CASP+　CAS-003 とCAS-004 出題範囲の比較

CompTIA Advanced Security Practitioner

サイバー攻撃が世界的に増加し続ける中、あらゆる組織において、現在そして将来の脅威に対応していくために、クラウドやハイブリッド環境などのあらゆる環境でセキュアなIT/ネットワーク環境を効率的かつ効果的に設計、実装できる上級ITセキュリティ人材のニーズが高くなっています。CASP+の取得により、さらに複雑となるエンタープライズネットワークでサイバーセキュリティソリューションを効果的に設計、実装、管理するために必要となる高度なスキルを習得することが可能です。

CASP+の改訂では、複雑なネットワークの管理、セキュリティ意識向上のための取り組み、またセキュリティリスク低減の施策を実施するためのスキルなどが強化されています。また、高度なテクノロジーを利用しベストプラクティスを適用することで企業を保護し、将来的なサイバーリスクを防ぐためのソリューションを適用するためのスキルが評価されます。

CASP +は、 ISO/IEC 17024規格に準拠していることをANSIにより認証されています。また、米国国防総省指令 8570.01(DoD Directive 8570.01)により承認され、連邦情報セキュリティ管理法（FISMA）に基づく政府規制に準拠しています

CompTIA

出題範囲の比較

改訂によりCASP+の出題範囲は、特にハイブリッド環境とクラウド環境におけるサイバーセキュリティのアーキテクチャとエンジニアリングをより反映するようになりました。また、ガバナンス、リスク、コンプライアンスと、企業のサイバーセキュリティの準備状況を評価する方法に重点が置かれ、企業全体のサイバーセキュリティソリューションを設計、実装、トラブルシューティングするためのスキルも問われます。

下記の表は、CASP+ CAS-004とCAS-003の出題範囲の比較表です。

CAS-004	CAS-003	RESULTS
1.1 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、新規または既存のネットワークに対して、適切かつセキュアなネットワークアーキテクチャを実現することができる。	2.1 設定を分析し、セキュリティ要件に合うようにネットワークやセキュリティ要素、コンセプトやアーキテクチャを導入することができる。	Maps
1.2 与えられたシナリオに基づいて、組織の要件を分析し、インフラストラクチャの正しいセキュリティ設計を決定することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.2 与えられたシナリオに基づいて、組織の要件を分析し、インフラストラクチャの正しいセキュリティ設計を決定することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Gap
1.3 与えられたシナリオに基づいて、ソフトウェアアプリケーションを、セキュアな形で企業のアーキテクチャに統合することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.3 与えられたシナリオに基づいて、ソフトウェアアプリケーションを、セキュアな形で企業のアーキテクチャに統合することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	2.1 設定を分析し、セキュリティ要件に合うようにネットワークやセキュリティ要素、コンセプトやアーキテクチャを導入することができる。	Maps
1.5 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、認証と認可を適切に制御することができる。	4.3 与えられたシナリオに基づいて、エンタープライズセキュリティの目的に沿うように高度な認証認可のテクノロジーを導入、トラブルシューティングすることができる。	Maps
1.6 一連の要件に基づいて、クラウドと仮想化のセキュアなソリューションを実装することができる。	4.2 与えられたシナリオに基づいて、クラウドや仮想化技術をエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.7 暗号化技術と公開鍵インフラストラクチャ (PKI) が、セキュリティの目標と要件をいかにサポートするかを説明することができる。	n/a	New Content
1.8 新興テクノロジーが企業のセキュリティとプライバシーに与える影響説明することができる。	5.1 与えられたシナリオに基づいて、業界のトレンドや企業へのインパクトを実施し、適切な調査手法を用いることができる。	Maps

CAS-004	CAS-003	RESULTS
2.1 与えられたシナリオに基づいて、脅威マネジメントアクティビティを実行することができる。	n/a	New Content
2.2 与えられたシナリオに基づいて、侵害の痕跡を分析し、適切な対応策を立案することができる。	n/a	New Content
2.3 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。	n/a	New Content
2.4 与えられたシナリオに基づいて、脆弱性アセスメントとペネトレーションテストに関する、適切な手法とツールを使用することができる。	3.2 設定や調査結果に基づき、セキュリティアセスメントのために適切な手段を選択することができる。	Maps
2.5 与えられたシナリオに基づいて、脆弱性を分析し、リスク低減策を推奨することができる。	2.4 与えられたソフトウェア脆弱性に関するシナリオに基づき、適切なセキュリティ管理策を選択することができる。	Maps
2.6 与えられたシナリオに基づいて、プロセスを用いてリスクを低減することができる。	n/a	New Content
2.7 与えられたインシデントに基づいて、適切な対応策を実施することができる。	3.3 与えられたシナリオに基づいて、インシデント対応および復帰手順を実行することができる。	Maps
2.8 フォレンジックコンセプトの重要性について説明することができる。	n/a	New Content
2.9 与えられたシナリオに基づいて、フォレンジック分析ツールを使用することができる。	n/a	New Content
3.1 与えられたシナリオに基づいて、企業のモビリティにセキュアな構成を適用することができる。	2.3 設定の分析、セキュリティ要件に合うモバイル・デバイスやスモール・フォームファクタ・デバイス向けセキュリティ管理策を導入することができる。	Maps
3.1 与えられたシナリオに基づいて、企業のモビリティにセキュアな構成を適用することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
3.2 与えられたシナリオに基づいて、エンドポイントセキュリティ管理を構成および実装することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
3.3 特定のセクターやオペレーション技術に影響を及ぼすセキュリティ上の検討事項を説明することができる。	n/a	New Content
3.4 クラウドテクノロジーの採用が組織のセキュリティにどう影響するかを説明することができる。	4.2 与えられたシナリオに基づいて、クラウドや仮想化技術をエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
3.4 クラウドテクノロジーの採用が組織のセキュリティにどう影響するかを説明することができる。	1.1 ビジネスおよび業界の影響やそれに関連するセキュリティリスクの概要を要約することができる。	Maps
3.5 与えられたビジネス要件に基づいて、適切な PKI ソリューションを実装することができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Maps
3.6 与えられたビジネス要件に基づいて、暗号化の適切なプロトコルとアルゴリズムを実装することができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Maps
3.7 与えられたシナリオに基づいて、暗号化技術の実装に関する問題をトラブルシューティングすることができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Gap

