Provii!!

ご利用マニュアル

（Audit Logs機能）

令和6年9月18日

株式会社フライトソリューションズ
Flight Solutions

目　次

1. はじめに

このたびは、弊社のサービスであるProvii!!（以下、当アプリケーション）をお申込みいただき、誠にありがとうございます。

今後もお客様の満足を第一と考え、製品及びサービスを提供することで、皆様のお役に立てるよう努力してまいります。

本マニュアルでは、監査ログ機能の詳細について記載しております。
「利用マニュアル（共通編）」をご確認のうえ、本マニュアルをご参照ください。
また、別機能の詳細については、各機能マニュアルをご確認ください。

監査ログ機能をご利用いただくにはオプション契約が必要となります。
オプション契約につきましては弊社サポート窓口までお問い合わせください。

2. システム概要

当アプリケーションの監査ログ機能は、*”Google Workspace™”*の監査ログを抽出しGoogleドライブへ格納するためのクラウドサービスとなります。

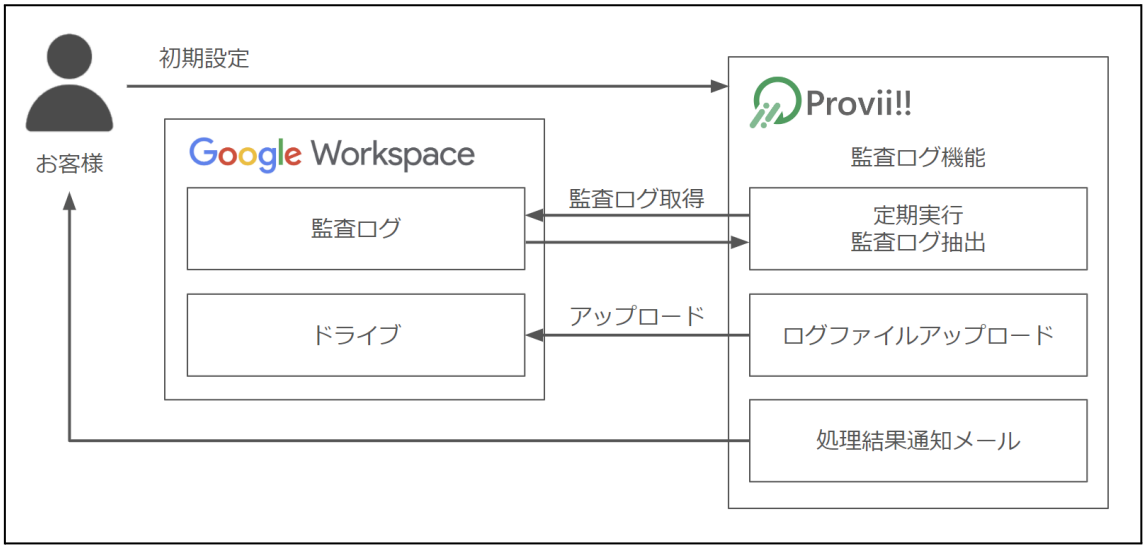
※監査ログではGoogleの各アプリごとに「いつ」「だれが」「何をした」といった操作ログの取得ができます。

「5. 初期設定」を実施後、監査ログ機能では以下の処理が定期的に実行されます。
処理の詳細は「4. 処理内容」をご確認ください。

処理	内容	実行時間
①監査ログ抽出	Google Workspaceの監査ログを抽出する	0:15
②アップロード	抽出したログファイルを初期設定で指定したドライブにアップロードする	監査ログ抽出完了後
③処理結果通知メール	前日の処理結果を集計してメール送信する	9:00

処理の概要図

処理の流れは以下のようになります。



3. 制限事項

- 監査ログ機能の利用につきましてはオプション契約が必要となります。
- *”Google Workspace™”*の契約プランによって、監査ログを取得できるアプリは異なります。

