Google for Education

Google Workspace for Education 有料エディションを活用するための 40 以上の方法

goo.gle/use-edu-workspace

この資料の使用方法

この資料では、Google Workspace for Education の**有料エディションをご利用のお客様に参考にしていただける代表的なユースケースをご紹介します。ここに記載されているツールを活用すれば、データ セキュリティの強化、教師による指導の効率と生徒の参加意欲の向上、学校全体のコラボレーション**　の改善などを実現できます。

この資料には、**機能別**に**一般的なユースケース**とわかりやすい**使用手順**が記載されています。資料全体をお読みになり、Google Workspace for Education の有料エディションのさまざまな活用方法をご確認いただければ幸いです。

Google Workspace for Education 有料エディション

Google Workspace for Education の 3 種類の有料エディションにより、
組織のニーズを満たすための選択肢が増え、管理性と柔軟性が向上

Google Workspace for Education Plus

Education Standard、Teaching and Learning Upgrade に加え、Plus 独自機能を追加

Education Plus は、**オールインワン**の EdTech ソリューションで生徒、教師、教育機関のリーダー/IT 管理者を支援し、
高度なセキュリティとモニタリング、充実した教育と学習 を実現する使いやすいツールを提供

Google Workspace for Education Standard

高度なセキュリティおよびモニタリング ツール で学習環境の可視性と管理性を高め、リスクと脅威を緩和

Teaching and Learning Upgrade

充実した教育・学習用ツール を活用し、あらゆる場所で生徒一人ひとりに合った効果的な学びを提供できるため、教育の質が向上

目次

セキュリティとモニタリング用の高度な機能

セキュリティ ダッシュボード

- 大量の迷惑メール
- 外部とのファイル共有
- サードパーティ製アプリケーション
- フィッシング攻撃

セキュリティの状況ページ

- おすすめのセキュリティ対策
- リスクの高い領域に関する推奨事項

調査ツール

- 共有されている不適切なコンテンツ
- 誤って共有されているファイル
- フィッシング メールとマルウェア メール
- 悪意のある人物による不正行為の阻止
- 詳しいセキュリティ分析情報
- 主催者不在の会議の防止

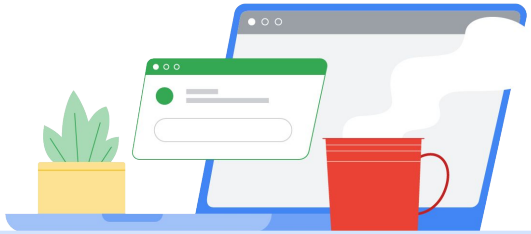
ドメインの管理、制御

- Gmailの添付ファイルをスキャンして脅威を検知
- 使用状況に関するダッシュボードやレポートの作成
- ファイル検索の容易化
- 内部ドキュメントの整理
- 部門グループへの自動編入
- 内部ファイル共有に関する監査の作成
- ファイル共有の制限
- Workspace アプリの制限
- ストレージの管理
- データの規制
- 許可に関する規制
- エンドポイント デバイスの管理
- Windows デバイスの管理
- Windows デバイスのカスタム設定
- Windows デバイス アップデートの自動化
- クライアントサイド暗号化の活用

目次

セキュリティとモニタリング用の高度な機能

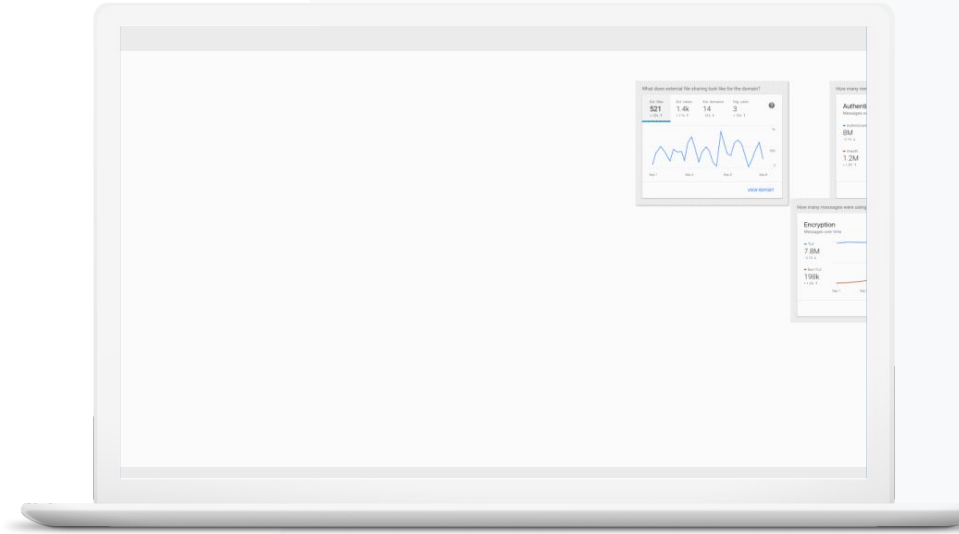
脅威からの防御、セキュリティ インシデントの分析、生徒と教職員のデータの保護に役立つ予防的なセキュリティ ツールを使用して、
ドメイン全体をより細かく管理



セキュリティ ダッシュボード

概要

セキュリティ ダッシュボードを使用すると、さまざまなセキュリティ レポートの概要を確認できます。セキュリティ レポートの各パネルには、デフォルトで過去 7 日間のデータが表示されます。今日、昨日、今週、先週、今月、先月、さかのぼる日数（180 日まで）を指定して、ダッシュボードに表示されるデータをカスタマイズできます。



ユースケース

大量の迷惑メール	詳細な手順
外部とのファイル共有	詳細な手順
サードパーティ製アプリケーション	詳細な手順
フィッシング攻撃	詳細な手順

「過剰なメールや不要なメールの受信を制御し、本校のセキュリティ上の脅威を減らす必要があります。」

大量の迷惑メール

セキュリティ ダッシュボードでは、Google Workspace for Education 環境における次のようなアクティビティを視覚的に確認できる

- 迷惑メール
- 不審な添付ファイル
- フィッシング
- その他
- マルウェア

詳細な手順

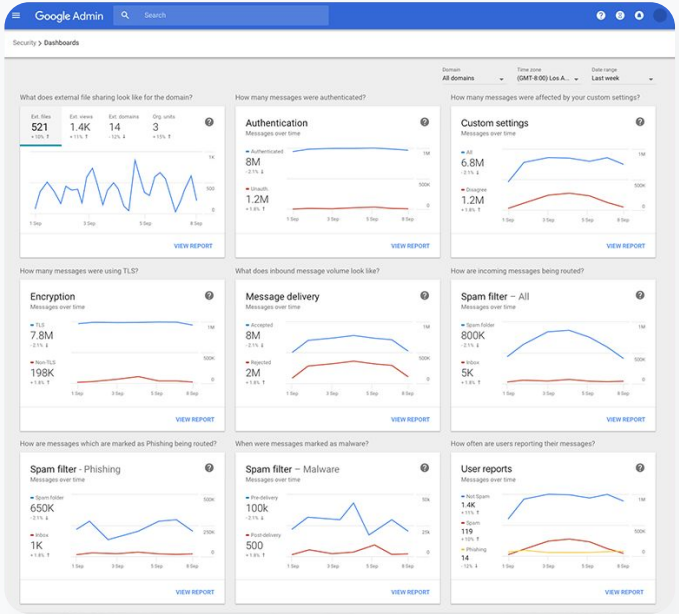
ヘルプセンターの関連記事

- セキュリティ ダッシュボードについて

手順: ダッシュボードの概要

セキュリティ ダッシュボードを表示する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**ダッシュボード**] をクリック
- セキュリティダッシュボードではデータの詳細な調査、Google スプレッドシートまたはサードパーティ製ツールへのエクスポート、調査ツールによる調査の開始が可能



ヘルプセンターの関連記事

- セキュリティ ダッシュボードについて

「機密データが第三者と共有されるのを防ぐために、外部とのファイル共有の状況を確認する必要があります。」

外部とのファイル共有

セキュリティ ダッシュボードのファイルの公開レポートを使用して、
ドメインにおける外部とのファイル共有に関する次のような指標を確認できる

- 指定した期間における、ドメイン外のユーザーとの共有イベント数
- 指定した期間に外部から受信したファイルの表示回数

詳細な手順

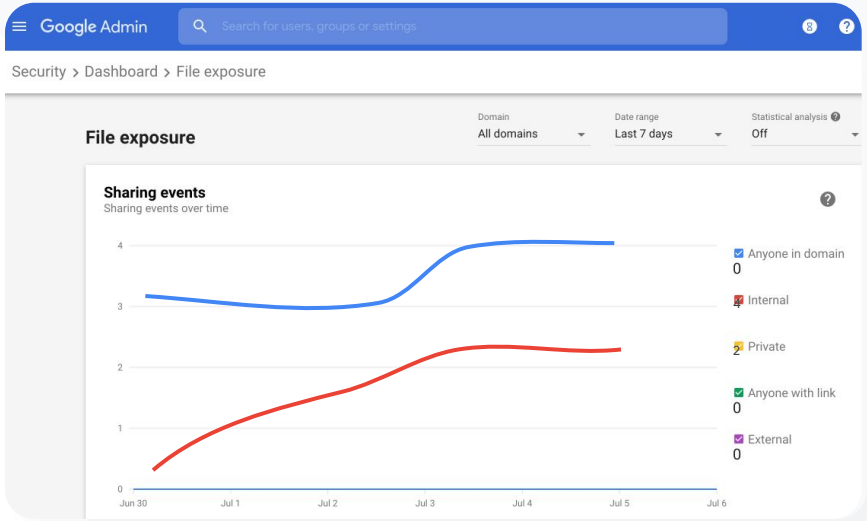
ヘルプセンターの関連記事

- セキュリティの状況ページを使ってみる

手順: 外部とのファイル共有

ファイルの公開レポートを表示する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**ダッシュボード**] をクリック
- [**ドメインの外部とのファイル共有の状況**] パネルの右下にある [**レポートを表示**] をクリック



ヘルプセンターの関連記事

- セキュリティ ダッシュボードについて
- ファイルの公開レポート

「ドメインのデータにアクセスできるサードパーティ製アプリケーションを確認する必要があります。」

サードパーティ製アプリケーション

セキュリティ ダッシュボードの OAuth 権限付与アクティビティ レポートを使用して、ドメインに接続しているサードパーティ製アプリケーションと、それらがアクセスできるデータを監視できる

- OAuth は、パスワードを開示することなく、ユーザーのアカウント情報へのアクセス権をサードパーティのサービスに付与する。アクセス権を付与するサードパーティ製アプリは限定することを推奨
- [OAuth 権限付与アクティビティ] パネルを使用して、権限付与アクティビティをアプリ別、範囲別、またはユーザー別に監視し、権限を更新できる

詳細な手順

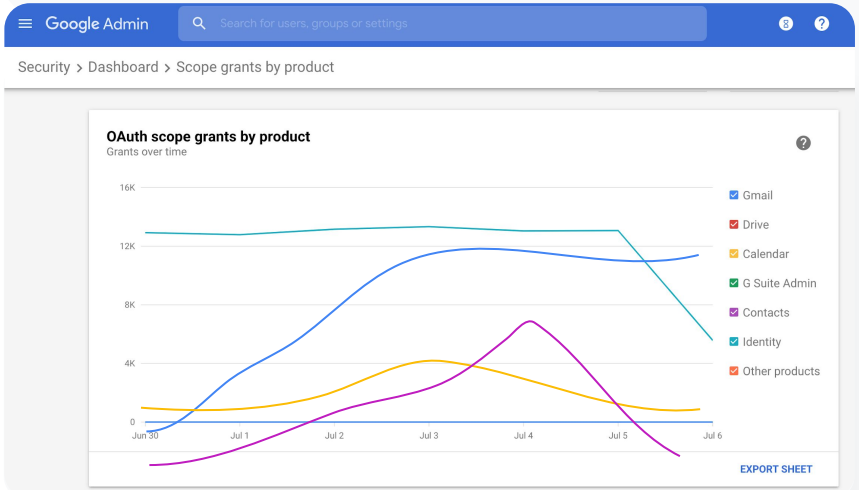
ヘルプセンターの関連記事

- OAuth 権限付与アクティビティ レポート

手順：サードパーティ製アプリケーション

OAuth 権限付与アクティビティ レポートを表示する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**ダッシュボード**] をクリック
- 下部にある [**レポートを表示**] をクリック
- OAuth 権限付与アクティビティがプロダクト（アプリ）別、範囲別、ユーザー別に表示される
- 情報をフィルタするには、[**アプリ**]、[**範囲**]、[**ユーザー**] をクリック
- スプレッドシートのレポートを生成するには [**シートをエクスポート**] をクリック



ヘルプセンターの関連記事

- OAuth 権限付与アクティビティ レポート

「フィッシング攻撃を受けたという報告がありました。フィッシング メールを受信した日時、メールの正確な内容、それがもたらすリスクを確認する必要があります。」

フィッシング攻撃

セキュリティ ダッシュボードの [ユーザー レポート] パネルでは、特定の期間にフィッシングまたは迷惑メールに分類されたメールを確認できる。フィッシングに分類されたメールについては、受信者や既読状況などの情報も確認可能

- ユーザー レポートでは、ユーザーが特定の期間に行ったマーク付けの操作（迷惑メール、迷惑メールではない、フィッシング）を確認できる
- 特定の種類のメール（内部に送信されたメール、外部に送信されたメール、特定の期間に送信されたメールなど）に関する情報のみが表示されるように、グラフをカスタマイズできる

詳細な手順

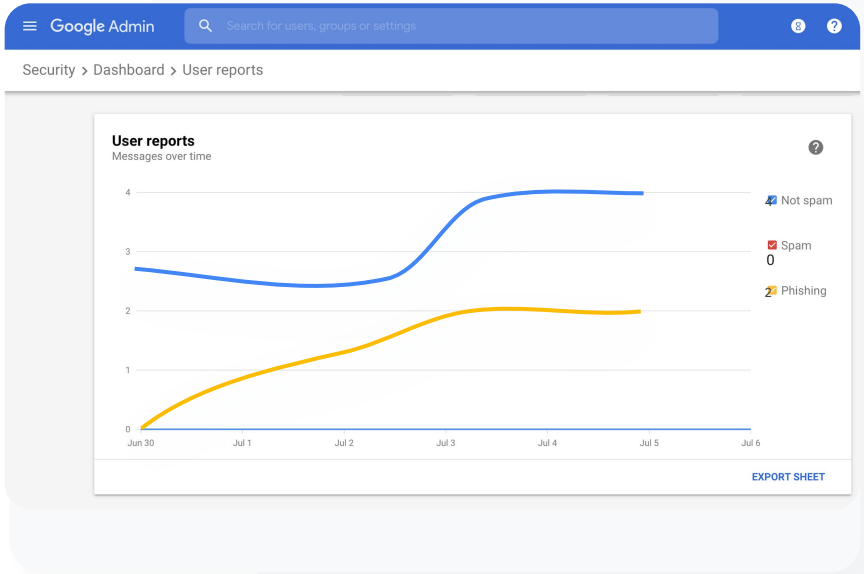
ヘルプセンターの関連記事

- ユーザーによるメールのマーク付け状況
- ユーザー レポート

手順：フィッシング攻撃

ユーザー レポート パネルを表示する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**ダッシュボード**] をクリック
- [**ユーザー レポート**] パネルの右下にある[**レポートを表示**] をクリック



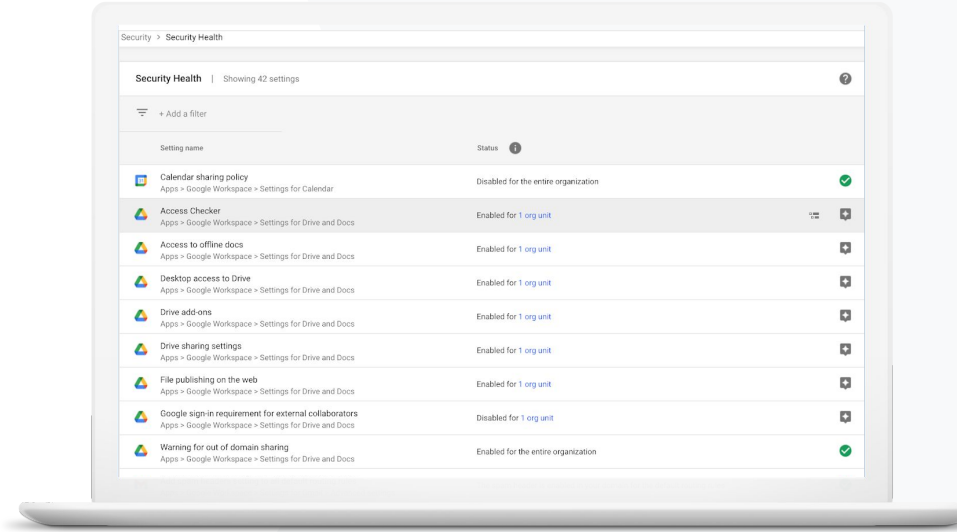
ヘルプセンターの関連記事

- セキュリティ ダッシュボードについて
- ファイルの公開レポート

セキュリティの状況

概要

セキュリティの状況ページで Google Workspace 環境のセキュリティ対策の概要を包括的に確認し、現在の設定を Google の推奨設定と比較することで、組織を予防的に保護できる



