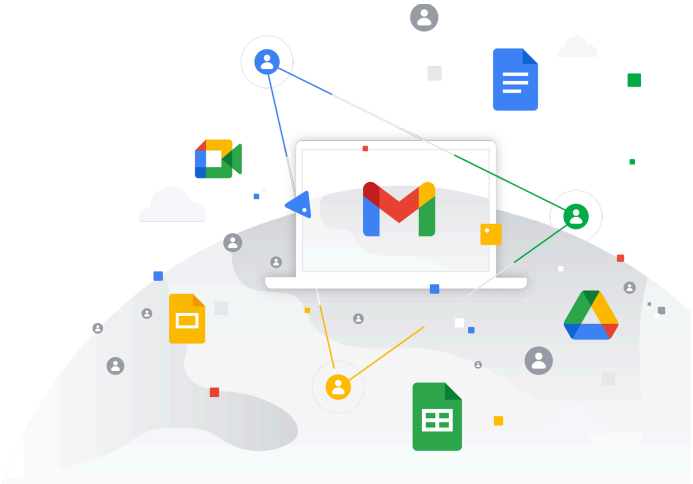
Google for Education

教育現場の日常に潜む情報漏えいの脅威と Google for Education を使った対策

学校におけるクラウド データ管理: 情報漏えいを防ぐために

2024 年も日本国内の学校において、個人情報を含む様々な情報漏えい事件が発生しました。これらの事件は、人的ミス、システムの脆弱性、サイバー攻撃など、様々な原因で発生しており、学校における情報セキュリティ対策の重要性を改めて認識させるものとなりました。特に、近年はランサムウェアによる被害が拡大しており、2024 年 12 月 15 日時点で国内組織でのランサムウェア被害公表件数は過去最多です。 また、標的型攻撃メールによる被害も増加しており、学校もその標的となる可能性があります。

本ガイドは、クラウド上のデータ管理と運用における情報漏えいリスク低減を目的としています。データの重要性に応じて適切な管理を行うことが重要です。



2025 年 1 月版

目次

情報漏えいの脅威とは

情報漏えいとは、意図的または偶発的に機密情報が外部に流出することを指します。教育現場における情報漏えいは、児童・生徒や教職員のプライバシーを侵害するだけでなく、学校の信頼性やセキュリティにも深刻な影響を及ぼします。

情報漏えいが引き起こすリスク

- **個人情報の悪用**: 児童・生徒や教職員の個人情報が漏えいすると、詐欺やなりすましに利用される可能性が高くなります。
- **教育機関の信頼性低下**: 情報漏えいが発覚すると、保護者や地域社会との信頼関係が損なわれ、学校の評判が悪化します。
- **法的・規制上の問題**: 情報漏えいが発生した場合、学校は法的責任を問われる可能性があり、罰金や訴訟が発生することもあります。

情報漏えい対策の課題

テクノロジーによる対策を施したからといって、情報漏えいのすべてを防ぐことはできません。例えば、無許可の SNS から情報が漏れてしまうといったシャドー IT 、印刷した資料の紛失といったアナログでの脅威などは、教育現場でいくらテクノロジーを活用した対策を施しても、防ぎ切ることはできません。

そのため、このドキュメントで記載するような技術的な設定に加えて、文部科学省の作成する「教育情報セキュリティ ポリシーに関するガイドライン」を参考にしながら、各都道府県・市区町村の規定に則った運用規則を定めることと、セミナーやトレーニングを通して、セキュリティに関する知識の定着、アップデートを定期的に確認することが重要です。

情報漏えいの主な原因と対策

2024 年に発生した情報漏えい事件を分析した結果、主な原因は以下の 3 つに分類できます。

01

人的ミス

多くの情報漏えい事件は、人的ミスに起因しています。 これは、教職員の情報セキュリティ意識の不足や、個人情報取り扱いに関する監査規定の不備など様々な原因が考えられます。

具体的な事例:

- USB メモリやデバイスの紛失
- 書類の置き忘れ
- メール誤送信
- 修学旅行中の資料紛失
- 教員の不注意によるアクセスコードの誤提示

主な対策:

- データ損失防止（DLP）ルール
- 信頼ルール
- ラベル
- USB 制御
- リモート消去
- ドライブ共有
- 教職員へのトレーニング
  等

02

情報管理体制の不備

情報セキュリティにおける管理体制とは、情報を適切に管理するためのルール、体制、手順などを指します。これが不十分だと、情報が適切に保護されず、漏えいにつながるリスクが高まります。

具体的な事例:

- アクセス権の不適切な設定
- 情報の分類・整理が不十分
- 監査・見直しの不足
- ID とパスワードの統一による無断利用

主な対策:

- 多要素認証
- 組織部門、グループの管理
- ラベル
- データ損失防止（DLP）ルール
- 監査ログ
- セキュリティダッシュボード
- コンテキストアウェア アクセス
  等

03

サイバー攻撃

近年、ランサムウェアや標的型攻撃メールなど、巧妙化するサイバー攻撃による被害が増加しています。 学校も、これらの攻撃の標的となる可能性があります。

具体的な事例:

- 学内ネットワークへの不正アクセス
- 教員 PC への不正アクセス
- マルウェア感染
- ランサムウェア攻撃
- ウェブサイトの改ざん
- フィッシング

主な対策:

- ChromeOS の利用
- 適切なネットワークの設定
  等

Google for Education の機能を活用した対策

アカウント種別と管理

人的ミス、情報管理体制の不備の対策に有効

アカウント種別の適切な使い分け

アクセス権の不適切な設定の対策

Google Workspace for Education（以下、Google Workspace）には、様々なアカウント種別が存在し、それぞれ権限が異なります。学校現場では、以下の種別を適切に使い分けることが重要です。**適切なアカウント管理を行うことで情報漏えいを防ぎ、教職員の業務効率を向上させることができます。**

- 特権管理者
    - Google Workspace 全体の管理権限を持ちます。教育委員会や学校長、情報システム担当者など、組織全体の設定やセキュリティ ポリシーを管理する責任者に付与します。

