Google.Google-Workspace-Administrator.v2026-06-23.q111

試験コード:	Google-Workspace-Administrator
試験名称:	Google Cloud Certified - Professional Google Workspace Administrator
認定資格:	Google
無料問題数:	111
バージョン:	v2026-06-23
アクセス数:	109
ページビュー数:	1110
https://www.jpnpdf.com/Google.Google-Workspace-Administrator.v2026-06-23.q111-mondaishu.html	

最新問題: **1**
組織では最近、Google ドライブのコンテキストアウェア アクセス ポリシーを導入し、ユーザーがドライブにアクセスできるのは企業管理のデスクトップからのみに制限しました。しかし残念ながら、一部のユーザーは依然として企業管理外のパソコンからドライブにアクセスできてしまいます。コンテキストアウェア アクセス ポリシーが意図したとおりに機能していない理由を特定するために、どのような事前チェックを行うべきでしょうか（2つ選択してください）。
A. ユーザーが Google Workspace Enterprise Plus ライセンスを持っていることを確認します。
B. コンテキスト認識アクセス デバイス ポリシーを削除し、新しいポリシーを再作成します。
C. ユーザーのデバイスにデバイス ポリシー アプリケーションがインストールされているかどうかを確認します。
D. ユーザーが少なくとも Google Workspace Business ライセンスを持っていることを確認します。
E. ユーザーのデスクトップに Endpoint Verification がインストールされているかどうかを確認します。
Answer: A,E (メーッセージを残す)
コンテキストアウェア アクセス ポリシーが正しく機能していることを確認するには、次のチェックを実行します。
Google Workspace ライセンスを確認します:

ユーザーが Google Workspace Enterprise Plus ライセンスを所有していることを確認してください。コンテキストアウェア アクセスは、Enterprise Plus のお客様のみが利用できる機能です。
管理コンソールで、 請求」> サブスクリプション」に移動し、ユーザーに割り当てられているライセンスの種類を確認します。
エンドポイント検証を確認します。
エンドポイント検証がユーザーのデスクトップにインストールされ、アクティブになっていることを確認します。
管理コンソールに移動し、[デバイス] > [エンドポイント検証] に移動します。
デバイスのリストをチェックして、Endpoint Verification がインストールされ、ユーザーのデバイスのステータスが報告されていることを確認します。
追加の手順:
ポリシーが正しく構成され、関連する組織単位 (OU) に適用されていることを確認します。
セキュリティ > コンテキストアウェア アクセス」でコンテキストアウェア アクセス ポリシーが正しく設定されていることを確認します。
正しいライセンスを確認し、Endpoint Verification がインストールされていることを確認することで、コンテキストアウェア アクセス ポリシーの適用に関連する問題をトラブルシューティングして解決できます。
参照：
コンテキストアウェアアクセスを設定する
エンドポイント検証の概要

最新問題**: 2**
QUESTION NO: 83組織の
法務部門は、時間的に重要な合併および買収 (M&A) 取引に取り組んでいます。
現在休暇中の従業員からの特定の電子メール通信に緊急にアクセスする必要があります。
組織の現在の保存ポリシーは 無期限」に設定されています。法務部門に必要なメールを、データプライバシーを確保しながら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、関連する電子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ます。
B. 法務部門に、M&A 関連の電子メールに限定した制限付きで従業員の電子メール アカウントへのアクセスを一時的に許可します。
C. 従業員のメールボックスへの代理アクセス権を持つ同僚に、関連する電子メールを特定して法務部門に転送するよう依頼します。
D. Google Vault を使用して、M&A 取引に関する案件を作成します。従業員のメールボックス内で関連メールを検索します。関連メールをエクスポートして法務部門と共有します。
Answer: D (メーッセージを残す**)**

Google Vault を使用して M&A 取引に固有の案件を作成することで、法的、セキュリティ、プライバシーを遵守したメールの取得が可能になります。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、合併と買収に関連する特定のメールを検索、エクスポートし、法務部門と共有できます。このアプローチにより、データのプライバシーと組織ポリシーの遵守の両方が確保されます。

最新問題**: 3**
組織では最近、Cloud Identity Premium のライセンスを 1,000 件購入しました。開発チームは、人事情報システム（HRIS）のユーザーデータを読み取り、Google Directory REST API 経由でアカウントを作成するアプリケーションをエンタープライズ サービス バス（ESB）内に作成しました。
本番環境への導入前のテスト中、数人のユーザーを作成した後にGoogle APIのレスポンスから503エラーが発生していることを確認しました。チームは、ESBが1秒あたり100件のリクエストを問題なく処理できるため、ESBが原因ではないと考えています。この問題を回避するために、開発チームにどのようなアドバイスをいただけますか？
A. アカウントごとの制限を回避するには、ドメイン全体の委任 API を使用します。
B. 指数バックオフ アルゴリズムを使用して、失敗した要求を再試行します。
C. パフォーマンス向上のため、REST API から gRPC プロトコルに切り替える
D. 1 つの HTTP リクエストに 1,000 件の API 呼び出しを詰め込むことができるため、バッチ リクエスト アーキテクチャを使用します。
Answer: B (メーッセージを残す**)**
エラーを理解する:
503 エラーは、一時的なサーバーの過負荷やメンテナンスなどにより、サービスが利用できないことを示します。
これは、API レート制限を超えた場合に発生する可能性があります。
指数バックオフアルゴリズム:
このアルゴリズムは、再試行間の待機時間を指数関数的に増加させることにより、リクエストが失敗した後の再試行を管理するのに役立ちます。
最初は短い遅延から始めて、再試行するたびに遅延を指数関数的に増やします。
実装：
ESB アプリケーションを変更して、指数バックオフ アルゴリズムを組み込みます。
無限ループを回避するために、再試行が適切な数に制限されていることを確認してください。
このアプローチは、リクエストの試行を分散させることで一時的な過負荷を軽減するのに役立ちます。
参照
Google Workspace 管理者ヘルプ: API エラーの処理
Google Developers: 指数バックオフ

最新問題**: 4**

組織では、一部のユーザーがビジネスで海外旅行中に Google ドライブにログインできないようにしたいと考えています。
これらのユーザーを組織部門（OU）に追加しました。この要件を満たすには、Google ドライブ アプリへのユーザーのアクセスを保護する必要があります。
何をすべきでしょうか?
A. OU 内のユーザーに対して Google ドライブを無効にします。
B. 位置情報に基づくアクセスレベルを定義します。組織単位（OU）のGoogleドライブアプリにレベルを割り当てます。
C. OU 内のユーザーがサインインするときに 2 段階認証 (2SV) を要求します。
D. ユーザーベースのアクセスレベルを定義します。組織単位（OU）のGoogleドライブアプリにレベルを割り当てます。
Answer: B (メーッセージを残す**)**
海外旅行中のユーザーのGoogleドライブへのアクセスを制限するには、位置情報に基づくアクセスレベルを定義できます。特定の組織部門（OU）のGoogleドライブアプリにこれらのレベルを割り当てることで、ユーザーの地理的な位置情報に基づいてアクセスを制御できます。これにより、ユーザーは承認された場所からのみGoogleドライブにアクセスできるため、出張中のユーザーによるアクセスを効果的に防止できます。

最新問題**: 5**
4 週間前、Google Vault からデータをエクスポートし、PST エクスポート ファイルを法務管理者にメールで送信しました。
誤ってPSTファイルを削除してしまったため、再度送信する必要があります。PSTファイルを法務担当者に再送信するには、どのような手順を踏めばよいでしょうか？
A. Google Vault エクスポート ページに戻り、ZIP ファイルを再度ダウンロードします。
B. 電子メール ログ検索ページに戻り、PST ファイルを再度ダウンロードします。
C. 法務管理者に、Google Vault に戻って PST ファイルを再度ダウンロードするよう依頼します。
D. 元の時間枠で元の検索を繰り返し、データを再度エクスポートします。
Answer: D (メーッセージを残す**)**
誤って削除された PST ファイルを法務管理者に再送信するには:
* Google Vault に戻ります。
* 以前と同じ基準と期間を使用して、元の検索を繰り返します。
* データを再度エクスポートして、新しい PST ファイルを作成します。
* 新しい PST ファイルを法務管理者に送信します。
これが必要なのは、Vault エクスポートは永続的に保存されず、元のエクスポート ファイルが失われた場合に再作成する必要があるためです。
参考文献:
* Google Vault ヘルプ: データのエクスポート

最新問題**: 6**
組織が Google Workspace に移行しており、新しく作成されたファイルの分類方法を改善したいと考えています。機密ファイルの取り扱いに関するセキュリティと透明性を向上させるスケーラブルなソリューションを見つける必要があります。どうすればよいでしょうか?
A. データ損失防止 (DLP) ポリシーを設定してデータにラベルを付け、ラベルのロックを自動的に無効にし、ユーザーに教育する
B. 分類ラベルを作成して自動分類を可能にし、ユーザーを教育する
C. データを Google Workspace のマップ分類に移行し、Drive Labels API を使用して移行します。
D. Cloud DLP API マップ識別子と分類を統合し、Google ドライブ ラベル クライアントをインストールしてアプリケーションを実行します。
Answer: (解答を表示する**)**
ステップバイステップの包括的詳細説明：
* 管理コンソールにアクセスする: 管理者アカウントを使用して Google 管理コンソールにログインします。
* ラベルに移動します。[アプリ] > [Google Workspace] > [ドライブとドキュメント] > [ラベル] に移動します。
* 分類ラベルの作成: さまざまな機密レベルとファイルの種類に対応する分類ラベルを定義および作成します。
* 自動分類を有効にする: 事前定義された基準とパターンに基づいて、新しく作成されたファイルを自動的に分類できるように設定を構成します。
* ユーザーの教育: トレーニング セッションを実施したり、ドキュメントを配布したりして、分類ラベルを効果的に使用する方法をユーザーに教え、データ セキュリティの維持における分類ラベルの重要性を理解させます。
参考文献:
* Google Workspace 管理者ヘルプ: ドライブのラベル
* Google Workspace の DLP と分類

最新問題**: 7**
最近、あなたの会社はGoogle Workspaceを活用していない組織を買収しました。現在、あなたの会社はGoogle Cloud Directory Sync（GCDS）を使用して、LDAPディレクトリからGoogle Workspaceへの同期を行っています。あなたはGCDSの2つ目のインスタンスをデプロイし、同じ戦略を、同じくLDAPディレクトリにユーザーが存在する買収した組織に適用したいと考えています。セットアップを成功させるには、GCDSインスタンスをどのように変更すればよいですか（2つ選択してください）。
A. 現在の GCDS インスタンスに、最近買収した組織の LDAP ディレクトリへの管理者認証情報を提供します。

B. 新しいユーザーを同期するには、現在の GCDS インスタンスに LDAP 同期ルールを追加します。
C. 買収した組織の LDAP から同期されたユーザーが停止されないように、除外ルールを設定します。
D. 別のサーバー上で実行される GCDS の追加インスタンスを設定し、取得した組織の同期を処理します。
E. GCDS の複数の LDAP バージョンにアップグレードします。
Answer: (解答を表示する**)**
* 追加のGCDSインスタンス:
* 別のサーバー上で GCDS の別のインスタンスを実行すると、買収した組織の同期を個別に管理できます。
* これにより競合が回避され、異なる LDAP ディレクトリの管理が簡素化されます。
* 複数の LDAP バージョン:
* GCDS の複数の LDAP バージョンにアップグレードすると、複数の LDAP ディレクトリからのデータの同期がサポートされます。
* これは、異なる LDAP 設定を持つさまざまな組織を処理する場合に便利です。
* セットアップの手順:
* 別のサーバーに GCDS の 2 番目のインスタンスをインストールします。
* 取得した組織の LDAP の詳細を使用して新しいインスタンスを構成します。
* 複数の LDAP バージョンを使用している場合は、既存の GCDS 設定をアップグレードし、両方の LDAP ディレクトリのルールを設定します。
* 同期をテストして、正しくセットアップされ、競合がないことを確認します。
参考文献
* Google Workspace 管理者ヘルプ: GCDS の設定

最新問題**: 8**
Your-company.com の財務部門は、スプレッドシートからデータを読み取る社内アプリケーションを作成したいと考えています。コラボレーションエンジニアであるあなたは、App Maker の使用を提案しました。財務チームは、App Maker でアプリケーションを作成する際のデータセキュリティを懸念しています。
データを保護するためにどのようなセキュリティ対策を実施する必要がありますか?
A. レコードおよびデータ関係に対する操作には、ロール、スクリプト、および所有者のアクセス権限を使用します。
B. 財務部門の組織単位に対してのみ App Maker アクセスを有効にします。
C. 各データ ソースにアクセスするには、権限が制限されたサービス アカウントを使用します。
D. 所有者のアクセス権限を変更して、内部使用のみを許可します。
Answer: A (メーッセージを残す**)**

App Maker でアプリケーションを開発するときに、ユーザーが必要とするさまざまなアクセス レベルに対応するロールを定義します。
スクリプトを使用して、ユーザーの役割に基づいてデータへのアクセスを制御します。これにより、許可されたユーザーのみが特定の操作を実行できるようになります。
所有者のアクセス権限を適切に設定して、必要な権限を持つユーザーのみがデータにアクセスまたは変更できるようにします。
組織やアプリケーションの使用状況の変更に適応するために、役割と権限を定期的に確認して更新します。
これらのセキュリティ対策を実装することで、内部アプリケーション内のデータが安全にアクセスおよび管理されるようになり、不正アクセスに関連するリスクが軽減されます。
参照：
Google Workspace 管理者ヘルプ - App Maker のセキュリティ

最新問題: **9**
あなたは国際的な組織に勤務しており、CEO は頻繁に他国に出張します。
電子メール アクセスを有効にし、複数の管理アシスタントのアカウントを構成する必要があります。
何をすべきでしょうか?
A. ユーザーが自分のアカウントから送信される委任メッセージに含める送信者情報を指定できるようにします。
B. CEOのGmailアカウントにログインします。2つのメールエイリアスを設定し、共有します。
C. 管理アシスタントのグループを作成します。そのグループに対して、CEOのメールボックスへの委任アクセスを有効にします。
D. エグゼクティブ管理アシスタントに CEO のアカウント パスワードを提供します。
Answer: C (メーッセージを残す**)**

最新問題: **10**
セキュリティ＆コンプライアンス部門は、Google Workspace データへのアクセスを許可する安全なサードパーティ製アプリケーションを特定しました。サードパーティによるアクセスを承認済みアプリケーションのみに制限する必要があります。どのような 2 つの対応を行う必要がありますか？ 2 つ選択してください。）
A. 信頼できるアプリをホワイトリストに登録する
B. Drive SDK を無効にする
C. APIスコープを制限する
D. Gmailのアドオンを無効にする
E. Google Workspace Marketplace アプリをホワイトリストに登録する
Answer: (解答を表示する**)**
* 信頼できるアプリをホワイトリストに追加:
* Google Workspace 管理コンソールで、[セキュリティ] > [API 制御] に移動します。

* 「アプリのアクセス制御」で、「サードパーティ製アプリのアクセスを管理」を選択します。
* 承認されたアプリケーションをホワイトリストに追加し、これらのアプリのみが Google Workspace データにアクセスできるようにします。
* Google Workspace Marketplace アプリをホワイトリストに追加する:
* 管理コンソールで、「アプリ」>「Google Workspace Marketplace アプリ」に移動します。
* Google Workspace データへのアクセスが必要な信頼できるアプリを参照して選択します。
* 検証済みのアプリケーションのみがデータにアクセスできるように、これらのアプリを承認してホワイトリストに登録します。
参考文献
* Google Workspace 管理者ヘルプ: Google Workspace データにアクセスするサードパーティ製アプリと社内アプリを制御する
* Google Workspace 管理者ヘルプ: Google Workspace Marketplace

最新問題: **11**
組織の幹部から、Workspace アカウントへのエグゼクティブ管理者アクセス権を付与するよう依頼されました。このエグゼクティブ管理者が幹部のアカウントのメールを管理できることを確認する必要があります。
役員のアカウントのセキュリティとプライバシーを維持する必要があります。どうすればよいでしょうか？
A. 幹部が幹部管理者への電子メール転送を設定できるように支援します。
B. 経営幹部に、経営幹部管理者とパスワードを共有するよう指示します。
C. Google グループを作成し、すべてのエグゼクティブ管理者を追加します。グループへの委任アクセスを有効にします。
D. 経営幹部の Gmail アカウントへの委任アクセスを許可し、Gmail 設定で経営幹部の管理者にアクセス権を割り当てます。
Answer: (解答を表示する**)**
委任アクセスを付与することで、経営管理者は経営幹部のパスワードにアクセスすることなく、経営幹部のメールを管理できます。このソリューションは、権限をメール管理のみに制限することでセキュリティとプライバシーを確保しながら、経営幹部のアカウントのセキュリティを維持します。経営管理者は経営幹部に代わってメールの送信、閲覧、削除を行うことができますが、アカウントの他の機能にはアクセスできません。

最新問題: **12**
貴社では、SSO プロバイダの変更を決定しました。Google Workspace やその他のクラウド サービスへの認証に外部 SSO システムを使用する代わりに、Google を他のサードパーティ クラウド サービスへの ID プロバイダ（IDP）および SSO プロバイダとして使用することになりました。

Google Workspace で再構成するために必須の 2 つの機能は何ですか (2 つ選択してください)。
A. アプリ > ドメインに SAML アプリを追加します。
B. Google Cloud Directory Sync 経由でユーザー プロビジョニングを再構成します。
C. サードパーティの IDP 検証証明書を置き換えます。
D. サードパーティの IDP による SSO を無効にします。
E. Google Cloud Platform の API 権限を有効にします。
Answer: (解答を表示する**)**
* アプリ > ドメインに SAML アプリを追加します:
* シングルサインオン（SSO）のIDプロバイダ（IDP）をGoogleに切り替える場合は、Google Workspaceをサードパーティ製アプリケーションのSSOプロバイダとして設定する必要があります。これには、Google Workspace内のドメインに必要なSAML（Security Assertion Markup Language）アプリケーションを追加することが含まれます。
* 管理コンソールに移動し、「アプリ」>「ウェブアプリとモバイルアプリ」に移動して、SAML アプリをドメインに追加します。これにより、Google がこれらのアプリでユーザーを認証できるようになります。
* サードパーティの IDP による SSO を無効にする:
* IDP として外部 SSO プロバイダから Google Workspace に切り替えるため、サードパーティ プロバイダでの現在の SSO 構成を無効にする必要があります。
* 管理コンソールにアクセスし、「セキュリティ」>「サードパーティのIdPでシングルサインオン（SSO）を設定する」に移動し、既存のSSO設定を無効にします。これにより、ユーザーは以前のSSOプロバイダではなく、Google Workspaceを介して直接認証するようになります。
参考文献:
* Google Workspace 管理者ヘルプ: 独自のカスタム SAML アプリを設定する
* Google Workspace 管理者ヘルプ: サードパーティの IdP による SSO を無効にする

最新問題**: 13**
あなたの会社には、広範囲かつきめ細かなIT管理チームがあり、あなたは適切な管理体制の確保を担っています。そのチームの一つであるセキュリティチームが、セキュリティ調査ツールへのアクセスを必要としています。どうすればよいでしょうか？
A. 事前に構築されたセキュリティ管理者ロールをセキュリティ チーム メンバーに割り当てます。
B. 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、そのロールを各セキュリティ チーム メンバーに割り当てます。
C. セキュリティ チーム メンバーにスーパー管理者ロールを割り当てます。
D. セキュリティ設定権限を持つカスタム管理者ロールを作成し、そのロールを各セキュリティ チーム メンバーに割り当てます。
Answer: B (メーッセージを残す**)**

https://support.google.com/a/answer/9043255#:~:text=To%20give%20access%20only%20to%20the%20investigation%20tool%2C%20check%20the%20individual%20boxes%20for%C2%A0Investigation%20Tool%20privileges.%20You%20can%20specific%20privileges%20for%20different%20types%20of%20data%20(for%20example%2C%20Gmail%2C%20Drive%2C%20Device%2C%20and%20User)%3A

最新問題**: 14**
アプリケーション開発チームから、社内ドメインで所有する新しい Google Workspace アプリに Google Drive API へのアクセスを許可するよう依頼がありました。現在、セキュリティポリシーに基づき、承認済みホワイトリストを使用してすべての API へのアクセスを制限しています。このアプリへのアクセスを許可する必要があります。
何をすべきでしょうか?
A. Google ドライブへのすべての API アクセスを有効にします。
B. 「ドメイン所有のアプリを信頼する」設定を有効にします。
C. OAuth クライアント ID を Google ドライブの信頼リストに追加します。
D. Google Workspace Marketplace でアプリをホワイトリストに登録します。
Answer: (解答を表示する**)**
* admin.google.com にある Google 管理コンソールに移動します。
* 管理コンソールのホームページから、「セキュリティ」に移動し、「API コントロール」に移動します。
* 「API コントロール」セクションで、「サードパーティ アプリのアクセスを管理」をクリックします。
* ここで、社内アプリのOAuthクライアントIDを信頼できるリストに追加できます。これにより、セキュリティポリシーに準拠し、審査・承認したアプリのみがGoogle Drive APIにアクセスできるようになります。
* 新しいアプリの OAuth クライアント ID を入力し、変更を保存します。
このプロセスにより、新しい内部ドメイン所有アプリが、既存のセキュリティ ポリシーに違反することなく Google Drive API にアクセスできるようになります。
参考文献:
* Google Workspace 管理者ヘルプ - API クライアント アクセスの管理

最新問題**: 15**
貴社のITチームは、法務部門から、電子情報開示のためにサードパーティパートナーと共有するMBOXファイルに関する問い合わせへの対応を依頼されています。この問い合わせは複数のユーザーに対して実行する必要があります。法務部門にはGoogle Vaultの管理者権限がありません。このリクエストに対応するにはどうすればよいでしょうか？
A. ユーザー アカウントごとに Google Vault の問題を作成し、法務管理者と共有します。
B. Google Vault の問題を作成し、データを検索し、法務部門向けにエクスポートを実行します。

