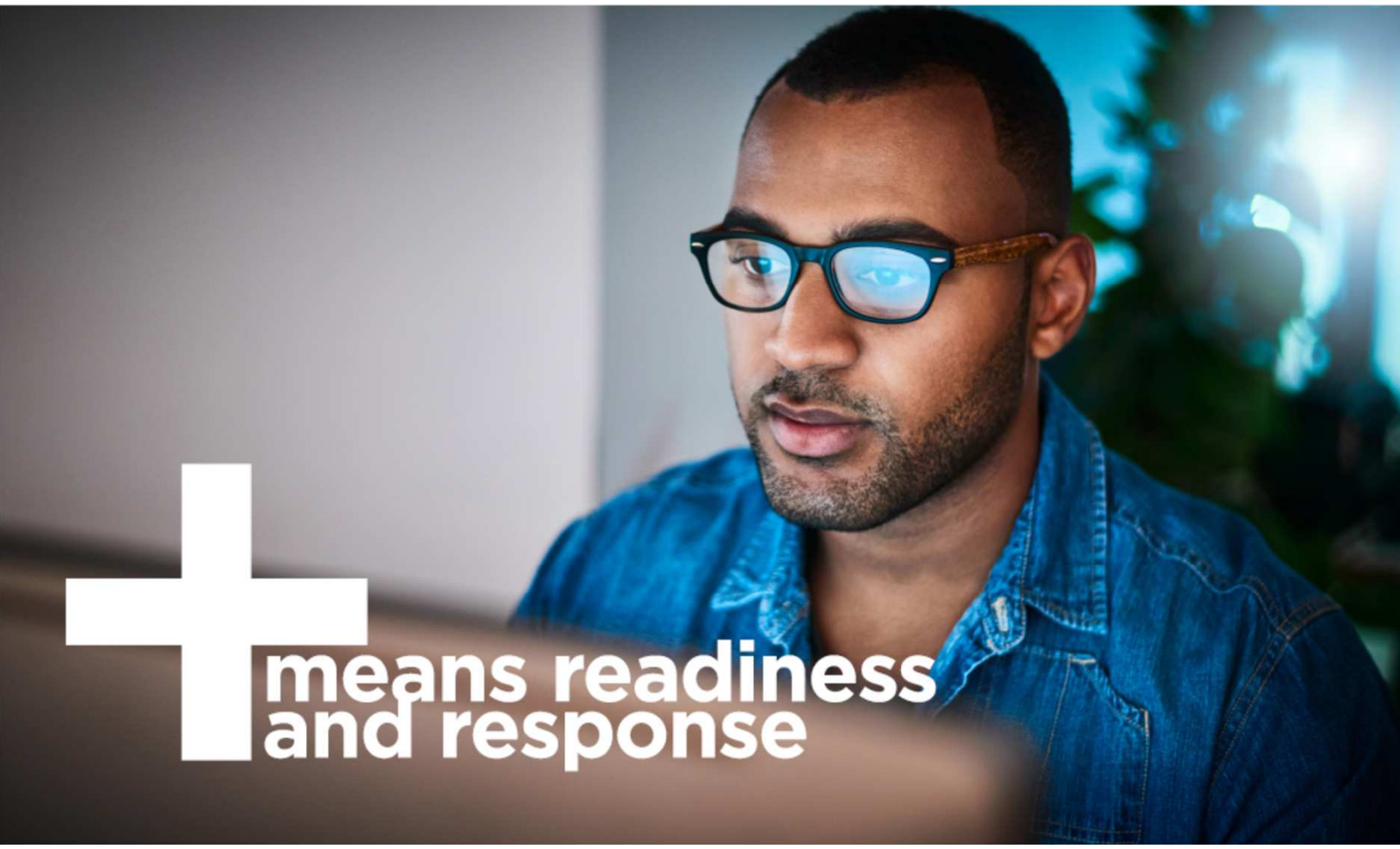
CompTIA




## CompTIA Security+ SY0-601とSY0-501 出題範囲の比較

サイバーセキュリティ攻撃が増加するにつれて、日頃からセキュリティ対策のための準備と改善をするベースとなるスキルと、インシデントレスポンスのためのスキルの両方が必要とされます。今回のCompTIA Security+の更新では、これらのスキルが必要とされる多くの職種に関連するスキルを反映し、認定資格を取得することで、よりプロアクティブな活動により、セキュリティ攻撃への準備に必要なスキルを修得することが可能です。

