# Google.Associate-Google-Workspace-Administrator.v2026-07-02.q61

| | |
|---|---|
| 試験コード: | Associate-Google-Workspace-Administrator |
| 試験名称: | Associate Google Workspace Administrator |
| 認定資格: | Google |
| 無料問題数: | 61 |
| バージョン: | v2026-07-02 |
| アクセス数: | 119 |
| ページビュー数: | 610 |
| https://www.jpnpdf.com/Google.Associate-Google-Workspace-Administrator.v2026-07-02.q61-mondaishu.html | |

最新問題: **1**
貴社は、従業員が新たに導入したクラウドベースのマーケティングプラットフォームにアクセスできるように、シングルサインオン $SO) を有効にしたいと考えています。マーケティングプラットフォームのベンダーは、SAML 2.0との互換性を確認し、必要なメタデータを提供しています。Google Workspace を通じてユーザーアクセスを効率化し、認証を一元化する必要があります。どうすればよいですか？
**A.** SAML統合のために、マーケティングプラットフォームベンダーからAPIキーをリクエストしてください。
**B.** SSOを実装する前に、セキュリティを強化するために、すべてのユーザーに対して二要素認証を有効にします。
**C.** 従業員に、Google でサインイン機能を使用してマーケティング プラットフォームにログインするように指示します。
**D.** Google管理コンソールで新しいSAMLアプリケーションを作成します。
**Answer: D (**メーッセージを残す**)**
Google Workspace を介したシングルサインオン (SSO) を有効にするには、Google 管理コンソールで新しい SAML アプリケーションを作成する必要があります。これにより、ユーザーは SAML 2.0 の互換性を活用し、マーケティングプラットフォームにアクセスする際に Google Workspace を介して一元的に認証を行うことができます。その後、マーケティングプラットフォームベンダーから提供されたメタデータをアップロードすることで、統合が完了します。この方法により、従業員のアクセスが効率化され、認証が一元化されます。

最新問題: **2**

貴社の財務部門の複数の従業員が、長期にわたる複数段階のプロジェクトで協力しています。このプロジェクトのために、できるだけ早く機密グループを作成する必要があります。同時に、管理上の負担を最小限に抑えたいと考えています。どうすればよいでしょうか？
**A.** Google Cloud Directory Sync (GCDS) を使用して Google グループを作成し、メンバーを自動的に同期します。
**B.** 動的グループを作成し、部門ユーザー属性をメンバーシップの条件として定義し、その値を財務部門とします。
**C.** Googleグループを作成し、設定を更新して組織内の誰でもグループに参加できるようにします。
**D.** Googleグループを作成し、グループのメンバーを管理するグループ管理者を任命します。
**Answer: B (**メーッセージを残す**)**
動的グループは、所属部署などのユーザー属性に基づいてメンバーシップを自動的に更新し、関連する従業員（例えば、財務部門の従業員）のみがグループに追加されるようにします。メンバーシップは手動での介入なしに自動的に更新されるため、管理上の負担が最小限に抑えられます。また、従業員が部署に加わったり離れたりする場合でも、グループが常に最新の状態に保たれます。

最新問題**: 3**
貴社は機密性の高い顧客データを取り扱っており、厳格な業界規制を遵守するために高いレベルのセキュリティを維持する必要があります。貴社のセキュリティチームがGoogle管理コンソールのセキュリティ調査ツールを使用して潜在的なセキュリティ侵害を調査できるようにする必要があります。
あなたはどうすべきでしょうか？
**A.** 高リスクのセキュリティイベントが発生した際に、セキュリティチームにメール通知を送信するアクティビティルールを作成します。
**B.** セキュリティチームにユーザー管理管理者ロールを割り当てます。
**C.** セキュリティチームにスーパー管理者ロールを割り当てる
**D.** セキュリティセンターへのアクセス権を持つ管理者ロールを作成します。そのロールをセキュリティチームに割り当てます。
**Answer: D (**メーッセージを残す**)**
セキュリティチームがセキュリティ調査ツールを使用して潜在的なセキュリティ侵害を調査できるようにするには、セキュリティセンターへのアクセス権を持つカスタム管理者ロールを作成する必要があります。
この役割により、セキュリティチームはセキュリティ調査ツールへのアクセスと使用に必要な権限を付与されますが、ユーザー管理やスーパー管理者といった不要な権限は付与されません。このアプローチにより、セキュリティと業界規制への準拠の両方が確保されます。

最新問題**: 4**

あなたは会社のGoogle Workspaceアカウントのメール設定を行っています。会社は、特定の種類のファイルがメールの添付ファイルとして送受信されないように、最もシンプルかつ費用対効果の高い方法で設定したいと考えています。あなたはどうすべきでしょうか？
**A.** 最大メッセージサイズ制限を調整して、大きなファイルの送受信を防ぎます。
**B.** Gmailでセキュリティサンドボックスを有効にすると、疑わしい添付ファイル付きのメールが自動的に隔離されます。
**C.** 業界標準のサードパーティ製メールセキュリティソリューションを使用して、送受信メールすべてをスキャンし、悪意のある添付ファイルがないか確認します。
**D.** Gmailの設定で添付ファイルコンプライアンスルールを設定し、特定のファイルタイプをブロックします。
**Answer: (**解答を表示する**)**
Gmailで添付ファイルコンプライアンスルールを設定すると、特定の種類のファイルがメールの添付ファイルとして送受信されないように設定できます。この方法は、サードパーティ製のソリューションや高度な設定を必要とせず、Google Workspaceの組み込み機能を活用するため、シンプルで費用対効果に優れています。ブロックするファイルの種類を簡単に指定できるため、組織を不要な添付ファイルから確実に保護できます。

最新問題: **5**
あなたの会社の営業チームは、Googleドキュメントで多くのビジネス提案書を作成しています。彼らはテンプレートを使用して提案書作成プロセスを効率化したいと考えています。営業チームがアクセスできる、あらかじめ項目が入力されたドキュメントテンプレートを作成する必要があります。どうすればよいでしょうか？
**A.** Googleドライブでテンプレートを作成します。営業チームに編集権限を付与します。
**B.** Googleドライブでテンプレートを作成します。各営業担当者用にコピーを作成します。各テンプレートの所有権を営業担当者に譲渡します。
**C.** 管理コンソールで組織のブランディングを有効にします。Google ドライブでテンプレートを作成します。作成したテンプレートを組織全体のデフォルトテーマとテンプレートに追加します。
**D.** Googleドライブでテンプレートを作成し、ファイルをPDFとしてダウンロードします。ダウンロードしたPDFファイルを、営業チームと共有しているドライブにアップロードします。
**Answer: (**解答を表示する**)**
営業チームが簡単にアクセスして提案プロセスを効率化できる、あらかじめ入力済みのセクションを含むドキュメントテンプレートを作成するには、Google Workspaceのテンプレートギャラリーを利用するのが最も効率的で一元管理しやすい方法です。これには、組織のブランディングを有効にし（基本的なテンプレートには必須ではありませんが、組織テンプレートではよく使用されます）、作成したテンプレートを組織全体または特定のグループのデフォルトのテーマとテンプレートに追加することが含まれます。

選択肢Cが正解である理由と、他の選択肢が理想的な解決策ではない理由を以下に説明します。
C. 管理コンソールで組織のブランディングを有効にします。Googleドライブでテンプレートを作成します。作成したテンプレートを組織全体のデフォルトテーマとテンプレートに追加します。
このオプションは、Google Workspace に組み込まれているテンプレートギャラリー機能を活用します。Google ドキュメントでテンプレートを作成し（Google ドライブに保存されます）、Google 管理コンソールから組織のデフォルトテーマとテンプレートに追加することで、すべてのユーザー（または特定の組織単位）がテンプレートギャラリーから新しいドキュメントを作成する際に、これらのテンプレートを簡単に見つけられるようになります。組織のブランディングを有効にすることで外観をカスタマイズできますが、重要なのはテンプレートをギャラリーに追加することです。
Google Workspace 管理者の関連トピックガイドまたはドキュメントの参照: 公式の Google Workspace 管理者ヘルプドキュメントには、「組織のドキュメント テンプレートの作成と管理」に関する詳細な手順が記載されています。このドキュメントでは、Google ドライブでドキュメントをテンプレートとして準備し、管理コンソールからテンプレートギャラリーに送信して、組織内のユーザーが利用できるようにする方法を説明しています。取り上げるトピックは次のとおりです。組織のギャラリーにテンプレートを送信する: このプロセスでは、管理コンソールで [アプリ] > [Google Workspace] > [ドライブとドキュメント] > [テンプレート] に移動します。
カスタムテンプレートギャラリーの設定 :このドキュメントでは、管理者がユーザーに表示されるテンプレートを管理する方法について説明しています。
組織単位 :テンプレートは特定の組織単位に提供されることが多く、営業チームなど、さまざまなチーム向けにカスタマイズされたテンプレートを利用できます。
A. Googleドライブにテンプレートを作成します。営業チームに編集権限を付与します。
マスターテンプレートへの編集権限を営業チームに付与することは問題があります。意図的または偶発的に元のテンプレートが変更され、矛盾が生じ、テンプレートが意図した状態を維持するための継続的な管理が必要になる可能性があります。理想的には、ユーザーはテンプレートのコピーを作成して作業し、元のテンプレートには手を加えないようにしてください。
Google Workspace 管理者向けトピックガイドまたはドキュメントのリファレンス: Google ドライブでのファイル共有とコラボレーションのベストプラクティスでは、適切なアクセスレベルの提供を重視しています。テンプレートの場合、通常はユーザーがテンプレートを使用して新しいドキュメントを作成することを目的としており、元のドキュメントを編集することではありません。
B. Googleドライブでテンプレートを作成します。各営業担当者用にコピーを作成します。各テンプレートの所有権を営業担当者に譲渡します。
この方法は非効率的で管理も困難です。テンプレートの個々のコピーを作成し、各営業担当者に所有権を移転するには、管理者にとって多くの時間がかかります。さらに、テンプ

レートを更新する必要がある場合、個々のコピーをすべて修正する必要があり、バージョン管理の問題や営業チーム全体での不整合につながります。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google ドライブの共有機能と所有権機能は、ドキュメントの共同作業を目的として設計されており、テンプレートの配布や管理には適していません。テンプレートギャラリーを通じた集中管理が推奨される方法です。
D. Googleドライブでテンプレートを作成し、PDFファイルとしてダウンロードします。ダウンロードしたPDFファイルを、営業チームと共有しているドライブにアップロードします。
テンプレートをPDFとして保存してしまうと、編集可能なテンプレートの本来の目的が損なわれてしまいます。営業チームは、あらかじめ入力された項目を簡単に修正したり、独自の提案内容をPDFに追加したりすることができなくなります。テンプレートは、新しい編集可能な文書を作成するための出発点となるべきものです。
Google Workspace 管理者向けトピックガイドまたはドキュメントのリファレンス:
Google ドキュメントは、ドキュメントの作成と編集のために設計されています。テンプレートは、この編集可能な形式の機能の一つであり、ユーザーはあらかじめ構造化されたドキュメントから始めて、それをカスタマイズすることができます。PDF は、編集不可能な最終版に使用されます。
したがって、適切なアプローチは、Google Workspaceのテンプレートギャラリーを活用して、営業チームが提案書テンプレートにアクセスして使用できる、効率的かつ一元管理された方法を提供することです。これは、Googleドライブでテンプレートを作成し、管理コンソールから組織のテンプレートに追加することで実現できます。オプションCでは組織のブランディングを有効にする方法について触れていますが、コア機能はテンプレートギャラリー機能に依存しています。

最新問題: **6**
貴社は大量の機密性の高い顧客データを取り扱っており、厳格な業界規制を遵守する必要があります。迫りくるコンプライアンス期限に対応するため、Googleドライブに保存されているファイルをその内容に基づいて自動的に分類するソリューションを迅速に導入する必要があります。
あなたはどうすべきでしょうか？
**A.** Drive のデータ損失防止 (DLP) ルールを作成します。コンテンツに基づいて Drive ラベルを適用するようにルールを設定します。
**B.** コンテンツに基づいてドライブラベルを適用します。Google Vaultを使用してドライブラベルに基づいた保持ルールを作成し、必要な期間データが保持されるようにします。
**C.** Driveと統合し、高度な分類機能を提供するサードパーティのデータガバナンスツールを導入する。
**D.** ユーザーを組織単位（OU）に追加します。目的のOUに対して、Driveでデフォルトのファイル分類を設定します。

**Answer: (**解答を表示する**)**
Google Workspace のデータ損失防止 (DLP) ルールを使用すると、機密性の高い顧客データなどのコンテンツに基づいて、Google ドライブ内のファイルを自動的に分類およびラベル付けできます。これにより、ファイルが保存される際に適切な分類が適用されるため、コンプライアンスが確保されます。また、定義済みの基準に基づいて分類プロセスを自動化することで、コンプライアンスの期限に迅速に対応できます。

最新問題: **7**
貴社のセキュリティチームは、不正な外部ファイル共有を調査できる必要があります。セキュリティチームがセキュリティ調査ツールを使用できるようにし、最小権限の原則に従う必要があります。では、どうすればよいでしょうか？
**A.** セキュリティチームの代理人にスーパー管理者権限を付与します。
**B.** 事前に構築されたレポートロールを作成します。そのロールをセキュリティチームのエイリアスに割り当てます。
**C.** Driveの監査ログをセキュリティチームと共有してください。
**D.** セキュリティセンターの権限を持つカスタム管理者ロールを作成します。そのロールを個々のセキュリティチームメンバーに割り当てます。
**Answer: D (**メーッセージを残す**)**
セキュリティセンターの権限を持つカスタム管理者ロールを作成することで、セキュリティチームが不正な外部ファイル共有を調査するために必要なアクセス権限を確保しつつ、最小権限の原則を遵守することができます。このアプローチにより、セキュリティチームはスーパー管理者ロールなど、不必要な広範な権限を付与することなく、必要な特定の権限のみを取得できます。

最新問題: **8**
貴社は、従業員が新たに導入したクラウドベースのマーケティングプラットフォームにアクセスできるように、シングルサインオン $SO）を有効にしたいと考えています。マーケティングプラットフォームのベンダーはSAML認証を確認済みです。
2.0との互換性を確保し、必要なメタデータを提供してください。Google Workspaceを通じて、ユーザーアクセスを効率化し、認証を一元化する必要があります。
あなたはどうすべきでしょうか？
**A.** SAML統合のために、マーケティングプラットフォームベンダーからAPIキーをリクエストしてください。
**B.** SSOを実装する前に、セキュリティを強化するために、すべてのユーザーに対して二要素認証を有効にします。
**C.** 従業員に、Google でサインイン機能を使用してマーケティング プラットフォームにログインするように指示します。
**D.** Google管理コンソールで新しいSAMLアプリケーションを作成します。
**Answer: (**解答を表示する**)**