ユースケース

おすすめのセキュリティ対策 — 詳細な手順

リスクの高い領域に関する推奨事項 — 詳細な手順

「セキュリティポリシーのおすすめの設定方法や推奨事項を教えてください。」

おすすめのセキュリティ対策

セキュリティの状況ページを開くと、セキュリティ ポリシーに関する以下のようなおすすめの対策情報が得られる

- ドメイン内で潜在的なリスクがある領域に関する推奨事項
- セキュリティ効果を高めるための最適な設定に関する推奨事項
- 設定に直接移動するリンク
- 詳細情報とサポート記事

詳細な手順

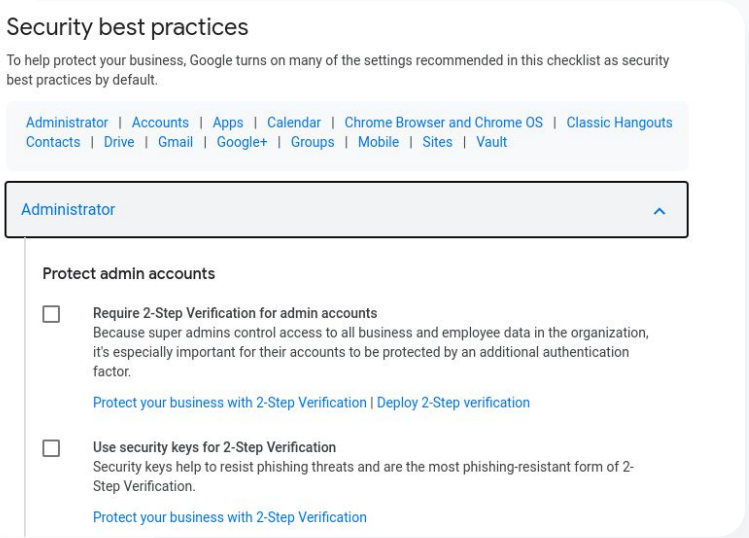
ヘルプセンターの関連記事

- セキュリティの状況ページを使ってみる

手順: セキュリティに関するベストプラクティス チェックリスト

組織を保護するため、このチェックリストに記載されている設定の多くは、おすすめのセキュリティ対策としてデフォルトで有効になっている。以下の設定については特に慎重に確認することを推奨

- **管理者:** 管理者アカウントを保護する
- **アカウント:** アカウントの不正使用を防止する、不正使用されたアカウントを保護する
- **アプリ:** サードパーティ製アプリによるコアサービスへのアクセスを見直す
- **カレンダー:** 外部カレンダーの共有を制限する
- **ドライブ:** ドメイン外での共有と共同編集を制限する
- **Gmail:** 認証とインフラストラクチャを設定する
- **Vault:** Vault アカウントを管理、監査、保護する



ヘルプセンターの関連記事

- セキュリティ設定の状況を確認する

「ドメインのセキュリティ設定の状況と、潜在的なリスクに対応するための具体的な提案を確認する手段が必要です。」

リスクの高い領域に関する推奨事項

セキュリティの状況ページでは現在のセキュリティ設定が確認され、変更が推奨される領域にマークが付いている。セキュリティの状況ページを使用すると以下のことが可能

- ドメイン内で潜在的にリスクがある領域を速やかに特定する
- セキュリティ効果を高めるための最適な設定に関する推奨事項を得る
- 推奨事項に関する詳細情報とサポート記事を参照する

詳細な手順

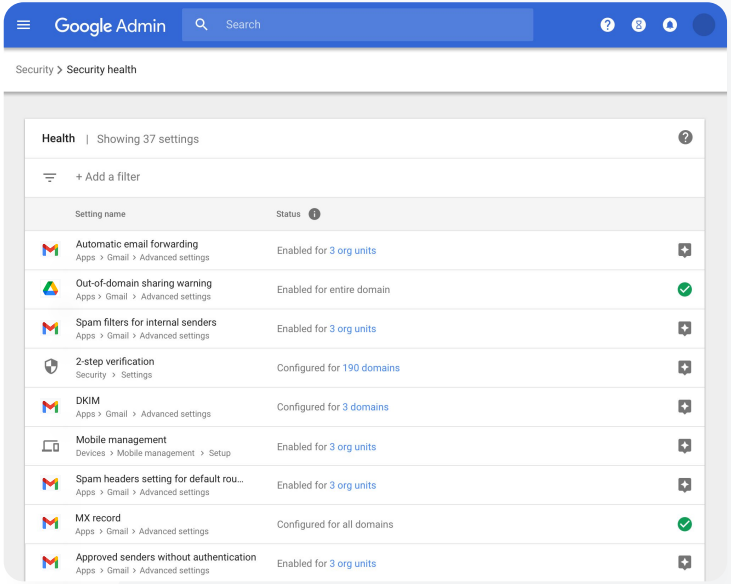
ヘルプセンターの関連記事

- セキュリティの状況ページを使ってみる

手順：セキュリティに関する推奨事項

推奨事項を確認する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**セキュリティの状況**] をクリック
- 右端の列でステータス設定を確認
  - 緑のチェックマークは設定が安全であることを示す
  - 灰色のアイコンはその設定に推奨事項があることを示し、アイコンをクリックすると詳細と手順が表示される



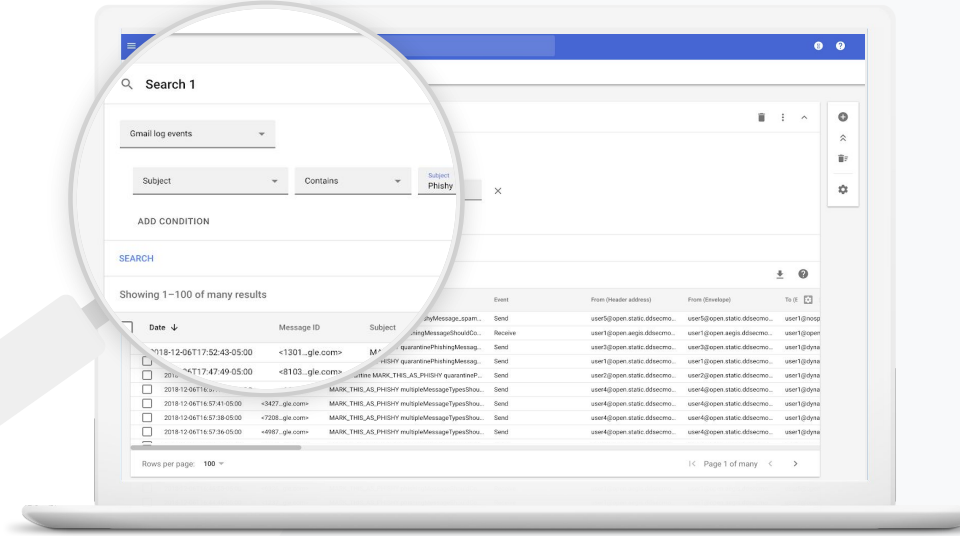
ヘルプセンターの関連記事

- セキュリティの状況ページを使ってみる

調査ツール

概要

調査ツールを使用すると、ドメイン内のセキュリティおよびプライバシーに関する問題を特定し、優先順位を付け、対処することができる



ユースケース

共有されている不適切なコンテンツ	詳細な手順
誤って共有されているファイル	詳細な手順
メールの優先順位付け	詳細な手順
フィッシング / マルウェア メール	詳細な手順
悪意のある人物による不正行為の阻止	詳細な手順
詳しいセキュリティ分析情報	詳細な手順
主催者不在の会議の防止	詳細な手順

「不適切なコンテンツを含むファイルが共有されていることがわかりました。このファイルを作成したユーザーと作成日、共有元と共有先のユーザー、編集したユーザーを確認し、ファイルを削除する必要があります。」

詳細な手順

ヘルプセンターの関連記事

- ドライブのログイベントの検索に使用できる条件
- ドライブのログイベントに関する操作

共有されている不適切なコンテンツ

調査ツールにあるドライブのログイベントを調べると、ドメインにある不適切なファイルを検出、追跡、隔離、削除できる。ドライブのログイベント データでは、以下のことが可能

- 名前、特定の操作を行ったユーザー、オーナーなどで検索してドキュメントを特定する
- 対処として、ファイルに設定されている権限を変更するかファイルを削除する
- ユーザーが Google Workspace で作成したコンテンツやドライブにアップロードしたコンテンツを検索する
- そのドキュメントに関連するすべてのログ情報を確認する
  - 作成日
  - オーナー、閲覧者、編集者
  - 共有された日時

「アクセス権限が付与されるべきではないグループと誤って共有されているファイルがありました。

このグループがファイルにアクセスできないようにする必要があります。」

詳細な手順

ヘルプセンターの関連記事

- 調査ツールで検索を行う
- 検索結果に基づいて対応する

誤って共有されているファイル

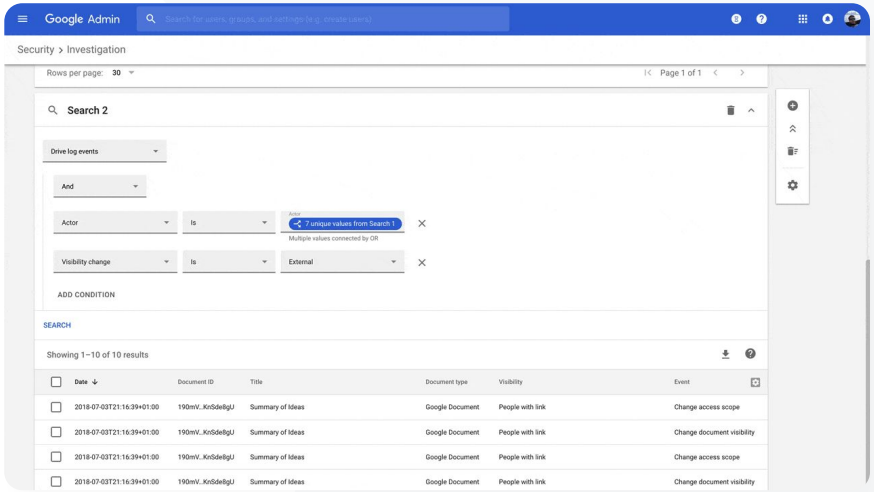
調査ツールにあるドライブのログイベントを調べると、ファイル共有に関する問題を追跡、解決できる。ドライブのログイベント データでは、以下のことが可能

- 名前、特定の操作を行ったユーザー、オーナーなどで検索してドキュメントを特定する
- そのドキュメントに関連するすべてのログ情報（閲覧者、共有された日時など）を確認する
- 対処として、権限を変更し、ダウンロード、印刷、コピーを無効にする

手順: ドライブのログイベント

ドライブのログイベントを調べる

- **管理コンソール**にログイン
- [**セキュリティ**] > [**調査ツール**] をクリック
- [**ドライブのログイベント**] を選択
- [**条件を追加**] > [**検索**] をクリック



対処する

- 検索結果から該当のファイルを選択
- [**操作**] > [**ファイル権限を監査**] をクリックして [**権限**] ページを開く
- [**ユーザー**] をクリックして、アクセスできるユーザーを確認
- [**リンク**] をクリックして、選択したファイルのリンク共有設定を確認または変更
- [**保留中の変更**] をクリックして、保存する前に変更内容を確認

ヘルプセンターの関連記事

- 調査ツールで検索を行う
- 検索結果に基づいて対応する

「誰かが不適切なメールを送信しました。送信者を特定し、受信者がメールを開いたかどうか、返信したかどうかを確認し、メールを削除する必要があります。メールの内容も確認しなければなりません。」

詳細な手順

ヘルプセンターの関連記事

- Gmail のログとメールの検索に使用できる条件
- Gmail のメールとログイベントに関する操作
- Gmail のメール コンテンツを閲覧する手順

メールの優先順位付け

調査ツールを使って Gmail のログを調べると、ドメインにある危険なメールや不適切なメールを特定し、対処できる。Gmail のログでは、以下のことが可能

- 件名、メッセージ ID、添付ファイル、送信者などで検索してメールを特定する
- メールの作成者、受信者、既読状況、転送の有無といった詳細な情報を確認する
- 検索結果に基づいて対応する。Gmail のメールへの対処として、削除、復元、迷惑メールやフィッシング メールへの分類、受信トレイへの送信、検疫への送信などがある

フィッシング メールとマルウェア メール

「フィッシング メールまたはマルウェア メールがユーザーに送信されました。メール内のリンクをクリックしたり添付ファイルをダウンロードしたりすると、ユーザーとドメインが危険にさらされる可能性があるため、このような行為をユーザーがしていないかどうかを確認する必要があります。」

詳細な手順

ヘルプセンターの関連記事

- Gmail のログとメールの検索に使用できる条件
- Gmail のメールとログイベントに関する操作
- Gmail のメール コンテンツを閲覧する手順
- VirusTotal レポートの表示

調査ツールを使って Gmail のログを調べると、ドメイン内の悪意のあるメールを特定し、隔離できる。Gmail のログでは、以下のことが可能

- メールを検索して特定のコンテンツ（添付ファイルなど）を見つける
- 特定のメールに関する情報（受信者や既読状況など）を確認する
- 悪意のあるメールかどうかを判断するためにメールの内容とスレッドを確認する
- メールの添付ファイルをスキャンして、VirusTotal レポートの脅威のコンテキストおよび評価データと照合する
- 対処として、メールを迷惑メールまたはフィッシングに分類するか、特定の受信トレイまたは検疫に送信するか、削除する

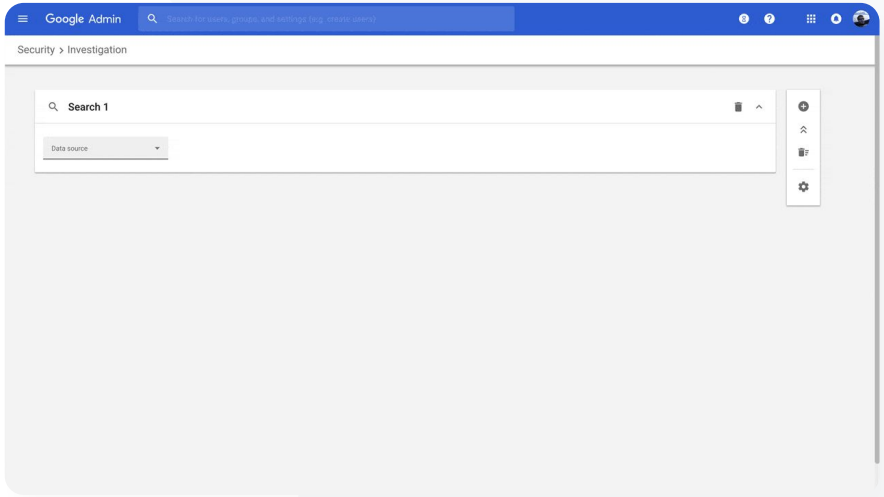
手順: Gmail のログ

Gmail のログを調べる

- **管理コンソール**にログイン
- [**セキュリティ**] > [**調査ツール**] をクリック
- [**Gmail のログイベント**] または [**Gmail のメール**] を選択
- [**条件を追加**] > [**検索**] をクリック

対処する

- 検索結果から該当のメールを選択
- [**操作**] をクリック
- [**メールを削除**] を選択
- 操作の結果を確認するには、ページ下部にある [**表示**] をクリック
- [**結果**] 列で、操作のステータスを確認



ヘルプセンターの関連記事

- Gmail のログとメールの検索に使用できる条件
- Gmail のメールとログイベントに関する操作
- Gmail のメール コンテンツを閲覧する手順

「不正な行為者がドメイン内の重要なユーザーを絶えず狙っていて、阻止しようとしても場当たり的な対応になってしまいます。

どうすれば阻止できますか？」

詳細な手順

ヘルプセンターの関連記事

- ユーザーのログイベントを検索して調査する
- 調査ツールを使用してアクティビティ ルールを作成する

悪意のある人物による不正行為の阻止

調査ツールにあるユーザーのログを調べると、以下のことが可能になる

- 組織内のユーザー アカウントに対する不正使用の試みを特定して調査する
- 組織内のユーザーがどの 2 段階認証プロセスを使用しているかを監視する
- 組織内のユーザーが失敗したログイン試行の詳細を調べる
- 調査ツールを使用してアクティビティ ルールを作成する: 特定の人物によるメールや悪意ある行為を自動的にブロックする
- 高度な保護機能プログラムで重要なユーザーを保護する
- ユーザーを復元または停止する

