AWS Certified Security - Specialty (SCS-C03) 試験ガイド

はじめに

AWS Certified Security - Specialty (SCS-C03) 試験は、クラウドソリューションのセキュリティを担う立場にある方を対象としています。この試験では、受験者が AWS の製品とサービスを保護するための知識を効果的に示せるかどうかが検証されます。

また、以下のタスクについての受験者の能力も検証します。

- 専門的なデータ分類と AWS のデータ保護メカニズムを適用する。
- データ暗号化方法と AWS 暗号化メカニズムを実装する。
- セキュアなインターネットプロトコルを遵守するための AWS の仕組みを実装する。
- AWS のセキュリティサービスと機能を使用して、セキュアな本番環境を確保する。
- 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、デプロイの複雑さのトレードオフを考慮した意思決定を行う。
- セキュリティオペレーションおよびリスクを理解する。

受験対象者について

受験対象者は、クラウドソリューションの保護について 3〜5 年相当の経験を有している必要があります。

推奨される AWS の知識

受験対象者は、以下の AWS に関する知識を有している必要があります。

- AWS の責任共有モデルとその適用
- アイデンティティの大規模な管理
- マルチアカウントガバナンス
- ソフトウェアサプライチェーンのリスク管理
- セキュリティインシデント防止および対応戦略
- クラウド内の脆弱性管理
- レイヤー 3〜7 のファイアウォールルールの大規模な開発
- インシデントの根本原因分析

- 監査対応の経験
- ロギング戦略とモニタリング戦略
- データ暗号化手法 (保管中のデータと転送中のデータの両方)
- バックアップ戦略を含むディザスタリカバリ管理

受験対象者の試験の範囲外となるジョブタスク

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、本試験の対象外です。

- 暗号化アルゴリズムの設計
- パケットレベルでのトラフィック分析
- クラウドデプロイ全体の設計
- エンドユーザーのコンピューティングリソースの管理
- 機械学習モデルのトレーニング

試験対象の AWS のサービスと機能のリスト、および試験対象外の AWS のサービスと機能のリストについては、「付録 A」を参照してください。

試験内容

解答タイプ

試験には、次の出題形式が 1 つ以上含まれています。

- **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。
- **並べ替え:** 指定されたタスクを完了することを目的とした 3〜5 つの答えのリストが提示される。設問に対する点数を得るには、正解を選択し、正しい順序に並べる必要がある。
- **内容一致:** 3〜7 つのプロンプトのリストと一致する答えのリストが提示される。設問に対する点数を得るには、すべてのペアを正しく一致させる必要がある。

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 [1]。

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パフォーマンス情報を収集し、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-C03) 試験は、合否判定方式の試験です。試験は、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き、AWS の専門家が定めた最低基準に照らして採点されます。

試験の結果は、100～1,000 の換算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換算スコアが使用されます。

スコアレポートには、各セクションのパフォーマンス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、受験者の得意分野と不得意分野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。

---

[1]試験のベータ版は該当しません。ベータ試験全般の詳細については、AWS 認定のウェブサイトをご覧ください。

試験内容の概要

この試験ガイドには、試験に設定された重み、コンテンツ分野、タスク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。

この試験のコンテンツ分野と重み設定は、以下のとおりです。

- コンテンツ分野 1: 検出 (採点対象コンテンツの 16%)
- コンテンツ分野 2: インシデント対応 (採点対象コンテンツの 14%)
- コンテンツ分野 3: 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 18%)
- コンテンツ分野 4: Identity and Access Management (採点対象コンテンツの 20%)
- コンテンツ分野 5: データ保護 (採点対象コンテンツの 18%)
- コンテンツ分野 6: セキュリティ基盤とガバナンス (採点対象コンテンツの 14%)

コンテンツ分野 1: 検出

タスク 1.1: AWS アカウントまたは組織向けのモニタリングおよびアラートソリューションを設計し、実装する。

スキル 1.1.1: ワークロードを分析してモニタリング要件を判断する。
スキル 1.1.2: ワークロードモニタリング戦略を設計して実装する (リソースのヘルスチェックの設定など)。
スキル 1.1.3: セキュリティとモニタリングイベントを集約する。
スキル 1.1.4: メトリクス、アラート、ダッシュボードを作成し、異常なデータやイベントを検出する (Amazon GuardDuty、Amazon Security Lake、AWS Security Hub、Amazon Macie など)。
スキル 1.1.5: オートメーションを作成して管理し、定期的な評価と調査を行う (AWS Config コンフォーマンスパック、Security Hub、AWS Systems Manager State Manager のデプロイなど)。