Google Workspace を介したシングルサインオン (SSO) を有効にするには、Google 管理コンソールで新しい SAML アプリケーションを作成する必要があります。これにより、ユーザーは SAML 2.0 の互換性を活用し、マーケティングプラットフォームにアクセスする際に Google Workspace を介して一元的に認証を行うことができます。
その後、マーケティングプラットフォームベンダーから提供されたメタデータをアップロードすることで、統合が完了します。この方法により、従業員のアクセスが効率化され、認証が一元化されます。

最新問題: **9**
組織向けにChromeブラウザのセキュリティポリシーを設定しています。これらのポリシーでは、特定のChromeアプリと拡張機能を制限する必要があります。
どのユーザーがデバイスにログインしても、これらのポリシーがデバイスに適用されることを確認する必要があります。どうすればよいでしょうか？
**A.** アプリと拡張機能の設定にあるデバイスページで、許可するアプリのリストを設定します。
**B.** Chromeのユーザー設定を構成して、Chromeアプリと拡張機能を使用する際にユーザーがサインインするようにします。
**C.** アプリと拡張機能に適用されるドメイン全体のポリシーを上書きするために、ポリシーの優先順位を設定します。
**D.** ユーザーログインに2段階認証を必須とする。
**Answer: A (**メーッセージを残す**)**
Chromeアプリと拡張機能のポリシーが、どのユーザーがデバイスにログインしても確実に適用されるようにするには、アプリと拡張機能の設定の 「デバイス」セクションで、許可するアプリのリストを設定する必要があります。このポリシーはデバイスレベルで適用されるため、そのデバイスにログインするすべてのユーザーに対して制限が適用され、組織全体で一貫したセキュリティが確保されます。

最新問題: **10**
貴社は大量の機密性の高い顧客データを取り扱っており、厳格な業界規制を遵守する必要があります。迫りくるコンプライアンス期限に対応するため、Googleドライブに保存されているファイルをその内容に基づいて自動的に分類するソリューションを迅速に導入する必要があります。
あなたはどうすべきでしょうか？
**A.** Drive のデータ損失防止 (DLP) ルールを作成します。コンテンツに基づいて Drive ラベルを適用するようにルールを設定します。
**B.** コンテンツに基づいてドライブラベルを適用します。Google Vaultを使用してドライブラベルに基づいた保持ルールを作成し、必要な期間データが保持されるようにします。
**C.** Driveと統合し、高度な分類機能を提供するサードパーティのデータガバナンスツールを導入する。

**D.** ユーザーを組織単位（OU）に追加します。目的のOUに対して、Driveでデフォルトのファイル分類を設定します。
**Answer: A (**メーッセージを残す**)**
Google Workspace のデータ損失防止 (DLP) ルールを使用すると、機密性の高い顧客データを識別するなど、コンテンツに基づいて Google ドライブ内のファイルを自動的に分類およびラベル付けできます。
これにより、ファイルが保存される際に適切な分類が適用されるため、コンプライアンスが確保されます。また、事前に定義された基準に基づいて分類プロセスを自動化することで、コンプライアンスの期限に迅速に対応できます。

最新問題**: 11**
あなたの組織では、従業員が個人のモバイル端末で業務メールを確認することを許可しています。従業員が退職する際には、その従業員の携帯電話から業務メールのデータを削除する必要があります。どうすればよいでしょうか？
**A.** デバイス上で基本的なモバイル管理を設定します。
**B.** デバイスに高度なモバイル管理を設定します。
**C.** 外部へのデータ共有を防止するためのデータ保護ルールを設定します。
**D.** デバイスで2SV認証を設定します。
**Answer: (**解答を表示する**)**
高度なモバイル管理機能により、従業員が退職する際に、個人デバイス上の業務関連データをリモートで管理・消去できます。これには、デバイスへのアクセスにパスワードを要求するなどのポリシーの適用、企業データのリモート消去、デバイス上の個人データに影響を与えることなく業務リソースへのアクセスを管理する機能が含まれます。このソリューションは、データセキュリティとコンプライアンスを確保するために必要なツールを提供します。

最新問題**: 12**
Gmailに関するサポートチケットが増加していることに気づきました。複数のユーザーから、メールが読み込まれず、エラーメッセージが表示されるという報告が寄せられています。この問題をトラブルシューティングし、潜在的な原因を特定する必要があります。どうすればよいでしょうか？
**A.** ユーザーのGmailラベルとフィルタを分析して、受信メールが意図せずブロックされていないかを確認します。
**B.** ユーザーのブラウザのバージョンと拡張機能を収集し、潜在的な互換性の問題を特定します。
**C.** ユーザーのメール転送設定を確認し、メールが誤ったアドレスに転送されていないことを確認してください。
**D.** 影響を受けたユーザーからHARファイルを集め、ネットワークトラフィックをキャプチャして、リクエスト/レスポンスの詳細を分析します。

**Answer: D (メッセージを残す)**
ユーザーが Gmail で 「メールが読み込まれない」 エラーメッセージが表示される」といった問題を報告した場合、特にそれが新しい問題や広範囲にわたる問題であれば、多くの場合、ネットワーク関連の問題、クライアント側の問題、またはブラウザと Google サーバー間のやり取りが原因であると考えられます。HAR (HTTP Archive) ファイルは、Web ブラウザで発生するすべてのネットワーク要求と応答をキャプチャします。この詳細なログは、以下のような Web アプリケーションの問題を診断する上で非常に役立ちます。
サーバーから特定のエラーコードを特定する。
リクエストヘッダーとレスポンスヘッダーを分析する。
リクエストのタイミングをチェックして、パフォーマンス上のボトルネックがないか確認する。
ブロックされたリクエストや障害が発生したリソースを特定する。
この種の広範囲にわたる問題に対する最初のトラブルシューティング手順として、他の選択肢が効果的でない理由を以下に示します。
A. ユーザーのGmailラベルとフィルタを分析し、受信メールが意図せずブロックされていないかを確認します。ラベルとフィルタはメールの表示に影響を与える可能性がありますが、通常は 「メールが読み込まれない」という問題や、Gmailインターフェース自体に一般的な 「エラーメッセージ」が表示される原因にはなりません。メールが単に表示されないだけで、インターフェース自体は正常に機能している場合に、この問題はより重要になります。
B. ユーザーのブラウザのバージョンと拡張機能を収集し、潜在的な互換性の問題を特定します。これは、適切な二次トラブルシューティング手順です。ブラウザのバージョン、拡張機能、あるいはキャッシュされたデータでさえ、問題を引き起こす可能性があります。しかし、HARファイルによって、問題がブラウザレベル（例えば、拡張機能がスクリプトをブロックしているなど）にあるのか、それともネットワークのやり取りのより深い部分にあるのかが明らかになることがよくあります。HARでネットワークトラフィックに問題がない場合は、ブラウザの詳細を調べることがより重要になります。
C. ユーザーのメール転送設定を確認し、メールが誤ったアドレスに転送されていないことを確認してください。メール転送は、Gmailに届いたメールの転送先に影響を与えるものであり、Gmailのインターフェース自体が読み込まれるか、エラーが表示されるかどうかには影響しません。これは、報告された症状とは無関係です。
Google Workspace管理者からの参考情報：
Google Workspace の管理者ヘルプには 「HAR ファイルを使用した Gmail のトラブルシューティング」という直接的なページはありませんが、Web アプリケーションのトラブルシューティングに HAR ファイルを使用するという概念は、基本的なベストプラクティスであり、Google のサポート担当者自身も、Google Workspace サービスにおける複雑なブラウザ関連の問題を診断する際に広く利用しています。
Google Workspace の一般的なトラブルシューティング手順 (暗黙的な HAR ファイルの使用): Google のサポートでは、ウェブベースのサービスにおけるブラウザやネットワーク関

連の問題を診断する際に、HAR ファイルを要求することがよくあります。これは一般的な診断ツールです。
HARファイルの生成方法：HARファイルの生成方法に関する手順は、一般的にブラウザ開発者（Chrome、Firefox、Edgeなど）から提供されており、Webアプリケーションの問題のトラブルシューティングを行う際にサポートチームによって共有されることがよくあります。
例（一般的なWeb開発／トラブルシューティングリソース）：様々なオンラインチュートリアルやブラウザ開発者向けドキュメントには、HARファイルの生成方法に関する説明が記載されています（例Chrome DevTools、Firefox Network Monitor）。これらはWebトラブルシューティングの標準的なツールです。
HARファイルをキャプチャすることで、ユーザーのブラウザとGoogleのサーバー間の通信状況を包括的に把握できます。これは、GmailのようなWebアプリケーションにおける読み込みエラーや一般的な機能問題の根本原因を特定する上で非常に重要です。

最新問題: **13**
あなたは会社向けにGmailを設定しており、多層防御型のセキュリティ対策を導入したいと考えています。
業界標準のメール認証プロトコルを導入することにしました。どのような手順を踏むべきでしょうか？
2つの回答を選択してください
**A.** すべてのユーザーに対してデフォルトのメール隔離を有効にして、疑わしいメールを隔離し、メッセージが認証されていないかどうかを判断します。
**B.** 不明な送信者からのすべてのメールをブロックするブロック送信者ルールを設定します。
**C.** DKIMを設定して、送信メールにデジタル署名を行い、送信元を検証します。
**D.** 外部クライアントが Gmail にアクセスできないように、組織内で IMAP を無効にします。
**E.** ドメインの承認済みメールサーバーを指定するために、SPFレコードを設定します。
**Answer: C,E (**メーッセージを残す**)**
Gmailの多層セキュリティ対策の一環として、業界標準のメール認証プロトコルを実装するには、ドメインに対してDKIM（DomainKeys Identified Mail）レコードとSPF（Sender Policy Framework）レコードを設定する必要があります。これらのプロトコルは、送信者の身元を確認し、メールメッセージの完全性を確保するために不可欠です。

最新問題: **14**
Workspace Enterprise Standardライセンスを使用していた従業員が組織を退職しました。退職した従業員がWorkspaceアカウントにアクセスできないようにするとともに、マネージャーとチームが退職した従業員のドキュメントにアクセスできるようにする必要があります。

ライセンス費用を最小限に抑えたい場合、どうすればよいでしょうか？
**A.** 元従業員のワークスペースアカウントを削除します。
**B.** 元従業員のワークスペースアカウントを停止する。
**C.** 元従業員のパスワードをリセットし、ワークスペースライセンスを有効な状態に保ちます。
**D.** 元従業員のワークスペースアカウントのライセンスタイプをアーカイブ済みユーザーライセンスに変更します。
**Answer: (**解答を表示する**)**
元従業員のアカウントをアーカイブユーザーライセンスに切り替えることで、データとドキュメントが確実に保存され、管理者とチームはアクティブなワークスペースライセンスの全額を支払うことなくアクセス権を維持できます。アーカイブユーザーライセンスは、アカウントへの不正アクセスを防ぎながらドキュメントへのアクセスを維持するための費用対効果の高い方法です。

最新問題**: 15**
あなたの会社の営業チームは、Googleドキュメントで多くのビジネス提案書を作成しています。彼らはテンプレートを使用して提案書作成プロセスを効率化したいと考えています。営業チームがアクセスできる、あらかじめ項目が入力されたドキュメントテンプレートを作成する必要があります。どうすればよいでしょうか？
**A.** Googleドライブでテンプレートを作成します。営業チームに編集権限を付与します。
**B.** Googleドライブでテンプレートを作成します。各営業担当者用にコピーを作成します。各テンプレートの所有権を営業担当者に譲渡します。
**C.** 管理コンソールで組織のブランディングを有効にします。Google ドライブでテンプレートを作成します。作成したテンプレートを組織全体のデフォルトテーマとテンプレートに追加します。
**D.** Googleドライブでテンプレートを作成し、ファイルをPDFとしてダウンロードします。ダウンロードしたPDFファイルを、営業チームと共有しているドライブにアップロードします。
**Answer: C (**メーッセージを残す**)**
営業チームが簡単にアクセスして提案プロセスを効率化できる、あらかじめ入力済みのセクションを含むドキュメントテンプレートを作成するには、Google Workspaceのテンプレートギャラリーを利用するのが最も効率的で一元管理しやすい方法です。これには、組織のブランディングを有効にし（基本的なテンプレートには必須ではありませんが、組織テンプレートではよく使用されます）、作成したテンプレートを組織全体または特定のグループのデフォルトのテーマとテンプレートに追加することが含まれます。

最新問題**: 16**
貴社は最近、Google Workspace Marketplaceから無料のメールマーケティングプラットフォームを導入しました。しかし、マーケティングチームはプラットフォームを通じて顧

客の連絡先情報にアクセスしたり、メールを送信したりすることができません。問題の原因を特定する必要があります。まず最初に何をすべきでしょうか？
**A.** メールマーケティングプラットフォームの購読が有効で最新の状態であることを確認してください。
**B.** メールマーケティングプラットフォームに付与されているOAuthスコープを確認し、プラットフォームが連絡先とGmailにアクセスできることを確認してください。
**C.** 管理コンソールの 『サードパーティアプリのアクセス管理」設定が有効になっていることを確認してください。
**D.** セキュリティ調査ツールを使用して、Gmail のログを確認します。
**Answer: B (**メーッセージを残す**)**
Google Workspace Marketplace からサードパーティ製アプリケーションをインストールすると、Google Workspace のデータとサービスにアクセスするための特定の権限 (OAuth スコープ) が要求されます。マーケティングチームが顧客の連絡先情報にアクセスできなかったり、メールを送信できなかったりする場合、最も可能性の高い原因は、インストールまたは承認プロセス中に、インストールされたメールマーケティングプラットフォームに連絡先と Gmail に必要な OAuth スコープが付与されていなかったことです。



最新問題**: 17**
規制要件に基づき、貴社はドイツに所在する従業員のデータを欧州域内に、米国に所在する従業員のデータを米国域内に保管する必要があります。ドイツの従業員は米国の従業員とは別の組織単位 (OU) に属しています。従業員データの保管場所が、それぞれの所在地に関する規制に準拠していることを確認する必要があります。
あなたはどうすべきでしょうか？
**A.** 従業員に、会社のコンピューターに文書を保存するために、デスクトップ版のDriveを使用するように指示してください。
**B.** 2つのグループを作成します。従業員を所在地に基づいてドイツグループまたは米国グループに割り当てます。
Googleドライブの信頼ルールを使用して、グループ間での共有を防止してください。