調査ツール　セキュリティとモニタリング用のツール

手順: 悪意のある人物による不正行為の阻止

ユーザーのログイベントを調べる

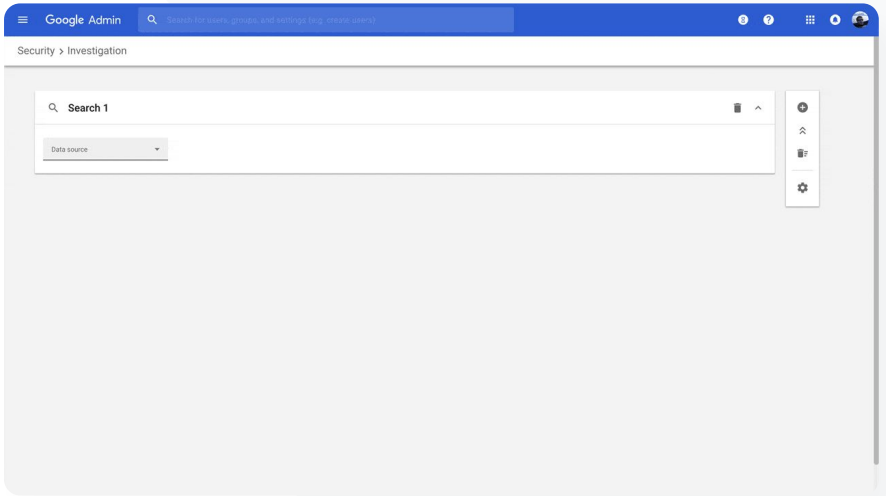
- **管理コンソール**にログイン
- [**セキュリティ**] > [**調査ツール**] をクリック
- [**ユーザーのログイベント**] を選択
- [**条件を追加**] > [**検索**] をクリック

ユーザーを復元または停止する

- 検索結果からユーザーを選択（複数可）
- [**操作**] プルダウン メニューをクリック
- [**ユーザーを復元**] または [**ユーザーを停止**] をクリック

特定のユーザーの詳細を表示する

- 検索結果ページからユーザーを1 人だけ選択
- [操作] プルダウン メニューから [**詳細を表示**] をクリック



ヘルプセンターの関連記事

- ユーザーのログイベントを検索して調査する

「ある教師が、Gmail で不審な添付ファイルにマークを付けました。

そのファイルがセキュリティ上の脅威であるかどうかをIT 部門が判断する方法はありますか？」

詳細な手順

ヘルプセンターの関連記事

- 調査ツールで検索を行う
- 調査ツールで VirusTotal レポートを表示する

詳しいセキュリティ分析情報を得る

VirusTotal レポートが提供する包括的な概要を利用することで、セキュリティ調査の結果を拡大し、管理者がクラウドソーシングによる分析情報に基づいて、特定のドメイン、添付ファイル、IP アドレス、または URL のセキュリティをチェックできる

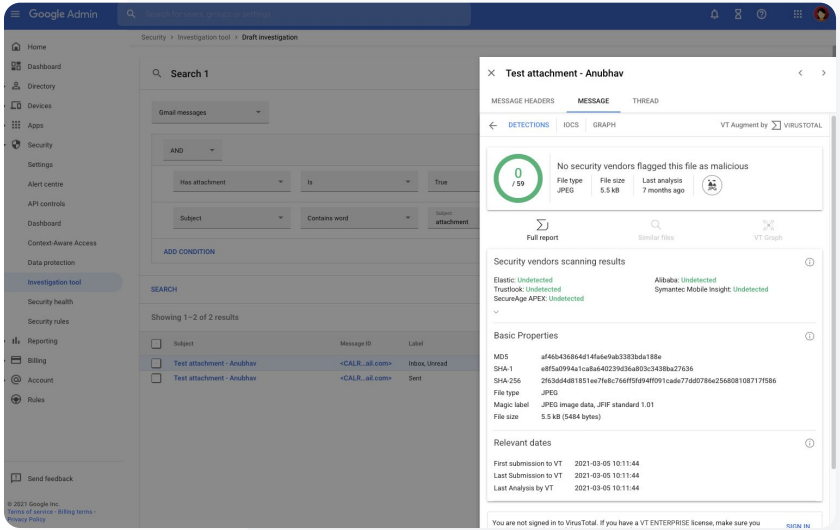
- Gmail と Chrome のログイベントに関する詳しいセキュリティ情報を得る
- 不審なファイル、URL、ドメイン、IP アドレスを分析する
- 添付ファイルやウェブサイトが危険と判断される理由をクラウドソーシングによる詳細情報で確認する
- セキュリティ上の懸念に対処するための意思決定に関する支援を受ける

手順: 詳しいセキュリティ分析情報を得る

Gmail に関する VirusTotal レポートを表示する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**セキュリティ センター**] > [**調査ツール**] をクリック
- [**Gmail のメール**] を選択
- [**条件を追加**] > [**添付ファイルあり**] をクリック
- 検索結果でメッセージ ID または件名列のリンクをクリック
- サイドパネルで[**メッセージ**] タブまたは [**スレッド**] タブをクリック
- [**VirusTotal レポートを表示**] を選択

Chrome 関連の VirusTotal レポートも表示できる。上記の手順で操作し、調査ツールで[**Chrome のログイベント**] を選択



ヘルプセンターの関連記事

- 調査ツールで VirusTotal レポートを表示する

「授業終了後もGoogle Meet の会議に居残る生徒がいます。学習の妨げにならないようMeet 通話を終わらせる方法が必要です。」

主催者不在のバーチャル会議を防止する

Google Workspace 管理者は、調査ツールにある [会議を終了して全員に退出してもらう] の操作を使用して、組織内のすべての会議からすべてのユーザーを削除できる。Google Meet の個々の会議では、会議主催者もこの機能を利用可能

- ブレイクアウト ルームにいるユーザーを含め、その会議に現在参加しているすべてのユーザーに対して会議が終了される
- 主催者が参加していないと、その会議の以降のセッションには誰も参加できない

詳細な手順

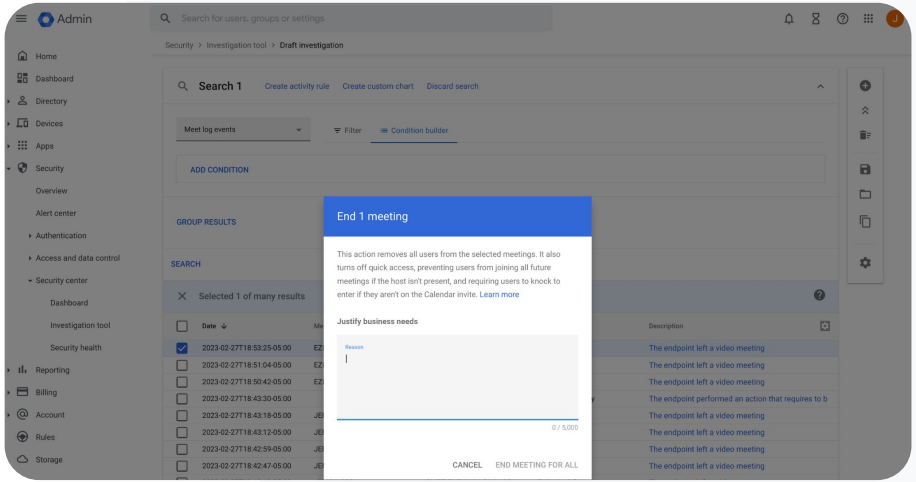
ヘルプセンターの関連記事

- 調査ツールを使用して会議を終了する

手順: 主催者不在のバーチャル会議を防止する

調査ツールを使用してすべてのユーザーに対して会議を終了する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**セキュリティ センター**] > [**調査ツール**] をクリック
- [**Meet のログイベント**] を選択
- [**検索**] をクリックすると、Meet のログイベントの検索結果が表示される
- 全ユーザーに対して終了する会議のチェックボックスをオンにする
- [**操作**] を選択
- [**会議を終了して全員を退出させる**] をクリック



ヘルプセンターの関連記事

- 調査ツールを使用して会議を終了する

ドメインの管理、制御

Google Workspace の高度なツールにアクセスすることで、組織のデータの管理、制御の設定、使用状況の監視、教育基準への準拠が可能になる

ユースケース

- Gmailの添付ファイルをスキャンして脅威を検知 — 詳細な手順
- 使用状況に関するダッシュボードやレポートの作成 — 詳細な手順
- ファイル検索の容易化 — 詳細な手順
- 内部ドキュメントの整理 — 詳細な手順
- 部門グループへの自動編入 — 詳細な手順
- 内部ファイル共有に関する対象グループの作成 — 詳細な手順
- ファイル共有の制限 — 詳細な手順
- Workspace アプリの制限 — 詳細な手順
- ストレージの管理 — 詳細な手順
- データの規制 — 詳細な手順
- 許可に関する規制 — 詳細な手順
- エンドポイント デバイスの管理 — 詳細な手順
- Windows デバイスの管理 — 詳細な手順
- Windows デバイスのカスタム設定 — 詳細な手順
- Windows デバイス アップデートの自動化 — 詳細な手順
- クライアントサイド暗号化の活用 — 詳細な手順

“How can I better protect my domain against zero-day malware and ransomware threats?”

Gmailの添付ファイルをスキャンして脅威を検知する

Email attachments can include malicious software. To identify these threats, Gmail can scan or run attachments in Security Sandbox. Attachments identified as threats are sent to the Spam folder.

- Detect malware by virtually “executing” it in a private, secure sandbox environment and analyzing the side effects to determine malicious behavior
- Scan Microsoft Word, PowerPoint, PDF, zip files, and more
- Enable scanning for the entire domain, or create scanning rules based on specific conditions like sender, domain, and more

Step-by-step how to

Relevant Help Center documentation

- Set up rules to detect harmful attachments

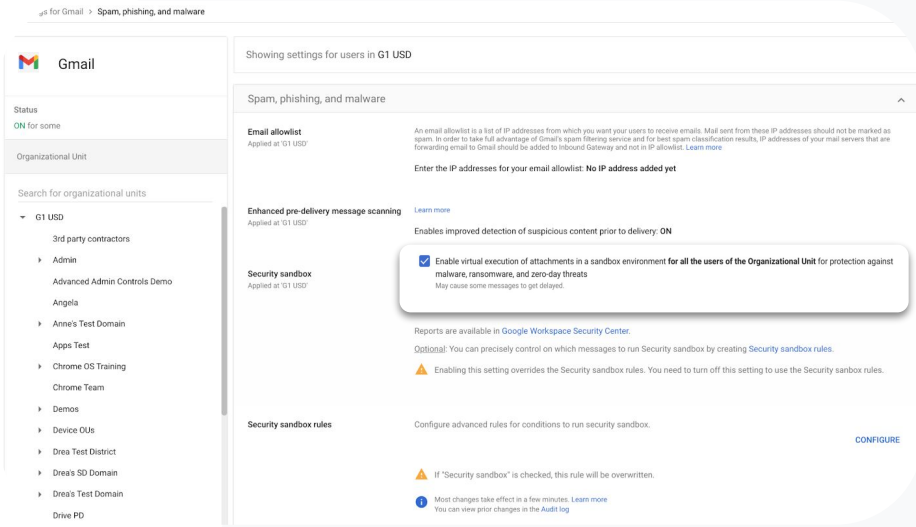
手順: Gmailの添付ファイルをスキャンして脅威を検知する

How it works

Email attachments are detonated within a sandbox in a matter of minutes prior to the delivery of the email, providing an extra layer of security.

How to scan all attachments in Security Sandbox

- Sign in to your **Admin console**
- Click **Menu** > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing, and Malware**
- Select an organizational unit or apply settings across your domain
- Scroll to **Security sandbox** under **Spam, Phishing, and Malware**
- Check the **Enable virtual execution of attachments in a sandbox environment** box
- Click **Save**



Relevant Help Center documentation

- Set up rules to detect harmful attachments

「どうすればドメイン全体の Classroom の使用状況を把握できますか？」

使用状況に関するダッシュボードやレポートの作成

管理者は BigQuery Export と Looker Studio テンプレート、Classroom のアクティビティ ログ、Looker Studio などの分析ツール、BigQuery に統合されたサードパーティのビジュアリゼーション パートナーを使って、カスタム ダッシュボードやレポートを作成できる

- 管理コンソールから Classroom のログデータを BigQuery と Looker Studio にエクスポート
- ドメイン全体の使用状況や普及率レポートをすばやく確認。誰がクラスから生徒を削除したか、誰が特定の日にクラスをアーカイブしたか、などをピンポイントで確認
- カスタマイズ可能な Looker Studio のダッシュボード テンプレートで、包括的なトレンドを理解し、より迅速に対処する

詳細な手順

ヘルプセンターの関連記事

- BigQuery Export と Looker Studio テンプレートを設定する

手順: 使用状況に関するダッシュボードやレポートの作成

01 BigQuery プロジェクトを設定、エクスポートする

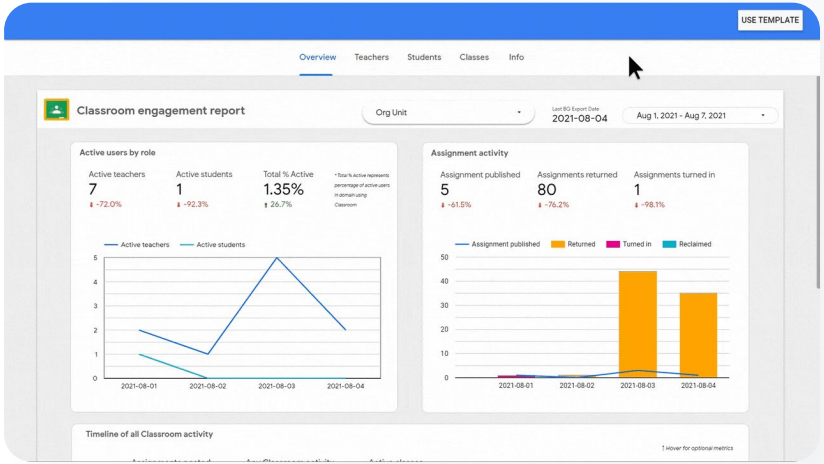
- console.cloud.google.com にログイン > **新規プロジェクトを作成**
- admin.google.com にログイン > [**レポート**] > [**BigQuery Export**]
- **Cloud BigQuery プロジェクト** > データセットを指定 > [**保存**] をクリック

02 Looker Studio で BigQuery Export を追加する

- Looker Studio にログイン > [**作成**] > [**データソース**]
- [**BigQuery**] > [**マイ プロジェクト**] を選択し、作成したプロジェクト > [**アクティビティ**] をクリック
- [**パーティション分割テーブル**] のチェックボックスをオン > [**接続**] をクリック

03 Looker Studio ダッシュボードを作成する

- テンプレートを開く > [**テンプレートを使用**] を選択
- [**新しいデータソース**] でアクティビティのデータソースを選択
- [**レポートをコピー**] をクリック



ヘルプセンターの関連記事

- BigQuery Export と Looker Studio テンプレートを設定する

「遠足を実施するにあたり、保護者から Gmail、Chat、ドキュメントで提出された許可証を確認する必要があります。

ドメイン全体からこれらのファイルを見つけるにはどうすればよいですか？」

詳細な手順

ヘルプセンターの関連記事

- Google Cloud Search スタートガイド
- 管理アカウントで Cloud Search の有効 / 無効を設定する

ファイル検索の容易化

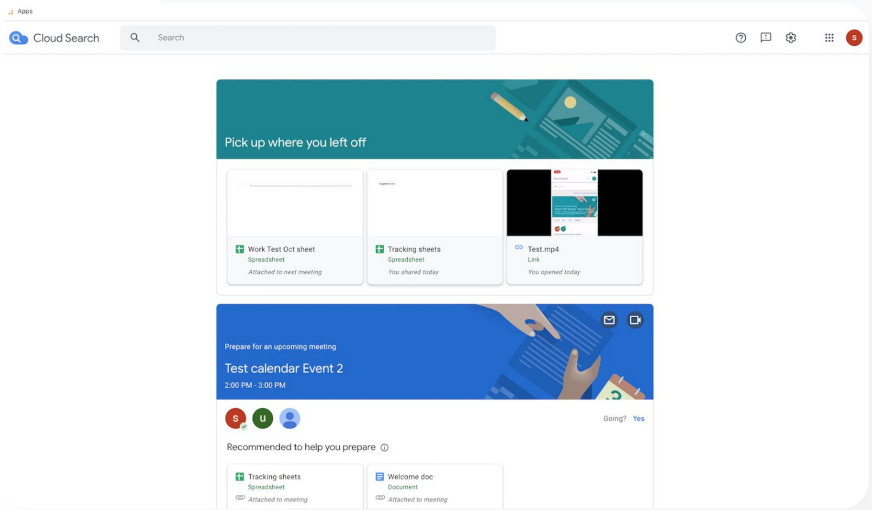
Google Cloud Search を使えば、Google Workspace やサードパーティ製アプリケーションからコンテンツをすばやく探し出せる

- ノートパソコン、スマートフォン、タブレットを使って、どこからでも必要な情報を探すことができる
- ドライブ、コンタクト、Gmail などの Google Workspace アプリやサードパーティのデータソースを横断検索できる