CompTIA Security+ SY0-601では、セキュリティ態勢の改善とサイバーセキュリティリスクの改善に焦点をあてています。
企業のセキュリティ態勢の評価、ハイブリッドクラウド環境のモニタリングと保護、さまざまなIT規制への準拠、リスクの評価とマネジメント、セキュリティイベント発生時のインシデントレスポンスなどが出題の対象となっています。

CompTIA Security+は、ISO17024に準拠しており、米国国防総省指令 8570.01(DoD Directive 8570.01)により承認された認定資格です。多くの企業や防衛関連の組織で活用されています。

CompTIA Security+

CompTIA

## 出題範囲の比較

下記の表は、CompTIA Security+ SY0-601とSY0-501の出題範囲の比較表です。SY0-501の出題範囲は、SY0-601の出題内容で類似するスキルに並び替えられています。

| SY0-601 | SY0-501 |
|---|---|
| 1.1 異なるタイプのソーシャルエンジニアリング手法を比較対照することができる。 | 1.1 与えられたシナリオに基づいて、不正の痕跡を分析してマルウェアの種類を特定することができる。 |
| 1.2 与えられたシナリオに基づいて、 可能性のあるインジケーターを分析して攻撃の種類を特定することができる。 | 1.2 さまざまな攻撃のタイプを比較対照することができる。 |
| 1.3 与えられたシナリオに基づいて、アプリケーション攻撃に関連する可能性のあるインジケーターを分析することができる。 | 2.3 与えられたシナリオに基づいて、一般的なセキュリティ問題のトラブルシューティングを実施することができる。 |
| 1.4 与えられたシナリオに基づいて、ネットワーク攻撃に関連する可能性のあるインジケーターを分析することができる。 | 2.4 与えられたシナリオに基づいて、セキュリティテクノロジーのアウトプットを分析・解釈することができる。 |
| 1.5 様々な脅威アクター、ベクター、インテリジェンスソースを説明することができる。 | 1.3 脅威となる行為主体のタイプと属性について説明することができる。 |
| 1.6 様々な脆弱性のタイプによるセキュリティの懸念について説明することができる。 | 1.6 脆弱性のタイプによる影響について説明することができる。 |
| 1.7 セキュリティ評価で使用する手法を要約することができる。 | 1.4 さまざまなペネトレーションテストのコンセプトについて説明することができる。 |
| 1.8 ペネトレーションテストで使用する手法を説明することができる。 | 1.5 脆弱性スキャンのコンセプトについて説明することができる。 |
| 2.1 エンタープライズ環境におけるセキュリティコンセプトの重要性を説明することができる。 | （前回バージョンの試験では、エンタープライズに特化した出題項目はありませんでした。） |
| 2.2 仮想化コンセプトとクラウドコンピューティングのコンセプトを要約することができる。 | 3.7 クラウドと仮想化に関するコンセプトを要約することができる。 |
| 2.3 セキュアなアプリケーションの開発、 デプロイ、 自動化に関するコンセプトを要約することができる。 | 3.4 セキュアなステージングデプロイメントのコンセプトの重要性を説明することができる。<br>3.6 セキュアなアプリケーションの開発とデプロイに関するコンセプトを要約することができる。 |
| 2.4 認証と認可の設計コンセプトを要約することができる。 | 4.1 アイデンティティとアクセス管理のさまざまなコンセプトを比較対照することができる。 |
| 2.5 与えられたシナリオに基づいて、 サイバーセキュリティのレジリエンスを実装することができる。 | 3.8 レジリエンスと自動化によってリスクを低減する戦略について説明することができる。 |
| 2.6 組み込みシステムおよび特殊システムがもたらすセキュリティ上の影響について説明することができる。 | 3.5 組み込みシステムがもたらすセキュリティ上の影響について説明することができる。 |
| 2.7 物理的セキュリティコントロールの重要性について説明することができる。 | 3.9 物理的セキュリティコントロールの重要性について説明することができる。 |
| （前回バージョンのこの項目は一般的な項目のため、SY0-601の出題範囲に分散されています。） | 5.8 与えられたシナリオに基づいて、データのセキュリティとプライバシーを守る手順を実行することができる。 |
| 2.8 暗号化コンセプトの基本を要約することができる。 | 6.1 暗号化の基本的なコンセプトを比較対照することができる。 |
| （SY0-601でも暗号化は出題されていますが、管理者の職務にとって暗号アルゴリズムは専門的なため、項目が削除されました。） | 6.2 各種の暗号アルゴリズムとそれぞれの基本的な特徴について説明することができる。 |
| 3.1 与えられたシナリオに基づいて、セキュアなプロトコルの実装を行うことができる。 | 2.6 与えられたシナリオに基づいて、セキュアプロトコルの実装を行うことができる。 |

