Google Cloud

Professional Google Workspace Administrator

認定試験ガイド

Professional Google Workspace 管理者は、ユーザー、コンテンツ、統合について統括的に考慮しながらビジネス目標を具体的な Google Workspace 構成、ポリシー、セキュリティ対策に変換します。Google Workspace 管理者は、組織のインフラストラクチャに関する知識を活かして、安全かつ効率的な方法で、共同作業、データ通信、データへのアクセスができるように支援します。エンジニアリングとソリューションの視点を持って業務に取り組む Google Workspace 管理者は、ツール、プログラミング言語、API を使用して、ワークフローの自動化、エンドユーザーの教育、業務効率を向上させながら、Google Workspace とツールセットをサポートします。

関連する職務: IT システム管理者、クラウド ソリューション エンジニア、コラボレーション エンジニア、システム エンジニア。

セクション 1: オブジェクトの管理（試験内容の 20% 以下）

1.1 プロビジョニング プロセスとデプロビジョニング プロセスを使用したアカウントのライフサイクルの管理。以下のような点を考慮します。

- 所有権データの別のアカウントへの移行
- 組織のポリシーによって決定されたプロセス（アカウントのリスト表示など）に基づくユーザーのプロビジョニング
- 次のようなアカウントのプロビジョニングとデプロビジョニング
    - アカウントの作成、確認、更新、削除（CRUD [作成、読み取り、更新、削除] オペレーション）。
    - ユーザーの追加（例: 個別、一括、自動）
    - アカウントのオフボーディング（例: 停止、削除、復元）
    - ユーザー属性の編集（例: 名前変更、パスワード、エイリアス）
    - 管理者ロールの作成（例: デフォルト ロール、カスタムロール）
- 一般的な組織のポリシーの外でのアカウントへのアクセスの取り消し（例: セキュリティの理由や人員の問題）

- Google Cloud Directory Sync（GCDS）を使用したライフサイクル管理の構成、モニタリング、トラブルシューティング、更新

    - GCDS の監査と確認（例: ログデータの解釈）

1.2 Google ドライブの構成。以下のような点を考察します。

- ユーザー リクエストと組織のポリシーに基づく共有ドライブのライフサイクルの管理（例: OU [組織部門] の配置）
- 特定の要件やシナリオに合わせた共有ドライブの権限の構成
- 組織のポリシーに基づく共有ドライブのメンバー権限の実装
- あるユーザーのドライブから別のドライブへのユーザーデータの移行
- ビジネスニーズに基づく共有ドライブへのセキュリティのベスト プラクティスの適用

1.3 カレンダーとカレンダー リソースの管理。以下のような点を考慮します。

- カレンダー リソースの作成と管理
- カレンダーのアクセス権とリソースの管理と委任
- 個々のカレンダーと共有カレンダーのライフサイクルの管理（例: 個々のカレンダーとカレンダー リソースを区別）
- Google ビデオ会議室のオプションの構成（例: Jamboard、Google Meet）
- Google Meet の会議とライブ ストリームによる会議やイベントのスケジュール設定
- 使用状況レポートのモニタリングと変更の推奨
- カレンダーに関する問題のトラブルシューティング

1.4 ビジネス向け Google グループの構成と管理。以下のような点を考慮します。

- 以下を含むメンバーシップと詳細設定の構成。
    - グループへのユーザーの追加
    - 現在の Google Workspace API の実装
    - Apps Script を使用したタスクの自動化
- Google グループを使用した共有ドライブに対するメンバーシップ権限の適用
- 特定の種類の Google ネイティブ グループの作成（例: 動的グループ、セキュリティ グループ、ID マッピング グループ、POSIX）
- Google グループのセキュリティ アクセス制御を実装してメンバーを制限
- Google グループでのトラブルシューティング（例: カレンダーの招待状が展開されない、招待状をグループに送信できない）

セクション **2:** サービスの構成（試験内容の **18%** 以下）

2.1 会社のポリシーに基づく Google Workspace 構成の実装と管理。以下のような点を考慮します。

- 組織部門（OU）と Google グループを使用した Google Workspace ツールへの権限の割り当てと構成
- OU ポリシーの修正
- 親 OU における組織部門の継承とオーバーライドの設定に応じたアプリケーションとセキュリティの設定の実装
- 粒度の高い Identity and Access Management（IAM）の管理者ロールと権限のドメイン内のユーザーへの委任
- Google Cloud Marketplace アプリケーションやアドオンをインストールまたは使用するためのセキュリティ構成オプションの実装
- データ組織のドライブラベルの構成
- 機能リリースの即時リリースまたは計画的リリースの構成
- 会社のポリシーや要件に合わせた Google Meet の構成
- セキュリティとデータ リージョンの設定の作成と構成
- セキュリティ統合プロトコルの実装とユーザーからの質問や否定的意見への対処
- コンテンツ コンプライアンス ルールの管理
- Security Health Analytics のチェック結果を使用した問題の調査と修正

