の準備に役立てることができます。

本試験のコンテンツドメインと重み設定は以下のとおりです。

- 第 1 分野: 脅威検出とインシデント対応 (採点対象コンテンツの 14%)
- 第 2 分野: セキュリティロギングとモニタリング (採点対象コンテンツの 18%)
- 第 3 分野: インフラストラクチャのセキュリティ (採点対象コンテンツの 20%)
- 第 4 分野: Identity and Access Management (採点対象コンテンツの 16%)
- 第 5 分野: データ保護 (採点対象コンテンツの 18%)
- 第 6 分野: 管理とセキュリティガバナンス (採点対象コンテンツの 14%)

第 1 分野: 脅威検出とインシデント対応

タスクステートメント 1.1: インシデント対応計画を策定して実装する。

対象知識:

- インシデント対応に関連する AWS のベストプラクティス
- クラウドで発生するインシデント
- インシデント対応計画における役割と責任
- AWS Security Finding Format (ASFF)

対象スキル:

- セキュリティ侵害に対応するための認証情報の無効化およびローテーション戦略の実装 (AWS Identity and Access Management [IAM] や AWS Secrets Manager の使用など)
- AWS リソースの分離
- セキュリティインシデントに対応するためのプレイブックとランブックの策定、実装
- セキュリティサービスのデプロイ (AWS Security Hub、Amazon Macie、Amazon GuardDuty、Amazon Inspector、AWS Config、Amazon Detective、AWS Identity and Access Management Access Analyzer など)
- AWS ネイティブサービスとサードパーティーサービスの統合の設定 (Amazon EventBridge や ASFF の使用など)

タスクステートメント 1.2: AWS のサービスを使用してセキュリティの脅威と異常を検出する。

対象知識:

- 脅威を検出する AWS マネージドセキュリティサービス
- サービス間でデータを結合するためのアノマリーおよび相関手法
- 異常を特定するための視覚化
- セキュリティ調査結果を一元化する戦略

対象スキル:

- セキュリティサービス (GuardDuty、Security Hub、Macie、AWS Config、IAM Access Analyzer など) から得られた結果の評価
- AWS のサービス全体にわたるセキュリティ脅威の検索と関連付け (Detective の使用など)
- セキュリティイベントを検証するためにクエリを実行 (Amazon Athena の使用など)
- 異常なアクティビティを検出するためのメトリクスフィルターとダッシュボードの作成 (Amazon CloudWatch の使用など)

タスクステートメント 1.3: 侵害されたリソースとワークロードに対応する。

対象知識:

- AWS セキュリティインシデント対応ガイド
- リソース分離メカニズム
- 根本原因分析の手法
- データ取得メカニズム
- イベント検証のためのログ分析

対象スキル:

- AWS のサービス (AWS Lambda、AWS Step Functions、EventBridge、AWS Systems Manager のランブック、Security Hub、AWS Config など) を使用した修復の自動化
- 侵害されたリソースへの対応 (Amazon EC2 インスタンスの分離など)
- 根本原因分析のための調査と分析 (Detective の使用など)
- 侵害されたリソースからの関連するフォレンジックデータの取得 (Amazon Elastic Block Store [Amazon EBS] のボリュームスナップショット、メモリダンプなど)

- Amazon S3 のログでセキュリティイベントに関連するコンテキスト情報のクエリを実行 (Athena の使用など)
- フォレンジックアーティファクトの保護、保存 (S3 オブジェクトロック、分離されたフォレンジックアカウント、S3 ライフサイクル、S3 レプリケーションの使用など)
- インシデントに備えてサービスを準備し、インシデント後のサービスを復旧

第 2 分野: セキュリティロギングとモニタリング

タスクステートメント 2.1: セキュリティイベントに対処するためのモニタリングとアラートを設計し、実装する。

対象知識:

- イベントをモニタリングしてアラームを提供する AWS のサービス (CloudWatch、EventBridge など)
- アラートを自動化する AWS のサービス (Lambda、Amazon Simple Notification Service [Amazon SNS]、Security Hub など)
- メトリクスとベースラインをモニタリングするツール (GuardDuty、Systems Manager など)

対象スキル:

- アーキテクチャを分析してモニタリング要件とセキュリティモニタリングのデータソースを特定
- 環境とワークロードを分析してモニタリング要件を決定
- ビジネス要件とセキュリティ要件に基づく環境モニタリングとワークロードモニタリングを設計
- 定期的な監査を実施するための自動化ツールとスクリプトを設定 (Security Hub でカスタムインサイトを作成するなど)
- アラートを生成するメトリクスとしきい値を定義

タスクステートメント 2.2: セキュリティモニタリングとアラートのトラブルシューティングを行う。

対象知識:

- モニタリングサービスの設定 (Security Hub など)
- セキュリティイベントを示す関連データ

対象スキル:

- 可視性やアラートが得られなかったイベントが発生した後のサービス機能、アクセス許可、リソース構成を分析
- 統計情報の報告がないカスタムアプリケーションの構成を分析、修正
- セキュリティ要件を満たすためのロギングサービスとモニタリングサービスを評価

タスクステートメント 2.3: ロギングソリューションを設計し、実装する。

対象知識:

- ロギング機能を提供する AWS のサービスと機能 (VPC フローログ、DNS ログ、AWS CloudTrail、Amazon CloudWatch Logs など)
- ロギング機能の属性 (ログレベル、タイプ、詳細度など)
- ログの保存先とライフサイクル管理 (保存期間など)

対象スキル:

- サービスとアプリケーションのロギングの設定
- ロギングの要件とログの取り込み元の特定
- AWS のベストプラクティスと組織の要件に合わせたログストレージとライフサイクル管理の実装

タスクステートメント 2.4: ロギングソリューションのトラブルシューティングを行う。

対象知識:

- データソースを提供する AWS サービスの機能とユースケース (ログレベル、タイプ、詳細度、頻度、適時性、不変性など)
- ロギング機能を提供する AWS のサービスと機能 (VPC フローログ、DNS ログ、CloudTrail、CloudWatch Logs など)
- ロギングに必要なアクセス許可

対象スキル:

- 設定ミスを特定し、ロギングに必要なアクセス許可がない場合の修正手順を決定 (読み取り/書き込み権限、S3 バケットのアクセス許可、パブリックアクセス、整合性の管理など)
- ログが見つからない原因を特定し、修正手順を実行

タスクステートメント 2.5: ログ分析ソリューションを設計する。

対象知識:

- キャプチャしたログを分析するサービスおよびツール (Athena、CloudWatch Logs フィルターなど)
- AWS のサービスのログ分析機能 (CloudWatch Logs Insights、CloudTrail インサイト、Security Hub インサイトなど)
- ログ形式とコンポーネント (CloudTrail ログなど)

対象スキル:

- ログ内のパターンを特定して異常や既知の脅威を指摘
- ログの正規化、解析、関連付け

第 3 分野: インフラストラクチャのセキュリティ

タスクステートメント 3.1: エッジサービスのセキュリティコントロールを設計し、実装する。

対象知識:

- エッジサービスのセキュリティ機能 (AWS WAF、ロードバランサー、Amazon Route 53、Amazon CloudFront、AWS Shield など)
- 一般的な攻撃、脅威、エクスプロイト (Open Web Application Security Project [OWASP] Top 10、DDoS など)
- 階層化ウェブアプリケーションアーキテクチャ

対象スキル:

- 一般的なユースケース (公開ウェブサイト、サーバーレスアプリケーション、モバイルアプリケーションバックエンドなど) 向けのエッジセキュリティ戦略を定義
- 予想される脅威や攻撃 (OWASP Top 10、DDoS など) に基づいて適切なエッジサービスを選択
- 予想される脆弱性とリスク (脆弱なソフトウェア、アプリケーション、ライブラリなど) に基づいて適切な保護手段を選択
- エッジセキュリティサービス (AWS WAF およびロードバランサーを使用した CloudFront など) を組み合わせて防御レイヤーを定義
- さまざまな基準 (地域、位置情報、レート制限など) に基づいてエッジで制限事項を適用

