CompTIA

Certification Guide

CompTIA CySA+

Strengthen your organization's ablity to combat malware and threats with behavioral analytics.

■ 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。
ネットワークとデバイスのビヘイビア分析と継続的なセキュリティモニタリングからサイバーセキュリティの脅威を検出、防止、対処するスキルを証明します。

CompTIA CySA+ を取得することで、以下の必要な知識とスキルを有していることを証明します。

- インテリジェンスと脅威検知技術の活用
- データの分析と解釈
- 脆弱性の特定と対処
- 予防措置の提案
- インシデントへの効果的な対応と復旧

脅威インテリジェンスアナリスト、アプリケーションセキュリティアナリスト、コンプライアンスアナリスト、インシデントレスポンダー / ハンドラー、セキュリティオペレーションセンター（SOC）といった職務の人材に必要とされるセキュリティアナリストのコアスキルを網羅し、脅威に対応し続けるための最新手法についても習得することが可能です。

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+ は実務経験 4 年を想定しており、実務経験 2 年を想定して開発された 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、実務経験が 5 ～ 10 年を想定している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
- Citrix Systems
- Deloitte
- Department of Defense
- Indeed
- Netflix
- Nike
- Target
- The Walt Disney Company
- US Government
- Volkswagen Group of America

他多数

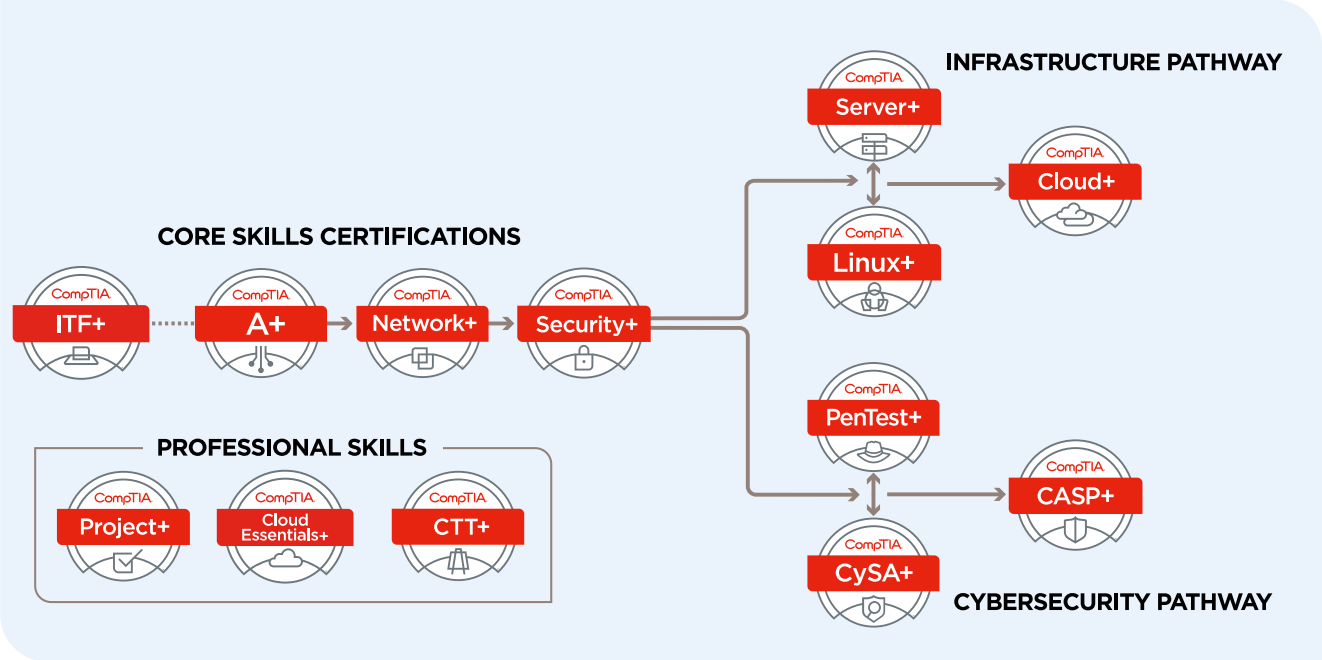
■日本（50 音順）

- NRI セキュアテクノロジーズ株式会社
- トレンドマイクロ株式会社
- 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 CySA+ の位置づけ



