CompTIA

Certification Guide

CompTIA Security+

Protect Your Organization with Security+ Certification

■ CompTIA Security+ とは

CompTIA Security+ は、セキュリティのコアとなるスキルを習得し、セキュリティキャリアを推進していく上で必要となるベースを育成できるワールドワイドの認定資格です。
ベンダーニュートラルで、業務上必要とされるセキュリティスキルが網羅された認定資格のため、世界中の企業 / 組織、セキュリティプロフェッショナルに活用されています。

CompTIA Security+ 認定資格を取得することで、下記のような知識とスキルを持っていることを証明します。

- エンタープライズ環境のセキュリティ態勢を評価し、適切なセキュリティソリューションを推奨および実装する
- ククラウド、モバイル、IoT などハイブリッド環境のセキュリティを確保しモニタリングする
- ガバナンス、リスク、コンプライアンスの原則を含む適切な法律やポリシーを認識したうえで運用する
- セキュリティイベントやインシデントの識別分析、対応を実施する

CompTIA Security+ は、セキュリティ / システム管理者として 2 年間の実務経験に相当するスキルを評価します

CompTIA Security+ は、ISO17024 を取得しています。また、米国国防総省による指令 8140/8570.01-M の要件を満たすことが承認されており、取得必須認定資格の 1 つとされています。

■ CompTIA Security+ の取得

CompTIA Security+ は、Core Skills Certification の一つに位置付けられ、すべてのキャリアパスにおいて必須とされるベースとなるセキュリティスキルを習得することが可能です。

CompTIA Security+ 認定資格試験には、**多肢選択式の問題**に加え、正確にスキルを評価するために**パフォーマンスベースの問題が含まれています。**

" 業界の業界による
業界のための資格"

CompTIA 認定資格は、試験作成委員会が中心となり、ニーズ調査・職務分析・リサーチを経て、SME（サブジェクトマターエキスパート）と呼ばれる現場関係者により開発が進められます。

CompTIA Security+ SME
■海外 / 一部抜粋
- Amazon Web Services
- Australian Government
- Cisco
- Deloitte
- Dept. of Navy
- Federal Government
- First American
- IBM
- NTT
- PwC
- The Johns Hopkins University Applied Physics Laboratory
- U.S. Army
- US Marine Corps

■日本（50 音順）
- NRI セキュアテクノロジーズ株式会社
- 日本電気株式会社
- 富士フイルムビジネスイノベーションジャパン株式会社
- 株式会社ラック

認定資格の詳細情報は、下記 Web サイトをご覧ください：
https://www.comptia.jp/certif/comptia_certificaiton/

■ CompTIA 認定資格のキャリアパスと CompTIA Security+ の位置づけ

■ CompTIA Security+ 出題範囲

CompTIA Security+（SY0-601）		
1.0 攻撃、脅威、脆弱性	24%	• 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。
2.0 アーキテクチャと設計	21%	• 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。 • 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。 • 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。 • 認証と認可の設計コンセプトを要約することができる。 • 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。 • 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。 • 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。 • 暗号化コンセプトの基本を要約することができる。
3.0 実装	25%	• 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。 • 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。
4.0 運用とインシデントレスポンス	16%	• 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。 • 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。 • 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。 • 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。 • 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。
5.0 ガバナンス、リスク、コンプライアンス	14%	• 様々な制御タイプを比較対照することができる。 • 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。 • 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。 • 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。 • 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。