C. 調査も使用して、要求されたデータを検索し、法務部門向けにエクスポートします。
D. Gmail でデータを検索し、法務部門向けにエクスポートします。
Answer: B (メーッセージを残す**)**
Google Vault にアクセスする: Google Vault に移動します。
案件の作成: 法的な問い合わせについて、Google Vault で新しい案件を作成します。
データの検索: 検索機能を使用して、法務部門の要件に基づいて複数のユーザー アカウント間で必要なデータを照会します。
エクスポートの実行: 検索結果を確認した後、MBOX ファイル形式へのデータのエクスポートを実行します。
共有エクスポート: エクスポートされた MBOX ファイルを法務部門に提供し、eDiscovery プロセスに使用します。
参照：
Google Vault ヘルプ - 案件の作成と管理
Google Vault ヘルプ - 検索結果のエクスポート

最新問題**: 16**
組織は2つの企業を買収し、事業拡大を図ろうとしています。両社ともGoogle Workspaceを使用しています。CISO（最高情報セキュリティ責任者）は、厳格な「外部コンテンツ共有禁止」ポリシーを策定し、遵守するよう指示しています。CISOの指示を満たしつつ、新たに買収した企業との外部共有を可能にするには、共有ポリシーをどのように安全に設定すればよいでしょうか？
A. IT グループのみにドライブ コンテンツの外部共有を許可します。
B. 許可リストに登録されたドメインとの共有のみを許可するドライブ DLP ポリシーを作成します。
C. 共有ドライブを使用してコンテンツを保存し、個々のファイルのみを外部と共有します。
D. 「信頼できるドメイン」機能を使用して、ユーザーが2社間でファイルを共有できるようにします。信頼できるドメインの許可リストを作成し、ユーザーの共有設定を選択します。
Answer: (解答を表示する**)**
管理コンソールにアクセスします。Google 管理コンソールにログインします。
共有設定に移動します。[アプリ] > [Google Workspace] > [ドライブとドキュメント] > [共有設定] に移動します。
信頼できるドメインの設定: 信頼できるドメイン機能を有効にし、新しく買収した会社のドメインを許可リストに追加します。
共有設定の調整：共有設定を調整し、外部との共有を制限しつつ、信頼できるドメインとの共有を許可します。これにより、CISOの指示を遵守しながら、新たに買収した企業とのコラボレーションが可能になります。
変更の伝達: 新しい共有ポリシーと、コンテンツの共有が許可される特定のドメインについて、すべてのユーザーに通知します。

コンプライアンスの監視: 共有アクティビティを定期的に監視して、新しいポリシーに準拠していることを確認し、必要に応じて調整します。
参照：
Google Workspace 管理者ヘルプ - 共有設定
Google Workspace 管理者ヘルプ - 信頼できるドメインを許可リストに登録する

最新問題: **17**
ある組織では、ユーザーがモバイルデバイスから企業データにアクセスする際の効率的な管理方法を模索しています。最近、組織のワイヤレス設定を変更したところ、個人所有デバイスを持つユーザーはWi-Fiにアクセスできるものの、企業アプリケーションやデータソースにアクセスできなくなってしまいました。会社所有デバイスを持つユーザーには、同様の問題は発生していません。あなたはこの問題のトラブルシューティングを任されています。どうすればよいでしょうか？
A. 高度なモバイル管理を有効にして、デバイスを承認します。
B. 高度なモバイル管理を無効にして、デバイスを承認します。
C. 高度なモバイル管理を有効にし、デバイスのブロックを解除します。
D. 高度なモバイル管理を無効にして、デバイスを有効にします。
Answer: A (メーッセージを残す**)**
A は正解です。デバイスが企業データにアクセスするにはデバイスの承認が必要であり、高度なモバイル管理を使用する場合にのみデバイスの承認を実装できます。
B は不正解です。デバイスを承認するには高度なモバイル管理が必要です。
C は不正解です。最初に高度なモバイル管理を有効にしないと、デバイスをブロックする機会がなかったためです。
D は不正解です。デバイスを承認するには高度なモバイル管理が必要です。
参照：
https://support.google.com/a/answer/6328699?hl=ja

最新問題: **18**
貴社ではGoogle Workspace Enterpriseをご利用いただいており、Google Workspaceの他のお客様との共同作業を容易にするため、Googleドライブのファイルの外部共有を許可し

ています。最近、ファイルやフォルダが外部のユーザーやグループと広範囲に共有されるというインシデントが複数発生しました。最高セキュリティ責任者（CSO）は、外部からのアクセスを無効化せずに済むよう、外部共有の範囲に関するデータと継続的なアラート通知を必要としています。
最高セキュリティ責任者の要求に応えるために、どのような 2 つのアクションを取る必要がありますか? (2 つ選択してください。)
A. Google ドライブ アクティビティ ダッシュボードを使用して、ファイルを閲覧したユーザーを確認します。
B. ドライブ監査レポートからアラートを作成し、外部ファイル共有を通知します。
C. 集計レポート セクションで外部共有の合計を確認します。
D. セキュリティ調査ツールで外部共有用のカスタム ダッシュボードを作成します。
E. DLP ルールを使用して外部共有を自動的にブロックします。
Answer: B,D (メーッセージを残す**)**
https://support.google.com/a/answer/7584076?hl=ja&ref_topic=7563358

最新問題**: 19**
あなたは30,000人のユーザーを抱える組織の管理者です。ドメイン内のエンドユーザーには、業務内容に応じて複数のWorkspaceライセンスオプションを提供しています。ユーザーは年間で複数回、異なるライセンスタイプに移行する可能性があります。組織では従業員の離職率が高いため、組織のライセンス管理を最も効率的に行う方法は何でしょうか？
A. ディレクトリ API を使用して、ユーザーのライセンスを毎日変更するカスタム バッチ スクリプトを作成します。
B. Google 管理コンソールでライセンス割り当てルールを作成し、ディレクトリ属性に基づいてユーザー ライセンスを設定します。
C. Google Cloud Directory Sync を使用して、組織の LDAP で利用可能な情報に従って、同期ごとにユーザー ライセンスを変更します。
D. 必要に応じて、管理コンソールのユーザー部分でユーザー ライセンスを更新します。
Answer: C (メーッセージを残す**)**
https://support.google.com/a/answer/10148746?hl=ja
Google Cloud Directory Sync（GCDS）を使用すると、Google アカウント内のユーザーのライセンスを管理、同期できます。
Configuration Managerの「ライセンス」ページで、「LDAPライセンスルール」をクリックし、「ルールの追加」をクリックします。「LDAPクエリ」フィールドで、LDAPクエリ表記法を使用して、ライセンスを割り当てるLDAPディレクトリ上のユーザーを指定します。詳細については、「LDAP検索ルールを使用してデータを同期する」を参照してください。

最新問題**: 20**

GmailのVaultのデフォルトの保持ポリシーは365日に設定されています。法務部門から、カスタマーサポート部門が送受信するメールは機密情報であるため、30日間のみ保持する必要があると通知されました。この新しい保持ポリシーを最も簡単な方法で適用する必要があります。どうすればよいでしょうか？
A. Gmail の現在のデフォルトの保持ポリシーを 30 日間に変更します。Vault で 2 つのカスタム保持ポリシーを設定します。1 つはカスタマーサポート組織単位 (OU) に適用する 30 日間のポリシー、もう 1 つはディレクトリ内の他のすべての組織単位に適用する 365 日間のポリシーです。
B. Gmail の Vault の現在のデフォルトの保持ポリシーを 30 日間に変更し、カスタマーサポート組織部門 (OU) に適用します。ドメインの Gmail に 365 日間のカスタム保持ポリシーを設定します。
C. Vault に 2 つのカスタム保持ポリシーを作成します。1 つは顧客サポート組織単位 (OU) に適用する 30 日間のポリシー、もう 1 つはディレクトリ内の他のすべての OU に適用する 365 日間のポリシーです。
D. Gmail の Vault で 30 日間のカスタム保持ポリシーを作成し、カスタマー サポートの組織単位 (OU) に適用します。
Answer: D (メーッセージを残す**)**

最新問題**: 21**
会社のCEOから、信頼できる連絡先からのメッセージがスパムメールに分類され、業務に大きな影響が出ているとの報告を受けました。これらの連絡先からのメッセージは、必ずしもスパムメールとして分類されているわけではありません。また、最近、ドメインにSPF、DKIM、DMARCを設定しました。あなたはこの問題のトラブルシューティングを任されています。
どのような 2 つのアクションを取る必要がありますか? (2 つ選択してください。)
A. 送信者をホワイトリストに追加する Gmail ルーティング ルールを設定します。
B. ドメインが Spamhaus のブラックリストに登録されていないことを確認します。
C. メッセージ ヘッダーを取得し、Google Workspace Toolbox を使用して分析します。
D. 電子メール ログ検索を実行して、メッセージのルートを追跡します。
E. Google Vault 内のメッセージの内容を確認します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 22**
組織のセキュリティチームは、エンドユーザーに対するフィッシング攻撃を懸念しています。フィッシング攻撃に対する最も強力な予防策を設定するには、どのような2つの対策を講じるべきでしょうか？
2つの回答を選択してください
A. スプーフィングと認証制御を設定し、脅威とみなされるメッセージを隔離します

B. 疑わしいメッセージを見つけた場合は、そのメッセージをスパムとしてマークするようにエンドユーザーをトレーニングします。
C. スプーフィングと認証の制御を構成して、脅威と認識されるメッセージについてエンドユーザーに警告します。
D. Workspace ドメインから送受信されるすべてのメッセージに機密モードを適用します
E. Workspace ドメインからのすべての受信メールと送信メールの暗号化を強制します。
Answer: A,C (メーッセージを残す**)**
* 管理コンソールにアクセスする: admin.google.com にアクセスし、管理者アカウントでログインします。
* Gmail 設定に移動します。管理コンソールで、[アプリ] > [Google Workspace] > [Gmail] > [セーフティ] に移動します。
* スプーフィングと認証制御を構成する:
* 受信メールを検証するために、SPF、DKIM、DMARC などのメール認証ポリシーを設定します。
* 認証チェックに失敗し、脅威と認識されたメッセージを隔離するオプションを有効にします。
* 潜在的に有害なメッセージについてユーザーに警告するように設定します。
* コンプライアンス ルールを作成する: Gmail の設定で、疑わしいメールを隔離し、フィッシングの可能性があるメッセージを受信したときにユーザーに通知するルールを作成します。
* ユーザーのトレーニング: フィッシング詐欺を認識する方法と、疑わしいメールをスパムとしてマークすることの重要性についてユーザーを教育します。
これらの設定を構成すると、疑わしい脅威を自動的に処理し、ユーザーに潜在的な危険を認識させることで、フィッシング攻撃に対するセキュリティが強化されます。
参考文献
* Gmailでスパムやフィッシングから保護
* メール認証 $PF、DKIM、DMARC）を設定する

最新問題**: 23**
あなたの会社では、短期契約のインターンを5〜10名ほど頻繁に採用しており、共通のGoogle Workspaceアカウント（例user1@your-company.com、user2@your-company.com、user3@your-company.com）を使用しています。このプログラムのマネージャーは、これらのアカウント宛てのすべてのメールをマネージャーのメールボックスアカウントにも転送することを希望しています。
何をすべきでしょうか?
A. 各アカウントの GMail 設定メニューでアドレス転送を設定します。
B. GMail の詳細設定で受信者アドレスのマッピングを設定します。
C. 受信ゲートウェイ ルートを構成します。
D. マネージャーにメールボックスへの委任アクセス権を付与します。

Answer: B (メーッセージを残す)
管理コンソールにアクセスします。
Google 管理コンソールにログインします。
Gmailの設定に移動します。
「アプリ」> 「Google Workspace」> 「Gmail」に移動します。
受信者アドレスマッピングの設定:
Gmail の設定で、「ルーティング」をクリックします。
「受信者アドレスマッピング」の下の 「構成」をクリックします。
アドレス マッピングを構成します。
汎用アカウント (例: user1@your-company.com、user2@your-company.com) を追加します。
これらのアドレスをマネージャーのメールボックス アカウントにマップします。
保存して適用:
設定を保存します。
メールをマネージャーのアカウントに転送するには、ルーティング ルールが正しく適用されていることを確認します。
テスト構成:
汎用アカウントにテストメールを送信し、マネージャーのメールボックスに正しく転送されていることを確認します。
参照：
Gmailのルーティング設定
受信者アドレスマッピング

最新問題: **24**
組織内のGoogle Cloud Directory Syncの自動化と設定を担当されています。会社のLDAPに大幅な変更があった場合、設定マネージャーでWorkspace環境内で広範囲にわたる削除が適用されないようにするにはどうすればよいでしょうか？
A. シミュレートされた同期を実行した後でのみ、Google Cloud Directory Sync を手動で実行します。
B. 各構成項目で同期するオブジェクトの最小数と最大数を指定します。
C. 構成マネージャーから実行した場合にのみユーザーを削除するようにツールを構成します。
D. 各同期における削除の最大数の制限を構成します。
Answer: (解答を表示する)
広範囲にわたる削除の防止:
削除制限を構成すると、LDAP ディレクトリに大幅な変更があった場合に、誤って削除されたり、大量に削除されたりするのを防ぐことができます。
削除制限を設定する手順:
Google Cloud Directory Sync（GCDS）設定マネージャを開きます。

「一般設定」に移動し、「削除制限」セクションを見つけます。
同期ごとに許可される削除の最大数を設定します。削除数が指定された制限を超えた場合、同期が一時停止され、変更を手動で確認して承認できるようになります。
構成を保存し、同期プロセスをテストして、制限が適切に適用されていることを確認します。
参照
Google Workspace 管理者ヘルプ: GCDS の削除制限

最新問題**: 25**
組織の従業員が、Google スライドのプレゼンテーションに埋め込まれている Google ドライブに保存されている動画を再生できないという問題が発生しています。問題のトラブルシューティングを行うために必要な詳細を収集する必要があります。どうすればよいですか?
A. ソースビデオがサポートされている形式と解像度であり、ユーザーがビデオを再生する権限を持っていることを確認します。画面共有セッションで動作を確認します。
B. 従業員にプレゼンテーションの編集権限を与えてもらい、変更履歴を確認します。スライドを削除して再度追加するとエラーメッセージが変わるかどうかを確認します。
C. Google ドライブの監査ログでスライドのプレゼンテーションにエラーがないか確認します。ヘルプセンターで適切なエラー メッセージを確認します。
D. プレゼンテーションのコピーを作成し、問題を再現できるかどうかを確認し、見つかったエラーを文書化します。
Answer: (解答を表示する**)**
ビデオ形式の確認: ビデオ形式が Google ドライブでサポートされていることを確認します (例: .mp4、.mov)。
ビデオ解像度を確認する: ビデオ解像度がサポートされており、スムーズに再生できるほど高くないことを確認します。
権限チェック: ユーザーがビデオにアクセスして再生するために必要な権限を持っていることを確認します。
画面共有セッション: ユーザーとの画面共有セッションを設定して、問題を直接観察します。
問題の再現: セッション中にビデオを再生して動作を確認し、エラー メッセージを特定します。
トラブルシューティング: 調査結果に基づいて、ビデオの再アップロード、権限の調整、ビデオをサポートされている形式に変換するなど、可能な修正方法をユーザーに案内します。
参照：
Google Workspace 管理者ヘルプ: サポートされている動画形式

最新問題**: 26**

組織では新しいCISOが任命されました。CISOは管理者アラートの受信登録を済ませ、不審なログイン試行に関するアラートを受け取りました。CISOは、組織内で不審なログイン試行がどのくらいの頻度で発生しているかを把握しようとしています。CISOは、過去1年間に不審なログイン試行があった各ユーザーアカウントの詳細と、各アカウントの発生回数を報告するよう依頼しています。
これらの要件を満たすにはどのようなアクションを実行する必要がありますか?
A. ログイン監査レポートを使用して、疑わしいログインの詳細をすべてエクスポートし、分析します。
B. 疑わしいログインを表示するセキュリティ調査ツールを備えたカスタム ダッシュボードを作成します。
C. アカウント アクティビティ レポートを使用して、疑わしいログインの詳細をすべてエクスポートし、分析します。
D. すべての疑わしいログイン詳細を表示するカスタム クエリを BigQuery で作成します。
Answer: A (メーッセージを残す**)**
ログイン監査ログ ユーザーのログインアクティビティを追跡 ログイン監査ログを使用すると、ドメインへのユーザーのログインを追跡できます。ウェブブラウザからのすべてのログインを確認できます。ユーザーがメールクライアントやブラウザ以外のアプリケーションからログインした場合は、不審なログインのレポートのみを確認できます。ログイベントデータをGoogle Cloud Platformに転送する ログイベントデータをGoogle Cloud Platformと共有するように設定できます。共有を有効にすると、データはCloud Loggingに転送され、そこでログのクエリと表示、ログのルーティングと保存方法の制御が可能になります。
https://support.google.com/a/answer/4580120?hl=ja

最新問題**: 27**
組織内のGoogle Cloud Directory Syncの自動化と設定を担当されています。会社のLDAPに大幅な変更があった場合、設定マネージャーでWorkspace環境内で広範囲にわたる削除が適用されないようにするにはどうすればよいでしょうか？
A. シミュレートされた同期を実行した後でのみ、Google Cloud Directory Sync を手動で実行します。
B. 各構成項目で同期するオブジェクトの最小数と最大数を指定します。
C. 構成マネージャーから実行した場合にのみユーザーを削除するようにツールを構成します。
D. 各同期における削除の最大数の制限を構成します。
Answer: D (メーッセージを残す**)**
Google Cloud Directory Sync（GCDS）の制限を使用すると、シミュレーションまたは同期ごとに許可される削除の最大数を設定できます。この制限に達すると、GCDS は停止し、変更は同期されません。https://support.google.com/a/answer/9520714?fl=1

最新問題**: 28**

同社の最高幹部10名のオフィスには、標準化された専用のビデオ会議用カメラ、マイク、スクリーンが設置される予定です。これは、多忙な日々の中で様々なモバイルデバイスやPCデバイスを頻繁に切り替える習慣があるため、必要となる技術サポートの量を削減することが目的です。
経営幹部が、手持ちのデバイスではなく専用の機器を使用して Meet ビデオ会議に簡単に参加できるようにする必要があります。
何をすべきでしょうか?
A. 管理対象外の Chromebox を設定し、Chrome 設定で幹部のホームページを meet.google.com に設定します。
B. エグゼクティブ オフィスを予約可能なカレンダー リソースとして設定し、Hangouts Meet ハードウェア キットを導入して、Meet ハードウェアを部屋のカレンダーに関連付けます。
C. 各役員オフィスに Hangouts Meet ハードウェア キットを導入し、Meet ハードウェアを役員のカレンダーに関連付けます。
D. 管理対象 Chromebox をプロビジョニングし、デバイス ポリシーを使用して幹部の Chrome ホームページを meet. google.com に設定します。
Answer: (解答を表示する**)**
* カレンダーリソースを作成する:
* Google Workspace 管理コンソールで、『ディレクトリ」> 『ビルディングとリソース」> 『リソースを管理する」。
* 各執行オフィスに新しいリソースを作成し、適切な名前を付けます。
* Hangouts Meet ハードウェア キットを導入する:
* 各役員オフィスに Hangouts Meet ハードウェア キットを設置します。
* ハードウェア キットをネットワークに接続し、正しく構成されていることを確認します。
* Meet ハードウェアを会議室カレンダーに関連付けます。
* 各 Hangouts Meet ハードウェア キットを対応する部屋のカレンダー リソースにリンクします。
* これにより、部屋でスケジュールされた会議が Meet ハードウェアに自動的に接続されるようになります。
* セットアップとテスト:
* ビデオ会議をテストして、ハードウェアが正しく機能していることを確認します。
* Meet ビデオ会議に参加するための専用機器の使用方法について幹部をトレーニングします。
参考文献
* Google Workspace 管理者ヘルプ: ビルディングとリソースの管理
* Google Workspace: Hangouts Meet ハードウェアのセットアップ

最新問題**: 29**

組織では、ユーザーに影響を与える可能性のあるフィッシング攻撃の脅威が高まっていることを懸念しています。経営陣は2段階認証の強制有効化を拒否しています。
ユーザー アカウントへの不正アクセスを防ぐために、セキュリティ対策を適用する必要があります。
何をすべきでしょうか?
A. 強力なパスワードポリシーの適用を有効にします。
B. 従業員 ID ログイン チャレンジを有効にします。
C. 最大ユーザーセッション長を短縮します。
D. 外部アプリケーションへのトークン認証を取り消します。
Answer: B (メーッセージを残す**)**
従業員IDをログイン時の本人確認情報として使用できます。従業員IDは、他の種類の本人確認情報よりも推測やフィッシングが困難です。従業員IDログイン時の本人確認情報を使用するには、IDがユーザーのアカウントに関連付けられていることを確認する必要があります。
https://support.google.com/a/answer/6002699?hl=ja

最新問題**: 30**
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するかに関係なく、これらのポリシーがデバイスに適用されていることを確認する必要があります。
何をすべきでしょうか?
A. アプリと拡張機能の設定の [デバイス] ページで、許可されたアプリのリストを構成します。
B. Chrome アプリや拡張機能を使用する際にユーザーのログインを要求するように Chrome ユーザー設定を構成します。
C. アプリと拡張機能に適用されたドメイン全体のポリシーをオーバーライドするようにポリシーの優先順位を構成します。
D. ユーザーのログインに 2SV を要求します。
Answer: (解答を表示する**)**
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たかに関係なく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、許可された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**: 31**
Workspace 管理者として、マーケティング部門の一時的な Google Workspace ユーザー アカウントを削除するよう依頼されました。このユーザーは 「マイ ドキュメント」にドライ

ブ ドキュメントを作成しており、マーケティング マネージャーは、このユーザーが退職し Workspace から削除された後も、これらのドキュメントを保持したいと考えています。このデータはマーケティング マネージャーのみが閲覧できるようにする必要があります。Workspace 管理者として、このユーザーのドライブ データを保持するにはどうすればよいでしょうか。