手順: ファイル検索の容易化

ユーザーに対して Cloud Search を有効にする

- **管理コンソール**にログインし、**メニュー アイコン** > [**アプリ**] > [**Google**] に移動
- [**サービスのステータス**] をクリック
- 組織内のすべてのユーザーに対してサービスを有効または無効にするには、[**オン**(すべてのユーザー)] または [**オフ(すべてのユーザー)**] をクリック
- [**保存**] をクリック
- 組織部門全体または組織部門内の一部のユーザーに対してサービスを有効にするには、**アクセス グループ**を選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- Google Cloud Search スタートガイド
- 管理アカウントで Cloud Search の有効 / 無効を設定する

「コンプライアンス要件への適合、不正使用の防止、ファイル整理の改善のために、教育機関のファイルに機密度別のラベルを適用したい。」

詳細な手順

ヘルプセンターの関連記事

- ドライブのラベルを管理する

ドメイン全体のドキュメントを整理する

ドライブのラベルを使用すると、ドメイン全体での検索、整理、ポリシー適用が容易になる。ドライブのラベルを作成、管理することで、ファイルの不正使用の防止と生徒データのコンプライアンス適合性確保が可能

- ラベルはメタデータであり、IEP、DOD、コンプライアンス ドキュメントのような機密性の高い教育関係ファイルの整理に役立つ
- ラベルの作成、構造定義、発行ができるのは管理者のみ。組織内のユーザーは、自分に編集権限のあるファイルにラベルを適用でき、項目の値を設定することもできる
- ドライブのラベルを使用すると、データ損失防止（DLP）を自動化できる

手順: ドメイン全体のドキュメントを整理する

機能の概要

Google ドライブのバッジ（視覚的なマーク）と標準ラベルを使用して、ドメイン全体でファイルを整理できる

教育機関に対してドライブのラベルを有効にする

- **管理コンソール**にログイン
- メニュー アイコン > [**アプリ**] > [**Google Workspace**] > [**ドライブとドキュメント**] をクリック
- [**ラベル**] を選択
- ラベルを**オン**または**オフ**にする
- [**保存**] をクリック

ヘルプセンターの関連記事

- ドライブのラベルを管理する

「新しい教師が着任するたびに『教育者』メールリストに含まれるように、グループ メンバーシップを自動化するにはどうしたらよいでしょうか？」

詳細な手順

ヘルプセンターの関連記事

- 動的グループを使用してメンバーを自動的に管理する

部門グループへの自動編入

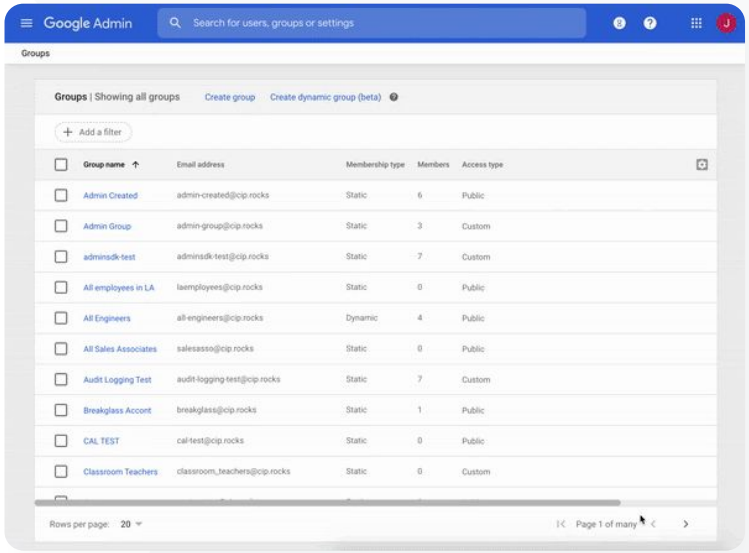
動的グループを使用すると、独自に設定した条件に基づいて学校全体でグループ メンバーを更新できる

- メンバーを自動管理する動的グループを作成する
- 作成したメンバーシップ クエリに基づいて、グループを最新の状態に保つ
- 動的グループは次の目的に使用できる
  - メーリング リスト、配布リスト
  - 管理対象グループ、共同トレイ
  - セキュリティ グループ

手順: グループ メンバーを自動追加する

動的グループを作成する

- **管理コンソール**にログインし、メニュー アイコン > [**ディレクトリ**] > [**グループ**] に移動
- [**動的グループを作成**] をクリック
- メンバーシップ クエリを次の場所で作成
  - [条件] リスト: メンバーシップの基準に使用（部門など）
  - [値] 欄: 使用する値
- 次の情報を入力
  - [名前]: リストおよびメッセージでグループを識別する名前
  - [説明]: グループの目的
  - [グループのメール]: グループで使用するメールアドレス
- [**保存**] をクリック
- [**完了**] をクリック



ヘルプセンターの関連記事

- 動的グループを使用してメンバーを自動的に管理する

「スタッフが誤って組織全体でドキュメントを共有してしまい、機密データを危険にさらしています。どうすれば、共有範囲をより小さく、より適切なグループに限定できるでしょうか？」

詳細な手順

ヘルプセンターの関連記事

- 対象グループについて
- 対象グループのおすすめの導入方法
- 対象グループを作成する

内部ファイル共有に関する対象グループの作成

対象グループを設定することで、ファイルを誤って必要以上の範囲に共有する危険性が低くなり、組織のデータのセキュリティを強化できる

- 適切な相手（特定のチームや部署など）とのみファイルを共有する
- 対象グループとは、ユーザーにアイテムの共有先として推奨できるグループ
- 管理者は、ユーザーの共有設定に対象グループを追加することで、特定のユーザーとの共有を促進できる
- Google ドライブ、ドキュメント、Chat で利用可能

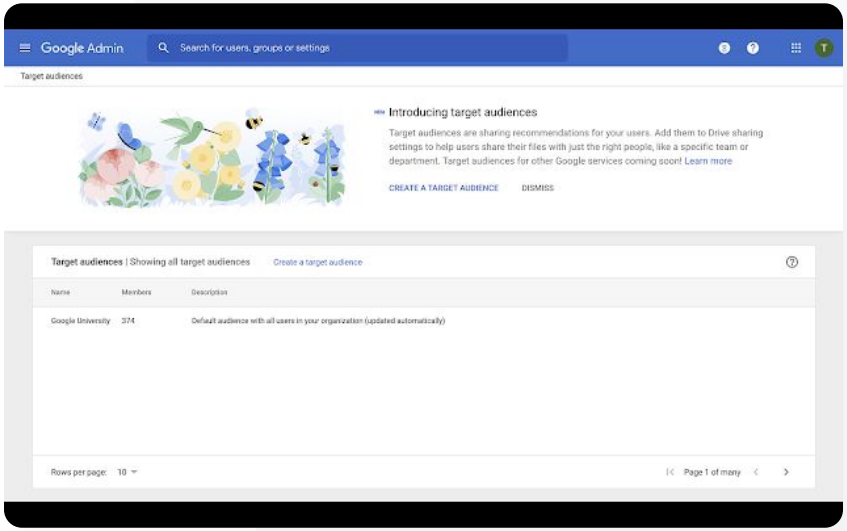
手順: 内部ファイル共有に関する対象グループの作成

機能の概要

対象グループの作成後に、メンバーを追加して Google ドライブに適用すると、ユーザーの共有設定で利用可能になる。たとえば、ドライブのファイルを共有する際に、スタッフに対して「スタッフ全員」の対象グループを表示できるようになる

教育機関に対してドライブのラベルを有効にする

- **管理コンソール**にログインし、**メニュー** アイコン > [**ディレクトリ**] > [**対象グループ**] に移動
- [**対象グループを作成**] をクリック
- [**名前**] に対象グループの名前を入力
- [**メンバーを追加**] を選択 > 目的のメンバーを指定
- [**完了**] をクリック



ヘルプセンターの関連記事

- 対象グループについて
- 対象グループのおすすめの導入方法
- 対象グループを作成する

「中等部の生徒が初等部の生徒とドキュメントを共有するのを防ぐにはどうすればよいですか？」

ファイル共有の制限

ドライブの信頼ルールを使用すると、ルールを設定して Google ドライブ ファイルにアクセス可能なユーザーを管理できるようになり、教育機関データの機密保護に役立つ。ポリシーは個々のユーザー、グループ、組織部門、ドメインに適用できる

- 機密情報を保護し、業界標準や規制への準拠を維持する
- ドメイン内外での共有を制限する。生徒が組織内でのみドライブ ファイルを共有するための信頼ルールを作成できる
- 「信頼ルール」を有効にすると、Google ドライブの「共有オプション」管理設定の後継となる

詳細な手順

ヘルプセンターの関連記事

- ドライブ共有の信頼ルールを作成、管理する

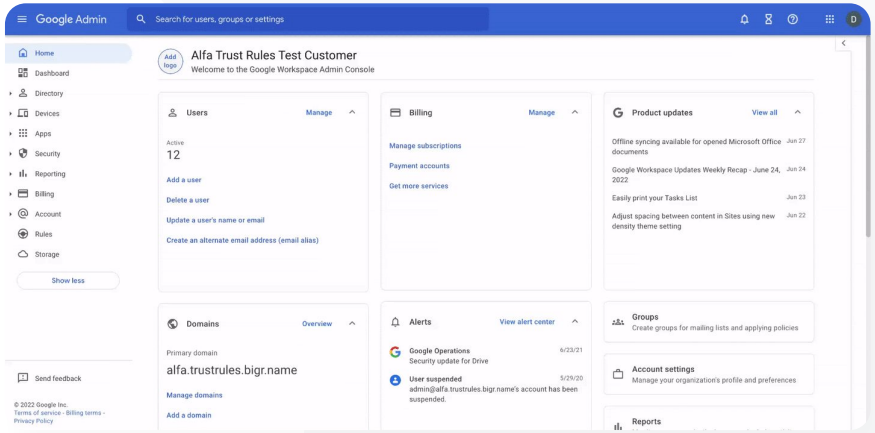
手順: ファイル共有の制限

ドライブの信頼ルールを有効にする

- **管理コンソール**にログインし、**メニュー アイコン** > [**ルール**] に移動
- ページ上部の [**安全なコラボレーション**] カードで、[**信頼ルールを有効にする**] をクリック
- タスクリストが自動的に開き、信頼ルール有効化の進行状況が表示される

管理者は、信頼ルールの作成、信頼ルールの詳細の表示と編集、信頼ルールの削除、信頼ルールのログイベントの表示が可能

信頼ルールを管理する方法の詳細については、管理者用ヘルプセンターを参照



ヘルプセンターの関連記事

- ドライブ共有の信頼ルールを作成、管理する

「ユーザーがネットワークに接続しているときに、アクセスを特定のアプリに制限する必要があります。」

詳細な手順

ヘルプセンターの関連記事

- コンテキストアウェア アクセスの概要
- アプリにコンテキストアウェア アクセスレベルを割り当てる

Google Workspace アプリの制限

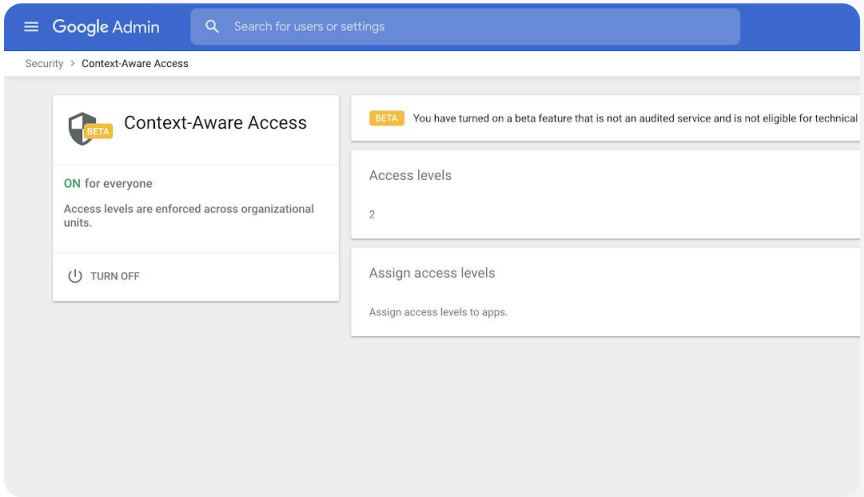
コンテキストアウェア アクセスを使用すると、ユーザー ID、アクセス元の地域、デバイスのセキュリティ状況、IP アドレスなどの属性に基づいて、Google Workspace やサードパーティ製 SAML（Security Assertion Markup Language）アプリに対する詳細なアクセス制御ポリシーを設定できる。ネットワーク外からのアプリへのアクセスを制限することも可能

- コンテキストアウェア アクセス ポリシーを Google Workspace for Education のコアサービスに適用できる
- 学校所有デバイスから Workspace アプリへのアクセスを制限する、ユーザーのストレージ デバイスが暗号化されている場合にのみドライブにアクセスする、など

手順: Google Workspace アプリの使用を制限する

コンテキストアウェア　アクセスを設定する

- **管理コンソール**にログイン
- [**セキュリティ**] > [**コンテキストアウェア アクセス**] > [**割り当てる**] を選択
- [**アクセスレベルの割り当て**] を選択してアプリのリストを表示
- **組織部門または設定グループ**を選択してリストを並べ替え
- レベルを調整するアプリの横にある[**割り当て**] を選択
- アクセスレベルを選択（複数可）
- ユーザーが複数の条件を満たすことを必須にする場合は、複数のレベルを設定
- [**保存**] をクリック



ヘルプセンターの関連記事

- コンテキストアウェア アクセスの概要
- アプリにコンテキストアウェア アクセスレベルを割り当てる

「ドメイン全体に新しいストレージ管理プランを導入する必要があります。」

ドメイン全体でストレージを管理する

Google Workspace for Education を導入している教育機関では、基本のストレージ プールが 100 TB に設定されており、これは約 1 億以上のドキュメント、800 万のプレゼンテーション、40 万時間のビデオに相当する容量。ドライブのストレージ プールを管理することで、教育機関のストレージ使用を効率化できる

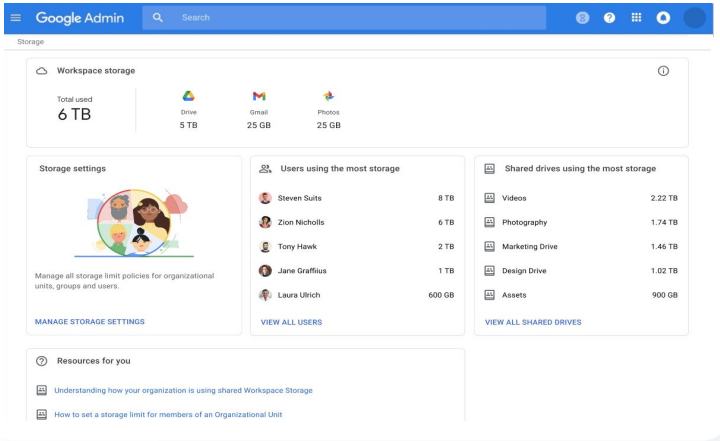
- 管理者向けツール、レポート、ログを使用して把握する
  - 使用中の保存容量
  - 保存容量の上限を設定する
  - 保存容量を過度に使用しているアカウントを特定する
- Teaching and Learning Upgrade と Education Plus では、基本の保存容量に加え、さらに容量を追加できる
  - Teaching and Learning Upgrade ではライセンスごとに 100 GB を共有プールに追加
  - Education Plus ではライセンスごとに 20 GB を共有プールに追加

詳細な手順

ヘルプセンターの関連記事

- 管理者向け保存容量ガイド
- 利用可能な保存容量と現在の使用量を把握する
- 空き容量を増やす、または保存容量を追加する
- 保存容量の上限を設定する

手順: ドメイン全体でストレージを管理する



ユーザーごとの保存容量を特定する

- **管理コンソール**にログインし、**メニュー アイコン** > [**ストレージ**] に移動
- 保存容量使用状況を組織部門やユーザー別に表示する

保存容量の上限を設定する

- **管理コンソール** > **メニュー アイコン** > [**ストレージ**]
- [**ストレージの設定**] で [**管理**] をクリック
- [**ユーザーの保存容量の上限**] > 制限を適用する相手を選択
  - 組織部門: 目的の組織部門をクリック
  - グループ: [グループ] をクリック > 検索フィールドをクリック > グループの名前を入力 > [グループ] をクリック
- [**オン**] を選択し、**保存容量**を設定
- [**保存**] をクリック