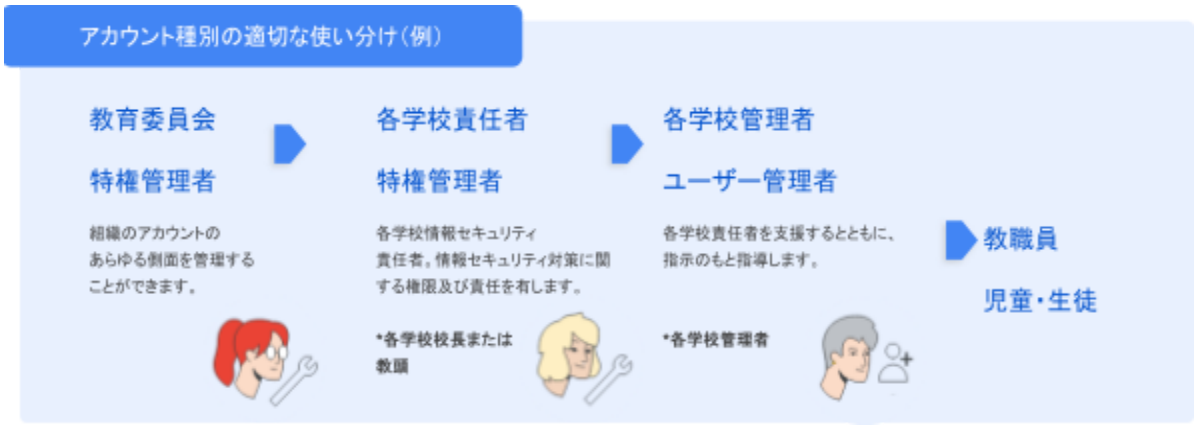
      特権管理者は、具体的には以下のような権限を有します。
        - ユーザーの追加、削除、管理
        - 各種サービス（Gmail、Google ドライブなど）の設定
        - セキュリティ ポリシーの設定（パスワード ポリシー、二段階認証など）
        - 請求およびライセンス管理
        - Google 管理コンソールおよび API へのフルアクセス

      特権管理者は Google Workspace の運用に関わる全ての操作が可能です。そのため、情報漏洩や不正アクセスなどのリスクを考慮し、付与対象者は必要最小限に留め、適切な管理体制を構築することが重要です。一方で、担当者の不在時やアカウントのロックアウトといった緊急時への対応、および不正行為の抑止の観点から、特権管理者は最低 2 名以上配置することを推奨します。特権管理者の責任の重さを理解し、慎重に運用する必要があります。

- グループ管理者
    - 特定のグループ（例: 教員グループ、生徒グループ、部活動グループ）の管理権限を持ちます。各グループの責任者や担当教員に付与することで、グループ内のユーザー管理や共有設定などを適切に行うことができます。
- ユーザー管理者
    - ユーザーの追加、削除、パスワードリセットなどの基本的なユーザー管理権限を持ちます。情報システム担当者や事務職員などに付与することで、日常的なユーザー管理業務を効率化できます。
- ヘルプデスク管理者
    - ユーザー情報の閲覧とパスワードの再設定のみが行えます。情報システム担当者やサポート担当者に付与することで、ユーザーからの問い合わせ対応をスムーズに行うことができます。
- サービス管理者
    - 特定のサービス（例: Gmail、Google ドライブ、Google カレンダー）の設定変更権限を

持ちます。各サービスの担当者に付与することで、サービスごとの設定を適切に行うことができます。

- 一般ユーザー
    - 上記の管理者権限を持たない、教職員や生徒などの通常のアカウントです。



管理権限の委任は、主に 2 つの方法があります。

1. 特定の管理タスクを委任する
2. 特定の組織部門（OU）の管理を委任する

システム全体の管理ができる特権管理者と、組織内の一部の管理タスクの管理権限を持つ管理者を、階層ごとに作成し適切に委任することで、全体の運用がスムーズになり、かつセキュリティを高めることができます。

二段階認証によるアカウント管理

端末の紛失、ID、パスワードの統一による無断利用の対策

管理者や教職員など、重要性の高い情報にアクセスするユーザーは、二段階認証等によるアカウント管理を行うことが有効です。**これにより、従来の認証方式の脆弱性を補い、セキュリティを大幅に向上させることができます。**

組織部門とグループの管理

情報管理体制の不備の対策に有効

組織部門の活用

アクセス権の不適切な設定の対策

組織部門（OU）は、ユーザーを階層的に分類するための機能です。**学校現場では、それぞれの部門に適切なポリシーを適用することで、効率的な管理が可能になります。**Google Workspace アカウントの初期状態では、ベースとなる最上位の組織部門（Organizational Unit = OU）が 1 つ用意されています。この最上位の組織の配下に、用途に合わせて組織の階層構造を作成します。アカウント内のすべてのユーザーおよび端末が、1 つの組織部門（OU）に所属します。

組織部門（OU）は、主に次の用途で使用します。

- ユーザーに対して Google for Education サービス（メール、カレンダーなど）の有効 / 無効を定義
- ユーザー権限（ユーザー ポリシー）の定義
- 端末権限（デバイス ポリシー）の定義

よくある組織部門（OU）構成

Google Workspace のよくある組織部門（OU）構成は、次の 3 パターンです。
いずれのパターンも最下位 OU は学年 / 卒業年度で、クラス単位はグループでの管理を想定しています。

1. **教育委員会の場合 ①（役割ベース）**
   教育委員会の ICT 管理者が、ポリシー設定およびユーザーの追加・削除作業などを一括して行う場合
2. **教育委員会の場合 ②（組織ベース）**
   各学校に、一部のポリシー設定およびユーザーの追加・削除作業などを委任する場合
3. **学校の場合（組織ベース）**
   単一の学校が Google for Education アカウントを利用する場合

Google グループの活用

アクセス権の不適切な設定の対策

Google グループは、グループ内でのコミュニケーションと情報共有をスムーズにするためのサービスです。複数の人々が 1 つのグループ アカウント（メールアドレス）を共有し、情報共有やコミュニケーションを効率的に行えるようにするツールです。グループ アカウントとして利用するだけでなく、**設定を行うための対象とすることができます。組織部門と組み合わせることでより細やかな設定を行うことが可能となります。**