A. ユーザーの削除プロセスで、他のアプリのデータセクションで 転送」を選択し、マネージャーのメールアドレスを追加します。

B. Google Vault を使用して、ユーザーが所属する OU に保持期間を設定します。

C. ユーザーを削除する前に、ユーザーをマーケティング共有ドライブに投稿者として追加し、ドキュメントを新しい場所に移動します。

D. ユーザーに、MyDrive の下にフォルダーを作成し、共有するドキュメントを移動して、そのフォルダーをマーケティング チーム マネージャーと共有するように依頼します。

Answer: A (メーッセージを残す**)**

https://support.google.com/a/answer/6223444?hl=en#zippy=%2Ctransfer-user-drive-or-google-data:~:text=You%20can%20transfer、 転送」をタップしてください。

最新問題**: 32**

アカウント アクティビティ レポートを使用して、大きなファイルをアップロードしている複数のユーザーにフラグを設定しました。

プールされたストレージが不足しないようにし、不正使用を阻止したい場合、まず何をすべきでしょうか？

A. フラグが付けられたユーザーを構成グループに配置し、グループのストレージ制限を設定します。

B. セキュリティ調査ツールを使用して、フラグが付けられたユーザーにアラートを設定します。

C. フラグが付けられたユーザーに警告し、ストレージ クォータに達しないようにプールされたストレージをさらに購入します。

D. フラグが付けられたユーザーに不正使用の可能性があるという警告を電子メールで送信します。

Answer: A (メーッセージを残す**)**

最新問題: **33**
組織では、ユーザーによる外部との共有が許可されていません。セキュリティチームは最近、マーケティングチームと営業チームの特定のメンバーが外部の顧客、見込み客、パートナーとドキュメントを共有することを例外として承認しました。これを実現する最善の方法は何でしょうか？
A. 承認されたユーザーをメンバーとして構成グループを作成し、それを使用してターゲット ユーザー グループを作成します。
B. マーケティングおよび営業組織単位での外部共有を有効にします。
C. マーケティング チームと営業チームによって提供された許可リストに登録されたドメインに対してのみ外部共有を有効にします。
D. 承認されたユーザーをメンバーとして構成グループを作成し、このグループの外部共有を有効にします。
Answer: D (メーッセージを残す**)**
構成グループを作成します。
Google 管理コンソールに移動します。
[ディレクトリ] > [グループ] に移動します。
「グループを作成」をクリックし、グループの詳細を入力します。
マーケティング チームと営業チームから承認されたユーザーをこのグループのメンバーとして追加します。
グループの外部共有を有効にする:
[アプリ] > [Google Workspace] > [ドライブとドキュメント] > [共有設定] に移動します。
「特定のグループの共有オプション」まで下にスクロールします。
新しく作成したグループを選択します。
このグループの外部共有を有効にします。
変更を保存します。
これにより、指定されたユーザーのみがドキュメントを外部で共有できるようになり、組織の他のユーザーは制限されたままになります。
参照
Google Workspace 管理者ヘルプ: 特定のグループとドライブとドキュメントを共有する

最新問題: **34**
組織にはカナダ、イタリア、米国にオフィスがあり、従業員がこれら 3 つの地理的な場所からのみ企業の Gmail と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. 企業の Gmail およびドライブへのアクセスには企業デバイスの使用を必須とする
B. 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、企業の Gmail とドライブに割り当てます。

C. 受信メッセージと送信メッセージの配信を制限し、Google ドキュメントのコメントから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. Google Workspace で、3 つの地理的な場所からのみデータへのアクセスを許可するデータ保護ルールを作成します。
Answer: (解答を表示する**)**
コンテキスト認識アクセスを有効にする:
Google 管理コンソールで、[セキュリティ] > [コンテキストアウェア アクセス] に移動します。
コンテキスト認識アクセス機能を有効にします。
アクセス レベルの作成:
地理的な場所 (カナダ、イタリア、米国) に基づいてアクセス レベルを定義します。
これらの地域を指定するには、IP アドレス範囲またはその他の場所インジケーターを使用します。
アクセス レベルの割り当て:
作成したアクセス レベルを Google Workspace サービス、具体的には企業の Gmail とドライブに割り当てます。
指定された地域からアクセスするユーザーのみがこれらのサービスにアクセスできるようにします。
適用と監視:
設定を保存して適用します。
コンプライアンスとセキュリティを確保するためにアクセス ログを監視します。
参照：
Google Workspace 管理者ヘルプ: コンテキストアウェア アクセスを設定する
Google Workspace 管理者ヘルプ: コンテキストアウェア アクセスレベルの管理

最新問題**: 35**
組織ではセキュリティ強化のため、従業員が海外旅行中に社内文書にアクセスできないように制限したいと考えています。ただし、メールの送受信は引き続き可能です。
コンテキストアウェアなアクセスレベルを設定しており、これらのセキュリティポリシーをサポートするように Workspace を構成する必要があります。どうすればよいでしょうか？
A. ユーザーのデバイスのOSをパラメータとしてアクセスレベルを設定します。このアクセスレベルをGoogleドライブに割り当てます。
B. ユーザーがWorkspaceサービスにアクセスする地理的な起点をパラメータとして、アクセスレベルを設定します。このアクセスレベルをGmailに割り当てます。
C. ユーザーのデバイスのオペレーティングシステムをパラメータとしてアクセスレベルを設定します。このアクセスレベルをGmailに割り当てます。
D. ユーザーが Workspace サービスにアクセスする地理的な起点をパラメータとして、アクセスレベルを設定します。このアクセスレベルを Google ドライブに割り当てます。
Answer: D (メーッセージを残す**)**

最新問題: **36**
組織では、ユーザーに影響を与える可能性のあるフィッシング攻撃の脅威が増大していることを懸念しています。
経営陣は2段階認証の強制有効化を拒否しました。ユーザーアカウントへの不正アクセスを防ぐため、セキュリティ対策を実施する必要があります。
何をすべきでしょうか?
A. 強力なパスワードポリシーの適用を有効にします。
B. 従業員 ID ログイン チャレンジを有効にします。
C. 最大ユーザーセッション長を短縮します。
D. 外部アプリケーションへのトークン認証を取り消します。
Answer: B (メーッセージを残す**)**
Google 管理コンソールにログインします。
管理コンソールのホームページから、 セキュリティ」に移動し、 ログイン時の本人確認」を選択します。 従業員 ID によるログイン時の本人確認」設定を有効にします。
ログイン プロセス中にユーザーが提供する必要がある従業員 ID を定義して、チャレンジを構成します。
従業員IDによるログイン認証を有効にすると、2段階認証を必要とせずにセキュリティを強化できます。これにより、ユーザーに本人のみが知る追加情報を提供することで、不正アクセスを防止できます。
参照：
Google Workspace 管理者ヘルプ - ログイン時の本人確認を設定する
"?>>?b GF\]\管理コンソールのホームページから、 セキュリティ」に移動します。
セキュリティ」の下で API コントロール」を選択します。
API コントロール」セクションで、 サードパーティ アプリのアクセスを管理」をクリックします。リストから Google Drive API を見つけます。
Google ドライブに対して すべてのアクセスを無効にする」を選択して、サードパーティ アプリに Google ドライブへの OAuth 権限が付与されないようにします。
この構成は、サードパーティ アプリが OAuth 経由で Google ドライブにアクセスするのを防ぐことで、最高情報セキュリティ責任者によって設定されたポリシーに準拠しています。
Google Workspace 管理者ヘルプ - API クライアント アクセスの管理

最新問題: **37**
会社は6階建ての新築ビルを購入しました。そこには様々な規模の会議室が20室あります。
会議室の1つは役員会議室で、閲覧と予約は1人だけに許可する必要があります。Google Workspace > カレンダー > リソース メニューでこの役員会議室を作成しましたが、共有設定を制限する必要があります。どのような2つの対策を講じるべきでしょうか？

A. リソースを削除し、そのユーザーのカレンダー アカウントに会議室をセカンダリ カレンダーとして作成します。
B. 会議室が常に使用中として表示されるため、空いている部屋として表示されません。
C. リソースの設定にアクセスして、変更を行う権限をユーザーに割り当てます。
D. リソースの設定の 「アクセス許可」のオプションをクリアして、他のユーザーがアクセスできないようにします。
E. 部屋で予定されている会議を監視する方法と、会議をキャンセルする方法を示します。
Answer: (解答を表示する**)**
A は不正解です。これはセカンダリ カレンダーではなく、カレンダー リソースである必要があります。
B は不正解です。他の人がまだ部屋を見ることができるという事実は変わりません。
C は正解です。これにより、その人にその部屋の予約変更を処理する権限が与えられます。
D は正解です。これにより、ドメイン上の他のユーザーからそのルームが見えなくなります。
E は不正解です。これは大変な作業であり、部屋を予約したユーザーの間で間違いや不安が生じる可能性があります。
参照：
https://support.google.com/a/answer/1034381?hl=ja

最新問題**: 38**
従業員が競合他社に移籍し、機密情報を外部に漏洩していました。元従業員がWorkspaceアカウントにアクセスできないようにする必要があります。マネージャーとチームメンバーは、元従業員が作成したドキュメントに引き続きアクセスする必要があります。ライセンスコストを最小限に抑え、元従業員のWorkspaceアカウントに法的ホールド（法的保留）を維持したいと考えています。どうすればよいでしょうか？
A. 元従業員の Workspace アカウントの名前を変更します。
B. 元従業員の Workspace アカウントを削除します。
C. 元従業員の Workspace アカウントを無効にし、ライセンスをアーカイブ ユーザー タイプに切り替えます。
D. 元従業員のパスワードを複雑なものにリセットし、Workspace アカウントのライセンスをアクティブなままにします。
Answer: C (メーッセージを残す**)**
元従業員のデータを維持するために、ライセンスをアーカイブユーザーに切り替える必要があります。また、さらなる漏洩を防ぐため、アカウントを無効化する必要があります。次のステップは、漏洩したデータのさらなる調査のため、Google Vault に案件を作成することです。

最新問題**: 39**
Google が特定した、ユーザーから報告されたスパムの増加をどのように監視できますか?

A. 電子メール ログで配信後のアクティビティを確認します。
B. 調査ツールでユーザーが報告したスパムを確認します。
C. アラート センターでユーザーから報告されたスパムの急増を確認します。
D. Rev]BigQuery Export での配信後のアクティビティ。
Answer: C (メーッセージを残す**)**
* Google 管理コンソールにログインします。
* 管理コンソールのホームページから、セキュリティ」に移動し、「アラート センター」に移動します。
* アラート センターで、ユーザーが報告したスパムに関連するアラートを探します。
* これらのアラートの詳細を確認して、ユーザーから報告されたスパム活動の急増を監視できます。
アラート センターは、アラートを確認および管理するための集中的な場所を提供し、スパム レポートの傾向や急増をより簡単に特定できるようにします。
参考文献:
* Google Workspace 管理者ヘルプ - アラートセンターの概要 BFbC

最新問題**: 40**
組織が Google Workspace に移行する前の数年間、ユーザーが会社のメールアドレスを使用して一般ユーザー向けの Google アカウントを作成するのは比較的一般的な方法でした（たとえば、アナリティクスのモニタリング、AdSense の管理、Google Workspace を利用している他のパートナーとのドキュメントでの共同作業など）。ロールアウト中に、現職従業員による一般ユーザー向けアカウントの使用には対処できましたが、現在は、会社のメール アカウントにアクセスできないにもかかわらず、それらのサービスに引き続きアクセスできる可能性のある元従業員をブロックすることについて懸念しています。
何をすべきでしょうか?
A. Google Enterprise サポートに連絡して、Google Workspace 以外の Google サービスにアクセスし、ブロックしているドメイン上のすべてのアカウントのリストを提供してください。
B. 管理対象外アカウントの転送ツールを使用して、以前のユーザーに、そのアカウントを管理対象アカウントとしてドメインに転送するようリクエストを送信します。
C. 会社の Analytics、AdSense などの管理者に、すべてのアクティブな従業員のリストを提供します。
アカウントを作成して、それぞれのアクセス制御リストをクリーンアップできるようにします。
D. 以前のユーザー アカウントに Cloud Identity ライセンスをプロビジョニングし、新しい Google パスワードを生成して、すべての Google Workspace とその他の Google サービスを無効にした OU に配置します。
Answer: B (メーッセージを残す**)**
* 転送ツールにアクセスします:

* Google Workspace 管理コンソールで、[ユーザー] > [管理対象外ユーザー向けの移行ツール] に移動します。
* 管理されていないアカウントを識別する:
* このツールを使用して、企業のメールアドレスを持つ管理対象外のアカウント（一般ユーザー向け Google アカウント）を検索します。
* 振替依頼を送信:
* 特定された管理対象外アカウントに移行リクエストを送信し、以前のユーザーにアカウントを管理対象ドメインに移行するよう依頼します。
* 転送の監視と完了:
* 転送プロセスを監視し、アカウントが正常に転送されたことを確認します。
* 移管したアカウントが Google Workspace ドメインで管理され、サービスへの不正アクセスを防止していることを確認します。
参考文献
* Google Workspace 管理者ヘルプ: 管理対象外ユーザー向けの移行ツール

最新問題: **41**
あるユーザーが、自身が所有するGoogleグループ（info@company.com）についてIT部門に問い合わせてきました。グループにはメールが届いており、各メッセージはユーザーのGmail受信トレイにも直接配信されています。ユーザーは、Gmailから直接メッセージに返信し、個人アカウントではなくグループとして送信できるようにしたいと考えています。現在、返信は個人アカウントから送信されています。ユーザーにどのような対応を指示すればよいでしょうか？
A. ユーザーの送信メッセージとコピーされたグループを一致させる新しいコンテンツ コンプライアンス ルールを作成し、送信者をグループ アドレスに変更します。
B. Gmailから送信できるメールアドレスとしてグループを追加し、ユーザーがアクセスできることを確認します。その後、ユーザーはグループから返信できるようになります。
C. ユーザーの個人アカウントをグループの受信トレイの代理人として追加します。代理人はアカウントを切り替えて、グループを代表してGmailインターフェースを使用できるようになります。
D. グループの投稿ポリシー内で、グループ アドレスをデフォルトの送信者に設定します。
Answer: (解答を表示する**)**
https://support.google.com/googlecloud/answer/10635789?hl=ja

最新問題: **42**
Google Workspace への移行後、法務チームから、進行中の訴訟に関与している従業員のすべてのメールを検索し、訴訟記録保持（リティゲーションホールド）を設定するためのアクセス権をリクエストされています。法務チームがこのリクエストに対応できるよう、サポートする必要があります。
何をすべきでしょうか?
A. 法務チームをユーザー管理管理者のシステム ロールに追加します。

B. Google Vault Google グループに法務チームを追加します。
C. Google Vault へのアクセス権を持つカスタムロールを作成し、法務チームを追加します。
D. Google Vault で問題を作成し、法務チームと共有します。
Answer: C (メーッセージを残す)
参考: https://gsuite.google.com/products/vault/

最新問題**: 43**
ユーザーがサインイン パターンに従わず、通常とは異なる場所からサインインしています。管理者として、この調査中にこのユーザーに対するこのアラートにどのように対応すればよいですか?
A. ドメインに2要素認証を追加する
B. まずアカウントを停止し、その後調査する
C. サインインパターンを追跡するためのセキュリティアラートを強化します
D. ログインおよびセキュリティ監査ログでアカウントの不正なアクティビティを調査します
Answer: D (メーッセージを残す)
* 管理コンソールにアクセスする: admin.google.com にアクセスし、管理者アカウントでログインします。
* レポートに移動します。管理コンソールで、[レポート] > [監査] > [ログイン] に移動します。
* ログイン アクティビティを確認する: 不明な IP アドレスや場所からのログインなど、異常または疑わしいログイン試行を探します。
* さらに詳しく調査する:
* ユーザーのアクティビティをチェックして、不正アクセスや異常な動作の兆候がないか確認します。
* セキュリティ監査ログを使用して、ログイン試行やその他のセキュリティ イベントに関する詳細を確認します。
* 適切な措置を講じる:
* 不正なアクティビティが確認された場合は、ユーザーのパスワードをリセットし、2 要素認証 (2FA) を有効にすることを検討してください。
* 脅威レベルが高い場合は、問題が解決するまでユーザーに通知し、アカウントを停止する場合があります。
ログイン ログとセキュリティ ログを調査することで、潜在的なセキュリティの脅威を効果的に特定し、軽減することができます。
参考文献
* セキュリティレポートとログを表示および分析する
* 監査と調査のページ

最新問題**: 44**

Google アナリティクス サービスは組織全体でオフに設定されています。マーケティング チーム OU 内のすべてのユーザーと営業 OU の一部のユーザーはアナリティクスにアクセスできる必要がありますが、組織の残りのユーザーにはアクセス権限を与えないでください。追加の Google サービスでアクセスを設定する必要があります。どうすればよいですか?
A. OU構造の最上部でGoogle Analyticsを有効にする
B. マーケティング部門と営業部門の Google アナリティクスを有効にする Google アナリティクスへのアクセスを拒否するグループを作成し、アクセスを許可すべきでない営業部門のユーザーに割り当てます
C. マーケティングOUでGoogleアナリティクスを有効にします。マーケティングOUの下に営業ユーザー用のサブOUを作成します。
D. マーケティング OU で Google アナリティクスを有効にする管理コンソールから営業ユーザーを含むグループを作成し、そのグループに対して Google アナリティクスをオンに設定します
Answer: D (メーッセージを残す)
管理コンソールにアクセスする: 管理者アカウントを使用して Google 管理コンソールにログインします。
その他の Google サービスに移動します。[アプリ] > [その他の Google サービス] > [Google アナリティクス] に移動します。
マーケティング OU を有効にする: マーケティング OU を選択し、Google アナリティクスをオンにします。
営業ユーザーのグループを作成する: 「ディレクトリ」> 「グループ」に移動し、Google アナリティクスへのアクセスが必要な営業ユーザーの新しいグループを作成します。
Google アナリティクス アクセスの割り当て: Google アナリティクス設定で、新しく作成した営業グループのアクセスをオンにします。
設定を確認する: マーケティング OU と特定の営業グループのユーザーのみが Google アナリティクスにアクセスでき、組織の他のユーザーはアクセスできないことを確認します。
参照：
Google Workspace 管理者ヘルプ: その他の Google サービスをオンまたはオフにする
Google Workspace サービス アクセス管理

最新問題**: 45**
社内のユーザーから、会社のGmailアカウントで一部のメールが受信できないという報告を受けています。Google Workspace ステータス ダッシュボードを確認しましたが、サービスに支障は見られませんでした。問題の根本原因を特定し、メール配信の問題を解決する必要があります。どのような対応をすべきでしょうか (2つ選択してください)。
A. 電子メール ログ検索 (ELS) を使用して、特定の配信失敗を識別します。
B. 組織のメール交換 (MX) レコードが正しく構成されているかどうかを確認します。

C. ユーザーのスパム フォルダーをチェックして、電子メールが誤って送信されていないかどうかを確認します。
D. Gmail のログ イベントでエラー メッセージや異常なパターンを調査します。
E. 受信メール ゲートウェイで送信者の IP アドレスを確認します。
Answer: (解答を表示する**)**
メールログ検索（MLS）を使用する：MLSを使用すると、メールの配信状況を追跡し、未配信やバウンスメールなどの問題を特定できます。これは、メール配信の問題の根本原因を特定するために不可欠なツールです。
組織のメール交換（MX）レコードが正しく設定されているかどうかを確認してください。MXレコードに誤りがあると、組織のGmailアカウントにメールが配信されない可能性があります。スムーズなメール配信を確保するには、これらのレコードが正しく設定されていることを確認することが重要です。

最新問題**: 46**
組織では、教育目的で特定のユーザーグループにYouTubeへのアクセスを許可し、それ以外のユーザー全員のYouTubeアクセスを制限したいと考えています。ユーザーの役割やグループに基づいてYouTubeへのアクセスをきめ細かく制御できるソリューションを実装する必要があります。どうすればよいでしょうか？
A. 選択したユーザー グループに属していないユーザーに対して YouTube をブロックする Chrome 拡張機能を Google Workspace Marketplace からデプロイします。
B. さまざまなユーザー グループの YouTube アクセスを管理するために SAML アプリケーションを構成します。
C. 選択したユーザーグループに、YouTube にアクセスするときに個人の Google アカウントに切り替えるように指示します。
D. 組織単位 (OU) を使用して、YouTube へのアクセスを制限するポリシーを適用し、選択したユーザー グループに対して例外を作成します。
Answer: D (メーッセージを残す**)**
Google Workspace 組織内で YouTube アクセスをきめ細かく制御し、特定のグループにはアクセスを許可しながら、他のグループにはアクセスを制限するには、組織部門（OU）とサービス設定の例外を組み合わせて使用することをおすすめします。まず、上位レベルの OU（ほとんどのユーザーを含む）に YouTube アクセスを制限するポリシーを適用し、次に特定のグループを含む子 OU を作成します。そこで継承されたポリシーをオーバーライドして YouTube アクセスを許可します。
オプション D が最も適切なソリューションである理由と、他のオプションが Google Workspace 内での一元管理されたきめ細かな制御にあまり適していない理由は次のとおりです。
D). 組織部門 (OU) を使用して YouTube へのアクセスを制限するポリシーを適用し、選択したユーザー グループに対して例外を作成します。