*Google Workspace™*は、*Google LLC*の商標です。

4. 処理内容

監査ログ機能の処理内容となります。
各画面の項目やステータスについては「6. ご利用方法」をご確認ください。

4.1. 監査ログ抽出

4日前の監査ログを抽出します。
ログファイルは各アプリごとに1時間間隔で分割しています。

4.2. アップロード

監査ログの抽出完了後、ログファイルをドライブへアップロードします。
ログのデータ量によってはログファイルが複数生成される場合があります。

ドライブのアップロード先

アップロード先のフォルダは、初期設定にてドライブIDを用いて指定します。
ログの対象日付に該当する以下階層のフォルダにファイルをアップロードします。

階層：指定フォルダ＞アプリ名フォルダ(※)＞年フォルダ＞年月日フォルダ＞ログファイル

※各アプリのフォルダ名は以下の通りです。

アプリ名	フォルダ名
アクセスの透明性	access_transparency
管理者	admin
カレンダー	calendar
Google Chat	chat
ドライブ	drive
GCP	gcp
Currents	gplus
グループ	groups
Groups Enterprise	groups_enterprise
Jamboard	jamboard
ログイン	login
Google Meet	meet
デバイス	mobile

アプリ名	フォルダ名
ルール	rules
SAML	saml
トークン	token
ユーザー アカウント	user_accounts
コンテキストアウェア アクセス	context_aware_access
Chrome	chrome
データポータル	data_studio
Google Keep	keep

アップロードフォルダの作成

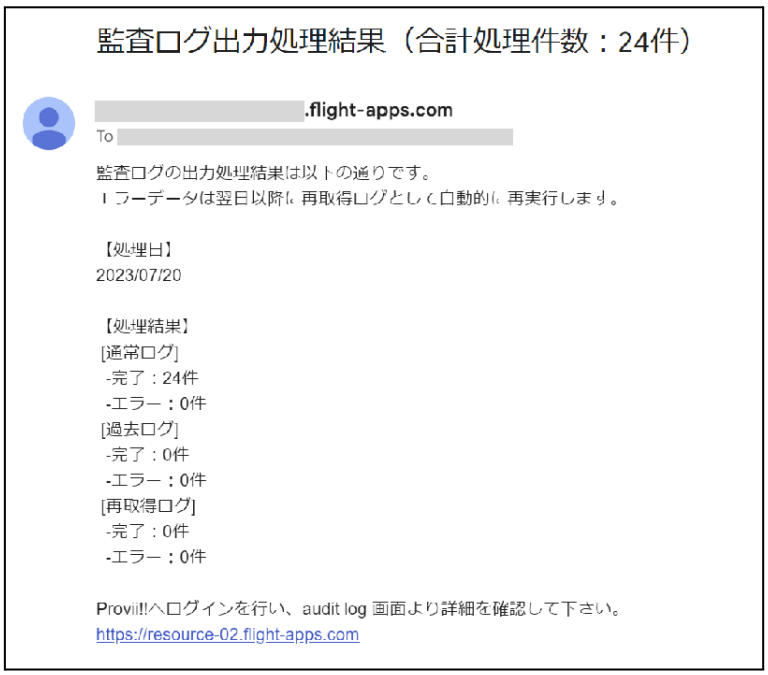
初回実行時や指定フォルダ変更後などでアップロード先のフォルダが存在しない場合、アップロード処理にてフォルダが自動で作成されます。
ただし、本機能の仕様上、同一名フォルダが複数作成されることがあります。

同一名フォルダが複数存在する場合は、最も古い作成日時のフォルダへログファイルがアップロードされます。
最も古い作成日時以外のフォルダについては、フォルダ内にログファイルがアップロードされていないことを確認のうえ、手動にて削除をお願いいたします。

