

デベロッパー プログラム ポリシー（2020 年 10 月 1 日発効）

アプリやゲームの提供元として世界で最も信頼される存在になろう

革新的なアプリは Google とデベロッパーの両方に成功をもたらしますが、責任も伴います。今後も両者がともに、革新的で信頼できるアプリを Google Play から世界中の多くのユーザーに提供できるよう、[デベロッパー販売 / 配布契約](#)と合わせて、このデベロッパー プログラム ポリシーが定められています。下記のポリシーをご確認ください。

制限されているコンテンツ

毎日、世界中のユーザーが Google Play を利用してアプリやゲームにアクセスしています。アプリを送信する前に、そのアプリが Google Play にふさわしいものかどうか、地域の法律を遵守しているかどうかをご自身でご確認ください。

児童を危険にさらす行為

未成年者に関する性的なコンテンツを含むアプリは、Play ストアから即時に削除されることがあります。これには、未成年者を性的欲求または不適切な行為（触る、愛撫するなど）の対象とすることを助長するアプリが含まれますが、これらに限定されません。

さらに、児童を対象にしたアプリで成人向けのテーマを扱うことも認められません。これには、過度の暴力、流血、殺人に関するコンテンツを含むアプリ、有害な行為または危険にさらす行為を描写または助長するアプリが含まれますが、これらに限定されません。また、身体や自己に否定的なイメージを持たせるようなアプリも認められません。これには、美容整形、減量など、身体の外観を整える美容上の矯正を説明するアプリなどが含まれます。

児童の性的虐待画像コンテンツの使用が判明した場合、Google は関係機関に報告し、このコンテンツの販売または配布に関与している者の Google アカウントを削除します。

不適切なコンテンツ

Google Play をこれからも信頼できる安全なプラットフォームとしてご利用いただけるようにするため、ユーザーにとって有害または不適切なコンテンツを定義し、禁止する基準を作成しました。

性的なコンテンツと冒とく的な表現

ポルノなどの性的なコンテンツや冒とく的な表現を含むまたは宣伝するアプリ、性的満足を意図したコンテンツやサービスなどは認められません。ただし、ヌードを含むコンテンツであっても、その主目的が教育、ドキュメンタリー、科学、または芸術で、不快感を与える内容でなければ認められる場合があります。

一般的な違反の例:

- 性的なヌードの描写のほか、裸の人物（全身や局部をばかした場合も含む）または最小限の衣服（公共の場で受け入れられないもの）しか身に着けていない人物が性的なものを暗示するポーズをとった描写。
- 性行為、性的内容を示唆するポーズ、または性的に描かれた人体部分の描写、アニメーション、イラスト。
- 性機能補助、セックスガイド、違法な性的テーマ、違法な性的嗜好を描写するコンテンツ。
- わいせつまたは冒とく的なコンテンツ。これには、ストアの掲載情報やアプリ内での、冒とく、中傷、露骨な表現、アダルトや性的なキーワードを含むコンテンツが含まれますが、これらに限定されません。
- 猥褻を描写、表現、奨励するコンテンツ。
- 報酬と引き換えに性行為を提供していると見なされる可能性のある、性関連のエンターテインメント、エスコート サービスなどのサービスを宣伝するアプリ。
- 人を辱める、または物と見なすアプリ。

ヘイトスピーチ

人種、民族、宗教、障がい、年齢、国籍、従軍経験、性的指向、性別、性同一性など、組織的な人種差別や疎外に結びつく特性に基づいて個人もしくは集団に対する暴力を助長、または差別を扇動するアプリは認められません。

教育、ドキュメンタリー、科学、芸術（EDSA）のコンテンツでもナチスに関するものを含むアプリは、一部の国で、現地の法規制に従ってブロックされることがあります。

一般的な違反の例:

- ・ 保護対象グループが、非人道的、劣っている、または排斥に値すると主張するコンテンツや表現。
- ・ 保護対象グループが否定的な特性を持っている（悪意がある、墮落している、邪悪であるなど）とする悪意のある中傷、固定観念、または言説が含まれるアプリ、またはその集団が脅威であると明示的または暗黙的に主張するアプリ。
- ・ 保護対象グループに属することを理由に、憎悪または差別すべきだと人々に信じ込ませようとするコンテンツや表現。
- ・ ヘイトグループに関連する旗、記号、バッジ、道具、動作などのヘイトシンボルを宣伝するコンテンツ。

暴力

無用な暴力やその他の危険な行為を描写または助長するアプリは認められません。アニメ、ハンティング、釣りなどのゲームにおける架空の暴力を描写するアプリは、通常許可されます。

一般的な違反の例:

- ・ 人や動物に対するリアルな暴力や暴力的脅しの画像や描写。
- ・ 自傷行為、自殺、いじめ、嫌がらせ、摂食障害、失神ゲームなど、重傷または死亡につながる恐れのある行為を助長するアプリ。

テロ関連のコンテンツ

メンバーの募集を含むいかなる目的であっても、テロ組織が **Google Play** でアプリを公開することは許可されません。

テロ行為を助長したり、暴力を扇動したり、テロ攻撃を称賛したりするコンテンツなど、テロに関連するコンテンツが含まれるアプリは認められません。教育、ドキュメンタリー、科学、または芸術を目的とするテロ関連のコンテンツを投稿する場合は、その背景を理解するのに十分な情報を提供するように心掛けてください。

配慮が求められる事象

自然災害、残虐行為、紛争、死、その他の悲劇的な事象に対する妥当な配慮を欠く、またはそのような事象を利用するアプリは認められません。配慮が求められる事象に関するアプリであっても、教育、ドキュメンタリー、科学、芸術（EDSA）上の価値のあるコンテンツや、配慮が求められる事象について警告する、または認知度を高めることを意図するコンテンツであれば、通常は認められます。

一般的な違反の例:

- ・ 自殺、薬物の過剰摂取、自然死などによる人間の死への配慮が欠けている。
- ・ 大規模な悲劇的事象を否定する。
- ・ 悲劇的な事象に便乗して利益を得ているように見える（被害者に恩恵が届いているのか明確でない）。

いじめや嫌がらせ

脅迫、嫌がらせ、いじめを行う、または助長するアプリは認められません。

一般的な違反の例:

- ・ 国際紛争または宗教対立の被害者をいじめる。
- ・ 他者からの搾取を目的としたコンテンツ（ゆすり、恐喝など）。
- ・ 公の場で誰かを辱めるためにコンテンツを投稿する。
- ・ 悲劇的な事象の被害者（またはその友人や家族）に対して嫌がらせを行う。

危険なプロダクト

爆発物、銃器、弾薬、特定の銃器用品の販売を促進するアプリは認められません。

- ・ 制限の対象となる銃器用品には、擬似的な自動発射を可能にする用品や銃器を自動発射式に改造する用品（バンプストック、ガトリングトリガー、ドロップインオートシア、改造キットなど）、銃弾を **31** 発以上携帯可能なマガジンやベルトが含まれます。

爆発物、銃器、弾薬、制限されている銃器用品など、武器および兵器の製造方法を説明するアプリは認められません。たとえば、銃器を自動発射式に改造する方法や擬似的な自動発射を可能にする方法などが該当します。

マリファナ

マリファナまたはマリファナ製品の販売を促進するアプリは、違法性の有無にかかわらず認められません。

一般的な違反の例:

- ユーザーがアプリ内のショッピング カート機能を通じてマリファナを注文できるようにする。
- ユーザーによるマリファナの受け渡しの手配を支援する。
- テトラヒドロカンナビノール（THC）を含有する製品（THC が含まれる CBD オイルなど）の販売を促進する。

タバコとアルコール

タバコ（電子タバコ、VAPE ペンを含む）の販売を促進したり、アルコールやタバコの違法または不適切な使用を推奨したりするアプリは認められません。

一般的な違反の例:

- 未成年によるアルコールやタバコの使用や売買を描写または奨励する。
- タバコを消費することで、社会的、職業的な地位や、性的、知的、身体的な魅力が向上するとほのめかす。
- 暴飲や飲み比べ競争など、過度の飲酒を好ましい行為として描写する。

金融サービス

虚偽のまたは有害な金融商品や金融サービスを紹介するアプリは認められません。

このポリシーにおいて「金融商品や金融サービス」とは、法定通貨および仮想通貨の管理または投資に関連する商品やサービス（個人向けのアドバイスも含む）を指します。

金融商品や金融サービスを含むまたは宣伝するアプリについては、そのアプリが対象とする国や地域の規定（たとえば地域の法律で義務付けられている特定の開示など）を遵守しなければなりません。

バイナリ オプション

バイナリ オプション取引機能をユーザーに提供するアプリは認められません。

暗号通貨

端末上で暗号通貨をマイニングするアプリは認められません。暗号通貨のマイニングをリモート管理するアプリは認められます。

個人ローン

このポリシーにおいて個人ローンとは、個人の消費者が個人、組織、または団体から、固定資産の購入や教育費を用途とせずに臨時に融資を受けることをいいます。個人ローンを利用するかどうかについて、消費者が適切な判断を下すためには、そのローン商品の品質、特徴、手数料、返済スケジュール、リスク、メリットについての情報が必要です。

- 例: 個人ローン、ペイデイローン、P2P ローン、タイトルローン
- 含まれないもの: 住宅ローン、自動車ローン、学資ローン、リボルビング方式のクレジット ライン（クレジット カード、個人向けクレジット ラインなど）