Google Workspace では、管理者は YouTube を含む様々な Google サービスの設定を組織部門レベルで行うことができます。最上位の組織部門、またはほとんどのユーザーを含む親組織部門に対して、YouTube へのアクセスをブロックするポリシーを設定できます。その後、アクセスが必要な特定のユーザーグループ専用の子組織部門を作成し、この子組織部門の設定内で、継承されたポリシーをオーバーライドして YouTube へのアクセスを許可することができます。これにより、一元管理が可能になり、組織構造に基づいて制限と例外が一貫して適用されます。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス：Google Workspace 管理者向け公式ヘルプドキュメントの「YouTube へのアクセスを制御する」または類似のタイトル）では、組織部門レベルで YouTube 設定を管理する方法について説明しています。利用可能な様々なアクセスオプション（例：無制限、制限付き、組織内のログイン済みユーザー、オフ）と、これらの設定を特定の組織部門に適用する方法について詳しく説明しています。
OU の継承と子 OU での設定の上書きという概念は、Google Workspace のポリシー管理の基本的なものであり、特定のユーザー グループに対して例外を作成できるようになります。
A). 選択したユーザー グループに属していないユーザーに対して YouTube をブロックする Chrome 拡張機能を Google Workspace Marketplace から導入します。
Chrome拡張機能を使用してアクセスのブロックと許可を行うと、管理コンソールから適用するサーバー側のポリシーに比べて信頼性が低く、一元管理が困難になる可能性があります。拡張機能は、ユーザーによってバイパスされたりアンインストールされたりする場合もあります。さらに、サードパーティ製拡張機能を使用してグループメンバーシップに基づいてアクセスを管理する場合、Google Workspaceのユーザーおよびグループ構造とシームレスに統合されない可能性があります。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス：Chrome 拡張機能はブラウザの機能を拡張できますが、Google が管理する組織全体のサービスアクセスポリシーを適用するための主要な手段ではありません。管理コンソールでは、Google サービスの設定をより強力かつ一元的に管理できます。
B). さまざまなユーザー グループの YouTube アクセスを管理するために SAML アプリケーションを構成します。
SAML（Security Assertion Markup Language）は、通常、サードパーティ製アプリケーションへのシングルサインオン（SSO）に使用されます。YouTube は Google のコアサービスであり、Google Workspace 組織内での YouTube へのアクセスは、SAML アプリケーション設定ではなく、管理コンソールのサービス設定を通じて直接管理されます。
同じ Google Workspace ドメイン内で YouTube アクセス用の SAML アプリを構成することは、不必要で、おそらくサポートされていない複雑さになります。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス：SAML に関する Google Workspace 管理者ヘルプドキュメントは、SSO のための外部アプリケー

ションの統合に重点を置いています。YouTube などのコア Google サービスへのアクセス管理は、管理コンソールのサービス設定で行います。
C). 選択したユーザーグループに、YouTube にアクセスするときに個人の Google アカウントに切り替えるように指示します。
このアプローチは集中管理型のソリューションではなく、いくつかの問題を引き起こします。ユーザーは手動でアカウントを切り替える必要があり、不便でエラーが発生する可能性が高くなります。さらに重要なのは、YouTubeでのアクティビティが組織アカウントではなく個人アカウントに関連付けられることです。これは教育目的に合致せず、組織の監督やポリシー（コンテンツ制限など）を回避してしまう可能性があります。また、組織アカウント内の他のユーザーのアクセスを効果的に制限することもできません。
Google Workspace 管理者向けトピックガイドまたはドキュメント参照 :Google Workspace は、組織のコンテキスト内でサービスへのアクセスを管理するように設計されています。ユーザーに組織目的で個人アカウントを使用するよう指示すると、この管理が回避されるため、制御とセキュリティの維持の観点から一般的に推奨される方法ではありません。
したがって、選択したユーザー グループに YouTube へのアクセスを提供しながら、他のユーザーへのアクセスを制限するためのベスト プラクティスは、組織単位 (OU) を使用して YouTube へのアクセスを制限するポリシーを適用し、選択したユーザー グループを含む OU に対して例外を作成する (ポリシーをオーバーライドする) ことです。

最新問題: **47**
組織には機密情報を扱うユーザーのグループがあり、そのアカウントには貴重なファイルが含まれています。これらのユーザーを標的型オンライン攻撃から保護する必要があります。どうすればよいでしょうか?
A. これらのユーザーに対して2段階認証を有効にし、Google Authenticatorの使用を推奨します。
B. これらのユーザーに対して2段階認証を有効にし、SMSコードの使用を推奨します。
C. エンドユーザーのパスワード回復を無効にする
D. これらのユーザーのすべてのアカウントを高度な保護プログラムに登録する
Answer: D (メーッセージを残す)

* 要件の理解:
* このシナリオには、機密情報を扱い、アカウントに貴重なファイルを持つユーザー グループが関係します。
* 目標は、これらのユーザーを標的型オンライン攻撃から保護することです。
* オプション分析:
* オプションA: これらのユーザーに対して2段階認証を有効にし、Google Authenticatorの使用を推奨する
* 2 段階認証 (2SV) は、認証層を追加することでセキュリティを強化します。
Google Authenticator は信頼できる方法ですが、高度に標的を絞った攻撃に対しては十分ではない可能性があります。
* オプションB: これらのユーザーに対して2段階認証を有効にし、SMSコードの使用を推奨する
* SMS コードは 2SV の一種ですが、SIM スワッピングなどの潜在的な脆弱性があるため、他の方法よりも安全性が低いと考えられています。
* オプションC: エンドユーザーのパスワード回復を無効にする
* パスワード回復を無効にすると、回復オプションによる不正アクセスを防ぐことができますが、標的型攻撃に対する積極的な保護は提供されません。
* オプションD: 対象のユーザーのすべてのアカウントを高度な保護プログラムに登録する
* 高度な保護プログラム (APP) は、標的型攻撃のリスクが高いユーザーを保護するために特別に設計されています。ログイン時に物理的なセキュリティキーを要求する、不正アクセスをブロックする、機密データへのアクセスを制限するといった強力な対策が含まれています。
* 推奨ソリューション:
* 高度な保護プログラム (APP) へのユーザー登録:
* ステップ1: 高リスクユーザーを特定する:
* 機密情報を扱い、貴重なファイルを保有するユーザーを特定します。
* ステップ2: APPに登録する:
* Google 管理コンソールに移動します。
* セキュリティ セクションに移動し、高度な保護プログラムを見つけます。
* 特定された高リスクユーザーを APP に登録します。
* ステップ3: セキュリティキーを実装する:
* ユーザーがログインするためのセキュリティ キー (例: Titan セキュリティ キー) を持っていることを確認します。
* セキュリティ キーの設定と使用のプロセスをユーザーに案内します。
* ステップ4: ユーザー教育:
* APP の重要性と、それがどのようにアカウントを保護するかについてユーザーに説明します。
* フィッシング攻撃の認識やその他のセキュリティのベストプラクティスに関するトレーニングを提供します。
* APPの利点:

* 強化されたセキュリティ:
* APP は Google アカウントに最高レベルのセキュリティを提供し、認証にはセキュリティ キーが必要です。
* フィッシングに対する保護:
* セキュリティ キーは、標的型オンライン攻撃でよく見られるフィッシング攻撃に対して高い耐性があります。
* アクセス制限:
* APP は機密データへのアクセスを制限し、信頼できるアプリとサービスのみが保護されたアカウントと対話できるようにします。
参考文献:
* Google Workspace 管理者ヘルプ: 高度な保護プログラム
* Google Workspace セキュリティ: 高度な保護プログラム
* Google セキュリティ ブログ: 高度な保護プログラム

最新問題**: 48**
組織では、複数のクラウドベースサービスにシングルサインオン (SSO) を導入しています。認証時に、あるサービスから、情報が無効であるためSSOプロバイダーにアクセスできないというメッセージが表示されました。
何をすべきでしょうか?
A. SAML レスポンスの NameID 要素がアサーション コンシューマー サービス (ACS) URL と一致することを確認します。
B. SAML レスポンスの Audience 要素が Assertion Consumer Service (ACS) URL と一致することを確認します。
C. SAML レスポンスの Subject 属性が Assertion Consumer Service (ACS) URL と一致することを確認します。
D. SAML レスポンスの受信者属性がアサーション コンシューマー サービス (ACS) URL と一致することを確認します。
Answer: B (メーッセージを残す**)**
https://support.google.com/a/answer/2463723?hl=ja

最新問題**: 49**
組織内のユーザーから、職場では不適切な言葉を含むメッセージが届くという苦情が頻繁に寄せられています。管理者として、これらのメッセージがユーザーのメールボックスに届かないようにするには、どのような対策を講じるべきでしょうか？
A. 不適切なコンテンツルールを設定する
B. 添付ファイルのコンプライアンスルールを設定する
C. 光学文字認識 (OCR) を有効にする
D. Gmail DLP ポリシーを設定します。
Answer: (解答を表示する**)**

不適切な表現を含むメッセージがユーザーのメールボックスに配信されないようにするには、次の手順に従います。
* Google 管理コンソールにログインします。特権管理者権限を持つアカウントを使用します。
* Gmail の設定に移動します。[アプリ] > [Google Workspace] > [Gmail] > [設定を管理] に移動します。
* 新しいコンテンツ コンプライアンス ルールを作成します。
* 「コンプライアンス」をクリックし、次に 「コンテンツ コンプライアンス」をクリックします。
* 「別のルールを追加」をクリックします。
* 「不適切な表現フィルター」など、ルールの名前を入力します。
* ルールの条件を設定します。
* 「設定を追加」セクションで、「次のいずれかがメッセージと一致する場合」を選択します。
* 「メタデーター致」または 「高度なコンテンツー致」を選択します。
* 「高度なコンテンツ マッチ」の場合は、定義済みのコンテンツ フィルターを使用するか、不適切な単語とみなされるカスタムの単語を追加します。
* アクションを設定します。
* アクションを 「メッセージを拒否する」または 「メッセージを隔離する」に設定します。
* オプションで、拒否または検疫について管理者または送信者に通知できます。
* ルールを保存する: 「保存」をクリックしてルールを有効にします。
参考文献:
* Google Workspace 管理者ヘルプ - コンテンツ コンプライアンスの設定
* Google Workspace 管理者ヘルプ - 不快なコンテンツ

最新問題: **50**
規制要件により、貴社はドイツに所在する従業員のデータを欧州内に、米国に所在する従業員のデータを米国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、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。
何をすべきでしょうか?
A. 従業員に、会社のパソコンにドキュメントを保存するためにパソコン版ドライブを使用するように指示します。
B. 2つのグループを作成します。従業員の所在地に基づいて、ドイツまたは米国の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、グループ間の共有を防止します。
C. 管理コンソールの 「データリージョン」機能に移動します。ドイツの従業員の場合はヨーロッパリージョンを選択し、米国の従業員の場合は米国リージョンを選択します。
D. 管理コンソールのデータリージョン機能に移動し、 「指定なし」を選択します。
Answer: (解答を表示する)

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、組織部門（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、ドイツの従業員データはヨーロッパ内に、米国の従業員データは米国内に保存され、データのローカリティに関する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設定が不要になります。
わかりました。質問を慎重に確認し、Google Workspace 管理者アソシエイトの公式ドキュメントに基づいて 100% 検証済みの回答を提供し、入力ミスを修正して、要求された形式で提示します。

最新問題: **51**
チームマネージャーとして、チームメンバーが休暇を共有できる休暇カレンダーを作成する必要があります。特に複数のメンバーが休暇中の場合、カレンダーを使ってチームメンバーのオンライン状況を視覚的に把握したいとします。このカレンダーを作成するにはどうすればよいでしょうか？
A. カレンダー リソースの作成をリクエストし、カレンダーを 競合しない招待を自動承認する」ように構成し、チームに すべてのイベントの詳細を表示」アクセス権を付与します。
B. アカウントの下にセカンダリカレンダーを作成し、チームに イベントを変更する」アクセス権を付与します。
C. カレンダー リソースの作成をリクエストし、カレンダーを すべての招待をこのカレンダーに自動的に追加する」ように構成し、チームに 空き時間情報のみを表示」アクセス権を付与します。
D. アカウントの下にセカンダリカレンダーを作成し、チームに 空き時間情報のみ表示」アクセス権を付与します。
Answer: B (メーッセージを残す**)**
https://support.google.com/a/users/answer/13293412?hl=ja#zippy=%2Clearn-how

最新問題: **52**
ユーザーから、普段連絡を取っている相手からのメールが届かないという報告がありました。問題の原因を調査するために、ユーザーからどのような情報を収集する必要がありますか？
A. 送信者のメール アドレス、紛失したメッセージの件名と日時。
B. 個人が使用しているデバイスの種類（OS バージョン、ブラウザ、ブラウザ バージョンなど）。
C. 送信者のドメイン。SPF および DKIM 構成を確認できます。
D. 送信者の IP アドレス、メール クライアント、メール プラットフォーム。
Answer: (解答を表示する**)**
メールが見つからない原因を調査するには、以下の情報を収集する必要があります。
送信者のメールアドレス。
失われたメッセージの件名。

メッセージが到着すると予想された日時。この情報を利用することで、管理コンソールでメールログを検索し、メールの経路を追跡し、遅延や未配信の原因となった可能性のある問題を特定できます。
参照：
Google Workspace 管理者ヘルプ - メールログ検索でメールを追跡する

最新問題: **53**
あなたの会社には、世界中に分散したリモートワークチームがあります。チームメンバー全員が会社のデータセキュリティポリシーを遵守し、所在地と役割に基づいて許可されたシステムのみにアクセスできるようにしたいと考えています。
何をすべきでしょうか?
A. データ損失防止 (DLP) ルールを作成して適用し、データ共有を制御します。
B. すべてのリモート アクセスに対して会社全体の VPN の使用を設定し、義務付けます。
C. すべてのリモート チーム メンバーに対して 2 要素認証を実装します。
D. 条件付きアクセスを使用してアクセス制御ポリシーを構成します。
Answer: (解答を表示する**)**
世界中に分散したリモートワークチームがデータセキュリティポリシーを遵守し、所在地と役割に基づいて許可されたシステムにのみアクセスできるようにするには、条件付きアクセスを含むアクセス制御ポリシーを構成する必要があります。条件付きアクセスを使用すると、ユーザーの所在地、使用デバイス、役割、アクセスしようとしているアプリケーションなど、さまざまな要素に基づいてリソースへのアクセスを許可またはブロックするルールを定義できます。
オプション D が規定の要件に対する最も包括的なソリューションである理由と、他のオプションが問題の一部にしか対処していない理由は次のとおりです。
D). 条件付きアクセスを使用してアクセス制御ポリシーを構成します。
条件付きアクセスは、リソースへのアクセスを許可する前に複数のシグナルを評価するセキュリティ フレームワークです。
条件付きアクセス ポリシーを実装すると、次のことが可能になります。場所に基づいてアクセスを制御する: ユーザーの地理的な場所に基づいて、特定のシステムまたはデータへのアクセスを制限します。
役割に基づいてアクセスを制御する: 特定の役割を持つユーザーのみが特定のアプリケーションまたはデータにアクセスできるようにします。
デバイスのコンプライアンスを強制: ユーザーが会社が管理するデバイスまたはコンプライアンス準拠のデバイスからのみリソースにアクセスすることを要求します。
多要素認証 (MFA) を実装する: アクセス試行のコンテキストに基づいて追加の検証手順を要求します。
条件付きアクセスは、各アクセス要求の特定のコンテキストに基づいてセキュリティ ポリシーをきめ細かく動的に適用する方法を提供し、データのセキュリティを維持しながら、

場所と役割に基づいて承認されたシステムへのアクセスのみを許可するという目標と一致しています。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス：Google Workspace 管理者向けヘルプドキュメントの「コンテキストアウェア アクセス」（Google による条件付きアクセスの実装）では、ユーザー属性（グループメンバーシップや役割など）、デバイスのセキュリティステータス、ネットワークロケーションに基づいてポリシーを設定する方法について説明しています。このドキュメントでは、アクセスレベルを作成し、特定の条件に基づいてアプリケーションに割り当てる方法について詳しく説明しています。これにより、要件が満たされた場合にのみアクセスが許可されます。
A). データ損失防止 (DLP) ルールを作成して適用し、データ共有を制御します。
DLPルールは、機密データの不適切な共有を防ぐために不可欠です。しかし、DLPルールは主に、ユーザーがアクセス権限を取得した後にデータに対して何ができるかを制御することに重点を置いています。DLP自体は、ユーザーの所在地や役割に基づいて、どのシステムに誰がアクセスできるかを制御するものではありません。DLPは補完的なセキュリティレイヤーであり、これらの要素に基づくアクセス制御の主要なソリューションではありません。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス：Google Workspace 管理者向けヘルプドキュメントのデータ損失防止（DLP）では、機密情報の共有を防止するためのルールの作成方法について説明しています。このドキュメントでは、場所や役割に基づく初期アクセス制御ではなく、データの内容と共有に関連するユーザーアクションに重点を置いています。
B). すべてのリモート アクセスに対して会社全体の VPN を設定し、その使用を義務付けます。
VPN（仮想プライベートネットワーク）は、トラフィックを暗号化し、場合によっては企業管理サーバーを経由させることで、リモートユーザーと企業ネットワーク間の接続を保護できます。VPNはセキュリティを強化し、ネットワークの発信元を統一できますが、ユーザーの役割や地理的な場所に基づいてアクセスを制御するものではありません（ただし、VPNインフラストラクチャがそのような制限を適用するように構成されている場合は、より広範なアクセス制御戦略の一環として有効です）。VPNの使用を義務付けることは優れたセキュリティ対策ですが、役割ベースおよび位置情報に基づくアクセス制御のニーズを完全に満たすものではありません。
Google Workspace 管理者のトピック ガイドまたはドキュメント参照の関連付け: VPN とリモート アクセスに関するドキュメントは、接続のセキュリティ保護の文脈で言及されることがありますが、これは、Google Workspace の管理フレームワーク内でユーザー属性と場所に基づいてきめ細かなアクセス制御を実装するための主要なメカニズムではありません。
C). すべてのリモート チーム メンバーに対して 2 要素認証を実装します。
二要素認証（2FA）は、ユーザーがアクセスする前に2種類の身分証明書1の提示を求めることで、セキュリティをさらに強化します。これにより、パスワード漏洩による不正アクセス

2のリスクが大幅に軽減されます。2FAはリモートチームにとって重要なセキュリティ対策ですが、それ自体では、ユーザーの所在地や役割に基づいてアクセスできるシステムを制御することはできません。ユーザーの身元は確認しますが、所在地や役割に基づく認証という観点から、アクセス試行のコンテキストは確認しません。
Google Workspace 管理者向けトピックのガイドまたはドキュメントの参照 :Google Workspace 管理者ヘルプでは、セキュリティ強化のため、2 段階認証プロセス（Google の 2FA 実装）を有効にすることを強く推奨しています。ただし、これは主にユーザー認証に重点を置いており、場所や役割に基づくコンテキスト アクセス制御には重点を置いていません。
したがって、世界中に分散したリモートワークチームにおいて、データセキュリティポリシーの遵守を確保し、場所と役割に基づいてアクセスを制御するための最も包括的なソリューションは、条件付きアクセスを含むアクセス制御ポリシーを構成することです。このフレームワークにより、様々な要因を考慮してリソースへのアクセスを許可するかブロックするかを決定する、コンテキストアウェアなルールを作成できます。

最新問題: **54**
サイバーセキュリティチームから、外部ドメイン宛てのすべてのメールをスキャンしてクレジットカード番号が含まれているか確認するよう要請されています。クレジットカード番号が含まれている場合は、クラウドベースのサードパーティ暗号化プロバイダーを使用して暗号化する必要があります。この要請を満たすための設定は、お客様の責任となります。
何をすべきでしょうか?
A. クレジットカード番号の定義済みルールを使用して、送信メールと内部送信メールのコンテンツ コンプライアンス ルールを作成し、サードパーティの暗号化プロバイダーがスキャンして暗号化できるカスタム ヘッダーを追加します。
B. クレジットカード番号の定義済みルールを使用して送信メールのコンテンツ コンプライアンス ルールを作成し、「暗号化されていない場合はメッセージを暗号化する」をオンにします。
C. クレジットカード番号の定義済みルールを使用して送信メールのコンテンツ コンプライアンス ルールを作成し、サードパーティの暗号化プロバイダーがスキャンして暗号化できるカスタム ヘッダーを追加します。
D. クレジットカード番号の定義済みルールを使用して送信メールのコンテンツ コンプライアンス ルールを作成し、「ルートの変更」をオンにしてサードパーティの暗号化プロバイダーに送信し、暗号化します。
Answer: (解答を表示する)
Google 管理コンソールにログインします。
管理コンソールのホームページから、「アプリ」に移動し、「Google Workspace」と「Gmail」の順に選択します。「コンプライアンス」を選択し、「コンテンツ コンプライアンス」を選択

します。 別のルールを追加」をクリックして、新しいコンテンツ コンプライアンス ルールを作成します。
新しいルールの設定で、条件を指定します。
 対象となるメールメッセージ」では、 送信」と 内部 - 送信」を選択します。 条件式を追加」では 次のいずれかがメッセージに一致する場合」を選択し、 定義済みコンテンツ一致」を選択してから クレジットカード番号」を選択します。 アクション」セクションで 受信者を追加」を選択し、暗号化プロバイダーが使用するカスタムヘッダーを指定します。
ルールを保存します。
これにより、クレジットカード番号を含む電子メールはサードパーティの暗号化プロバイダーによってフラグが付けられ、暗号化され、サイバー セキュリティ チームによって設定されたセキュリティ要件が満たされます。
参照：
Google Workspace 管理者ヘルプ - コンテンツ コンプライアンスのルールを設定する

最新問題: **55**
組織は2つの企業を買収し、事業拡大を図ろうとしています。両社ともGoogle Workspaceを使用しています。CISO（最高情報セキュリティ責任者）は、厳格な 外部コンテンツ共有禁止」ポリシーを策定し、遵守するよう指示しています。CISOの指示を満たしつつ、新たに買収した企業との外部共有を可能にするには、共有ポリシーをどのように安全に設定すればよいでしょうか？
A. 信頼できるドメイン」機能を使用して、ユーザーが2社間でファイルを共有できるようにします。信頼できるドメインの許可リストを作成し、ユーザーの共有設定を選択します。
B. IT グループのみにドライブ コンテンツの外部共有を許可します。
C. 共有ドライブを使用してコンテンツを保存し、個々のファイルのみを外部と共有します。
D. 許可リストに登録されたドメインとの共有のみを許可するドライブ DLP ポリシーを作成します。
Answer: A (メーッセージを残す**)**

最新問題: **56**
Google Workspace アカウントをスケジュールされたリリース トラックに設定することで、新製品リリースの準備とユーザーへの影響の把握に時間を割くことができます。最新のロードマップには、一般提供開始後すぐにテストしてほしい新機能がいくつかあり、ディレクターから、組織全体のリリース トラックを変更せずにテストしてほしいとの依頼がありました。
何をすべきでしょうか?
A. 新しい OU を作成し、この OU 専用の迅速リリース トラックをオンにします。
B. テストユーザーを含む新しい Google グループを作成し、迅速なリリース トラックを有効にします。