2.2 Gmail の構成。以下のような点を考慮します。

- 分割配信の基本的なメール ルーティング シナリオの構成
- メールホストの構成
- Google Workspace Sync for Microsoft Outlook（GWSMO）またはメール クライアント（POP、IMAP、Thunderbird、Outlook など）を使用して、Gmail へのエンドユーザー アクセスを構成する
- 会社のポリシーや要件に合わせた POP と IMAP アクセスの構成
- Gmail の高度な設定を使用したメール転送用の管理者権限の構成（例: コンプライアンス ルール、デフォルト ルーティング、API）
- 利用可能なすべてのスパム制御の管理と把握（例: 許可リスト、拒否リスト、受信ゲートウェイ、IP 許可リストなど）
- OU を対象としたメールの委任の有効化
- Gmail のアーカイブの管理

セクション **3:** トラブルシューティング（試験内容の **24%** 以下）

3.1 ユーザーから報告されたメール配信問題のトラブルシューティング。以下のような点を考慮します。

- ユーザーの行動や広範な問題が原因でエラーが発生しているかどうかの確認（例: ルール、Cloud Data Loss Prevention [DLP]）
- 問題が想定された動作かどうかの判断（例: 添付ファイルの欠落や添付ファイル フィルタの問題）
- メールフロー構造とエンドユーザーのアクションを監査して確認し、配信の問題の根本原因を特定する
- Google Workspace ツールやセキュリティ調査ツールを使用したメッセージ ヘッダーやメール監査ログの分析
- メール配信の問題に関連する適切な対応方針の推奨と適用（例: メールポリシーの変更の適用）

3.2 サポートチームと連携するために必要なトラブルシューティングとログとレポートの収集。以下のような点を考慮します。

- 問題を再現するためのエンドユーザーが実施した手順の文書化
- 適切なログファイル形式の収集
- 既知の問題とアプリケーションのステータスの検索
- HAR ファイルの生成

3.3 基本的なメール攻撃の特定、分類、トラブルシューティング、軽減。以下のような点を考慮します。

- 以下を構成します:
    - ブロックされている送信者
    - メールの許可リスト
    - 不快なコンテンツ
    - フィッシング設定
    - 迷惑メールの設定
    - Gmail の安全性設定
    - 管理者検疫
    - 添付ファイルのコンプライアンス
    - セキュアなトランスポート コンプライアンス
- SPF（Sender Policy Framework）、DMARC（Domain-based Message Authentication, Reporting, and Conformance）、MTA-STS（Mail Transfer Agent Strict Transport Security）および DomainKeys Identified Mail（DKIM）を実装してメール送信を保護する
- カスタム構成が問題や脆弱性の原因であるかどうかの調査（例: メールの許可リストや IP アドレス）
- 利用可能な Google Workspace のメールツールを使用したメール攻撃の範囲の調査

- メッセージ攻撃のコンテンツに対する一般的な攻撃パターンの分析（例: 名前、ドメイン、ブランドのなりすまし）
- Google Workspace のメールツールの使用による実害に至る攻撃の軽減と将来の攻撃の防止（例: 問題の特定や対処）

3.4 Google Workspace のアクセスとパフォーマンスに関する問題のトラブルシューティング。以下のような点を考慮します。

- ユーザーが単一の Google アプリ（例: ドライブ）にアクセスしたときに問題が発生する理由の特定
- Google Workspace アプリケーションにアクセスする際のパフォーマンス問題の根本原因の特定（例: 既知の問題、サービスの停止、ネットワーク、デバイス）
- 重要なメールを確実に配信するための設定の分析、評価、変更（例: 特定の IP 範囲、X ヘッダーなど）
- ユーザーが報告した認証に関する問題のトラブルシューティング
- ユーザーがモバイル デバイスで Google Workspace を設定する際に報告した問題のトラブルシューティング
- 管理コンソールからの Google Meet ビデオ通話の問題のトラブルシューティング
- 管理コンソールを使用した Google Meet デバイスの問題のトラブルシューティング
- Google Meet を使用して高品質の会議を実現するためのネットワーク構成に関する問題のトラブルシューティング
- Jamboard のトラブルシューティング
- Google Workspace サービス（例: Gmail やドライブ）へのアクセスに関するトラブルシューティング
- ライセンスまたはサービスを有効または無効にすることによるデータの可視化に関する問題のトラブルシューティング
- OU 向けアプリケーションでのアクセスの問題の調査
- Alert Center API でのアラートの解釈と対応

セクション **4:** データアクセスと認証（試験内容の **24%** 以下）

4.1 すべてのデバイス（例: モバイル デバイス、パソコン、Chrome OS、Google Meet ハードウェア、Jamboard、Google Voice、ブラウザ）のポリシーの構成。以下のような点を考慮します。

- 以下を構成します:
    - Chrome ユーザーとブラウザ ポリシーの設定
    - ChromeOS デバイス ポリシーの設定（例: Enterprise）
    - Windows 10 のログインとデバイス ポリシー（例: Windows 用 Google 認証情報プロバイダ（GCPW））

