AWS Security Essentials

AWS クラスルームトレーニング

コースの説明

このコースでは、AWS クラウドのセキュリティに関する基礎概念について取り上げます。これには AWS のアクセスコントロール、データ暗号化方式、AWS インフラストラクチャへのネットワークアクセスを保護する方法などが含まれます。このコースの内容は、AWS の共有責任モデルを反映した以下の 2 つの主要セクションに分かれています。

- クラウドのセキュリティ
- クラウド内のセキュリティ

AWS クラウドにおけるセキュリティに対して AWS が担う責任とお客様が担う責任について説明し、AWS クラウド内でお客様がセキュリティを実装する責任を担う対象、利用可能なセキュリティサービス、そうしたセキュリティサービスが組織のセキュリティニーズを満たすのに役立つ理由とその方法について学びます。 また、受講者が AWS のリソースとインフラストラクチャを安全に保護する方法を学べる、ガイド付きのハンズオンも用意されています。

レベル	実施形式	所要時間
基礎	クラスルームトレーニング、ハンズオンラボ	1 日

コースの目標

このコースの学習内容は以下のとおりです。

- AWS クラウドを使用する際のセキュリティ上の利点と責務を認識する
- AWS のアクセスコントロール機能とアクセス管理機能について説明する
- AWS にデータを保存する際、転送時と保管時のデータの暗号化に使用できる方法について説明する
- AWS リソースへのネットワークアクセスを保護する方法について説明する
- モニタリングとインシデント対応に使用できる AWS のサービスを判断する

対象者

このコースは以下のような方を対象としています。

aws training and certification

AWS Security Essentials

AWS クラスルームトレーニング

- クラウドのセキュリティプラクティスに興味がある、IT ビジネスレベルのセキュリティプロフェッショナル
- AWS についてほとんどまたはまったく実務的知識のないセキュリティプロフェッショナル

前提条件

このコースを受講するにあたって、以下の前提条件を満たしておくことをお勧めします。

- IT セキュリティプラクティスとインフラストラクチャの概念に関する実務的知識、クラウドコンピューティングの概念に関する知識

登録

https://www.aws.training/training/schedule?courseId=44517&countryName=JP&trainingProviderId=1

コースの概要

モジュール 1: AWS のセキュリティ

- AWS クラウドにおけるセキュリティの設計原則
- AWS の責任共有モデル

モジュール 2: クラウドのセキュリティ

- AWS グローバルインフラストラクチャ
- データセンターのセキュリティ
- コンプライアンスとガバナンス

モジュール 3: クラウド内のセキュリティ – パート 1

- アイデンティティとアクセスの管理
- データ保護の基本
- ラボ 1 – セキュリティポリシーの概要

モジュール 4: クラウド内のセキュリティ – パート 2

- インフラストラクチャの保護

AWS Security Essentials

AWS クラスルームトレーニング

- モニタリングと発見的統制
- ラボ 2 – セキュリティグループを使用して VPC リソースを保護する

モジュール 5: クラウド内のセキュリティ – パート 3

- DDoS の緩和
- インシデント対応の基本
- ラボ 3 – AWS Config コンフォーマンスパックを使用して問題を修正する

モジュール 6: コースのまとめ

- AWS Well-Architected Tool の概要