個人ローンを提供するアプリには、融資を直接提供するアプリ、利用者獲得のためのアプリ、および消費者と第三者の融資元の間を仲介するアプリなどが含まれます。これらのアプリは、メタデータで以下の情報を開示する必要があります。

- 最短および最長の返済期間
- 最大 APR（実質年利）。通常、利率に年間の手数料その他の費用を加えたものまたはこれに類する料率を地域の法律に則って算出したものをいいます。
- 該当するすべての費用を含む、ローンの総費用の代表例
- ユーザーの個人情報や機密情報に対するアクセス、収集、使用、共有を完全に開示するプライバシー ポリシー

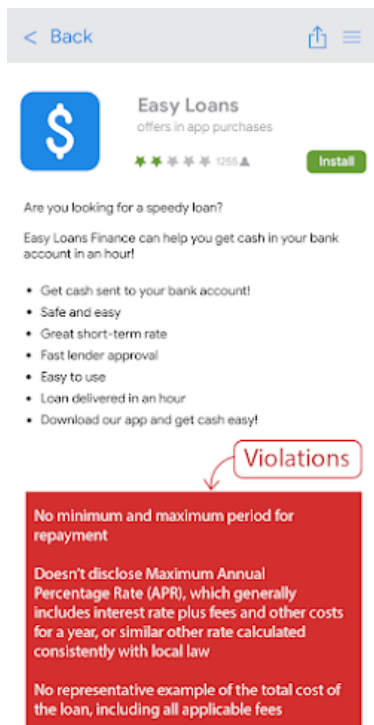
融資日から 60 日以内に全額返済を求める個人ローンを宣伝するアプリは認められません（このようなローンを Google では「短期個人ローン」と呼んでいます）。

APR の高い個人ローン

Google Play において、米国では実質年利（APR）が 36% 以上の個人ローンのアプリは認められていません。米国内の個人ローンのアプリでは、[貸付真実法（TILA）](#) に則って算出された最大 APR を表示する必要があります。

このポリシーは、融資を直接提供するアプリ、見込み客獲得のためのアプリ、および消費者と第三者の融資元の間を仲介するアプリに適用されます。

一般的な違反の例:



現金を伴うギャンブル、ゲーム、コンテスト

現金を伴うギャンブルに関するアプリ、現金を伴うギャンブルに関する広告、デイリー ファンタジー スポーツ アプリは、特定の条件を満たす場合に限り、許可されています。

ギャンブル アプリ

（現在、英国、アイルランドおよびフランスでのみ許可されています。）

その他の地域では、オンライン ギャンブルを促進するコンテンツやサービスを含むアプリは許可されていません。

オンライン ギャンブルを推進するコンテンツおよびサービスについては、以下の要件を満たす場合に限り、許可されています。

- デベロッパーは、**Play** でアプリを配信するために、**お申し込み手続きを完了**する必要があります。
- アプリは、配信される各国で適用される法律および業界における基準を、すべて遵守する必要があります。
- デベロッパーは、アプリを配信する各国で有効なギャンブル ライセンスを取得する必要があります。
- 未成年のユーザーに対しては、アプリでギャンブルを行えないようにする必要があります。
- デベロッパーは、ギャンブル ライセンスを取得した国以外では、アプリが利用できないようにする必要があります。
- アプリを **Google Play** の有料アプリとして購入可能にすることはできません。また、アプリで **Google Play** アプリ内課金を使用することもできません。
- アプリは、ストアからのダウンロードとインストールが無料であることが必要です。
- アプリは、**AO**（成人のみ）または **IARC** の同等のレーティングであることが必要です。
- アプリおよびアプリの掲載情報には、責任あるギャンブルに関する情報を明確に表示する必要があります。

その他の現金でのゲーム、コンテスト、トーナメントのアプリ

ユーザーが現金（現金で購入されるアプリ内アイテムを含みます）を賭けたり、参加費を払う等により、実世界で金銭的価値のある賞品を得られるようなコンテンツやサービスは許可されていません。これには、上記のギャンブル アプリの要件を満たさないオンライン カジノ、スポーツ ギャンブルおよび宝くじのほか、現金などの実世界で価値を有する賞品を提供するゲームなどが含まれますが、これらに限定されません。

違反の例:

- 物理的な賞品または金銭的価値を有する賞品を獲得するチャンスと引き換えに、金銭を支払うゲーム
- 「ロイヤルティ」（エンゲージメントやアクティビティ）ポイント（（1）現金による購入に伴って獲得または増加し、（2）実世界で金銭的価値を有するアイテムまたは賞品と交換できるポイント）があるゲーム
- ギャンブルの賭け金、参加に必要なアプリ内通貨、賞金のほか、物理的な賞品または金銭的価値を有する賞品を得る資格を取得する（またはチャンスを高める）ためのデポジットを受け取ったり、管理したりするアプリ。

現金を使用するゲーム、コンテスト、トーナメントに賭けたり、参加するなどの「行動を促すフレーズ」を提示するアプリ。たとえば、賞金獲得のチャンスがあるようなトーナメントに「登録しよう」または「挑戦しよう」と誘うナビゲーション要素（メニュー項目、タブ、ボタンなど）を有するアプリ。

Play 配信アプリ内でのギャンブルや、現金を伴うゲーム、コンテスト、トーナメントに関する広告

ギャンブルや、現金を伴うゲーム、コンテスト、トーナメントを宣伝するアプリについては、以下の要件を満たすものに限り許可します。

- アプリや広告（広告主を含む）は、広告が表示される地域で適用される法律と業界における基準をすべて遵守する必要があります。
- 広告は、宣伝対象のギャンブル関連の商品とサービスすべてについて、地域のライセンス要件を満たす必要があります。
- 18 歳未満であることが明らかになった個人には、アプリにギャンブルの広告を表示できません。
- ファミリー向けプログラムにはアプリを登録できません。
- 18 歳未満の個人はアプリのターゲットに設定できません。
- ギャンブル アプリ（上記に定義されるアプリ）を宣伝する広告は、ランディング ページ、宣伝対象のアプリの掲載情報、またはアプリ内に、責任あるギャンブルに関する情報を明確に表示する必要があります。
- ギャンブルをシミュレーションするコンテンツをアプリで提供してはなりません（ソーシャル カジノ アプリ、仮想スロットマシンを含むアプリなど）。
- ギャンブル サービス、または現金でのゲーム、宝くじ、トーナメントをサポートする機能（ギャンブル、支払い、スポーツのスコアやオッズの追跡、参加資金の管理を支援する機能など）をアプリで提供してはなりません。
- アプリ内で宣伝するギャンブル サービスや現金でのゲーム、宝くじ、トーナメントのサービスの所有権を保有してはなりません。
- アプリのコンテンツで、ギャンブル サービスや現金でのゲーム、宝くじ、トーナメントのサービスを宣伝したり、そのサービスにユーザーを案内したりしてはなりません。

ギャンブル アプリ（上記で定義）、またはこれらのギャンブル広告の要件をすべて満たすアプリにのみ、現金を伴うギャンブルや現金でのゲーム、宝くじ、トーナメントの広告を掲載できます。

違反の例:

- 未成年のユーザー向けに設計され、ギャンブル サービスを宣伝する広告が表示されるアプリ
- ユーザーに実世界のカジノを宣伝または案内するカジノのシミュレーション ゲーム
- スポーツ ギャンブル サイトにリンクするギャンブル広告を含む、専用のスポーツオッズ追跡アプリ
- アプリの開発者が所有または運営するギャンブル サービスの広告を表示するニュースアプリ
- ボタン、アイコン、その他のインタラクティブなアプリ内要素としてユーザーに表示される広告など、[虚偽の広告](#)に関するポリシーに違反するギャンブル広告を掲載するアプリ

デイリー ファンタジー スポーツ（DFS）アプリ

デイリー ファンタジー スポーツ（DFS）アプリ（提供地域の法令で定義されるもの）は、以下の要件を満たす場合に限り許可されます。

- アプリは、1) 米国国内でのみ配布されるか、2) 上記のギャンブル アプリの要件を満たすものとします。
- 開発者が **Play** でアプリを配信するには、[DFS のお申し込み](#)手続きを完了し、承認される必要があります。
- アプリは、配信先の国で適用される法律と業界基準をすべて遵守する必要があります。
- 未成年のユーザーに対しては、アプリ内でギャンブルや金銭の取引を行えないようにする必要があります。
- アプリを **Google Play** の有料アプリとして購入可能にすることはできません。また、アプリで **Google Play** アプリ内課金を使用することもできません。
- アプリは、ストアからのダウンロードとインストールが無料であることが必要です。
- アプリは、**AO**（成人のみ）または **IARC** の同等のレーティングであることが必要です。
- アプリおよびアプリの掲載情報には、責任あるギャンブルに関する情報を明確に表示する必要があります。

米国で配布する場合は、以下の追加要件が適用されます。

- アプリは、配信される米国の州または準州で適用される法律と業界基準をすべて遵守する必要があります。
- 開発者は、デイリー ファンタジー スポーツ アプリにライセンスが必要な米国の州または準州ごとに、有効なライセンスを取得する必要があります。
- 開発者はデイリー ファンタジー スポーツ アプリに必要なライセンスを保有していない米国の州または準州では、アプリを使用できないようにする必要があります。

