Google Cloud

Associate Google Workspace Administrator

認定試験ガイド

Associate Google Workspace Administrator は、チームメンバーによる安全かつ効果的なコラボレーションとコミュニケーションのために、Google Workspace 環境の日常的な管理を担当します。ユーザー アカウントの管理、Gmail やドライブなどの Workspace コアサービスの構成、Workspace データのセキュリティとコンプライアンスの確保などが主な業務です。また、組織部門の設定、グループの管理、共有権限の構成、一般的な問題のトラブルシューティングなどのタスクも責任範囲です。

セクション 1: ユーザー アカウント、ドメイン、ディレクトリの管理（試験内容の約 22%）

1.1 ユーザー ライフサイクルの管理。次のような内容が含まれます。

- ユーザー アカウントを手動で作成する。
- ユーザーのプロビジョニングとデプロビジョニングを自動化する。
- サードパーティの ID プロバイダ（IdP）を使用して、ユーザーをプロビジョニングおよび認可する。
- 基本的な SAML SSO を構成する。
- GCDS を構成する。
- ユーザー属性（名前、メールアドレス、パスワード、エイリアスなど）を変更する。
- アカウントを削除、一時停止、復元、アーカイブする。
- データの所有権を別のアカウントに移行する。
- ライセンスを割り当てる。
- パスワードを管理する（再設定、強制変更、安全度のモニタリングなど）。

1.2 組織部門の設計と作成。次のような内容が含まれます。

- Google が推奨する方法に沿って、組織構造に対応する組織部門階層を設計する。
- 階層的なユーザー管理のための組織部門を作成および管理する。

1.3 グループの管理。次のような内容が含まれます。

- グループ階層を設計する。
- 配信リストを作成および管理する。

- 共有メールボックス（共同トレイ）を作成および管理する。
- 動的グループを作成および管理する。
- セキュリティ グループを作成および管理する。

1.4 ドメインの管理。次のような内容が含まれます。

- プライマリドメインとセカンダリドメインを追加し、所有権を証明する。
- ドメイン エイリアスを管理する。
- メール ルーティング用の MX レコードを構成する。

1.5 ビルディングとリソースの管理。次のような内容が含まれます。

- ビルディングと会議室を一括作成する。
- 予約とスケジュールの対象となる新しいリソースを作成および管理する。
- リソース予約に必要な権限を設定する。
- リソースに具体的な詳細（定員、ホワイトボード、車椅子対応など）を追加する機能を作成する。

セクション 2: Workspace コアサービスの管理（試験内容の約 20%）

2.1 Gmail の構成。次のような内容が含まれます。

- メール ルーティング用の MX レコードを構成する。
- 分割配信と二重配信の基本的なメール ルーティング シナリオを構成する。
- コンテンツ コンプライアンス ルールを使用して、内容に基づいてメールをフィルタリングおよびルーティングする。
- 迷惑メール、フィッシング、マルウェアの設定を行う（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）。
- メールの添付ファイルのサイズ制限とブロックするファイル形式を管理する。
- Gmail の転送と POP / IMAP アクセスを構成する。
- Google が推奨するメール セキュリティ対策（SPF、フィッシング防止、DKIM、DMARC など）を導入する。
- メールデータを Gmail から外部に、または外部から Gmail に移行する（他のメール プロバイダからメールを移行する場合など）。
- Gmail へのアクセス権を他のユーザーに委任する。
- コンプライアンス フッターとメール検疫を管理する。

2.2 Google ドライブと Google ドキュメントの構成。次のような内容が含まれます。

- 新しいファイル、フォルダ、ドキュメントのデフォルト共有オプションを構成する（内部共有や外部共有、Google ドライブの信頼ルールなど）。
- 組織のポリシーに基づいて外部共有が制限されるよう、Google ドライブを構成する。
- 対象グループを管理する。
- Google ドキュメントのカスタム テンプレートを作成、管理、共有する。
- Google ドキュメントのアドオンを有効にする。
- 共有ドライブを作成および管理する。
- 個々のユーザーまたは組織部門の保存容量を設定および調整する。
- パソコン版 Google ドライブをインストールおよび構成する。
- ファイルやフォルダのオーナー権限を他のユーザーに移行する。
- ドライブのラベルを管理する。
- オフライン アクセスを有効または無効にする。