C. 別個の開発環境を確立し、迅速なリリースに設定します。
D. 新しい機能へのベータ版アクセスが可能なデモ アカウントを Google に依頼してください。
Answer: C (メーッセージを残す**)**
https://support.google.com/a/answer/172177

最新問題**: 57**
貴社ではGoogle Workspace Enterpriseをご利用いただいており、Google Workspaceの他のお客様との共同作業を容易にするため、Googleドライブのファイルの外部共有を許可しています。最近、ファイルやフォルダが外部のユーザーやグループと広範囲に共有されるというインシデントが複数発生しました。最高セキュリティ責任者（CSO）は、外部からのアクセスを無効化せずに済むよう、外部共有の範囲に関するデータと継続的なアラート通知を必要としています。
最高セキュリティ責任者の要求に応えるために、どのような 2 つのアクションを取る必要がありますか? (2 つ選択してください。)
A. Google ドライブ アクティビティ ダッシュボードを使用して、ファイルを閲覧したユーザーを確認します。
B. ドライブ監査レポートからアラートを作成し、外部ファイル共有を通知します。
C. 集計レポート セクションで外部共有の合計を確認します。
D. セキュリティ調査ツールで外部共有用のカスタム ダッシュボードを作成します。
E. DLP ルールを使用して外部共有を自動的にブロックします。
Answer: B,D (メーッセージを残す**)**
外部共有のアラートを作成する:
Google 管理コンソールにアクセスします。admin.google.com にアクセスし、管理者アカウントでサインインします。
ルールに移動します。「セキュリティ」>「アラート センター」>「ルールの管理」に移動します。
新しいルールを作成する:「ルールの作成」を選択し、イベント ソースとして「ドライブ監査」を選択します。
ルール設定の構成: ファイルまたはフォルダーが外部で共有されたときにアラートをトリガーする条件を設定します。
通知設定を行う: アラートを受信するユーザーと通知方法を設定します。
ルールを保存: ルールを保存して有効にすると、外部共有アクティビティに関するアラートの受信が開始されます。
外部共有用のカスタムダッシュボードを作成します。
セキュリティ調査ツールにアクセスする: 管理コンソールで、「セキュリティ」>「調査ツール」に移動します。
新しい調査を作成する:「作成」をクリックし、データ ソースとして「ドライブ」を選択します。

調査パラメータの設定: 外部共有アクティビティ (外部で共有されたファイル、関係するユーザーなど) を追跡するためのパラメータを定義します。
ダッシュボードの作成: 調査をカスタム ダッシュボードとして保存し、外部共有アクティビティを継続的に監視します。
レビューと監視: ダッシュボードを定期的に確認し、必要に応じて自動レポートを設定します。
参照
Google Workspace 管理者ヘルプ - アラートの作成と管理
Google Workspace 管理者ヘルプ - セキュリティ調査ツールを使用する

最新問題**: 58**
昨年、パートナーの協力を得てGoogle Workspaceを導入し、プラットフォームにおける急速なイノベーションと開発の進展を目の当たりにしてきました。CIO（最高情報責任者からは、新機能の活用に備え、組織がプラットフォームを最大限に活用できるよう、Google Workspaceに関するあらゆる最新情報を把握するための手段を構築するよう依頼されています。
何をすべきでしょうか?
A. パートナーと定期的なロードマップとビジネスレビューのサイクルを確立します。
B. 管理コンソールを定期的にスキャンし、特定した新しい機能を追跡します。
C. 新しい機能に関するアラートを受け取るには、アラート センターで機能リリース アラートを作成します。
D. 違いを強調するために、組織の半分を Rapid Release Schedule に登録します。
Answer: A (メーッセージを残す**)**
* Google Workspace パートナーとの定期的な会議をスケジュールします。
* これらの会議では、Google Workspace のロードマップと今後の機能を確認します。
* 新しい機能をどのように活用して組織に利益をもたらすかについて話し合います。
* プラットフォームの機能を最大限に活用し、最新の開発状況を把握できるように、ビジネスレビューを計画します。
ロードマップとビジネス レビューを定期的に実施することで、最新の Google Workspace イノベーションとの継続的な連携が確保され、組織は新機能を最大限に活用できるようになります。
参考文献:
* Google Workspace 管理者ヘルプ - Google Workspace パートナー

最新問題**: 59**
あなたの会社には、広範囲かつきめ細かなIT管理チームがあり、あなたは適切な管理体制の確保を担っています。そのチームの一つであるセキュリティチームが、セキュリティ調査ツールへのアクセスを必要としています。どうすればよいでしょうか？
A. 事前に構築されたセキュリティ管理者ロールをセキュリティ チーム メンバーに割り当てます。

B. 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、そのロールを各セキュリティ チーム メンバーに割り当てます。
C. セキュリティ チーム メンバーにスーパー管理者ロールを割り当てます。
D. セキュリティ設定権限を持つカスタム管理者ロールを作成し、そのロールを各セキュリティ チーム メンバーに割り当てます。
Answer: B (メーッセージを残す**)**
セキュリティ チームにセキュリティ調査ツールへのアクセス権を付与するには、カスタム管理者ロールを通じて適切な権限を付与する必要があります。
カスタム管理者ロールの作成:
Google 管理コンソールで、管理者の役割に移動します。
「新しいロールの作成」をクリックします。
セキュリティ センターの権限を割り当てます。
「セキュリティ調査員」など、役割に適切な名前を付けます。
[権限] の下で、[セキュリティ センター] セクションを展開します。
セキュリティ調査ツールへのアクセスを含む、必要な権限を選択します。
ユーザーに役割を割り当てる:
ロールを作成したら、管理者ロールのセクションに移動します。
「ユーザーの割り当て」をクリックし、関連するセキュリティ チーム メンバーをこのカスタム ロールに追加します。
保存して確認:
ロールを保存し、割り当てられたユーザーに正しいアクセス権があることを確認します。
特定のセキュリティ権限を持つカスタム管理者ロールを作成すると、セキュリティ チームは過剰な権限を付与することなく、職務を遂行するために必要なツールを利用できるようになります。
参照：
管理者ロールを管理する
セキュリティ センターの概要

最新問題**: 60**
特定のドメインで TLS を強制するには、管理者がどのような手順を実行する必要がありますか?
A. 受信ドメインで電子メールの安全性機能を有効にします。
B. 受信ドメインとの安全なトランスポート準拠を設定します。
C. 受信ドメインとの代替の安全なルートを構成します。
D. 受信ドメインで DKIM 認証を設定します。
Answer: (解答を表示する**)**
* セキュアトランスポートコンプライアンス:
* TLS (トランスポート層セキュリティ) により、送信メール サーバーと受信メール サーバー間の転送中にメールが暗号化されます。

* セキュア トランスポート コンプライアンスを設定すると、特定のドメインとの間で送受信される電子メールで TLS が使用されるようになります。
* TLS を強制する手順:
* Google 管理コンソールに移動します。
* [アプリ] > [Google Workspace] > [Gmail] > [詳細設定] に移動します。
* 「コンプライアンス」セクションで、「セキュアトランスポート (TLS) コンプライアンス」を選択します。
* 「設定を追加」をクリックし、以下を設定します。
* 適切な組織単位を選択します。
* TLS を強制する受信ドメインを指定します。
* 受信メッセージ、送信メッセージ、または両方の種類のメッセージに TLS を適用することを選択します。
* 変更を保存して適用します。
参考文献
* Google Workspace 管理者ヘルプ: TLS コンプライアンスの設定

最新問題**: 61**
チームマネージャーとして、チームメンバーが休暇を共有できる休暇カレンダーを作成する必要があります。特に複数のメンバーが休暇中の場合、カレンダーを使ってチームメンバーのオンライン状況を視覚的に把握したいとします。このカレンダーを作成するにはどうすればよいでしょうか？
A. カレンダー リソースの作成をリクエストし、カレンダーを「競合しない招待を自動承認する」ように構成し、チームに「すべてのイベントの詳細を表示」アクセス権を付与します。
B. アカウントの下にセカンダリカレンダーを作成し、チームに「イベントを変更する」アクセス権を付与します。
C. カレンダー リソースの作成をリクエストし、カレンダーを「すべての招待をこのカレンダーに自動的に追加する」ように構成し、チームに「空き時間情報のみを表示」アクセス権を付与します。
D. アカウントの下にセカンダリカレンダーを作成し、チームに「空き時間情報のみ表示」のアクセス権を付与します。
Answer: (解答を表示する**)**
セカンダリ カレンダーを作成する: チーム マネージャーとして、チームの休暇を追跡するためだけに、Google アカウントで新しいカレンダーを作成します。
アクセス設定: カレンダー設定に移動し、「特定のユーザーと共有」に移動します。
アクセスを許可: チーム メンバーを追加し、「イベントを変更する」アクセスを許可して、休暇時間をカレンダーに直接追加できるようにします。
チームを教育する: このカレンダーを使用して休暇時間を追加したり、他の人のスケジュールを確認したりする方法についてチーム メンバーに通知します。

使用状況の監視: 定期的にカレンダーを確認し、すべてのチーム メンバーによってカレンダーが正しく効果的に使用されていることを確認します。
参照：
Google Workspace 管理者ヘルプ - カレンダーを共有する
Google Workspace 管理者ヘルプ - チームカレンダーを作成する

最新問題: **62**
メディア＆エンターテイメント企業であるあなたの雇用主は、世界的に有名な複数のセレブリティのために、自社ドメインでGoogle Workspace Enterpriseアカウントをプロビジョニングしたいと考えています。経営陣は、これらのVIPに高度なプライバシーを提供することに懸念を抱いています。VIPの連絡先情報を参照し、ドキュメント、チャット、カレンダーなどのGoogle Workspaceサービスを使用してVIPとの共同作業を開始できるのは、少数の上級社員のみである必要があります。
これらの要件を満たすように設定するのはあなたの責任です。何をすべきでしょうか?
A. ユーザー リストで VIP を見つけて、ユーザー設定の ディレクトリ共有」をオフにします。
B. VIP とそのハンドラーのグループを作成し、グループ アクセス レベルを [制限] に設定します。
C. ディレクトリ設定で、連絡先の共有を無効にします。
D. VIP と一般従業員用に個別のカスタム ディレクトリを作成します。
Answer: D (メーッセージを残す)
管理コンソールにアクセスします。
Google 管理コンソールにログインします。
カスタムディレクトリの設定:
ディレクトリ」> ディレクトリ設定」に移動します。
カスタムディレクトリ」をクリックします。
VIP 用のカスタム ディレクトリを作成します。
VIP 専用の新しいディレクトリを作成します。
このディレクトリに VIP を追加します。

アクセス制御を設定する:
VIP ディレクトリを表示およびアクセスできるユーザーを構成します。
このディレクトリへのアクセスは上級従業員または特定のグループのみに許可します。
ディレクトリの可視性を構成する:
VIP の連絡先情報がメイン ディレクトリに表示されないようにします。
設定を調整して、表示とアクセスを適切に制限します。
テスト構成:
一般従業員と上級従業員の両方のアカウントからディレクトリの可視性をチェックして、設定を確認します。
参照 :
ディレクトリの可視性を管理する
カスタムディレクトリの設定と管理

最新問題**: 63**
人事 (HR) チームは、機密文書を保護し、退職時の文書紛失のリスクを軽減しながら、組織全体で重要な文書を共有できる一元的な場所を必要としています。これらの文書は、HR チームのメンバーが編集できる必要があります。最適な設定方法は何でしょうか？
A. 機密ではないファイル用の共有ドライブを作成し、HR チーム マネージャーにアクセス権を付与し、組織全体に貢献者アクセス権を付与します。
B. 機密でないファイル用の共有ドライブを作成し、HR チームにコンテンツ マネージャー アクセス権を付与し、組織に表示アクセス権を付与します。
C. HR リーダーに、MyDrive 内に非機密ファイル用のフォルダーを作成してもらい、HR チームに編集アクセス権を与え、組織に表示アクセス権を与えてもらいます。
D. すべてのファイル用の共有ドライブを作成し、HR チームにコンテンツ マネージャー アクセス権を付与し、組織に表示アクセス権を付与します。
Answer: B (メーッセージを残す**)**

最新問題**: 64**
あなたの会社では、機密情報を含む社内ニュースレターを全従業員に電子メールで配布しています。
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おり、データ漏洩の恐れがあります。これを防ぐには、社内での正当な共有は許可しつつ、このような転送を自動的に検知・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。どうすればよいでしょうか？
A. 外部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ニュースレターに追加します。
B. 社内ニュースレターを対象とし、外部への転送を検知するGmailコンテンツコンプライアンスルールを作成します。転送が検出された場合は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を自動的に取り消します。
D. コンテンツ コンプライアンス ルールを作成し、ニュースレターの件名を変更して、外部転送に対する警告を追加します。
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ターゲットに指定し、外部アドレスへの転送を自動検出できます。このようなメッセージを拒否することで、社内での共有を許可しながらも、機密情報の不正な共有を防ぐことができます。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**: 65**
最近、あなたの組織は複数のユーザーに影響を与えるフィッシング攻撃の標的となりました。フィッシング攻撃の全容を効率的に把握し、さらなる問題の発生を防ぐ必要があります。どうすればよいでしょうか？
A. 1. BigQuery ログでフィッシングとしてマークされたすべてのメッセージを検索します。
2. すべての電子メール通信にトランスポート層セキュリティ (TLS) を要求します。
3. すべてのユーザーにパスワードをリセットするよう指示します。
B. 1. 電子メール ログ検索を使用して、過去 3 日間のすべての電子メールを取得します。
2. 受信した一般的なメールのログを分析し、ユーザーに連絡します。
3. 悪意のあるメール アドレスをブロックするための Gmail フィルターを作成する方法をユーザーに指導します。
C. 1. セキュリティ ダッシュボードを使用して、なりすましの可能性がある証拠を示すメッセージの数を確認し、影響を受けるユーザーに対して調査ツールを使用して悪意のある電子メールを削除します。
2. 高度なフィッシングおよびマルウェア対策を有効にします。
3. Chrome 用の Google のパスワード アラート拡張機能を展開します。
D. 1. ユーザーから転送されたフィッシングサンプルを収集します。
2. IP アドレスとメール アドレスを拒否リストに追加します。
3. 影響を受けるユーザーのみを多要素認証 (MFA) に登録します。
Answer: C (メーッセージを残す**)**
セキュリティダッシュボードと調査ツールを使用すると、影響を受けたユーザーを迅速に特定し、悪意のあるメールを削除できます。高度なフィッシングおよびマルウェア対策を有効にすると、セキュリティがさらに強化され、パスワードアラートを導入することでパスワードの侵害を検出できます。

最新問題**: 66**

カレンダーリソースで自動部屋割り当てを有効にしていますが、重複予約があった場合、自動割り当てが機能しません。何が問題なのでしょうか？
A. 定期的なイベントでは自動ルーム置換は機能しません。
B. この機能を使用するには、カレンダーイベントの所有者に建物とリソースの管理者権限が必要です。
C. カレンダーリソースのリソースカテゴリがCONFERENCE_ROOMとして設定されていません
D. イベントには 20 人を超える参加者がいます。
Answer: A (メーッセージを残す)
自動部屋交換機能は、定期的なイベントでは機能しません。この制限により、定期的なイベントで予約が重複した場合、システムは自動的に代替の部屋を見つけられません。この機能は、単発イベントでのみ機能するように設計されています。
参照：
Google Workspace 管理者ヘルプ - 会議室の自動交換を設定する

最新問題: **67**
組織の Google Workspace 管理者として、Google Workspace データにアクセスできるサードパーティ製アプリを管理する役割を担っています。管理を実装する前に、まず、Workspace データへのアクセスを許可されているすべてのサードパーティ製アプリ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. 管理コンソールを開き、[セキュリティ] > [API コントロール] > [アプリのアクセス制御] > [サードパーティ アプリのアクセスを管理] を選択します。
B. 管理コンソールを開き、[セキュリティ] > [API コントロール] > [アプリのアクセス制御] > [Google サービスの管理] を選択します。
C. 管理コンソール > セキュリティ > 安全性の低いアプリを開きます。
D. 管理コンソールを開き、[セキュリティ] > [API コントロール] > [アプリのアクセス制御] > [設定] を選択します。
Answer: (解答を表示する)
管理コンソールにアクセスする: Google Workspace 管理コンソールにログインします。
セキュリティ設定に移動します。セキュリティ > API コントロールに移動します。
サードパーティ アプリのアクセスを管理する: 『アプリ アクセス制御」を選択し、 『サードパーティ アプリのアクセスを管理」をクリックします。
承認済みアプリを確認する: ここでは、Google Workspace データへのアクセスが承認されているサードパーティ製アプリの一覧が表示されます。
アクセスを評価する: 各サードパーティ アプリの権限とアクセス スコープを確認し、引き続きアクセスを許可するか、または制限する必要があるかを判断します。
参照
Google サポート: Google Workspace データにアクセスするサードパーティ製アプリと社内アプリを制御する

最新問題: **68**
Madeupcorp.com は、サードパーティ製のメールシステムから Google Workspace への移行を進めています。マーケティング担当副社長は、チームが既に @madeupcorp.com のメールアドレスを使用して企業の AdSense、AdWords、YouTube チャンネルを管理しているものの、どのユーザーがどのサービスにアクセスしているかを把握していないことに懸念を抱いています。業務に支障が生じないよう、万全の体制を整える必要があります。
何をすべきでしょうか?
A. 管理対象外ユーザー向けに転送ツールを実行します。
B. Google フォームを使用してマーケティング部門のユーザーを調査します。
C. Google Workspace を構成するために必要なアクションがないことを VP に保証します。
D. 影響を受けるユーザーを特定するには、Google Enterprise サポートにお問い合わせください。
Answer: (解答を表示する**)**
* 現在の状態を評価する: AdSense、AdWords、YouTube などのサービスに @madeupcorp.com のメール アドレスを使用しているユーザーを特定します。
* 管理対象外ユーザー用の転送ツールを使用する:
* Google 管理コンソールにアクセスします。admin.google.com にアクセスし、管理者アカウントでログインします。
* ツールに移動します。管理コンソールで、「ツール」に移動し、「管理対象外ユーザー向けの移行ツール」を選択します。
* ドメイン情報の入力: ドメイン名 (madeupcorp.com) を入力し、ドメインを確認します。
* 管理対象外ユーザーのリスト: ツールは、自分のアカウントを使用している管理対象外ユーザーのリストを生成します。
@madeupcorp.com の電子メール アドレス。
* 移行リクエストの送信: これらのユーザーに移行リクエストを送信し、管理対象の Google Workspace アカウントへの移行を承認するよう促します。
* フォローアップ: 企業のメール アドレスを使用して Google サービスにアクセスする際に中断が生じないように、すべてのユーザーが移行リクエストを承認していることを確認します。
* 確認: 移管したアカウントが Google Workspace ドメインで管理されていることを確認します。
参考文献
* Google Workspace 管理者ヘルプ - 管理対象外ユーザー向けの移行ツール

最新問題: **69**
ある小売企業は、消費者市場の循環的な性質により、従業員の離職率が高いという問題を抱えています。機密情報の漏洩が増加したため、従業員のセキュリティ調査を継続的に監

視するための特別な管理職が必要になりました。このような調査の可視性を高めるために、どのような対策を講じるべきでしょうか？
A. 「スーパー管理者」権限を持つ管理者に「サービス管理者」ロールを割り当てます。
B. 「カスタムロール」を作成し、新しい管理者のすべての Google Vault 権限を追加します。
C. 新しい管理者が Google Vault にアクセスできることを確認します。
D. 「カスタムロール」を作成し、Google Vault の問題、記録保持、検索、エクスポートを管理する権限を追加します。
Answer: D (メーッセージを残す)
管理コンソールにアクセスします。Google 管理コンソールにログインします。
管理者ロールに移動します。アカウント設定の下にある管理者ロールに移動します。
カスタム ロールの作成: 「新しいロールの作成」をクリックし、適切な名前を付けます。
Vault 権限の割り当て: 案件、記録保持、検索、エクスポートの管理など、Google Vault に関連する権限を選択します。
ユーザーにロールを割り当てる: セキュリティ調査を担当する指定された管理者にこのカスタム ロールを割り当てます。
アクセスの確認: 新しい管理者が、進行中のセキュリティ調査を監視および管理するために必要な Google Vault へのアクセス権を持っていることを確認します。
参照：
Google Workspace 管理者ヘルプ - カスタム管理者ロールの作成
Google Workspace 管理者ヘルプ - Google Vault の権限

最新問題**: 70**
組織の従業員が、期間は不明ですが長期休暇を取ることになりました。
休暇中の従業員のチームメイトは共有プロジェクトに取り組んでおり、休暇中の従業員が所有するすべてのプロジェクトファイルにアクセスする必要があります。これらのファイルへのアクセス権を効率的に付与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 ファイルを見つけてダウンロードし、チームメイトと共有します。
B. セキュリティ調査ツールを使用して、プロジェクトファイルを含むフォルダを見つけます。チームメイトのためにファイルのコピーを作成します。
C. 休暇中の従業員の Workspace アカウントを停止します。
D. 所有権の譲渡機能を使用して、チームメイトにプロジェクト ファイルへのアクセス権を付与します。
Answer: D (メーッセージを残す)

最新問題**: 71**
会社では、一部の従業員向けにGemini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するために、最も効率的な方法を検討する必要があります。どうすればよいでしょうか？

A. マーケティング部門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. マーケティングと営業用の組織単位（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に対してのみ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。他の部門のユーザーにはGeminiを使用しないよう指示します。
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に別々の組織単位（OU）を作成することで、Geminiライセンスをこれらの部門のみに適用できます。そのOUのみでGeminiを有効にすると、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、効率的で拡張性の高いソリューションを実現できます。これにより、手動での割り当てや、他部門のユーザーへの不要な指示が不要になります。