タスク 1.2: ロギングソリューションを設計し、実装する。

スキル 1.2.1: 要件に基づいてログの取り込みとストレージのソースを特定する。
スキル 1.2.2: AWS のサービスとアプリケーションのロギングを設定する (組織の AWS CloudTrail 証跡の設定、専用の Amazon CloudWatch ロギングアカウントの作成、Amazon CloudWatch Logs エージェントの設定など)。

スキル 1.2.3: ログストレージとログデータレイク (Security Lake など) を実装し、サードパーティーのセキュリティツールと統合する。
スキル 1.2.4: AWS のサービスを使用してログを分析する (CloudWatch Logs Insights、Amazon Athena、Security Hub の検出結果など)。
スキル 1.2.5: AWS のサービスを使用してログの正規化、解析、関連付けを行う (Amazon OpenSearch Service、AWS Lambda、Amazon Managed Grafana など)。
スキル 1.2.6: ネットワーク設計、脅威、攻撃に基づいて適切なログソースを判断し、設定する (VPC フローログ、Transit Gateway フローログ、Amazon Route 53 Resolver ログなど)。

タスク 1.3: セキュリティモニタリング、ロギング、アラートソリューションをトラブルシューティングする。

スキル 1.3.1: リソースの機能、アクセス許可、設定を分析する (Lambda 関数ロギング、Amazon API Gateway ロギング、ヘルスチェック、Amazon CloudFront ロギングなど)。
スキル 1.3.2: リソースの設定ミスを修正する (CloudWatch Agent 設定のトラブルシューティング、不足しているログのトラブルシューティングなど)。

コンテンツ分野 2: インシデント対応

タスク 2.1: インシデント対応計画を策定し、テストする。

スキル 2.1.1: セキュリティインシデントに対応するための対応計画とランブックを策定し、実装する (Systems Manager OpsCenter、Amazon SageMaker AI ノートブックなど)。
スキル 2.1.2: AWS のサービスと機能を使用し、インシデントに備えてサービスを設定する (アクセスのプロビジョニング、セキュリティツールのデプロイ、影響範囲の最小化、AWS Shield Advanced 保護の設定など)。
スキル 2.1.3: インシデント対応計画の有効性のテストと検証のための手順を推奨する (AWS Fault Injection Service、AWS Resilience Hub など)。
スキル 2.1.4: AWS のサービスを使用してインシデントを自動的に修復する (Systems Manager、Automated Forensics Orchestrator for Amazon EC2、AWS Step Functions、Amazon Application Recovery Controller、Lambda 関数など)。

タスク 2.2: セキュリティイベントに対応する。

スキル 2.2.1: 関連するシステムログとアプリケーションログをフォレンジックアーティファクトとしてキャプチャし、保存する。

スキル 2.2.2: アプリケーションと AWS サービス全体のセキュリティイベントのログを検索し、関連付ける。
スキル 2.2.3: AWS のセキュリティサービスの検出結果を検証し、イベントの範囲と影響を評価する。
スキル 2.2.4: 脅威を封じ込めて根絶することにより、影響を受けたリソースに対応し、リソースを復旧する (ネットワーク封じ込めコントロールの実装、バックアップの復元など)。
スキル 2.2.5: 根本原因分析を行う方法を説明する (Amazon Detective など)。

コンテンツ分野 3: インフラストラクチャのセキュリティ

タスク 3.1: ネットワークエッジサービスのセキュリティコントロールを設計、実装、トラブルシューティングする。

スキル 3.1.1: 予想される脅威と攻撃に基づいてエッジセキュリティ戦略を定義し、選択する。
スキル 3.1.2: 適切なネットワークエッジ保護を実装する [CloudFront ヘッダー、AWS WAF、AWS IoT ポリシー、OWASP Top 10 の脅威からの保護、Amazon S3 クロスオリジンリソース共有 (CORS)、Shield Advanced など]。
スキル 3.1.3: 要件に基づいて AWS エッジコントロールとルールを設計し、実装する (地理、位置情報、レート制限、クライアントフィンガープリントなど)。
スキル 3.1.4: AWS エッジサービスとサードパーティーサービスとの統合を設定する [Open Cybersecurity Schema Framework (OCSF) 形式のデータの取り込み、サードパーティーの WAF ルールの使用など]。