CAS-004	CAS-003	RESULTS
4.1 一連の要件に基づいて、適切なリスク戦略を適用することができる。	1.2 組織の要件に基づくセキュリティ、プライバシーポリシー、手順を比較対照することができる。	Gap
4.2 ベンダーリスクの管理と低減の重要性を説明することができる。	n/a	New Content
4.3 コンプライアンスのフレームワークと法的検討事項とそれらが組織に与える影響を説明することができる。	1.2 組織の要件に基づくセキュリティ、プライバシーポリシー、手順を比較対照することができる。	Maps
4.3 コンプライアンスのフレームワークと法的検討事項とそれらが組織に与える影響を説明することができる。	1.3 与えられたシナリオに基づいて、リスク緩和戦略とこれらを実行することができる。	Maps
4.4 事業継続性と災害復旧のコンセプトの重要性を説明することができる。	1.3 与えられたシナリオに基づいて、リスク緩和戦略とこれらを実行することができる。	Maps
4.4 事業継続性と災害復旧のコンセプトの重要性を説明することができる。	1.4 リスクの測定項目設定を分析し、企業のセキュリティ保護を実施 することができる。	Maps

CASP+　CAS-003 とCAS-004 出題範囲の比較

CompTIA Advanced Security Practitioner

サイバー攻撃が世界的に増加し続ける中、あらゆる組織において、現在そして将来の脅威に対応していくために、クラウドやハイブリッド環境などのあらゆる環境でセキュアなIT/ネットワーク環境を効率的かつ効果的に設計、実装できる上級ITセキュリティ人材のニーズが高くなっています。CASP+の取得により、さらに複雑となるエンタープライズネットワークでサイバーセキュリティソリューションを効果的に設計、実装、管理するために必要となる高度なスキルを習得することが可能です。

CASP+の改訂では、複雑なネットワークの管理、セキュリティ意識向上のための取り組み、またセキュリティリスク低減の施策を実施するためのスキルなどが強化されています。また、高度なテクノロジーを利用しベストプラクティスを適用することで企業を保護し、将来的なサイバーリスクを防ぐためのソリューションを適用するためのスキルが評価されます。

CASP +は、 ISO/IEC 17024規格に準拠していることをANSIにより認証されています。また、米国国防総省指令 8570.01(DoD Directive 8570.01)により承認され、連邦情報セキュリティ管理法（FISMA）に基づく政府規制に準拠しています

CompTIA

出題範囲の比較

改訂によりCASP+の出題範囲は、特にハイブリッド環境とクラウド環境におけるサイバーセキュリティのアーキテクチャとエンジニアリングをより反映するようになりました。また、ガバナンス、リスク、コンプライアンスと、企業のサイバーセキュリティの準備状況を評価する方法に重点が置かれ、企業全体のサイバーセキュリティソリューションを設計、実装、トラブルシューティングするためのスキルも問われます。

