

Google Drive データアクセス条件

この条件は、顧客組織の承認済みユーザーまたは管理者が、顧客組織の文書ワークフローのために Google Drive を接続する場合に DynamicMail が要求する Google Drive アクセスについて説明します。

この文書は Google Drive のみを対象とします。同じ Google Workspace アセットファミリーの Gmail 読み取り専用条件と併せて使用されることを想定しています。

スコープ

DynamicMail は、顧客組織の承認済みユーザーまたは管理者が顧客組織の文書ワークフローのために Google Drive を接続する場合に限り、<https://www.googleapis.com/auth/drive> を要求します。これは広範な制限付き Drive スコープであり、接続された Google Drive アカウント内のすべてのファイルを DynamicMail が表示および管理できる可能性があります。これには、ユーザーが所有するファイル、ユーザーと共有されたファイル、フォルダ、およびそのアカウントがアクセスできる共有ドライブのコンテンツが含まれます。

DynamicMail は、顧客組織が選択した、開示済みで表示される Drive 文書ワークフローに限り Drive スコープを使用しなければなりません。openid、email、profile などの Google サインインの ID スコープは、この Drive データアクセス同意とは別のものです。Google でログインすることは、Google Drive アクセスへの同意を意味しません。

DynamicMail がアクセスできるデータ

Google Drive が接続されている場合、DynamicMail は顧客組織が選択したワークフローを提供するために必要な Drive データにアクセスできます。これには以下が含まれます。

- ファイル ID、名前、MIME タイプ、チェックサム、サイズ、タイムスタンプ、説明、ラベル、フォルダ参照、親フォルダ、およびその他のファイルメタデータ。
- 顧客組織の文書を見つけるために必要なフォルダメタデータ、共有ドライブメタデータ、および検索または一覧表示の結果。
- ファイルコンテンツ、プレビュー、サムネイル、エクスポート、ダウンロード、アップロード、および生成または編集されたファイルペイロード。
- 表示される Drive ファイル操作を表示または完了するために必要な場合の共有および権限メタデータ。
- 接続されたアカウントおよび接続状態を確認するために必要な Drive アカунトレベルの概要情報。
- DynamicMail に取り込まれた Drive ファイルの保存コピーまたはキャッシュされた抽出物。
- Drive ファイルから作成された派生データ。例として、OCR テキスト、解析済み文書フィールド、分類ラベル、抽出結果、要約、監査イベント、および文書レコードがあります。

DynamicMail は、表示される Drive 文書ワークフローに関係しない Drive データを要求、閲覧、コピー、ダウンロード、変更、削除、またはその他の方法で処理すべきではありません。

目的

DynamicMail は、顧客組織が選択した Drive 文書ワークフローを提供するために Google Drive データを使用します。想定される目的は以下のとおりです。

- 承認済みユーザーが Drive を文書のソースまたは宛先として接続できるようにすること。
- 製品フローで選択された顧客組織の業務文書を検索、一覧表示、取り込み、ダウンロード、エクスポート、アップロード、または更新すること。
- Drive 文書を抽出、分類し、DynamicMail ワークフローヘルパーティングすること。
- 承認済みの顧客組織ユーザーに、接続、ファイル操作、同期、および処理の状態を表示すること。
- どの Drive 操作が要求され完了したかを示す監査記録および運用ログを維持すること。
- 適用されるポリシーおよび顧客組織との契約で許可されるトラブルシューティング、セキュリティ、不正利用防止、紛争対応、および法令遵守の活動を行うこと。

DynamicMail は、Google Drive データを販売したり、広告またはリターゲティングに使用したり、データブローカーへ移転したり、監視目的で使用したり、信用力または融資適格性を判断するために使用してはなりません。

広範なスコープと最小スコープに関する注記

<https://www.googleapis.com/auth/drive> スコープは、接続されたアカウントで利用可能なすべての Drive ファイルへのアクセスを許可する可能性があるため、広範です。DynamicMail は、製品およびコンプライアンスのレビューにより、実装されたワークフローに対してより狭い Drive スコープでは不十分である理由が文書化されるまで、このスコープを暫定的なものとして扱わなければなりません。

本番利用の前に、DynamicMail は

`drive.file`、`drive.readonly`、`drive.metadata.readonly`、`drive.appdata`、または `drive.appfolder` など、より狭い Drive スコープを評価すべきです。より狭いスコープで表示される機能をサポートできる場合は、リリース前に、要求スコープ、同意記録、OAuth 設定、ソースアセット、レンダリング済みアセット、およびテストを更新しなければなりません。

