CompTIA

Certification Guide

CompTIA CySA+

Build on your foundational skills to help organizations address, monitor and respond to threats and manage risk.

■ CompTIA CySA+ とは

CompTIA Cybersecurity Analyst（CySA+）は、国際的に認知されているベンダーニュートラルの認定資格です。
継続的なセキュリティモニタリングによるインシデントの検出、予防、レスポンスを任務とするサイバーセキュリティプロフェッショナル向けの認定資格です。

■現在のトレンドに関するスキルを証明する
クラウドやハイブリッド環境などさまざまに変化し、セキュリティに影響を与える IT トレンドに関するスキルを習得し、セキュリティアナリスト業務のスキルを証明することが可能です。

■プロアクティブなモニタリングと検出
脅威インテリジェンス、セキュリティ情報イベント管理（SIEM）、エンドポイントでの検知と対応（EDR）、拡張検知と対応（XDR）など最新の手法とツールを使用して、悪意のあるアクティビティの兆候を検知、分析するスキルを証明します。

■脅威、攻撃、脆弱性への対応
インシデントレスポンスと脆弱性管理プロセスに関する知識を証明し、セキュリティ分析とコンプライアンス遵守に不可欠となるコミュニケーションスキルを習得します。

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。

■ CompTIA CySA+ の取得

CompTIA CySA+ はサイバーセキュリティのテクノロジー職種で 4 年以上の実務経験で得られる知識やスキルを目安に設計されており、2 年の実務経験で得られる知識とスキルを目安に設計された CompTIA Security+ の次のキャリアとして最適な認定資格です。CompTIACySA+ を取得後は、5 ～ 10 年の実務経験で得られる知識とスキルを目安に設計された実践的なサイバーセキュリティスキルを習得できる CASP+ へのキャリアパスへとつながります。

CompTIA CySA+ 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。

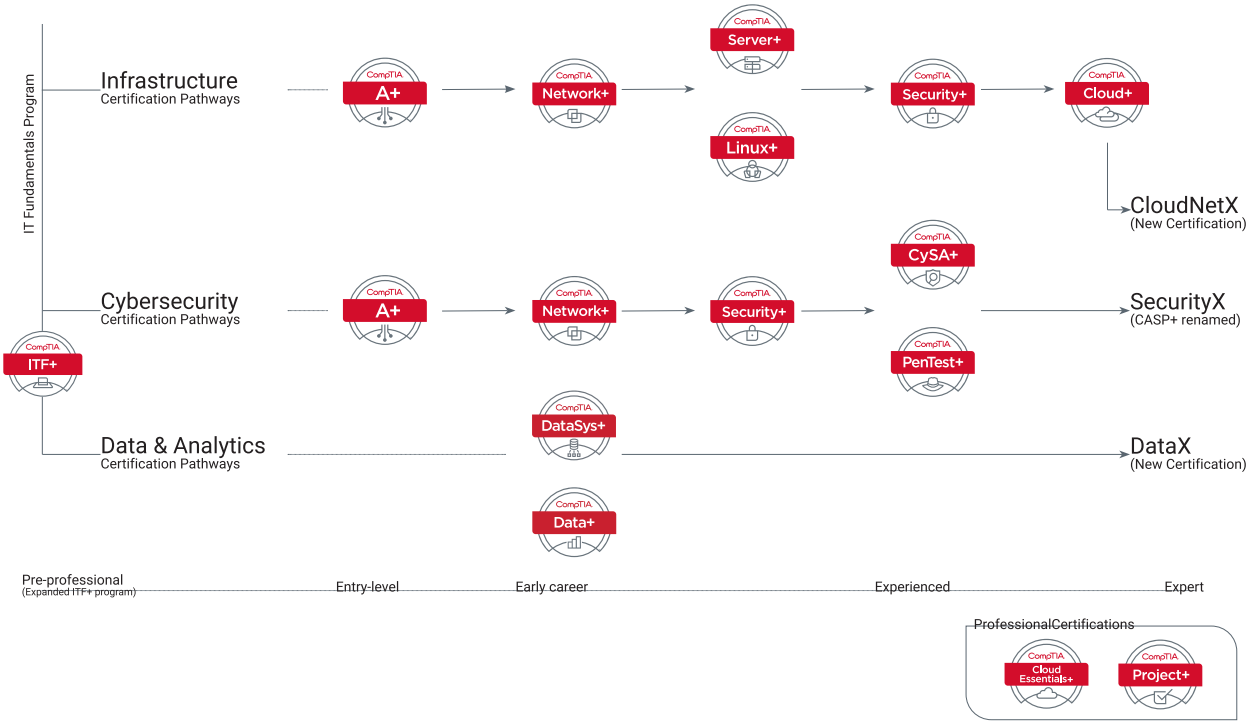
CompTIA CySA+ SME
■海外 / 一部抜粋
- Amazon Web Services
- Cisco
- Citrix Systems
- Indeed
- The Johns Hopkins University Applied Physics Laboratory
- Netflix
- Palo Alto Networks
- U.S. Department of Defense
- US Navy
- Visa
- Volkswagen Group of America

