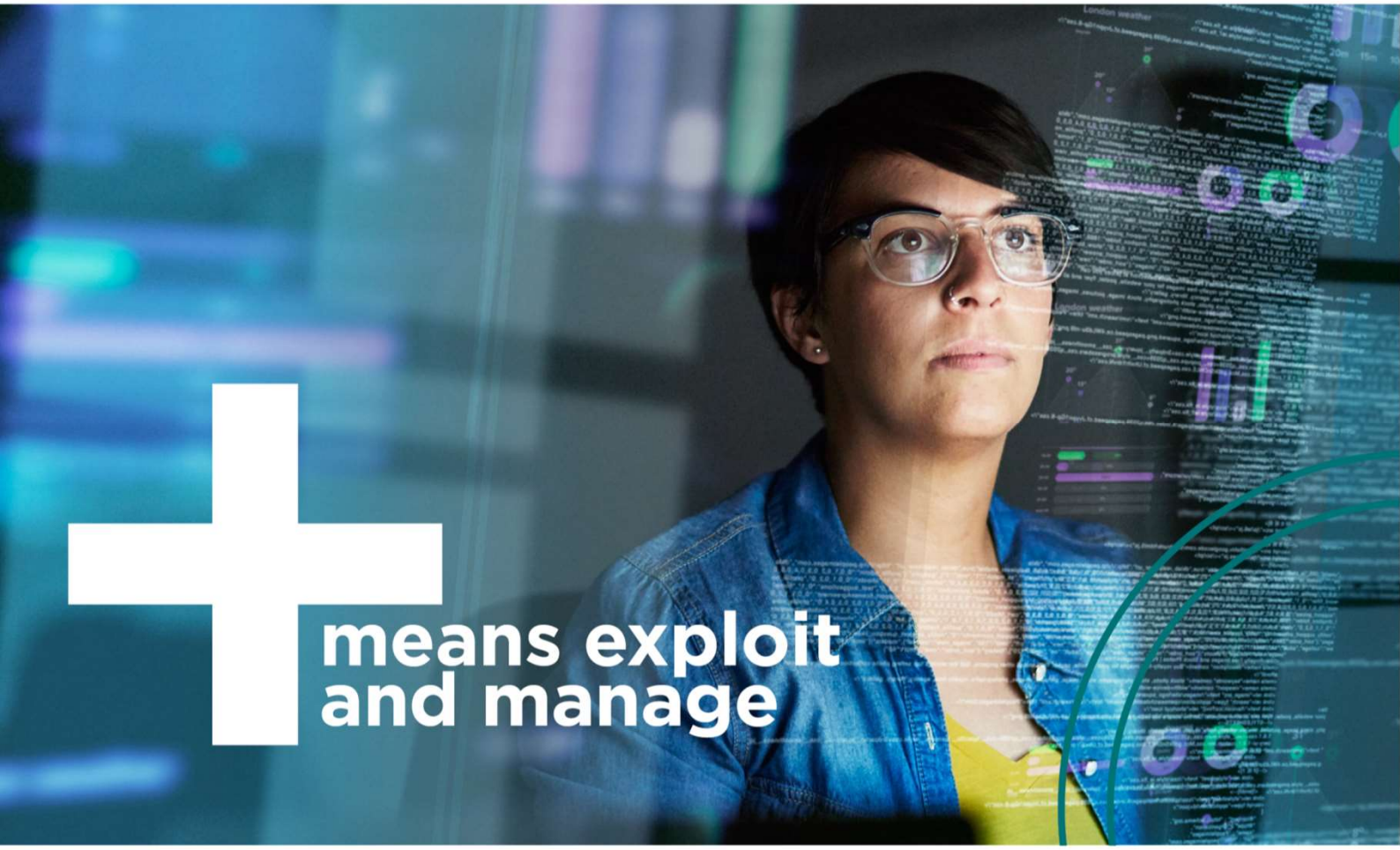
CompTIA



CompTIA PenTest+ PT0-001とPT0-002 出題範囲の比較

サイバー犯罪は、年々急速に増加の一途をたどっており、その結果、より多くのIT職務において、より広い範囲にわたって脆弱性の特定や修復手法を担当するようになりました。また、機密データが悪用されることを防ぐため、組織がよりオフェンシブな戦略を取り続ける中、ネットワークとセキュリティに対して、プロアクティブにテストを実施できるスキルを持ったITプロフェッショナルのニーズは、かつてない程高まっています。
改訂CompTIA PenTest+では、攻撃に対するネットワークのレジリエンスを判断するために必要とされるスキルを評価できるように、最新のペネトレーションテストや脆弱性評価、マネジメントスキルを評価します。

CompTIA PenTest+（PT0-002）では、クラウド、ハイブリッド環境、Webアプリケーションなどの最新の攻撃対象に対するペネトレーションテストの手法、倫理的なハッキングコンセプト、脆弱性スキャン、コード解析などのスキルを評価できるように更新されています。さらに、サイバーセキュリティのプロフェッショナルが一時的な対応をするのではなく、計画、スコープ、マネジメントのためのベストプラクティスや最新の手法を学習することで、組織のセキュリティを強化し、次の攻撃を防止するための策を講じるスキルを習得することができます。

CompTIA PenTest+は、ISO/IEC 17024規格に準拠していることをANSIにより認証されています。
また、米国国防総省指令 8570.01(DoD Directive 8570.01)により承認され、連邦情報セキュリティ管理法（FISMA）に基づく政府規制に準拠しています

CompTIA PenTest+

CompTIA

出題範囲の比較

下記の表は、CompTIA PenTest+ PT0-002とPT0-001の出題範囲の比較表です。

PT0-001	PT0-002	RESULTS
1.2 主要な法的概念を説明することができる。	1.1 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。	Maps
1.4 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。	1.1 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。	Maps
1.3 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。	1.2 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。	Gap
n/a	1.3 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。	New Content
2.1 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。	2.1 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。	Maps
2.1 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。	2.2 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。	Maps
n/a	2.3 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。	New Content
2.2 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。	2.4 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。	Maps
4.1 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。	2.4 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。	Maps
3.2 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。	3.1 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。	Maps
3.3 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。	3.2 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。	Maps
3.4 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。	3.3 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。	Maps
n/a	3.4 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。	New Content
n/a	3.5 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。	New Content
3.1 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。	3.6 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。	Gap

PT0-001	PT0-002	RESULTS
3.6 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。	3.6 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。	Gap
3.7 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。	3.7 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。	Maps
2.1 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。	3.7 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。	Maps
5.1 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。	4.1 レポートの重要な要素を比較対照することができる。	Maps
5.3 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。	4.2 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。	Gap
5.4 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。	4.3 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。	Maps
5.2 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。	4.4 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。	Maps
n/a	5.1 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。	New Content
4.4 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。	5.2 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。	Maps
4.2 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。	5.3 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。	Maps