**C.** 管理コンソールで 「データリージョン」機能に移動します。ドイツの従業員には 「ヨーロッパ」リージョンを選択し、米国の従業員には 「米国」リージョンを選択します。
**D.** 管理コンソールで 「データ領域」機能に移動します。 「設定なし」を選択します。
**Answer: C (**メーッセージを残す**)**
Google管理コンソールの 「データリージョン」機能を使用すると、組織単位 (OU) ごとに地理的な場所に基づいてデータの保存場所を指定できます。これにより、ドイツに勤務する従業員のデータはヨーロッパ内に、米国に勤務する従業員のデータは米国内に保存され、データ所在地の規制要件を満たすことができます。このアプローチにより、コンプライアンスが自動化され、手動での追跡や追加の設定が不要になります。

最新問題**: 18**
退職する従業員がおり、その従業員のマイドライブには多数のファイルが保存されています。その従業員のマネージャーは、これらのファイルへのアクセスを維持したいと考えています。退職する従業員のGoogle Workspaceアカウントをオフボーディングしつつ、マネージャーが引き続きファイルにアクセスできるようにし、Googleが推奨する手順に従う必要があります。どうすればよいでしょうか？
**A.** Google Vault を使用して、退職する従業員の所属する組織単位 (OU) のデータ保持ポリシーを設定します。Google アーカイブユーザーライセンスを割り当てます。
**B.** 退職する従業員に、退職前に自分のマイドライブフォルダをマネージャーと共有するように指示してください。退職する従業員の最終日に、Google Workspaceアカウントを削除してください。
**C.** Google Takeoutを使用して、退職する従業員のGoogleドライブデータをダウンロードします。退職する従業員のGoogle Workspaceアカウントを削除する前に、データを管理者のGoogleドライブにアップロードします。
**D.** ユーザー削除プロセス中に、退職する従業員のファイルの所有権をマネージャーに譲渡します。
**Answer: D (**メーッセージを残す**)**
退職する従業員のファイルの所有権をマネージャーに移管することで、マネージャーはマイドライブに保存されているファイルを含め、すべてのファイルにアクセスでき、ファイルのダウンロードや共有といった追加の手順は不要になります。この方法はGoogleが推奨する手順に準拠しており、従業員のアカウントが削除された後もファイルが適切に管理されることを保証します。このプロセスは、退職手続き中に効率的に実行することで、アクセスの継続性を確保できます。

最新問題**: 19**
貴社は、Google Chat スペースにおける注意散漫や不適切なコンテンツを最小限に抑えたいと考えています。信頼できる従業員に、メッセージの削除や特定のチャットスペースへのユーザーのアクセス禁止権限を与える必要があります。どうすればよいでしょうか？
**A.** 信頼できる従業員を関連するチャットスペースのモデレーターに任命してください。

**B.** 不適切なコンテンツの共有をブロックするデータ損失防止（DLP）ルールを作成する
**C.** セキュリティ調査ツールを使用して、チャットメッセージを監査および監視します。
**D.** 管理者が特別に承認したものを除くすべてのチャットスペースを無効にします。
**Answer: A (**メーッセージを残す**)**
信頼できる従業員を該当するチャットスペースのモデレーターに任命することで、必要に応じてメッセージの削除やユーザーのブロックを行うための権限を与えることができます。これは、不適切なコンテンツを管理し、スペース内で良好かつ生産的な環境を維持するための最も効率的な方法です。モデレーターは、より複雑で制限的な解決策を必要とせずに、問題に直接対処することができます。

最新問題**: 20**
組織内でChromeブラウザに関するサポート案件が増加していることに気付きました。Chromeブラウザに障害やサービス停止が発生している可能性があると疑っています。この問題に関する情報が公開されているかどうか、また解決までの予定期間が発表されているかどうかを確認する必要があります。まず最初に何をすべきでしょうか？
**A.** Google管理コンソール内のヘルプアシスタントを使用して、最近障害が発生したかどうかを確認してください。
**B.** HAR ファイルを収集し、Google Admin Toolbox を使用して潜在的な障害を特定します。
**C.** Google Workspace ステータス ダッシュボードを確認します。
**D.** Chrome Enterprise サポートにケースを登録してください。
**Answer: (**解答を表示する**)**
Chromeブラウザなど、Google製品でサービス障害が発生し、組織に影響が出ている場合、既知の障害とその復旧予定を確認するための最初で最も効率的な手順は、Google Workspaceステータスダッシュボードを確認することです。このダッシュボードでは、Chrome Enterpriseを含むさまざまなGoogle Workspaceサービスのステータスに関するリアルタイム情報が表示されます。
オプションCが正しい最初のステップである理由と、他のオプションが即効性に欠ける、あるいは必要な初期情報が得られる可能性が低い理由を以下に示します。
C. Google Workspaceのステータスダッシュボードを確認します。
Google Workspace ステータス ダッシュボードは、Google Workspace サービスに影響を与える障害、サービスの中断、およびメンテナンスに関する公式情報源です。各サービスの現在のステータス、報告された問題が表示され、障害が確認された場合は、調査の進捗状況や解決までの推定時間などの最新情報も提供されることがよくあります。このダッシュボードを最初に確認することで、Google が Chrome の広範囲にわたる問題を認識しているかどうか、また、利用可能な情報があるかどうかをすぐに把握できます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照情報 :Google Workspace 管理者ヘルプドキュメントでは、サービス停止状況を確認するためにステータスダッシュボードを使用するよう管理者に明示的に指示しています。 Google Workspace

のステータスを確認する」などの記事や類似のタイトルの記事では、ダッシュボードの情報にアクセスして解釈する方法が説明されています。これは、Google からサービスの状態に関する情報が提供される主要なチャネルです。
A. Google管理コンソール内のヘルプアシスタントを使用して、最近障害が発生したかどうかを確認してください。
Google 管理コンソールのヘルプアシスタントは、一般的なトラブルシューティングやヘルプ記事の検索に役立つツールです。ステータスダッシュボードへのリンクを提供したり、既知の問題に関する情報を提供したりすることはできますが、障害発生状況を即座に把握するための最も直接的でリアルタイムな情報源ではありません。障害発生状況を即座に特定するには、ステータスダッシュボードを直接確認する方が迅速かつ確実です。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: ヘルプ アシスタントは、主に管理者がタスクを実行できるようにガイドし、サポート ドキュメントへのアクセスを提供することを目的として設計されており、サービス停止のリアルタイム ステータス インジケーターとして設計されているわけではありません。
B. HARファイルを取得し、Google管理ツールボックスを使用して潜在的な障害を特定します。
HAR（HTTPアーカイブ）ファイルの収集とGoogle管理ツールボックスの使用は、ユーザーレベルまたはネットワークレベルでの特定の技術的問題の診断に適しています。これらのツールは、既知の障害ではないことを確認した後、個々の問題のトラブルシューティングや根本原因の調査に役立ちますが、広範囲にわたるサービス障害が疑われる場合の最初のステップではありません。これらは、より詳細な技術分析のためのツールです。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google 管理ツールボックスのドキュメントでは、特定の問題を診断およびトラブルシューティングするためのさまざまなユーティリティについて説明しています。これらのツールは、多くの場合、技術的な専門知識を必要とし、広範囲にわたるサービス停止ではなく、ローカルまたはアカウント固有の問題に焦点を当てています。
D. Chrome Enterpriseサポートに問い合わせてください。
調査の結果、既知の障害に関する情報が見つからない場合、または一般的なサービス障害とは関係のない特定の問題についてサポートが必要な場合は、サポートケースを登録するのが適切です。サポートからの回答には時間がかかるため、既知の障害とその期間を確認する最も迅速な方法ではありません。まずは公式のステータスダッシュボードをご確認ください。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google Workspace 管理者ヘルプでは、サポートへの問い合わせ方法とタイミングについて説明しています。サービス関連の問題が発生した場合は、通常、まずステータスダッシュボードを確認することをお勧めします。
したがって、Chromeブラウザで既知の障害やサービス中断が発生しているかどうか、また解決までの見込み期間を把握するための最も効率的な最初のステップは、Google Workspaceのステータスダッシュボードを確認することです。

最新問題: **21**
貴社の営業組織単位（OU）の現在のデータ保存制限は、
ユーザーあたり10GBのストレージ容量が必要です。この組織単位（OU）内の営業担当者の一部は、共有サービス全体で100GBのストレージを必要としています。最小限の混乱と最小限の設定手順で、この営業担当者の一部のみのストレージ容量を増やす必要があります。どうすればよいですか？
**A.** ユーザーのサブセットをサブOUに移動し、そのサブOUに100GBのストレージ制限を割り当てます。
**B.** 特定のユーザーグループに、100GBの制限がある共有ドライブにドキュメントを保存するように指示します。
**C.** 販売OUのストレージ制限を100GBに変更します。
**D.** 設定グループを作成し、ユーザーのサブセットをそのグループに追加します。グループのストレージ制限を100GBに設定します。
**Answer: A (**メーッセージを残す**)**
営業担当者のサブセットをサブ組織単位（OU）に移動させ、
そのサブOUのストレージ制限を100GBに設定することで、営業チームの他のメンバーに影響を与えることなく、該当ユーザーのストレージ容量を効率的に増やすことができます。このアプローチにより、ストレージ容量の増加を必要とする特定のユーザーを対象にすることができ、業務への影響や設定手順を最小限に抑えることができます。

最新問題: **22**
貴社の従業員が、機密文書を許可されていない外部関係者と共有している可能性があります。機密情報が漏洩していないかを迅速に確認する必要があります。どうすべきでしょうか？
**A.** セキュリティ調査ツールで従業員のドライブログイベントを確認してください。
**B.** Admin SDK Reports API を使用してドライブへのアクセスを監査します。
**C.** セキュリティ調査ツール内で従業員のユーザーログイベントを確認します。
**D.** セキュリティダッシュボードを使用して、ユーザーの外部共有に関するカスタムレポートを作成します。
**Answer: A (**メーッセージを残す**)**
従業員が機密文書を外部に共有したかどうかを迅速に判断するには、Google 管理コンソールのセキュリティ調査ツールを使用し、該当従業員のアカウントに関連付けられたドライブのログイベントを具体的に確認してください。このツールは、共有操作を含む Google ドライブに関連するユーザーアクティビティを一元的に監査できる場所を提供します。
オプションAが最も直接的かつ効率的な第一歩である理由は以下のとおりです。
A. セキュリティ調査ツールで、従業員のドライブログイベントを確認する。
セキュリティ調査ツールを使用すると、管理者はユーザーアクティビティや潜在的なセキュリティインシデントに関連するさまざまなログを調べることができます。対象となる

従業員のドライブログイベントに焦点を当てることで、ファイル共有、アクセス許可の変更、外部アクセスなどの操作をすばやくフィルタリングして確認できます。これにより、従業員が実際に外部にドキュメントを共有したかどうか、また誰と共有したかを直接把握できます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google Workspace 管理者向け公式ヘルプドキュメントの 「セキュリティ調査ツール」 または類似のタイトル）には、その機能が説明されています。特に、 「ドライブログイベントの調査」のセクションでは、管理者がフィルタを使用して、特定のユーザーと期間による外部共有を含むファイル共有アクティビティを表示する方法が詳しく説明されています。このツールは、データアクセスと共有に関連するユーザーの操作を迅速に監査する必要があるシナリオに最適です。
B. Admin SDK Reports APIを使用してドライブへのアクセスを監査する。
Admin SDK Reports API を使用すると、Drive のアクティビティに関する詳細な情報を取得できますが、使用するにはプログラミングスキルとカスタムスクリプトまたはアプリケーションの設定が必要です。これは、潜在的なセキュリティ上の懸念を迅速に調査する方法ではありません。セキュリティ調査ツールは、管理者がコーディングを必要とせずにこのような調査を実行できる、ユーザーフレンドリーなインターフェースを提供します。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google Workspace 管理者 SDK のドキュメントには、レポート API とその機能について説明されています。カスタム レポートや自動化には強力ですが、組み込みのセキュリティ調査ツールと比較すると、迅速なアドホック セキュリティ調査には最速の方法ではありません。
C. セキュリティ調査ツール内で、従業員のユーザーログイベントを確認する。
セキュリティ調査ツールのユーザーログイベントは、Googleドライブだけでなく、ログイン試行、パスワード変更、デバイス管理操作など、より広範なアクティビティを網羅しています。これによりある程度の状況把握はできますが、ドライブログイベントに比べるとファイル共有アクティビティへの特化度は低くなっています。機密文書が共有されたかどうかを迅速に判断するには、ドライブ関連のアクションを直接フィルタリングする方が効率的です。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :セキュリティ調査ツールのドキュメントには、ユーザーログやドライブログなど、利用可能なさまざまなログソースについて説明されています。ファイル共有の調査には、ドライブログがより具体的で関連性の高い情報を提供します。
D. セキュリティダッシュボードを使用して、ユーザーの外部共有に関するカスタムレポートを作成します。
セキュリティダッシュボードは、組織のセキュリティ体制の概要を示し、あらかじめ用意されたレポートと分析結果を提供します。カスタムレポートを作成することもできますが、その場合、セキュリティ調査ツールで特定の従業員のドライブログイベントを直接調査するよりも時間がかかる可能性があります。調査ツールは、ユーザーの操作に関連する

潜在的なセキュリティインシデントを的確かつ迅速に分析できるように設計されています。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google Workspace 管理者ヘルプの 「セキュリティ ダッシュボード」に関するドキュメントでは、セキュリティの全体的な傾向と洞察に焦点を当てたその機能について説明しています。パターンを特定するのに役立つ場合もありますが、セキュリティ調査ツールは、特定のユーザー操作や潜在的なデータ漏洩をオンデマンドで調査するのに適しています。
したがって、従業員が機密文書を外部に共有したかどうかを迅速かつ効率的に直接的に判断する最も方法は、セキュリティ調査ツールで従業員のドライブログイベントを確認することです。