2.3 Google カレンダーの構成。次のような内容が含まれます。

- リソース カレンダー（会議室、設備など）を作成および管理する。
- リソースの予約ポリシーを構成する。
- カレンダーとリソースへのアクセス権を別のユーザーに委任する。
- チームやグループの共有カレンダーを構成する。
- カレンダーの外部共有オプションを管理する。
- サードパーティのウェブ会議ツールがサポートされるようにカレンダーを構成する。
- 予定をキャンセルしたり、別のユーザーに転送したりする。
- 不明な送信者からの招待状がカレンダーに追加されないようにする。

2.4 Google Meet の構成。次のような内容が含まれます。

- 組織や特定の組織部門に対して Meet を有効または無効にする。
- Meet の安全設定を構成する。
- Meet の動画設定（品質、録画、音声文字変換など）を構成する。
- ストリーミング設定を有効にし、管理する。

2.5 Google Chat の構成。次のような内容が含まれます。

- 組織や特定の組織部門に対して Chat を有効または無効にする。
- 管理コンソールで Chat 設定を構成する（チャットの履歴、スペースの設定、外部ドメインが Chat スペースに参加するための許可、管理など）。
- Chat の招待設定を管理する。
- Chat 用アプリを追加する。

2.6 Gemini for Google Workspace の構成。次のような内容が含まれます。

- 組織や特定の組織部門に対して Gemini を有効または無効にする。
- Gemini ライセンスを特定のユーザーまたはグループに割り当てる。
- アルファ版機能を有効にする。
- Gemini の利用状況をモニタリングする。

2.7 Workspace の開発のサポート。次のような内容が含まれます。

- AppSheet と Apps Script のユースケース（タスクの自動化など）を特定する。
- 組織または特定の組織部門に対して AppSheet を有効にする。

セクション **3:** データ ガバナンスとコンプライアンスの管理（試験内容の約 **14%**）

3.1 Google Vault を使用した電子情報開示とデータの保持。次のような内容が含まれます。

- Gmail のコンテンツ コンプライアンス ルールと DLP ルールの違いを特定する。
- 機密データの不正な共有や損失を防止するための DLP ルールを構成する。
- コンテンツ検出項目（クレジット カード番号、個人情報など）または正規表現に基づいて、自動 DLP ルールとアクションを作成および構成する。
- 特定の Workspace サービス（Gmail、ドライブ、Chat など）に DLP ルールを適用する。
- DLP に関する通知メッセージをカスタマイズする。

3.2 データ損失防止（DLP）ルールの作成と管理。以下のような点を考察します。

- Gmail のコンテンツ コンプライアンス ルールと DLP ルールの違いを特定する。
- 機密データの不正な共有や損失を防止するための DLP ルールを構成する。
- コンテンツ検出項目（クレジット カード番号、個人情報など）または正規表現に基づいて、自動 DLP ルールとアクションを作成および構成する。
- 特定の Workspace サービス（Gmail、ドライブ、Chat など）に DLP ルールを適用する。
- DLP に関する通知メッセージをカスタマイズす

3.3 ドライブの信頼ルールの作成と管理。次のような内容が含まれます。

- 特定の組織部門グループ、ドメイン、またはユーザーに共有対象を制限する。
- 特定の組織部門グループ、ドメイン、またはユーザーからの共有をブロックする。
- 組織外のユーザー（訪問者、外部ユーザーなど）との共有を許可または制限する。

3.4 環境データの保存方法およびエクスポート方法の決定。次のような内容が含まれます。

- Google データ エクスポートの設定を管理する（特定のデータ型の許可や制限など）。
- データ エクスポート ツールを使用する。
- データの地理的な保管場所を選択する。
- 業界の規制に基づいて、法務関連およびコンプライアンスの設定を構成する。

3.5 データの分類。次のような内容が含まれます。

- データにラベルを適用するユースケースを特定する（ユーザー分類、DLP、デフォルトの分類、AI 分類など）。
- ドライブのラベルを適用する。
- Gmail のラベルを適用する。

セクション **4:** セキュリティ ポリシーとアクセス制御の管理（試験内容の約 **20%**）

4.1 ユーザー アクセスの保護。次のような内容が含まれます。

- 安全なパスワード ポリシーと 2 段階認証プロセス（2SV）ルールを適用する。
- パスワード ポリシーと復元オプション（セキュリティ保護用の質問、確認コードなど）を構成する。
- 2 段階認証プロセスの実施方法（Google 認証システム アプリ、テキスト メッセージ、パスキーなど）を構成する。
- コンテキストアウェア アクセス ポリシーを管理する。
- 特定の組織部門にセキュリティ ポリシーとアクセス制御を適用する。
- リソース（ファイル、カレンダーなど）へのアクセスを制御するセキュリティ グループを作成および管理する。
- 事前構築されたカスタムの管理者ロール（特権管理者、グループ管理者、ユーザー管理者など）をユーザーに割り当て、特定の管理タスクを委任する。

