

コースコード：CO-DATASYSPLUS
税込価格：170,500円 (税抜価格：155,000円)
日数：3日間

ここに注目!!

CompTIA DataSys+ は、セキュリティと事業継続のベストプラクティスを実践しながら、データベース環境におけるスクリプトとプログラミングの基礎を採用することを含め、データベースの展開、管理、メンテナンスに必要な知識とスキルを評価します。

データベース管理者として2~3

年間の実務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。

本トレーニング以外のデータ分析関連トレーニングは以下でご紹介しています。

[データ分析 / AI / IoT / RPA](#)

受講対象者

このトレーニングはこのような方におすすめです。

データベース管理者としての職務に必要な知識とスキルを養成するために、受講が推奨される初級トレーニングです。

職務として1種類以上のデータシステムのデータを管理、保守、保護して、データの保管、体系化、ストレージ、提示、使用率、分析などを技術的視点から考慮する際に、必要となります。

CompTIA DataSys+ (試験番号：DS0-001)認定試験の準備のために受講することができます。

前提条件/前提知識

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。

このトレーニングを確実に修了するには、2年から3年のデータベース管理者としての実務経験があることが望ましいとされています。

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。

- ・ データベースの種類と構造を理解できる
- ・ 標準とコマンドを識別できる
- ・ データとデータシステム向けのスクリプトを実行する
- ・ プログラミングがデータベースの動作に与える影響を説明できる
- ・ データベース操作におけるプログラミング上の影響を説明する
- ・ データベースの計画と設計を理解できる
- ・ データベースを実装し、テストし、展開できる
- ・ データベース性能を監視し、報告できる
- ・ 共通のデータ保守処理を理解できる
- ・ ガバナンスと法規制遵守を理解できる
- ・ データを保護できる
- ・ データアクセスを保護できる
- ・ データベースとサーバーを保護できる
- ・ 攻撃の種類を分類できる



- ・ディザスタリカバリ（災害からの復旧計画）を計画できる
- ・バックアップとリストアのベストプラクティス（最善の方法）を実装できる

アウトライン

データベースの種類と構造の理解

リレーショナルデータベースと非リレーショナルデータベースの区別

NoSQLデータベースとツールのさまざまな種類の理解

リレーショナルデータベースの設計の理解

その他のデータシステムの識別

標準とコマンドの認識

標準と原則の理解

オペレーティングシステムとコマンドラインスクリプティングの試験

データとデータシステムでのスクリプト実行

データ定義言語を使用したオブジェクトの作成および変更

データ操作言語（DML）を用いたデータ操作

トランザクションの取り扱い

データ管理タスクの実施

プログラミングがデータベースの動作に与える影響

ビューによる操作

Object-Relational Mappingの理解

SQLでのプログラミング

関数の記述



データベースの計画と設計の理解

アーキテクチャの種類を理解

データシステム要件の収集

ドキュメント要件の確認

データベースの実装、テスト、展開

展開の準備

テストおよびその他の品質対策の実施

検証のテクニックと方法の理解

データベースパフォーマンスに関する監視とレポート

データベース接続のニーズを検討する

データベースの監視

デッドロックに関する理解と対処

共通のデータ保守処理の理解

パッチ処理についての説明

データベースパフォーマンスの保証

データベース整合性の保証

ガバナンスと法令順守の理解

データ保護とデータ損失防止の重要性の理解

データ保持ポリシーの理解

データの分類

グローバルな司法権と地域の規制に関する考慮

第三者契約とリリース承認の理解

データ保護

データの暗号化

データマスキング

データ破壊手法の説明

データアクセスの監査

コードと変更の監査

データアクセスの保護

Identity and Access Management (IAM) を理解する

アクセス制御を理解する

パスワードポリシーの理解

サービスアカウントの取り扱い

データベースとサーバーの保護

物理セキュリティの活用

論理セキュリティの活用

攻撃の種類のカテゴリ

SQLインジェクション攻撃への対処

サービス拒否 (DoS) 攻撃への対処

オンパス攻撃への対処

ブルートフォース攻撃への対処



ソーシャルエンジニアリング攻撃への対処

マルウェアへの対処

ディザスタリカバリ（災害からの復旧）計画

ディザスタリカバリ（DR）の計画

DR計画のテスト実施

通常の業務への移行 / フェイルバック

バックアップとリストアのベストプラクティスの実装

バックアップの種類の特定

バックアップ戦略の実装

バックアップの保管とパージ