CompTIA

Certification Guide

CompTIA PenTest+

Go on Cyber Offense with PenTest+ Certification

■ CompTIA PenTest+ とは

CompTIA PenTest ＋は、ネットワーク上の脆弱性を特定、報告、管理するための実践的なペネトレーションテストを行う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。

CompTIA PenTest+ は、ペネトレーションテストの手法、脆弱性評価、また攻撃があった際のネットワークを回復するために必要となるスキルを評価します。効率的に作業を進めるためにフレームワークをカスタマイズし、結果を適切に報告すると共に、IT セキュリティ全般的な状態の改善を図るための戦略を提案できるスキルとベストプラクティスを育成します。
また、従来のデスクトップやサーバーに加えて、クラウドやモバイルなどの新しい環境でデバイスをテストするための実践的なスキルと知識も評価することが可能です。

■ CompTIA PenTest+ の取得

CompTIA PenTest ＋は、最新のペネトレーションテスト、攻撃に対するネットワークのレジリエンスを維持するために必要な脆弱性評価および管理スキルを評価します。
CompTIA PenTest+ を取得することで、効率的に作業を進める上で必要な評価フレームワークをカスタマイズし、結果を適切に報告するためのスキルを証明します。実践的なペネトレーションテストの手法と、脆弱性評価をカバーしているだけではなく、セキュリティ管理上の弱点となりうる点への改善計画、実装、管理をするためのスキルが網羅されています。また、従来の PC やサーバー環境に加えて、クラウドやモバイルなどの新しい環境でデバイスをテストを実施するための実践的なスキルと知識が含まれています。

CompTIA PenTest+ は、サイバーセキュリティのキャリアパスにおいて、CompTIA CySA+ と共に中級のスキルに位置されます。

CompTIA CySA+ が、インシデントの検出と対応による「防御」に重点を置いているのに比べ、CompTIA PenTest+ は、ペネトレーションテストと脆弱性診断による「攻撃」に重点を置いています。これら 2 つの認定資格は、一見反するスキルのように見えますが、依存関係にあると言えます。サイバーセキュリティにおいて高いスキルを有するためには、これら 2 つの「防御」と「攻撃」の両方のスキルを備えている必要があります。

CompTIA PenTest+ 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**が出題されます。

" 業界の業界による
業界のための資格”

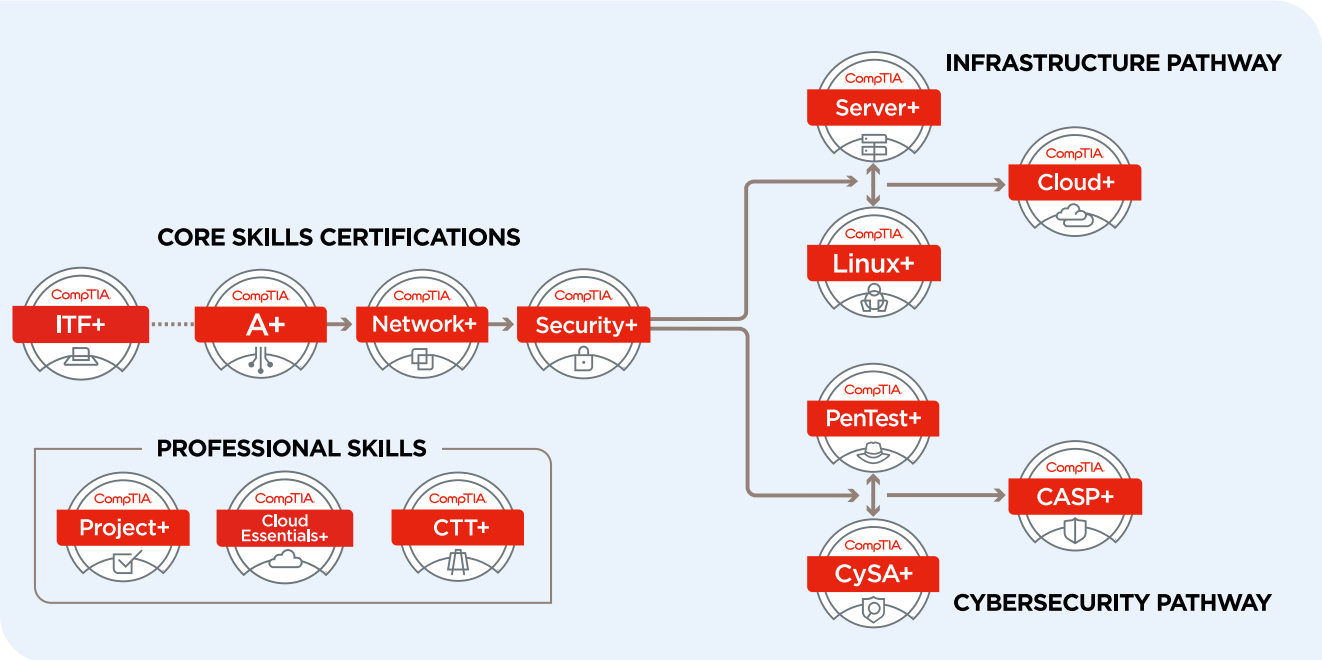
CompTIA 認定資格は、試験作成委員会が中心となり、ニーズ調査・職務分析・リサーチを経て、SME（サブジェクトマターエキスパート）と呼ばれる現場関係者により開発が進められます。