最新問題: **23**
貴社はカナダ、イタリア、米国にオフィスを構えています。従業員がこれらの地域からのみ社内GmailとGoogleドライブにアクセスできるようにしたいと考えています。どうすればよいでしょうか？
**A.** コンテキスト認識アクセスを使用して、地理的な場所に基づいてアクセスレベルを作成し、それを Gmail と Drive に割り当てます。
**B.** 会社のGmailおよびDriveへのアクセスには、会社のデバイスの使用を必須とする。
**C.** メール配信を制限し、Google ドキュメントの通知をブロックするためのアドレス リストを作成します。
**D.** 地理的に3つの場所からのみアクセスを許可するデータ保護ルールを作成します。
**Answer: A (**メーッセージを残す**)**
コンテキスト認識型アクセスにより、管理者は地理的位置などのユーザー属性に基づいてアクセスレベルを定義できます。これは、地域ごとにサービスへのアクセスを制限するための、適切かつサポートされている方法です。

最新問題: **24**
貴社では最近、Google Workspaceインスタンスへの不正アクセス試行が増加しています。Googleが推奨する対策に従いながら、ユーザーアカウントのセキュリティを強化する必要があります。どのような対策を講じるべきでしょうか？
**A.** パスワード回復オプションを無効にして、権限のない人物がユーザーアカウントにアクセスするのを防ぎます。
**B.** 強力なパスワードポリシーを導入し、テキストメッセージを使用した2段階認証（2SV）としてテキストメッセージを有効にする。
**C.** すべてのユーザーに対して、2段階認証（2SV）方法として物理的なセキュリティキーの使用を強制します。
**D.** 特殊文字、数字、大文字を含めることをユーザーに義務付ける強力なパスワードポリシーを強制します。
**Answer: C (**メーッセージを残す**)**

2段階認証（2SV）に物理セキュリティキーの使用を義務付けることで、ユーザーアカウントを不正アクセスから保護する非常に安全な方法が実現します。物理セキュリティキーは、たとえ攻撃者がユーザーのパスワードを知っていたとしても、フィッシングや盗難が容易ではないため、最も堅牢な2要素認証方法の一つです。Googleは、不正アクセスに対する強力な保護を提供する物理セキュリティキーを2SVの方法として使用することを推奨しています。

最新問題: **25**
あなたは、特定の共有ドライブへのアクセス権を付与するために使用する、社内のグループ構造を設計しています。このソリューションでは、従業員の職務に基づいて自動的に従業員を追加および削除する必要があります。どうすればよいでしょうか？
**A.** セキュリティグループを作成します。目的の職務役割を持つすべての従業員を追加します。セキュリティグループに共有ドライブへのアクセス権を付与します。
**B.** 配布リストを作成します。目的の職務役割を持つすべての従業員を追加します。配布リストに共有ドライブへのアクセス権を付与します。
**C.** 動的グループを作成します。メンバーシップの条件を希望する職務に設定します。動的グループに共有ドライブへのアクセス権を付与します。
**D.** 構成グループを作成します。例外的にユーザーを追加します。構成グループに共有ドライブへのアクセス権を付与します。
**Answer: (**解答を表示する**)**
動的グループは、職務などのユーザー属性に基づいてメンバーシップを自動的に管理します。このアプローチにより、従業員は役割に基づいてグループに自動的に追加または削除されるため、手作業を最小限に抑え、グループが常に最新のチーム構成を反映することが保証されます。この動的グループに共有ドライブへのアクセス権を付与することで、適切なユーザーが適切な権限を持つようになり、頻繁な手動更新は不要になります。

最新問題: **26**
貴社のイノベーションチームには、試作機器を備えた専用の部屋があります。この部屋を予約可能にし、機器を追加し、予約の重複がないようにする必要があります。この部屋にアクセスできるのは、イノベーションチームと営業部長のみです。どうすればよいでしょうか？
**A.** 会議室専用のGoogleカレンダーリソースを別途作成します。両チームからの予約リクエストを手動で管理します。
**B.** イノベーションチーム用のGoogleグループと、営業部長用のGoogleグループをそれぞれ作成します。両方のグループに会議室のカレンダーを共有します。
**C.** 会議室のGoogleカレンダーイベントを作成します。イベントをイノベーションチームと営業部長と共有します。

**D.** 会議室リソースの Google カレンダー設定を編集します。権限設定を調整して、イノベーションチームと営業部長グループのみがこのカレンダーで時間を表示および予約できるようにします。
**Answer: D (**メーッセージを残す**)**
会議室専用のGoogleカレンダーリソースを作成し、アクセス権限設定を調整することで、イノベーションチームと営業部長のみが会議室を予約できるようにすることができます。この方法により、会議室予約を一元管理できるだけでなく、Googleカレンダーが自動的にスケジュールを管理し、重複予約を防ぐため、競合も防止できます。

最新問題**: 27**
本日、貴社は既存のドメイン名を使用してGoogle Workspace Business Starterに登録されました。チームメンバーを追加し、メールやその他のサービスへのアクセス権限を管理したいと考えています。
しかし、新しいユーザーアカウントを作成したり、ユーザー設定を変更したりすることができません。この問題を解決する必要があります。どうすればよいでしょうか？
**A.** 転送ツールを実行して、管理されていないユーザーをワークスペースアカウントに移動します。
**B.** DNS設定でドメインの所有権を確認してください。
**C.** 機能が有効になるまで、登録後24時間お待ちください。
**D.** Google Workspace Enterprise エディションにアップグレードします。
**Answer: B (**メーッセージを残す**)**
Google Workspaceでユーザーと設定を管理するには、ドメインの所有権を確認する必要があります。ドメインが確認できない場合、新しいユーザーアカウントを作成したり、ユーザー設定を変更したりすることはできません。
DNS設定を確認し、ドメイン認証プロセスを完了することで問題が解決し、Google Workspaceでユーザーとサービスを管理できるようになります。

最新問題**: 28**
貴社は規制遵守監査を受けています。監査の一環として、特定のプロジェクトに関連するすべての電子通信を、将来の法的証拠開示手続きに備えて保存できることを証明する必要があります。この目的を達成するには、Google Vault を設定する必要があります。どうすればよいでしょうか？
**A.** セキュリティ調査レポートを使用して、Vault ログイベントを表示します。
**B.** 検索およびエクスポート機能を使用して、プロジェクト期間内のすべての関連する通信を特定します。
**C.** Google Workspace 内で、メール、チャット、ドライブなど、プロジェクトに関連するすべてのデータソースに対して、案件と保留を作成します。
**D.** プロジェクトデータ用のカスタム保持ポリシーを作成します。ポリシーが必要な保持期間を網羅していることを確認してください。

**Answer: C (メーッセージを残す)**
案件を作成し、関連するデータソースに保留措置を講じることで、ユーザーが削除しようとした場合でも、特定のプロジェクトに関連するすべての通信が確実に保存されます。これは、電子情報開示に関する法的または規制上の要件への準拠を維持するのに役立ち、監査プロセス中にデータが変更または削除されないことを保証します。

最新問題: **29**
外部データへのコネクタを備え、Google スプレッドシートのデータを活用し、モバイル アプリケーションとして簡単に共有できる自動化されたアプリケーションまたはプロセスを作成する必要があります。どうすればよいでしょうか？
**A.** App Engineを使用してアプリケーションを作成します。アプリケーションをワークスペース環境に接続します。
**B.** 外部データをBigQueryにコピーします。接続されたシートを使用してデータを操作します。
**C.** さまざまなデータソースを接続するためのAppSheetアプリケーションを作成します。モバイルアプリケーションを設定します。
**D.** Apps Scriptを使用して自動化プロセスを作成します。Google スプレッドシートでそのプロセスを実行します。
**Answer: C (メーッセージを残す)**
AppSheetは、Googleスプレッドシートなどの外部データソースに接続できるモバイルアプリケーションを簡単に作成できるノーコードプラットフォームです。さまざまなソースからのデータを統合し、モバイルデバイス上で簡単に共有できる自動化アプリを迅速に構築するのに最適です。AppSheetを使えば、高度な開発スキルを必要とせずに、モバイルアプリケーションを効率的に作成、カスタマイズ、展開できます。

最新問題: **30**
あなたは、従業員によるGoogleサイトの使用を禁止している大規模組織に勤務しています。しかし、最高情報責任者室から割り当てられたプロジェクトに取り組むため、5つの異なる部署から3名ずつで構成されるタスクフォースが最近結成されました。このタスクフォースのユーザーに一時的にGoogleサイトの使用を許可する必要があります。あなたは、業務への影響を最小限に抑え、最も効率的な方法を採用したいと考えています。どうすればよいでしょうか？
**A.** タスクフォースの15人のユーザーそれぞれに対して、Googleサイトへのアクセスを有効にしてください。
**B.** タスクフォースの15人のユーザー用の構成グループを作成します。Google Sitesにそのグループへのアクセス権を付与します。
**C.** 15名のタスクフォースユーザーを新しい組織単位（OU）に配置します。OUに対してGoogleサイトへのアクセスを有効にします。

**D.** タスクフォースのユーザー15名分のアクセスグループを作成します。Google Sitesにそのグループへのアクセス権を付与します。
**Answer: C (**メーッセージを残す**)**
タスクフォースメンバー専用の新しい組織単位（OU）を作成し、そのOUに対してGoogleサイトへのアクセス権限を付与するのが、最も混乱が少なく効率的な方法です。この方法であれば、タスクフォースのユーザーのみを対象に、組織の他のメンバーに影響を与えることなく、Googleサイトへの一時的なアクセス権を付与できます。また、このソリューションはアクセス権限を明確に制御できるため、タスクフォースの作業完了後には簡単に変更できます。

最新問題**: 31**
エンドユーザーは、Googleドライブに数千ものファイルを保存しています。これらのファイルは、ドライブのラベルを使ってきちんと整理されています。エンドユーザーに対し、契約書であるファイルを素早く特定する方法をアドバイスする必要があります。
あなたはどうすべきでしょうか？
**A.** ユーザーにGoogleドライブAPIを使用して 契約書」というキーワードでファイルを検索するようアドバイスしてください。
**B.** ユーザーに、Drive で 契約書」というキーワードを含むファイルを検索し、 自分が変更したファイル」フィルターを使用するようにアドバイスします。
**C.** ユーザーに 契約書」とラベル付けされたファイルを検索するようにアドバイスします。
**D.** ユーザーに調査ツールを使用して、 契約」というキーワードを含む、あなたが更新したファイルを検索するようにアドバイスします。
**Answer: (**解答を表示する**)**
Googleドライブではファイルが既にラベル付けされて整理されているため、ユーザーが契約書であるすべてのファイルを素早く特定する最も効率的な方法は、 契約書」というラベルが付いたファイルを検索することです。
これにより、契約書としてラベル付けされたファイルのみがフィルタリングされて表示されるため、必要なファイルを見つけるための最も迅速かつ簡単な方法となります。

最新問題: **32**
貴社のセキュリティチームは、従業員のモバイルデバイスのセキュリティを確保するために、パスコードの強制適用とリモートアカウント消去機能という2つの要件を要求しています。セキュリティチームは、モバイルデバイスにエージェントをインストールしたり、追加のライセンスを購入したりすることを望んでいません。
従業員はiOSとAndroidのデバイスを混在させて使用しています。これらの要件を満たす必要があります。どうすればよいでしょうか？
**A.** サードパーティ製のエンタープライズモビリティ管理（EMM）プロバイダーを導入する。
**B.** iOSデバイス向けに高度なモバイル管理を設定し、Androidデバイス向けに基本的なモバイル管理を設定します。
**C.** iOSおよびAndroidデバイス両方の基本管理を設定します。
**D.** iOSおよびAndroidデバイスの両方に対して高度な管理を設定します。
**Answer: (**解答を表示する**)**
Google Workspace の高度なモバイル管理機能は、サードパーティ製アプリや追加ライセンスを必要とせずに、モバイルデバイスを保護するために必要な機能を提供します。これには、パスコードの強制適用や、iOS および Android デバイス両方でのリモートアカウント消去機能の有効化が含まれます。高度な管理機能により、セキュリティ要件を満たしながら、効率的な設定と組織の既存ライセンスの範囲内での運用を実現します。

最新問題: **33**
貴社で Workspace Business Plus ライセンスをご利用の従業員が、まもなく長期休暇に入ります。従業員は Google Workspace データへのアクセスを必要としませんが、チームメンバーは従業員のデータにアクセスする必要があります。従業員が休暇から復帰したら、アカウント、データ、メール、共有ドキュメントへのアクセスを復元する必要があります。休暇中のコストを最小限に抑えつつ、従業員の Workspace データを保持する必要があります。どうすればよいでしょうか？
**A.** 管理者コンソールでアカウントを停止します。
**B.** アーカイブユーザーライセンスを購入し、そのライセンスを従業員に割り当てます。
**C.** Takeoutを使用してアカウントデータをエクスポートし、管理コンソールでユーザーライセンスを削除します。
**D.** 従業員のメールをコピーし、ファイルの所有権をチームメイトに譲渡します。ユーザーアカウントを削除します。
**Answer: B (**メーッセージを残す**)**
従業員が長期休暇中にGoogle Workspaceのデータを保持し、チームメンバーがそのデータにアクセスできるようにし、従業員の復帰時にアカウントを完全に復元することを前提と

してコストを最小限に抑えるには、アーカイブユーザーライセンスを購入して従業員に割り当てるのが最善の方法です。
オプションBがすべての要件を満たす最も適切かつ費用対効果の高い解決策である理由は以下のとおりです。
B. アーカイブユーザーライセンスを購入し、そのライセンスを従業員に割り当てます。
Google Workspace では、フルユーザーライセンスよりも大幅に低コストでアーカイブユーザーライセンスを提供しています。アーカイブユーザーライセンスをアカウントに割り当てると、データ（Gmail、Drive、その他の Workspace サービスを含む）は保持され、他の承認済みユーザー（管理者や委任されたチームメンバーなど）がアクセスできます。ユーザー自身はログインしたりサービスを利用したりできないため、コストを最小限に抑えることができます。従業員が復帰したら、フル Business Plus ライセンスを簡単にアカウントに再割り当てでき、データの損失や複雑な復元プロセスなしに、フルアクセスを復元できます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料: Google Workspace 管理者向け公式ヘルプドキュメントの「アーカイブ済みユーザーライセンスについて」または類似のタイトル）には、このシナリオがアーカイブ済みユーザーライセンスの想定される使用例として明記されています。このドキュメントでは、コスト削減、データの保持、管理者によるデータへのアクセス（およびアクセス権の委任）、ユーザーが復帰した際のフルライセンスへのスムーズな移行について説明しています。
A. 管理者コンソールでアカウントを停止する。
アカウントを一時停止すると、ユーザーはアカウントにアクセスできなくなりますが、通常はライセンス費用全額が発生します。管理者は一時停止中のアカウント内の一部のデータにアクセスできる場合がありますが、アーカイブ済みユーザーライセンスのようなコスト削減効果は得られません。さらに、一時停止期間やGoogleのポリシーによっては、有効なライセンスまたはアーカイブ済みライセンスがない場合、長期的なデータ保持に影響が出る可能性があります。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料: Google Workspace 管理者ヘルプの「ユーザーの一時停止または復元」に関するドキュメントでは、アカウントの一時停止機能について説明しています。このドキュメントは、アクセス権の一時的な取り消しに重点を置いており、委任アクセスの可能性を伴う長期的な費用対効果の高いデータ保存については扱っていません。
C. Takeoutを使用してアカウントデータをエクスポートし、管理コンソールでユーザーライセンスを削除します。
Google Takeout を使用するとユーザーデータをエクスポートできますが、これは Google Workspace と直接統合されていない別のアーカイブを作成します。エクスポートされたデータへのチームメンバーのアクセス権限を付与するのは煩雑で、元の Workspace 環境内でアクセスするほどスムーズではありません。ユーザーライセンスを削除すると、Google Workspace でのデータ保持が停止され、従業員が復帰した際にアカウントを完全に復元するにはデータを再インポートする必要があり、これは複雑で時間がかかり、データ損失や