- ・ デイリー ファンタジー スポーツ アプリが合法ではない米国の州または準州では、アプリを使用できないようにする必要があります。

違法行為

違法行為を助長するまたは推進するアプリは認められません。

一般的な違反の例:

- ・ 違法薬物の売買や、処方薬の処方箋なしの売買の推進。
- ・ 未成年による薬物、アルコール、タバコの使用や売買の描写または奨励。
- ・ 違法薬物の栽培や製造の説明。

ユーザー作成コンテンツ

ユーザーがアプリに投稿したコンテンツが他のユーザーにも、または少なくともアプリユーザーの一部にも表示される、またはアクセスできるようになる場合、それをユーザー作成コンテンツ（UGC）といいます。

UGC を含む、または掲載するアプリは、以下の要件を満たす必要があります。

- ・ ユーザーがアプリの利用規約やユーザー ポリシーに同意しない限り、ユーザーが **UGC** を作成またはアップロードできないようにします。
- ・ 不適切なコンテンツや行為を（**Play** のデベロッパー プログラム ポリシーを遵守する方法で）定義し、アプリの利用規約やユーザー ポリシーで禁止します。
- ・ アプリがホストする **UGC** の種類に対して合理的で一貫性があり、徹底的かつ効果的で継続的な **UGC** モデレーションを実装します。
 - ・ ライブストリーミング アプリの場合、不適切な **UGC** は合理的に可能な限り即時に削除する必要があります。
 - ・ 拡張現実（AR）アプリの場合、不適切な **AR UGC**（露骨な性的 **AR** 画像など）にも、配慮が求められる場所に置かれた **AR** アンカーにも、**UGC** のモデレーション（アプリ内の報告システムを含む）が責任を負う必要があります。たとえば、軍事基地のような立ち入り禁止区域や、**AR** アンカーを置くことで所有者に対して問題が発生する恐れのある私有地にアンカーを置いた **AR** コンテンツがそれに該当します。
- ・ 不適切な **UGC** を報告するための、ユーザー フレンドリーなアプリ内システムを提供し、その **UGC** に対して適宜措置を取ってください。
- ・ アプリの利用規約やユーザー ポリシーに違反する嫌がらせ行為者を削除またはブロックします。
- ・ アプリ内での収益化によって、ユーザーの不適切な行動が助長されないよう安全保護対策を提供します。

不適切な **UGC** を掲載することを主な目的とするアプリは、**Google Play** から削除されます。同様に、主に不適切な **UGC** をホストするために使用されているアプリや、そうしたコンテンツが横行しているという評判がユーザーの間で広まっているアプリも、**Google Play** から削除されます。

一般的な違反の例:

- ・ 性的に露骨なユーザー作成コンテンツの宣伝（不適切なコンテンツの共有促進を主な目的とした有料機能の実装や許可を含む）。
- ・ ユーザー作成コンテンツ（UGC）を扱い、特に未成年への脅し、嫌がらせ、いじめに対する十分な安全保護対策のないアプリ。
- ・ アプリ内で、特定の人に対して嫌がらせ、悪意のある攻撃、嘲笑を主な目的とした投稿、コメント、写真。
- ・ 不適切なコンテンツに関するユーザーからの苦情に継続的に対応できないアプリ。

不承認の薬物

Google Play では、合法性の主張の有無にかかわらず、不承認の薬物を宣伝または販売するアプリは認められません。例:

- ・ [禁止されている医薬品とサプリメント](#) のリストにあるすべての商品（このリストは、禁止対象商品をすべて網羅しているわけではありません）
- ・ エフェドラを含有する商品
- ・ ヒト絨毛性ゴナドトロピン（hCG）が減量や体重管理に関連して、またはアナボリック ステロイドとともに宣伝される場合
- ・ 医薬品有効成分や危険な成分を含有するハーブ系サプリメントや栄養補助食品
- ・ 虚偽または誤解を与える効果効能（処方薬や規制薬物と同等の効果があるなど）
- ・ 政府の承認を得ていない商品で、病気や疾患の予防や治療における安全性や効果があると示唆しているもの
- ・ 政府または規制機関による措置や警告の対象となったことのある商品

- ・ 未承認の医薬品やサプリメント、または規制薬物と混同される可能性がある名前の商品

Google が監視している未承認のまたは誤解を与える医薬品とサプリメントについて詳しくは、www.legitscript.com をご覧ください。

知的財産

他者が作成したものをデベロッパーがコピーしたり、必要な許可を得ずに使用したりすると、その作品の所有者に害を及ぼす恐れがあります。他者の作品を不正に使用しないでください。

知的財産

アプリやデベロッパー アカウントが他者の知的所有権（商標権、著作権、特許権、企業秘密、その他の専有的権利を含む）を侵害する行為は認められません。知的所有権の侵害を助長または誘導するアプリも認められません。

Google では、著作権を侵害しているとする明確な通知を受けた場合には、それに対し適切に対応します。DMCA に基づく申し立てを行う方法など、詳しくは、[著作権に関する手続き](#)をご覧ください。

アプリ内での偽造品の販売または宣伝について申し立てを行うには、[偽造品を報告](#)してください。

Google Play のアプリがご自身の商標権を侵害していると思われる場合は、該当のデベロッパーに直接連絡して、問題の解決にあたることをおすすめします。デベロッパーと問題を解決できない場合は、[こちらのフォーム](#)から商標権侵害を申し立ててください。

アプリ内またはストアの掲載情報で第三者の知的財産（ブランド名、ロゴ、画像、映像など）を使用する許可を受けていることを証明する文書がある場合は、知的所有権の侵害を理由にアプリが否認となることがないよう、アプリを送信する前に [Google Play チーム](#)にご連絡ください。

著作権で保護されているコンテンツの無断使用

著作権を侵害するアプリは認められません。著作権で保護されているコンテンツを改変することも違反となる場合があります。著作権で保護されているコンテンツを使用する場合は、その権利の証拠を示すよう求められることがあります。

著作権で保護されているコンテンツをアプリ機能のデモとして使用する場合は、注意が必要です。通常、最も安全な方法は、オリジナルなものを作成することです。

法的に有効な理由なく無断で、著作権で保護されているコンテンツがよく使用される例を紹介します。

- ・ 音楽のアルバム、ビデオゲーム、書籍のカバーアート
- ・ 映画、テレビ、ビデオゲームのマーケティング画像
- ・ マンガ、アニメ、映画、ミュージック ビデオ、テレビのアートワークや画像
- ・ 大学やプロのスポーツチームのロゴ
- ・ 有名人のソーシャル メディア アカウントから取得した写真
- ・ 有名人のプロによる画像
- ・ 著作権で保護されているオリジナル作品と区別がつきにくい複製または「ファンアート」
- ・ 著作権で保護されているコンテンツの音声クリップを再生するサウンドボードを持つアプリ
- ・ パブリック ドメイン以外の書籍の完全な複製や翻訳

著作権侵害の助長

著作権侵害を誘導または助長するアプリは認められません。アプリを公開する前に、著作権の侵害をアプリが助長することにならないかどうか確認し、必要に応じて法律上の助言を受けてください。

一般的な違反の例:

- ・ 著作権で保護されているコンテンツのローカルコピーをユーザーが許可なくダウンロードできるストリーミング アプリ。
- ・ 音楽や動画などの著作権で保護されているコンテンツを、該当する著作権法に違反して、ユーザーがストリーミングやダウンロードすることを助長するアプリ:



- ① アプリの掲載情報の説明で、著作権で保護されているコンテンツを許可なくダウンロードすることをユーザーにすすめています。
- ② アプリの掲載情報のスクリーンショットで、著作権で保護されているコンテンツを許可なくダウンロードすることをユーザーにすすめています。

商標権侵害

他者の商標を侵害するアプリは認められません。商標とは、商品やサービスの提供元を識別する語句、シンボル、またはその組み合わせです。商標権を取得した所有者には、特定の商品やサービスにその商標を使用する独占的な権利があります。

商標権の侵害とは、商品の提供元を混同させる可能性のある方法で、同一または類似の商標を不正にまたは無断で使用することです。こうした紛らわしい方法で他者の商標を使用するアプリは、公開が停止されることがあります。

偽造

偽造品の販売や宣伝を行うアプリは認められません。偽造品とは、他の商標と同一、またはほとんど区別がつかない商標やロゴを使用している商品を指します。このような商品は、正規品と偽って販売するために商品のブランドの特徴を模倣しています。

プライバシー、詐欺、デバイスの不正使用

Google では、ユーザーのプライバシーを保護し、安全な環境をユーザーに提供するように努めています。虚偽のあるアプリ、悪意のあるアプリ、ネットワーク、デバイス、個人データを悪用または不正使用する意図のあるアプリは一切禁止しています。

ユーザーデータ

ユーザーデータ（デバイス情報を含む、ユーザーについての情報やユーザーから収集する情報など）を扱う場合は、その処理方法を明らかにする必要があります。つまり、アプリがこのデータにアクセスし、収集、使用、共有することを開示し、開示した目的にのみデータを使用することが求められます。さらに、アプリが個人情報や機密情報を扱う場合は、以下の「個人情報や機密情報」に記載されている追加の要件もご確認ください。これらの Google Play の要件は、プライバシー保護とデータ保護に関する適用法令が規定する要件に加えて適用されます。