4.2 セキュリティ リスクやセキュリティ イベントの報告、監査、調査。次のような内容が含まれます。

- セキュリティ調査ツールを使用して、ログやセキュリティ イベントを調査および分析する。
- セキュリティ センターを使用して、セキュリティ リスクと脅威を特定する。
- セキュリティ センターのセキュリティの状況ページを使用して、セキュリティ関連の構成の改善点を特定する。
- アクティビティのルールとアラートを作成する。

4.3 Google やサードパーティのアプリケーションの有効化。次のような内容が含まれます。

- Marketplace の許可リストを管理する。
- Google Workspace Marketplace や Google Play ストアのアプリケーションをデプロイおよび制限する。
- サードパーティ アプリケーションで SAML を構成する。
- その他の Google サービス（AdSense や YouTube）へのアクセスを、複数の特定ユーザー向けに管理する。
- 接続されているアプリケーションとサイトを削除する。
- ドメイン内の組織部門に対して、ブラウザ拡張機能の自動リリースを実装する。

セクション 5: エンドポイントの管理（試験内容の約 10%）

5.1 モバイル デバイスの管理。次のような内容が含まれます。

- モバイル管理において、基本のソリューション、高度なソリューション、サードパーティのソリューションをそれぞれどのような場合に使用するかを判断する。
- Google のモバイルの基本管理を使用して、モバイル デバイスにセキュリティ ポリシーを適用する。
- 会社所有と Bring Your Own Device（BYOD）の両方を含む登録済みデバイスの、可視性と管理性を維持する。
- 離職した従業員のモバイル デバイスをオフボーディングする。

5.2 Chrome ブラウザの管理。次のような内容が含まれます。

- Chrome ブラウザのポリシー（オフライン アクセス、更新ポリシーなど）を適用する。
- ブラウザを登録し、ポリシーを適用する。
- 拡張機能とアプリを管理する（許可、ブロック、自動インストールなど）。

セクション 6: 一般的な問題のトラブルシューティング（試験内容の約 14%）

6.1 Workspace の問題の特定と診断。次のような内容が含まれます。

- 管理コンソールから監査ログにアクセスする。
- ログエントリを分析して、エラー メッセージ、不審なアクティビティ、問題に紐づけられるパターンを特定する。
- Google Workspace ステータス ダッシュボードで、サービスの中断や停止がないか確認する。

- メール配信の問題に対する解決策を推奨する（メールポリシーの変更の適用など）。

6.2 一般的な問題のトラブルシューティングと解決。次のような内容が含まれます。

- ユーザー アカウント、パスワード、サービスへのアクセスに関する問題をトラブルシューティングする。
- メール配信に関する問題（未配信メッセージや迷惑メールのフィルタに関する問題など）をトラブルシューティングする。
- メール転送、フィルタ、ラベルに関する問題をトラブルシューティングする。
- Workspace ツール、セキュリティ調査ツール、Google 管理者ツールボックスを使用して、メッセージ ヘッダーやメールの監査ログを分析する（例: SPF、DMARC、DKIM）。
- カレンダーの予定が同期されない、または正しく表示されない問題をトラブルシューティングする（Apple カレンダー、Outlook など）。
- カレンダーの共有や権限管理に関する問題をトラブルシューティングする。
- 予定の有無の共有に関するカレンダーの問題をトラブルシューティングする。
- 共有や権限管理に関するドライブの問題をトラブルシューティングする。
- パソコン版ドライブに関する問題を解決する。
- ドライブで誤って削除されたファイルを復元する。
- ドライブのオフライン アクセスに関する問題をトラブルシューティングする。
- Meet 品質管理ツールを使用して、ネットワーク パフォーマンスの問題（動画や音声の品質など）を診断する。
- Meet に関する問題（ユーザーが Meet イベントにアクセスできないなど）をトラブルシューティングする。

6.3 サポート リソースの使用。次のような内容が含まれます。

- 問題を再現するためにエンドユーザーが実施した手順を文書化する。
- 適切な形式のログファイルを収集する。
- アプリケーションのステータスと既知の問題を検索する。
- HAR ファイルを生成する。