■日本（50 音順）
- NRI セキュアテクノロジーズ株式会社
- さくらインターネット株式会社
- トレンドマイクロ株式会社
- 株式会社ラック
- 釜山　公徳 氏

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 CySA+ の位置づけ



■ CompTIA CySA+ 出題範囲

CompTIA CySA+（CS0-003）		
1.0 セキュリティオペレーション	33%	• 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。 • 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。 • 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。 • 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。 • 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。
2.0 脆弱性管理	30%	• 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。 • 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。 • 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。 • 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。 • 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。
3.0 インシデントレスポンス・管理	20%	• 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。 • 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。 • 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。
4.0 報告とコミュニケーション	17%	• 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。 • 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。

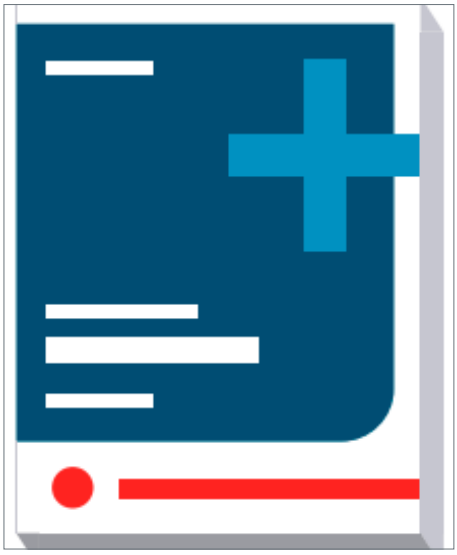
■ CompTIA CySA+ 試験概要

試験番号	問題数	制限時間	合格ライン
CS0-003	最大で 85 問	165 分	100 ～ 900 のスコア形式 750 以上

■ CompTIA CySA+ 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 CySA+ Self-Paced Study Guide（試験番号：CS0-003）日本語版



学習範囲
自学で学習を進める方向けのコンテンツです。最新の CompTIA CySA+ (CS0-003) 出題範囲を網羅しており、多くの図解を含む十分な情報量の理解しやすいコンテンツです。

含まれる内容
- 実際の業務に合わせたコンテンツ－すべてのトピックスは、業務上の職務に関連しており、レッスンでは実際の業務で発生する内容を取り上げています。
- 各トピックの最後にある確認問題で理解度を確認することができます。
- 重要な用語および頭字語の包括的用語集

学習内容
The Official CompTIA CySA+ Study Guide (CS0-003) は、CompTIA に よ って CompTIA 認定資格受験者のために開発されました。本書は、CompTIA CySA+（CS0-003）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 CySA+ の取得に必要なスキルを学習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。