個人情報と機密情報

ユーザーの個人情報や機密情報には、個人を特定できる情報、財務情報、支払い情報、認証情報、電話帳、連絡先、[デバイスの位置情報](#)、SMS や通話に関するデータ、マイク、カメラなどのデバイスや使用状況に関するその他の機密情報が含まれますが、これらに限定されません。アプリがユーザーの機密情報を扱う場合は、以下の要件を満たす必要があります。

- ・アプリを通じて取得した個人情報や機密情報へのアクセス、収集、使用、および共有の目的を、アプリの機能（Play ストアのアプリの説明文に記載および宣伝されていてユーザーが予想できる機能）の提供や改善に直接関係するものに限定すること。このデータを広告配信でも利用するアプリは、[広告ポリシー](#)を遵守していなければなりません。
- ・プライバシー ポリシーを、**Play Console** の所定の欄とアプリ内の両方に掲載すること。プライバシー ポリシーでは、アプリ内での開示内容と併せて、アプリがユーザーデータにアクセスし、収集、使用、共有する方法を包括的に開示する必要があります。アプリがアクセス、収集、使用、共有する個人情報や機密情報の種類、またユーザーの個人情報や機密情報の共有先についてもプライバシー ポリシーで開示する必要があります。
- ・最新の暗号手法を使用して（HTTPS 経由などで）転送するなど、ユーザーのすべての個人情報または機密情報を安全に扱うこと。
- ・**Android の権限**によって制限されているデータにアクセスする前に、可能な限りランタイム権限をリクエストすること。
- ・ユーザーの個人情報または機密情報を販売しないこと。

認識しやすい開示と同意の要件

ポリシーを遵守したアプリ内機能の提供または改善のために自分の個人情報や機密情報が必要となることをユーザーが合理的に予想できない可能性のあるアプリの場合（たとえば、バックグラウンドのアプリでデータを収集する場合）、以下の要件を満たす必要があります。

データの収集、使用、共有について、アプリ内で開示する必要があります。アプリ内での開示に関する要件は以下のとおりです。

- ・アプリ内で開示すること。アプリの説明文やウェブサイトでの開示だけでは不十分です。
- ・アプリの通常使用時に表示すること。表示するのにメニューや設定に移動する必要のある開示方法では不十分です。
- ・アクセスまたは収集するデータの種類について説明すること。
- ・データをどのように使用、共有するかについて説明すること。
- ・掲載場所を、プライバシー ポリシーや利用規約のみとしないこと。
- ・個人情報や機密情報の収集に関係のない他の開示の中に掲載しないこと。

アプリ内での開示は、ユーザーの同意（可能であれば関連するランタイム権限）をリクエストするダイアログを表示する直前に行う必要があります。ユーザーの同意を得る前に、個人情報や機密情報にアクセスしたり、収集したりすることはできません。同意をリクエストするアプリの要件は以下のとおりです。

- ・同意ダイアログは、あいまいにならないよう明確に表示する。
- ・同意を示すための明確な操作をユーザーに求める（例: タップで同意する、チェックボックスをオンにする）。
- ・開示画面から他へ移動する操作（例: タップで移動する、戻るボタンやホームボタンを押す）を同意と**見なさない**。
- ・ユーザーの同意を得る方法として、自動で非表示になるメッセージや閲覧期限付きメッセージを使用**しない**。

一般的な違反の例:

- ・ユーザーのインストール済みアプリの一覧にアクセスできるにもかかわらず、そのデータを個人情報や機密情報として扱わず、上記のプライバシー ポリシー、データの処理、認識しやすい方法での開示、および同意の各要件を満たしていないアプリ。
- ・ユーザーの電話機能や連絡帳のデータにアクセスできるにもかかわらず、そのデータを個人情報や機密情報として扱わず、プライバシー ポリシー、データの処理、認識しやすい方法での開示、および同意の各要件を満たしていないアプリ。
- ・ユーザーの画面を記録するにもかかわらず、そのデータを個人情報や機密情報として、このポリシーに沿って扱わないアプリ。
- ・**デバイスの位置情報**を収集するにもかかわらず、上記の要件に沿ってその情報の使用について包括的に開示せず、同意を得ていないアプリ。
- ・追跡、調査、またはマーケティングの目的などのため、アプリのバックグラウンドで制限付きの権限を使用するにもかかわらず、上記の要件に沿って各権限の使用について包括的に開示せず、同意を得ていないアプリ。

機密情報へのアクセスに関する特定の制限事項

上記の要件に加えて、特定の操作における要件を下記の表に記載します。

操作	要件
個人の財務情報、支払い情報、政府発行の個人識別番号をアプリが扱う場合	財務処理、支払い処理、政府発行の個人識別番号に関する個人情報や識別情報は一切公開してはなりません。
非公開の電話帳や連絡先の情報をアプリが扱う場合	個人の非公開の連絡先を許可なく公開または開示することは認められません。

ウイルス対策、マルウェア対策、セキュリティ関連の機能など、ウイルス対策機能やセキュリティ機能を持つアプリの場合	アプリ内での開示と併せて、アプリが収集、転送するユーザーデータの種類と内容、使用方法、共有先について説明するプライバシーポリシーを掲載する必要があります。
---	---

EU-U.S. Privacy Shield（EU-US プライバシー シールド）

プライバシー シールド

欧州連合またはスイスにおいて収集された直接または間接的に個人を特定できる個人情報（「EU 個人情報」）に、Google からの提供を経てアクセスする場合や、そうした個人情報を利用、処理する場合は、以下の義務が発生します。

- 適用のある法域におけるプライバシー、データセキュリティ、データ保護に関するあらゆる法律、指令、規制、ルールを遵守すること
- EU 個人情報のアクセス、使用、処理は、その EU 個人情報に関連する人物が同意した目的の範囲内に限って行うこと
- データの消失、不正使用、不正アクセス、違法アクセス、漏えい、改変、破壊などから EU 個人情報を保護するために適切な組織的および技術的な措置をとること
- **Privacy Shield（プライバシー シールド）原則**で要求されているものと同水準の保護を確保すること

上記の義務を遵守していることを定期的に監視し、上記の条件を満たせない（または満たせなくなるリスクが高い）場合は、いつでも直ちに data-protection-office@google.com 宛てのメールで Google に通知するとともに、直ちに EU 個人情報の処理を停止するか、適切な水準の保護を回復するための合理的かつ適切な措置を講じなければなりません。

権限

権限のリクエストは、ユーザーにとって理に適うものでなければなりません。そのため、アプリで現在提供しているストアの掲載情報にも掲載されている機能やサービスの実装に必要な権限に限り、リクエストが可能となっています。ユーザーデータやデバイスデータへのアクセスを必要とする機能や目的が公開されていないもしくは実装されていない場合、または認可されていない場合には、そのような権限を利用できません。権限を通じてアクセスした個人情報や機密情報を販売することは禁止されています。

データにアクセスする権限のリクエストは、アプリが権限をリクエストする理由をユーザーが理解しやすいように、状況に合わせて（段階的認証の形で）行うようにしてください。データの使用は、ユーザーが同意した目的に限り行わなければなりません。後になって他の目的でデータを使用する必要がある場合は、その追加の用途に関して、あらかじめユーザーにリクエストし、同意を得る必要があります。

制限付きの権限

上記に加えて、制限付きの権限とは、「[Dangerous](#)」、「[Special](#)」、または「[Signature](#)」と指定される権限であり、以下に示す追加の要件と制限が適用されます。

- 制限付き権限を通じてアクセスしたユーザーやデバイスの機密情報を第三者に転送できるのは、データを収集したアプリの現在の機能やサービスを提供または改善するために必要な場合のみです。また、適用される法律を遵守するために必要な場合、または合併、買収、資産売買の一環として必要な場合には、法的に適切な通知を行ったうえでデータを転送できます。上記以外でのユーザーデータの転送または販売はすべて禁止されています。
- ユーザーが制限付き権限のリクエストを承認しない場合はその決定を尊重してください。重要でない権限についてユーザーに同意するよう誘導または強制することも認められません。機密情報に関わる権限へのアクセスを許可しないユーザーにも対応する（たとえば、ユーザーが通話履歴へのアクセスを制限している場合であれば電話番号を手動で入力できるようにするなど）よう、合理的な努力を尽くす必要があります。

一部の制限付き権限には、下記の追加要件が適用されることがあります。これらの制限の目的は、ユーザーのプライバシーを守ることにあります。ただし、非常にまれなケースですが、アプリがきわめて必要性の高いまたは重要な機能を提供していて、その機能を実現する他の手段が現時点で他に存在しない場合には、下記の要件について例外が認められることがあります。例外の申請があった場合は、ユーザーに対して想定されるプライバシーまたはセキュリティ上の影響を考慮して審査します。

SMS と通話履歴の権限

SMS と通話履歴に関する権限は、ユーザーの個人情報および機密情報と見なされ、[個人情報と機密情報](#)に関するポリシーおよび以下の制限が適用されます。

制限付きの権限

要件

アプリのマニフェストで通話履歴に関する権限グループ（`READ_CALL_LOG`、`WRITE_CALL_LOG`、`PROCESS_OUTGOING_CALLS` など）をリクエストする場合