最新問題**: 72**
貴社ではGoogle Workspace Business Plusエディションをご利用いただいておりますが、セキュリティチームから、現地従業員がいない国から貴社のGoogle Workspaceドメインへのログイン試行が複数回失敗したとの報告がありました。影響を受けたアカウントは、本社の複数の幹部のアカウントです。
このセキュリティリスクを軽減するための対策を講じるよう求められています。予算は問題ではありませんが、会社としてはこの問題の解決にかかる費用を最小限に抑えたいと考えており、あなたはその管理を任されています。最小限のコストでリスクを軽減するには、どの2つの解決策が効果的でしょうか？（2つ選択してください。）
A. すべてのアカウントに対して Cloud Identity Premium を登録し、会社の従業員がいる国のリストに対してのみコンテキストアウェア アクセス レベルを定義します。
B. 専用プロジェクトに Google Cloud Armor をデプロイし、特定の場所からのみ Google Workspace へのアクセスを許可するルールを作成します。
C. すべての幹部に対して、Google のベスト プラクティスに合わせてランダムな文字で新しいアカウントを作成し、以前のアカウントからデータを移行してから削除します。
D. セキュリティ キーを持つすべてのユーザーに対して 2 段階認証プロセスを展開します。
E. すべてのアカウントを Google Workspace Enterprise Plus にアップグレードし、会社の従業員がいる国のリストに対してのみコンテキストアウェア アクセス レベルを定義します。
Answer: A,D (メーッセージを残す**)**

最新問題**: 73**
会社は従業員に安全なアクセスを提供したいと考えています。最高情報セキュリティ責任者はデバイスへの周辺機器アクセスを無効にしましたが、2段階認証は有効にしたいと考え

ています。そのため、Google Workspaceを使用してアプリケーションへの安全なアクセスを提供する必要があります。
何をすべきでしょうか?
A. 電子メールによる追加のセキュリティ検証を有効にします。
B. Google Authenticator による認証を有効にします。
C. Google Workspace 経由でブラウザまたはデバイスの証明書をデプロイします。
D. すべてのユーザーの USB Yubikey を構成します。
Answer: B (メーッセージを残す)
* 2段階認証 (2SV):
* 2段階認証は、パスワードに加えて2つ目の要素による本人確認を要求することで、セキュリティをさらに強化します。これにより、パスワードが漏洩した場合でも、不正アクセスから保護されます。
* Google 認証システム:
* Google Authenticatorは、時間ベースのワンタイムパスコード (TOTP) を生成するモバイルアプリです。
2SV。デバイスがオフラインの場合でも機能し、安全で信頼性の高い2段階認証を提供します。
* 実装手順:
* 2段階認証を有効にする:
* Google 管理コンソール (admin.google.com) にアクセスします。
* 「セキュリティ」>「認証」>「2段階認証」に移動します。
* 組織に対して 2 段階認証プロセスを有効にします。
* Google Authenticator を導入する:
* ユーザーに、それぞれのアプリ ストア (iOS または Android) から Google 認証システム アプリをダウンロードするよう指示します。
* Google Workspace アカウントで Google Authenticator を設定するためのガイダンスを提供します。
* ユーザーは、セットアップ プロセス中に提供される QR コードをスキャンして、自分のアカウントを Authenticator アプリにリンクします。
* Google Authenticator の利点:
* セキュリティ: コードはユーザーのデバイス上で生成され、30 秒ごとに変更されるため、非常に安全な 2 段階認証方式を提供します。
* 使いやすさ: わかりやすいユーザー インターフェイスにより、セットアップと使用が簡単です。
* オフライン機能: インターネットにアクセスできない場合でもコードを生成できるため、一貫性が保たれます。
* 2SV コードへのアクセス。
他の選択肢があまり適していない理由:
* A. 電子メールによる追加のセキュリティ検証を有効にする:

* メールベースの認証は、メールアカウントが簡単に侵害される可能性があるため、アプリベースの 2SV よりも安全性が低くなります。
* C. Google Workspace 経由でブラウザまたはデバイスの証明書を展開する:
* デバイス証明書はセキュリティを強化しますが、通常は 2 段階認証ではなく、デバイス管理とアクセス制御のために使用されます。
* D. すべてのユーザーのUSB Yubikeyを設定します。
* USB YubiKeyは非常に安全で2段階認証に適していますが、ハードウェアトークンの物理的な配布と管理が必要であり、ロジスティクスが複雑でコストがかかる可能性があります。周辺機器へのアクセスが制限されている状況を考えると、このオプションは最高情報セキュリティ責任者 (CIO) のポリシーに反する可能性があります。
参考文献:
* Google Workspace 管理者ヘルプ: 2 段階認証プロセスの設定
* Google Workspace セキュリティ: 2 段階認証プロセス

最新問題: **74**
組織では、Workspace ドメインに到達する前にメールをフィルタリングするサードパーティ製品を使用しています。この製品から受信するメールの量が多いため、受信メッセージがスパム攻撃とみなされないようにするには、Gmail をどのように設定すればよいでしょうか？
A. 製品の IP アドレスを承認済み送信者として追加します。
B. サードパーティのフィルタリング製品の IP アドレスを許可リストに追加します。
C. 製品の IP アドレスを組織の SPF レコードに追加します。
D. 製品の IP アドレスを受信ゲートウェイとして一覧表示します。
Answer: D (メーッセージを残す**)**
サードパーティのフィルタリング製品からの受信メッセージがスパム攻撃とみなされないようにするには、その製品のIPアドレスを受信ゲートウェイとして設定する必要があります。この設定により、GmailはこれらのIPアドレスから送信されるメールが信頼できるものであり、受信メールの量に基づいてスパムとして分類されないことを認識します。
参照：
Google Workspace 管理者ヘルプ - 受信メールゲートウェイの設定
Google Workspace 管理者ヘルプ - 受信ゲートウェイ設定を使用してメールのなりすましやスパムを防ぐ

最新問題: **75**
従業員が組織を退職したため、その従業員のドライブ データを 3 年間保持する必要があります。保持ルールは 3 年間に設定されています。従業員のデータが Vault で表示され、最もコスト効率の高い方法で Vault 管理者がアクセスでき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. ユーザーにアーカイブユーザー(AU)ライセンスを割り当てます
B. 3年間の期間が終了するまでユーザーを停止します

C. Vault からユーザーのドライブ データをエクスポートし、ユーザーを削除します。
D. ドライブデータの所有権をユーザーのマネージャーに変更し、ユーザーを削除します
Answer: A (メーッセージを残す**)**

最新問題**: 76**
組織の従業員がGoogle Meetのビデオ通話で問題が発生しており、自力で解決できませんでした。この問題を解決する必要があるのですが、まず何をすべきでしょうか？
A. 従業員の Meet 品質レポートを表示します。
B. ネットワーク管理者に、ユーザー専用の Meet IP アドレス範囲を追加するよう依頼してください。
C. 従業員のデバイスを再起動します。
D. 従業員の Meet 設定を確認します。
Answer: A (メーッセージを残す**)**
これにより、問題の診断に不可欠な、ネットワークやシステムのパフォーマンスなど、通話品質に関する詳細なメトリックにアクセスできるようになります。

最新問題**: 77**
社内ではGoogle Workspace Enterprise Plusをご利用いただいており、人事部門から全社員のGoogle Workspaceの導入状況を分析するため、ワークインサイトへのアクセスを求められております。ワークインサイトの権限を 全チームのデータの閲覧」に設定したカスタムロールを人事グループに割り当てましたが、アプリケーションへのアクセス時にエラーが発生します。どうすればよいでしょうか？
A. 会社の全従業員に 全チームのデータを表示する」権限を割り当てます。
B. すべての従業員に対して Work Insights アプリがオンになっていることを確認します。
C. セキュリティ > APIコントロール > アプリアクセスコントロールでWork Insights APIが設定されていることを確認します。
制限なし」
D. レポート > BigQuery エクスポートでジョブが有効になっていることを確認します。
Answer: B (メーッセージを残す**)**
* 管理コンソールにアクセス: Google 管理コンソールにログインします。

* Work Insights の設定に移動します。[アプリ] > [その他の Google サービス] > [Work Insights] に移動します。
* Work Insights をオンにする: 組織内のすべての従業員に対して Work Insights アプリが有効になっていることを確認します。
* 権限の確認: 「すべてのチームのデータを表示する」権限を持つカスタム ロールが HR グループに正しく割り当てられていることを確認します。
* アクセスをテスト: HR ユーザーに Work Insights への再度アクセスを試みるように依頼し、エラーが解決されたことを確認します。
* 監視とレビュー: アクセスと使用状況を監視して、HR が Google Workspace の導入を問題なく分析できるようにします。
参考文献:
* Google Workspace 管理者ヘルプ - ワーク インサイトのオン/オフを切り替える
* Google Workspace 管理者ヘルプ - ワーク インサイトの権限

最新問題**: 78**
あなたの会社には、広範囲かつきめ細かなIT管理チームがあり、あなたは適切な管理体制の確保を担っています。そのチームの一つであるセキュリティチームが、セキュリティ調査ツールへのアクセスを必要としています。どうすればよいでしょうか？
A. 事前に構築されたセキュリティ管理者ロールをセキュリティ チーム メンバーに割り当てます。
B. 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、そのロールを各セキュリティ チーム メンバーに割り当てます。
C. セキュリティ チーム メンバーにスーパー管理者ロールを割り当てます。
D. セキュリティ設定権限を持つカスタム管理者ロールを作成し、そのロールを各セキュリティ チーム メンバーに割り当てます。
Answer: B (メーッセージを残す**)**
セキュリティ チームにセキュリティ調査ツールへのアクセス権を付与するには、カスタム管理者ロールを通じて適切な権限を付与する必要があります。
* カスタム管理者ロールの作成:
* Google 管理コンソールで、管理者の役割に移動します。
* 「新しいロールの作成」をクリックします。
* セキュリティ センターの権限を割り当てます:
* 「セキュリティ調査員」など、役割に適切な名前を付けます。
* [権限] の下で、[セキュリティ センター] セクションを展開します。
* セキュリティ調査ツールへのアクセスを含む、必要な権限を選択します。
* ユーザーに役割を割り当てる:
* ロールを作成したら、管理者ロール セクションに移動します。
* 「ユーザーの割り当て」をクリックし、関連するセキュリティ チーム メンバーをこのカスタム ロールに追加します。

* 保存して確認:
* ロールを保存し、割り当てられたユーザーに正しいアクセス権があることを確認します。特定のセキュリティ権限を持つカスタム管理者ロールを作成すると、セキュリティ チームは過剰な権限を付与することなく、職務を遂行するために必要なツールを利用できるようになります。
参考文献:
* 管理者の役割を管理する
* セキュリティセンターの概要

最新問題: **79**
あなたの会社は訴訟に巻き込まれており、法務部門は特定の2人のユーザーのすべてのメールの開示と保管を依頼されています。さらに、以下の内容を含むメールの開示と保管も依頼されています。
「秘密プロジェクト123」
この要求を満たすにはどのような手順を踏む必要がありますか?
A. 案件と保留を作成します。保留をGmailに設定し、最上位の組織に設定し、検索語を「secret project 123」に設定します。2つ目の保留を作成します。2つ目の保留をGmailに設定し、アカウントに設定し、user1@your-company.com、user2@your-company.comと入力します。保存します。
B. 案件と保留を作成します。保留をGmailに設定し、アカウントに設定し、ユーザー名を次のように設定します。
user1@your-company.com、user2@your-company。検索語を「(secret project 123)」に設定し、保存します。
C. 案件と保留を作成します。保留をGmailに設定し、アカウントを選択し、「user1@your-company.com AND user2@your-company.com」と入力します。検索語句を「secret AND project AND 123」と設定します。
保存。
D. 案件と保留を作成します。保留をGmailに設定し、アカウントに設定し、ユーザー名を次のように設定します。
user1@your-company.com、user2@your-company。検索語を「secret OR project OR 123」に設定してください。
保存。
Answer: B (メーッセージを残す**)**
* 案件を作成: Google Vault にアクセスし、訴訟に関する新しい案件を作成します。案件は、訴訟記録保持（リティゲーションホールド）や検索の管理に使用されます。
* 保留を作成: 案件内で新しい保留を作成します。
* 保留範囲を設定する: メールを検出して保留することが要件であるため、保留範囲を Gmail に設定します。

* アカウントの指定: ユーザー名を user1@your-company.com と user2@your-company.com に設定します。
これにより、特定のユーザーのすべての電子メールが保持されるようになります。
* 検索語の設定：§ecret project 123」という検索語を使用すると、この特定の用語に言及するメールをすべて保持できます。これは、 §ecret project 123」に言及するすべてのメールを捕捉する、広範な検索です。
* 保留を保存: 指定されたユーザーと検索用語に関連するすべてのメールを確実に取得できるように、保留を保存します。
参考文献
* Google サポート: 保留を作成または更新する

最新問題**: 80**
貴社の法務部門は、緊急を要する合併・買収（M&A）案件に取り組んでいます。現在休暇中の従業員からの特定のメールに緊急にアクセスする必要があります。組織の現在の保存ポリシーは 無期限」に設定されています。法務部門に必要なメールを、データ プライバシーを確保しながら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、関連する電子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ます。
B. 法務部門に、M&A 関連の電子メールに限定した制限付きで従業員の電子メール アカウントへのアクセスを一時的に許可します。
C. 従業員のメールボックスへの代理アクセス権を持つ同僚に、関連する電子メールを特定して法務部門に転送するよう依頼します。
D. Google Vault を使用して、M&A 取引に関する案件を作成します。従業員のメールボックス内で関連メールを検索します。関連メールをエクスポートして法務部門と共有します。
Answer: D (メーッセージを残す**)**
Google Vault を使用して M&A 取引に固有の案件を作成することで、法的、セキュリティ、プライバシーを遵守したメールの取得が可能になります。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、合併と買収に関連する特定のメールを検索、エクスポートし、法務部門と共有できます。このアプローチにより、データのプライバシーと組織ポリシーの遵守の両方が確保されます。

最新問題**: 81**
建物内の既存の会議室に新しい Google Meet ハードウェア デバイスを登録しました。ユーザーから、会議室の新しいハードウェアに予定されていたカレンダー イベントが表示されないという報告がありました。問題を調査して修正する必要があります。どうすればよいですか?
A. 会議室リソースカレンダーが作成され、Meet ハードウェアがそのリソースに関連付けられていることを確認します。

B. 新しいリソースカレンダーを作成し、Meet ハードウェアをその新しいリソースに関連付けます。
C. コントロール パネルの Meet 品質ツールを使用して、新しくインストールされた Meet ハードウェアを検索します。
D. リソースカレンダーのアクセス権限が 「すべてのイベントの詳細を表示」に設定されていることを確認します。
Answer: A (メーッセージを残す**)**
新しいハードウェアに予期したカレンダー イベントが表示されない問題を調査して修正するには、次の手順に従います。
Google 管理コンソールにログインします。特権管理者権限を持つアカウントを使用します。
リソース カレンダーを確認します。
[アプリ] > [Google Workspace] > [カレンダー] > [リソース] に移動します。
会議室のリソース カレンダーが作成されていることを確認します。
Meet ハードウェアを関連付けます。
[デバイス] > [Google Meet ハードウェア] に移動します。
新しいハードウェア デバイスを見つけて、その設定を確認します。
デバイスが正しい会議室リソース カレンダーに関連付けられていることを確認します。
カレンダーの権限を確認します:
[カレンダー] > [リソースの管理] に移動します。
Meet ハードウェアに関連付けられたカレンダーのアクセス権限が 「すべての予定の詳細を表示」に設定されていることを確認してください。参考:
Google Workspace 管理者ヘルプ - リソースの管理
Google Workspace 管理者ヘルプ - Google Meet ハードウェア

最新問題**: 82**
マーケティング責任者から次のメールを受け取りました:
こんにちは、ワークスペース管理者:
来週、新しいコンサルタントが 「大量マーケティングメール配信」プロジェクトに着任します。コンサルタントにはマーケティングチームの他のメンバーの連絡先情報は閲覧できるものの、社内の他のメンバーの連絡先情報は閲覧できないようにしたいと考えています。この点について、何かご支援いただけることはありますか？
この要求を満たすために実行する必要がある 2 つの手順は何ですか?
2つの回答を選択してください
A. 制限された連絡先アクセスを必要とするコンサルタント用に、分離された OU を作成します。
B. コンサルタントが表示できる連絡先を含むグループを作成します。
C. グループ設定でコンサルタントにオーナーの役割を適用します。
D. マーケティング OU の下にコンサルタントを作成します。

E. サービス > サービス設定の管理者権限が割り当てられていること、およびサービス > 連絡先 > 連絡先設定メッセージが設定されていることを確認します。
Answer: A,B (メーッセージを残す**)**
マーケティング責任者からのリクエストを満たすには、次のことが必要です。
連絡先へのアクセスを制限する必要があるコンサルタントのために、独立した組織単位（OU）を作成します。これにより、他のユーザーに影響を与えることなく、コンサルタントに特定のポリシーを管理および適用できます。
コンサルタントが閲覧できる連絡先を含むグループを作成します。このグループにはマーケティングチームメンバーの連絡先情報が含まれ、コンサルタントがアクセスできるのは特定の連絡先のみになります。
参照：
Google Workspace 管理者ヘルプ - 連絡先へのユーザー アクセスを管理する
Google Workspace 管理者ヘルプ - グループの作成と管理

最新問題**: 83**
組織には、Google ドライブ内の機密ファイルの外部共有を検出してユーザーに警告するデータ損失防止 (DLP) ルールがあり、外部ユーザーが閲覧権限を持つファイルをローカルマシンにダウンロードできない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. 何もしません。ドライブのファイルを閲覧専用にすると、ユーザーはファイルをダウンロードできなくなります。
B. 既存のDLPルールを変更して、コメント投稿者と閲覧者によるダウンロード、印刷、コピーを無効にします。
C. 既存のコンテンツ検出条件を使用して新しいDLPルールを作成しますが、新しいルールのアクションを ダウンロードを無効にする」、 印刷する」、 ロメント投稿者と閲覧者へのコピー」に変更します。
D. 新しいDLPルールを作成し、制限する組織単位またはグループにスコープを設定します。
Answer: C (メーッセージを残す**)**
管理コンソールにアクセスする: 管理者アカウントを使用して Google 管理コンソールにログインします。
DLP ルールに移動します。[アプリ] > [Google Workspace] > [ドライブとドキュメント] > [データ損失防止] に移動します。
新しいルールを作成する: ルールの作成」をクリックし、テンプレートから開始するか、カスタム ルールを作成するかを選択します。
コンテンツ検出条件の設定: 機密ファイルを識別する既存のコンテンツ検出条件を使用します。

アクションの設定 :コメント投稿者と閲覧者に対してダウンロード、印刷、コピーを無効にするアクションを設定します。これにより、閲覧権限を持つ外部ユーザーがファイルをダウンロードできなくなります。
関連する OU/グループにルールを適用する: この制限を適用する特定の組織単位またはグループにルールの範囲を設定します。
保存して適用 :ルールを保存し、有効化されていることを確認してください。これにより、外部で共有される機密ファイルに対して新しい制限が適用されます。
参照 :
Google Workspace 管理者ヘルプ: ドライブのデータ損失防止
Google Workspace DLP のベスト プラクティス

最新問題**: 84**
ユーザーAはBasicライセンスを保有しています。ユーザーBはBusinessライセンスを保有しています。これら2人のユーザーは、多くの追加ユーザーとともに、同じ会社の同じ組織部門に所属しています。ユーザーAがドライブにアクセスしようとすると、次のエラーが表示されます。 申し訳ございませんが、Googleドキュメントエディタへのアクセス権がありません。」
アクセスするには、組織の管理者に問い合わせてください。」ユーザー B には同じエラーは表示されず、問題なくサービスにアクセスします。
ユーザー A にドライブへのアクセスを提供するにはどうすればよいでしょうか?
A. ディレクトリでユーザー A を選択し、[アプリ] セクションで [ドライブとドキュメント] が無効になっているかどうかを確認します。
もしそうなら、ユーザー レコードで有効にします。
B. [アプリ] > [Google Workspace] > [ドライブとドキュメント] で、ユーザーが所属する組織部門を選択し、その組織部門に対してドライブを有効にします。
C. 「アプリ」> 「Google Workspace」で、ドライブとドキュメントがサービスとして有効になっているグループを特定します。このグループにユーザーAを追加します。
D. ディレクトリでユーザー A を選択し、[ライセンス] セクションでライセンスを Basic から Business に変更して、ドライブとドキュメント サービスを追加します。
Answer: D (メーッセージを残す**)**
* 管理コンソールにアクセスする: Google Workspace 管理コンソールにログインします。
* ユーザー A を選択: ディレクトリに移動し、ユーザー A のアカウントを選択します。
* ライセンスの確認: [ライセンス] セクションで、ユーザー A の現在のライセンスの種類を確認します。ユーザー A は基本ライセンスを保有しているため、ビジネス ライセンス保有者が利用できる特定のサービスにアクセスできません。
* ライセンスの変更 :ユーザーAのライセンスをBasicからBusinessに変更します。これは、「ライセンス」セクションでユーザーAにBusinessライセンスを割り当てることで実行できます。

* アクセスの確認: ライセンスを変更した後、ユーザー A がエラーなく Google ドライブとドキュメントにアクセスできることを確認します。
参考文献
* Google サポート: ユーザー ライセンスの割り当てまたは削除

最新問題: **85**
マーケティング責任者から次のメールを受け取りました:
こんにちは、ワークスペース管理者:
来週、新しいコンサルタントが 「大量マーケティングメール配信」プロジェクトに着任します。コンサルタントにはマーケティングチームの他のメンバーの連絡先情報は閲覧できるものの、社内の他のメンバーの連絡先情報は閲覧できないようにしたいと考えています。この点について、何かご支援いただけることはありますか？
この要求を満たすために実行する必要がある 2 つの手順は何ですか?
2つの回答を選択してください
A. マーケティング OU の下にコンサルタントを作成します。
B. 制限された連絡先アクセスを必要とするコンサルタント用に、分離された OU を作成します。
C. コンサルタントが表示できる連絡先を含むグループを作成します。
D. グループ設定でコンサルタントにオーナーの役割を適用します。
E. サービス > サービス設定の管理者権限が割り当てられていることを確認し、サービス > 連絡先 > 連絡先設定メッセージが設定されていることを確認します。
Answer: B,C (メーッセージを残す**)**