- 脆弱性への対応、対処、管理について理解する
- 脅威インテリジェンスと脅威ハンティングのコンセプトを探る
- 重要なシステム・アーキテクチャとネットワークアーキテクチャの概念を説明する
- セキュリティオペレーションにおけるプロセス改善を理解する
- 脆弱性スキャン手法の導入
- 脆弱性分析の実施
- 脆弱性情報の伝達
- インシデント対応プロセスを説明する
- インシデントレスポンスコミュニケーションの実証
- 悪意のある活動を特定するツールを適用する
- 潜在的に悪質な活動を分析する
- アプリケーションの脆弱性評価を理解する
- スクリプトツールと分析コンセプトの探求
- アプリケーションセキュリティと攻撃軽減のベストプラクティスを理解する

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。

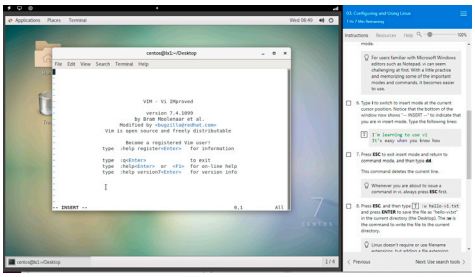
即戦力の育成に最適
CompTIA CertMaster Labs は、受講者が業務における実践的なスキルを育成する際に役立つと共に、CompTIA 認定資格試験を受験の際に、パフォーマンスベーステストを想定した準備のためにも役立ちます。

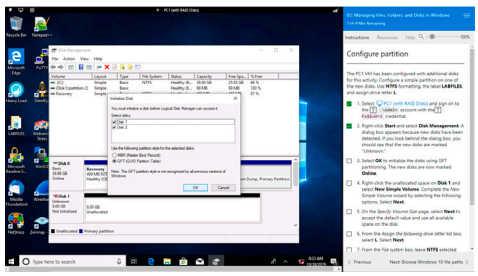
Officla CompTIA Content との高い親和性
CompTIA CertMaster Labs は、Official CompTIA Content のアクティビティに基づいており、知識と実践的なスキルの両方を習得するためのシームレスな学習体験を提供します。

CompTIA CertMaster Labs for Security+（CS0-003）

本 Labs には、以下の内容が含まれています。

- サポートラボ：ラボ環境を確認する
- サポートラボ：制御機能を構成する
- サポートラボ：IoC と脅威インテリジェンスの情報源を確認する
- サポートラボ：脅威ハンティングを実行する
- サポートラボ：一元管理型ロギングを構成する
- 応用ラボ：システム強化を行う
- サポートラボ：時刻同期エラーを評価する
- サポートラボ：自動化を構成する
- サポートラボ：アセットディスカバリーを行う
- サポートラボ：脆弱性スキャンを実行する
- サポートラボ：パッシブスキャンを実行する
- サポートラボ：コンテキスト認識を確立する
- サポートラボ：脆弱性レポートを分析する
- サポートラボ：レガシーシステムを検知する
- 応用ラボ：インシデント後のフォレンジック分析を実行する
- 応用ラボ：IoC の検出と分析を実行する
- 適応ラボプレイブックインシデント対応を実施する
- 応用ラボ：フォレンジックエビデンスを収集する
- サポートラボ：根本原因の分析を実施する
- 応用ラボ：ネットワークスニファを使用する
- 応用ラボ：DNS と IP 評判を調査する
- サポートラボ：ファイル分析手法を使用する
- サポートラボ：悪意のある可能性のあるファイルを分析する
- サポートラボ：従来型以外の脆弱性スキャンツールを使用する
- 応用ラボ：Web 脆弱性スキャンを実行する
- サポートラボ：弱い暗号をエクスプロイトする
- サポートラボ：ディレクトリトラバーサルとコマンドインジェクションを実行・検出する
- サポートラボ：特権エスカレーションを実行し検出する
- サポートラボ：XSS を実行し検出する
- サポートラボ：LFI/RFI を実行し検出する
- サポートラボ：SQLi を実行し検出する
- サポートラボ：CSRF を実行し検出する
- 応用ラボ：セキュリティ設定の誤りの検出と悪用





※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/