タスク 3.2: 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、実装、トラブルシューティングする。

スキル 3.2.1: コンピューティングワークロードを保護し、セキュリティコントロールを組み込むために、強化された Amazon EC2 AMI とコンテナイメージを設計し、実装する (Systems Manager、EC2 Image Builder など)。
スキル 3.2.2: コンピューティングワークロードを認可するために、インスタンスプロファイル、サービスロール、実行ロールを適切に適用する。
スキル 3.2.3: コンピューティングリソースに既知の脆弱性がないかスキャンする (Amazon Inspector を使用したコンテナイメージと Lambda 関数のスキャン、GuardDuty を使用したコンピューティングランタイムのモニタリングなど)。

スキル 3.2.4: 更新プロセスを自動化し、継続的な検証を統合することで、コンピューティングリソース全体にパッチをデプロイし、セキュアな準拠環境を維持する (Systems Manager Patch Manager、Amazon Inspector など)。
スキル 3.2.5: コンピューティングリソースへのセキュアな管理アクセスを設定する (Systems Manager Session Manager、EC2 Instance Connect など)。
スキル 3.2.6: パイプライン内の脆弱性を検出して修正するためのセキュリティツールを設定する (Amazon Q Developer、Amazon CodeGuru Security など)。
スキル 3.2.7: 生成 AI アプリケーションの保護とガードレールを実装する (GenAI OWASP Top 10 for LLM Applications 保護の適用など)。

タスク 3.3: ネットワークセキュリティコントロールを設計し、トラブルシューティングする。

スキル 3.3.1: 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ための適切なネットワークコントロールを設計し、トラブルシューティングする (セキュリティグループ、ネットワーク ACL、AWS Network Firewall など)。
スキル 3.3.2: ハイブリッドネットワークとマルチクラウドネットワークの間のセキュアな接続を設計する [AWS Site-to-Site VPN、AWS Direct Connect、MAC セキュリティ (MACsec) など]。
スキル 3.3.3: ハイブリッド環境と AWS の間の通信に関するセキュリティワークロード要件を判断し、設定する (AWS Verified Access の使用など)。
スキル 3.3.4: セキュリティ要件に基づいてネットワークセグメンテーションを設計する (north-south と east-west のトラフィック保護、分離されたサブネットなど)。
スキル 3.3.5: 不必要なネットワークアクセスを特定する (AWS Verified Access、Network Access Analyzer、Amazon Inspector のネットワーク到達可能性の検出結果など)。

コンテンツ分野 4: Identity and Access Management

タスク 4.1: 認証戦略を設計、実装、トラブルシューティングする。

スキル 4.1.1: 人間、アプリケーション、システムの認証のためのアイデンティティソリューションを設計し、確立する [AWS IAM アイデンティティセンター、Amazon Cognito、多要素認証 (MFA)、ID プロバイダー (IdP) 統合など]。
スキル 4.1.2: 一時的な認証情報を発行するためのメカニズムを設定する [AWS Security Token Service (AWS STS)、Amazon S3 署名付き URL など]。

スキル 4.1.3: 認証に関する問題をトラブルシューティングする (CloudTrail、Amazon Cognito、IAM アイデンティティセンターのアクセス許可セット、AWS Directory Service など)。

タスク 4.2: 認可戦略を設計、実装、トラブルシューティングする。

スキル 4.2.1: 人間、アプリケーション、システムのアクセスのための認可コントロールを設計し、評価する (Amazon Verified Permissions、IAM パス、IAM Roles Anywhere、クロスアカウントアクセスのためのリソースポリシー、IAM ロール信頼ポリシーなど)。
スキル 4.2.2: 属性ベースのアクセス制御 (ABAC) 戦略およびロールベースのアクセス制御 (RBAC) 戦略を設計する (タグまたは属性に基づいたリソースアクセスの設定など)。
スキル 4.2.3: 最小権限の原則に従って IAM ポリシーを設計、解釈、実装する (アクセス許可境界、セッションポリシーなど)。
スキル 4.2.4: 認可障害を分析して原因または影響を判断する (IAM Policy Simulator、IAM Access Analyzer など)。
スキル 4.2.5: 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、または権限を調査し、修正する (IAM Access Analyzer など)。