- エッジサービスに関するログ、メトリクス、モニタリングを有効化して攻撃を検知

タスクステートメント 3.2: ネットワークのセキュリティコントロールを設計し、実装する。

対象知識:

- VPC のセキュリティメカニズム (セキュリティグループ、ネットワーク ACL、AWS Network Firewall など)
- VPC 間の接続 (AWS Transit Gateway、VPC エンドポイントなど)
- セキュリティテレメトリのソース (トラフィックミラーリング、VPC フローログなど)
- VPN テクノロジー、用語、使用法
- オンプレミス接続オプション (AWS VPN、AWS Direct Connect など)

対象スキル:

- セキュリティ要件に基づくネットワークセグメンテーションの実装 (パブリックサブネット、プライベートサブネット、機密性の高い VPC、オンプレミス接続など)
- 必要に応じてネットワークトラフィックを許可または禁止するネットワークコントロールの設計 (セキュリティグループ、ネットワーク ACL、Network Firewall の使用など)
- データがパブリックインターネットを通過しないネットワークフローを設計 (Transit Gateway、VPC エンドポイント、VPC での Lambda の使用など)
- ネットワーク設計、脅威、攻撃に基づいて、モニタリングするテレメトリソースを決定 (ロードバランサーのログ、VPC フローログ、トラフィックミラーリングなど)
- オンプレミス環境と AWS クラウド間の通信に関する冗長性とセキュリティワークロードの要件を決定 (AWS VPN、Direct Connect 経由の AWS VPN、MACsec の使用など)
- 不要なネットワークアクセスを特定、削除
- 要件の変化に応じてネットワーク設定を管理 (AWS Firewall Manager の使用など)

タスクステートメント 3.3: コンピューティングワークロードのセキュリティコントロールを設計し、実装する。

対象知識:

- EC2 インスタンスのプロビジョニングとメンテナンス (パッチ適用、検査、スナップショットと AMI の作成、EC2 Image Builder の使用など)
- IAM インスタンスロールと IAM サービスロール
- コンピューティングワークロードの脆弱性をスキャンするサービス (Amazon Inspector、Amazon Elastic Container Registry [Amazon ECR] など)
- ホストベースのセキュリティ (ファイアウォール、強化など)

対象スキル:

- 強化された EC2 AMI の作成
- コンピューティングワークロードを認可するために、必要に応じてインスタンスロールとサービスロールの適用
- 既知の脆弱性について EC2 インスタンスとコンテナイメージのスキャニング
- EC2 インスタンスのフリートまたはコンテナイメージ全体にパッチの適用
- ホストベースのセキュリティメカニズム (ホストベースのファイアウォールなど) の有効化
- Amazon Inspector の調査結果を分析し、適切な対処法を決定
- コンピューティングワークロードへのシークレットと認証情報の安全な受け渡し

タスクステートメント 3.4: ネットワークセキュリティのトラブルシューティングを行う。

対象知識:

- 到達可能性の分析方法 (VPC Reachability Analyzer と Amazon Inspector の使用など)
- TCP/IP ネットワークの基本概念 (UDP と TCP の比較、ポート、OSI 参照モデル、OS のネットワークユーティリティなど)
- 関連するログソース (Route 53 ログ、AWS WAF ログ、VPC フローログなど) を読む方法

対象スキル:

- ネットワーク接続の問題を特定、解釈、優先順位付け (Amazon Inspector のネットワーク到達可能性の使用など)

- 望ましいネットワーク動作を実現するためのソリューションを決定
- ログソースを分析して問題を特定
- 問題分析のためのトラフィックサンプルのキャプチャ (トラフィックミラーリングの使用など)