4.3. 処理結果通知メール

初期設定にて指定したメール宛先へ、前日の処理結果を集計したものを送信します。
以下に該当するログの件数が記載されます。

- 通常ログ（出力完了件数、エラー件数）
- 過去ログ（出力完了件数、エラー件数）
- 再取得ログ（出力完了件数、エラー件数）



5. 初期設定

監査ログ機能を利用するための初期設定となります。

※必ず「利用マニュアル（共通編）」に記載の初期設定を行ったうえで、本設定を実施してください。

5.1. Drive SDKの設定

監査ログ機能を利用する前に、Google Workspaceの管理コンソールから設定を行う必要があります。

【設定手順】

1. Google Workspaceに特権管理者アカウントでログインし、管理コンソールへアクセスします。

   （URL：https://admin.google.com/）

2. サイドメニューから、「アプリ ＞ Google Workspace ＞ ドライブとドキュメント」を選択し、「機能とアプリケーション」を押下します。

3. Drive SDKの設定を許可して、保存します。

5.2. Audit Log Settings画面の設定

バックアップデータ格納場所や自動実行時のユーザーを設定します。

【設定手順】

1. 当アプリケーションへログイン後、サイドメニューからAudit Log Settingsを押下し、Audit Log Settings画面へ遷移します。

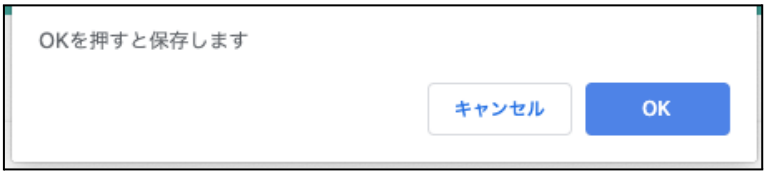
2. 必須項目に適宜値を設定します。

項目名	説明
監査ログ出力処理を有効にする	チェックをオンにした場合、監査ログ出力処理が実行されます。
実行ユーザー	必須。当アプリケーションにログイン済みの特権管理者のメールアドレスを入力してください。
ドライブID	必須。ログファイルの保存先となるドライブIDを入力してください。 ※ドライブのURLのスラッシュから後ろ部分がIDです。 https://drive.google.com/drive/folders/[ドライブID] ※マイドライブ、共有ドライブ、どちらも設定可能です。 ※実行ユーザーにアクセス権がある必要があります。
メール宛先	必須。処理結果通知メールを送信するメールアドレスを入力してください。 ※カンマ区切りで複数設定できます。
過去の監査ログを取得	抽出しない：毎日4日前の監査ログを取得します。 抽出する：4日前の監査ログ（通常ログ）取得に加えて、60日前の監査ログ（過去ログ）を取得します。 ※過去ログが通常ログに追いついた際に「過去データ処理停止通知」メールが送信されます。必要に応じて「抽出しない」に変更してください。
アプリ ・アクセスの透明性 ・監理者 ・カレンダー ・Google Chat ・ドライブ ・GCP(※1) ・Currents ・グループ ・Groups Enterprise ・Jamboard(※2) ・ログイン ・Google Meet ・デバイス ・ルール ・SAML ・トークン ・ユーザーアカウント ・コンテキスト アウェア アクセス ・Chrome ・データポータル ・Google Keep	対象アプリの監査ログを出力する場合は「出力する」を選択します。 (※1)GCPのログはGoogle Workspaceの仕様により、監査ログには出力されません。 (※2)Jamboardのログ取得にはJamboardライセンスが必要です。

[アプリ名]の 出力ファイル名	出力ファイル名を入力してください。 使用できる文字列は半角英数字記号(ハイフン、アンダースコア)になります。 ※"{設定値}_YYYYMMDD_hhmmss_{time zone}.json"の形式で出力されます。