コンテンツ分野 5: データ保護

タスク 5.1: 転送中のデータのコントロールを設計し、実装する。

スキル 5.1.1: リソースへの接続時に暗号化を義務付けるメカニズムを設計し、設定する [Elastic Load Balancing (ELB) セキュリティポリシーの設定、TLS 設定の強制適用など]。
スキル 5.1.2: リソースへのセキュアなプライベートアクセスのためのメカニズムを設計し、設定する (AWS PrivateLink、VPC エンドポイント、AWS Client VPN、AWS Verified Access など)。
スキル 5.1.3: 転送中のリソース間暗号化を設計し、設定する [Amazon EMR、Amazon Elastic Kubernetes Service (Amazon EKS)、SageMaker AI、Nitro 暗号化のためのノード間暗号化設定など]。

タスク 5.2: 保管中のデータのコントロールを設計し、実装する。

スキル 5.2.1: 特定の要件に基づいて、保管中のデータ暗号化を設計、実装、設定する [AWS CloudHSM や AWS Key Management Service (AWS KMS) などの適切な暗号化キーサービスの選択、クライアント側の暗号化やサーバー側の暗号化などの適切な暗号化タイプの選択など]。

スキル 5.2.2: データの整合性を確保するためのメカニズムを設計し、設定する (S3 Object Lock、S3 Glacier Vault Lock、バージョニング、デジタルコード署名、ファイル検証など)。
スキル 5.2.3: データの自動ライフサイクル管理および保持ソリューションを設計する [S3 ライフサイクルポリシー、S3 Object Lock、Amazon Elastic File System (Amazon EFS) ライフサイクルポリシー、Amazon FSx for Lustre バックアップポリシーなど]。
スキル 5.2.4: セキュアなデータレプリケーションおよびバックアップソリューションを設計し、設定する (Amazon Data Lifecycle Manager、AWS Backup、ランサムウェア対策、AWS DataSync など)。

タスク 5.3: 機密データ、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。

スキル 5.3.1: 認証情報とシークレットの管理とローテーションを設計する (AWS Secrets Manager など)。
スキル 5.3.2: インポートされたキーマテリアルを管理し、使用する (インポートされたキーマテリアルの管理とローテーション、外部キーストアの管理と設定など)。
スキル 5.3.3: インポートされたキーマテリアルと AWS によって生成されたキーマテリアルの違いを説明する。
スキル 5.3.4: 機密データをマスクする [CloudWatch Logs データ保護ポリシー、Amazon Simple Notification Service (Amazon SNS) メッセージデータ保護など]。
スキル 5.3.5: 単一の AWS リージョンまたは複数のリージョンにわたる暗号化キーと証明書を作成し、管理する (AWS KMS カスタマーマネージド AWS KMS キー、AWS Private Certificate Authority など)。

コンテンツ分野 6: セキュリティ基盤とガバナンス

タスク 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。

スキル 6.1.1: AWS Organizations を使用して組織をデプロイし、設定する。
スキル 6.1.2: AWS Control Tower を新規および既存の環境に実装して管理し、オプションのカスタムコントロールをデプロイする。
スキル 6.1.3: アクセス許可を管理するための組織ポリシーを実装する (SCP、RCP、AI サービスオプトアウトポリシー、宣言型ポリシーなど)。
スキル 6.1.4: セキュリティサービスを一元管理する (委任管理者アカウントなど)。

スキル 6.1.5: AWS アカウントのルートユーザー認証情報を管理する (メンバーアカウントのルートアクセスの一元化、MFA の管理、ブレークグラス手順の設計など)。

タスク 6.2: クラウドリソースのためのセキュアで一貫したデプロイ戦略を実装する。

スキル 6.2.1: Infrastructure as Code を使用して、クラウドリソースをアカウント間で一貫したセキュアな方法でデプロイする (CloudFormation スタックセット、サードパーティーの IaC ツール、CloudFormation Guard、cfn-lint など)。
スキル 6.2.2: タグを使用して、AWS リソースを管理用のグループに整理する (部門、コストセンター、環境別のグループ化など)。
スキル 6.2.3: 中央のソースからポリシーと設定をデプロイし、強制適用する (AWS Firewall Manager など)。
スキル 6.2.4: AWS アカウント間でリソースをセキュアな方法で共有する [AWS Service Catalog、AWS Resource Access Manager (AWS RAM) など]。