ユーザーの端末で、アプリがデフォルトの電話ハンドラまたはアシスタント ハンドラとして能動的に登録されている必要があります。

アプリのマニフェストで SMS に関する権限グループ（**READ_SMS**、**SEND_SMS**、**WRITE_SMS**、**RECEIVE_SMS**、**RECEIVE_WAP_PUSH**、**RECEIVE_MMS**）をリクエストする場合

ユーザーのデバイスで、アプリがデフォルトの SMS ハンドラまたはアシスタント ハンドラとして有効に登録されている必要があります。

デフォルトの SMS ハンドラ、電話ハンドラまたはアシスタント ハンドラとしての機能をアプリが備えていない場合、マニフェストで上記の権限の使用を宣言することはできません（マニフェスト内のプレースホルダ テキストである場合を含みます）。また、ユーザーに上記の権限の許可をリクエストする前に、アプリがデフォルトの SMS ハンドラ、電話ハンドラまたはアシスタント ハンドラとして有効に登録されている必要があります。アプリがデフォルトのハンドラではなくなったときは、直ちに該当する権限の使用を停止しなければなりません。許可されている使用方法と例外については、[ヘルプセンターのこちらのページ](#)をご覧ください。

アプリが使用できるのは、アプリの承認済みの重要な機能を提供するために必要な権限（およびその権限で取得したデータ）のみです。重要な機能とは、アプリの主たる目的である機能をいいます。いくつかの機能のセットの場合もあり、そのすべてがアプリの説明文の中に認識しやすい形で明記されている必要があります。その機能がなければアプリが動作不良になる、あるいは使用できないと見なされるような機能が「重要な機能」に該当します。このデータの転送、共有、またはライセンス下での使用は、アプリ内で重要な機能やサービスを提供することのみを目的として許可されるものであり、その他の目的（他のアプリやサービスの改善、広告、マーケティング目的など）でデータを使用することはできません。通話履歴や SMS に関連する権限に基づくデータを取得するために、他の権限、API、第三者の提供元など、代わりの方法を使用することはできません。

位置情報の権限

[デバイスの位置情報](#)は、ユーザーの個人情報および機密情報と見なされ、[個人情報と機密情報](#)に関するポリシーおよび以下の要件が適用されます。

- アプリで現在の機能やサービスを提供する必要がなくなった後は、位置情報の権限（**ACCESS_FINE_LOCATION**、**ACCESS_COARSE_LOCATION**、**ACCESS_BACKGROUND_LOCATION** など）で保護されているデータにアプリからアクセスすることはできません。
- 広告や分析のみを目的として、ユーザーに位置情報の権限をリクエストしてはなりません。このデータの許可された利用の範囲を広告配信にも適用するアプリは、[広告ポリシー](#)を遵守しなければなりません。
- アプリがリクエストするアクセスのレベルは、位置情報を必要とする現在の機能やサービスを提供するうえで必要最低限に留め（つまり、高精度よりも低精度、バックグラウンドよりもフォアグラウンド）、そのレベルの位置情報が機能やサービスに必要であることをユーザーが合理的に予期できる必要があります。たとえば、バックグラウンドで位置情報をリクエストまたは利用することに合理的な根拠がないアプリは承認されない可能性があります。
- バックグラウンドで位置情報が利用できるのは、ユーザーにとってメリットがあり、かつアプリの重要な機能に関連する機能を提供する場合のみです。

アプリからフォアグラウンド サービスの権限で（たとえば「使用中」のみ許可されるなど、フォアグラウンドでのアクセス権でのみ）位置情報にアクセスするのが認められるのは、以下の場合です。

- アプリ内でユーザーが開始したアクションの続きとして位置情報の利用が開始され、かつ
- ユーザーが開始したアクションの意図されたユースケースが完了した後、直ちにその利用が終了する場合

子供を主な対象とするアプリは、[ファミリー向け](#)ポリシーを遵守する必要があります。

すべてのファイルへのアクセス権限

ユーザーのデバイス上のファイルとディレクトリの属性は、ユーザーの個人情報および機密情報と見なされ、[個人情報と機密情報](#)に関するポリシーおよび以下の要件が適用されます。

- アプリがリクエストするアクセスの対象は、アプリが機能するうえで不可欠なデバイス ストレージに限定する必要があります。ユーザー向けの不可欠なアプリ機能と関係のない目的で第三者のためにデバイス ストレージへのアクセスをリクエストしてはなりません。
- R（Android 11、API レベル 30）以降を搭載している Android デバイスでは、共有ストレージ内のアクセスを管理するために、[MANAGE_EXTERNAL_STORAGE](#) 権限が必要です。R をターゲットとし、共有ストレージへの幅広いアクセス（「すべてのファイルへのアクセス」）をリクエストするアプリは必ず、公開前に適切なアクセスに関する審査に合格する必要があります。この権限の使用を許可されたアプリは、[特別なアプリアクセス] 設定で [すべてのファイルへのアクセス] を有効にするように求めるメッセージを、ユーザーにはっきり表示する必要があります。R のこの要件について詳しくは、こちらのヘルプ記事をご覧ください。

デバイスやネットワークでの不正行為

ユーザーのデバイス、その他のデバイス、パソコン、サーバー、ネットワーク、アプリケーション プログラミング インターフェース（API）、またはサービス（デバイス上の他のアプリ、Google サービス、承認された携帯電話会社のネッ

トワークが含まれますが、これらに限定されません）を妨害、阻害、破損する、またはそれらに不正にアクセスするアプリは認められません。

Google Play に公開するアプリは、[Google Play のアプリの中核品質に関するガイドライン](#)に定めるデフォルトの Android システム最適化要件を遵守する必要があります。

Google Play で販売または配布されるアプリについては、Google Play の更新機能以外の方法によりアプリ自体の変更、差し替え、更新を行うことはできません。同様に、Google Play 以外の提供元から実行コード（dex、JAR、.so などのファイル）をダウンロードすることもできません。こうした制限は、仮想マシンで実行され Android API へのアクセス（ウェブ表示やブラウザでの JavaScript などの使用）が制限されているコードには適用されません。

セキュリティの脆弱性を組み込むまたは悪用するコードは許可されません。デベロッパーに報告された最近のセキュリティに関する問題については、[アプリ セキュリティ向上プログラム](#)をご確認ください。

一般的な違反の例:

- 広告を表示して他のアプリをブロックまたは妨害するアプリ。
- 他のアプリのゲームプレイに影響を与えるようなゲームチート アプリ。
- サービス、ソフトウェア、ハードウェアのハッキングやセキュリティ保護の回避を支援するまたはその方法を説明するアプリ。
- サービスや API に対してその利用規約に違反する方法でアクセスまたは利用するアプリ。
- [システムの電源管理](#)を迂回しようとするアプリのうち[ホワイトリストへの登録](#)が認められないもの。
- 第三者に対するプロキシ サービスの利用を支援するアプリのうち、その利用支援がアプリのユーザー向けの主たる基本目的ではないもの。
- アプリまたはサードパーティのコード（SDK など）のうち、Google Play 以外の提供元から実行可能コード（dex ファイル、ネイティブ コードなど）をダウンロードするもの。
- ユーザーの事前の同意なしに他のアプリをデバイスにインストールするアプリ。
- 不正なソフトウェアにリンクするアプリや、その配信やインストールを推進するアプリ。

虚偽の振る舞い

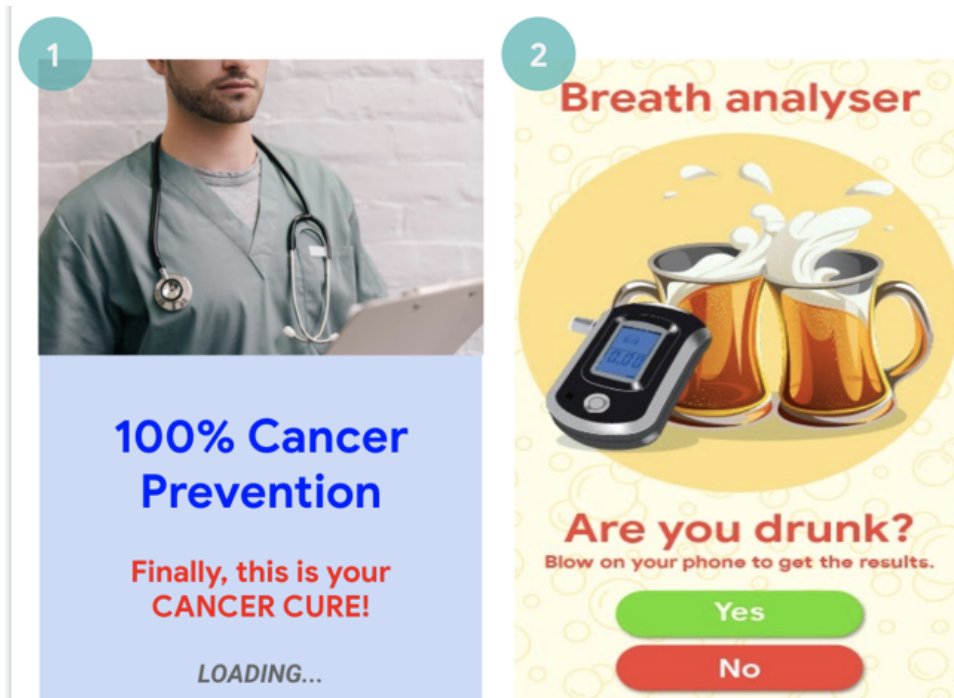
ユーザーを欺こうとするアプリや不正行為を助長するアプリは認められません。たとえば、機能的に不可能だと判断されるアプリが含まれますが、これに限定されません。アプリは、メタデータのあらゆる部分で、アプリの機能に関する説明、画像または動画を正確に開示しなければなりません。オペレーティング システムや他のアプリの機能または警告であるかのように装うことも認められません。デバイスの設定を変更する場合は、ユーザーに通知して同意を得ること、およびユーザーが簡単に元に戻せることが必要です。