第 4 分野: Identity and Access Management

タスクステートメント 4.1: AWS リソースの認証を設計、実装、トラブルシューティングする。

対象知識:

- アイデンティティを作成および管理する方法とサービス (フェデレーション、ID プロバイダー、AWS IAM Identity Center [AWS Single Sign-On]、Amazon Cognito など)
- 長期的および一時的な認証情報管理メカニズム
- 認証の問題をトラブルシューティングする方法 (CloudTrail、IAM アクセスアドバイザー、IAM ポリシーシミュレーターの使用など)

対象スキル:

- 要件に基づいて、認証システムでアイデンティティを確立
- 多要素認証 (MFA) のセットアップ
- AWS Security Token Service (AWS STS) を使用して一時的な認証情報を発行する場合を決定

タスクステートメント 4.2: AWS リソースの認可を設計、実装、トラブルシューティングする。

対象知識:

- さまざまな IAM ポリシー (マネージドポリシー、インラインポリシー、アイデンティティベースのポリシー、リソースベースのポリシー、セッション制御ポリシーなど)
- ポリシーの構成要素と影響 (プリンシパル、アクション、リソース、条件など)
- 認可の問題をトラブルシューティングする方法 (CloudTrail、IAM アクセスアドバイザー、IAM ポリシーシミュレーターの使用など)

対象スキル:

- 属性ベースのアクセス制御 (ABAC) 戦略とロールベースのアクセス制御 (RBAC) 戦略を構築
- 特定の要件とワークロードに対する IAM ポリシータイプの評価
- IAM ポリシーが環境とワークロードに及ぼす影響の解釈
- 環境全体に最小権限の原則を適用
- 適切な職務分掌の実施
- アクセスエラーまたは認可エラーを分析し、原因または影響を特定
- リソース、サービス、またはエンティティに付与された意図しないアクセス許可、認可、または権限を調査

第 5 分野: データ保護

タスクステートメント 5.1: 転送中のデータに機密性と整合性を提供するコントロールを設計し、実装する。

対象知識:

- TLS の概念
- VPN の概念 (IPsec など)
- 安全なリモートアクセス方法 (SSH、Systems Manager Session Manager 経由の RDP など)
- Systems Manager Session Manager の概念
- TLS 証明書がさまざまなネットワークサービスやリソース (CloudFront、ロードバランサーなど) で機能するしくみ

対象スキル:

- AWS とオンプレミスネットワーク間の安全な接続の設計 (Direct Connect や VPN ゲートウェイの使用など)
- リソース (Amazon RDS、Amazon Redshift、CloudFront、Amazon S3、Amazon DynamoDB、ロードバランサー、Amazon Elastic File System [Amazon EFS]、Amazon API Gateway など) への接続時に暗号化を要求するメカニズムの設計
- AWS API コールに TLS を要求 (Amazon S3 を使用する場合など)
- 安全な接続を介してトラフィックを転送するメカニズムの設計 (Systems Manager と EC2 Instance Connect の使用など)

- プライベート VIF とパブリック VIF を使用したクロスリージョンネットワークの設計

タスクステートメント 5.2: 保管中のデータに機密性と整合性を提供するコントロールを設計し、実装する。

対象知識:

- 暗号化技術の選択 (クライアント側、サーバー側、対称、非対称など)
- 整合性チェックの手法 (ハッシュアルゴリズム、デジタル署名など)
- リソースポリシー (DynamoDB、Amazon S3、AWS Key Management Service [AWS KMS] など)
- IAM ロールとポリシー

対象スキル:

- 認可されたユーザーにアクセスを制限するリソースポリシーの設計 (S3 バケットポリシー、DynamoDB ポリシーなど)
- 不正なパブリックアクセスを防止するメカニズムの設計 (S3 パブリックアクセスブロック、パブリックスナップショットおよびパブリック AMI の防止など)
- 保管中のデータの暗号化を有効にするサービスの設定 (Amazon S3、Amazon RDS、DynamoDB、Amazon Simple Queue Service [Amazon SQS]、Amazon EBS、Amazon EFS など)
- 変更を防止してデータの整合性を保護するメカニズムの設計 (S3 オブジェクトロック、KMS キーポリシー、S3 Glacier ボールトロック、AWS Backup ボールトロックの使用など)
- リレーショナルデータベース (Amazon RDS、RDS カスタム、EC2 インスタンス上のデータベースなど) に AWS CloudHSM を使用した保管時の暗号化の設計
- ビジネス要件に基づいた暗号化技術の選択

タスクステートメント 5.3: 保存中のデータのライフサイクルを管理するためのコントロールを設計し、実装する。

対象知識:

- ライフサイクルポリシー
- データ保持基準

対象スキル:

- 必要な保持期間にわたってデータを保持するための S3 ライフサイクルメカニズムの設計 (S3 オブジェクトロック、S3 Glacier ボールトロック、S3 ライフサイクルポリシーなど)
- AWS のサービスとリソースの自動ライフサイクル管理の設計 (Amazon S3、EBS ボリュームスナップショット、RDS ボリュームスナップショット、AMI、コンテナイメージ、CloudWatch ロググループ、Amazon Data Lifecycle Manager など)
- AWS のサービス全体での AWS Backup のスケジュールと保持の設定

タスクステートメント 5.4: 認証情報、シークレット、暗号化キーマテリアルを保護するためのコントロールを設計し、実装する。

対象知識:

- Secrets Manager
- Systems Manager Parameter Store
- 対称キーと非対称キーの使用と管理 (AWS KMS など)

対象スキル:

- ワークロードのシークレットの管理とローテーションの設計 (データベースアクセス認証情報、API キー、IAM アクセスキー、AWS KMS カスタマー管理キーなど)
- 認可されたユーザーにキーの使用を限定する KMS キーポリシーの設計
- 顧客提供のキーマテリアルをインポートおよび削除するメカニズムの確立

第 6 分野: 管理とセキュリティガバナンス

タスクステートメント 6.1: AWS アカウントを一元的にデプロイして管理する戦略を策定する。

対象知識:

- マルチアカウント戦略
- 管理を委任できるマネージドサービス
- ポリシー定義のガードレール
- ルートアカウントのベストプラクティス
- クロスアカウントロール

対象スキル:

- AWS Organizations のデプロイ、設定
- AWS Control Tower をデプロイするタイミングと方法の決定 (デプロイを成功させるためにどのサービスを無効化する必要があるかなど)
- ポリシーを適用するための技術的ソリューションとしての SCP の実装 (ルートアカウントの使用制限、AWS Control Tower でのコントロールの実装など)
- セキュリティサービスを一元管理し、調査結果を集計 (委任管理や AWS Config アグリゲーターの使用など)
- AWS アカウントのルートユーザーの認証情報のセキュリティでの保護

タスクステートメント 6.2: クラウドリソースのための安全で一貫したデプロイ戦略を実装する。

対象知識:

- Infrastructure as Code (IaC) を使ったデプロイのベストプラクティス (AWS CloudFormation テンプレートのハードニングやドリフト検出など)
- タグ付けのベストプラクティス
- AWS のサービスの一元管理、デプロイ、バージョン管理
- AWS インフラストラクチャの可視性と制御

対象スキル:

- CloudFormation を使用したクラウドリソースの一貫性のある安全なデプロイ
- マルチアカウントタグ付け戦略の実装、実施
- 承認された AWS のサービスのポートフォリオの設定、デプロイ (AWS Service Catalog の使用など)
- AWS リソースをさまざまなグループに整理し管理
- ポリシーを適用するために Firewall Manager をデプロイ
- AWS アカウント間でリソースを安全に共有 (AWS Resource Access Manager [AWS RAM] の使用など)

タスクステートメント 6.3: AWS リソースのコンプライアンスを評価する。

対象知識:

- AWS のサービスを使用したデータ分類
- AWS リソースの設定を評価、監査、審査する方法 (AWS Config の使用など)

対象スキル:

- Macie を使用した機密データの特定
- 非準拠の AWS リソースを検出するための AWS Config ルールの作成
- Security Hub と AWS Audit Manager を使用して証拠を収集、整理

タスクステートメント 6.4: アーキテクチャレビューとコスト分析を通じて
セキュリティギャップを特定する。

対象知識:

- 異常特定にかかる AWS のコストと使用量
- 攻撃対象領域を減らすための戦略
- AWS Well-Architected フレームワーク

対象スキル:

- リソース使用率と傾向を基に異常を特定
- AWS のサービスとツール (AWS Trusted Advisor、AWS Cost Explorer など) を活用して使用されていないリソースを特定
- AWS Well-Architected Tool を使用してセキュリティギャップを特定

付録

試験に出題される可能性のあるテクノロジーと概念

以下は、試験に出題される可能性のあるテクノロジーと概念のリストです。このリストはすべてを網羅しているわけではなく、また、変更される場合があります。このリストにおける項目の掲載順序や配置は、その項目の相対的な重みや試験における重要性を示すものではありません。

- AWS CLI
- AWS SDK
- AWS マネジメントコンソール
- セキュアなリモートアクセス
- 証明書管理
- Infrastructure as code (IaC)

範囲内の AWS のサービスと機能

注意: セキュリティはすべての AWS のサービスに影響します。サービス全体は範囲外であるため、多くのサービスはこのリストに表示されませんが、サービスのセキュリティの側面は範囲内です。例えば、この試験の受験者は、S3 バケットのレプリケーションをセットアップする手順については問われません。ただし、受験者は S3 バケットポリシーの設定について問われる場合があります。

以下に、試験範囲の AWS のサービスと機能のリストを示します。このリストはすべてを網羅しているわけではなく、また、変更される場合があります。各 AWS のサービスは、サービスの主な機能に応じたカテゴリに分けられています。

マネジメントとガバナンス:

- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- AWS Organizations
- AWS Systems Manager
- AWS Trusted Advisor

ネットワークとコンテンツ配信:

- Amazon VPC
  - Network Access Analyzer
  - ネットワーク ACL
  - セキュリティグループ
  - VPC エンドポイント

セキュリティ、アイデンティティ、コンプライアンス:

- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Amazon GuardDuty
- AWS IAM Identity Center (AWS Single Sign-On)
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Security Hub
- AWS Shield
- AWS WAF

範囲外の AWS のサービスと機能

以下に、試験対象外の AWS のサービスと機能のリストを示します。このリストはすべてを網羅しているわけではなく、また、変更される場合があります。試験の対象となる職務内容に完全に関係のない AWS のサービスは、このリストから除外されています。

ブロックチェーン:

- Amazon Managed Blockchain
- Amazon Quantum Ledger Database (Amazon QLDB)

ビジネスアプリケーション:

- Alexa for Business
- Amazon Chime
- Amazon Chime SDK
- Amazon Connect
- Amazon Honeycode
- Amazon Pinpoint
- AWS Supply Chain
- AWS Wickr
- Amazon WorkDocs

エンドユーザーコンピューティング:

- Amazon AppStream 2.0

メディアサービス:

- Amazon Elastic Transcoder
- AWS Elemental Appliances and Software
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Interactive Video Service (Amazon IVS)
- Amazon Kinesis Video Streams
- Amazon Nimble Studio

移行と転送:

- AWS Application Discovery Service
- AWS Application Migration Service
- AWS Database Migration Service (AWS DMS)
- Migration Evaluator
- AWS Migration Hub
- AWS Transfer Family

量子テクノロジー:

- Amazon Braket

ロボティクス:

- AWS RoboMaker

人工衛星

- AWS Ground Station

アンケート

この試験ガイドはどの程度役に立ちましたか？ アンケートに答えてお知らせください。