ヘルプセンターの関連記事

- 管理者向け保存容量ガイド
- 利用可能な保存容量と現在の使用量を把握する
- 空き容量を増やす、または保存容量を追加する
- 保存容量の上限を設定する

「法規制により、生徒と教職員のデータを EU 内に保管する必要があります。」

データの規制

管理者はデータ リージョン ポリシーを設定することで、データをどの地理的エリア（米国、または英国 / ヨーロッパ）に保管するかを指定できる

- Education Plus および Education Standard では、一部のユーザーに対して 1 つのデータ リージョンを選択したり、部門ごとに異なるデータ リージョンを選択したり、データ リージョンの移動の進捗を確認したりできる
- データ リージョンを部門ごとに設定するには、対象のユーザーを組織部門に追加する。複数部門をまたいで、または部門内の一部のユーザーを対象にデータ リージョンを設定するには、対象のユーザーを設定グループに追加する
- Education Standard または Education Plus のライセンスが割り当てられていないユーザーは、データ リージョン ポリシーの適用対象外

詳細な手順

ヘルプセンターの関連記事

- データの地理的な保管場所を選択する

「助成金に関する規制により、教職員の研究データを米国国内に保管する必要があります。」

許可に関する規制

管理者はデータ リージョン ポリシーを設定することで、教職員の研究データをどの地理的エリア（米国またはヨーロッパ）に保管するかを指定できる

- データ リージョン ポリシーの適用対象となるのは、こちらの一覧にある大半の Google Workspace for Education コアサービスのプライマリ保存データ（バックアップを含む）
- データ リージョン ポリシーを設定する前にトレードオフを考慮すること。データが保管されているリージョン外のユーザーにとって待ち時間が長くなる場合がある

詳細な手順

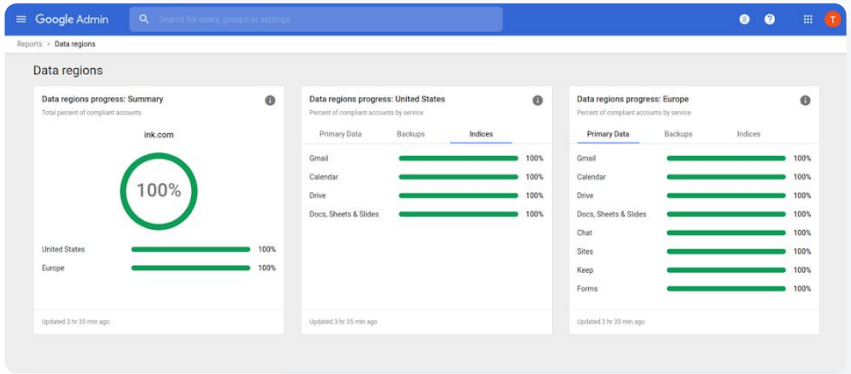
ヘルプセンターの関連記事

- データの地理的な保管場所を選択する

手順：データの規制

データ リージョンを指定する

- **管理コンソール**にログイン
  - 注: 特権管理者としてログインする
- [**会社プロフィール**] > [**すべて表示**] > [**データ リージョン**] をクリック
- リージョンを制限する組織部門または設定グループを選択するか、すべての部門とグループを含める場合は列全体を選択
- [**指定しない**]、[**米国**]、[**ヨーロッパ**] からリージョンを選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- データの地理的な保管場所を選択する

「Chromebook に限らず、iOS や Windows 10 など学区内で使用されているあらゆる種類のデバイスを管理し、ポリシーを適用する必要があります。特に、デバイスが不正使用されている場合には必須です。」

詳細な手順

ヘルプセンターの関連記事

- Google エンドポイント管理でデバイスを管理する
- モバイルの詳細管理を設定する

エンドポイント デバイスの管理

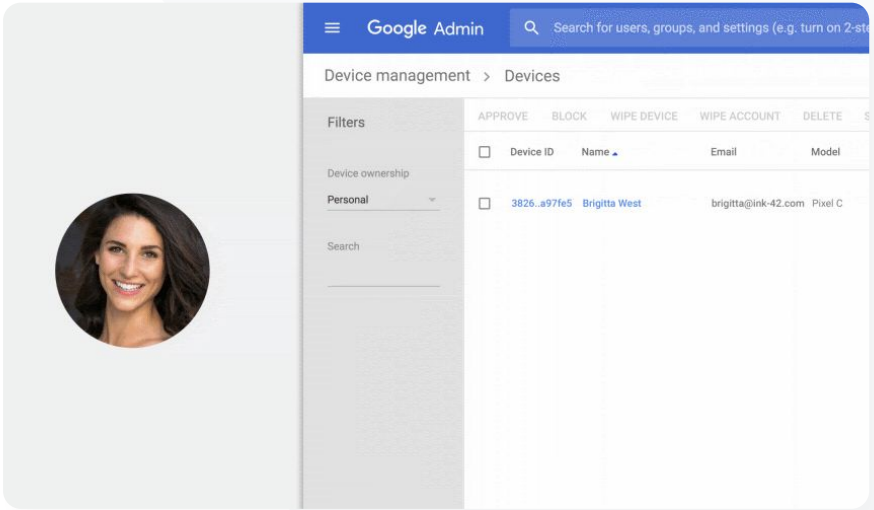
エンタープライズ エンドポイント管理を使用して、モバイル デバイスから組織のデータへのアクセスをより詳細に制御できる。モバイル デバイスの機能を制限したり、デバイスの暗号化を必須にしたり、Android デバイスや iPhone、iPad にあるアプリを管理したりできるほか、デバイスからデータをワイプすることも可能

- 管理コンソールからデバイスの承認、ブロック、ブロック解除、削除
- ユーザーがデバイスを紛失した場合や学校を離れた場合、その管理対象モバイル デバイスからユーザーのアカウント、プロファイル、全データをワイプ。このデータはその後もパソコンまたはウェブブラウザで使用可能

手順: エンドポイント デバイスの管理

モバイルの詳細管理を有効にする

- **管理コンソール**にログイン
- 管理コンソールの [**デバイス**] に移動
- 左側で [**設定**] > [**一般設定**] をクリック
- [**全般**] > [**モバイル管理**] をクリック
- 全ユーザーに設定を適用する場合は最上位の組織部門を選択したままにし、それ以外の場合は子組織部門を選択
- [**詳細**] を選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- Google エンドポイント管理でデバイスを管理する
- モバイルの詳細管理を設定する

「Windows 10 デバイスを使っている教師もいます。どうすれば当校のすべてのデバイスを一元管理できますか？」

Microsoft Windows デバイスを管理する

Android、iOS、Chrome、Jamboard の各デバイスと同様に、Windows 10 デバイスも管理コンソールで管理し、保護できる

- シングル サインオンを有効にすることで、ユーザーが Windows 10 デバイスから Google Workspace に簡単にアクセスできるようになる
- 管理コンソールでデバイスを管理することで、Google Workspace へのアクセスに使用されるデバイスが更新され、安全で、コンプライアンスに即した状態であることを確認できる
- クラウドから Windows 10 デバイスにワイプ、設定更新のプッシュなどを行う

詳細な手順

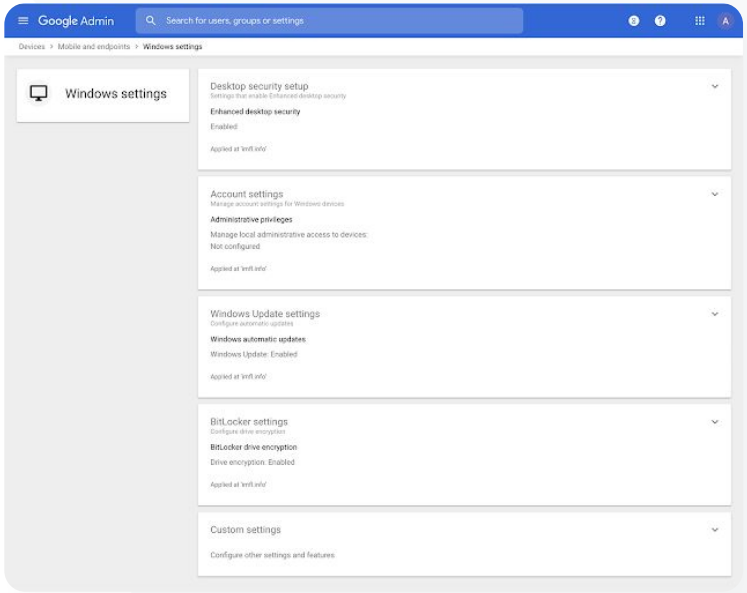
ヘルプセンターの関連記事

- Windows デバイス管理を有効にする
- デバイスを Windows デバイス管理に登録する

手順: Microsoft Windows デバイスを管理する

Windows デバイス管理を有効にする

- **管理コンソール**で**メニュー** アイコン > [**デバイス**] > [**モバイルとエンドポイント**] > [**設定**] > [**Windows の設定**] に移動
- [**Windows 管理の設定**] を選択
- 全ユーザーに設定を適用する場合は最上位の組織部門を選択したままにし、
- [**Windows デバイス管理**] の横にある [**有効**] を選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- Windows デバイス管理を有効にする
- デバイスを Windows デバイス管理に登録する

「Windows 10 デバイスでWi-Fi プロファイルを設定するにはどうすればよいですか？」

Windows 10 デバイスのカスタム設定

Google の Windows デバイス管理を利用することで、管理者は保有するデバイスにカスタム設定を追加できる

- 管理コンソールからデバイスのカスタム設定を管理する
- 次の設定を適用する
  - デバイス管理
  - セキュリティ
  - ハードウェアとネットワーク
  - ソフトウェア
  - プライバシー

詳細な手順

ヘルプセンターの関連記事

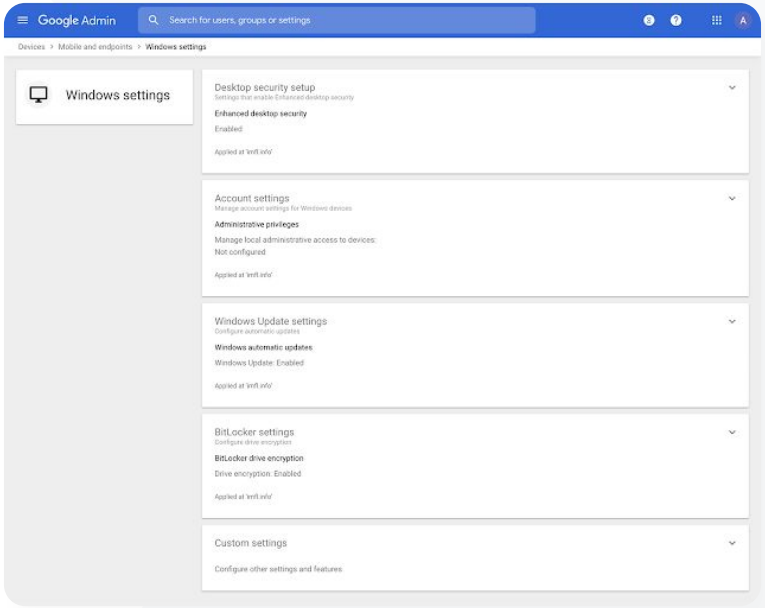
- 一般的なカスタム設定
- カスタム設定を追加する

手順: Windows 10 デバイスのカスタム設定

新しいカスタム設定を追加する

- **管理コンソール**で**メニュー** アイコン > [**デバイス**] > [**モバイルとエンドポイント**] > [**設定**] > [**Windows の設定**] に移動
- [**カスタム設定**] を選択
- [**カスタム設定を追加**] をクリック > 必須項目を入力
- [**次へ**] をクリック
- 設定の適用先である**組織部門**を選択
- [**適用**] をクリック

Google がサードパーティのプロダクトや設定について技術サポートを提供することはなく、責任も負いません。



ヘルプセンターの関連記事

- 一般的なカスタム設定
- カスタム設定を追加する

「保有するWindows 10 デバイスに最新のアップデートを確実に適用する必要があります。」

Windows 10 デバイスの自動更新

セキュリティ更新などの重要なダウンロード プログラムが、いつどのように Windows の自動更新サービス経由で教育機関の Windows 10 デバイスに適用されるようにするかを指定できる

- Windows Update コントロール パネルからアップデートをダウンロードする際の通知、アップデートの再起動がスケジュールされない時間などを設定する
- 教育機関全体または特定の組織部門に設定を適用する
- 変更には最長で 24 時間ほどかかることがある（通常はこれより短い時間で完了）

詳細な手順

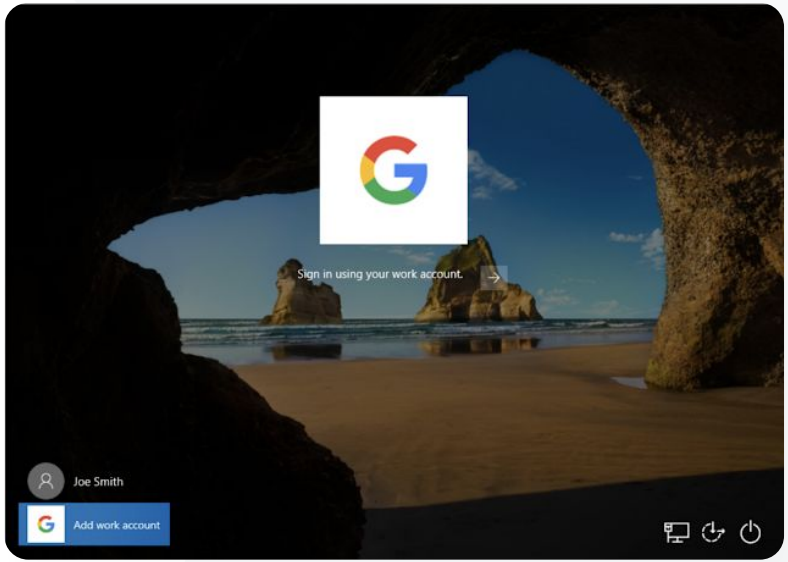
ヘルプセンターの関連記事

- 自動更新を管理する

手順: Windows 10 デバイスの自動更新

更新を設定する

- **管理コンソール**で**メニュー アイコン** > [**デバイス**] > [**モバイルとエンドポイント**] > [**設定**] > [**Windows の設定**] に移動
- [**Windows Update の設定**] > [**有効**] を選択
- [**Windows デバイス管理**] の横にある [**有効**] を選択
- オプションを設定 (その他のオプション)
  - Microsoft アプリケーションのアップデートを承認する
  - 自動更新の挙動
  - 自動更新の頻度
- [**保存**] をクリック



ヘルプセンターの関連記事

- 自動更新を管理する

「データの暗号化に関する Google の基準は最高レベルであることは承知していますが、大学の知的財産、そして助成金での研究のための暗号鍵を自分で管理する必要があります。」

詳細な手順

ヘルプセンターの関連記事

- クライアントサイド暗号化について

クライアントサイド暗号化の活用

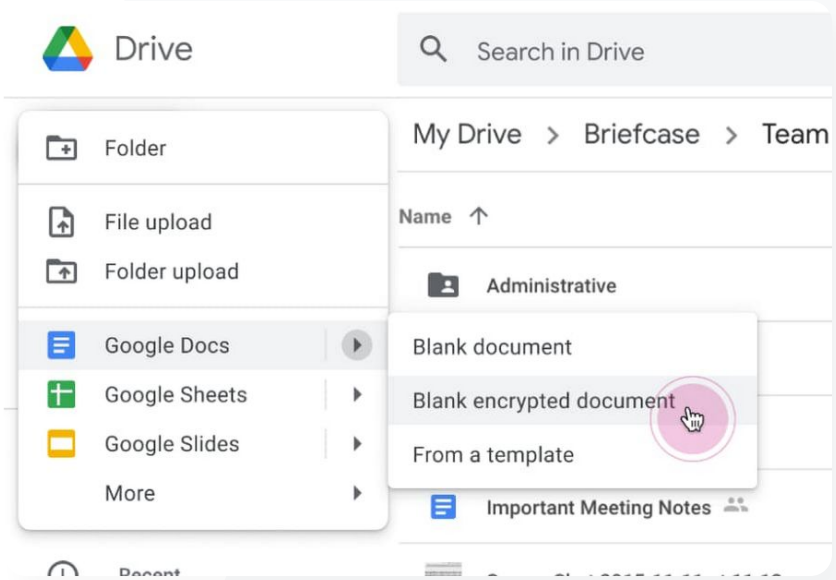
Google Workspace ではすでに最新の暗号基準を採用しており、Google の施設内のデータは、保存時および施設間での転送時にすべて暗号化されるが、さらにクライアントサイド暗号化を使用することで、暗号鍵と、その鍵へのアクセスに使用する ID プロバイダをユーザーが直接制御可能

- 教育機関の知的財産などの機密データを暗号化するために、独自の暗号鍵を使用する
- コンテンツの暗号化は、データが送信されたり、Google のクラウドベースのストレージに保存されたりする前に、ブラウザで処理される
- どのユーザーがクライアントサイド暗号化コンテンツを作成して内外で共有できるか選択可能