Google グループは、主に次の用途で使用します。

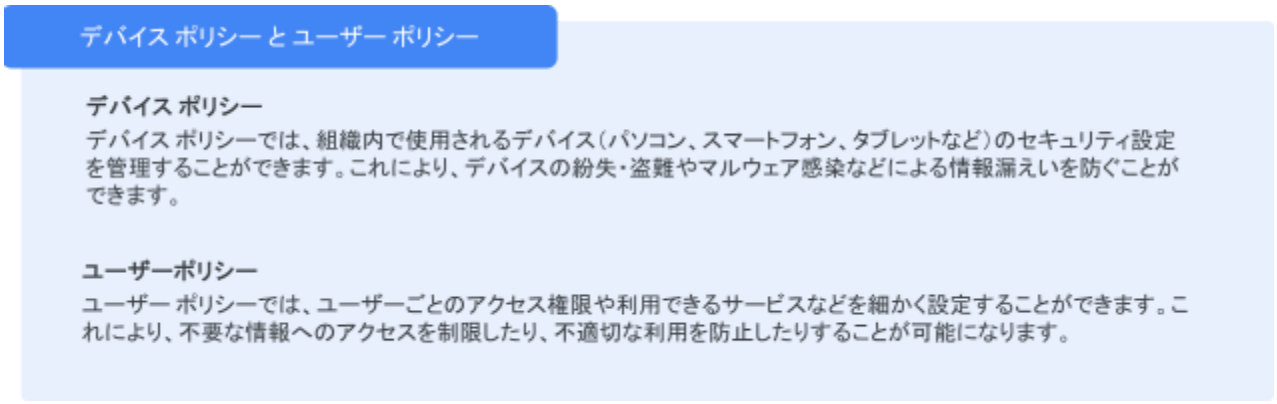
- 組織部門の一部や、横断するユーザーに対する設定を行う対象とする

- 複数人をまとめてカレンダーに招待するなど特定の属性のユーザーをひとまとめにする
- 複数人で対応する必要のあるグループアドレス

デバイス ポリシーとユーザー ポリシー

人的ミス、情報管理体制の不備の対策に有効

組織部門ごとに異なるポリシーを適用することで、**各部門の特性に合わせたセキュリティ対策を行うことができます**。例えば、生徒部門では外部とのファイル共有を禁止したり、特定のアプリの利用を制限したりするポリシーを適用し、教職員部門ではより緩やかなポリシーを適用するなどが考えられます。



デバイス ポリシーの推奨設定例

	防止できる情報漏えいの例	対応するポリシー
1	**故障、紛失対策に有効** 故障や紛失、盗難時にワイプ（出荷時の状態へ初期化）された際にも端末を自動的にドメインに再登録する設定が可能です。 これによって必ず他のポリシーが適用された状態にできます。	端末を強制的にドメインに再登録
2	**故障、紛失対策に有効** 端末の紛失時に遠隔で利用不可能な状態にすることが可能です。 無効になっている端末の画面に表示されるカスタムの文字列を以下のように設定できます： *この端末は [学校名] の資産です。ご返却を*	無効になっている端末の返却手順

	お願いいたします。	
3	**監査・見直し不足対策に有効** ログインすることなく端末を利用できるゲストモードを無効にすることで、必ずポリシーの適用された状態で利用させることが可能です。	ゲストモード
4	**監査・見直し不足対策に有効** ログインできるユーザーを *@yourdomain.edu のように組織のドメインで制限することができます。これによって個人の Gmail アカウントなどでのログインを防ぐことができます。	ログインの制限
5	**監査・見直し不足対策に有効** ユーザーがログアウトした後にローカルに保存された設定やユーザーデータを削除しない	ユーザー データ
6	**監査・見直し不足対策に有効** 組織で指定した期間利用していない端末に関するレポートの送信を設定することができます。これによって予備機などを定期的に確認し、盗難、紛失等に備えることができます。	利用していない端末の通知の報告
7	**監査に有効** デバイスのレポート機能は、学校の端末（パソコンなど）の使用状況を記録し、管理者に報告します。これにより、不正なソフトの有無、不適切な利用、紛失時の追跡、セキュリティ対策の確認などができ、情報漏えいのリスクを減らすのに役立ちます。	ユーザーとデバイスのレポート

ユーザーとブラウザ ポリシーの推奨設定例

	防止できる情報漏えいの例	対応するポリシー
1	**ダウンロード先を制限することで、情報漏えいのリスクを軽減** ChromeOS デバイスでのダウンロード先を必ず Google ドライブに設定し、さらにデータ セキュリティを強化し、監査を容易にするために、ローカル ストレージを無効にできます。これらによって、端末の紛失、盗難やポリシーの適用されないファイルを減らすことができます。	ダウンロード先 ローカル ストレージの構成
2	**不在時の情報漏えいや不正アクセスを防止** ユーザーが席を離れているときに他のユーザーがそのユーザーの Chrome 端末を使わないようにするために、アイドル状態のときは常に画面を自動的にロックするよう設定します。これによって教員端末への不正アクセスを防ぐことにつながります。	画面ロック
3	**複数のユーザーが同一端末を使用する場合の混同を防ぎ、セキュリティリスクを軽減** Chrome ブラウザへの新しいプロファイルの追加を無効にし、学校アカウントでの利用のみとする	プロファイルの追加 予備のアカウントにログインする マルチログイン アクセス
4	**管理対象アカウント以外の利用や閲覧履歴が残らないようにし、情報漏えいのリスクを軽減** ログインすることなくブラウザを利用できるシークレット モードを許可しないことで、必ずポリシーの適用された状態で利用させることが可能です。	シークレット モードの無効化
5	**特定の Web サイトへのアクセスを禁止し、情報漏えいやマルウェア感染のリスクを軽減** URL のホワイトリスト・ブラックリストを指定。独自のウェブ フィルタリング リスト	URL のブロック

	を作って、許可するコンテンツ・ブロックするコンテンツを制御することができます。	
6	**フィッシング詐欺やマルウェア感染からユーザーを保護** それぞれ不正なソフトウェアやフィッシング コンテンツを含む可能性のあるウェブサイトからユーザーを保護する設定になります。	セーフブラウジング・悪意のあるサイト・セーフサーチと YouTube 制限付きモード
7	**機密情報の漏えいを防止** 校務スタッフユーザーのみ、スクリーンショットおよび端末からの印刷を許可。外部ストレージ デバイスは無効化	スクリーンショット・印刷・外部ストレージ デバイス
8	**Chrome のデベロッパー ツールの悪用によるハッキングや拡張機能の改ざんの危険性を回避** Chrome のデベロッパー ツールの使用禁止と拡張機能ページのデベロッパー モードの使用を禁止します。	デベロッパー ツール
9	**監査・機密情報の漏えいを防止** データ管理、ブラウザ、インストール済みアプリのレポートは、学校の端末で何が使われているかを把握するのに役立ちます。不正なデータ持ち出し、不適切なサイトへのアクセス、許可されていないアプリの利用などを早期に発見し、情報漏えいを防ぐことができます。	データ管理のレポート ブラウザに関するレポート インストール済みアプリのレポート