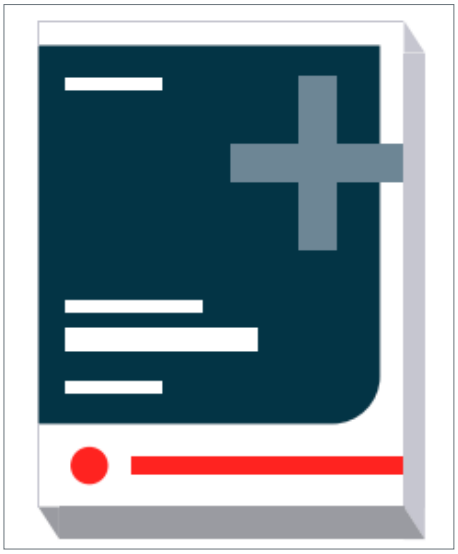
■ CompTIA Security+ 試験概要

試験番号	問題数	制限時間	合格ライン
SY0-601	最大で 90 問	90 分	100 ～ 900 のスコア形式 750 以上

■ CompTIA Security+ トレーニング教材 : The Official CompTIA Study Guide

The Official CompTIA Study Guide は、CompTIA 認定資格試験の出題範囲がすべて網羅されているテキストです。
eBook 版と書籍版の 2 種類が提供されています。

The Official CompTIA Security+ Self-Paced Study Guide（試験番号 : SY0-601）日本語版



学習範囲
最新の CompTIA Security+（SY0-601）出題範囲を網羅しており、多くの図解を含み理解しやすく設計されているため、自学で学習を進める方向けにも学習しやすいコンテンツです。

含まれる内容
- 実際の業務で活用できるように設計されたコンテンツ－レッスンでは、実際の業務で取り扱う項目ごとに学習ができ、すべてのトピックスでは職務における特定のタスクに関連した項目が取り上げられています。
- トピックスごとの確認問題で理解度を確認することができます。
- 重要な用語と略語集

学習内容
The Official CompTIA Security+ Study Guide (SY0-601) は、CompTIA 認定資格試験を自学で学習される方向けに作成されています。本書は、CompTIA Security+ (SY0-601) の出題範囲がすべて網羅されていることを第三者により評価されており、CompTIA Security+ 取得に必要なスキルを取得することが可能です。

本書には、以下の内容が含まれています。

- セキュリティのロールとセキュリティコントロールを比較する
- 脅威アクターと脅威インテリジェンスについて説明する
- セキュリティ評価を実行する
- ソーシャルエンジニアリングとマルウェアを特定する
- 基本的な暗号化の概念を要約する
- 公開鍵インフラストラクチャを実装する
- 認証コントロールを実装する
- アイデンティティ管理とアクセス管理（IAM）を実装する
- セキュアなネットワーク設計を実装する
- ネットワークセキュリティアプライアンスを実装する
- セキュアなネットワークプロトコルを実装する
- ホストセキュリティソリューションを実装する
- セキュアなモバイルソリューションを実装する
- セキュアなアプリケーションの概念を要約する
- セキュアクラウドソリューションの実装
- データのプライバシーと保護の概念を説明する
- インシデントレスポンスの実行
- デジタルフォレンジックについて説明する
- リスクマネジメントの概念を要約する
- サイバーセキュリティのレジリエンスを実装する
- 物理的セキュリティについて説明する

The Official CompTIA Contents の購入は、下記 CompTIA Store から :

https://jp-store.comptia.org/

■ CompTIA Security+ トレーニング教材：CompTIA CertMaster Labs

CompTIA CertMaster Labs では、リモート環境を通して、実際のソフトウェアを体験学習することが可能です。CompTIA CertMaster Labs の学習内容は、CompTIA 認定資格試験の出題範囲に沿っており、より実践的な学習を行うことができます。

ブラウザーベース
CompTIA CertMaster Labs は、インターネット接続とブラウザを使用してアクセスが可能で、学習のためにセットアップは必要ありません。受講者は、特定の機材やソフトウェアといった学習教材をリモートからセキュアに利用することが可能です。

実際の IT 環境やソフトウェアを使用
CompTIA CertMaster Labs では、実際のソフトウェアアプリケーションとオペレーティングシステムで構成された仮想マシンを使用しています。タスクに対して柔軟に対応できるだけではなく、受講者の業務での実体験を再現することが可能です。