不整合につながる可能性があります。このオプションはライセンスを削除することでコストを最小限に抑えることができますが、容易なアクセスとシームレスな復元という利点が失われます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google Takeout のドキュメントでは、Google サービスからデータをエクスポートする目的について説明しています。これは主に個人利用またはデータ移行を目的としたものであり、Workspace 環境内での一時的なデータ保存や共同アクセスを目的としたものではありません。通常、ライセンスを削除すると、代替手段 (アーカイブ済みユーザー ライセンスなど) が適用されていない限り、一定期間後にデータが削除されます。
D. 従業員のメールをコピーし、ファイルの所有権をチームメイトに譲渡します。ユーザーアカウントを削除します。
この方法は、データの大幅な操作とコンテキストの喪失を伴います。メールをコピーしてもメールボックスの構造全体が保持されない可能性があり、重要な情報が欠落する可能性があります。ファイルの所有権の移転は複雑になる場合があり、すべての種類のデータや共有アイテムを網羅できない可能性があります。ユーザーアカウントを削除するとデータが完全に削除されるため、従業員が復帰した際に完全に復元することは不可能になります。このオプションは、従業員のワークスペースデータを保持し、後でアカウントを復元するには適していません。
Google Workspace のアソシエイト管理者向けトピックガイドまたはドキュメントの参考資料 :Google Workspace のアカウント管理のベストプラクティスでは、復帰する従業員のためにユーザーアカウントとデータを保持することを重視しています。一時的な休暇を目的としたアカウントの削除は、データ復旧やアカウント再作成に伴う困難とリスクがあるため、強く推奨されません。
したがって、データの保存、チームメンバーへのアクセス権の付与、休暇中のコストの最小化、復帰時の完全な復元といったすべての要件を満たす最も適切な対策は、アーカイブユーザーライセンスを購入し、従業員に割り当てることです。

最新問題: **34**
あなたの組織は、ユーザー数がわずか5人の小規模代理店を買収しました。これらの新しい従業員のためにユーザーアカウントを作成する必要があります。代理店のユーザーは、元のメールアドレスを使用する必要があります。代理店のドメインをセカンダリドメインとして追加しました。どうすればよいですか？
**A.** ディレクトリAPIを使用して、ユーザーアカウントを自動的に作成します。
**B.** 管理コンソールからユーザーを手動で作成します。ユーザーアカウントを作成する際に、メールアドレスに使用する代理店ドメインを選択してください。
**C.** Google Cloud Directory Sync (GCDS) を使用して、既存のディレクトリからユーザーを同期します。
**D.** CSVファイルを使用してすべてのユーザーを一括アップロードします。
**Answer: B (**メーッセージを残す**)**

ここで重要な情報は、「ユーザーは5人まで」と「代理店ユーザーは元のメールアドレスを使用する必要があります。代理店のドメインをセカンダリドメインとして追加しました」です。ユーザー数が少ない場合（5人）、管理コンソールで手動で作成するのが最も簡単でシンプルな方法です。新しいユーザーを作成する際、管理コンソールでは、Google Workspaceアカウントに追加したセカンダリドメインの中から、プライマリメールアドレスのドメインを選択できます。

最新問題: **35**
社内の特定のユーザーグループにYouTubeへのアクセス権を付与し、Merchant Centerへのアクセスを制限したい場合、どうすればよいでしょうか？
**A.** 社内の全ユーザーに対してYouTubeを有効にします。特定のグループまたは組織単位（OU）に対しては、Merchant Centerへのアクセスを個別に制限します。
**B.** YouTubeとMerchant CenterをカスタムWebアプリとして作成します。グループまたは組織単位（OU）レベルでアクセス ポリシーを適用します。
**C.** Google サポートに連絡し、特定のユーザーグループに対して YouTube へのアクセスを有効にし、Merchant Center へのアクセスを制限するよう依頼してください。
**D.** 特定のユーザーグループまたは組織単位（OU）レベルでYouTubeへのアクセスを有効にします。Merchant Centerへのアクセスを無効にします。
**Answer: D (**メーッセージを残す**)**
グループまたは組織単位（OU）レベルでYouTubeへのアクセスを有効にすることで、特定のユーザーグループを対象にYouTubeへのアクセスを許可できます。同時に、同じユーザーに対してMerchant Centerへのアクセスを無効にすることで、YouTubeにはアクセスできるがMerchant Centerにはアクセスできないように設定できます。この方法は、Google Workspaceの組み込み機能を利用して、ユーザーグループまたは組織単位に基づいてアクセスを管理します。

最新問題: **36**
貴社は、業務でChromeブラウザを使用するすべての従業員が特定のセキュリティ設定と構成設定を遵守することを徹底したいと考えています。社内で使用されるChromeブラウザを管理・制御しつつ、最も費用対効果の高いソリューションを選択する必要があります。どのような対策を講じるべきでしょうか？
**A.** Chromeブラウザを管理するために、サードパーティ製のソフトウェア展開ソリューションを使用してください。
**B.** 従業員のデバイスすべてをリモートでワイプし、最新バージョンのChromeブラウザを使用していることを確認します。
**C.** Chromeブラウザを組織のドメインに登録し、Chromeブラウザのポリシーを適用します。
**D.** 潜在的なセキュリティリスクを防ぐため、従業員のChromeブラウザ上のすべての拡張機能を無効にしてください。

**Answer: C (メーッセージを残す)**
Google Workspace（特にChrome Enterprise Core。Google Workspaceのエディションに付属または無料で提供されることが多い）は、組織全体でChromeブラウザを管理するための組み込み機能を提供します。ドメインにChromeブラウザを登録することで、Google管理コンソールからポリシーを一元的に適用し、セキュリティ設定、拡張機能、アップデートなどを制御できます。これは、既存のGoogle Workspaceサブスクリプション以外に追加のソフトウェアやライセンス費用を必要としない、Google独自のクラウドベースのソリューションであり、「最も費用対効果の高いソリューション」と言えます。他のオプションが、費用を抑えてChromeブラウザを管理するのに適していない理由は以下のとおりです。
A. サードパーティのソフトウェア展開ソリューションを使用して Chrome ブラウザを管理する。これは可能ですが、サードパーティのソフトウェア、そのライセンス、および場合によってはメンテナンスに追加のコストがかかります。Google Workspace はネイティブのブラウザ管理を提供しているため、サードパーティのソリューションは「最も安価」ではありません。B. すべての従業員デバイスをリモートでワイプして、最新の Chrome ブラウザ バージョンを使用していることを確認する。デバイスのリモートワイプは、紛失/盗難デバイスまたは退職時に通常使用される、極端で混乱を招く措置です。これは、ブラウザ バージョンを管理したり、構成設定を適用したりするための標準的または適切な方法ではありません。また、生産性の低下と IT 作業のコストの面でも非常に高額になります。
D. 従業員のChromeブラウザで全ての拡張機能を無効にして、潜在的なセキュリティリスクを防止します。拡張機能を無効にすることでリスクを軽減できる場合もありますが、これは広範囲にわたる、場合によっては業務に支障をきたす可能性のある措置であり、正当かつ必要な拡張機能が無効になった場合、従業員の生産性を阻害する可能性があります。さらに重要なのは、これは適用できる可能性のあるポリシーの1つに過ぎず、ブラウザを一元的に、かつ費用対効果の高い方法で管理するための唯一の方法ではないということです。Chromeブラウザのポリシーでは、特定の拡張機能を許可/ブロックするなど、より詳細な制御が可能です。
Google Workspace管理者からの参考情報：
ユーザーまたはブラウザに対する Chrome ポリシーの設定 :これは、Chrome ブラウザを管理するための重要な管理機能です。組織のドメインに登録されている Chrome ブラウザにポリシーを適用する方法について説明します。
参照：
Chrome Enterprise Core :これは、Chromeブラウザで利用できる無料のクラウドベースの管理機能の概要を示しており、多くの場合、Google Workspaceと統合されています。Chrome Enterprise Coreでは、「クラウドベースの管理とレポート機能が無料で利用可能」であることが明記されています。
Google Workspace で Google Chrome の管理を最大限に活用する :この記事では、「Google Workspace では、Google Chrome 管理のための基本的なポリシーが無料で利用できる」ことを改めて強調しています。Google Workspace 管理コンソールに組み込まれている Chrome ブラウザ管理機能を活用することで、組織は追加のソフトウェア費用をかけ

ずに Chrome の設定とセキュリティを一元的に管理でき、最も費用対効果の高いソリューション」という要件を満たすことができます。

最新問題: **37**
貴社では、機密情報を含む社内ニュースレターを全従業員にメールで配信しています。このニュースレターが外部アドレスに不正に転送されていることが判明し、データ漏洩につながる恐れがあります。これを防ぐため、正当な社内共有は許可しつつ、不正転送を自動的に検知してブロックするソリューションを導入する必要があります。
あなたはどうすべきでしょうか？
**A.** ニュースレターに、外部への共有が禁止されていることをユーザーに警告するバナーを追加する。
**B.** 社内ニュースレターを対象としたGmailコンテンツコンプライアンスルールを作成し、外部転送の事例を特定します。転送が検出された場合、メッセージを拒否するようにルールを設定します。
**C.** Gmail APIを使用して送信済みメールをスキャンし、ニュースレターの内容と外部受信者を特定するApps Scriptプロジェクトを開発します。違反したユーザーのアクセス権を自動的に取り消します。
**D.** ニュースレターの件名を変更し、外部への転送に対する警告を追加するコンテンツコンプライアンスルールを作成します。
**Answer: B (**メーッセージを残す**)**
Gmailのコンテンツコンプライアンスルールを使用すると、社内ニュースレターを特定の対象に絞り込み、外部アドレスに転送された際に自動的に検出できます。このようなメッセージを拒否することで、機密情報の不正な共有を防ぎつつ、社内での共有は許可できます。
このソリューションは、手動による介入なしにデータセキュリティポリシーを効果的に適用できます。

最新問題: **38**
貴社のある部署が、Google Workspaceの最新のAI搭載機能を利用したいと考えています。Geminiは高度な機能を備えていることはご存知でしょう。企業データが人間の目に触れないように、Geminiの導入を管理しつつ、その部署にGeminiの機能への即時アクセスを提供する必要があります。どうすればよいでしょうか？
**A.** 部門の組織単位でGeminiを有効にし、部門内のユーザーにGeminiライセンスを割り当てます。
**B.** 管理者コンソールを通じてGeminiの導入状況を監視し、ライセンスを割り当てる前に、より多くのユーザーが導入するまで待ちます。
**C.** その部署の非ライセンスユーザー向けにGeminiを有効にして、無料サービスにすぐにアクセスできるようにします。

**D.** 組織に対してアルファ機能を有効にし、すべてのユーザーにジェミニライセンスを割り当てます。
**Answer: A (**メーッセージを残す**)**
特定の部署がGoogle WorkspaceでGeminiの機能にすぐにアクセスできるようにすると同時に、管理権限を維持し、企業データのプライバシーを確保するには、その部署が属する組織単位でGeminiを有効にし、その組織単位内のユーザーに必要なライセンスを割り当てる必要があります。この方法により、対象を絞った展開が可能になり、機能が管理されたGoogle Workspace環境内で確実に使用されるようになります。

最新問題: **39**
貴社の法務部から、特定のプロジェクトに関連するすべてのデータを保存するよう求める訴訟保留命令が出されました。メール、文書、チャットなど、このプロジェクトに関するすべてのデータが永久に保存され、ユーザーが削除できないようにする必要があります。どうすればよいでしょうか？
**A.** プロジェクトに関連付けられているすべてのユーザーとデータソースを含むホールドを Google Vault に作成します。
**B.** プロジェクトに関わるすべてのユーザーにアーカイブユーザーライセンスを割り当てます。
**C.** Google Vaultで、GmailとDriveのすべてのデータを無期限に保持する保持ルールを設定します。
**D.** Google Workspace からプロジェクト関連のすべてのデータをエクスポートし、データを別の安全な場所に保存します。
**Answer: A (**メーッセージを残す**)**
プロジェクトに関連するすべてのデータ（メール、ドキュメント、チャットなど）を保存し、ユーザーによる削除を防ぐには、Google Vaultでホールドを作成する必要があります。ホールドを設定することで、ユーザーの操作に関わらずデータが無期限に保存され、プロジェクトに関連付けられているユーザーおよびデータソース（Gmail、Drive、Chatsなど）に適用されます。これは、訴訟ホールドの要件を満たすための最も効率的かつコンプライアンスに準拠した方法です。

最新問題: **40**
最近、組織のGoogleドライブの使用状況に不審な傾向が見られました。複数のユーザーが機密文書を組織外に共有しており、会社のデータセキュリティポリシーに違反している可能性があります。不正共有に関与したユーザーと、その範囲を特定する必要があります。どうすればよいでしょうか？
**A.** 管理コンソールで組織の共有ポリシーを確認し、外部共有を防止するようにポリシーを更新してください。
**B.** セキュリティ状態ページを使用して、Drive の共有設定の誤りを特定します。
**C.** セキュリティ調査ツールを使用してドライブのログを分析し、ユーザーを特定します。