下記の表は、CASP+ CAS-004とCAS-003の出題範囲の比較表です。

CAS-004	CAS-003	RESULTS
1.1 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、新規または既存のネットワークに対して、適切かつセキュアなネットワークアーキテクチャを実現することができる。	2.1 設定を分析し、セキュリティ要件に合うようにネットワークやセキュリティ要素、コンセプトやアーキテクチャを導入することができる。	Maps
1.2 与えられたシナリオに基づいて、組織の要件を分析し、インフラストラクチャの正しいセキュリティ設計を決定することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.2 与えられたシナリオに基づいて、組織の要件を分析し、インフラストラクチャの正しいセキュリティ設計を決定することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Gap
1.3 与えられたシナリオに基づいて、ソフトウェアアプリケーションを、セキュアな形で企業のアーキテクチャに統合することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.3 与えられたシナリオに基づいて、ソフトウェアアプリケーションを、セキュアな形で企業のアーキテクチャに統合することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。	2.1 設定を分析し、セキュリティ要件に合うようにネットワークやセキュリティ要素、コンセプトやアーキテクチャを導入することができる。	Maps
1.5 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、認証と認可を適切に制御することができる。	4.3 与えられたシナリオに基づいて、エンタープライズセキュリティの目的に沿うように高度な認証認可のテクノロジーを導入、トラブルシューティングすることができる。	Maps
1.6 一連の要件に基づいて、クラウドと仮想化のセキュアなソリューションを実装することができる。	4.2 与えられたシナリオに基づいて、クラウドや仮想化技術をエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
1.7 暗号化技術と公開鍵インフラストラクチャ (PKI) が、セキュリティの目標と要件をいかにサポートするかを説明することができる。	n/a	New Content
1.8 新興テクノロジーが企業のセキュリティとプライバシーに与える影響説明することができる。	5.1 与えられたシナリオに基づいて、業界のトレンドや企業へのインパクトを実施し、適切な調査手法を用いることができる。	Maps

CAS-004	CAS-003	RESULTS
2.1 与えられたシナリオに基づいて、脅威マネジメントアクティビティを実行することができる。	n/a	New Content
2.2 与えられたシナリオに基づいて、侵害の痕跡を分析し、適切な対応策を立案することができる。	n/a	New Content
2.3 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。	n/a	New Content
2.4 与えられたシナリオに基づいて、脆弱性アセスメントとペネトレーションテストに関する、適切な手法とツールを使用することができる。	3.2 設定や調査結果に基づき、セキュリティアセスメントのために適切な手段を選択することができる。	Maps
2.5 与えられたシナリオに基づいて、脆弱性を分析し、リスク低減策を推奨することができる。	2.4 与えられたソフトウェア脆弱性に関するシナリオに基づき、適切なセキュリティ管理策を選択することができる。	Maps
2.6 与えられたシナリオに基づいて、プロセスを用いてリスクを低減することができる。	n/a	New Content
2.7 与えられたインシデントに基づいて、適切な対応策を実施することができる。	3.3 与えられたシナリオに基づいて、インシデント対応および復帰手順を実行することができる。	Maps
2.8 フォレンジックコンセプトの重要性について説明することができる。	n/a	New Content
2.9 与えられたシナリオに基づいて、フォレンジック分析ツールを使用することができる。	n/a	New Content
3.1 与えられたシナリオに基づいて、企業のモビリティにセキュアな構成を適用することができる。	2.3 設定の分析、セキュリティ要件に合うモバイル・デバイスやスモール・フォームファクタ・デバイス向けセキュリティ管理策を導入することができる。	Maps
3.1 与えられたシナリオに基づいて、企業のモビリティにセキュアな構成を適用することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
3.2 与えられたシナリオに基づいて、エンドポイントセキュリティ管理を構成および実装することができる。	2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。	Maps
3.3 特定のセクターやオペレーション技術に影響を及ぼすセキュリティ上の検討事項を説明することができる。	n/a	New Content
3.4 クラウドテクノロジーの採用が組織のセキュリティにどう影響するかを説明することができる。	4.2 与えられたシナリオに基づいて、クラウドや仮想化技術をエンタープライズアーキテクチャにセキュアに統合することができる。	Maps
3.4 クラウドテクノロジーの採用が組織のセキュリティにどう影響するかを説明することができる。	1.1 ビジネスおよび業界の影響やそれに関連するセキュリティリスクの概要を要約することができる。	Maps
3.5 与えられたビジネス要件に基づいて、適切な PKI ソリューションを実装することができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Maps
3.6 与えられたビジネス要件に基づいて、暗号化の適切なプロトコルとアルゴリズムを実装することができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Maps
3.7 与えられたシナリオに基づいて、暗号化技術の実装に関する問題をトラブルシューティングすることができる。	4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。	Gap

CAS-004	CAS-003	RESULTS
4.1 一連の要件に基づいて、適切なリスク戦略を適用することができる。	1.2 組織の要件に基づくセキュリティ、プライバシーポリシー、手順を比較対照することができる。	Gap
4.2 ベンダーリスクの管理と低減の重要性を説明することができる。	n/a	New Content
4.3 コンプライアンスのフレームワークと法的検討事項とそれらが組織に与える影響を説明することができる。	1.2 組織の要件に基づくセキュリティ、プライバシーポリシー、手順を比較対照することができる。	Maps
4.3 コンプライアンスのフレームワークと法的検討事項とそれらが組織に与える影響を説明することができる。	1.3 与えられたシナリオに基づいて、リスク緩和戦略とこれらを実行することができる。	Maps
4.4 事業継続性と災害復旧のコンセプトの重要性を説明することができる。	1.3 与えられたシナリオに基づいて、リスク緩和戦略とこれらを実行することができる。	Maps
4.4 事業継続性と災害復旧のコンセプトの重要性を説明することができる。	1.4 リスクの測定項目設定を分析し、企業のセキュリティ保護を実施 することができる。	Maps