誤解を与える表現

アプリの説明、タイトル、アイコン、スクリーンショットなどに、虚偽のまたは誤解を招くような情報や宣伝文句を含めたアプリは認められません。

一般的な違反の例:

- 機能の説明が誤っている、または不正確でわかりにくいアプリ:
 - アプリの説明やスクリーンショットにはレーシング ゲームのように記載されているのに、実際は自動車の絵のブロックパズル ゲーム。
 - ウイルス対策アプリのように記載されているのに、ウイルスを削除する方法を説明したテキストガイドしか含まれていないアプリ。
- Google Play で現在のステータスやパフォーマンスを偽って伝えるデベロッパー名やアプリ名（例: エディターのおすすめ、No.1 アプリ、人気（有料））。
- 医療や健康に関連するコンテンツや機能を備えたアプリのうち、誤解を招くものまたは有害な可能性のあるもの。
- 虫よけアプリなど、実現できない機能を宣伝するアプリ（いたずら、フェイク、冗談として表示されているものも含まれる）。
- レーティングやカテゴリなど（これらに限らず）について、不適切に分類されたアプリ。
- 選挙の投票プロセスに影響を与える可能性のある明らかに虚偽のコンテンツ。
- 政府機関との協力関係があるように偽るアプリ、あるいは適切な認可を受けずに行政サービスを提供または支援するアプリ。
- 定評のある組織の正式なアプリであるかのように偽るアプリ。「ジャスティン ビーバー公式」のようなタイトルは、必要な許可や権利を得ていない限り、認められません。



- (1) 医療や健康に関する誤解を招く宣伝（がんを治す）を掲載しています
 (2) 実現できない機能を宣伝しています（スマートフォンを使った呼吸分析）

デバイス設定の不正な変更

ユーザーの理解や同意を得ずに、アプリ外でユーザーの端末の設定や機能を変更するアプリは認められません。デバイスの設定や機能には、システムやブラウザの設定、ブックマーク、ショートカット、アイコン、ウィジェット、ホーム画面でのアプリの表示などがあります。

その他、次のようなアプリは認められません。

- ・ユーザーの同意を得るが、簡単には元に戻せない方法でデバイスの設定や機能を変更するアプリ。
- ・サードパーティへのサービスとして、または広告表示を目的として、デバイスの設定や機能を変更するアプリや広告。
- ・ユーザーを欺いて、サードパーティ アプリの削除や無効化、またはデバイスの設定や機能の変更を誘導するアプリ。
- ・セキュリティ サービスの一環として確認可能な場合を除き、サードパーティ アプリの削除や無効化、またはデバイスの設定や機能の変更をユーザーに促したり、報奨付きで奨励したりするアプリ。

不正行為の助長

人を欺くことを可能にするアプリや機能的に虚偽の振る舞いをするアプリは認められません。たとえば、ID カード、社会保障番号、パスポート、卒業証書、クレジットカード、運転免許証などを偽造できる、または偽造を補助するアプリが該当します（ただし、これらに限定されません）。アプリは、アプリの機能や内容に関してタイトル、説明、画像または動画を正確に開示し、ユーザーが期待するとおり合理的に正確に機能しなければなりません。

追加のアプリリソース（ゲームアセットなど）は、ユーザーによるアプリの利用に不可欠な場合にのみダウンロード可能です。ダウンロードされるリソースは **Google Play** のすべてのポリシーを遵守する必要があります。また、ダウンロード開始前に、ユーザーにメッセージを表示し、ダウンロード サイズを明確に開示する必要があります。

アプリが「いたずら」や「娯楽目的」などである、と主張する場合でも、アプリがポリシーの適用対象外となることはありません。

一般的な違反の例:

- ・他のアプリやウェブサイトを装ってユーザーに個人情報や認証情報を開示するようにだますアプリ。
- ・同意を得ていない個人や団体の、未確認のまたは実在する電話番号、連絡先、住所、個人情報などを表示するアプリ。
- ・ユーザーの地域、デバイス パラメータ、またはその他のユーザーに応じたデータに基づいて、主たる機能が異なり、その違いについてストアの掲載情報でユーザーに明確に宣伝していないアプリ。
- ・バージョン間で大幅に変更され、その変更についてユーザーに（「[最新情報](#)」欄などで）通知をせず、ストアの掲載情報も更新しないアプリ。
- ・審査時の動作を変更した、またはごまかしているアプリ。

- ・ダウンロードにコンテンツ配信ネットワーク（CDN）を利用しているのに、ダウンロードの前にユーザーにメッセージを表示してダウンロードサイズを開示しないアプリ。

操作されたメディア

虚偽のまたは誤解を招くような情報や宣伝文句を画像、動画、テキストを通じて伝えることを助長する、またはその作成を支援するアプリは認められません。誤解を招く、または虚偽であることが明らかな画像、動画、テキストを助長、または固定化し、配慮が求められる事象、政治、社会問題など、社会的関心事に悪影響をもたらす可能性があるとは判断されたアプリは認められません。

メディアを操作または改変するアプリでは、明瞭さや品質の改善を目的とした慣習的で編集上許容される範囲の調整を超え、メディアが改変されていることを一般的な人が明確に識別できない可能性がある場合は、そのことを明示するか、改変したメディアの透かしを入れなければなりません。ただし、公共性が高い場合や、風刺やパロディーであることが明らかな場合は例外として認められることがあります。

一般的な違反の例:

- ・ 政治的に配慮が求められるイベント中のデモに著名人を登場させるアプリ。
- ・ 配慮が求められるイベントに登場した著名人やメディアを利用して、アプリストアの掲載情報でメディア改変機能を宣伝するアプリ。
- ・ メディア クリップを改変してニュース番組を模倣するアプリ。



(1) このアプリは、メディア クリップを変更してニュース番組を模倣し、有名人や公人を透かしなしで追加する機能を提供します。

不実表示

他者や組織になりすましたアプリやデベロッパー アカウント、または自らの所有者や主な目的を偽ったり隠したりしているアプリやデベロッパー アカウントは認められません。ユーザーに誤解を与えるよう組織的に取り組んでいるアプリやデベロッパー アカウントも許可されません。たとえば、配信元の国を偽装、隠蔽したり、コンテンツを別の国のユーザーに配信したりするアプリやデベロッパー アカウントなどが該当しますが、これらに限定されません。

マルウェア

マルウェアとは、ユーザー、ユーザーのデータ、またはデバイスを危険にさらす恐れのあるすべてのコードを指します。マルウェアには、有害な可能性があるアプリ（PHA）、バイナリ、フレームワーク変更などがあり、トロイの木馬、フィッシング、スパイウェア アプリなど、さまざまなカテゴリに分類できます。ただし、これらに限定せず、継続的に情報を更新して新しいカテゴリを追加しています。

マルウェア

マルウェアに対する **Google** のポリシーはシンプルです。**Google Play** ストアやユーザー デバイスを含め、**Android** エコシステムから悪意のある行為（マルウェアなど）を完全になくす必要があると考えています。この基本原則に沿って、**Google** ユーザーとその **Android** デバイスに安全な **Android** エコシステムを提供できるよう努めています。

マルウェアは、種類や能力はそれぞれ異なりますが、通常は以下のいずれかを目的としています。

- ユーザーのデバイスの完全性を損なわせる。
- ユーザーのデバイスの制御能力を奪う。
- 感染したデバイスをリモートで操作できるようにし、攻撃者自身がアクセスして不正利用する。
- 適切な開示や同意なく、デバイス上の個人データや認証情報を送信する。
- 感染したデバイスからスパムやコマンドを広く送信し、他のデバイスやネットワークに影響を及ぼす。
- ユーザーに対して詐欺行為をする。

アプリ、バイナリ、フレームワーク変更は有害である可能性があります。害を及ぼすことを意図していなかった場合でも、悪意のある動作につながるおそれがあります。アプリ、バイナリ、フレームワークを変更すると、環境に応じて動作も変わるためです。したがって、ある **Android** デバイスには有害であっても、別の **Android** デバイスにはまったく危害を及ぼさない可能性もあります。たとえば、最新バージョンの **Android** が動作しているデバイスは、廃止された **API** を使って悪意のある動作を実行しようとする有害なアプリの影響を受けません。一方、かなり古いバージョンの **Android** が動作しているデバイスは、その危害を受けるおそれがあります。**Android** デバイスとユーザーの一部またはすべてに危険を及ぼすことが明白なアプリ、バイナリ、フレームワーク変更は、マルウェアまたは **PHA** として報告されます。