    - 管理対象 Chrome ブラウザ（例: Chrome ブラウザ クラウド管理）
    - 基本的なデバイス管理
    - Android と iOS 向けのデバイスの基本的な管理と高度な管理
    - Android と iOS 向けの会社所有デバイスの管理
    - コンテキストアウェア アクセス ポリシー
    - Android と iOS 向けの個人用デバイス設定（例: パスワード、詳細設定、デバイスの承認、アプリケーションの管理、分析情報）
- BeyondCorp を使用した Endpoint Verification のセキュリティの有効化

4.2 ガバナンス ポリシーに基づく Gmail DLP の構成および実装とアクセス制御リスト（ACL）の共有。以下のような点を考慮します。

- データの引き出しレポートに基づく安全なコラボレーションの改善点の特定
- Gmail の DLP を使用したメールのスキャン
- 機密データのオーバーシェアリングを防ぐための Gmail の DLP ポリシーの実装
- データ分類用の Gmail DLP オプションの構成と実装
- ドライブでのデータ分類設定の構成と実装
- データ ガバナンス ポリシーに基づくコンテキストアウェア アクセス ポリシーの実装
- 組織のポリシーに基づくドライブの外部共有を制限するための設定の構成
- 組織のポリシーに基づくメール配信を制限するための設定の構成
- ドライブ向けクライアントサイド暗号化サービスの構成と実装

4.3 サードパーティ アプリケーションの管理。以下のような点を考慮します。

- ドメイン内の OU に対するブラウザ拡張機能の自動リリースの実装
- Google Cloud Marketplace アプリケーションやアドオンをインストールまたは使用するためのセキュリティ構成オプションの実装
- 新しい Google Workspace Marketplace アプリケーション、Google Play、または Chrome 拡張機能に対するユーザー リクエストの確認と承認
- Google のモバイル デバイス管理（MDM）を使用したアプリケーションのユーザーのスマートフォンへの push
- サードパーティ アプリケーション用の Security Assertion Markup Language（SAML）プロバイダとして Google を構成
- パスワードが保管されたアプリのデプロイ
- Google Workspace Marketplace アプリケーションと Google Play ストア アプリケーションのデプロイと制限
- アプリケーションへの API アクセスの許可
- サードパーティのユーザー プロビジョニングの統合
- Google Workspace の特定の OU へのサードパーティ製 Marketplace アプリケーションの統合

- 特定のユーザーのグループに対する追加の Google サービス（例: AdSense や YouTube ）へのアクセスの管理
- サードパーティ作成者アクセスの取り消し
- 接続されているアプリケーションとサイトの削除

4.4 ユーザー認証の構成。以下のような点を考慮します。

- 以下を構成します:
  - 管理者アカウントとリスクの高いアカウントに対する 2 段階認証プロセス（例: 物理キーを必要とする、SMS を許可しない）
  - リスクの低いアカウントおよび標準アカウントに対する 2 段階認証プロセス（例: Google 認証システム）
  - サードパーティのシングル サインオン（SSO）プロバイダへの Google 側の接続
  - SSO のための Google の Multi-IdP オプション
  - Google が SSO プロバイダの場合のサードパーティ アプリケーション認証の基本的な SAML SSO 構成
  - Google Workspace 向けサードパーティ SSO
  - API の制御でのセキュリティ機能の使用に基づくアクセス制御
  - 企業の法的ポリシーに基づく Google セッションの管理
- 基本的なユーザー セキュリティ制御の実装（例: パスワードの長さの適用）
- ID 管理、境界セキュリティ、データ保護のセキュリティ要素の実装

セクション **5:** ビジネス イニシアチブのサポート（試験内容の **14%** 以下）

5.1 Vault を使用した法的取り組みのサポート。以下のような点を考察します。

- 法的なセキュリティ ポリシーに基づく保持ルールの構成（例: 保持ルールの設定、訴訟のための記録保持の設定、追加の処理およびレビューのためのデータのエクスポート、レポートの監査、ユーザー アカウント / OU / 日付 / キーワードによるドメインのデータの検索）
- 以下を支援または作成します:
  - データを保持するための法的事項
  - 分析する案件コンテンツ（データ）をエクスポートする
  - Vault アクセスの委任プロトコル
  - Vault を使用した Google Workspace のコンテンツ（検索）
  - Vault を使用した Google Workspace コンテンツの訴訟のための記録保持
  - Vault 監査レポート（実行中）

5.2 ビジネスに関するレポートの作成と解釈。以下のような点を考慮します。

- ユーザー導入レポート（例: ワーク インサイト）の生成と解釈
- アラート センターを使用した問題の調査
- 特定の Google Workspace アプリケーションのサービス停止の調査とモニタリング
- アクティビティ レポートで利用可能なデータ オブジェクトと指標を使用した問題の調査
- 特定のイベントによってトリガーされたグループ アラートの構成
- 監査ログの作成と確認
- BigQuery を使用して、複数の Google Workspace ログと使用状況レポートを組み合わせ、行動につながるインサイトを提供する

5.3 データのインポートとエクスポートのサポート。以下のような点を考慮します。

- 従業員の退職とデータの移行の支援（例: ドライブ、カレンダー、Google データポータル）
- Google Workspace アカウント間での Gmail データの移行
- Google Workspace からオフラインまたは他のプラットフォームへのデータのエクスポート