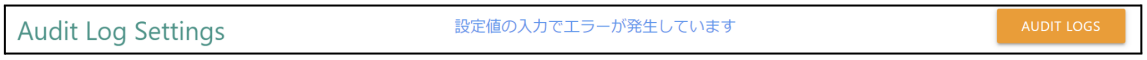
3. 設定を変更後[保存]ボタンを押下します。

4. 確認画面の[OK]を押下すると設定が登録されます。



5. 設定に成功すると「設定を変更しました」と表示されます。

6. 設定に失敗すると「設定値の入力でエラーが発生しています」と表示されます。エラー内容を確認し、再設定をお願いいたします。

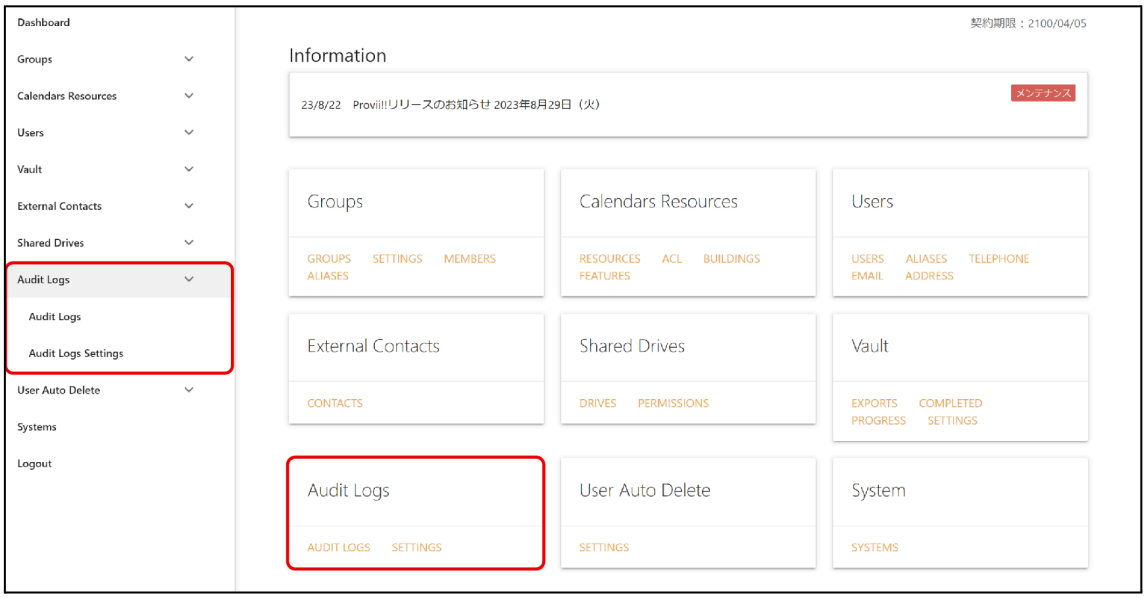


6. ご利用方法

監査ログ機能の利用方法です。

サイドメニューまたはDashboard画面のAudit Logsカードのオレンジ色のリンクから、各画面へ遷移できます。

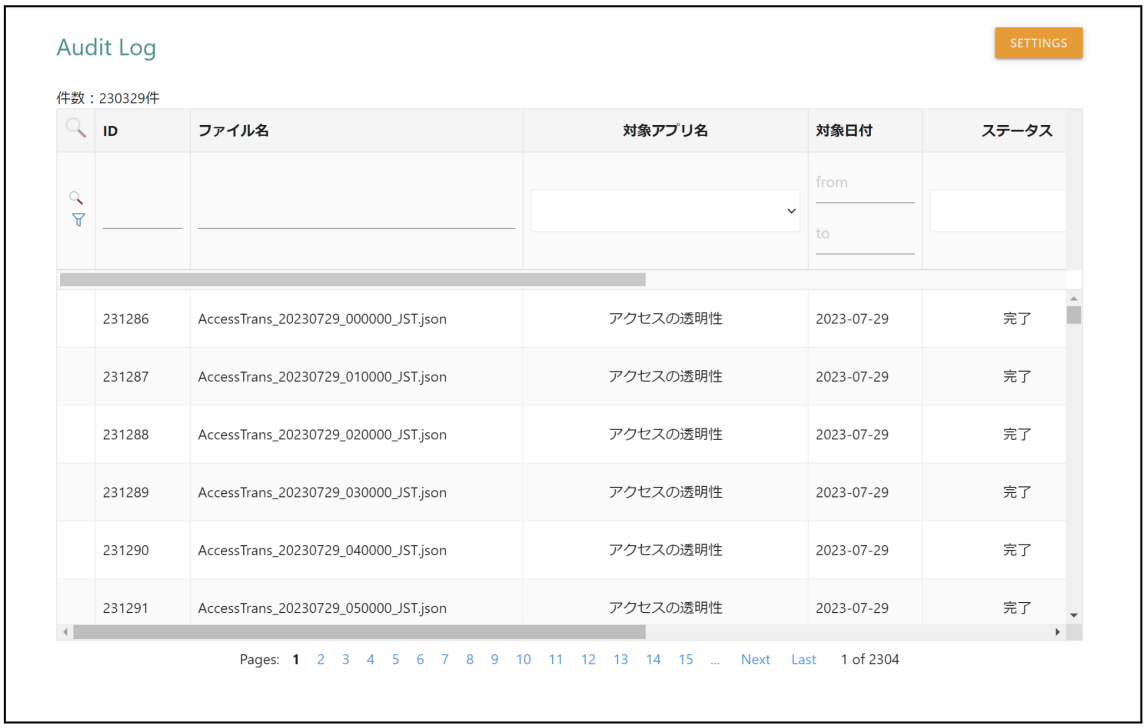
※オプション契約をしていない場合は、Audit Logsカードが非活性になり、監査ログ機能は使用できません。