CompTIA PenTest+ SME
■海外 / 一部抜粋
- ASICS
- Accenture Security
- Deloitte Ireland
- Hacktive Security
- Las Vegas Sands Corporation
- Paylocity

■日本（50 音順）
- S&J 株式会社
- NRI セキュアテクノロジーズ株式会社
- 自衛隊指揮通信システム隊

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 PenTest+ の位置づけ



■ CompTIA PenTest+ 出題範囲

CompTIA PenTest+（PT0-001）		
1.0 計画とスコープ	15%	• エンゲージメントを計画することの重要性を説明することができる。 • 主要な法的概念を説明することができる。 • エンゲージメントに対する適切なスコープの重要性を説明することができる。 • コンプライアンスに基づく評価の重要な側面について説明することができる。
2.0 情報収集と脆弱性の識別	22%	• 与えられたシナリオに基づき、適切な手法を用いて情報収集を行うことができる。 • 与えられたシナリオに基づき、脆弱性スキャンを実行することができる。 • 与えられたシナリオに基づき、脆弱性スキャン結果を分析することができる。 • エクスプロイトの準備に情報を活用するプロセスを説明することができる。 • 特化したシステムに関連する弱点を説明することができる。
3.0 攻撃とエクスプロイト	30%	• ソーシャルエンジニアリング攻撃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き、ネットワークベースの脆弱性を利用することができる。 • 与えられたシナリオに基づき、ワイヤレスと RF ベースの脆弱性を利用することができる。 • 与えられたシナリオに基づき、アプリケーションベースの脆弱性を利用することができる。 • 与えられたシナリオに基づき、ローカルホストの脆弱性を利用することができる。 • 施設に関連する物理的なセキュリティ攻撃を要約することができる。 • 与えられたシナリオに基づき、エクスプロイト後のテクニックを実行することができる。
4.0 ペネトレーションテストツール	17%	• 与えられたシナリオに基づき、Nmap を使って情報収集演習を実施することができる。 • さまざまなツールの使用例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き、ペネトレーションテストに関連するツールからのアプトプットや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き、基本的なスクリプト（Bash、Python、Ruby、PowerShell に限る）を分析することができる。
5.0 報告とコミュニケーション	16%	• 与えらえたシナリオに基づき、レポートの作成とベストプラクティスを使用することができる。 • レポート後の実施アクティビティを説明することができる。 • 与えられたシナリオに基づき、発見された脆弱性に対する軽減戦略を提案することができる。 • ペネトレーションテストのプロセスにおけるコミュニケーションの重要性を説明することができる。

■ CompTIA PenTest+ 試験概要

試験番号	問題数	制限時間	合格ライン
PT0-001	最大で 90 問	165 分	100 ～ 900 のスコア形式 750 以上

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

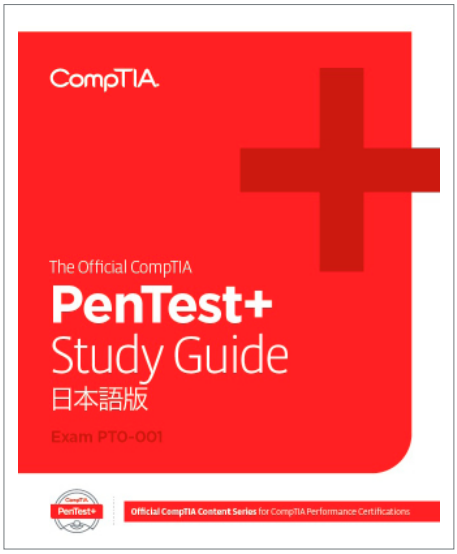
学習範囲
自学で学習を進める方向けのコンテンツです。最新の CompTIA PenTest+（PT0-001）出題範囲を網羅しており、多くの図解を含んでおり、充分な情報量の理解しやすいコンテンツです。

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 PenTest+（PT0-001）Student 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、PenTest+ 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、PenTest+ 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。

- ペネトレーションテストの計画とスコープ
- パッシブ偵察の実行
- 情報収集のための非テクニカルテストの実施
- アクティブ偵察の実行
- 脆弱性の分析
- ネットワークの侵入
- ホストベース脆弱性のエクスプロイト
- テストアプリケーション
- ポストエクスプロイトタスクの完了
- ペネトレーションテスト結果の分析と報告



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

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