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。様々な IT 環境での攻撃対象領域がカバーされており、クラウド、ハイブリッド、Web アプリケーション、IoT、オンプレミスなどに関連するペネトレーションテストのスキルとそれぞれの実施計画、報告などのスキルを評価します。
CompTIA PenTest+ は 3 ～ 4 年間の ペネトレーションテスト、脆弱性評価、および脆弱性管理の実践経験で得られる知識やスキルを目安に設計されています。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。

■ CompTIA PenTest+ の取得

CompTIA PenTest ＋は、最新のペネトレーションの手法やネットワークのレジリエンスを判断するために必要となる脆弱性評価と管理などのスキルを評価します。
改訂 CompTIA PenTest+ を取得することで、下記のようなスキルと知識を習得していることを証明します。

・ペネトレーションテストの実施を計画、スコープ設定する
・法的要件とコンプライアンス要件を理解する
・適切なツールと手法を使用して脆弱性スキャンとペネトレーションテストを実施する
・ペネトレーションテストの結果を分析する
・提案すべき修復の手法を含むレポートを作成し、結果を効率的に伝え、実用的な推奨事項を提示する

CompTIA PenTest+ は、世界的に認知される品質規格に準拠しているとして、2011 年 12 月 31 日に、国際標準化機構 (ISO) および米国規格協会 (ANSI) より認定を受けています。また、米国国防総省によって指令 8140/8570.01-M 要件を満たすことが承認されています。

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
- Amazon Web Services
- IBM
- Johns Hopkins University Applied Physics Laboratory
- Las Vegas Sands Corporation
- NTT
- SecureWorks
- Trend Micro

■日本（50 音順）
- NTT コミュニケーションズ株式会社
- NRI セキュアテクノロジーズ株式会社
- 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 PenTest+ の位置づけ

■ CompTIA PenTest+ 出題範囲

CompTIA PenTest+（PT0-002）		
1.0 計画とスコープ	14%	• ガバナンス、リスク、コンプライアンスの概念を比較対照することができる。 • スコープ、組織 / 顧客要件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、プロフェッショナリズムと完全性を維持することによって、倫理的ハッキングマインドセットを実証することができる。
2.0 情報収集と脆弱性のスキャン	22%	• 与えられたシナリオに基づいて、パッシブな偵察を実施することができる。 • 与えられたシナリオに基づいて、アクティブな偵察を実施することができる。 • 与えられたシナリオに基づいて、偵察の結果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、脆弱性スキャンを実行することができる。
3.0 攻撃とエクスプロイト	30%	• 与えられたシナリオに基づいて、攻撃ベクターを調査し、ネットワーク攻撃を実施することができる。 • 与えられたシナリオに基づいて、攻撃ベクターを調査し、ワイヤレス攻撃を実施することができる。 • 与えられたシナリオに基づいて、攻撃ベクターを調査し、アプリケーションベース攻撃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、攻撃ベクターを調査し、クラウド技術での攻撃を実施することができる。 • 特化したシステムに対する共通攻撃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、ソーシャルエンジニアリングまたは物理攻撃を実行することができる。 • 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 報告とコミュニケーション	18%	• レポートの重要な要素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、発見事項を分析し、レポート内の適切な修復を推奨することができる。 • 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。 • 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。
5.0 ツールとコード分析	16%	• スクリプトとソフトウェア開発の基本概念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、ペネトレーションテストで使用するスクリプトまたはコードのサンプルを分析することができる。 • ペネトレーションテストのフェーズにおいて次のツールの用途を説明することができる。 （** この出題範囲は、特定ベンダーの機能をテストすることではありません。）

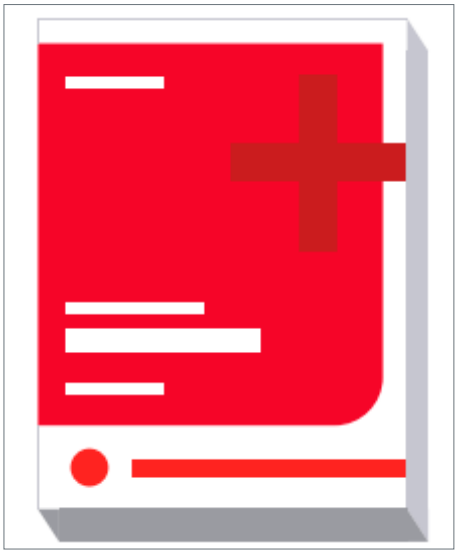
■ CompTIA PenTest+ 試験概要

試験番号	問題数	制限時間	合格ライン
PT0-002	最大で 85 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：PT0-002) 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 PenTest+ (PT0-002) 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。
- 重要な用語と略語集

学習内容
The Official CompTIA PenTest+ Study Guide (PT0-002) 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 PenTest+ (PT0-002) 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 PenTest+ 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。

- 組織 / 顧客要件のスコープを策定する
- エンゲージメントのルールを定義する
- フットプリントとインテリジェンスを収集する
- 人的および物理的な脆弱性を評価する
- 脆弱性スキャンを準備する
- 論理的な脆弱性をスキャンする
- スキャン結果を分析する
- 検出回避と回避手法を理解する
- LAN とクラウドを活用する
- ワイヤレスネットワークをテストする
- モバイルデバイスをターゲットにする
- 特殊なシステムを攻撃する
- Web アプリケーションベースの攻撃
- システムハッキングを実行する
- スクリプトとソフトウェア開発
- 攻撃を活用：ピボットとペネトレーション
- ペネトレーションテスト中にコミュニケーションをとる
- レポートコンポーネントを要約する
- 修正事項を推奨する
- レポート後の配信アクティビティを実行する

The Official CompTIA Contents 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