■ CompTIA CySA+ 出題範囲

CompTIA CySA+（CS0-002）		
1.0 脅威および脆弱性マネジメント	22%	• 脅威データとインテリジェンスの重要性を説明することができる。 • 与えられたシナリオに基づいて、脅威インテリジェンスを使用して組織のセキュリティをサポートすることができる。 • 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。 • 与えられたシナリオに基づいて、一般的な脆弱性アセスメントツールからの出力を分析することができる。 • 特定のテクノロジーに関連する脅威と脆弱性を説明することができる。 • クラウド運用に関連する脅威と脆弱性を説明することができる。 • 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実装することができる。
2.0 ソフトウェアおよびシステムセキュリティ	18%	• 与えられたシナリオに基づいて、インフラストラクチャマネジメントのためのセキュリティソリューションを適用することができる。 • ソフトウェアアシュアランスのベストプラクティスを説明することができる。 • ハードウェア保証のベストプラクティスを説明することができる。
3.0 セキュリティオペレーションおよびモニタリング	25%	• 与えられたシナリオに基づいて、セキュリティモニタリングアクティビティの一環としてデータ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、セキュリティを向上させるために既存のコントロールへ構成変更を実装することができる。 • プロアクティブな脅威ハンティングの重要性を説明することができる。 • 自動化の概念とテクノロジーを比較対照することができる。
4.0 インシデントレスポンス	22%	• インシデントレスポンスプロセスの重要性を説明することができる。 • 与えられたシナリオに基づいて、適切なインシデント対応プロセスを適用することができる。 • 想定されたインシデントに基づき、潜在的なセキュリティ侵害インジケーター（IoC）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、基本的なデジタルフォレンジックテクニックを使用することができる。
5.0 コンプライアンスおよびアセスメント	13%	• データのプライバシーと保護の重要性を理解する。 • 与えられたシナリオに基づいて、組織のリスク軽減をサポートするセキュリティコンセプトを適用することができる。 • フレームワーク、ポリシー、プロシージャー、およびコントロールの重要性を説明することができる。

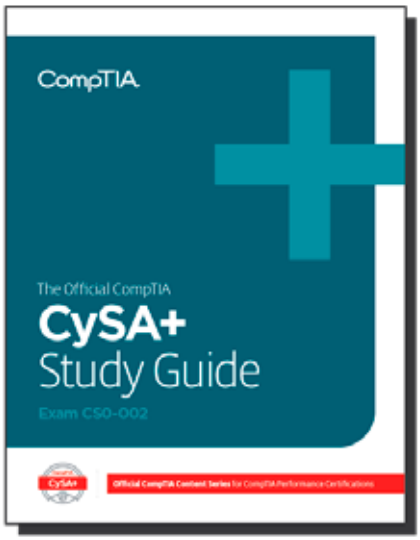
■ CompTIA CySA+ 試験概要

試験番号	問題数	制限時間	合格ライン
CS0-002	最大で 90 問	90 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：CS0-002）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 CySA+（CS0-002）出題範囲を網羅しており、多くの図解を含んでおり、充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。重要な用語と略語用語集

学習内容
The Official CompTIA CySA+（CS0-002）Study Guide 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 CySA+ 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+ 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。