手順: クライアントサイド暗号化の活用

クライアントサイド暗号化（CSE）を設定する

- 暗号鍵サービスを設定する
  - 鍵サービスを作成することで、鍵管理と制御機能を使ってデータを保護
- Google Workspace と外部鍵サービスを接続する
  - 管理コンソールで鍵サービス URL を設定し、クライアントサイド暗号化用の鍵サービスを追加、管理する
- 鍵サービスを組織部門またはグループに割り当てる
  - 教育機関全体のデフォルトとして 1 つの鍵サービスを割り当てる
- Google Workspace と IdP を接続する
  - コンテンツの暗号化や暗号化されたコンテンツへのアクセスを許可する前にユーザーの ID を確認するため、クライアントサイド暗号化用の ID プロバイダ（IDP）を接続する
- ユーザーに対してCSE を有効にする
  - クライアントサイド暗号化を有効にして、組織部門またはグループがクライアントサイド暗号化コンテンツを作成できるようにする

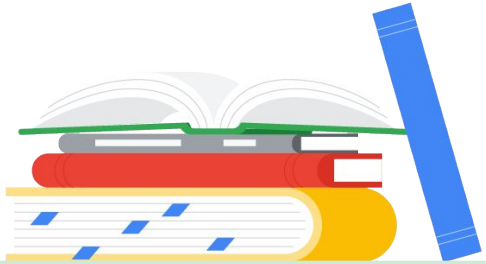


ヘルプセンターの関連記事

- クライアントサイド暗号化について

教育と学習の機能

授業を充実させる機能、学問的誠実性を培うためのツール、動画での高度なコミュニケーションなど、デジタル学習環境をより豊かにする機能を教育者の方々にご提供

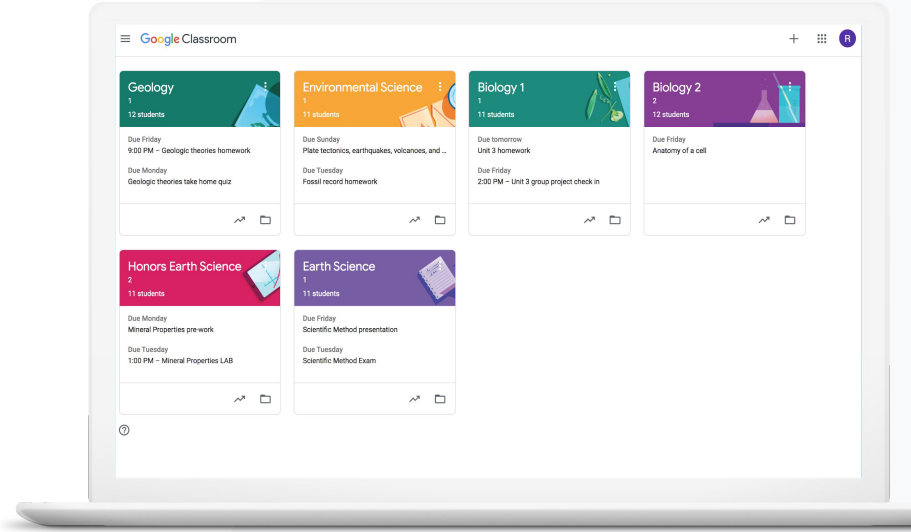


- Google Classroom
- 独自性レポート
- Google ドキュメント、スプレッドシート、スライド
- Google Meet

Google Classroom

概要

Google Classroom は教育と学習を一元管理できる場所であり、Classroom の有料機能を使えば、授業用ツールを 1 か所にまとめることができる。教育者は Classroom でお気に入りのツールに直接アクセスでき、クラスリストを外部システムと同期させることができる



ユースケース

Classroom アドオンへのアクセスを管理する	詳細な手順
魅力のあるコンテンツを Classroom に組み込む	詳細な手順
大規模なクラスを作成する	詳細な手順

「教育者が愛用しているEdTech ツールにシングル サインオンでアクセスできる方法があれば便利です。」

詳細な手順

ヘルプセンターの関連記事

- Google Workspace Marketplace アプリを管理する
- Classroom でアドオンを使用する
- 許可リストに登録された Marketplace アプリを管理する
- ユーザーに対する Marketplace アプリの配布
- Classroom アドオン（管理者用スタートガイド）

Classroom アドオンへのアクセスを管理する

どのサードパーティ製教育用アプリへのアクセスを許可するかをドメインの許可リストで指定する。教育者は数クリックで簡単にアドオンをインストールし、生徒の課題に含めることができるようになる

- ドメイン全体の許可リストを作成し、教育者が Google Workspace Marketplace からインストールできるサードパーティ製アプリを指定する
- 副教材アプリで学習成果をサポートする。教育者は Google Classroom 内で割り当て、レビュー、採点を行える
- Google Workspace Marketplace には、Adobe Creative Cloud Express、BookWidgets、CK-12、Formative、Genially、Google Arts & Culture、IXL、Kahoot!、Nearpod、Newsela、Pear Deck、SAFARI Montage、Sora、Wordwall などがある

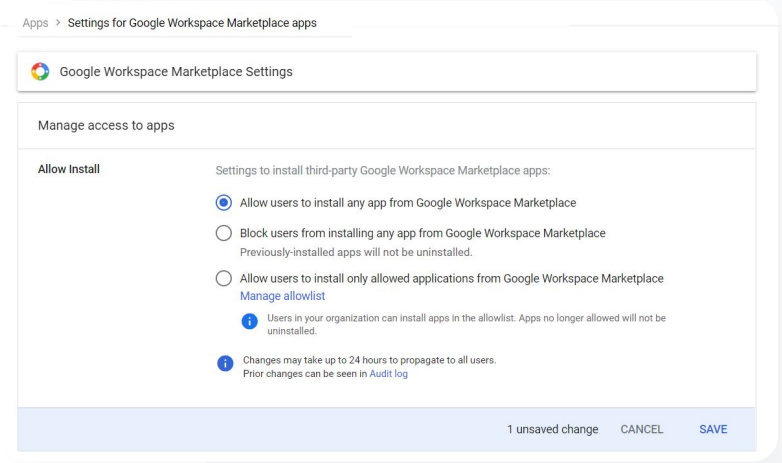
手順: Classroom アドオンへのアクセスを管理する

ドメインの許可リストでアドオンへのアクセスを管理する

- **管理コンソール**で**メニュー アイコン** > [**Google Workspace Marketplace アプリ**] > [**アプリのリスト**] を選択
- [**アプリを許可リストに登録**] を選択
- 追加または検索するアドオンの名前を入力
- [**選択**] をクリックし、[**ユーザーにこのアプリのインストールを許可する**] が選択されていることを確認
- [**続行**]、[**完了**] をクリック

アドオンに許可リストへのアクセス権を付与する

- **管理コンソール**で**メニュー アイコン** > [**Google Workspace Marketplace アプリ**] > [**アプリのリスト**] を選択
- 配布するアドオンを選択
- [**ユーザー アクセス**] で [**組織部門とグループを表示**] をクリック
- **すべてのユーザーが利用できる**ようにするか、**特定のグループ**または**組織部門に限定**するかを選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- Google Workspace Marketplace アプリを管理する
- Classroom でアドオンを使用する
- 許可リストに登録された Marketplace アプリを管理する
- ユーザーに対する Marketplace アプリの配布
- Classroom アドオン（管理者用スタートガイド）

「Google Classroom から離れることなく、生徒たちに Kahoot! の学習ゲームを割り当てて採点する必要があります。」

魅力のあるコンテンツを Classroom に組み込む

Classroom アドオンを使用して、Classroom 内で課題、質問、資料、お知らせにアドオンを添付することで、魅力的なアクティビティやコンテンツをクラスで共有できる

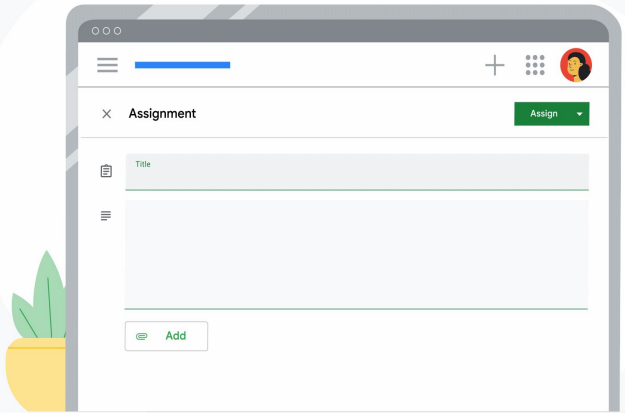
- 教師も生徒も、Kahoot!、Nearpod、Pear Deck といったお気に入りのツールを Classroom から移動する必要なしに使用可能
- アドオンを使えば、生徒が複数のパスワードを管理したり外部ウェブサイトにアクセスしたりする必要がない
- Classroom 内でアドオンから生徒の提出物を採点、確認できる

詳細な手順

ヘルプセンターの関連記事

- Classroom でアドオンを使用する
- Classroom アドオン（教師用スタートガイド）

手順: 魅力のあるコンテンツを Classroom に組み込む



課題、テスト、質問にアドオンを添付する

- classroom.google.com で Classroom アカウントにログイン
- リストから該当するクラスを選択し、[**授業**] を選択
- [**作成**] > 作成したいものを選択
- タイトルと説明を入力
- [**アドオン**] で、使用するアドオンを選択
- [**割り当て**] を選択

アドオンをお知らせに添付する

- クラスの [**ストリーム**] ページで [**クラスへの連絡事項を入力**] を選択
- お知らせの内容を入力
- [**アドオン**] で、使用するアドオンを選択
- [**投稿**] を選択

ヘルプセンターの関連記事

- Classroom でアドオンを使用する
- Classroom アドオン（教師用スタートガイド）

「Google Classroom で授業の設定や生徒名簿の管理を自動化する方法が必要です。」

大規模なクラスを作成する

SIS 名簿インポートを使えば、クラスを自動作成し、Clever を通じてクラス名簿を学校の生徒情報システム（SIS）と同期した状態に維持できる

- Education Plus を利用している米国およびカナダの K-12（義務教育課程の学校）の学区で利用可能
- 管理者は SIS から Google Classroom にクラス名簿をインポートして、クラスを自動設定できる
- Google Classroom のクラスリストをシームレスに自動化、管理できる

詳細な手順

ヘルプセンターの関連記事

- SIS の名簿インポートを使ってみる
- Clever を通じた SIS 名簿インポートを設定する

手順: 大規模なクラスを作成する

SIS の名簿インポートを設定する

- Clever で Google Classroom の名簿同期を設定する
- Clever の District Administrator と Google Workspace 特権管理者が、Clever の詳細な手順に沿って操作

学区に Clever アカウントがない場合 :

- Clever アカウントを作成

学区に Clever アカウントがある場合 :

- Clever ダッシュボードで名簿インポートをリクエスト

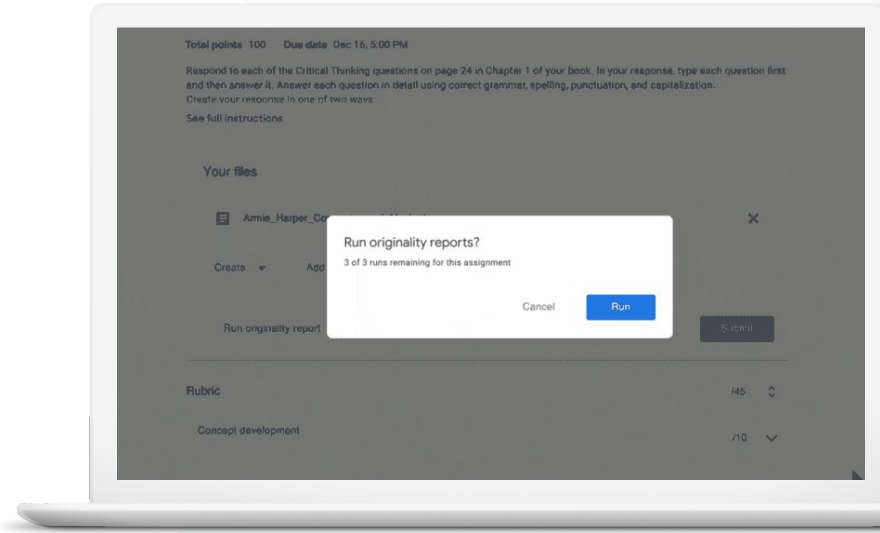
ヘルプセンターの関連記事

- Clever を通じた SIS 名簿インポートを設定する

独自性レポート

概要

独自性レポートでは、教育者や生徒が Google 検索を利用して、数十億のウェブページや 4,000 万冊以上の書籍と比較し、提出物の正当性をチェックできる。無制限にアクセスできる独自性レポートの有料版では、教育者が生徒の提出物と学校が所有する生徒の過去の提出物のリポジトリを照合できる



ユースケース

盗用の検出	詳細な手順
生徒の過去の提出物との照合で独自性を確認する	詳細な手順
盗用の検出を学びの機会に変える	詳細な手順

「生徒の提出物に盗用や正しくない形式での引用がないかを確認する必要があります。」

盗用の検出

教師は独自性レポートを使用して、生徒の提出物にオリジナルではないコンテンツが含まれていないかどうかを確認できる。引用表記のないテキストは、検出された引用元にリンクされて報告される

- ドキュメント、スライド、Microsoft Word 形式のドキュメントに対して独自性レポートを実行
- Teaching and Learning Upgrade または Education Plus では、教育関係者は次のことが可能
  - 独自性レポートに無制限にアクセスする
  - 生徒の過去の提出物の学校所有リポジトリで生徒間の一致を比較する

データは教育機関のものであり、そのデータのプライバシーとセキュリティを維持する責任は Google にある

詳細な手順

ヘルプセンターの関連記事

- 独自性レポートを有効にする
- 独自性レポートとプライバシー

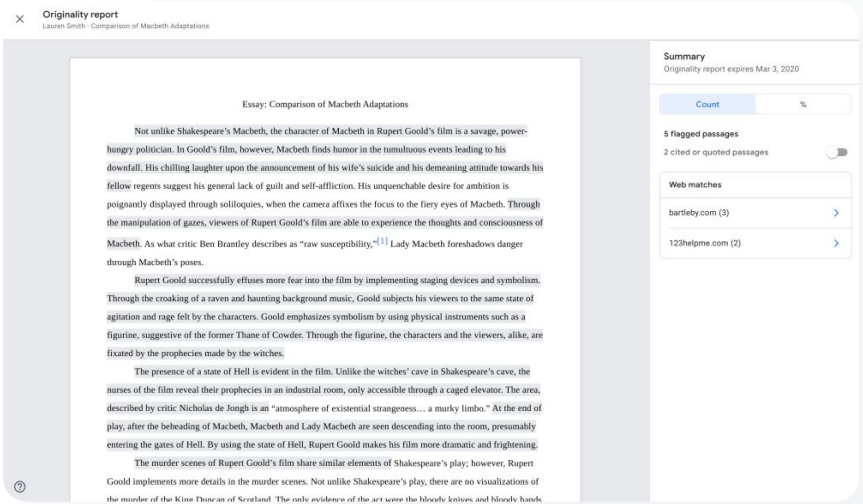
手順: 盗用の検出

Classroom で課題の独自性レポートを有効にする

- classroom.google.com で Classroom アカウントにログイン
- リストから該当するクラスを選択し、[**授業**] を選択
- [**作成**] > [**課題**] を選択
- [**盗用(独自性)を確認する**] チェックボックスをオンにして、有効にする

提出物の独自性レポートを作成する

- 該当する生徒のファイルをリストから選択し、クリックして採点ツールで開く
- 生徒の提出物の下にある [**独自性を確認**] をクリック



学習管理システムで課題の独自性レポートを有効にする

- 学習管理システムにログイン
- 関連するコースを選択
- 課題を作成 > [**Google アサインメント**] を選択
- [**独自性レポートを有効にする**] チェックボックスをオンにする

ヘルプセンターの関連記事

- Classroom: 独自性レポートを有効にする
- Google アサインメント: 独自性レポートを有効にする

「どうすれば、教師が生徒の提出物を過去の生徒の提出物と比較して盗用かどうかを判断できるようになりますか？」

生徒の過去の提出物との照合で独自性を確認する

校内での一致は、教育者が生徒の課題を教育機関の非公開リポジトリと照合することで、過去の生徒の提出物と比較する独自性レポート内の機能

- Teaching and Learning Upgrade または Education Plus では、生徒間の一致を現在および過去の生徒の提出物と比較し、盗用を検出できる
- 生徒の提出物は、学校所有のドメイン単位の非公開リポジトリ内に安全に保存され、バックフィルされる