| SY0-601 | SY0-501 |
|---|---|
| 3.2 与えられたシナリオに基づいて、ホストまたはアプリケーションのセキュリティソリューションを実装することができる。 | 3.2 与えられたシナリオに基づいて、セキュアネットワークアーキテクチャのコンセプトを導入することができる。 |
| 3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。 | 3.3 与えられたシナリオに基づいて、セキュアなシステムデザインを導入することができる。 |
| （前回バージョンのこの項目は一般的な項目のため、SY0-601の出題範囲に分散されています。） | 2.1 組織のセキュリティを維持するために、ハードウェアおよびソフトウェアのネットワークコンポーネントをインストール・設定することができる。 |
| 3.4 与えられたシナリオに基づいて、ワイヤレスセキュリティ設定をインストール、構成することができる。 | 6.3 与えられたシナリオに基づいて、ワイヤレスセキュリティ設定をインストール、実装することができる。 |
| 3.5 与えられたシナリオに基づいて、セキュアなモバイルソリューションを実装することができる。 | 2.5 与えられたシナリオに基づいて、モバイルデバイスを安全に導入することができる。 |
| 3.6 与えられたシナリオに基づいて、クラウドにサイバーセキュリティソリューションを適用することができる。 | 3.7 クラウドと仮想化に関するコンセプトを要約することができる。 |
| 3.7 与えられたシナリオに基づいて、 認証管理とアカウント管理の制御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、アイデンティティ管理サービスのインストールと設定ができる。 |
| 3.8 与えられたシナリオに基づいて、 認証と認可のソリューションを導入することができる。 | 4.3 与えられたシナリオに基づいて、認証管理とアクセス管理のコントロールを実装することができる。<br>4.4 与えられたシナリオに基づいて、一般的なアカウント管理手法の差異を明らかにすることができる。 |
| 3.9 与えられたシナリオに基づいて、 公開鍵インフラストラクチャを実装することができる。 | 6.4 与えられたシナリオに基づいて、公開鍵インフラストラクチャを実装することができる。 |
| 4.1 与えられたシナリオに基づいて、 適切なツールを利用して組織のセキュリティにアクセスすることができる。 | 2.2 与えられたシナリオに基づいて、組織のセキュリティ対策に最適なソフトウェアツールを活用することができる。 |
| 4.2 インシデントレスポンスのポリシー、 プロセス、 手順の重要性を要約することができる。<br>4.3 想定されたインシデントに基づき、適切なデータソースを使用して調査をサポートすることができる。<br>4.4 想定されたインシデントに基づき、低減技術や制御を適用して環境を保護することができる。 | 5.4 与えられたシナリオに基づいて、インシデント対応の手順を実行することができる。<br>5.6 災害復旧と事業継続のコンセプトについて説明することができる。 |
| 4.5 デジタルフォレンジックの重要な側面について説明することができる。 | 5.5 フォレンジックの基本的なコンセプトを要約することができる。 |
| 5.1 様々な制御タイプを比較対照することができる。 | 5.7 さまざまな管理タイプを比較対照することができる。 |
| 5.2 組織のセキュリティ態勢に影響を及ぼす適用される規制、 標準、 フレームワークの重要性について説明できる。 | 3.1 フレームワーク、ベストプラクティス、セキュア構成ガイドの適用例と目的について説明することができる。 |
| 5.3 組織のセキュリティに関連するポリシーの重要性について説明することができる。 | 5.1 組織のセキュリティに関連するポリシー、プラン、手順の重要性について説明することができる。 |
| 5.4 リスク管理のプロセスとコンセプトについて要約することができる。 | 5.2 ビジネスインパクト分析に関するコンセプトを要約することができる。<br>5.3 リスク管理のプロセスとコンセプトについて説明することができる。 |
| 5.5 セキュリティに関連するプライバシーおよび機密データの概念を説明することができる。 | 3.1 フレームワーク、ベストプラクティス、セキュア構成ガイドの適用例と目的について説明することができる。 |