タスク 6.3: AWS リソースのコンプライアンスを評価する。

スキル 6.3.1: 準拠していない AWS リソースを検出して修正し、通知を送信するためのルールを作成または有効にする (AWS Config を使用したアラートの集約と非準拠のリソースの修正、Security Hub など)。
スキル 6.3.2: AWS 監査サービスを使用してエビデンスを収集し、整理する (AWS Audit Manager、AWS Artifact など)。
スキル 6.3.3: AWS のサービスを使用して、アーキテクチャが AWS セキュリティのベストプラクティスに準拠しているかどうかを評価する (AWS Well-Architected フレームワークツールなど)。

付録 A

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)

試験対象の AWS のサービスと機能

注: セキュリティはすべての AWS のサービスに影響します。サービス全体は試験対象外であるため、多くのサービスはこのリストに表示されていませんが、サービスのセキュリティの側面は試験対象です。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、試験対象の 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。

分析:

- Amazon Athena
- Amazon OpenSearch Service

アプリケーション統合:

- Amazon Simple Notification Service (Amazon SNS)
- AWS Step Functions

コンピューティング:

- Amazon API Gateway
- Amazon EC2 (EC2 Image Builder、EC2 Instance Connect を含む)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EMR
- AWS Lambda
- Amazon Data Lifecycle Manager

デベロッパーツール

- AWS Fault Injection Service

IoT

- AWS IoT Core

機械学習:

- Amazon Bedrock
- Amazon CodeGuru Security
- Amazon Q Business
- Amazon Q Developer
- Amazon SageMaker AI

マネジメントとガバナンス:

- AWS CloudFormation
- AWS CloudTrail
- AWS CloudTrail Lake
- Amazon CloudWatch
- AWS Config
- AWS Control Tower
- Amazon Managed Grafana
- AWS Organizations
- AWS Resilience Hub
- AWS Resource Access Manager (AWS RAM)
- AWS Service Catalog
- AWS Systems Manager

- AWS Trusted Advisor
- AWS User Notifications
- AWS Well-Architected Tool

ネットワークとコンテンツ配信:

- Amazon Application Recovery Controller
- 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
    - AWS Site-to-Site VPN
    - フローログ
    - VPC エンドポイント
    - AWS Verified Access
- AWS Client VPN
- Amazon CloudFront
- Amazon Verified Permissions
- Amazon Route 53 (Route 53 Resolver DNS Firewall を含む)
- AWS Direct Connect
- Elastic Load Balancing (ELB)
- Network Access Analyzer
- AWS Transit Gateway

セキュリティ、アイデンティティ、コンプライアンス:

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- AWS Firewall Manager
- Automated Forensics Orchestrator for Amazon EC2
- Amazon GuardDuty

- AWS IAM アイデンティティセンター
- AWS Identity and Access Management (AWS IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Private Certificate Authority
- AWS Secrets Manager
- AWS Security Hub
- Amazon Security Lake
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS Shield Advanced
- AWS WAF

ストレージとデータ管理:

- Amazon S3
- AWS Backup
- AWS DataSync
- Amazon Elastic File System (Amazon EFS) (EFS ライフサイクルポリシーを含む)
- Amazon FSx for Lustre

試験対象外の 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まったく関係のない AWS のサービスは、このリストから除外されています。

アプリケーション統合:

- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)

セキュリティ、アイデンティティ、コンプライアンス:

- AWS Payment Cryptography

付録 B: SCS-C02 と SCS-C03 の比較

対照比較

SCS-C02 試験 (2025 年 12 月 1 日まで実施) と SCS-C03 試験 (2025 年 12 月 2 日 から実施) の分野と各分野の採点対象設問の割合は、以下の表のとおりです。