詳細な手順

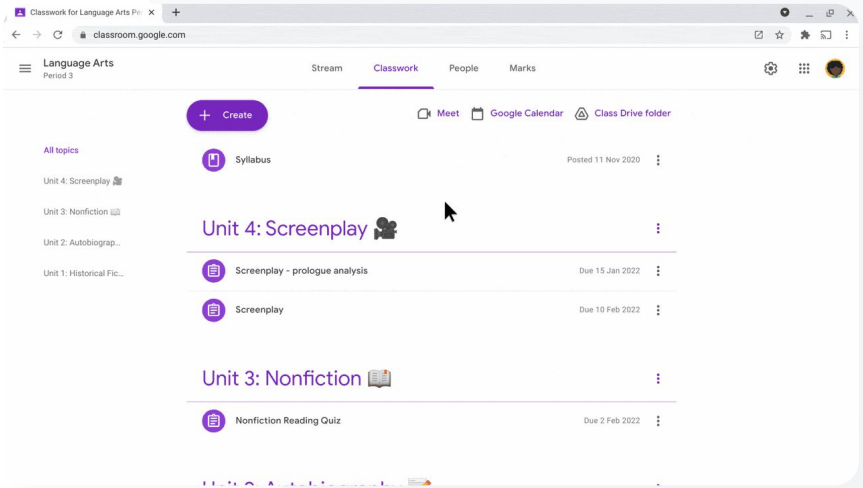
ヘルプセンターの関連記事

- 独自性レポートを有効にする
- Classroom の独自性レポートで校内での一致を有効にする

手順: 生徒の過去の提出物との照合で独自性を確認する

独自性レポートで校内での一致を有効にする

- **管理コンソール**で**メニュー アイコン** > **[アプリ]** > **[その他の Google サービス]** > **[Classroom]** を選択
- 教師用の組織部門を選択
- **[独自性レポート]** > **[独自性レポートで校内での一致を有効にする]** チェックボックスをオンにする
- **[保存]** をクリック



ヘルプセンターの関連記事

- Classroom の独自性レポートで校内での一致を有効にする

「出典を正しく引用する方法を学ぶ機会を生徒に提供する必要があります。」

盗用の検出を学びの機会に変える

生徒は独自性レポートを課題ごとに最大 3 回利用して、引用表記のないコンテンツや意図しない盗用が提出物に含まれていないかどうかを提出前に確認できる。独自性レポート機能は、生徒の Google ドキュメントをさまざまな参考文献と比較し、引用表記のないテキストを報告する。これにより、生徒は学習の機会を与えられ、誤りを訂正したうえで自信を持って課題を提出できる

- Teaching and Learning Upgrade または Education Plus では、教師が独自性レポートを有効にできる回数に制限はない。Education Fundamentals をご利用の場合、有効にできる回数はクラスあたり 5 回に限られる
- 課題の提出後、Classroom によりレポートが自動作成され、その結果は教師のみが確認できる。生徒が課題の提出を取り消して再提出した場合、教師向けに独自性レポートがもう一度作成される

詳細な手順

ヘルプセンターの関連記事

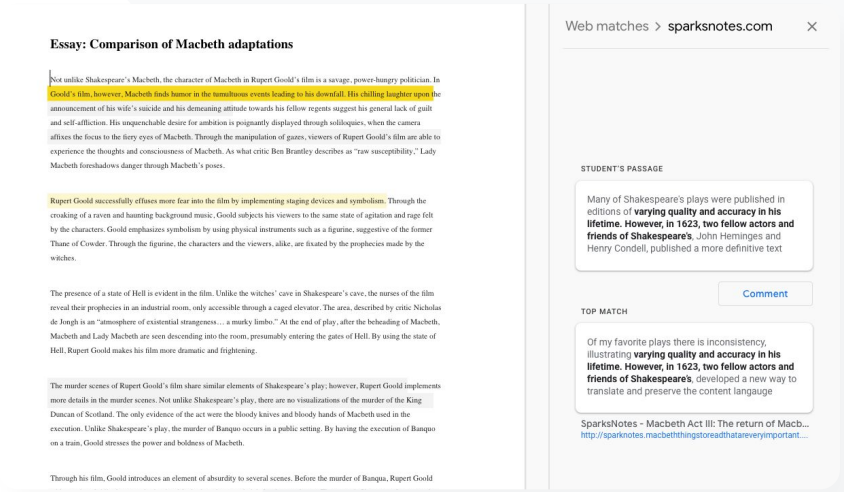
- 提出物の独自性レポートを作成する

手順：盗用の検出を学びの機会に変える

Classroom で生徒が独自性レポートを実行する

- classroom.google.com で Classroom アカウントにログイン
- リストから該当するクラスを選択し、**[授業]** を選択
- リストから該当する課題を選択し、**[課題を表示]** をクリック
- **[あなたの課題]** で、ファイルをアップロードまたは作成
- **[独自性レポート]** の横にある **[実行]** をクリック
- レポートを開くには、ファイルの課題名の下にある **[独自性レポートを表示]** をクリック
- 問題がある文を書き直すか適切に引用を表記して課題を修正するには、下部にある **[編集]** をクリック

生徒は Google アサインメントを使って学習管理システムで独自性レポートを実行できる



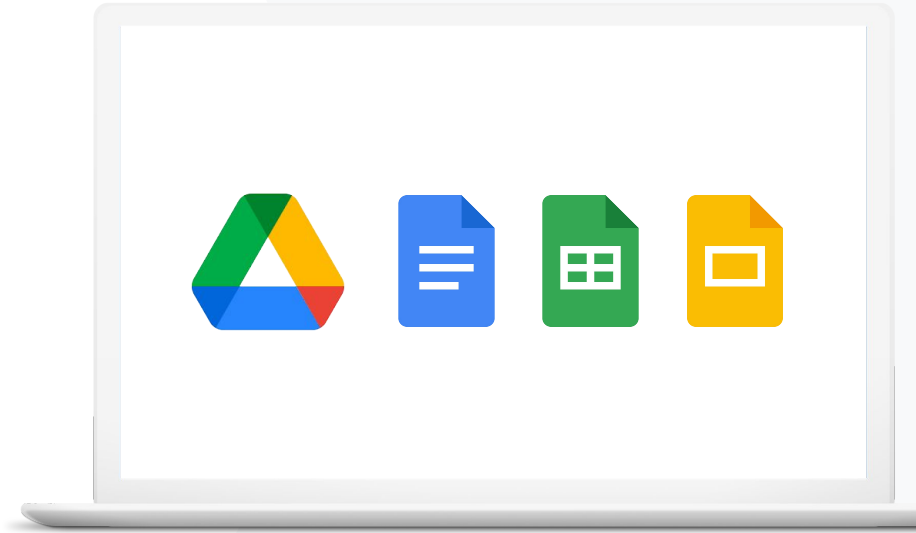
ヘルプセンターの関連記事

- Classroom で独自性レポートを実行する
- 学習管理システムで独自性レポートを実行する

Google ドキュメント、スプレッドシート、スライド

概要

学校コミュニティでドキュメント、スプレッドシート、スライドを使用すれば、リアルタイムでのコラボレーション、共同作成、確認、同時編集が可能。Education Plus の有料機能により、教育関係者や管理者は、教育機関全体の内部ドキュメントの承認プロセスを確立できる



ユースケース

内部ドキュメントを承認する　詳細な手順

「自然科学の学部で開発中の新カリキュラムを

確実にすべての学部長に承認してもらうための方法が必要です。」

内部ドキュメントを承認する

学校コミュニティで承認機能を使用して、Google ドライブのドキュメントを正式な承認プロセスに通すことができる

- レビュー担当者はドキュメントに対して、承認または却下したり、フィードバックしたりできる。これらはすべて、ドライブ、ドキュメントなどの Google Workspace アプリから直接行うことが可能
- 承認者はドキュメントへのリンクをクリックし、ドキュメントの内容の確認、コメントの追加、ドキュメントの却下または承認ができる
- 契約や新規採用の承認の管理、公開するドキュメントの変更承認などを行える

詳細な手順

ヘルプセンターの関連記事

- 承認プロセスを管理する

Google ドキュメント、スプレッドシート、スライド

教育と学習用のツール

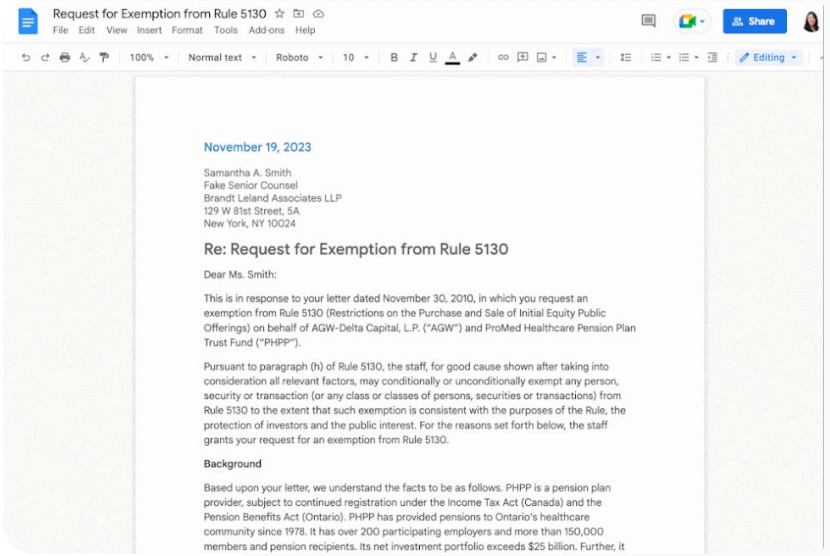
手順: 内部ドキュメントを承認する

機能の概要

管理者は、ユーザーが承認プロセスにどのように参加するか、ファイルがそのプロセスでどのように処理されるかを管理できる

承認を管理する

- **管理コンソール**にログインし、**メニュー アイコン** > [**アプリ**] > [**Google Workspace**] > [**ドライブとドキュメント**] に移動
- [**承認**] をクリック
- 全ユーザーに設定を適用する場合は、子組織部門または設定グループを選択
- [**保存**] をクリック



ヘルプセンターの関連記事

- 承認プロセスを管理する

Google Meet

概要

Google Meet の高度な機能には、ライブ配信、ブレイクアウト ルーム、大規模な会議、会議の録画、リアルタイム字幕などがある

ユースケース

会議を録画する	詳細な手順	質問を投げかける	詳細な手順
授業で扱った内容を確認する	詳細な手順	意見の収集	詳細な手順
言語の壁をなくす	詳細な手順	生徒のグループ分け	詳細な手順
集会や学校行事をブロードキャストする	詳細な手順	出欠状況の確認	詳細な手順

「オンラインで大規模な専門能力開発クラスを提供していますが、出席できない教育者のために録画する必要があります。」

会議を録画する

Teaching and Learning Upgrade および Education Plus では、授業や職員会議、専門能力開発トレーニングなどを録画できる。会議はドライブに自動保存される

- 録画は会議の主催者の Google ドライブに保存される。録画前に、ドライブの保存容量が十分にあることを確認すること
- IT 管理者には教職員に対してのみ録画機能を有効にすることを推奨

詳細な手順

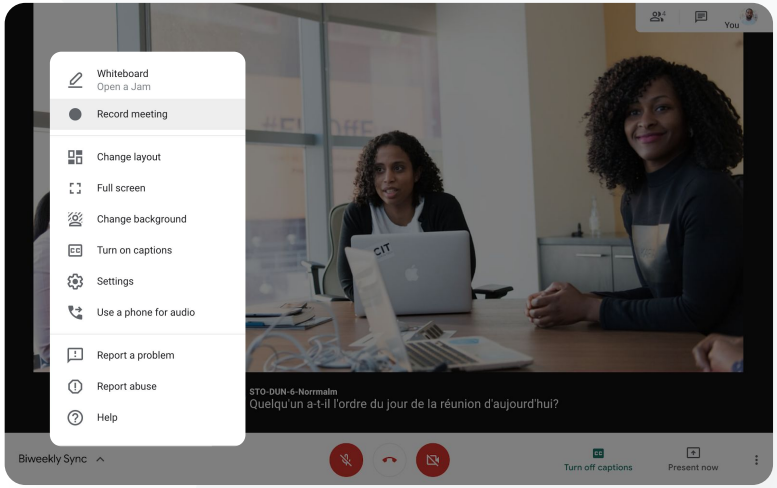
ヘルプセンターの関連記事

- ビデオ会議を録画する

手順: 会議を録画する

録画を開始する

- Google Meet で会議を開始する、または会議に参加する
- **アクティビティ アイコン** > [**録画**] をクリック
- [**録画を開始**] を選択
- 開いたウィンドウで[**開始**] をクリック
- 右下に、会議が録画中であることを示す赤い丸印が表示される
- 会議の動画ファイルが自動的にGoogle ドライブに保存される



ヘルプセンターの関連記事

- ビデオ会議を録画する

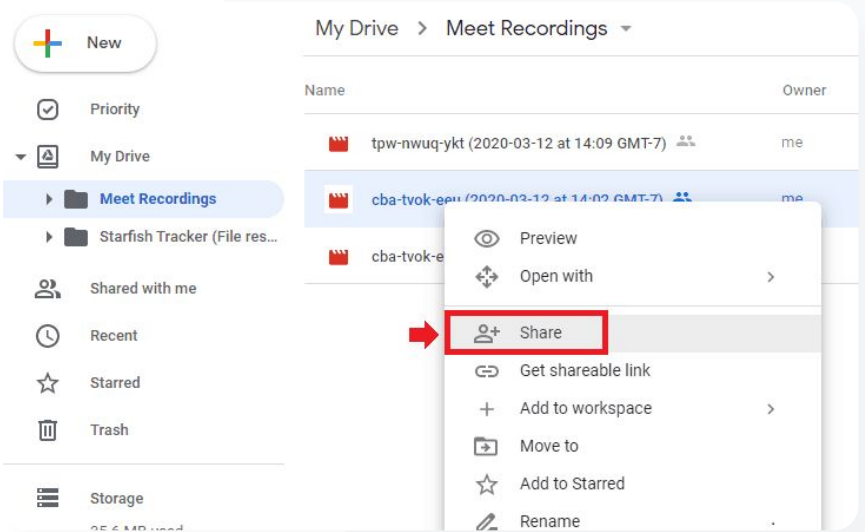
手順: 録画の閲覧と共有

録画を開始する

- ファイルを選択
- 共有アイコンをクリック
- 閲覧を許可するユーザーを追加

または

- リンクアイコンを選択
- メールまたはチャットメッセージにリンクを貼り付ける



録画をダウンロードする

- ファイルを選択
- **その他アイコン** > [**ダウンロード**] をクリック
- 再生するには、ダウンロードしたファイルをダブルクリック

録画を Google ドライブから再生する

- Google ドライブで録画ファイルをダブルクリックして再生（ファイルがオンラインで閲覧できる状態になるまでは「処理中」と表示される）
- 録画をマイドライブに追加するには、ファイルを選択して[**マイドライブに追加**] をクリック

ヘルプセンターの関連記事

- ビデオ会議を録画する

「生徒が後で概念を復習できるように、どうすればバーチャル授業を文字に起こすことができますか？」

授業で扱った内容を確認する

会議の文字起こしがあれば、教育者は自分の授業やクラスの議論を自動的に記録でき、生徒が概念を再確認することが容易になる。文字起こしを使用して、会議の出欠を記録したり、会議での発言者とその内容を示したりすることができる

- パソコンやノートパソコンでは Google Meet を英語で利用可能
- 管理者は学校コミュニティに対して音声文字変換を有効にできる
- 文字起こしは会議主催者のドライブに自動的に保存される
- 会議の文字起こしがオンになっている場合、会議に参加している全員の左上に文字起こしアイコンが表示される
- 文字起こしには会議で話された言葉が含まれる。チャット メッセージの文字起こしを取得するには、会議を録画する

詳細な手順

ヘルプセンターの関連記事

- Google Meet で文字起こしを使用する
- 音声文字変換をオンまたはオフにする

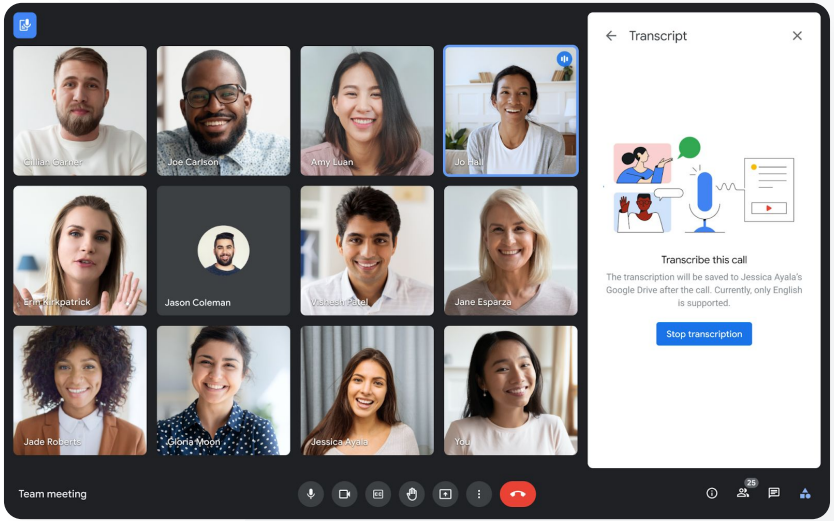
手順: 授業で扱った内容を確認する

Google Meet で文字起こしを有効にする

- 会議画面の右下にあるアクティビティアイコンを選択
- **[文字起こし]** > **[文字起こしを開始]** > **[開始]** をクリック

Google Meet で文字起こしを停止する

- アクティビティアイコン > **[文字起こし]** > **[文字起こしを停止]** > **[停止]** を選択



ヘルプセンターの関連記事

- Google Meet で文字起こしを使用する
- 音声文字変換をオンまたはオフにする

「保護者会もバーチャルで開催していますが、言葉が通じないこともあります。

どうすれば言葉の壁を乗り越え、会議をインクルーシブにできますか？」

言語の壁をなくす

字幕翻訳があれば、言葉の壁が効果的に取り除かれ、会議がよりインクルーシブなものになる。会議の参加者は、各自が選択した言語で発言内容を表示できるため、全員が情報を等しく共有、理解して、コラボレーションを行うことが可能