※画像は 2023/8/23 時点のものです。

6.1. Audit Logs

Audit Logs画面では抽出した監査ログのデータを一覧で確認することができます。



リソース情報の一覧画面には以下の機能があります。

フィルタ

- 左側の大きい虫眼鏡マークを押下すると、フィルタの表示/非表示を切り替えます。
- 項目名の下の入力欄にキーワードを入力もしくは選択し、左側の小さい虫眼鏡マークを押下すると絞り込みを実行します。

  ※キーワードは部分一致で検索されます。
  （取得件数のみ完全一致検索となります。）
  ※キーワードを複数項目設定するとAND検索になります。

- 日付検索の書式は「YYYY-mm-dd」になります。
- 左のロートマークを押下するとフィルタの値がリセットされます。

ソート機能

- 項目名を押下するとソートを行います。

  ※複数項目のソートは行うことができません。

メッセージリンク

- ドライブに格納されたログファイルへ遷移します。
  ※ログの抽出が完了した場合にリンクが表示されます。

ボタン

- SETTINGSボタン：Audit Log Settings画面に遷移します。

Audit Logs画面の内容

抽出した監査ログのデータが表示されます。

項目	内容
ID	ログのID
ファイル名	ログファイルの名前 出力ファイル名_YYYYMMDD_hhmmss_{time zone}.json
対象アプリ名	対象アプリの名前
対象日付	ログの日付
ステータス	処理状況
メッセージ	正常終了：ログファイルの格納先リンク エラー発生：エラーメッセージ
取得件数	ログの取得件数
過去データ	過去：設定画面で「過去の監査ログを取得」を設定した場合 に出力されるデータ 通常：上記以外のデータ
更新日	更新した日付

ステータス

ステータスには以下の種類があります。

ステータス	説明	備考
ログ抽出中	監査ログ抽出中	
格納ドライブ確認中	ログファイルの格納ドライブを確認中	
アップロード中	ドライブへログファイルをアップロード中	

ステータス	説明	備考
完了	アップロードが正常に完了	
ログ抽出エラー	ログ抽出時のエラー	翌日のログ抽出処理で 再実行されます。
ドライブエラー	格納ドライブ確認中のエラー	翌日のアップロード処理で再実行されます
アップロードエラー	アップロード中のエラー	翌日のアップロード処理で再実行されます
予期せぬエラー	予期せぬエラーが発生	サポートまでお問い合わせください

※エラー内容はAudit Logs画面のメッセージ項目、またはGoogle同期ログをご確認ください。

取得件数

Google Workspaceの監査ログ上で表示されるログ件数と、Audit Logs画面で表示されるログの取得件数が異なる場合があります。
件数が異なる際、以下の場合があります。

アプリ名	件数が異なる場合
管理者	複数件のログイベント「グループ設定の変更」はProvii!!上は1件のログとして出力されます。
カレンダー	ログイベント「予定の作成」「予定へのゲストの追加」はProvii!!上は1件のログとして出力されます。
ドライブ	ログイベント「ストレージ使用量の更新 」がGoogle Workspaceの監査ログには表示されません。
	ログイベント「編集」「名前を変更」はProvii!!上は1件のログとして出力されます。
	ログイベント「作成」「作成時に付けられたラベル」はProvii!!上は1件のログとして出力されます。
グループ	ログイベント「基本設定の変更」「ACLの変更」はProvii!!上は1件のログとして出力されます。
Groups Enterpirse	ログイベント「ユーザーの削除」「メンバーの削除」はProvii!!上は1件のログとして出力されます。

※1件にまとめて出力されるイベントログは、同時間帯に行われたイベントログに限ります。

7. 問い合わせ先

操作が継続不可能な状況に陥った場合や、操作や対応方法が分からない状態に陥った等のトラブルが起きた際は、お手数ですが下記の弊社サポート窓口までご連絡ください。

※ お問い合わせ内容によっては対応まで日数をいただく場合があります。

弊社サポート窓口：provii@flight.co.jp

営業時間：平日 10時-18時