コースコード：CO-SECURITYX
税込価格：280,500円 (税抜価格：255,000円)
日数：3日間

トレーニング内容

本トレーニングは、2026年4月より
受講価格を改定いたします。価格改定の詳細については以下をご確認ください。
一部トレーニング 受講価格改定のお知らせ

CompTIA SecurityXは、セキュリティアーキテクトおよびシニアセキュリティエンジニア向けの高度なサイバーセキュリティ認定資格です。エンタープライズ内の複雑な環境全体にわたってセキュアなソリューションを設計、構築、実装するスキルを証明します。また、ガバナンス、リスク、コンプライアンスのニーズに対応しながら、レジリエンスの高い環境を維持するスキルを有していることも証明できます。

ここに注目!!

CompTIA SecurityX (CAS-005) の公式カリキュラム (5日間) と教材をベースに、ご受講いただきやすいよう3日間に短縮したトレーニングです。試験対策に特化したトレーニングではございませんのでご注意ください。

SecurityX（2024年12月以前の名称はCASP+ (CompTIA Advanced Security Practitioner)）認定資格（試験番号：CAS-005）は、企業や組織でより高度なセキュリティ分野を担当するセキュリティアーキテクトや上級セキュリティエンジニアなどのセキュリティ実務者を対象にした認定資格です。

SecurityX試験の詳細については、こちらをご覧ください。

本トレーニングは、経済産業省が認定する「第四次産業革命スキル習得講座認定制度 (Reスキル講座)」認定講座です。
「人材開発支援助成金」対象講座です。詳細は こちら (経済産業省Webページ)
※本制度の認定講座では、講座修了時および受講後6～12ヶ月後に、経済産業省規定のアンケート項目へ回答するよう定められています。受講者様におかれましては、ご理解ご了承のほどよろしくお願いいたします。

※受講証明書（修了証）は、70%以上の出席率を満たしているお客様に発行します。

本トレーニング以外のセキュリティ関連トレーニングは以下でご紹介しています。
セキュリティトレーニング

ワンポイントアドバイス

受講対象者

このコースの受講対象者は次の通りです。

・SecurityX 認定資格 (試験番号：CAS-005)の取得を目指す方
・IT全般の管理者として10年以上の経験、そのうち5年以上をセキュリティに関連する実務で得られる知識やスキルと同等のレベルを証明したい方

前提条件

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

IT全般の管理者やエンジニアとして10年以上の経験、そのうち5年以上をセキュリティに関連する実務で得られる知識やスキル (目安)

下記のコースを受講済み、または同等の知識を有する方

CompTIA Security+ 任意、受講されていれば望ましい
CompTIA Cybersecurity Analyst (CySA+) 任意、受講されていれば望ましい
CompTIA PenTest+ 任意、受講されていれば望ましい

目的

このコースを修了すると次のことができるようになります。

・複雑な環境全体にわたり、セキュアなソリューションの設計、構築、統合、実装を行い、レジリエンスのある企業をサポートする
・自動化、モニタリング、検出、インシデント対応を使用して、企業の環境で継続的なセキュリティ運用をプロアクティブにサポートする
・クラウド、オンプレミス環境、ハイブリッド環境でセキュリティ対策を適用する
・暗号技術や手法、（例：人工知能）新たなトレンドの影響が、情報セキュリティに与える影響を考慮する
・企業全体にわたり、適切なガバナンス、コンプライアンス、リスク管理、脅威モデリング戦略を活用する

アウトライン

ガバナンス、リスク、コンプライアンスの概要

適切なガバナンスコンポーネントの実装

法令遵守の説明

リスク管理戦略の適用

アーキテクチャと設計の実装

- ソフトウェア開発の応用
- ソフトウェアアーキテクチャの統合
- 運用上のレジリエンスへの対応
- クラウドインフラストラクチャの実装
- ゼロトラストの概念の統合
- AAAとIAMを使用するトラブルシューティング

セキュリティエンジニアリングの理解

- エンドポイントセキュリティの強化
- ネットワークインフラストラクチャの構成
- セキュリティ自動化の開始
- 暗号概念の適用

セキュリティ運用とインシデント対応の実施

- 脅威モデリングの実行
- セキュリティ監視の検証
- 既知の攻撃手法とそれに対応する是正対策の分析
- 脅威ハンティングのツールと技術の応用
- インシデント分析と対応の評価