情報セキュリティに基づく資産分類と管理

人的ミス、情報管理体制の不備の対策に有効

マイドライブと共有ドライブについて

アクセス権の不適切な設定の対策

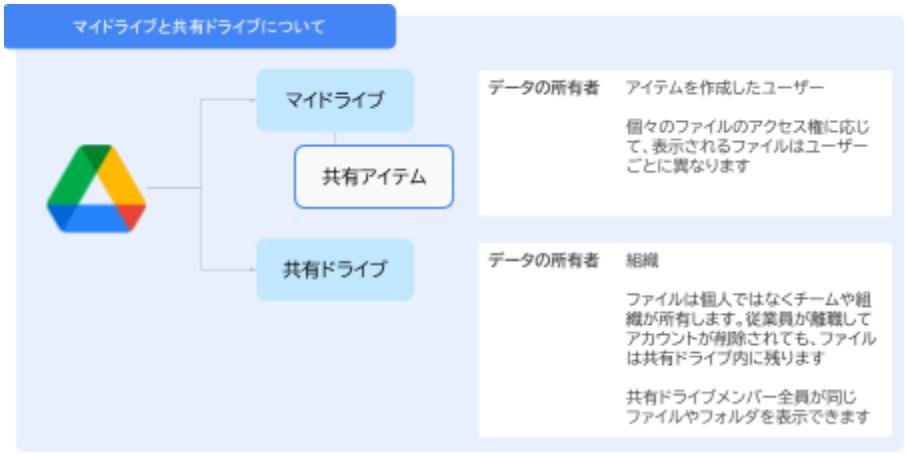
USB メモリや紙媒体など、情報の流れの記録（ログ）の取れない物理的なメディアを使った情報の共有は、情報漏えいのリスクを高めます。Google ドライブを活用することで、ログを残しつつ、アクセス権を用いた適切な情報管理が行えます。
「マイドライブ」「共有ドライブ」とは、Google Workspace の Google ドライブにおけるファイルの保存場所であり、それぞれ異なる特徴を持っています。**学校現場での情報管理を考える上で、これらの違いを理解することは非常に重要です。**以下、それぞれの特徴と違いについて詳しくご説明いたします。

マイドライブ

- **個人のための保存場所**: マイドライブは、個々のユーザーが個人的なファイルやフォルダを保存するための場所です。個人の所有物として扱われ、作成者本人がファイルの所有者となります。
- **個人の管理**: ファイルの作成、編集、削除など、すべての操作はファイルの所有者である個人が行います。他のユーザーとファイルを共有することはできますが、共有相手に対する権限設定も所有者が行うため、誤って生徒のグループや生徒個人に権限を付与すると情報漏洩リスクが発生します
- **退職・異動時の影響**: ファイルの所有者が退職や異動などで組織から離れる場合はそのユーザーのデータの取り扱いについて予め検討する必要があります。

共有ドライブ

- **チーム・組織のための保存場所**: 共有ドライブは、特定のチームや組織全体でファイルを共有し、共同作業を行うための場所です。ファイルやフォルダの所有者は「チーム」または「組織」となり、個人ではありません。
- **チームでの管理**: 共有ドライブ内のファイルは、チームのメンバー全員がアクセスできます。各メンバーには、コンテンツ管理者、投稿者、閲覧者などの役割が割り当てられ、それぞれの役割に応じた権限が付与されます。
- **退職・異動時の影響**: 共有ドライブはチームや組織の所有物であるため、メンバーが退職や異動などで組織から離れても、ファイルは共有ドライブに残ります。これにより、情報の継続性を保つことができます。



Google Classroom を使ったファイル共有

アクセス権の不適切な設定の対策

学習環境においてファイル共有を行う際には、利便性・安全性双方の観点から、Classroom が最適な選択肢です。

Classroom での共有方法を適切に使い分け、**個別にファイルを共有することで操作を誤って発生する情報漏洩を防ぎながら、スムーズなファイル共有を実現できます。**特に、**課題の配布においては、生徒一人ひとりにコピーが作成されるため、情報セキュリティの観点からも推奨される方法です。**

1. 課題としてファイルを配布する

- **方法:** 課題を作成する際に、Google ドライブに保存されているファイル（ドキュメント、スライド、スプレッドシートなど）を添付します。
- **特徴:**
    - 生徒一人ひとりにファイルのコピーが作成され、それぞれが個別に編集できます。課題の提出・回収も Classroom 上で完結します。
    - 生徒は自分の課題のみを閲覧・編集でき、他の生徒の課題を見ることはできません。プライバシー保護の観点からも安全です。
    - 教師は提出状況を一覧で確認でき、採点やフィードバックも Classroom 上で行えます。

2. 資料としてファイルを共有する

- **方法:** 授業ストリームに、Google ドライブに保存されているファイルを添付して投稿します。
- **特徴:**
    - 生徒はファイルを閲覧のみ可能です。編集はできません。
    - クラス全員に一斉に資料を配布する場合に便利です。

3. リンクを共有する

- **方法:** Google ドライブでファイルの共有設定を行い、共有リンクをコピーして Classroom のストリームや課題の説明欄に貼り付けます。特定のウェブサイトを参照させたい場合や、複数のファイルやフォルダをまとめて共有したい場合に便利です。ただし、共有設定を適切に行わないと情報漏洩のリスクがあるため、注意が必要です。

- **特徴:**
    - 共有設定でアクセス権限（閲覧のみ、編集可能など）を細かく設定できます。リンクを知っている人であれば誰でもファイルにアクセスできるような設定も可能です。
    - 外部のウェブサイトへのリンクや、Google ドライブ以外のファイルへのリンクも共有できます。