Google の基本的な信念として、ユーザーの皆様にもデバイスがどのように利用されているのかをご理解いただき、着実なイノベーションと信頼性の高いユーザー エクスペリエンスを実現できるよう、エコシステムの安全性向上にご協力いただきたいと考えています。以下に、これらのマルウェアをカテゴリ別にまとめましたので、ぜひ参考にしてください。

詳しくは、[Google Play プロテクトの記事](#)をご覧ください。

バックドア

有害な可能性のある望ましくない操作を、デバイスに対してリモート制御で実行できるようにするコード。

この操作には、自動的に実行されたときに、他のカテゴリのマルウェアにアプリ、バイナリ、フレームワーク変更を挿入する動作などが含まれます。バックドアとは一般に、悪用も可能な、デバイスへの侵入方法を指します。請求詐欺や商用スパイウェアのようなカテゴリと完全に同列ではありません。そのため、状況によってはバックドアのサブセットが、**Google Play** プロテクトで脆弱性として取り扱われる場合があります。

請求詐欺

詐欺的な方法で、ユーザーに対して自動的な請求を行うコード。

モバイル請求詐欺には、**SMS** 不正利用、通話不正利用、通信不正利用などがあります。

SMS 不正利用

ユーザーの同意なく有料の **SMS** を送信したり、**SMS** アクティビティを偽装（情報開示契約を非表示にし、請求の通知や定期購入の確認のため携帯通信会社から送信される **SMS** メッセージを隠蔽）したりしてユーザーに請求するコード。

SMS の送信動作を技術的には開示していても、**SMS** 不正利用に関係する追加の動作が含まれているコードもあります。例として、情報開示契約の一部を隠してユーザーが読めないようにし、請求の通知や定期購入の確認のため携帯通信会社から送信される **SMS** メッセージを条件付きで隠蔽する場合などがあります。

通話不正利用

ユーザーの同意なく有料番号に電話をかけ、ユーザーに料金を請求するコード。

通信不正利用

ユーザーを欺き、携帯電話料金の請求を通じてコンテンツを購入または定期購入させるコード。

通信不正利用には、有料の **SMS** や通話の不正利用を除く、あらゆるタイプの請求詐欺が含まれます。たとえば、キャリア決済詐欺、ワイヤレス アプリケーション プロトコル（**WAP**）詐欺、モバイルエアタイム送金詐欺なども電話料金詐欺の一種です。中でも最も蔓延しているのが **WAP** 詐欺です。**WAP** 詐欺には、目に見えない **WebView** を気付かれないように読み込み、ユーザーを欺いてボタンをクリックさせるものなどがあります。アクションを実行すると定期購入が開始されますが、確認の **SMS** やメールが隠蔽されることが多いため、料金の請求などの情報がユーザーに通知されません。

ストーカーウェア

適切な通知や同意なく、永続通知を表示せずにデバイス上の個人情報を送信するコード。

ストーカーウェア アプリは通常、**PHA** プロバイダ以外の相手にデータを送信します。

この種のアプリの合法的な使用方法としては、保護者が子どもの居場所を追跡するケースがあります。ただし、データの送信中に永続通知を表示しない場合、本人の理解や許可を得ずに対象者（たとえば配偶者）を追跡する目的でこの種のアプリを使用することはできません。

追跡機能と報告機能を備えたアプリの場合、**Play** ストアで配信できるのは、保護者（家族）による監視または企業管理のみを目的として設計、販売され、ポリシーを遵守しているアプリに限られます。また、下記の要件を完全に遵守する必要があります。

デバイス上のユーザーの行動を監視したり追跡したりする非ストーカーウェア アプリを **Play** ストアで配信するには、最低限、以下の要件を遵守する必要があります。

- ・スパイ行為や内偵をアプリの用途として掲げてはなりません。
- ・追跡機能をユーザーに隠したり、偽装したり、ごまかそうとしたりしてはなりません。
- ・アプリの存在を明確に識別できる永続通知や固有のアイコンをユーザーに表示する必要があります。
- ・利用規約に違反する機能を有効にする手段やそのような機能にアクセスする手段（たとえば、**Google Play** 以外でホストされているポリシー非遵守 **APK** へのリンクなど）を、アプリ内や **Google Play** のアプリ掲載情報で提供してはなりません。
- ・公開する地域でのアプリの合法性の判断については、デベロッパーが全責任を負います。公開先地域で違法と判断されるアプリは削除されます。

サービス拒否（DoS）

ユーザーが気付かないうちにサービス拒否（**DoS**）攻撃を実行するコード、または他のシステムやリソースに対する分散型 **DoS** 攻撃の一部を担うコード。

たとえば、リモート サーバーに大量の **HTTP** リクエストを送信し、過剰な負荷をかけることによって **DoS** を発生させます。

悪意のあるダウンローダ

他の **PHA** をダウンロードするコード（コード自体は有害ではない場合があります）。

次のいずれかに該当するコードは、悪意のあるダウンローダと見なされる可能性があります。

- ・**PHA** を拡散するために作られたと判断するに足る理由があり、ダウンロードされた **PHA** がある、またはアプリをダウンロードしてインストールする可能性のあるコードが含まれている場合。
- ・そのコードによってダウンロードされたアプリの 5% 以上が **PHA** である場合（観測されたアプリ ダウンロード 500 件の最小しきい値で **PHA** のダウンロードが 25 件）。

主要なブラウザとファイル共有アプリは、次の条件を満たす限り、悪意のあるダウンローダとは見なされません。

- ・ユーザーによる操作なしでダウンロードを実行することがない。
- ・すべての **PHA** ダウンロードをユーザーの同意に基づいて開始している。

Android 以外への脅威

Android 以外への脅威を含むコード。

このようなアプリは、**Android** のユーザーやデバイスには危害を及ぼしませんが、他のプラットフォームに危害を及ぼす恐れのある要素を含んでいます。

フィッシング

信頼できる提供元を装い、ユーザーの認証情報や支払い情報を要求してそのデータを第三者に送信するコード。このカテゴリには、伝送中のユーザー認証情報を傍受するコードも該当します。

フィッシングの対象として一般的なのは、銀行口座の認証情報、クレジットカード番号、ソーシャルネットワークやゲームのオンライン アカウント認証情報などです。

昇格させた権限の悪用

アプリ サンドボックスの破壊、昇格権限の取得、セキュリティ関連の重要な機能へのアクセスの変更または無効化などにより、システムの完全性を損なうコード。

次に例を示します。

- **Android** の権限モデルに違反するアプリ、他のアプリから認証情報（たとえば **OAuth** トークン）を窃取するアプリ。
- アプリのアンインストールや停止を防止する機能を悪用するアプリ。
- **SELinux** を無効にするアプリ。

ユーザーの許可なくデバイスの **root** 権限を取得する権限昇格アプリは、**root** 権限取得アプリに分類されます。

ランサムウェア

デバイスまたはデバイス上のデータの一部またはすべてを制御不能にし、元に戻すことと引き換えに、ユーザーに金銭の支払いや操作を要求するコード。

ランサムウェアには、デバイス上のデータを暗号化して復号化する代わりに支払いを要求するものや、デバイスの管理機能を利用して一般的なユーザーでは除去できないようにするものもあります。次に例を示します。

- ユーザーがデバイスを利用できない状態にし、利用できる状態に戻す見返りとして金銭を要求します。
- デバイス上のデータを暗号化し、それを復号するという名目で支払いを要求します。
- デバイスのポリシー管理機能を利用して、ユーザーが除去できないようにします。

デバイス管理の有償化を主な目的としてデバイスと一緒に配布されるコードは、安全なロックと管理の要件、およびユーザーへの適切な開示と同意の要件を満たせば、ランサムウェアから除外される場合があります。

root 権限の取得

デバイスの **root** 権限を取得するコード。

root 権限を取得するコードにも、悪意のあるものといひがあります。たとえば悪意のない **root** 権限取得アプリは、デバイスの **root** 権限を取得することを事前にユーザーに知らせ、他の **PHA** カテゴリに該当する有害な可能性のあるアクションを実行しません。

悪意のある **root** 権限取得アプリは、デバイスの **root** 権限を取得することをユーザーに知らせなかったり、事前にユーザーに知らせつつ、他の **PHA** カテゴリに該当するようなアクションを実行したりします。

スパム

ユーザーの連絡先情報を使って迷惑メールを送信したり、ユーザーのデバイスを迷惑メールの中継機として使用したりするコード。

スパイウェア

適切な通知や同意なく、デバイス上の個人データを送信するコード。

たとえば以下のような情報を、ユーザーに開示せずに、または予期せぬ方法で送信するコードは、スパイウェアと見なされます。

- 連絡先リスト
- アプリが所有していない（たとえば **SD** カードに保存された）写真やその他のファイル
- ユーザーのメールの内容
- 通話履歴
- **SMS** のログ
- デフォルト ブラウザのウェブ履歴やブックマーク
- 他のアプリの **/data/** ディレクトリの情報

ユーザーについて密かに調査していると見なされる行為も、スパイウェアとして報告されます。たとえば、音声や通話の録音、アプリデータの窃取などがこれに該当します。

トロイの木馬

一見すると無害でも（たとえばただのゲームだと謳っているゲーム）、ユーザーに対して望ましくないアクションを実行するコード。

通常、このカテゴリは他の **PHA** カテゴリと組み合わせて使用します。トロイの木馬は、無害なコンポーネントと、隠された有害なコンポーネントで構成されています。たとえば、ユーザーがゲームをしているバックグラウンドで、気付か