**D.** セキュリティセンターでアクティビティルールを作成し、今後の外部共有イベントを通知します。
**Answer: C (**メーッセージを残す**)**
問題の核心は、責任のあるユーザーと、過去に不正に共有されたデータの範囲を特定することです。セキュリティ調査ツールは、まさにこの目的のために設計されています。このツールを使用すると、管理者はドライブログを含むさまざまな監査ログを検索および分析し、特定のイベント、ユーザー、およびデータを特定できます。

最新問題**: 41**
あなたの組織は、ユーザー数がわずか5人の小規模代理店を買収しました。これらの新しい従業員のためにユーザーアカウントを作成する必要があります。代理店のユーザーは、元のメールアドレスを使用する必要があります。代理店のドメインをセカンダリドメインとして追加しました。どうすればよいですか？
**A.** ディレクトリAPIを使用して、ユーザーアカウントを自動的に作成します。
**B.** 管理コンソールからユーザーを手動で作成します。ユーザーアカウントを作成する際に、メールアドレスに使用する代理店ドメインを選択してください。
**C.** Google Cloud Directory Sync (GCDS) を使用して、既存のディレクトリからユーザーを同期します。
**D.** CSVファイルを使用してすべてのユーザーを一括アップロードします。
**Answer: B (**メーッセージを残す**)**
ここで重要な情報は、「ユーザーは5人まで」と「代理店ユーザーは元のメールアドレスを使用する必要があります。代理店のドメインをセカンダリドメインとして追加しました」です。ユーザー数が少ない場合（5人）、管理コンソールで手動で作成するのが最も簡単でシンプルな方法です。新しいユーザーを作成する際、管理コンソールでは、Google Workspaceアカウントに追加したセカンダリドメインの中から、プライマリメールアドレスのドメインを選択できます。
他の選択肢が適さない理由は以下のとおりです。
A. ディレクトリAPIを使用してユーザーアカウントを自動的に作成する。ディレクトリAPIは自動化に利用できますが、スクリプト作成またはプログラミングの知識が必要です。たった5人のユーザーであれば、これは過剰であり、不必要な複雑さを招きます。
C. Google Cloud Directory Sync (GCDS) を使用して、既存のディレクトリからユーザーを同期します。GCDS は、オンプレミスのディレクトリ (Active Directory など) から Google Workspace へ多数のユーザーとグループを同期するように設計されています。ユーザーが 5 人だけで、継続的な同期が必要な既存のディレクトリがない場合は、GCDS は複雑すぎて不要です。
D. CSVファイルを使用して全ユーザーの一括アップロードを行う。CSVファイルを使用した一括アップロードは、ユーザー数が多い場合（例えば、数十人、数百人、数千人）に効率的です。ユーザーが5人だけの場合、特に一度限りの作業であれば、CSVファイルを作成する

のにかかる時間は、グラフィカルインターフェースで1人ずつ作成するのと同等かそれ以上になる可能性があります。
Google Workspace管理者からの参考情報：
ユーザーを一人ずつ追加する :この方法は、少数のユーザー（例：10人以下）を追加する場合に特におすすめです。ユーザー作成プロセス中に、利用可能なドメインの中からユーザーのメインメールアドレスに使用するドメインを選択できます。
参照：
ドメインまたはドメインエイリアスを追加します。これは質問で言及されている前提条件となる手順です（「代理店のドメインをセカンダリドメインとして追加しました」）。これにより、そのドメインをユーザーのメールアドレスに使用できるようになります。

最新問題: **42**
あなたは、従業員によるGoogleサイトの使用を禁止している大規模組織に勤務しています。しかし、最高情報責任者室から割り当てられたプロジェクトに取り組むため、5つの異なる部署から3名ずつで構成されるタスクフォースが最近結成されました。このタスクフォースのユーザーに一時的にGoogleサイトの使用を許可する必要があります。あなたは、業務への影響を最小限に抑え、最も効率的な方法を採用したいと考えています。
あなたはどうすべきでしょうか？
**A.** タスクフォースの15人のユーザーそれぞれに対して、Googleサイトへのアクセスを有効にしてください。
**B.** タスクフォースの15人のユーザー用の構成グループを作成します。Google Sitesにそのグループへのアクセス権を付与します。
**C.** 15名のタスクフォースユーザーを新しい組織単位（OU）に配置します。OUに対してGoogleサイトへのアクセスを有効にします。
**D.** タスクフォースのユーザー15名分のアクセスグループを作成します。Google Sitesにそのグループへのアクセス権を付与します。
**Answer: C (**メーッセージを残す**)**
タスクフォースメンバー専用の新しい組織単位（OU）を作成し、そのOUに対してGoogleサイトへのアクセス権限を付与するのが、最も混乱が少なく効率的な方法です。この方法であれば、タスクフォースのユーザーのみを対象に、組織の他のメンバーに影響を与えることなく、Googleサイトへの一時的なアクセス権を付与できます。また、このソリューションはアクセス権限を明確に制御できるため、タスクフォースの作業完了後には簡単に変更できます。

最新問題: **43**
組織内でChromeブラウザに関するサポート案件が増加していることに気付きました。Chromeブラウザに障害やサービス停止が発生している可能性があると疑っています。この問題に関する情報が公開されているかどうか、また解決までの予定期間が発表されているかどうかを確認する必要があります。まず最初に何をすべきでしょうか？

**A.** Google管理コンソール内のヘルプアシスタントを使用して、最近障害が発生したかどうかを確認してください。
**B.** HAR ファイルを収集し、Google Admin Toolbox を使用して潜在的な障害を特定します。
**C.** Google Workspace ステータス ダッシュボードを確認します。
**D.** Chrome Enterprise サポートにケースを登録してください。
**Answer: C (**メーッセージを残す**)**
Chromeブラウザなど、Google製品でサービス障害が発生し、組織に影響が出ている場合、既知の障害とその復旧予定を確認するための最初で最も効率的な手順は、Google Workspaceステータスダッシュボードを確認することです。このダッシュボードでは、Chrome Enterpriseを含むさまざまなGoogle Workspaceサービスのステータスに関するリアルタイム情報が表示されます。

最新問題**: 44**
貴社では、従業員が独自のメール配信リストやウェブフォーラムを作成・管理できるように、Google Groups for Business を有効にしています。社内グループの利用を妨げることなく、ユーザーが Google Workspace アカウントで外部の Google グループに参加できないようにする必要があります。
あなたはどうすべきでしょうか？
**A.** Google Groups for Business の「この組織外からのグループへのアクセス」の設定を「非公開」に設定します。
**B.** 「その他の Google サービス」で、ルート組織単位で Google グループをオフにします。
**C.** ディレクトリ API を使用して、ユーザーが作成したグループの設定を変更し、外部ユーザーがグループにアクセス、表示、または投稿できるようにする機能を無効にします。
**D.** Google Groups for Business の「デフォルト」設定で、会話の表示権限を「すべての組織ユーザー」に設定します。
**Answer: (**解答を表示する**)**
「組織外からのグループへのアクセス」を「非公開」に設定すると、組織内のユーザーがGoogleグループを利用できる一方で、外部のユーザーが外部のGoogleグループに参加することはできなくなります。この設定により、組織のメンバーのみが内部グループに参加してやり取りできるようになり、内部グループの利用に影響を与えることなく、外部からのアクセスを効果的に遮断できます。

最新問題**: 45**
本日、貴社は既存のドメイン名を使用してGoogle Workspace Business Starterに登録しました。チームメンバーを追加し、メールやその他のサービスへのアクセスを管理したいと考えていますが、新しいユーザーアカウントを作成したり、ユーザー設定を変更したりすることができません。この問題を解決する必要があります。どうすればよいでしょうか？

**A.** 転送ツールを実行して、管理されていないユーザーをワークスペースアカウントに移動します。
**B.** DNS設定でドメインの所有権を確認してください。
**C.** 機能が有効になるまで、登録後24時間お待ちください。
**D.** Google Workspace Enterprise エディションにアップグレードします。
**Answer: (**解答を表示する**)**
Google Workspaceでユーザーと設定を管理するには、ドメインの所有権を確認する必要があります。ドメインが検証されていない場合、新しいユーザーアカウントを作成したり、ユーザー設定を変更したりすることはできません。DNS設定を確認し、ドメイン検証プロセスを完了することで、この問題が解決し、Google Workspaceでユーザーとサービスを管理できるようになります。

最新問題**: 46**
貴社のセキュリティチームは、不正な外部ファイル共有を調査できるはずです。
セキュリティチームがセキュリティ調査ツールを使用できることを確認する必要があり、最小権限の原則に従わなければなりません。どうすればよいでしょうか？
**A.** セキュリティチームの代理人にスーパー管理者権限を付与します。
**B.** 事前に構築されたレポートロールを作成します。そのロールをセキュリティチームのエイリアスに割り当てます。
**C.** Driveの監査ログをセキュリティチームと共有してください。
**D.** セキュリティセンターの権限を持つカスタム管理者ロールを作成します。そのロールを個々のセキュリティチームメンバーに割り当てます。
**Answer: (**解答を表示する**)**
セキュリティセンターの権限を持つカスタム管理者ロールを作成することで、セキュリティチームが不正な外部ファイル共有を調査するために必要なアクセス権限を確保しつつ、最小権限の原則を遵守することができます。このアプローチにより、セキュリティチームはスーパー管理者ロールなど、不必要な広範な権限を付与することなく、必要な特定の権限のみを取得できます。

最新問題: **47**
貴社の従業員数名が、悪意のあるウェブサイトへのリンクを含むメッセージを受け取りました。これらのメッセージは、貴社の人事部から送信されたようです。どの従業員がこれらのメールを受け取ったかを特定し、今後同様の事態が再発しないようにする必要があります。どうすればよいでしょうか？
**A.** メールログ検索を使用して送信者のメールアドレスを検索します。メッセージを受信したユーザーを特定します。Gmailでスパムとしてマークし、メッセージを削除し、ゴミ箱を空にするように指示します。
**B.** セキュリティ調査ツールを使用して送信者のメールアドレスを検索します。メッセージをフィッシングとしてマークします。Gmailの「スパム、フィッシング、マルウェア」設定で送信者のメールアドレスをブロック済み送信者リストに追加して、今後のメッセージを自動的に拒否します。
**C.** メッセージを受信したユーザーのリストを作成します。受信者のメールアドレスをGoogle Vaultで検索します。悪意のあるメールをPSTファイル形式でエクスポートしてダウンロードします。送信者のメールアドレスをGmailの隔離リスト設定に追加し、今後その送信者からのメールが隔離されるようにします。
**D.** セキュリティ調査ツールを使用して送信者のメールアドレスを検索します。メッセージを削除します。Gmailの設定で、なりすましと認証保護のセキュリティオプションを有効にします。
**Answer: B** (メーッセージを残す)
Google Workspace のセキュリティ調査ツールを使用すると、影響を受けたユーザーとメッセージを特定できます。メッセージをフィッシングとしてマークすることで、その悪意のある性質を認識し、ユーザーを保護することができます。送信者のメールアドレスをブロック済み送信者リストに追加すると、その送信者からの今後のメッセージが自動的にブロックされ、同様のインシデントの再発を防ぐことができます。

最新問題: **48**
貴社は最近、社内メールアドレスに使用する新しいドメイン名を取得しました。しかし、ドメインが認証されていないため、Google Workspaceの一部の機能にアクセスできません。ドメインを認証する必要があります。どうすればよいでしょうか？
**A.** Googleサポートに連絡して、手動認証を依頼してください。
**B.** Google WorkspaceをMXレコードをDNSゾーンに追加します。
**C.** ドメインレジストラにDNSゾーンにTXTレコードを追加するよう依頼してください。
**D.** ドメイン用のSSL証明書を購入してください。
**Answer:** (解答を表示する)

Google Workspaceでドメイン名を認証し、すべての機能にアクセスするには、通常、そのドメインの所有権を証明する必要があります。最も一般的な方法の1つは、ドメインのDNS（ドメインネームシステム）ゾーンに特定のTXTレコードを追加することです。Googleはこの固有のTXTレコードを提供しており、DNSに公開されると、Googleは所有権を確認できます。
オプションCが正しい方法である理由と、他の方法がGoogle Workspaceにおけるドメイン検証の標準的な方法ではない理由を以下に示します。
C. ドメイン登録業者に、DNSゾーンにTXTレコードを追加するよう依頼してください。
Google Workspaceでは、ドメインのDNS設定に追加する必要のある固有のTXTレコードが提供されます。このレコードには、Googleのシステムがチェックする特定のコードが含まれています。ドメインのパブリックDNSでこのレコードを見つけることで、Googleはユーザーがドメインを管理しており、Google Workspaceで使用する権限があることを確認できます。通常、DNSレコードは、ドメイン登録業者またはDNSホスティングプロバイダーが提供するインターフェースを通じて管理します。
Google Workspace 管理者の関連トピックガイドまたはドキュメントの参照: 「Google Workspace のドメインを確認する」または類似のタイトル）に関する公式の Google Workspace 管理者ヘルプドキュメントには、ドメインを確認するさまざまな方法が明確に説明されています。TXT レコードの追加は、一貫して主要な推奨方法として提示されています。ドキュメントには、次の正確な手順が記載されています。ドメインホスト (ドメインレジストラ) にサインインします。
ドメインのDNSレコードにアクセスしてください。
Googleから提供された値を使用してTXTレコードを追加します。
TXTレコードを保存します。
Google管理コンソールで検証プロセスを開始します。すると、GoogleがTXTレコードを確認します。
A. Googleサポートに連絡し、手動認証を依頼してください。
Googleサポートはドメイン認証の問題解決を支援してくれますが、それが最初の標準的な手順ではありません。手動認証は通常、TXTレコードやCNAMEレコードなどの標準的な方法が使えない場合や失敗した場合にのみ行われます。まずは、標準的なDNSベースの認証方法のいずれかを試してみてください。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照情報 :Google Workspace 管理者ヘルプに記載されている標準的なドメイン検証プロセスは、主に DNS レコードの変更を伴います。これらの標準的な方法で問題が発生した場合は、通常、サポートに問い合わせることになります。
B. Google Workspaceを指すMXレコードをDNSゾーンに追加します。
MXレコードは、メールを適切なメールサーバーに転送するためのものです。ドメインでGmailを使用するには、最終的にはMXレコードを設定する必要がありますが、MXレコードの追加はドメインの所有権を確認するための主要な手順ではありません。ドメインの所有