最新問題: **86**
ある企業は、営業部門の従業員のみにiOSデバイスを配布したいと考えています。配布したデバイスで以下の操作を実行できるようにしたいと考えています。
パスワード ポリシーを制御します。
企業アプリをユーザーが利用できるようにします。
紛失または不正アクセスされた場合にデバイスをリモートで消去する
デバイス ポリシーを構成する前に必要な 2 つの手順は何ですか (2 つ選択してください)。
A. ドメインの高度なモバイル管理をオンにします。
B. 営業部門の高度なモバイル管理をオンにする
C. デバイスの承認を設定します。
D. Apple Push 証明書を設定します。
E. すべてのデバイスに Apple 証明書を展開します。
Answer: (解答を表示する**)**
https://support.google.com/a/answer/7396025?hl=ja
https://support.google.com/a/answer/6080359?hl=ja

最新問題: **87**

組織が小規模な代理店を買収しました。これらの新入社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。新規ユーザーは、新しい組織のメールアドレスと、サブ代理店のドメイン名を持つメールアドレスの両方を使用できる必要があります。どうすればよいでしょうか？
組織が小規模な代理店を買収しました。これらの新入社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。新規ユーザーは、新しい組織のメールアドレスと、サブ代理店のドメイン名を持つメールアドレスの両方を使用できる必要があります。どうすればよいでしょうか？
A. 取得したドメインを Google の MX レコードにリダイレクトし、アカウントを 送信者」アドレスとして追加します。
B. ドメインの管理ページから、取得した代理店をセカンダリ ドメインとして設定します。
C. [ドメインの管理] ページから、取得した代理店をユーザー エイリアス ドメインとして設定します。
D. 取得した代理店をセカンダリ ドメインとして設定し、プライマリ ドメインに交換します。
Answer: C (メーッセージを残す**)**
買収した代理店をユーザーエイリアスドメインとして設定することで、ユーザーは新しい組織のメールアドレスを使用しながら、サブ代理店ドメインで以前のメールアドレスを使用してメールの送受信を継続できます。このアプローチにより、別々のアカウントを追加設定することなく、両方のメールアドレスを効率的に使用できます。

最新問題**: 88**
組織では、サードパーティ製アプリケーションによる連絡先情報へのアクセスを懸念しています。Google Workspace の特権管理者として、ユーザーが手動で連絡先を共有する機能を制限することなく、サードパーティによるアクセスを制限することが求められています。どうすればよいでしょうか？
A. 連絡先の共有を無効にします。
B. Google 連絡先への API アクセスを無効にし、ディレクトリ共有を有効にします。
C. Google 連絡先への API アクセスを有効にし、ディレクトリ共有を無効にします。
D. 連絡先の共有を有効にします。
Answer: B (メーッセージを残す**)**
A は不正解です。API アクセスが制限されないためです。
B は正解です。ユーザーの共有機能を維持しながら API アクセスを防止します。
C は不正解です。API アクセスが制限されないためです。
D は不正解です。API アクセスが制限されないためです。
参照：
https://support.google.com/a/answer/60218?hl=ja

最新問題**: 89**

あなたの会社は最近、Google Workspace を活用していない組織を買収しました。
現在、会社では Google Cloud Directory Sync（GCDS）を使用して、LDAP ディレクトリから Google Workspace への同期を行っています。新たに買収した組織（ユーザーも LDAP ディレクトリに登録されている）にも GCDS の 2 つ目のインスタンスを導入し、同じ戦略を適用したいと考えています。設定を成功させるには、GCDS インスタンスをどのように変更すればよいでしょうか。
（2つ選択してください。）
A. 現在の GCDS インスタンスに、最近買収した組織の LDAP ディレクトリへの管理者認証情報を提供します。
B. 新しいユーザーを同期するには、現在の GCDS インスタンスに LDAP 同期ルールを追加します。
C. 買収した組織の LDAP から同期されたユーザーが停止されないように、除外ルールを設定します。
D. 別のサーバー上で実行される GCDS の追加インスタンスを設定し、取得した組織の同期を処理します。
E. GCDS の複数の LDAP バージョンにアップグレードします。
Answer: C,D (メーッセージを残す**)**
https://support.google.com/a/answer/7177266?hl=ja#zippy=%2Ccan-i-sync-gcds-from-multiple- ldap-directories GCDS は単一の LDAP ディレクトリからのみ同期できます。複数の LDAP ディレクトリがある場合は、LDAP サーバーのデータを 1 つのディレクトリに統合することをおすすめします。
停止/削除を防ぐための除外ルールを作成する際は、2 つの個別の GCDS インスタンスを実行する必要があります。

最新問題**: 90**
会社で Workspace Business Plus ライセンスを保有する従業員が、まもなく長期休暇に入ります。従業員は Google Workspace データにアクセスする必要はありませんが、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。休暇中の従業員の Workspace データを保護し、コストを最小限に抑える必要があります。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、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. 従業員のメールアドレスをコピーし、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 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、復帰時にアカウントを完全に復元できるように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策です。
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ソリューションである理由は次のとおりです。
B). アーカイブ ユーザー ライセンスを購入し、従業員に割り当てます。
Google Workspace では、アーカイブ ユーザー ライセンスをフル ユーザー ライセンスよりも大幅に低価格で提供しています。アカウントにアーカイブ ユーザー ライセンスを割り当てると、データ（Gmail、ドライブ、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 ライセンスをそのアカウントに簡単に再割り当てし、データ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リファレンス：Google Workspace 管理者向け公式ヘルプドキュメントの「アーカイブ ユーザー ライセンスについて」または類似のタイトル）では、アーカイブ ユーザー ライセンスの想定されるユースケースとして、このシナリオが明確に説明されています。コスト削減、データの保全、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）、そしてユーザーが復帰した際にフルライセンスへのシームレスな移行が実現されることが概説されています。
A). 管理コンソールでアカウントを停止します。
アカウントを停止すると、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は全額発生します。管理者は停止中のアカウントの一部のデータにアクセスできる場合がありますが、アーカイブユーザーライセンスのようなコスト削減効果はありません。また、停止期間と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されたライセンスがない場合、データが長期間保持され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リファレンス：Google Workspace 管理者向けヘルプドキュメント「ユーザーの停止または復元」では、アカウント停止の機能について説明しています。このドキュメントは、一時的なアクセスの取り消しに主眼を置いており、委任アクセスを可能にする長期的かつ費用対効果の高いデータ保護には焦点を当てていません。
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 ではユーザーデータをエクスポートできますが、Google Workspace と直接統合されていない別のアーカイブが作成されます。チームメンバーがこのエクスポートされたデータにアクセスできるようにするのは面倒で、元の Workspace 環境内でアクセスする場合ほどシームレスではありません。ユーザーライセンスを削除すると Google Workspace へのデータ保持が停止し、従業員の復帰時にアカウントを完全に復元するには

データの再インポートが必要になります。これは複雑で時間がかかり、データの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が犠牲になります。
関連する Google Workspace 管理者向けのトピック ガイドまたはドキュメント リファレンス: Google Takeout に関するドキュメントでは、一時的なデータ保存や Workspace 環境内での共同アクセスではなく、主に個人的な使用やデータ移行のために 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。
ライセンスを削除すると、代替ライセンス (アーカイブ ユーザー ライセンスなど) が設定されていない限り、通常は一定期間後にデータが削除されます。
D）従業員のメールアドレスをコピーし、ファイルの所有権をチームメンバーに譲渡します。ユーザーアカウントを削除します。
このアプローチには、大幅なデータ操作とコンテキストの損失が伴います。メールをコピーすると、メールボックスの構造全体が維持されない可能性があり、重要な情報が失われる可能性があります。ファイルの所有権の移行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カバー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、データが永久に削除され、従業員が復帰した際に完全な復元が不可能になります。このオプションは、従業員のWorkspaceデータを保持し、後でアカウントを復元する場合には適していません。
関連する Google Workspace 管理者向けのトピック ガイドまたはドキュメント参照: Google Workspace のアカウント管理のベスト プラクティスでは、復職する従業員のユーザー アカウントとデータを保持することに重点が置かれています。
データの回復とアカウントの再作成に伴う困難とリスクのため、一時的な休止を目的としてアカウントを削除することは強くお勧めしません。
したがって、データの保存、チーム メンバーへのアクセスの提供、休暇中のコストの最小化、復帰時の完全な復元を可能にするというすべての要件を満たす最も適切なアクションは、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ことです。

最新問題**: 91**
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活用して提案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、事前に入力されたセクションを備え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。
B. Google ドライブに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、組織全体のデフォルトの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。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、事前入力済みのセクションを備えたドキュメントテンプレートを作成するには、Google Workspace テンプレートギャラリーを活用するのが最も効率的で一元管理しやすい方法です。この方法では、組織のブランディングを有効にし（基本テンプレートでは必須ではありませんが、組織テンプレートでは多くの場合、ブランディングが関連付けられています）、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します。
オプション C が正しい理由と、他のオプション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、組織全体のデフォルトの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（Google ドライブに保存されます）でテンプレートを作成し、Google 管理コンソールから組織のデフォルトの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（または特定の組織部門）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とデザインや操作性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 管理者向けトピックガイドまたはドキュメントリファレンス：公式の Google Workspace 管理者ヘルプドキュメントには、「組織用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について説明しています。以下のトピックが取り上げられています。組織のギャラリーへのテンプレートの送信：
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、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管理者に説明します。
組織単位: 多くの場合、テンプレートは特定の組織単位で利用できるようにすることができ、営業チームなどのさまざまなチームに合わせてカスタマイズされたテンプレートを作成できます。
A) Googleドライブでテンプレートを作成し、営業チームに編集権限を付与します。
営業チームにマスターテンプレートの編集権限を与えることは問題があります。元のテンプレートが意図せず、あるいは意図的に変更され、不整合が生じる可能性があり、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、ユーザーは作業用にテンプレートのコピーを作成し、元のテンプレートはそのまま残しておくべきです。
Google Workspace管理者向けトピックガイドまたはドキュメントリファレンス :Googleドライブでのファイル共有と共同作業に関するベストプラクティスでは、適切なレベルのアクセス権限の提供が重視されています。テンプレートの場合、通常、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が目的であり、元のドキュメントを編集することは目的ではありません。
B) Googleドライブにテンプレートを作成し、各営業担当者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。
このアプローチは非効率で管理が困難です。各営業担当者にテンプレートの個別のコピーを作成し、所有権を委譲するのは、管理者にとって時間のかかる作業です。さらに、テンプレートを更新する必要がある場合、個々のコピーを修正する必要があり、バージョン管理上の問題や営業チーム全体での不整合が生じます。
Google Workspace 管理者向けトピックガイドまたはドキュメントリファレンス :Googleドライブの共有機能とオーナーシップ機能は、ドキュメントの共同作業を目的として設計されており、このような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 ギャラリーを介した一元管理が推奨されます。
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。営業チームと共有しているドライブにPDFファイルをアップロードします。
テンプレートをPDF形式で保存すると、編集可能なテンプレートの目的が損なわれます。営業チームは、あらかじめ入力されたセクションを簡単に変更したり、提案の詳細を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、新しい編集可能なドキュメントの出発点となるものです。
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を目的として設計されています。テンプレートはこの編集可能なフォーマットの機能であり、ユーザーは事前に構造化されたドキュメントから始めて、後でカスタマイズすることができます。PDF は最終版であり、編集はできません。
したがって、正しいアプローチは、Google Workspace テンプレート ギャラリーを活用し、営業チームが提案テンプレートに効率的かつ一元管理された方法でアクセスして使用できるようにすることです。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: 92
組織内のユーザーから、社内の予定受信者にカレンダーの予定招待状が届か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ます。
B. イベント作成者のカレンダー サービスがオフになっているかどうかを確認します。
C. カレンダー イベントに 50 人を超えるゲスト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設定で新しいイベントの電子メール通知をオフにしているかどうかを確認します。
E. イベントの受信者がカレンダー設定で新しいイベントの電子メール通知をオフにしているかどうかを確認します。
Answer: D (メーッセージを残す)
Google カレンダーでは、新しいイベント、イベントの変更、リマインダーなどのメール通知を受信するかどうかなど、さまざまな通知設定をユーザーが構成できます。受信者が新しい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が届きません。
Google Workspace 管理者向けのトピックガイドまたはドキュメントの参照 :Google カレンダーの公式ヘルプドキュメント 」ユーザー向け） 「通知設定の変更」など）では、ユーザーが予定の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、新しい予定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できませんが、これらのユーザーレベルの制御を理解することは、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指示するとよいでしょう。
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ます。
Google カレンダーの営業時間は、主に会議のスケジュール提案と、ユーザーの空き状況が他のユーザーに表示される方法に影響します。ユーザーがイベントの招待状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係なく、新しいイベントのメール通知が送信され続け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例外的なケースを除きます。この点についてはここでは説明しません）。
Google Workspace 管理者向けトピック ガイドまたはドキュメント リファレンス: Google カレンダーのヘルプ ドキュメントの 勤務時間と場所を設定する」では、招待状の受信ではなく、空き時間やスケジュールに関連する営業時間の目的について説明しています。
B . イベント作成者のカレンダー サービスがオフになっているかどうかを確認します。

イベント作成者のカレンダーサービスがオフになっている場合、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と述べているように、ユーザーが招待状を作成して送信したため、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 管理者向けトピックガイドまたはドキュメントリファレンス :Google Workspace 管理者向けヘルプドキュメントの 「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」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。ユーザーが Google カレンダーを無効にしている場合、カレンダー機能は利用できません。
C . カレンダーイベントに 50 人を超えるゲストがいるかどうかを確認します。
カレンダーの1つの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、この制限を超えると、通常、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ますが、受信者が招待を受け取れないということではありません。たとえ受信に影響するような制限があったとしても（社内ユーザーにとって、妥当な範囲内ではあまり文書化されていない問題です）、最初に確認すべき事項ではありません。
関連する Google Workspace 管理者のトピック 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数の制限について記載されている場合がありますが、これらの制限は通常、ゲストの追加、更新の送信、返信の表示の機能に関係するものであり、組織内の一部の受信者への配信が完全に失敗するというものではありません。
したがって、内部の受信者がカレンダー イベントの招待を受信できない原因をトラブルシューティングする最も論理的な最初の手順は、受信者に自分のカレンダー通知設定をチェックしてもらい、新しいイベントの電子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状が届かないという報告があった場合、受信者側ですぐに調査すべき原因として最も可能性が高いのは、Googleカレンダー内の通知設定です。ユーザーは通知設定をカスタマイズできるため、新しいイベントの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 が最も関連性の高い最初のステップである理由と、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は次のとおりです。

最新問題**: 93**
会社のポリシーでは、従業員が退職したらマネージャーにドライブ データへのアクセス権を与えることが義務付けられています。
このアクセスをどのように許可すればよいでしょうか?
A. マネージャーを元従業員のアカウントの代理人にします。
B. 元従業員のマイドライブからマネージャーのマイドライブにデータをコピーします。

C. Google Workspace 管理コンソールのファイル転送オーナー権限ツールを使用して、すべてのドライブ データのオーナー権限を譲渡します。
D. ユーザーとしてログインし、すべてのドライブ ファイルの 所有者」権限を使用してファイル権限に管理者を追加します。
Answer: C (メッセージを残す**)**
* 管理コンソールにアクセス: Google Workspace 管理コンソールにログインします。
* 転送ツールに移動します。[アプリ] > [Google Workspace] > [ドライブとドキュメント] > [オーナー権限を譲渡] に移動します。
* 転送の開始: 元従業員とデータを受け取るマネージャーのメールアドレスを入力します。
* データを選択: すべてのドライブ データを管理者のアカウントに転送することを選択します。
* 移管の完了：移管を確定します。これにより、すべてのドライブデータの所有権が元従業員からマネージャーに移管され、マネージャーが必要な情報にアクセスできるようになります。
参考文献
* Google サポート: ドライブのファイルを新しいオーナーに譲渡する

最新問題**: 94**
組織では、Gmail を使用した新しいカスタマーサポートプロセスを導入しています。外部の顧客がカスタマーサポートチームにサポートリクエストメールを送信できる、費用対効果の高いソリューションを構築する必要があります。
リクエストはカスタマーサポート担当者間で均等に分配する必要があります。どうすればよいでしょうか？
A. Google グループを作成し、共同トレイの設定を有効にし、投稿権限を 「ウェブ上のすべてのユーザー」に設定して、カスタマー サポート エージェントをグループ メンバーとして追加します。
B. 顧客サポート グループを表す特定の電子メール アドレスに対して委任されたアクセスを使用し、その電子メール アドレスの代理人として顧客サポート チームを追加します。
C. Google グループを作成し、サポート エージェントをグループに追加して、投稿権限を 「公開」に設定します。
D. カスタマーサポートチーム用の受信トレイを設定します。カスタマーサポートチームにログイン資格情報を提供します。
Answer: A (メッセージを残す**)**
共同トレイ設定を備えたGoogleグループを使用すると、サポートリクエストメールをチーム内で均等に分配できます。投稿権限を 「ウェブ上の全員」に設定することで、外部の顧客がグループに直接メールを送信でき、メールはタスクとしてサポートエージェントに配信されます。これは費用対効果の高いソリューションであり、顧客からのサポートリクエストを体系的に管理・追跡する手段も提供します。

最新問題: **95**
組織内のユーザーから、職場では不適切な言葉を含むメッセージが届くという苦情が頻繁に寄せられています。管理者として、これらのメッセージがユーザーのメールボックスに届かないようにするには、どのような対策を講じるべきでしょうか？
A. 不快なコンテンツ ルールを構成します。
B. 添付ファイルのコンプライアンス ルールを構成します。
C. 光学文字認識 (OCR) を有効にします。
D. Gmail DLP ポリシーを設定します。
Answer: A (メーッセージを残す**)**
https://support.google.com/a/answer/1346936?hl=ja

最新問題: **96**
あなたの会社は世界中に多数の拠点を持っています。各拠点には複数のオフィスマネージャーがおり、従業員からの質問にメールエイリアスを通じて対応しています。しかし、オフィスマネージャーが回答していない質問もあります。Workspace を使用して、会話を複数の受付担当者に割り当てるシステムをどのように構築すればよいでしょうか？
A. Google グループの共同受信トレイを作成します。
B. App Script を使用して、会話の所有権をマークするチケット システムを設計します。
C. ServiceNow などのサードパーティ ソリューションと契約します。
D. Google タスクを作成し、受付担当者に割り当てて、未回答の質問に対処します。
Answer: A (メーッセージを残す**)**
管理コンソールにアクセスします。Google 管理コンソールにログインします。
グループを作成する：「グループ」に移動し、新しいグループを作成します。グループの種類として 「共同トレイ」を選択します。
グループ設定を構成する: グループに適切な権限を設定し、オフィス マネージャーが受付担当者に会話を割り当てることができるようにします。
メンバーの追加: オフィス マネージャーと受付担当者をグループに追加します。
トレーニングとドキュメント: 共同受信トレイを使用して会話を割り当て、管理する方法について、オフィス マネージャーと受付担当者にトレーニングとドキュメントを提供します。
監視と調整: 共同受信トレイの使用状況を定期的に監視し、質問がタイムリーに割り当てられ、対処されていることを確認し、必要に応じて調整します。
参照：
Google Workspace 管理者ヘルプ - 共同トレイの作成と使用
Google グループ ヘルプ - 共同トレイについて

最新問題: **97**
あなたの会社ではGoogle Workspace Business Standardを使用しています。会社には5つの会議室があり、すべてGoogle Workspaceのリソースとして登録されており、従業員が日

常的に会議を開催する際に利用しています。先週末にオフィスのレイアウトが変更され、会議室の1つが経営陣専用の会議室になりました。CEOは誰でもその部屋を予約できることに不満を抱いており、この部屋は経営陣とエグゼクティブアシスタント（EA）のみが使用するように要求しています。Googleカレンダー経由で他のユーザーが予約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. スーパー管理者として、部屋のカレンダーの共有設定を変更し、管理者と EA グループに制限します。
B. Google Workspace リソースから部屋を削除し、部屋のスケジュール用に管理者と EA のみと共有するスプレッドシートを使用することを提案します。
C. スーパー管理者として、「管理ルーム」という名前のグループ カレンダーを作成し、管理者と EA とのみ共有します。
D. 部屋のリソースを管理者と EA グループに移動して、管理者と EA グループだけが使用できるようにします。
Answer: A (メーッセージを残す**)**
アクセスルームカレンダー設定:
Google 管理コンソールに移動します。
[建物とリソース] > [リソースの管理] に移動します。
特定の会議室を見つけて選択します。
共有設定を変更する:
部屋のリソースをクリックして設定を開きます。
「共有設定」で、管理者と EA グループへのアクセスを制限します。
これらのグループのみが部屋を予約する権限を持っていることを確認します。
変更を保存:
更新された設定を保存して、新しい制限を適用します。
これにより、指定されたグループ メンバーだけが Google カレンダー経由で管理室を予約できるようになります。
参照
Google Workspace 管理者ヘルプ: 会議室の予約を管理する

最新問題**: 98**
組織の業務の性質上、ユーザーは悪意のあるメール添付ファイルの影響を受けやすい状況にあります。受信メールの添付ファイルをすべてスキャンするには、どのように実装すればよいでしょうか？
A. セキュリティ サンドボックス セクションで、対象 OU の添付ファイルの仮想実行を有効にします。
B. 信頼できない送信者からの暗号化された添付ファイルから保護するための安全ルールを構成します。
C. セキュリティ サンドボックス セクションで、組織全体に対して添付ファイルの仮想実行を有効にします。