4. クラスのドライブフォルダを利用する

- **方法:** Classroom の「授業」ページ右上にある「クラスのドライブフォルダ」をクリックすると、そのクラス専用の Google ドライブフォルダが開きます。このフォルダにファイルを保存することで、クラスのメンバー全員とファイルを共有できます。
- **特徴:**
    - フォルダ内のファイルはクラスのメンバー全員が閲覧できます。必要に応じて編集権限を与えることもできます。
    - 生徒が提出した課題ファイルは、このフォルダに自動的に保存されます。
    - ファイルの状況（提出済み、返却済みなど）に応じて、アクセス権や所有権が自動的に変化します。

各共有方法の使い分け例

- **生徒にレポートを作成させる場合:**「課題としてファイルを配布する」
- **授業で使用するスライドを共有する場合:**「資料としてファイルを共有する」
- **参考になるウェブサイトのURLを教える場合:**「リンクを共有する」
- **クラスの活動写真を共有する場合:**「クラスのドライブフォルダを利用する」

なお、Classroom は授業でのみ使用するのではなく、校務や、教職員のセキュリティ意識向上に利用することも効果的です。一例として、教職員向けに Classroom を活用した情報セキュリティトレーニングを定期的に行い、結果を記録することなどが考えられます。

ドライブラベルの作成

ラベルとは、ファイルに付与できる分類の目安で、**ファイルの整理、検索、管理を効率化するために使用されます。**フォルダによる分類に加えて、複数のラベルを自由に付与して、フォルダを横断した分類ができる点が大きな特徴です。

ラベルの種類：Google ドライブには、「標準ラベル」と「バッチラベル」の 2 種類のラベルがあります。

- **標準ラベル**: ユーザーが個別に作成し、ファイルに付与するラベルです。自由に名前を付けることができ、色分けも可能です。
- **バッチラベル**: 管理者が組織全体で利用するために作成するラベルです。標準ラベルと異なり、組織全体で統一されたラベルを使用することができます。学校現場では、管理者（例: 情報システム担当者）が作成し、教職員全員で使用するようなケースが想定されます。

ラベルによる情報漏えい対策

アクセス権の不適切な設定、情報の分類・整理が不十分であることの対策

- **検索性の向上による誤共有の防止**: ラベルを使ってファイルを素早く検索できるため、必要な情報にすぐにアクセスできます。これにより、誤って不要な情報（例えば、過去のデータや関係のない情報）を共有してしまうリスクを低減できます。
- **整理整頓による紛失・見落としの防止**: ラベルを使ってファイルを整理することで、情報が散乱することを防ぎ、管理しやすくすることができます。これにより、重要な情報を見落としたり、紛失したりするリスクを低減できます。重要な情報がどこにあるのか分からなくなることで、不要にコピーを作成し、結果的に情報が拡散してしまうことを防ぐ効果も期待できます。
- **情報共有の効率化によるミスの削減**: 共有ドライブなどでラベルを活用することで、チーム メンバー間での情報共有がスムーズになります。例えば、「〇〇プロジェクト」「レビュー待ち」「承認済み」などのラベルを付与することで、誰がどのファイルにアクセスすべきか、ファイルの現在の状態はどうなっているのかが明確になり、情報共有の際の誤解やミスを減らし、情報漏えいのリスクを低減できます。

データ損失防止（DLP）ルールとラベルを用いた情報資産分類

アクセスコードの誤掲示、資料の紛失、アクセス権の不適切な設定、不十分な情報分類の対策

データ損失防止（DLP: Data Loss Prevention）ルールとは**機密情報や重要データを特定して監視し、漏えいや消失を防ぐシステム**です。ラベルと組み合わせることで柔軟にファイル共有の制御が可能になります。

DLP ルールによる情報漏えい対策

- **ファイルに応じた自動ラベル付与**: キーワードや正規表現を用いて作成されたファイルに自動でラベルを付与することができます。これにより、ユーザーが意識することなく、重要性分類に該当するファイルを分類することができます。
- **ラベルに基づいた外部共有制御**: ファイルに付与されたラベルに応じた外部共有の範囲をルールとして設定できます。これによって重要なファイルの共有をブロックしたり、共有前に警告を表示して注意を促すことができます。
- **スクリーンショットの制御**: 指定した URL のコンテンツでスクリーンショットや動画の撮影を制御する事ができます。これによってファイルの共有を介さない情報の漏えいをブロックしたり、ログを取得したり、注意を促したりすることができます。
- **印刷の制御**: 指定した URL のコンテンツの印刷を制御することができます。これによって重要な情報の物理的な漏えいを防いだり、ログを取得したり、注意を促したりすることができます。
- **コピー＆ペースト**: 指定した URL のコンテンツでコピーした文章や動画などのコンテンツを、指定した URL （例: SNS など）へペーストすることを制御することができます。これによって意図しない機密情報の流出を防いだり、ログを取得したり、注意を促したりすることができます。
- **ビデオ通話アプリなどでの画面共有の制御:** 指定した URL のコンテンツのビデオ通話アプリなどからのキャプチャ（画面共有）を制御できます。これによって形に残らない映像としての共有を防いだり、ログを取得したり、注意を促すことができます。

ドライブとドキュメントでのアクセス権限設定

アクセス権の不適切な設定の対策

管理コンソールから組織部門やグループ別に Google ドライブのファイル共有の設定を行うことができます。生徒や重要な情報を扱うユーザーの組織部門は外部共有を禁止し、グループを使うことで禁止した組織の一部のユーザーだけ外部共有を許可するといった設定を行うことも可能です。

ファイルごとのアクセス権限設定

アクセス権の不適切な設定の対策

Google ドライブに保存しているファイルやフォルダは組織外の Google Workspace のユーザーや同じドメイン内のどのユーザーとも共有できます。またファイルを共有する際に共有相手のファイルに対する権限（編集、コメント、閲覧のみ）を管理できます。ラベルや、DLP ルールと組み合わせることで、組織外のユーザーとの共有も適切に行うことが可能になります。