SCS-C02 の分野	SCS-C03 の分野
第 1 分野: 脅威検出とインシデント対応 (14%)	コンテンツ分野 1: 検出 (採点対象コンテンツの 16%)
第 2 分野: セキュリティロギングとモニタリング (18%)	コンテンツ分野 2: インシデント対応 (14%)
第 3 分野: インフラストラクチャのセキュリティ (20%)	コンテンツ分野 3: インフラストラクチャのセキュリティ (18%)
第 4 分野: Identity and Access Management (16%)	コンテンツ分野 4: Identity and Access Management (20%)
第 5 分野: データ保護 (18%)	コンテンツ分野 5: データ保護 (18%)
第 6 分野: 管理とセキュリティガバナンス (14%)	コンテンツ分野 6: セキュリティ基盤とガバナンス (14%)

SCS-C03 でのコンテンツの追加

タスク 2.2.3 に、以下のコンテンツが追加されました。

- 2.2.3 AWS のセキュリティサービスの検出結果を検証し、イベントの範囲と影響を評価する。

タスク 3.1.4 に、以下のコンテンツが追加されました。

- 3.1.4 AWS エッジサービスとサードパーティーサービスとの統合を設定する [Open Cybersecurity Schema Framework (OCSF) 形式のデータの取り込み、サードパーティーの WAF ルールの使用など]。

タスク 3.2.7 に、以下のコンテンツが追加されました。

- 3.2.7 生成 AI アプリケーションの保護とガードレールを実装する (GenAI OWASP Top 10 for LLM Applications 保護の適用など)。

タスク 5.1.3 に、以下のコンテンツが追加されました。

- 5.1.3 転送中のリソース間暗号化を設計し、設定する [Amazon EMR、Amazon Elastic Kubernetes Service (Amazon EKS)、SageMaker AI、Nitro 暗号化のためのノード間暗号化設定など]。

タスク 5.3.3 に、以下のコンテンツが追加されました。

- 5.3.3 インポートされたキーマテリアルと AWS によって生成されたキーマテリアルの違いを説明する。

タスク 5.3.4 に、以下のコンテンツが追加されました。

- 5.3.4 機密データをマスクする [CloudWatch Logs データ保護ポリシー、Amazon Simple Notification Service (Amazon SNS) メッセージデータ保護など]。

タスク 5.3.5 に、以下のコンテンツが追加されました。

- 5.3.5 単一の AWS リージョンまたは複数のリージョンにわたる暗号化キーと証明書を作成し、管理する (AWS KMS カスタマーマネージド AWS KMS キー、AWS Private Certificate Authority など)。

SCS-C03 でのコンテンツの削除

タスク 6.4 で、以下のコンテンツが削除されました。

- 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。

タスク 1.1 で、以下のコンテンツが削除されました。

- AWS Security Finding Format (ASFF)

タスク 1.3 で、以下のコンテンツが削除されました。

- AWS セキュリティインシデント対応ガイド

タスク 2.5 で、以下のコンテンツが削除されました。

- ログ形式とコンポーネント (CloudTrail ログなど)

タスク 3.3 で、以下のコンテンツが削除されました。

- 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)
- 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

タスク 3.4 で、以下のコンテンツが削除されました。

- 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]
- 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)

タスク 4.2 で、以下のコンテンツが削除されました。

- 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)

タスク 5.1 で、以下のコンテンツが削除されました。

- TLS の概念
- 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 5.2 で、以下のコンテンツが削除されました。

- S3 の静的ウェブホスティングを設定する。

SCS-C03 でのコンテンツの再分類

SCS-C02 から SCS-C03 への移行に伴い、以下の主要なコンテンツの再編成が行われました。

SCS-C02 の第 1 分野と第 2 分野が再構築されました。

- 「脅威の検出とインシデント対応」と「セキュリティロギングとモニタリング」は、以下のようになりました。
    - 第 1 分野: 検出
    - 第 2 分野: インシデント対応

第 6 分野は SCS-C03 で以下のように名称変更されました。

- 「管理とセキュリティガバナンス」から「セキュリティ基盤とガバナンス」へ

以下のタスクステートメントが再分類されました。

SCS-C02 タスクステートメント 1.1 は、SCS-C03 では以下のタスクにマップされています。

- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。
- 1.2 ロギングを設計し、実装する。
- 2.1 インシデント対応計画を策定し、テストする。
- 2.2 セキュリティイベントに対応する。