- セキュリティコントロールとセキュリティインテリジェンスの重要性を説明する
- 脅威データとインテリジェンスを活用する
- セキュリティモニタリングデータを分析する
- セキュリティモニタリングデータの収集とクエリを実行する
- デジタルフォレンジックとインジケーター分析テクニックを活用する
- インシデントレスポンス手順を適用する
- リスク軽減とセキュリティフレームワークを適用する
- 脆弱性マネジメントを実行する
- インフラストラクチャ管理にセキュリティソリューションを適用する
- データのプライバシーとプロテクションを理解する
- ソフトウェアアシュアランスのためセキュリティソリューションを適用する
- クラウドと自動化にセキュリティソリューションを適用する

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

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

■ CompTIA CySA+ トレーニング教材：CompTIA Labs

CompTIA 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 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 Lab 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 Lab 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。

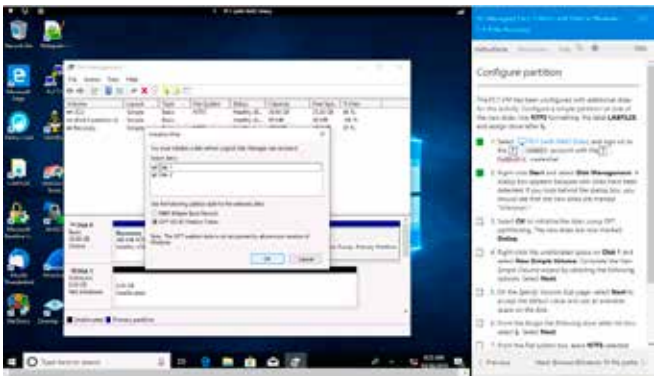
即戦力の育成に最適
CompTIA Lab は、受講者が業務における実践的なスキルを育成する際に役立つと共に、CompTIA 認定資格試験を受験の際に、パフォーマンスベーステストを想定した準備のためにも役立ちます。

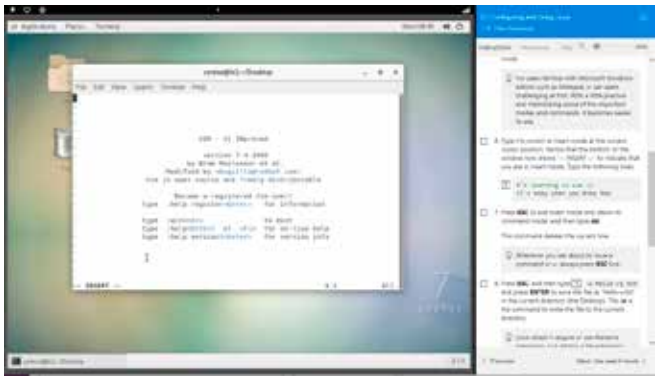
Officla CompTIA Content との高い親和性
CompTIA Lab は、Official CompTIA Content のアクティビティに基づいており、知識と実践的なスキルの両方を習得するためのシームレスな学習体験を提供します。

CompTIA Labs for CySA+（CS0-002）

本 Lab には、以下の内容が含まれています。

- ネットワークセキュリティモニタリングツールからの出力の分析
- ラボ環境の構築
- セキュリティアプライアンスから出力されたログの分析
- エンドポイントセキュリティモニタリングツールからの出力の分析
- 電子メールヘッダーの分析
- SIEM エージェントとコレクターの構成
- イベントログと syslog 出力の分析、フィルタリング、検索
- デジタル証拠の収集と検証
- ネットワーク関連の IoC の分析
- ホストとアプリケーションの IoC の分析
- セキュリティインシデント中の IoC のモニタリング
- トポロジおよびホストエニュメレーションツールからの出力の分析
- 資格情報のセキュリティテスト
- 脆弱性スキャンの構成と出力の分析
- 脆弱性スキャン出力の評価
- 脆弱性管理に対する規制の影響評価
- アカウントと権限の監査の実行
- ネットワークセグメンテーションとセキュリティの構成
- 共有権限の構成と分析
- Web アプリケーションの脆弱性の影響評価
- Web アプリケーション評価ツールからの出力の分析
- クラウドインフラストラクチャ評価ツールからの出力の分析





※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 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