アプリごとのアクセス権限設定

アクセス権の不適切な設定の対策、不正アクセス

Google Workspace のコンテキストアウェア アクセスとは、学校のデータを安全に守るための機能です。

なぜ、この機能が必要なのか？

例えば、生徒さんが自宅のパソコンで学校の課題をしようとした時、そのパソコンが安全でない場合、大切な学校の情報が外に漏れてしまう可能性があります。

コンテキストアウェア アクセスでできること

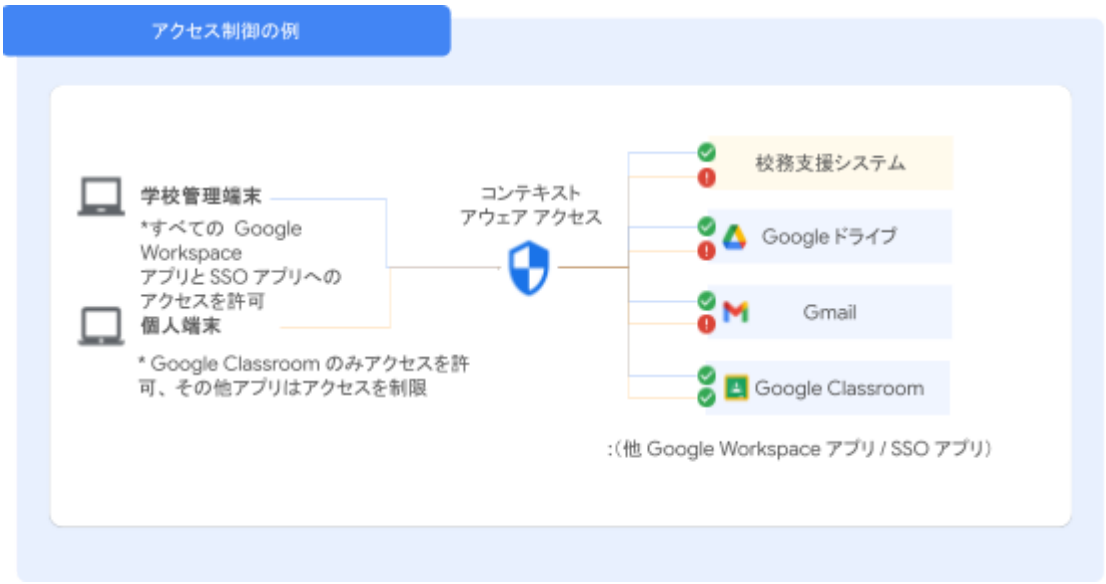
この機能を使うと、**「どこから」「どんなパソコンで」「誰が」アクセスしようとしているか**を**アプリケーションごとに**細かくチェックすることができます。

設定方法の一例

- **場所:** 海外からのアクセスを禁止する
- **端末:** 学校設置者が管理している端末からのみアクセスを許可する
- **時間:** 利用できる時間帯を設定する

なぜ安全なのか？

この機能を使うことで、**不正なアクセスを事前に防ぎ、情報漏洩のリスクを大幅に減らす**ことができます。まるで、学校の入り口にセキュリティーゲートを設置しているようなものです。



信頼ルールを利用してドメイン内の共有を制限する

アクセスコードの誤掲示、アクセス権の不適切な設定対策

目的: 信頼ルールは、Google ドライブ のファイルへのアクセスを制御するための詳細なポリシーを作成できる機能です。これにより、機密情報の保護や規制への準拠を維持するのに役立ちます。

信頼ルールの主な特徴は以下の通りです。

- **柔軟なファイル共有設定: 学校の内外**の様々な関係者とのファイル共有を、細かく設定できます。例えば、**特定の学校の**ファイルは、**連携している他の学校**とのみ共有を許可し、**他の学校との**共有を制限するといった設定が可能です。

- **内部共有の管理: 学校内**で、誰がどのファイルを見たり、使ったりできるかを細かく設定できます。例えば、**先生方の会議で使うファイル**は、**校長先生や副校長先生**など、**限られた先生方のみ**が共有できるようにし、**他の先生方や児童・生徒**には共有しないといった設定が可能です。

- **詳細な制御**: ドライブ の共有設定よりも詳細な制御が可能で、範囲、トリガー、条件、操作のコンポーネントを定義してルールを作成できます。
    - **範囲**: ルールの適用対象となるユーザー（ファイルのオーナーや受信者）。
    - **トリガー**: ルールで許可またはブロックするアクティビティ（ファイルの共有または受信）。
    - **条件**: ファイルの共有相手または受信ファイルのオーナー。
    - **操作**: ルールがトリガーされたときの結果（共有を許可、警告を表示、またはブロック）。
- **ルールの優先順位**: 複数のルールが競合する場合、共有をブロックするルールが最も優先され、次に共有を許可する、最後に共有を許可して警告を表示するの順で優先されます。

- **組織構造に合わせた設定**: 組織部門やグループごとに異なる共有ルールを設定できるため、組織の構造に合わせた柔軟なアクセス制御が可能です。

信頼ルールは、従来のドライブの共有設定に代わる機能であり、より詳細な設定を可能にします。信頼ルールを有効にすると、ドライブの共有設定は無効になり、作成したルールが適用されます。信頼ルールはいつでも無効化して、ドライブの共有設定に戻すことも可能です。

ドメインのホワイトリスト

アクセス権の不適切な設定、不正アクセス、フィッシング、マルウェア対策

目的: 信頼できるドメインとのみ外部共有を許可することは、情報セキュリティの観点から非常に重要です。以下にその理由をまとめます。

- **機密情報の保護**: 組織の**機密情報**が、**許可されていない外部の組織**に漏えいするリスクを大幅に低減できます。**許可リスト**に登録されたドメインとのみ共有を許可することで、**情報漏えいのリスク**を抑制します。

- **フィッシングやスパム対策**: **信頼できるドメイン**からのアクセスのみを許可することで、**悪意のある第三者**によるフィッシング攻撃やスパムメールのリスクを軽減できます。これにより、**不正アクセス**や**マルウェア感染**のリスクを減らせます。

- **共同編集の安全性の確保**: **許可されたドメイン**とのみファイルの共有や共同編集を行うことで、**安全なコラボレーション環境**を維持できます。

- **アクセス制御の強化**: **信頼ルール**と組み合わせることで、**ファイルへのアクセス権**をより細かく制御できます。例えば、特定の学校のファイルは、他の特定の学校とのみ共有を許可するといった設定が可能です。これにより、**組織の構造**や**業務内容**に合わせた、**柔軟なアクセス制御**が実現します。

- **コンプライアンスの遵守**: **業界標準**や**規制**に準拠するために、**外部との情報共有**を制限する必要がある場合、**許可リスト**を使用することで、**コンプライアンス**を遵守できます。