権確認は、メールを完全に設定し、Googleがドメインのメールフローを管理する前に完了する必要があります。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google Workspace 管理者ヘルプドキュメントでは、ドメイン検証の手順とメールの MX レコードの設定手順が明確に区別されています。所有権を証明するために、まず検証を行う必要があります。
D. ドメイン用のSSL証明書を購入する。
SSL（Secure Sockets Layer）証明書は、主にウェブサイトにおいて、ウェブサーバーとブラウザ間の通信を保護するために使用されます。これは、Google Workspaceサービスのドメイン所有権の検証とは関係ありません。SSL証明書はウェブサイトのセキュリティにとって重要ですが、Google Workspaceの設定において、Googleがドメインの所有権を確認する手段にはなりません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google Workspace のドメイン検証方法は、ドメインの DNS レコードに対する制御権限を証明することに特化しています。SSL 証明書は、ウェブセキュリティの別の側面です。
したがって、Google Workspaceでドメインを認証するための正しい手順は、GoogleにTXTレコードをリクエストし、ドメイン登録業者の管理インターフェースを通じて、そのレコードをドメインのDNSゾーンに追加することです。

最新問題: **49**
エンドユーザーは、Googleドライブに数千ものファイルを保存しています。ファイルはドライブのラベルできちんと整理されています。エンドユーザーに、契約書であるすべてのファイルを素早く特定する方法をアドバイスする必要があります。あなたは何をすべきでしょうか？
**A.** ユーザーにGoogleドライブAPIを使用して 契約書」というキーワードでファイルを検索するようアドバイスしてください。
**B.** ユーザーに、Drive で 契約書」というキーワードを含むファイルを検索し、 自分が変更したファイル」フィルターを使用するようにアドバイスします。
**C.** ユーザーに 契約書」とラベル付けされたファイルを検索するようにアドバイスします。
**D.** ユーザーに調査ツールを使用して、 契約」というキーワードを含む、あなたが更新したファイルを検索するようにアドバイスします。
**Answer: C (**メーッセージを残す**)**
Googleドライブではファイルが既にラベル付けされて整理されているため、ユーザーが契約書を素早く特定する最も効率的な方法は、 契約書」というラベルが付いたファイルを検索することです。これにより、契約書としてラベル付けされたファイルのみが表示されるため、必要なファイルを最も迅速かつ簡単に見つけることができます。

最新問題: **50**

貴社は機密性の高い社内プロジェクトのために臨時社員を雇用しました。Googleドライブに保存されている機密性の高いプロジェクトデータは、社内ドメイン内でのみ共有されるようにする必要があります。しかし、過度に制限したくはありません。どうすればよいでしょうか？
**A.** ドメインのドライブ共有オプションを許可リストに登録されたドメインに制限します。
**B.** チームダッシュボードからドライブ共有設定をオフにします。
**C.** Drive DLP ルールを作成し、機密性の高い内部プロジェクト名を検出対象として使用します。
**D.** ドメインのドライブ共有オプションを内部のみに設定します。
**Answer: D (**メーッセージを残す**)**
ドメインのドライブ共有オプションを 内部のみ」に設定することで、機密性の高いプロジェクトデータが組織の内部ユーザーのみに限定されます。これにより、外部への共有を防ぎつつ、チームメンバーが組織内で自由に共同作業を行うことができます。セキュリティの維持と、コラボレーションに対する不必要な制限の回避という、適切なバランスが実現されます。

最新問題: **51**
貴社では、従業員が機密性の高い企業データにアクセスするために、共有のChromebookワークステーションを提供しています。機密データがローカルに保存されないこと、および使用後に閲覧データが消去されるようにデバイスを設定する必要があります。どうすればよいですか？
**A.** Chromeで一時モードを強制します。ドキュメント、スプレッドシート、ドライブなどの機密性の高いワークスペースアプリのオフラインアクセスを無効にします。
**B.** ゲストセッション管理機能を有効にし、最大ユーザーセッション時間を設定します。
**C.** Chromeで一時モードを強制します。有効期限が厳密に設定されているすべてのワークスペースアプリでオフラインアクセスを許可します。
**D.** すべてのワークスペースアプリのオフラインアクセスを無効にします。Chromeブラウザセッションでシークレットモードを有効にします。
**Answer: A (**メーッセージを残す**)**
Chromeで一時モードを有効にすると、閲覧データはセッションごとに完全に消去され、Chromebookにローカルに保存されることはありません。また、ドキュメント、スプレッドシート、ドライブなどの機密性の高いワークスペースアプリのオフラインアクセスを無効にすることで、ユーザーが機密データをローカルにダウンロードまたは保存することを防ぎます。この組み合わせにより、使用後にデバイスに機密データが残ることを防ぎ、安全な環境が実現します。

最新問題: **52**
貴社は顧客ファイルにクレジットカード情報を収集しています。Googleドライブのデータに関して、クレジットカード番号を含むファイルが誤って外部ユーザーと共有されること

を防止するポリシーを策定する必要があります。また、共有が発生した場合は、報告のために記録する必要があります。どのような対策を講じるべきでしょうか？
**A.** 事前定義されたクレジットカード番号検出器を使用するデータ損失防止（DLP）ルールを作成し、アクションを「外部共有をブロック」に設定し、「イベントをログに記録」オプションを有効にします。
**B.** Gmailのコンテンツコンプライアンスを有効にし、クレジットカード番号を含むメール添付ファイルが外部の受信者に送信されないようにするルールを作成します。
**C.** サードパーティ製のデータ損失防止ソリューションを導入し、Driveと統合して高度なコンテンツ検出機能を提供する。
**D.** クレジットカード番号を含むファイルを、指定した期間後に自動的に削除するデータ保持ポリシーを設定します。
**Answer: (**解答を表示する**)**
事前定義されたクレジットカード番号検出機能を備えたデータ損失防止（DLP）ルールを使用すると、機密性の高いクレジットカード情報を含むファイルの意図しない共有を特定して防止できます。「外部共有をブロック」アクションを設定することで、そのようなファイルが外部に共有されることを確実に防ぐことができます。「イベントをログに記録」オプションを有効にすると、監査および報告のために外部共有のインシデントが記録され、セキュリティ要件と報告要件の両方を満たすことができます。

最新問題**: 53**
貴社は一部の従業員向けにGeminiのライセンスを購入しました。マーケティング部門と営業部門のユーザーのみがGeminiの機能にアクセスできるように、最も効率的な方法を用いる必要があります。どのような対策を講じるべきでしょうか？
**A.** マーケティングまたは営業部門の新規ユーザーにGeminiライセンスを割り当てるスクリプトを作成します。このスクリプトを毎日実行します。
**B.** マーケティングおよび営業用の組織単位（OU）を作成します。そのOUにGeminiライセンスを割り当て、そのOUのみでGeminiを有効にします。
**C.** マーケティング部門と営業部門の各ユーザーにGeminiライセンスを割り当てます。
**D.** 組織全体でGeminiを有効にします。他の部署のユーザーにはGeminiを使用しないように指示します。
**Answer: B (**メーッセージを残す**)**
マーケティング部門と営業部門をそれぞれ独立した組織単位（OU）として作成することで、Geminiライセンスをこれらの部門のみに適用できます。Geminiを特定のOUのみに適用することで、マーケティング部門と営業部門の従業員のみがGeminiの機能にアクセスできるようになり、効率的で拡張性の高いソリューションが実現します。これにより、他の部門のユーザーへの手動割り当てや不要な指示が不要になります。

最新問題**: 54**

組織内のユーザーから、社内イベントの受信者がカレンダーイベントの招待状を受け取っていないという報告がありました。この問題の原因を特定する必要があります。どうすればよいですか？
**A.** イベント受信者のカレンダー設定で営業時間が設定されているかどうかを確認してください。
**B.** イベント作成者に対してカレンダーサービスがオフになっていないか確認してください。
**C.** カレンダーイベントに50人以上の参加者がいるかどうかを確認します。
**D.** イベントの受信者がカレンダーの設定で新しいイベントのメール通知をオフにしていないか確認してください。
**Answer: D (**メーッセージを残す**)**
社内ユーザーからGoogleカレンダーのイベント招待が届かないという報告があった場合、まず最初に確認すべき原因は、受信者側のGoogleカレンダーの通知設定です。ユーザーは通知設定をカスタマイズできるため、新しいイベントに関するメール通知をオフにしている可能性があります。
オプションDが最も重要な第一歩である理由と、他のオプションがこの特定の問題の主な原因である可能性が低い理由を以下に示します。
D. イベントの受信者がカレンダーの設定で新しいイベントのメール通知をオフにしていないか確認してください。
Googleカレンダーでは、新規イベント、イベントの変更、リマインダーなどに関するメール通知を受け取るかどうかなど、さまざまな通知設定を構成できます。受信者が新規イベントのメール通知を無効にしている場合、イベントがカレンダーに正しく追加されていても、受信トレイに招待状は届きません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google カレンダーの公式ヘルプドキュメント（通知設定の変更」など）では、ユーザーがイベント通知をカスタマイズする方法が説明されています。これには、新しいイベントのメール通知をオフにするオプションも含まれます。管理者は個々のユーザーの通知設定を直接管理することはありませんが、これらのユーザーレベルのコントロールを理解することは、トラブルシューティングを行う上で非常に重要です。管理者は、ユーザーにこれらの設定を確認するよう案内する場合があります。
A. イベントの受信者のカレンダー設定で営業時間が設定されているかどうかを確認してください。
Googleカレンダーの営業時間設定は、主に会議のスケジュール提案や、ユーザーの空き状況が他のユーザーにどのように表示されるかに影響します。営業時間設定によって、ユーザーがイベントの招待を受け取れなくなるわけではありません。受信者が営業時間を設定しているかどうかに関わらず、新しいイベントのメール通知が送信されるのを妨げることはありません ただし、リソースのスケジュール設定に関連する非常に特殊で特殊なケースは除きますが、ここではその詳細は示されていません）。

Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google カレンダーのヘルプドキュメント 勤務時間と場所を設定する」では、営業時間の目的が説明されています。営業時間は、招待状の受信ではなく、空き状況とスケジュールに関連しています。
B. イベント作成者に対してカレンダーサービスがオフになっていないか確認してください。
イベント作成者のカレンダーサービスが無効になっている場合、そもそもカレンダーイベントを作成したり送信したりすることはできません。受信者が招待状を受け取っていないことからもわかるように、ユーザーが招待状を作成して送信した以上、作成者のカレンダーサービスは有効になっているはずです。
Google Workspace 管理者向けの関連トピックガイドまたはドキュメントのリファレンス: Google Workspace 管理者ヘルプの ユーザーに対して Google カレンダーを有効または無効にする」に関するドキュメントでは、管理者がカレンダー サービスへのアクセスを制御する方法について説明しています。ユーザーに対してサービスが無効になっている場合、そのユーザーはカレンダー機能を利用できません。
C. カレンダーイベントに50人以上の参加者がいるかどうかを確認します。
カレンダーイベントに追加できるゲストの数には制限があるかもしれませんが、通常、この制限を超えると、招待プロセス中にイベント作成者にエラーメッセージが表示され、受信者が招待を受け取れないという事態にはなりません。仮に受信に影響を与えるような制限があったとしても （これは、妥当な範囲内の内部ユーザーにとって一般的な問題として文書化されていません）、最初に確認すべき事項ではありません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google カレンダーのヘルプドキュメントには、ゲストの数の制限について記載されている場合があります。ただし、これらの制限は通常、ゲストの追加、更新の送信、または応答の表示に関するものであり、組織内の一部の受信者への配信が完全に失敗することを意味するものではありません。
したがって、社内受信者がカレンダーイベントの招待を受け取らない理由をトラブルシューティングする際の最も論理的な最初のステップは、受信者自身にカレンダーの通知設定を確認してもらい、新しいイベントのメール通知が有効になっていることを確認することです。

最新問題: **55**
貴社はメールにGoogle Workspaceを使い始めたいと考えています。ドメインはサードパーティプロバイダーを通じて認証済みです。メールをGoogle Workspaceにルーティングする必要があります。どうすればよいでしょうか？
**A.** ドメインのAレコードをGoogleのメールサーバーを指すように変更してください。
**B.** 現在お使いのメールシステムで転送ルールを設定し、すべてのメッセージをGmailに転送します。

**C.** ドメインのMXレコードを、セットアップ手順に記載されているGoogle WorkspaceのMXレコードに更新してください。
**D.** ドメインを「gmail.com」にマッピングするCNAMEレコードを作成します。
**Answer: C (メーッセージを残す)**
メールを Google Workspace にルーティングするには、ドメインの MX (メール交換) レコードを更新して、Google のメールサーバーを指すようにする必要があります。この手順により、ドメイン宛てのメールが Google Workspace の Gmail アカウントに確実に配信されます。MX レコードは、Google Workspace の設定プロセス中に表示されるセットアップ手順に記載されています。

最新問題: **56**
貴社の法務部は、時間的制約のある合併・買収（M&A）案件に取り組んでいます。現在休職中の従業員からの特定のメール通信へのアクセスが緊急に必要です。貴社の現在のデータ保持ポリシーは無期限に設定されています。データプライバシーを確保しながら、法務部が必要とするメールを取得する必要があります。どうすればよいでしょうか？
**A.** IT部門に、関連するメールに直接アクセスして法務部門に転送するよう指示してください。
**B.** 法務部門に、M&A関連のメールに限定した制限付き範囲で、従業員のメールアカウントへのアクセス権を一時的に付与する。
**C.** 従業員のメールボックスへの代理アクセス権限を持つ同僚に、関連するメールを特定して法務部に転送するよう依頼してください。
**D.** Google Vaultを使用して、M&A取引に特化した案件を作成します。従業員のメールボックス内から関連するメールを検索します。関連するメールをエクスポートして、法務部門と共有します。
**Answer:** (解答を表示する)
Google Vaultを使用してM&A取引専用の案件を作成することで、法的要件を満たし、安全かつプライバシーに準拠したメールの取得が可能になります。合併・買収に関連する特定のメールを検索し、エクスポートして、従業員のメールボックスへの直接アクセスを許可することなく法務部門と共有できます。この方法により、データのプライバシーと組織のポリシーへの準拠の両方が確保されます。

最新問題: **57**
貴社では、購入承認アプリケーションが必要です。ユーザーは購入に必要な情報を入力し、管理者の承認を得るために提出する必要があります。ウェブとモバイルデバイスの両方で利用できるアプリケーションを作成するためのソリューションを提案してください。貴社にはソフトウェア開発者がおらず、外部のソフトウェア開発会社に依頼する予算もありません。どうすればよいでしょうか？

