CompTIA Security+ SY0-701とSY0-601 出題範囲の比較

改訂CompTIA Security+（SY0-701）は、主要なサイバーセキュリティの最新スキルが反映されています。現在の脅威、自動化、ゼロトラスト、IoT、リスク管理など、サイバーセキュリティの中でも需要の高いスキルが網羅されています。
CompTIA Security+（SY0-701）を取得することで、業務を遂行するために必要なコアとなるスキルを理解し、そのスキルを業務で活かすことが可能です。また、サイバーセキュリティ分野でのキャリアを構築するために重要となるコアスキルを習得することにも可能です。
CompTIA Security+は、多くの職種でベースラインのサイバーセキュリティスキルの習得のため、業界の他の認定資格よりも活用されています。

CompTIA Security+は、セキュリティスペシャリスト、システム管理者、セキュリティ管理者などの職務において、ネットワークの保護、脅威の検出、データの保護などの業務に必要とされるスキルと知識を習得することが可能です。

CompTIA Security+（SY0-701）に含まれる出題内容は、下記の通りです。

- 企業環境でのセキュリティ態勢（security posture）を評価し、適切なセキュリティソリューションを推奨、実装する。
- クラウド、モバイル、IoT、オペレーショナルテクノロジー（OT）などのハイブリット環境のセキュリティモニタリングと保護。
- ガバナンス、リスク、コンプライアンスを含む適用される規制やポリシーを意識し、運営する。
- セキュリティイベントやインシデントを特定、分析し、対応する。

CompTIA

出題範囲の比較

下記の表は、CompTIA Security+ SY0-701とSY0-601の出題範囲の比較表です。

SY0-701	SY0-601	MAPPING
1.1 さまざまなタイプのセキュリティコントロールを比較対照することができる。	5.1 様々な制御タイプを比較対照することができる。	項目の移動
1.2 基本的なセキュリティコンセプトを要約することができる。	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。	項目の移動
1.2 基本的なセキュリティコンセプトを要約することができる。	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。	項目の移動
1.2 基本的なセキュリティ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。	項目の移動
1.3 変更管理プロセスの重要性とセキュリティへの影響を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。	項目の移動
1.4 適切な暗号化ソリューションを用いる重要性を説明することができる。	2.8 暗号化コンセプトの基本を要約することができる。	項目の移動
2.1 一般的な脅威アクターと誘因を説明することができる。	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。	項目の移動
2.2 一般的な脅威ベクターと攻撃対象領域を説明することができる。	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。	項目の移動
2.3 様々な種類の脆弱性を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。	項目の移動
2.4 与えられたシナリオに基づいて、悪意あるアクティビティの指標を分析することができる。	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。	項目の移動
2.4 与えられたシナリオに基づいて、悪意あるアクティビティの指標を分析することができる。	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。	項目の移動
2.4 与えられたシナリオに基づいて、悪意あるアクティビティの指標を分析することができる。	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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を説明することができる。	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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を説明することができる。	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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を説明することができる。	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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を説明することができる。	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。	項目の移動
2.5 企業の保護に用いられる軽減手法の目的を説明することができる。	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。	
3.1 様々なアーキテクチャモデルのセキュリティ関連事項を比較対照することができる。	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。	
3.1 様々なアーキテクチャモデルのセキュリティ関連事項を比較対照することができる。	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。	

CompTIA

SY0-701	SY0-601	MAPPING
3.1 様々なアーキテクチャモデルのセキュリティ関連事項を比較対照することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の更新
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。	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。	項目の移動
3.3 データ保護のコンセプトと戦略を比較対照することができる。	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。	項目の移動
3.4 セキュリティアーキテクチャにおけるレジリエンスと復旧の重要性を説明することができる。	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。	項目の移動
3.4 セキュリティアーキテクチャにおけるレジリエンスと復旧の重要性を説明することができる。	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。	項目の移動
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の更新
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の更新
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の移動
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の更新
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の移動
4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。	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。	項目の移動

SY0-701	SY0-601	MAPPING
4.2 適切なハードウェア、ソフトウェア、およびデータアセット管理のセキュリティ関連事項を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。	項目の移動
4.2 適切なハードウェア、ソフトウェア、およびデータアセット管理のセキュリティ関連事項を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。	項目の移動
4.2 適切なハードウェア、ソフトウェア、およびデータアセット管理のセキュリティ関連事項を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。	項目の移動
4.3 脆弱性管理に関連する様々なアクティビティを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。	項目の移動
4.3 脆弱性管理に関連する様々なアクティビティを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。	項目の移動
4.3 脆弱性管理に関連する様々なアクティビティを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。	項目の移動
4.3 脆弱性管理に関連する様々なアクティビティを説明することができる。	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。	項目の移動
4.3 脆弱性管理に関連する様々なアクティビティを説明することができる。	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。	項目の移動
4.4 セキュリティアラートとモニタリングのコンセプトとツールを説明することができる。	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。	項目の移動
4.4 セキュリティアラートとモニタリングのコンセプトとツールを説明することができる。	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。	項目の移動
4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。	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。	項目の移動
4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。	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。	項目の移動
4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。	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。	項目の移動
4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。	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。	項目の移動
4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。	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。	項目の移動
4.6 与えられたシナリオに基づいて、ID とアクセスの管理を実施および維持することができる。	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。	項目の更新
4.7 セキュアなオペレーションに関連する自動化とオーケストレーションの重要性を説明することができる。	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。	項目の移動
4.8 適切なインシデントレスポンスアクティビティを説明することができる。	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。	項目の移動
4.8 適切なインシデントレスポンスアクティビティを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。	項目の移動

CompTIA

SY0-701	SY0-601	MAPPING
4.9 与えられたシナリオに基づいて、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。	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。	項目の移動
5.1 効果的なセキュリティガバナンスの要素を説明することができる。	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。	項目の移動
5.1 効果的なセキュリティガバナンスの要素を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。	項目の移動
5.2 リスク管理プロセスの要素を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。	項目の移動
5.3 サードパーティーのリスク評価とリスク管理に関連するプロセスを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。	項目の移動
5.3 サードパーティーのリスク評価とリスク管理に関連するプロセスを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。	項目の移動
5.4 効果的なセキュリティコンプライアンスの要素を説明することができる。	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。	項目の移動
5.4 効果的なセキュリティコンプライアンスの要素を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。	項目の移動
5.5 監査および評価のタイプと目的を説明することができる。	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。	項目の移動
5.5 監査および評価のタイプと目的を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。	項目の移動
5.6 与えられたシナリオに基づいて、セキュリティ意識向上のプラクティスを実施することができる。	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。	項目の更新