Google for Education

Google Workspace for Education

機密データの管理およびデータ漏洩の防止チェックリスト

Google Workspace for Education の有償エディション（Education Standard、Teaching and Learning Upgrade、Education Plus）は、教育向けにカスタマイズされたエンタープライズ級のツールを備えており、革新的な学習環境の実現に役立ちます。ここでは、機密データを管理し、データ漏洩を防止するための対策をご紹介します。

> Google Workspace for Education のご検討は初めてですか？
>
> エキスパートが詳しくご案内しますので、こちらからお問い合わせください。

Google Workspace 管理者の方には、機密データを管理するために以下のような基本的対策を行っていただくことをおすすめいたします。

- Gmail とドライブのデータ損失防止（DLP）を有効にする。DLP を使用すると、ユーザーが共有できるコンテンツを管理者が指定することができ、クレジット カード番号や個人識別番号といった機密情報の意図せぬ漏洩を防ぐことができます。
- 管理者アカウントのセキュリティ強化に役立つおすすめの方法を確認し、Workspace アプリ全体に設定を適用する際にこちらのセキュリティ チェックリストの手順を行う。[セキュリティの状況] ページでは、セキュリティ設定を監視し、ベスト プラクティスに基づくおすすめの対策を確認することもできます。
- ユーザーのプライバシーを保護するための管理者権限を設定する
- ユーザーが教育機関を離れた後にデータ セキュリティを確保する
- ドメイン内で特定のアクティビティが発生したときに通知を受け取るようにルールを設定する