- **一元管理**: **許可リスト**は、**ドライブ**、**Classroom**、**Google Chat**、**Looker Studio** など、複数の Google Workspace サービスで共有されるため、**一元的な管理**が可能です。これにより、**管理の手間**を削減し、**設定の不整合**を防ぐことができます。

信頼できるドメインとのみ外部共有を許可することは、組織の**情報資産**を保護するための重要なセキュリティ対策です。**適切な設定**と**運用**によって、**安全な情報共有**と**コラボレーション**を実現できます。

この設定は、**信頼ルール**と組み合わせて使用することで、より詳細な**アクセス制御**が可能になります。例えば、特定の組織部門やグループに対して、**許可リスト**に登録されたドメインとのみファイルの共有を許可するといった、柔軟なルールを設定できます。

監査ログを用いた監査

監査・見直しの不足、教員端末への不正アクセス対策

目的: 組織内のユーザーおよび管理者のアクティビティを詳細に記録し、**情報漏えいにつながる可能性のある不正行為やセキュリティ インシデント発生時の追跡と原因特定**を可能にすることです。

- **記録対象**:
    - **管理者の操作**: Google 管理コンソールで行われた設定変更やユーザー管理などの操作を記録し、**意図しない設定変更や不正な管理者権限の利用**を監視します。
    - **ユーザーの操作**: Google ドライブでのファイル操作、メールの送受信、ログイン履歴などを記録し、**不審なファイル共有、不正なメール送信、不正アクセス**を検知します。
    - **システムイベント**: 認証の失敗、デバイスの変更、ルール違反など、システム内で発生したイベントを記録し、**セキュリティ侵害の兆候**を把握します。
- **対策方法**:
    - **インシデント調査**: **セキュリティ侵害やデータ漏えい**が発生した場合、監査ログを分析することで、**情報漏えいの原因を特定**し、**影響範囲を把握**します。
    - **コンプライアンス遵守**: 監査ログは、**業界標準や規制**への準拠を証明するために必要な**証拠**となり、**法規制違反による情報漏えいリスク**を低減します。
    - **不正行為の発見**: **不審なアクティビティや不正な操作**を監査ログから検出し、**早期に対応**することで、**情報漏えいの未然防止**につなげます。
    - **セキュリティ対策の評価**: 監査ログを分析することで、**セキュリティ ポリシーや設定**の有効性を評価し、**情報漏えい対策の改善**につなげます。例えば、**DLP ルール**違反のログを分析することで、**機密情報の共有を制限**するルールの効果を評価できます。
    - **内部不正の監視**: 従業員による**機密情報の持ち出しや不正なアクセス**を監視し、**内部からの情報漏えいリスク**を低減します。
- **アクセス権**: 監査ログにアクセスするには、**監査と調査の権限**を持つ管理者である必要があります。
- **データ保持期間**: 監査ログの種類によって、**データの保持期間**が異なります。

セキュリティ ダッシュボードを用いた可視化

監査・見直しの不足、サイバー攻撃への対策

目的: 組織の**セキュリティ状況を視覚的に把握**し、**情報漏えいの可能性のある脅威を早期に検出**するためのツールです。

- **表示内容**:
  - **ファイル共有**: 外部とのファイル共有状況、共有イベント数、閲覧回数を表示し、**意図しない機密情報の共有や公開**を監視します。
  - **認証**: 認証済みメールと未認証メールの割合を表示し、**フィッシング メールやなりすましメール**による情報漏えいリスクを把握します。
  - **暗号化**: TLS で暗号化されたメールの割合を表示し、**通信経路での傍受による情報漏えいリスク**を監視します。
  - **メール配信**: 受信メールの量、迷惑メール、フィッシング メール、不正なソフトウェアとしてマークされたメールの件数を表示し、**メール経由の情報漏えいリスク**を把握します。
  - **デバイスセキュリティ**: デバイスのパスワード入力失敗回数、デバイスの不正使用、不審なアクティビティを表示し、**デバイス紛失や不正アクセスによる情報漏えいリスク**を監視します。
  - **OAuth**: OAuth スコープの付与状況、OAuth 権限付与アクティビティ、新しく OAuth 権限が付与されたアプリを表示し、**不正なアプリによる情報アクセスリスク**を監視します。
  - **その他**: DLP インシデント、上位ポリシー インシデント、ユーザー レポートなどを表示し、**機密情報の漏えい状況**を把握します。
- **対策方法**:
  - **セキュリティ リスクの監視**: ダッシュボードを通じて、**組織全体のセキュリティ リスク**を継続的に監視し、**情報漏えいにつながる可能性のある兆候**を早期に発見します。
  - **脅威の早期発見**: **不審なアクティビティやセキュリティ インシデント**の兆候を早期に検出し、**迅速に対応**することで、**情報漏えいを未然に防ぎ**ます。
  - **セキュリティ対策の評価**: **既存のセキュリティ対策**の効果を評価し、**情報漏えい対策の改善点**を特定します。例えば、**外部共有**が多い場合は、**共有設定**を見直し、**信頼ルール**を適用して**情報漏えいリスクを低減**できます。
  - **データに基づいた意思決定**: ダッシュボードのデータに基づいて、**セキュリティ ポリシーや設定**を調整し、**情報漏えい対策を強化**します。
  - **カスタムグラフ**: **セキュリティ調査ツール**の検索結果に基づいて**カスタムグラフ**を作成し、ダッシュボードで**より詳細な分析**を行い、**情報漏えいに関連する特定の脅威**に焦点を当てます。
  - **傾向分析**: ダッシュボード上で、**データの経時的な変化や傾向**を把握し、**情報漏えいリスクの変化**を監視します。
  - **セキュリティ調査ツールとの連携**: 一部のレポートは**セキュリティ調査ツール**と連携しており、ダッシュボードから**直接調査を開始**し、**情報漏えいインシデントに迅速に対応**します。
- **カスタマイズ**: ダッシュボードは、**グラフの追加、非表示、並び替え**など、ユーザーごとにカスタマイズでき、**重要な情報漏えいリスク**に焦点を当てた監視が可能になります。