SCS-C02 タスクステートメント 1.2 は、SCS-C03 では以下のタスクにマップされています。

- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。
- 1.2 ロギングを設計し、実装する。

SCS-C02 タスクステートメント 1.3 は、SCS-C03 では以下のタスクにマップされています。

- 2.1 インシデント対応計画を策定し、テストする。
- 2.2 セキュリティイベントに対応する。

SCS-C02 タスクステートメント 2.1 は、SCS-C03 では以下のタスクにマップされています。

- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。

SCS-C02 タスクステートメント 2.2 は、SCS-C03 では以下のタスクにマップされています。

- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。
- 1.2 ロギングを設計し、実装する。
- 1.3 セキュリティモニタリング、ロギング、アラートをトラブルシューティングする。

SCS-C02 タスクステートメント 2.3 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。

SCS-C02 タスクステートメント 2.4 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。
- 1.3 セキュリティモニタリング、ロギング、アラートをトラブルシューティングする。

SCS-C02 タスクステートメント 2.5 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。

SCS-C02 タスクステートメント 3.1 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。
- 3.1 ネットワークエッジサービスのセキュリティコントロールを設計、実装、トラブルシューティングする。

SCS-C02 タスクステートメント 3.2 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。
- 3.3 ネットワークセキュリティコントロールを設計し、トラブルシューティングする。
- 5.1 転送中のデータのコントロールを設計し、実装する。
- 6.2 クラウドリソースのためのセキュアで一貫したデプロイ戦略を実装する。

SCS-C02 タスクステートメント 3.3 は、SCS-C03 では以下のタスクにマップされています。

- 3.2 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、実装、トラブルシューティングする。
- 5.3 機密データ、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。

SCS-C02 タスクステートメント 3.4 は、SCS-C03 では以下のタスクにマップされています。

- 1.2 ロギングを設計し、実装する。
- 3.3 ネットワークセキュリティコントロールを設計し、トラブルシューティングする。

SCS-C02 タスクステートメント 4.1 は、SCS-C03 では以下のタスクにマップされています。

- 4.1 認証戦略を設計、実装、トラブルシューティングする。

SCS-C02 タスクステートメント 4.2 は、SCS-C03 では以下のタスクにマップされています。

- 4.2 認可戦略を設計、実装、トラブルシューティングする。

SCS-C02 タスクステートメント 5.1 は、SCS-C03 では以下のタスクにマップされています。

- 3.2 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、実装、トラブルシューティングする。
- 3.3 ネットワークセキュリティコントロールを設計し、トラブルシューティングする。
- 5.1 転送中のデータのコントロールを設計し、実装する。

SCS-C02 タスクステートメント 5.2 は、SCS-C03 では以下のタスクにマップされています。

- 4.2 認可戦略を設計、実装、トラブルシューティングする。
- 5.2 保管中のデータのコントロールを設計し、実装する。

SCS-C02 タスクステートメント 5.3 は、SCS-C03 では以下のタスクにマップされています。

- 5.2 保管中のデータのコントロールを設計し、実装する。

SCS-C02 タスクステートメント 5.4 は、SCS-C03 では以下のタスクにマップされています。

- 5.2 保管中のデータのコントロールを設計し、実装する。
- 5.3 機密データ、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。

SCS-C02 タスクステートメント 6.1 は、SCS-C03 では以下のタスクにマップされています。

- 4.2 認可戦略を設計、実装、トラブルシューティングする。
- 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。

SCS-C02 タスクステートメント 6.2 は、SCS-C03 では以下のタスクにマップされています。

- 6.2 クラウドリソースのためのセキュアで一貫したデプロイ戦略を実装する。

SCS-C02 タスクステートメント 6.3 は、SCS-C03 では以下のタスクにマップされています。

- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。
- 5.2 保管中のデータのコントロールを設計し、実装する。
- 6.3 AWS リソースのコンプライアンスを評価する。

SCS-C02 タスクステートメント 6.4 は、SCS-C03 では以下のタスクにマップされています。

- 2.1 インシデント対応計画を策定し、テストする。
- 1.1 AWS アカウントまたは組織向けのモニタリングおよびアラートを設計し、実装する。
- 6.3 AWS リソースのコンプライアンスを評価する。

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？ アンケートへの回答にご協力ください。