AWS 認定セキュリティ専門知識

(SCS-C01) 試験ガイド

はじめに

「AWS 認定セキュリティ専門知識」は、セキュリティロールを遂行する人を対象としており、AWS プラットフォームのセキュリティ保護についての理解度を評価するものです。

この試験で評価する能力は次のとおりです。

- 専門的なデータの分類と AWS のデータ保護の仕組みに関する知識。
- データ暗号化の手法とそれを実現する AWS の仕組みに関する知識。
- セキュアなインターネットプロトコルとそれを実現する AWS の仕組みに関する知識。
- AWS のセキュリティサービスとセキュアな運用環境を実現するサービスの機能に関する実践的な知識。
- AWS のセキュリティに関するサービスおよび機能を使用した、運用環境における 2 年以上の経験を通じて得られたコンピテンシー。
- 一連のアプリケーション要件に応じて、コスト、セキュリティ、導入の複雑さのバランスを勘案した意思決定を行える能力。
- セキュリティの運用とリスクに関する知識。

試験の前提条件

この試験を受けるには、AWS 認定の基礎または役割ベース認定 (アソシエイトまたはプロフェッショナル) を取得している必要があります。

推奨される AWS の知識

- セキュリティソリューションの設計や実装に関する 5 年以上の IT セキュリティに関する経験。
- AWS のワークロードのセキュリティ保護に関する 2 年以上の実務経験。
- AWS のワークロードに関するセキュリティ制御。

試験準備

本試験の準備に役立つトレーニングコースと資料は次のとおりです。

AWS に関するトレーニング (aws.amazon.com/training)

- AWS Security Fundamentals: 自分のペースで進められる 3 時間のオンラインコース
- Advanced Architecting on AWS: インストラクター主導による、ライブまたは仮想クラスでの 3 日間のコース
- Security Operations on AWS: インストラクター主導による、ライブまたは仮想クラスでの 3 日間のコース
- AWS Digital Training: セキュリティに関するサービスおよびトピックに特化した、自分のペースで進められるデジタルコース

AWS に関するホワイトペーパー (aws.amazon.com/whitepapers) Kindle 版および PDF 版

- セキュリティおよびコンプライアンスに関するドキュメント
- コンプライアンス関連のリソース

試験内容

回答タイプ

試験の質問には以下の 2 種類があります。

- **択一選択問題:** 選択肢には 1 つの正解と 3 つの不正解 (誤答) があります。
- **複数選択問題:** 5 つ以上の選択肢の中に 2 つ以上の正解があります。

文章に最もよく当てはまるもの、または質問の回答となるものを 1 つ以上選択します。不正解の選択肢は、知識やスキルが不十分な受験者が間違えやすいもので構成されています。多くの場合、試験の目的に応じた出題分野に当てはまる、もっともらしい回答になっています。

回答しなかった場合は不正解とされるため、推測でも答える方が有利です。

採点対象外の内容

試験には、採点の対象にはならない項目が含まれる場合があります。これは統計的な情報を集めるために試験に組み込まれています。フォーム上でこれらの項目を区別することはできませんが、スコアに影響を与えることもありません。

試験の結果

「AWS 認定セキュリティ専門知識」 (SCS-C01) 試験の結果は、合格または不合格のいずれかになります。試験は、認定業界のベストプラクティスとガイドラインに従って、AWS プロフェッショナルにより設定された最低基準に達しているかどうかに応じて採点されます。

試験結果は 100～1000 点の範囲のスコアでレポートされます。最低合格スコアは 750 点です。スコアによって、試験での全体的な成績と合否がわかります。スケールドスコアモデルは、難易度にわずかな違いのある複数の試験形式のスコアを平均化するために使用されます。

スコアレポートには各セクションレベルでの成績の等級表が掲載されています。この情報は、試験成績に関する全体的なフィードバックを提供することを目的として設計されています。試験では補填形式のスコアモデルが使用されるため、個別のセクションごとに「合格」する必要はなく、試験全体で合格することのみが求められます。試験の各セクションには特定の重み付けがされているため、一部のセクションでは質問数が他のセクションよりも多くなっています。表には、長所と弱点を示す総合的な情報が含まれています。セクションレベルのフィードバックは慎重に解釈するようにしてください。

試験内容の概要

この試験ガイドには、比重、出題分野、および試験の目的のみが記載されています。試験の出題内容全体を記載しているわけではありません。出題分野と比重を以下の表に示します。

分野	試験における比重
分野 1: インシデント対応	12%
分野 2: ログと監視	20%
分野 3: インフラストラクチャのセキュリティ	26%
分野 4: ID およびアクセス管理	20%
分野 5: データ保護	22%
合計	**100%**

分野 1: インシデント対応

1.1 AWS の悪用に関する通知を受け取った場合の、セキュリティ侵害が疑われるインスタンスまたは漏洩が疑われるアクセスキーの診断。

1.2 インシデント対応計画に適切な AWS サービスが含まれていることの確認。

1.3 自動的なアラートの構成の確認、およびセキュリティ関連のインシデントや新たな問題に対する対応策の実施。

分野 2: ログと監視

2.1 セキュリティの監視およびアラートの設計と実装。

2.2 セキュリティの監視およびアラートのトラブルシューティングの実施。

2.3 ログ収集ソリューションの設計と実装。

2.4 ログ収集ソリューションのトラブルシューティングの実施。

分野 3: インフラストラクチャのセキュリティ

3.1 AWS のエッジセキュリティの設計。

3.2 セキュアなネットワークインフラストラクチャの設計と実装。

3.3 セキュアなネットワークインフラストラクチャのトラブルシューティングの実施。

3.4 ホストベースのセキュリティの設計と実装。

分野 4: ID およびアクセス管理

4.1 AWS リソースへのアクセスを実現する拡張性の高い認証および権限付与のシステムの設計と実装。

4.2 AWS リソースへのアクセスを実現する拡張性の高い認証および権限付与のシステムのトラブルシューティングの実施。

分野 5: データ保護

5.1 キーの管理および使用に関する設計と実装。

5.2 キーの管理に関するトラブルシューティングの実施。

5.3 保存時および転送中のデータに適用するデータ暗号化ソリューションの設計と実装。