ネットワーク設定、Chrome のセキュリティ

サイバー攻撃対策に有効

ネットワーク設定

ネットワーク セキュリティ

ChromeOS は、ネットワークを信頼しないゼロトラストの原則に基づいて設計されており、どのようなネットワーク環境でも高いセキュリティを維持できます。**ChromeOS 自体のセキュリティ機能が非常に強力であり、また様々なネットワーク環境で利用できるようにネットワーク設定の互換性もあります。**

- **Wi-Fi 自動接続**: 管理対象ネットワークへの自動接続を有効にすることで、**ユーザーが誤って危険なネットワークに接続**するのを防ぎます。
  例えば、学校から端末の持ち帰りを許可せずに、学校が**指定したネットワークにのみ接続**を許可する場合などに便利です。
- DNS の乗っ取りやルーターを踏み台にする攻撃のように、**ネットワーク インフラ自体の脆弱性**を突く脅威に備えて、**最新の Wi-Fi テクノロジー**に対応したデバイスを選ぶことが望ましいです。

ChromeOS のセキュリティ

サイバー攻撃対策

ChromeOS のセキュリティ機能は、**ランサムウェア攻撃やウイルス攻撃の成功例が報告されていない**、非常に安全性の高い OS です。ITに詳しくない方でも、Chromebook を導入することで、ウェブサイトの改ざん、フィッシング、マルウェア感染、ランサムウェア攻撃などのサイバー攻撃から、情報漏洩のリスクを大幅に低減できます。

Chromebook がこれらの脅威からどのように保護するのか、その具体的な機能と対策を説明します。

- **ウェブサイトの改ざん、フィッシング対策**
  - **ChromeOS は、基本的に Web アプリしか使えないように作られています。**
    そのため、パソコンに直接アプリをインストールして使う従来の方法と比べて、ウイルスやランサムウェアなどの攻撃を受けるリスクが減ります。
    サンドボックス化: すべてのアプリはブラウザのサンドボックス内で動作します。これにより、**たとえ悪意のある Web ページを開いたとしても、他のアプリやシステムに影響を与えることがありません。**マルウェアはサンドボックス内に隔離され、システムやデータにアクセスすることが困難です。
  - **Chrome のセーフブラウジング**: Chrome には、**リアルタイムでセキュリティ スキャンを行い、危険なウェブサイトやダウンロード、拡張機能へのアクセスを警告・ブロックする**機能があります。これにより、フィッシングサイトへのアクセスや不正なファイルのダウンロードを未然に防ぐことができます。
  - **サイトごとのデータ管理**: ChromeOS では、**画面共有、スクリーンショット、コピー＆ペーストなどの操作を、サイトごとに許可・禁止する**ことができます。これにより、機密情報が特定のサイトから漏洩するリスクを低減できます。

- **マルウェア感染対策**
    - **信頼できない実行ファイルのブロック**: ChromeOS は、デフォルトで**信頼できない実行ファイルをすべてブロック**します。そのため、メールの添付ファイルや Web サイトから侵入したマルウェアが実行されるのを防ぎます。
    - **OS 領域の読み取り専用**: ChromeOS のシステム領域は読み取り専用になっており、ユーザーやアプリが書き込むことはできません。そのため、**マルウェアが OS を改ざんすることができず、システムは常に Google が配布した状態に保たれます**。
    - **多層防御**: ChromeOS は、ファームウェア、OS、アプリケーション、データの各層で連携してシステムを保護する多層防御を採用しています。この多層防御により、**攻撃者がシステムに侵入するためのハードルが大幅に上がり**、マルウェア感染のリスクを低減します。
    - **自動更新**: ChromeOS は、バックグラウンドで自動的に更新が行われ、**常に最新のセキュリティパッチが適用**されます。これにより、既知の脆弱性を突いた攻撃を防ぎ、常に安全な状態を保つことができます。
    - **EDR（Endpoint Detection and Response）機能**: ChromeOS には EDR 機能が組み込まれており、**マルウェアやシステムの改ざんを検出し、自動的に修復**します。これにより、万が一マルウェアが侵入した場合でも、被害を最小限に抑えることができます。
- **ランサムウェア攻撃対策**
    - **ランサムウェアの実行を阻止**: ChromeOS では、ランサムウェアなどの多くのマルウェアに「実行」する権限を与えません。そのため、**これらの危険なソフトウェアは、ChromeOS では動作することができません**。
    - **確認付きブート**: Chromebook は、起動時に Titan C セキュリティチップによってファームウェアと OS の改ざんを検出し、不正な OS 起動を防止します。これにより、**ランサムウェアが OS を起動時に攻撃することを防ぎます**。
    - **自動復旧**: システムに異常が発生した場合、バックアップ OS に自動的に切り替わり、数分で復旧します。これにより、**ランサムウェア攻撃によってシステムが使用不能になった場合でも、迅速に業務を再開**できます。
- **情報漏洩対策**
    - **ユーザーデータの暗号化**: ユーザーデータは、ユーザーごとに異なる鍵で暗号化され、Titan C チップ内に安全に保管されます。これにより、**たとえ端末が盗難されても、データが復号化されるリスクを大幅に低減**できます。
    - **データ管理**: ChromeOS では、**画面共有、スクリーンショット、コピー＆ペーストなどの操作を、サイトごとに許可・禁止する**ことができます。これにより、機密情報が不正に持ち出されるリスクを減らすことができます。
    - **Chrome の脅威対策**: Chrome の脅威となるアクティビティの発生件数、データ保護ルールごとのインシデント数、リスクの高いユーザーやドメインを監視することで、**情報漏えいリスク**を可視化し、**早期に対策**を講じることができます。
    - **信頼できない実行ファイルのブロック**: ChromeOS はデフォルトで信頼できない実行ファイルをブロックすることで、**ランサムウェア**や**マルウェア**の実行を防ぎます。

更新履歴

- 2025 年 1 月 27 日 作成

便利なリンク集

- Google for Education GIGA School
- Google Workspace セキュリティ チェックリスト
- ChromeOS セキュリティ ガイド
- Google Workspace 管理者ヘルプ
- Chrome Enterprise and Education ヘルプ
- Chrome Enterprise and Education ヘルプ コミュニティ
- Chromebook ヘルプ
- Google Workspace for Education 管理者向けチュートリアル動画
- Chromebook のセキュリティ強化のためのベスト プラクティス ガイド
- サイバーセキュリティ ガイドブック（小中高教育機関向け）