保持

DynamicMail は、表示される Drive ワークフロー、顧客組織の文書保持設定、監査記録、セキュリティ、紛争対応、または法令遵守に必要な期間に限り、Drive 由来データを保持します。OAuth トークンおよび Drive 操作メタデータは、接続された Drive 統合を運用するため、または必要な監査記録を保持するために必要な期間に限り保持されます。

Drive ファイルコンテンツ、キャッシュされたファイル、メタデータ、OCR テキスト、抽出フィールド、および派生文書データは、開示された目的に不要になった時点で削除または匿名化され

るべきです。ただし、法的、セキュリティ、監査、または顧客組織の保持義務により継続的な保持が必要な場合を除きます。

削除

顧客組織の承認済みユーザーまたは管理者は、Google 由来のキャッシュデータ、取り込まれた Drive ファイル、抽出テキスト、および派生文書レコードの削除を要求できます。DynamicMail は、顧客組織の保持設定および適用法で許可される場合、要求されたデータを削除または匿名化すべきです。

DynamicMail に取り込まれたレコードを削除しても、Google Drive 内の元のファイルが必ず削除されるわけではありません。DynamicMail は、承認済みユーザーが表示される製品ワークフローを通じて明示的に Drive アクションを要求し、そのアクションが顧客組織のポリシーおよび適用法で許可される場合に限り、元の Drive ファイルを変更、移動、ゴミ箱へ移動、または削除すべきです。

取消しと接続解除

顧客組織は DynamicMail 内で Google Drive を接続解除できます。接続解除またはローカル同意の取消し後、DynamicMail は Google Drive 用に保存された OAuth トークンの使用を停止し、接続済みアカウントから追加の Drive ファイルを読み取り、書き込み、ダウンロード、アップロード、変更、または削除することを停止しなければなりません。

Google アカウント所有者は、Google アカウント設定でアプリの承認を取り消すこともできます。Google の承認が取り消された場合、DynamicMail はトークン更新または API 呼び出しが失敗した時点で Drive API アクセスを停止し、接続は切断済みまたは再接続が必要な状態として表示されるべきです。

ローカルでの取消しは、すでに取り込まれた DynamicMail 文書を自動的に削除しません。これらのレコードは、上記の削除および保持ルールに従って処理されます。

AI、OCR、および抽出の使用

DynamicMail は、Drive ファイルコンテンツおよびメタデータに対して、顧客組織向けに表示される Drive 文書ワークフローを提供または改善する目的に限り、OCR、解析、分類、要約、およびその他の AI 支援処理を使用できます。Drive データおよび派生データは、顧客組織が要求した機能の外で汎用の機械学習モデルまたは AI モデルを作成、訓練、または改善するために使用してはなりません。

AI 支援による結果は誤っている可能性があります。DynamicMail は、抽出データを、承認済みユーザーが製品フローに従って確認、修正、承認、拒否、または削除できるワークフロー出力として提示すべきです。

サポートおよび人によるアクセス

DynamicMail の担当者、請負業者、またはサブプロセッサは、以下のいずれかに該当する場合を除き、特定の Drive ファイル、抽出テキスト、ファイルメタデータ、または派生 Drive データを

読むべきではありません。

- ユーザーが、特定データへのアクセスを必要とするサポートを明示的に依頼した場合。
- セキュリティ調査、不正利用防止、またはインシデント対応のためにアクセスが必要な場合。
- 法律、法的手続、または顧客組織の拘束力ある指示に従うためにアクセスが必要な場合。
- データが内部運用のために集計または匿名化され、特定ユーザーの Drive コンテンツを読めない場合。

サポートアクセスは最小権限に基づき、実務上可能な場合は時間制限され、監査可能性のために記録されるべきです。

法務レビュー状況

これは実装およびローカライズ用の資料であり、最終的な法的助言ではありません。 別個のレビュー証拠なしに、Google の承認、外部弁護士の承認、または本番環境での制限付きスコープ利用許可があるものとして提示してはなりません。

参照元

- DynamicMail restricted-scope contract:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Google Drive API scopes:
<https://developers.google.com/workspace/drive/api/guides/api-specific-auth>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>