CompTIA CySA+取得のプロフェッショナルは、自信をもって業務を遂行します
CompTIA CySA+ CS0-003 とCS0-002 出題範囲の比較

セキュリティアリストに求められる必要なスキルは、この数年、大きな変化があります。
CompTIA CySA+（CompTIA Cybersecurity Analyst+）の改訂試験では、組織が脅威に対処するため、適切なモニタリングを行い、リスク管理ができるようにスキルセットが更新されています。
具体的には、セキュリティオペレーション、脆弱性管理、インシデントレスポンスと管理、報告とコミュニケーションの分野から出題されるスキルを評価します。
CompTIA CySA+を取得することで、セキュリティアナリスト、セキュリティオペレーションセンター（SOC）アナリスト、インシデントレスポンスアナリスト、脆弱性管理アナリスト、セキュリティエンジニア、脅威ハンターなどの職務においてスキルを発揮することを可能とします。

また、改訂試験の更新ポイントとして、自動化されたインシデントレスポンス、脅威インテリジェンス、クラウドベースのツール、通信プロセスなど最新のセキュリティ分析における手法、ツールが反映されています。
CompTIA CySA+を取得することで、以下のようなスキルを習得することが可能です。

- 悪意のあるアクティビティの兆候を検出、分析する
- 脅威ハンディングと脅威インテリジェンスの概念を理解する
- 適切な手法とツールを使用して管理を行い、優先順位をつけながら攻撃と脆弱性に対応する
- インシデントレスポンスプロセスの実行
- 脆弱性管理とインシデントレスポンスに関連するレポートとコミュニケーションの概念を理解する

CompTIA CySA+は、ISO17024の要件に適合しており、米国国防総省による指令8570.01-Mの資格要件として承認されています。また、連邦情報セキュリティマネジメント法（FISMA）に基づく、政府規制に準拠しています。

出題範囲の比較

下記の表は、CompTIA CySA+ CS0-003とCS0-002の出題範囲の比較表です。

CS0-003	CS-002	MAPPING
1.1 セキュリティオペレーションにおけるシステムとネットワークアーキテクチャの概念の重要性を説明できる。	2.1 与えられたシナリオに基づいて、インフラストラクチャマネジメントのためのセキュリティソリューションを適用することができる。	項目の更新
1.1 セキュリティオペレーションにおけるシステムとネットワークアーキテクチャの概念の重要性を説明できる。	3.2 与えられたシナリオに基づいて、セキュリティを向上させるために既存のコントロールへ構成変更を実装することができる。	項目の更新
1.2 与えられたシナリオに基づいて、潜在的な悪意あるアクティビティの指標を分析できる。	4.3 想定されたインシデントに基づき、潜在的なセキュリティ侵害インジケーター (IoC) を分析することができる。	出題分野の変更
1.3 与えられたシナリオに基づいて、適切なツールまたはテクニックを使用して悪意のあるアクティビティを判断できる。	1.4 与えられたシナリオに基づいて、一般的な脆弱性アセスメントツールからの出力を分析することができる。	項目の更新
1.4 脅威インテリジェンスと脅威ハンティングの概念を比較対照できる。	1.1 脅威データとインテリジェンスの重要性を説明することができる。	項目の更新
1.4 脅威インテリジェンスと脅威ハンティングの概念を比較対照できる。	1.2 与えられたシナリオに基づいて、脅威インテリジェンスを使用して組織のセキュリティをサポートすることができる。	出題分野の変更
1.4 脅威インテリジェンスと脅威ハンティングの概念を比較対照できる。	3.3 プロアクティブな脅威ハンティングの重要性を説明することができる。	出題分野の変更
1.5 セキュリティオペレーションにおける効率化とプロセス改善の重要性を説明できる。	3.4 自動化の概念とテクノロジーを比較対照することができる。	出題分野の変更
2.1 与えられたシナリオに基づいて、脆弱性スキャンの方法と概念を実装できる。	1.3 与えられたシナリオに基づいて、脆弱性マネジメントアクティビティを実行することができる。	出題分野の変更
2.2 与えられたシナリオに基づいて、脆弱性評価ツールからの出力を分析できる。	1.4 与えられたシナリオに基づいて、一般的な脆弱性アセスメントツールからの出力を分析することができる。	出題分野の変更
2.3 与えられたシナリオに基づいて、データを分析して脆弱性の優先順位付けができる。	n/a	新しい項目
2.4 与えられたシナリオに基づいて、攻撃とソフトウェアの脆弱性を低減するためのコントロールを推奨することができる。	1.7 与えられたシナリオに基づいて、攻撃とソフトウェアの脆弱性を低減するためのコントロールを実装することができる。	出題分野の変更
2.5 脆弱性への対応、取り扱い、管理に関連する概念を説明できる。	n/a	新しい項目
3.1 攻撃手法のフレームワークに関連する概念を説明できる。	1.2 与えられたシナリオに基づいて、脅威インテリジェンスを使用して組織のセキュリティをサポートすることができる。	項目の更新
3.2 与えられたシナリオに基づいて、インシデントレスポンスアクティビティを実行できる。	4.2 与えられたシナリオに基づいて、適切なインシデント対応プロセスを適用することができる。	出題分野の変更

CS0-003	CS-002	MAPPING
3.3 インシデント管理ライフサイクルの準備段階とインシデント後のアクティビティ段階を説明できる。	4.2 与えられたシナリオに基づいて、適切なインシデント対応プロセスを適用することができる。	項目の更新
4.1 脆弱性管理の報告とコミュニケーションの重要性を説明できる。	n/a	新しい項目
4.2 インシデントレスポンスの報告とコミュニケーションの重要性を説明できる。	4.1 インシデントレスポンスプロセスの重要性を説明することができる。	出題分野の変更