**A.** 組織内でデータベース、データ取得のためのバックエンドサービス、およびアプリケーションのユーザーインターフェースのためのフロントエンドサービスを備えたアプリケーションを開発することを提案します。
**B.** サードパーティのアプリケーションプロバイダーを利用できる予算が確保できるまで、組織は引き続き手動でリクエストを承認することを提案します。
**C.** アプリケーションの作成にAppSheetを使用することを組織に提案します。
**D.** 組織がAppScriptを使用して、購入データを保存するためのGoogleスプレッドシートにリンクされたフォームを作成することを提案します。
**Answer: C (**メーッセージを残す**)**
AppSheetは、ソフトウェア開発スキルを必要とせずにカスタムアプリケーションを作成できるノーコードプラットフォームです。Webとモバイルデバイスの両方で使用できるアプリケーションを構築できます。AppSheetを使用することで、組織は購入プロセスの要件を満たす承認アプリケーションを効率的に作成でき、開発者を雇用したりサードパーティのアプリケーションプロバイダーを利用したりする必要のない、費用対効果の高いソリューションとなります。

最新問題: **58**
組織内のユーザーから、社内イベントの受信者がカレンダーイベントの招待状を受け取っていないという報告がありました。この問題の原因を特定する必要があります。どうすればよいですか？
**A.** イベント受信者のカレンダー設定で営業時間が設定されているかどうかを確認してください。
**B.** イベント作成者に対してカレンダーサービスがオフになっていないか確認してください。
**C.** カレンダーイベントに50人以上の参加者がいるかどうかを確認します。
**D.** イベントの受信者がカレンダーの設定で新しいイベントのメール通知をオフにしていないか確認してください。
**E.** イベントの受信者がカレンダーの設定で新しいイベントのメール通知をオフにしていないか確認してください。
**Answer: (**解答を表示する**)**
Googleカレンダーでは、新規イベント、イベントの変更、リマインダーなどに関するメール通知を受け取るかどうかなど、さまざまな通知設定を構成できます。受信者が新規イベントのメール通知を無効にしている場合、イベントがカレンダーに正しく追加されていても、受信トレイに招待状は届きません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :Google カレンダーの公式ヘルプドキュメント（通知設定の変更」など）では、ユーザーがイベント通知をカスタマイズする方法が説明されています。これには、新しいイベントのメール通知をオフにするオプションも含まれます。管理者は個々のユーザーの通知設定を直接管理することはありませんが、これらのユーザーレベルのコントロールを理解することは、トラ

ブルシューティングを行う上で非常に重要です。管理者は、ユーザーにこれらの設定を確認するよう案内する場合があります。
A. イベントの受信者のカレンダー設定で営業時間が設定されているかどうかを確認してください。
Googleカレンダーの営業時間設定は、主に会議のスケジュール提案や、ユーザーの空き状況が他のユーザーにどのように表示されるかに影響します。営業時間設定によって、ユーザーがイベントの招待を受け取れなくなるわけではありません。受信者が営業時間を設定しているかどうかに関わらず、新しいイベントのメール通知が送信されるのを妨げることはありません ただし、リソースのスケジュール設定に関連する非常に特殊で特殊なケースは除きますが、ここではその詳細は示されていません）。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google カレンダーのヘルプドキュメント 勤務時間と場所を設定する」では、営業時間の目的が説明されています。営業時間は、招待状の受信ではなく、空き状況とスケジュールに関連しています。
B. イベント作成者に対してカレンダーサービスがオフになっていないか確認してください。
イベント作成者のカレンダーサービスが無効になっている場合、そもそもカレンダーイベントを作成したり送信したりすることはできません。受信者が招待状を受け取っていないことからもわかるように、ユーザーが招待状を作成して送信した以上、作成者のカレンダーサービスは有効になっているはずです。
Google Workspace 管理者向けの関連トピックガイドまたはドキュメントのリファレンス: Google Workspace 管理者ヘルプの ユーザーに対して Google カレンダーを有効または無効にする」に関するドキュメントでは、管理者がカレンダー サービスへのアクセスを制御する方法について説明しています。ユーザーに対してサービスが無効になっている場合、そのユーザーはカレンダー機能を利用できません。
C. カレンダーイベントに50人以上の参加者がいるかどうかを確認します。
カレンダーイベントに追加できるゲストの数には制限があるかもしれませんが、通常、この制限を超えると、招待プロセス中にイベント作成者にエラーメッセージが表示され、受信者が招待を受け取れないという事態にはなりません。仮に受信に影響を与えるような制限があったとしても これは、妥当な範囲内の内部ユーザーにとって一般的な問題として文書化されていません）、最初に確認すべき事項ではありません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google カレンダーのヘルプドキュメントには、ゲストの数の制限について記載されている場合があります。ただし、これらの制限は通常、ゲストの追加、更新の送信、または応答の表示に関するものであり、組織内の一部の受信者への配信が完全に失敗することを意味するものではありません。
したがって、社内受信者がカレンダーイベントの招待を受け取らない理由をトラブルシューティングする際の最も論理的な最初のステップは、受信者自身にカレンダーの通知

設定を確認してもらい、新しいイベントのメール通知が有効になっていることを確認することです。
Explanation:
社内ユーザーからGoogleカレンダーのイベント招待が届かないという報告があった場合、まず最初に確認すべき原因は、受信者側のGoogleカレンダーの通知設定です。ユーザーは通知設定をカスタマイズできるため、新しいイベントに関するメール通知をオフにしている可能性があります。
オプションDが最も重要な第一歩である理由と、他のオプションがこの特定の問題の主な原因である可能性が低い理由を以下に示します。

最新問題: **59**
貴社のある部署が、Google Workspaceの最新のAI搭載機能を利用したいと考えています。Geminiは高度な機能を備えていることはご存知でしょう。企業データが人間の目に触れないように、Geminiの導入を管理しつつ、その部署にGeminiの機能への即時アクセスを提供する必要があります。どうすればよいでしょうか？
**A.** 部門の組織単位でGeminiを有効にし、部門内のユーザーにGeminiライセンスを割り当てます。
**B.** 管理者コンソールを通じてGeminiの導入状況を監視し、ライセンスを割り当てる前に、より多くのユーザーが導入するまで待ちます。
**C.** その部署の非ライセンスユーザー向けにGeminiを有効にして、無料サービスにすぐにアクセスできるようにします。
**D.** 組織に対してアルファ機能を有効にし、すべてのユーザーにジェミニライセンスを割り当てます。
**Answer: A (**メーッセージを残す**)**
特定の部署がGoogle WorkspaceでGeminiの機能にすぐにアクセスできるようにすると同時に、管理権限を維持し、企業データのプライバシーを確保するには、その部署が属する組織単位でGeminiを有効にし、その組織単位内のユーザーに必要なライセンスを割り当てる必要があります。この方法により、対象を絞った展開が可能になり、機能が管理されたGoogle Workspace環境内で確実に使用されるようになります。
選択肢Aが正解である理由と、他の選択肢が不適切な理由を以下に示します。
A. 部門の組織単位でGeminiを有効にし、部門内のユーザーにGeminiライセンスを割り当てます。
Google Workspace では、管理者は組織単位 (OU) レベルでサービスと機能を管理できます。Gemini を必要とする部門の OU に対してのみ Gemini を有効にすることで、そのユーザーのみにアクセス権を付与できます。Gemini ライセンスを割り当てることで、高度な AI 機能を使用するために必要な権限がユーザーに付与されます。重要な点として、適切な制御が設定された Google Workspace アカウント内で Gemini が有効化され使用される場合、生成されるデータは Google Workspace のデータプライバシーとセキュリティに関する規定に準拠し、企業データがプライバシーを侵害するような形で人間の目に触れること

がないように保護されます。管理者は、Gemini for Workspace が組織データとどのように連携するかを制御できます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参照: Google Workspace 管理者ヘルプの「ユーザー向けに Gemini for Google Workspace を有効または無効にする」または類似のタイトル）ドキュメントでは、組織単位またはグループレベルで Gemini 機能へのアクセスを制御する方法について説明しています。また、Gemini for Workspace のライセンス要件と、これらのライセンスを特定のユーザーに割り当てる方法についても詳しく説明しています。さらに、「Gemini for Google Workspace におけるデータのプライバシーとセキュリティ」に関するドキュメントでは、Google Workspace 環境内でこれらの機能を使用する際にユーザーデータがどのように処理され、保護されるかについて概説し、企業データの不適切な人間による閲覧を防ぐための制御について強調しています。
B. 管理者コンソールを通じてGeminiの導入状況を監視し、ライセンスを割り当てる前に、より多くのユーザーが導入するまで待つ。
この方法では、Geminiをすぐに必要とする部署へのアクセス権の付与が遅れてしまいます。導入状況のモニタリングは、より広範な展開には役立つかもしれませんが、特定の部署の差し迫ったニーズには対応できません。
Google Workspace 管理者の関連トピックガイドまたはドキュメントの参照: 管理コンソールは、さまざまな Google Workspace サービスの使用状況と導入状況に関する情報を提供しますが、特定のチームに Gemini などの新機能への初期アクセス権を付与するための主要なメカニズムとしては機能しません。
C. その部署のライセンスを持たないユーザー向けにGeminiを有効にし、無料サービスにすぐにアクセスできるようにする。
このオプションで提案されているように、ライセンスや組織の管理を回避してGoogle Workspaceに直接統合されたGeminiの「無料サービス」は存在しません。Google Workspace向けGeminiはライセンスが必要な機能であり、管理者が有効化して割り当てる必要があります。適切なガバナンスなしに企業環境で「ライセンスを持たないユーザー」向けに機能を有効にすることは、標準的でも安全でもありません。これは、ユーザーがGeminiのコンシューマー版にアクセスしていることを意味し、ライセンス版のGoogle Workspace版と同じデータプライバシーおよびセキュリティ管理の対象とならないため、組織のポリシー外で企業データが人間の目に触れる可能性が生じます。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料: Google の Gemini for Workspace に関するドキュメントでは、ライセンス要件と Google Workspace 環境内での統合について明確に説明されており、その展開と使用に対する管理者の制御が強調されています。
D. 組織に対してAlpha機能を有効にし、すべてのユーザーにGeminiライセンスを割り当てます。
アルファ版機能を組織全体で有効化することは、これらの機能がまだ開発段階であり、安定性やセキュリティが確保されていない可能性があるため、重大なリスクを伴います。必

要な部門が1つだけであるにもかかわらず、すべてのユーザーにGeminiライセンスを割り当てることは、不必要なコストであり、適切な評価と対象を絞った展開を行う前に導入規模を拡大することになります。また、当初は要求元の部門のみにアクセスを制限するというニーズにも具体的に対応していません。
Google Workspace 管理者向けトピックガイドまたはドキュメントの参考資料 :リリースチャネル（迅速リリース、スケジュールリリース、アルファ/ベータ版）に関する Google のガイドラインでは、不安定性や完全なサポートの欠如の可能性があるため、アルファ版などのプレリリース機能を本番環境で有効にすることは強く推奨していません。新機能については、特定の組織単位（OU）への段階的なロールアウトが推奨されます。
したがって、最も適切な対応策は、リクエスト元の部署の特定の組織単位（OU）に対してGeminiを有効にし、そのOU内のユーザーにGeminiライセンスを割り当てることです。これにより、管理権限を維持しながら即座にアクセスが可能になり、Google Workspace環境内でのAI機能の使用が組織のデータプライバシーポリシーに準拠することが保証されます。

最新問題: **60**
外部のGoogleドライブにホストされている悪意のあるファイルへのリンクを含むフィッシングメールが増加していることに気付いた。これらのファイルは正規のドキュメントを模倣し、ユーザーを騙してアカウントへのアクセス許可を得ようとする。ユーザーがこれらの悪意のある外部ドライブファイルにアクセスできないようにしつつ、正規の外部ファイルにはアクセスできるようにする必要がある。どうすればよいでしょうか？
（2つ選択してください。）
**A.** より厳格なパスワードポリシーを適用する。
**B.** ユーザーを教育するために、定期的なセキュリティ意識向上トレーニングを実施する。
**C.** 事前に承認された信頼できるパートナーのリストを除くすべての外部ドメインをブロックするドライブの信頼ルールを作成します。
**D.** すべてのユーザーデバイスに高度なマルウェア検出ソフトウェアを導入し、悪意のあるファイルをスキャンしてブロックします。
**E.** すべてのユーザーに対して二要素認証を実装する
**Answer: B,C (**メーッセージを残す**)**
定期的なセキュリティ意識向上トレーニングを実施してユーザーを教育しましょう。
フィッシングの脅威や安全なオンライン利用方法についてユーザーに教育することで、フィッシングの試みを認識して回避できるようになり、そのような詐欺に引っかかる可能性を減らすことができます。
事前に承認された信頼できるパートナーのリストを除くすべての外部ドメインをブロックするドライブの信頼ルールを作成します。外部ドメインからのファイルへのアクセスを制限するドライブの信頼ルールを設定することで、信頼できない外部の Google ドライブにホストされている悪意のあるファイルへのリンクをブロックしながら、信頼できるソースからの正当な外部ファイルへのアクセスは許可できます。

最新問題: **61**
貴社では、従業員が業務目的で個人所有のデバイスを使用することを許可しています。これらのデバイスが会社のセキュリティポリシーに準拠していることを確認したいと考えており、パスコードの強制を最小限に抑え、管理者がデバイスからユーザーアカウントをリモートで消去できるモバイル管理ソリューションを選択する必要があります。また、従業員の個人所有デバイスにエージェントをインストールする必要がないようにしたいと考えています。どのような対策を講じるべきでしょうか？
**A.** モバイルデバイスにGoogleの高度な管理機能を実装します。
**B.** モバイルデバイスにGoogleの基本管理機能を実装する。
**C.** 強力なパスワードポリシーを適用し、次回のサインイン時にパスワードポリシーを適用します。
**D.** サードパーティ製のモバイルデバイス管理（MDM）ソリューションを導入する。
**Answer: (**解答を表示する**)**
Googleのモバイルデバイス向け基本管理機能を使えば、管理者は従業員の個人デバイスにエージェントをインストールすることなく、パスコードの強制など、最低限のセキュリティポリシーを適用できます。また、必要に応じてデバイスからユーザーアカウントをリモートで消去することも可能で、個人デバイスに対する管理をより負担の少ない方法で行いながら、データのセキュリティを確保します。