モジュール形式のタスク
各ラボ内のタスクは、それぞれ独立しており、任意の順番で進めていただくことが可能です。

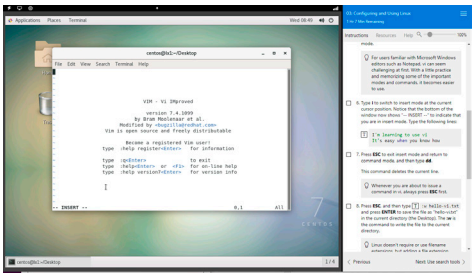
即戦力の育成に最適
CompTIA CertMaster Labs は、受講者が業務における実践的なスキルを育成する際に役立つと共に、CompTIA 認定資格試験を受験の際に、パフォーマンスベーステストを想定した準備のためにも役立ちます。

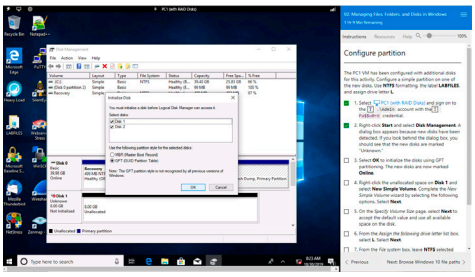
Officla CompTIA Content との高い親和性
CompTIA CertMaster Labs は、Official CompTIA Content のアクティビティに基づいており、知識と実践的なスキルの両方を習得するためのシームレスな学習体験を提供します。

CompTIA CertMaster Labs for Security+（SY0-601）

本 Labs には、以下の内容が含まれています。

- Assisted Lab: ラボ環境の調査
- Assisted Lab: ネットワークノードのスキャンと特定
- Assisted Lab: パケットスニッフィングツールを使用したネットワークトラフィックのインターセプトとインターラプト
- Assisted Lab: クレデンシャル脆弱性スキャン結果の分析
- Assisted Lab: マルウェアベースのバックドアのインストール、使用、ブロック
- APPLIED LAB: ネットワーク偵察と脆弱性スキャンの実行
- Assisted Lab: 証明書のライフサイクルの管理
- Assisted Lab: OpenSSL を使用した証明書の管理
- Assisted Lab: パスワードクラッキングユーティリティを使用したパスワードの監査
- Assisted Lab: 一元管理された認証の管理
- Assisted Lab: Windows Server でのアクセスコントロールの管理
- Assisted Lab: 監査ポリシーシステムの構成
- Assisted Lab: Linux でのアクセスコントロールの管理
- APPLIED LAB: Identity and Access Management コントロールの構成
- Assisted Lab: セキュアなネットワーク設計の実装
- Assisted Lab: ファイアーウォールの構成
- Assisted Lab: 侵入検知システムの構成
- Assisted Lab: セキュアなネットワークアドレスサービスの実装
- Assisted Lab: 仮想プライベートネットワークの実装
- Assisted Lab: セキュア SSH サーバーの実装
- Assisted Lab: エンドポイントプロテクションの実装
- APPLIED LAB: セキュアなネットワークインフラストラクチャの実装
- Assisted Lab: アプリケーション攻撃の特定
- Assisted Lab: ブラウザー攻撃の特定
- Assisted Lab: PowerShell セキュリティの実装
- Assisted Lab: 悪意あるコードの特定
- APPLIED LAB: アプリケーション攻撃の特定
- Assisted Lab: インシデントレスポンスのためのデータソースの管理
- Assisted Lab: 緩和制御の構成
- Assisted Lab: デジタルフォレンジックの証拠の取得
- Assisted Lab: Windows および Linux でのデータバックアップと復元
- APPLIED LAB: インシデントレスポンス、リスク軽減、回復の管理





※イメージはサンプルです。各認定資格で表示される画面とは異なります。

CompTIA CertMaster Labs の購入は、下記 CompTIA Store から：

https://jp-store.comptia.org/

CompTIA 日本支局 www.comptia.jp
facebook.com/CompTIAJP twitter.com/CompTIA_JP