- 教育者は異なる言語を話す生徒、保護者、地域の関係者と交流できる
- 英語からフランス語、ドイツ語、ポルトガル語、スペイン語、またはその逆の字幕翻訳を使用可能
- また、英語を日本語、中国語、スウェーデン語に翻訳できる

詳細な手順

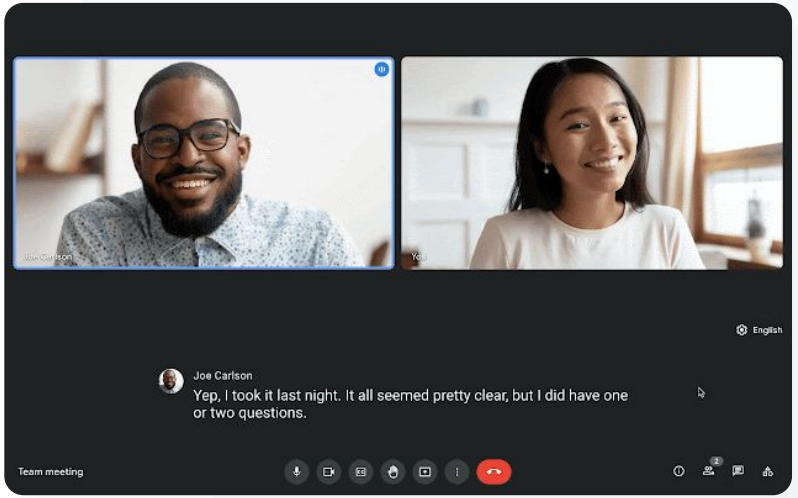
ヘルプセンターの関連記事

- Google Meet で字幕の翻訳機能を利用する

手順: 言語の壁をなくす

字幕翻訳を有効にする

- 会議画面下部にある**その他アイコン** > [**設定**] > [**字幕**] をクリック
- [**字幕**] をオンにする
- **会議の使用言語**を選択
- [**字幕の翻訳**] をオンにする
- **翻訳先の言語**を選択



ヘルプセンターの関連記事

- Google Meet で字幕の翻訳機能を利用する

「教職員の会議を、他の関係者や保護者にライブ配信できる機能が必要です。」

集会、学校行事、会議をブロードキャストする

Teaching and Learning Upgrade では最大 1 万人のユーザーが、Education Plus では最大 10 万人のユーザーがライブ配信を視聴可能。参加者は、主催者からメールまたはカレンダーの招待状で受け取ったライブ配信用リンクを選択して視聴を開始できる

- ライブ配信の共有範囲を次から指定する
  - 自組織のドメインのユーザーのみ視聴可能
  - 信頼できる Google Workspace ドメインでも視聴可能
  - YouTube で視聴可能
- IT 管理者には教職員に対してのみライブ配信機能を有効にすることを推奨
- ライブ配信を見逃したユーザーは、会議の終了後に録画を再生できる
- 字幕、アンケート、Q&A をライブ配信に追加すると、インクルーシブの度合いと参加意欲が高まる

詳細な手順

ヘルプセンターの関連記事

- Meet のライブ ストリーミングを有効または無効にする
- ビデオ会議のライブ配信

手順: 集会、学校行事、会議をブロードキャストする

ライブ配信イベントを作成する

- **Google カレンダー**を開く
- [**作成**] > [**その他のオプション**] を選択
- 予定の詳細（日時、説明など）を追加
- ビデオ会議に完全な権限で参加できるゲストを追加（完全な権限があると、自分の映像と音声が会議に配信され、画面共有を行える）
- [**ビデオ会議を追加**] > [**Meet**] をクリック
- [Google Meet に参加する] の横にある下矢印 > [**ライブ ストリームを追加**] を選択
- ご利用の有料エディションで許可される人数のドメイン内ユーザーを招待するには、[**コピー**] をクリックしてからライブ配信用のURL を共有
- [**保存**] を選択
- 会議中に**その他アイコン** > [**ストリーミングを開始**] を選択（ストリーミングは自動的には開始しない）

ヘルプセンターの関連記事

- Meet のライブ ストリーミングを有効または無効にする
- ビデオ会議のライブ配信

「質問を投げかける、生徒の理解度を測る、生徒と対話して授業に積極的に参加させるといったことを手早くできる手段が必要です。」

質問を投げかける

Google Meet の Q&A 機能を使用すると、授業への積極的な参加を生徒に促し、クラスの対話を活発にすることができる。バーチャル授業の最後に、すべての質問と回答をまとめた詳細なレポートが教師に送信される

- 会議の管理者による質問の数には制限なし。質問のフィルタや並べ替え、回答済みのマーク付け、非表示や、優先順位付けを行うこともできる
- 質問が有効になっている会議が終わるたびに、質問レポートが会議の管理者にメールで自動送信される

詳細な手順

ヘルプセンターの関連記事

- Google Meet で参加者に質問する

手順: 質問を投げかける

質問する

- 会議画面の右上にある**アクティビティ アイコン** > [**質問**] を選択（Q&A 機能を有効にするには[**Q&A を有効にする**] をオンにする）
- 質問するには、画面右下にある[**質問を入力**] をクリック
- 質問を入力 > [**投稿**] を選択

質問レポートを表示する

- 会議の終了後、会議の管理者にレポートが**メールで届く**
- メールを開き、**レポートの添付ファイル**をクリック

ヘルプセンターの関連記事

- Google Meet で参加者に質問する

「授業や職員会議を主催しているときに、生徒や他の先生方から簡単に意見を集められる手段が必要です。」

意見の収集

バーチャル会議を設定または開始したユーザーは、参加者向けにアンケートを実施できる。この機能を使用すると、会議の出席者全員（生徒など）から参加型のアプローチですばやく情報を集めることができる

- 会議の管理者はアンケートを保存し、後から会議中に投稿可能。アンケートにはバーチャル会議画面の [アンケート] セクションから簡単にアクセスできる
- 会議の終了後、アンケート結果のレポートが会議の管理者にメールで自動送信される

詳細な手順

ヘルプセンターの関連記事

- Google Meet でアンケートを実施する

手順: 入力情報を収集する

アンケートを作成する

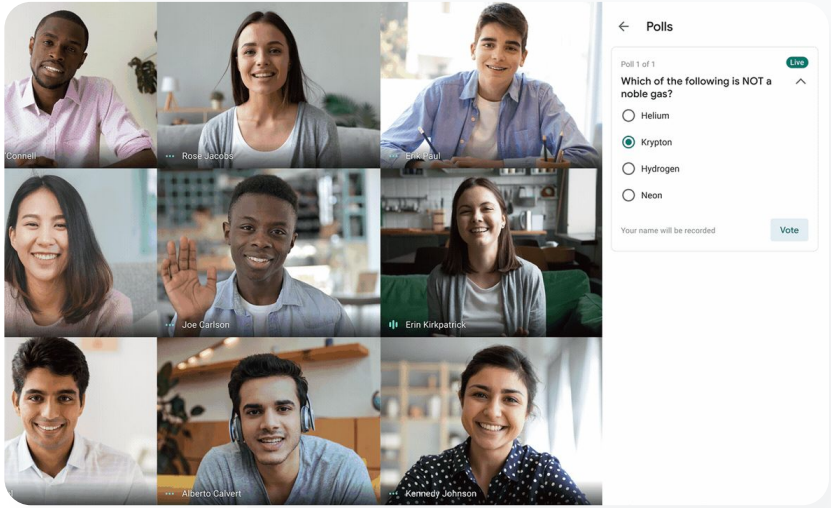
- 会議画面の右上にある**アクティビティ アイコン** > [**アンケート**] を選択
- [**アンケートを開始**] を選択
- 質問を入力
- [**公開**] または [**保存**] を選択

アンケートを管理する

- 会議画面の右上にある**アクティビティ アイコン** > [**アンケート**] を選択
- 参加者にアンケート結果をリアルタイムで見せるには、[**全員に結果を表示する**] の横にあるスイッチをオンにする
- アンケートを終了して回答の受け付けを締め切るには、[**アンケートを締め切る**] をクリック
- アンケートを完全に削除するには、削除アイコンを選択

アンケートのレポートを確認する

- 会議の終了後、会議の管理者にレポートが**メールで届く**
- メールを開き、**レポートの添付ファイル** を選択



ヘルプセンターの関連記事

- Google Meet でアンケートを実施する

「生徒が自宅学習をすることもあります。少人数のグループ作業をするとき、あらかじめ設定したグループに基づいて簡単にブレイクアウト ルームを作る方法が必要です。」

詳細な手順

ヘルプセンターの関連記事

- Google Meet でブレイクアウト ルームを使用する

生徒のグループ分け

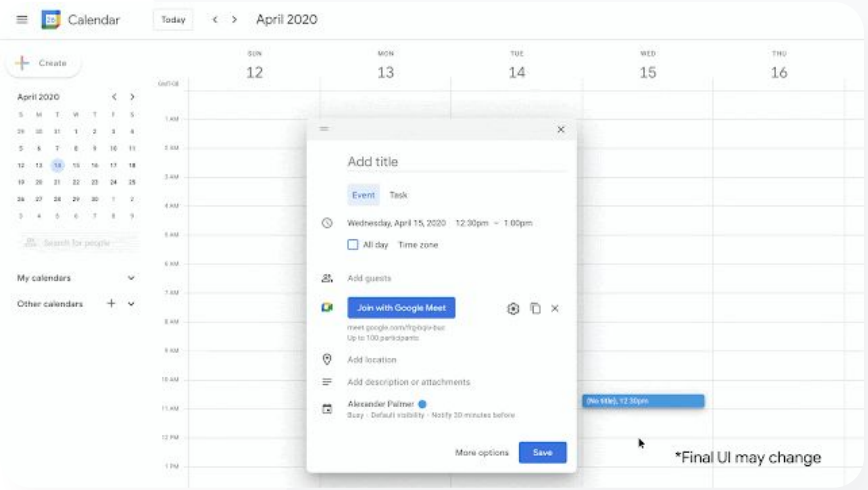
教師はブレイクアウト ルームを使用して、バーチャル授業、対面式授業、またはその混合の生徒を少人数のグループに分けることができる。ブレイクアウト ルームは、パソコンでビデオ会議を行っている最中に、会議の管理者が開始する必要がある

- ブレイクアウト ルームは、イベントの作成時にあらかじめ作成しておくことも、会議中に作成することもできる
- バーチャル会議ごとに最大 100 個のブレイクアウト ルームを作成できる
- 教師は必要に応じてブレイクアウト ルーム間を簡単に移動し、各グループを指導できる
- 管理者は、教職員のみにブレイクアウト ルームの開始を許可できる

手順: 少人数の生徒グループを作成する

会議前にブレイクアウト　ルームを作成する

- Google カレンダーの新しい予定を作成
- [**Google Meet のビデオ会議を追加**] をクリック
- 参加者を追加 > [**この会議の設定を変更**] を選択
- [**ブレイクアウト ルーム**] をクリック
- ブレイクアウトルームの数を選択し、次のいずれかを行う
  - 参加者を目的のブレイクアウト ルームにドラッグ
  - ブレイクアウト ルームに参加者の名前を直接入力
  - シャッフル アイコンをクリックして、参加者のグループを入れ替える
- [**保存**] をクリック



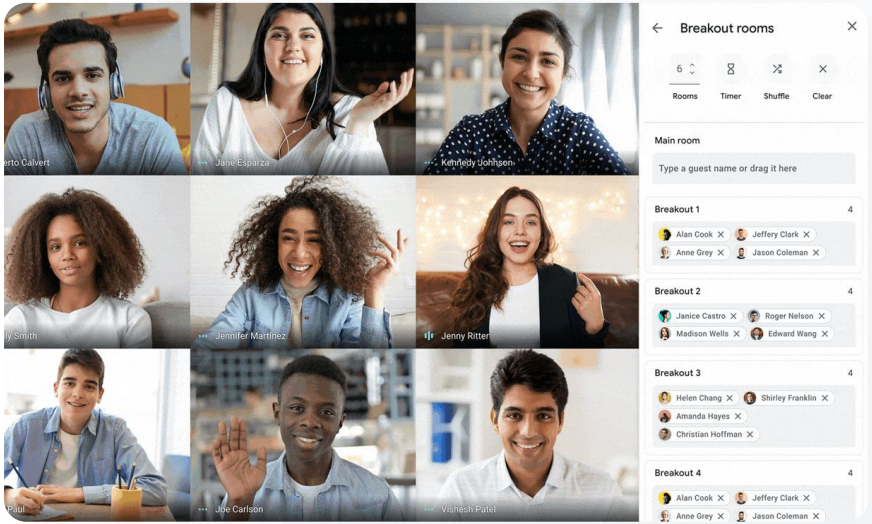
ヘルプセンターの関連記事

- Google Meet でブレイクアウト ルームを使用する

手順: 少人数の生徒グループを作成する

会議中にブレイクアウト　ルームを作成する

- ビデオ会議を開始
- 画面の右上にある**アクティビティ アイコン** > [**ブレイクアウト ルーム**] を選択
- [**ブレイクアウト ルーム**] パネルで、必要なブレイクアウトルームの数を選択
- 生徒が各ルームに分かれる（会議の管理者は必要に応じてメンバーを手動で別のルームに移動可能）
- 右下の [**セッションを開く**] をクリック



それぞれのブレイクアウト　ルームで質問に答える

- 会議の管理者の画面下部に参加者からのサポートリクエスト通知が表示されたら、[参加] を選択してその参加者のブレイクアウトルームに入る

ヘルプセンターの関連記事

- Google Meet でブレイクアウト ルームを使用する

「オンライン授業の出席状況をうまく把握できず、困っています。ドメイン全体における授業の出席状況を簡単に報告できる手段が必要です。」

出欠状況の確認

出席状況の確認機能により、5 人以上が参加した会議の場合は出席レポートが自動的に作成される。レポートには、参加者の名前とメールアドレス、バーチャル授業に参加していた時間が記載される

- ライブ配信イベントの参加者に関する情報は、ライブ ストリーム レポートで確認できる
- 会議の管理者は、会議画面上またはカレンダーの予定から、出席状況の確認機能とライブ ストリーム レポート機能を有効または無効に設定できる

詳細な手順

ヘルプセンターの関連記事

- Google Meet で出席状況を確認する

手順: 出欠状況の確認

会議の出席状況を確認する

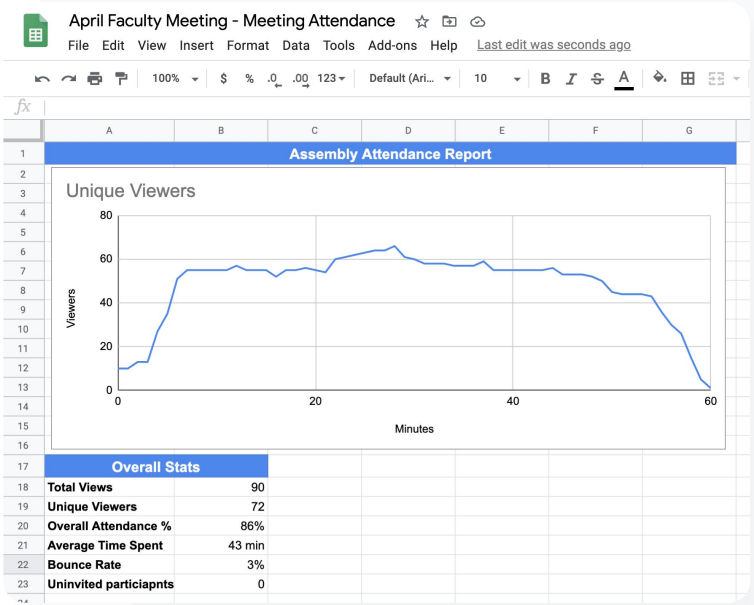
- ビデオ会議を開始
- 画面下部のその他アイコンを選択
- 設定アイコン > [**主催者用ボタン**] を選択
- [**出席状況の確認**] をオンまたはオフにする

カレンダーで出欠状況を確認する

- カレンダーの予定で**Google Meet の会議を有効**にする
- 右側で**設定アイコン**を選択
- [**出席状況の確認**] チェックボックスをオンにし、[**保存**] をクリック

出席レポートを取得する

- 会議の終了後、会議の管理者にレポートが**メールで届く**
- メールを開き、**レポートの添付ファイル**を選択



ヘルプセンターの関連記事

- Google Meet で出席状況を確認する

ありがとう
ございました