D. 信頼できない送信者からのスクリプトを含む添付ファイルから保護するための安全ルールを構成します。
Answer: C (メーッセージを残す**)**

最新問題**: 99**
貴社は、規制が厳しく、離職率も非常に高い業界に属しています。新入社員のライセンスを再利用し、データ保持規制を遵守するため、特定の Google Workspace データを別のバックアップ環境に保存する必要があると判断しました。
このような状況ではデータをどのように保存すればよいでしょうか?
A. ルーティング ルールを使用して、オンプレミスの SMTP サーバーと Google Workspace にメールを二重配信します。
B. スクリプトを記述し、Google Workspace API を使用してユーザーデータにアクセスしてダウンロードします。
C. サードパーティ ツールを使用して、Google Workspace データの安全なバックアップを構成します。
D. Google Takeout を使用してアーカイブをローカルに保存するようにユーザーをトレーニングします。
Answer: C (メーッセージを残す**)**
サードパーティ製バックアップ ソリューションを評価する: Google Workspace 向けの安全なバックアップ ソリューションを提供するサードパーティ製ツールを特定します。例としては、Backupify、Spanning Backup、Afi.ai などがあります。
適切なツールを選択する: 組織のニーズとコンプライアンス要件に基づいて、堅牢なデータ保持、安全なストレージ、簡単な回復オプションを提供するツールを選択します。
バックアップ ソリューションをセットアップします。
アカウントの作成: 選択したサードパーティのバックアップ サービスにサインアップします。
バックアップ設定を構成する: Google Workspace アカウントをリンクし、データ保持ポリシーを満たすようにバックアップ設定を構成します。
バックアップのスケジュール: データが継続的にバックアップされるように、定期的なバックアップ スケジュールを設定します。
バックアップとリカバリのテスト: 初期バックアップを実行し、リカバリ プロセスをテストして、必要なときにデータを効率的に取得できることを確認します。
監視と保守: バックアップの状態を定期的に監視し、組織のデータ保持規制に準拠するようにシステムを保守します。
参照
Google Workspace 管理者ヘルプ - サードパーティのバックアップ ツールを選択する
Backupify - Google Workspace バックアップ

最新問題**: 100**

最近、あなたの組織は、複数のユーザーに影響を与えるフィッシング攻撃の標的となりました。フィッシング攻撃の全容を効率的に特定し、さらなる問題の発生を防ぐ必要があります。何をすべきでしょうか?
A. * 1 BigQuery 0Q9 Km b I メッセージがフィッシングとしてマークされました
* 2 すべての電子メール通信にトランスポート層セキュリティ (TLS) を要求する
* 3 すべてのユーザーにパスワードをリセットするよう指示する
B. * 1 メールログ検索を使用して、過去3日間のすべてのメールを取得します。
* 2 よく受信したメールのログを分析し、ユーザーに連絡します。
* 3 悪意のあるメールアドレスをブロックするためのGmailフィルタの作成方法をユーザーに指示する
C. * 1 セキュリティダッシュボードを使用して、なりすましの可能性があるメッセージの数を確認し、影響を受けたユーザーに対して調査ツールを使用して悪意のあるメールを削除します。
* 2 高度なフィッシングおよびマルウェア対策を有効にする
* 3 ChromeにGoogleのパスワードアラート拡張機能を導入する
D. * 1 ユーザーから転送されたフィッシングサンプルを収集する
* 2 IPアドレスとメールアドレスをブラックリストに追加する
* 3. 影響を受けるユーザーのみを多要素認証 (MFA) に登録する
Answer: (解答を表示する**)**
セキュリティ ダッシュボードを使用する:
Google 管理コンソールにアクセスし、[セキュリティ] > [ダッシュボード] に移動します。
フィッシングやスプーフィング活動に関する指標とログを確認します。
影響を受けるユーザーと潜在的な脅威を特定します。
調査ツールを使用する:
セキュリティ ダッシュボードから調査ツールにアクセスします。
影響を受けるユーザーに送信された悪意のある電子メールを検索して隔離します。
これらのメールを削除する措置を講じてください。
高度な保護を有効にする:
管理コンソールで、[アプリ] > [Google Workspace] > [Gmail] > [セーフティ] に移動します。
高度なフィッシングおよびマルウェア対策機能を有効にします。
パスワードアラート拡張機能を展開する:
パスワード侵害の検出に役立つように、パスワード アラート Chrome 拡張機能が組織全体に展開されていることを確認します。
参照 :
Google Workspace 管理者ヘルプ: セキュリティ ダッシュボード
Google Workspace 管理者ヘルプ: 調査ツール
Google Workspace 管理者ヘルプ: フィッシングとマルウェア対策
Google Workspace 管理者ヘルプ: パスワード アラートを導入する

最新問題: **101**
訴訟チームが実施している調査への協力を依頼されました。現在、メールのデフォルトの保存期間は180日で、カスタムメール保存ポリシーは設定されていません。訴訟チームは調査の中心人物を特定し、このユーザーに関連するメールデータをユーザーに知られずに調査したいと考えています。どのような2つの対応を取るべきですか？ 2つ選択してください。）
A. ユーザーのデータをセカンダリ アカウントにコピーします。
B. ユーザーのパスワードをリセットし、新しいパスワードを訴訟チームと共有します。
C. Google Vault でユーザーのメールボックスに記録保持を作成します。
D. Google Vault を使用して案件を作成し、訴訟チームのメンバーと共有します。
E. ユーザーを独自の組織単位に移動し、カスタム保持ポリシーを設定します。
Answer: (解答を表示する**)**

最新問題: **102**
最近、組織内でスパムとしてマークされたメッセージが増加しています。各メッセージに関する詳細情報を迅速かつ効率的に取得する必要があります。どうすればよいでしょうか?
A. SQL クエリを使用して、BigQuery にエクスポートされたすべてのスパム監査ログを検索し、調査を作成します。
B. すべてのユーザーにアラートを送信し、疑わしいGmailメッセージをスパムとしてマークし、アラートセンターのメッセージを確認します。
C. Google Vault を使用して、スパムとしてマークされたすべてのメッセージを法的記録保持の対象とし、メッセージを確認します。
D. セキュリティ ダッシュボードのスパム フィルタ レポートを使用して、特定の期間に Google のスパム フィルタによってスパムとしてマークされたメッセージを確認します。
Answer: D (メーッセージを残す**)**
セキュリティ ダッシュボードにアクセスする: Google 管理コンソールに移動し、 セキュリティ」セクションに移動します。
スパム フィルター レポートを開く: セキュリティ ダッシュボードで、スパム フィルター レポートを開きます。
期間によるフィルタリング: 分析する特定の期間を選択します。
スパム メッセージを確認する: Google のスパム フィルタによってスパムとしてマークされた各メッセージに関する詳細情報を確認します。
必要なアクションを実行する: レポートの情報を使用して、スパム フィルターやユーザー アラートを調整したり、スパムをより効果的に管理するために必要なその他のアクションを実行したりします。
参照
セキュリティダッシュボード
メールログ検索

最新問題: **103**
貴社は訴訟に巻き込まれており、法務部門は特定の2名のユーザーのすべてのメールの開示と保管を依頼されています。さらに、「秘密プロジェクト123」に言及するすべてのメールの開示と保管も依頼されています。この依頼に応えるには、どのような手順を踏むべきでしょうか？
A. 案件と保留を作成します。保留をGmailに設定し、最上位の組織に設定し、検索語を「secret project 123」に設定します。2つ目の保留を作成します。2つ目の保留をGmailに設定し、アカウントに設定し、user1@your-company.com、user2@your-company.comと入力します。保存します。
B. 案件と保留を作成します。保留をGmailに設定し、アカウントに設定し、ユーザー名をuser1@your-company.com、user2@your-companyに設定します。検索キーワードを(secret project 123)に設定します。保存します。
C. 案件と保留を作成します。保留をGmailに設定し、アカウントを設定し、「user1@your-company.com AND user2@your-company.com」と入力します。検索語句を「secret AND project AND 123」に設定します。保存します。
D. 案件と保留を作成します。保留をGmailに設定し、アカウントに設定し、ユーザー名をuser1@your-company.com、user2@your-companyに設定します。検索キーワードをsecretまたはprojectまたは123に設定します。保存します。
Answer: (解答を表示する**)**
案件を作成: Google Vault にアクセスし、訴訟に関する新しい案件を作成します。案件は、訴訟記録保持（リティゲーションホールド）や検索の管理に使用されます。
保留の作成: 案件内で新しい保留を作成します。
保留範囲を設定する: メールを検出して保留することが要件であるため、保留範囲を Gmail に設定します。
アカウントの指定 :ユーザー名をuser1@your-company.comとuser2@your-company.comに設定します。これにより、これらのユーザーのすべてのメールが保持されます。
検索語の設定: 「secret project 123」という検索語を使用して、この特定の語句を含むすべてのメールを保留します。これは、「Secret Project 123」を含むすべてのメールを対象とする広範な検索です。保留の保存: 指定したユーザーと検索語句に関連するすべてのメールを確実に取得するために、保留を保存します。
参照
Google サポート: 保留を作成または更新する

最新問題: **104**
ワークスペース管理者として、会社所有のコンピューターとモバイルデバイスのインベントリを管理し、デバイスの種類や割り当て先などの詳細情報を追跡したいと考えています。デバイスを会社所有のインベントリに追加するにはどうすればよいでしょうか？

A. 管理パネルから会社所有の在庫テンプレートの CSV ファイルをダウンロードし、デバイスのシリアル番号を入力して、管理パネルの会社所有の在庫にアップロードし直します。
B. 管理パネルから会社所有の在庫テンプレートの CSV ファイルをダウンロードし、デバイスの OS とシリアル番号を入力して、管理パネルの会社所有の在庫にアップロードします。
C. 管理パネルから会社所有のインベントリ テンプレートの CSV ファイルをダウンロードし、デバイスの資産タグを入力して、管理パネルの会社所有のインベントリにアップロードします。
D. 管理パネルから会社所有の在庫テンプレートの CSV ファイルをダウンロードし、デバイスの OS、資産タグを入力して、管理パネルの会社所有の在庫にアップロードします。
Answer: A (メーッセージを残す**)**
https://support.google.com/a/answer/7129612?hl=ja&fl=1

最新問題**: 105**
人事部から、あるユーザーが解雇され、アカウントが停止されたという連絡を受けました。当該ユーザーは現在、法務調査の対象となっており、人事部はユーザーのメールデータを引き続き保留にするよう求めています。解雇されたユーザーのチームは、当該ユーザーが所有するファイルを使用する重要なプロジェクトに積極的に取り組んでいます。新しいユーザーにライセンスをプロビジョニングする前に、解雇されたユーザーのコンテンツが適切に保管されていることを確認する必要があります。
どのような 2 つのアクションを取る必要がありますか? (2 つ選択してください。)
A. ユーザーの電子メールデータに対する法的保留を拡張します。
B. プロジェクト ファイルをチームドライブに移動する、または所有権を譲渡します。
C. 来週からアカウントの名前を新しいユーザーに変更します。
D. アカウントを削除して、Google Workspace ライセンスを解放します。
E. 終了したユーザー アカウントにアーカイブ ユーザー ライセンスを割り当てます。
Answer: B,E (メーッセージを残す**)**
https://support.google.com/a/answer/9048836

最新問題**: 106**
組織では、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を遵守していることを確認したいと考えています。社内で使用されるChromeブラウザを、最も低コストのソリューションで管理 制御する必要があります。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 ブラウザを管理します。
B. すべての従業員のデバイスをリモートでワイプし、最新の Chrome ブラウザ バージョンが使用されていることを確認します。

C. 組織のドメインに Chrome ブラウザを登録し、Chrome ブラウザ ポリシーを適用します。
D. 潜在的なセキュリティ リスクを防ぐために、従業員の Chrome ブラウザのすべての拡張機能を無効にします。
Answer: C (メーッセージを残す**)**
Google Workspace（特にChrome Enterprise Coreは、Google Workspaceの各エディションに同梱または無料で提供されることが多い）には、組織全体のChromeブラウザを管理するための機能が組み込まれています。ドメインにChromeブラウザを登録すると、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。これはファーストパーティのクラウドベースのソリューションであり、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がかからないため、「最も安価なソリューション」となっています。他の選択肢がChromeブラウザを最も低コストで管理するのに適していない理由は次のとおりです。
* A. Chromeブラウザの管理にはサードパーティ製のソフトウェア導入ソリューションを使用します。これは可能ですが、サードパーティ製ソフトウェア、そのライセンス、そして場合によってはメンテナンス費用が追加される可能性があります。Google Workspaceはネイティブのブラウザ管理機能を提供しているため、サードパーティ製のソリューションは最適ではありません。
「最も安い。」
* B. 従業員の全デバイスをリモートワイプし、Chromeブラウザの最新バージョンを使用していることを確認します。デバイスのリモートワイプは、紛失・盗難時やオフボーディング時に通常使用される、抜本的で混乱を招く対策です。ブラウザのバージョン管理や設定の適用には、標準的な方法ではなく、適切な方法ではありません。また、生産性の低下やIT部門の負担という点でも、非常に大きなコストがかかります。
* D. 潜在的なセキュリティリスクを防ぐために、従業員の Chrome ブラウザのすべての拡張機能を無効にします。
拡張機能を無効にすると、ある程度のリスクを軽減できますが、正当かつ必要な拡張機能が無効にされると、範囲が広すぎて混乱を招く可能性があり、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、これは適用可能なポリシーの一つに過ぎず、ブラウザを一元的にコスト効率よく管理する方法ではないということです。Chromeブラウザポリシーでは、特定の拡張機能の許可/ブロックなど、きめ細かな制御が可能です。
Google Workspace 管理者からの参照:
* ユーザーまたはブラウザの Chrome ポリシーを設定する :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。
参考資料 :Chrome Enterprise および Education ヘルプ :ユーザーまたはブラウザの Chrome ポリシーを設定する Chrome Enterprise Core :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について説明しています。これらの機能は多くの場

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作成を 0 ドルで」利用できることが明記されています。
参考: Chrome Enterprise ウェブサイト: Chrome Enterprise - ビジネス向けの信頼できるエンタープライズ ブラウザ (Chrome Enterprise Core の機能と価格について説明しているセクションをご覧ください)。
Google Workspace での Google Chrome 管理の最大化: この記事では、「Google Chrome 管理の基本ポリシーは Google Workspace で無料で利用できる」という点がさらに強調されています。参考: itGenius ブログ: Google Workspace での Google Chrome 管理の最大化
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管理でき、「最も安価なソリューション」という要件に適合します。

最新問題**: 107**
Your-company.com の財務部門は、スプレッドシートからデータを読み取る社内アプリケーションを作成したいと考えています。コラボレーションエンジニアであるあなたは、App Maker の使用を提案しました。財務チームは、App Maker でアプリケーションを作成する際のデータセキュリティを懸念しています。
データを保護するためにどのようなセキュリティ対策を実施する必要がありますか?
A. レコードおよびデータ関係に対する操作には、ロール、スクリプト、および所有者のアクセス権限を使用します。
B. 財務部門の組織単位に対してのみ App Maker アクセスを有効にします。
C. 各データ ソースにアクセスするには、権限が制限されたサービス アカウントを使用します。
D. 所有者のアクセス権限を変更して、内部使用のみを許可します。
Answer: A (メーッセージを残す**)**
* App Maker でアプリケーションを開発するときに、ユーザーが必要とするさまざまなアクセス レベルに対応するロールを定義します。
* スクリプトを使用して、ユーザーの役割に基づいてデータへのアクセスを制御します。これにより、許可されたユーザーのみが特定の操作を実行できるようになります。

* 所有者のアクセス権限を適切に設定し、必要な権限を持つユーザーのみがデータにアクセスまたは変更できるようにします。
* 組織やアプリケーションの使用状況の変更に適応するために、役割と権限を定期的に確認して更新します。
これらのセキュリティ対策を実装することで、内部アプリケーション内のデータが安全にアクセスおよび管理されるようになり、不正アクセスに関連するリスクが軽減されます。
参考文献:
* Google Workspace 管理者ヘルプ - App Maker のセキュリティ

最新問題**: 108**
不満を持った従業員が会社を辞め、Google ドライブにあるすべてのメール メッセージとファイルを削除しました。
セキュリティ チームは、一部の知的財産が公的なソーシャル メディア サイトに公開された可能性があることを認識しています。
この漏洩に関する調査を開始するための最初のステップは何ですか?
A. 管理コンソールでユーザーのアカウントを削除します。
B. エンドユーザーの Workspace アカウント間でデータを転送します。
C. Google Vault 管理者に案件を作成するよう指示し、すべてのユーザーデータを「保留」状態にします。
D. Google Vault を使用してすべてのユーザー データをエクスポートし、セキュリティ チーム間で共有します。
Answer: C (メーッセージを残す**)**
* Google Vault にアクセスする: Vault 管理者は Google Vault にログインする必要があります。
* 新しい案件を作成する: Google Vault で、不満を抱えた従業員に関連するこの調査専用の新しい案件を作成します。
* データを保留にする :ユーザーのすべてのメールとドライブデータを保留状態にし、データの保存を確実にします。これにより、データが完全に削除または変更されるのを防ぎます。
* データの検索: Google Vault の検索機能を使用して、漏洩に関連する可能性のあるメールやドキュメントを見つけます。
* 必要に応じてデータをエクスポートする: 必要に応じて、保存したデータをエクスポートし、セキュリティ チームによるさらなる分析とレビューを行います。
* セキュリティ チームとの連携: 調査結果をセキュリティ チームと共有し、データ漏洩の調査に役立てます。
参考文献:
* Google Vault ヘルプ - 案件の作成と管理
* Google Vault ヘルプ - データを保留にする

最新問題: **109**
セキュリティ担当者がセキュリティヘルスチェックを実施した結果、 提供元不明のモバイルアプリケーションのインストール」が発生しているというアラートを発見しました。セキュリティ担当者から、このアラートの発生を防ぐ方法を見つけるよう依頼されました。モバイル デバイス管理 (MDM) を使用して、不明なソースからのモバイル アプリケーションのインストールを許可しないポリシーを構成する必要があります。
この要件を満たすにはどのような MDM 構成が必要ですか?
A. アプリケーション管理メニューで、Android および iOS デバイスにインストールを許可するアプリのホワイトリストを構成します。
B. アプリケーション管理メニューで、Android、iOS デバイス、および Active Sync デバイスがインストールできるアプリのホワイトリストを構成します。
C. Android の設定で、 Play ストア以外の提供元不明のアプリのインストールを許可する」のチェックがオフになっていることを確認します。
D. デバイス管理 > セットアップ > デバイス承認メニューで、 管理者の承認が必要」オプションを設定します。
Answer: C (メーッセージを残す**)**
参考: https://support.google.com/a/answer/7491893?hl=en

最新問題: **110**
あなたの会社の Google Workspace のプライマリ ドメインは mycompany.com」です。この会社は、 mystartup.com」というドメインを持つ別のクラウド プロバイダを使用しているスタートアップ企業を買収しました。このスタートアップ企業の全従業員の現在のメールアドレスはそのままに、Google Workspace ドメインに追加する予定です。スタートアップ企業の CEO のメールアドレスは andrea@mystartup.com で、これはあなたの会社の CEO のメールアドレス andrea@mycompany.com と一致しています（両者は別人です）。各従業員は自分のメールアドレスを引き続き使用する必要があります。さらに、上司から、新しい従業員に対して既存のセキュリティ ポリシーをすべて重複なく適用するよう指示されました。移行を実施するにはどうすればよいでしょうか？
A. mystartup.com」で新しい Google Workspace ドメインを作成し、両方のドメイン間に信頼関係を作成して、同じセキュリティ ポリシーを再利用し、社内で従業員情報を共有します。
B. mycompany.com」ドメインにスタートアップの従業員を作成し、ユーザー名の末尾に重複する数字を追加します。Gmail > ルーティングで、スタートアップの従業員を対象とするOUに特定のルートを定義します。これにより、メールアドレスのドメインが次のように変更されます。
mystartup.com」に変更し、以前に追加された数字を削除してください。また、SPFレコードとDKIMレコードが正しく設定されていることを確認してください。

C. 既存の Google Workspace ドメインにエイリアス ドメイン mystartup.com を作成し、必要な DNS レコードを設定し、エイリアス ドメインをプライマリ メール アドレスとして持つスタートアップ企業の従業員全員を作成します。
D. 現在の Google Workspace ドメイン内にセカンダリ ドメイン mystartup.com を作成し、必要な DNS レコードを設定し、セカンダリ ドメインをプライマリ メール アドレスとしてすべてのスタートアップ従業員に作成します。
Answer: (解答を表示する**)**

最新問題**: 111**
Alice というユーザーが組織を離れることになりました。Alice のすべてのデータを、できるだけシンプルかつ効率的な方法で Bob のドライブに転送する必要があります。どうすればよいでしょうか。
A. Google 管理コンソールを使用して、アリスのドライブからボブのドライブにファイルを移動します。
B. Google Takeout サービスを使用して Alice のデータを zip ファイルにエクスポートし、Bob にその zip ファイルをドライブにインポートするように指示します。
C. Google Drive API を使用して、Alice のドライブから Bob のドライブにファイルをプログラムで転送します。
D. アリスに、自分のドライブからすべてのファイルをダウンロードし、ボブのドライブにアップロードするように指示します。
Answer: (解答を表示する**)**
最もシンプルかつ効率的な方法で Alice のすべてのデータを Alice のドライブから Bob のドライブに転送するには、次の手順に従います。
Google 管理コンソールにログインします。特権管理者権限を持つアカウントを使用します。
データ転送ツールに移動します。
[アプリ] > [Google Workspace] > [ドライブとドキュメント] に移動します。
「所有権の譲渡」をクリックします。
転送を開始します:
現在の所有者として Alice のメール アドレスを入力します。
新しい所有者として Bob の電子メール アドレスを入力します。
すべてのファイルとフォルダを Alice のドライブから Bob のドライブに転送するオプションを選択します。
「ファイルを転送」をクリックしてプロセスを開始します。
転送を確認します:
転送が完了したら、すべてのファイルとフォルダが Bob の所有になり、Bob のドライブでアクセスできるようになっていることを確認します。
参照：
Google Workspace 管理者ヘルプ - ドライブのファイルを転送する

Valid Google-Workspace-Administrator Dumps shared by GoShiken.com for Helping Passing Google-Workspace-Administrator Exam! GoShiken.com now offer the **newest Google-Workspace-Administrator exam dumps**, the GoShiken.com Google-Workspace-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com Google-Workspace-Administrator dumps with Test Engine here: https://www.goshiken.com/Google/Google-Workspace-Administrator-mondaishu.html (**103** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)