ないうちにユーザーのデバイスから有料の SMS メッセージを送信するゲームは、トロイの木馬です。

一般的ではないアプリに関する注意

新しいアプリやあまり見かけないアプリは、安全と確認できるだけの十分な情報がないため、Google Play プロテクトで「一般的ではないアプリ」として分類されることがあります。そのアプリが必ずしも有害であることを意味するわけではありませんが、安全であることを確認するにはさらに審査が必要になります。

バックドア カテゴリに関する注意

バックドア マルウェア カテゴリに分類されるかどうかは、コードの動作に応じて判断されます。バックドアに分類される必要条件是、そのコードが自動的に実行されたときに、他のカテゴリのマルウェアにコードを挿入する動作が可能になるかどうかです。たとえば、動的コードの読み込みが可能で、動的に読み込まれたコードがテキスト メッセージを抽出する場合、そのアプリはバックドア マルウェアに分類されます。

ただし、アプリが任意のコード実行を許可していて、そのコード実行を追加した目的が悪意のある行為だと判断できる理由がない場合、そのアプリはバックドア マルウェアではなく脆弱性として取り扱われ、デベロッパーにパッチの適用が要請されます。

モバイルの望ましくないソフトウェア

このポリシーは、Google の望ましくないソフトウェアのポリシーを土台とし、Android エコシステムと Google Play ストアの原則を概説するものです。原則に反するソフトウェアはユーザーの利便性に悪影響を与える可能性があるため、Google はそうしたソフトウェアからユーザーを守る措置を取ります。

モバイルの望ましくないソフトウェア

Google には、「成功の条件はユーザーを第一にすること」という理念があります。Google の [ソフトウェア原則](#)と [望ましくないソフトウェアのポリシー](#)では、優れたユーザー エクスペリエンスを提供するソフトウェアに関する一般的な推奨事項を紹介しています。このポリシーは、Google の望ましくないソフトウェアのポリシーを土台とし、Android エコシステムと Google Play ストアの原則を概説するものです。原則に反するソフトウェアはユーザーの利便性に悪影響を与える可能性があるため、Google はそうしたソフトウェアからユーザーを守る措置を取ります。

[望ましくないソフトウェアのポリシー](#)に記載のとおり、望ましくないソフトウェアの大半にいくつかの共通点があります。

- 表示に虚偽がある。すなわちできていないことをできると約束している。
- ユーザーをだましてインストールさせようとする、または別のプログラムのインストールに便乗する。
- ユーザーにメインとなる重要な機能の一部を説明していない。
- ユーザーのシステムに予期しない方法で影響を与える。
- ユーザーが気付かいうちに個人情報を収集または送信する。
- 安全な処理 (HTTPS による送信など) を行わずに個人情報を収集または送信する。
- 他のソフトウェアとバンドル (同梱) され、その存在が開示されていない。

モバイル デバイスにおけるソフトウェアは、アプリ、バイナリ、フレームワーク変更などのコードで形成されます。ソフトウェア エコシステムにとって有害なソフトウェア、またはユーザー エクスペリエンスに悪影響を与えるソフトウェアを防ぐため、Google はこうした原則に反するコードに対して措置を取ります。

下記のように、望ましくないソフトウェアのポリシーに基づき、その適用範囲をモバイル ソフトウェアに拡大します。望ましくないソフトウェアのポリシーと同様に、Google では引き続きモバイルの望ましくないソフトウェアのポリシーを手直しし、新たな不正行為に対処していきます。

透明性の高い動作と明確な開示

コードはすべて、ユーザーへの約束のとおり配信する必要があります。アプリは通知済みの機能をすべて提供する必要があります。アプリがユーザーを混乱させてはなりません。

- アプリは機能と目的を明確にする必要があります。
- アプリがシステムに対して行う変更について、ユーザーに明示して、わかりやすく説明します。すべての重要なインストール オプションと変更についてユーザーが確認して承認できるようにします。
- ソフトウェアがユーザーのデバイスの状態に関して、偽ってはなりません (システムがセキュリティ上危機的な状況にある、ウイルスに感染しているなど)。
- 広告トラフィックやコンバージョンを増やすことを目的とした無効な操作を行ってはなりません。
- 他者 (別のデベロッパー、会社、組織など) または別のアプリになりまして、ユーザーを誤解させるようなアプリは認められません。アプリが無関係の誰かに関係がある、または承認されているとほめかしてはなりません。

違反の例:

- 広告の不正行為
- なりすまし

ユーザーデータの保護

ユーザーの個人情報や機密情報のアクセス、収集、使用、共有について明らかにして、透明性を高めます。ユーザーデータの使用に関して、該当するすべてのユーザーデータ ポリシーを遵守し、データ保護の予防措置をすべて講じる必要があります。

- ユーザーデータを収集してデバイスから送信する前に、収集に関してユーザーに同意を求めます。これには、サードパーティ アカウント、メールアドレス、電話番号、インストール済みのアプリ、ファイル、位置情報に関するデータのほか、ユーザーが収集を予想していない個人情報や機密情報が含まれます。
- 収集したユーザーの個人情報や機密情報は、最新の暗号手法を使用して（HTTPS 経由などで）転送するなど、安全に取り扱う必要があります。
- モバイルアプリなどのソフトウェアが、ユーザーの個人情報や機密情報をサーバーに送信する場合、アプリの機能に関連する場合のみに限定する必要があります。

違反の例:

- データ収集（[スパイウェア](#)を参照）
- 制限付き権限の不正使用

ユーザーデータ ポリシーの例:

- [Google Play ユーザーデータ ポリシー](#)
- [GMS 要件のユーザーデータ ポリシー](#)
- [Google API サービスのユーザーデータ ポリシー](#)

モバイル エクスペリエンスへの悪影響を防止

ユーザー エクスペリエンスは、単純でわかりやすく、ユーザーの明確な選択に基づく必要があります。ユーザーに明確な価値を提案すべきであり、宣伝した、または期待されているユーザーの利便性を損なってはなりません。

- 予期しない方法で広告をユーザーに表示してはなりません。これには、デバイス機能のユーザビリティが低下するまたは妨げられる場合、広告が適切な同意や出所の明示なく、配信元のアプリの環境外で表示され簡単に閉じられない場合などが該当します。
- アプリは他のアプリやデバイスのユーザビリティを妨げないようにする必要があります。
- アンインストールが必要な場合は、ユーザーにその旨を明示してください。
- モバイル ソフトウェアが、デバイスの OS や他のアプリからのメッセージであるかのように装ってはなりません。他のアプリやオペレーティング システムからのユーザーへの通知、特に OS への変更に関する通知を抑制してはなりません。

違反の例:

- 混乱させる広告
- システム機能の不正使用または模倣

広告の不正行為

広告の不正行為は固く禁止されています。広告ネットワークを騙す広告インタラクション、つまり本物のユーザーがクリックしたかのように装ってトラフィックを生成する行為は、[無効なトラフィック](#)に該当します。広告の不正行為は、デベロッパーが禁止されている方法で広告を実装した結果による場合があります。たとえば、非表示の広告を掲載する、広告を自動的にクリックする、情報を変更する、その他の方法で人間以外によるアクション（スパイダー、ボットなど）または細工された人間のアクティビティを利用して無効な広告トラフィックを生成する場合などがあります。無効なトラフィックや広告の不正行為は、広告主、デベロッパー、ユーザーにとって有害であり、モバイル広告エコシステムにおける長期的な信頼の損失につながります。

一般的な違反の例:

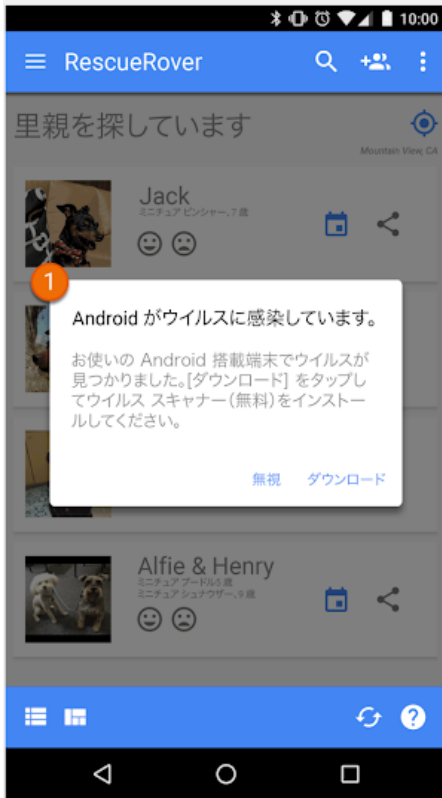
- ユーザーに表示されない広告を掲載するアプリ。
- ユーザーの意図に反して広告のクリックを自動的に生成する、またはクリック件数を不正に付与できるネットワークトラフィックを生成するアプリ。
- インストール アトリビューション クリックを偽造して送信し、送信元のネットワークからではないインストールに対して報酬を得るアプリ。
- ユーザーがアプリ インターフェース内にいないときに広告をポップアップ表示するアプリ。
- アプリによる広告枠の虚偽の表示や表明。たとえば、実際には **Android** デバイスで実行されているのに **iOS** デバイスで実行されていると広告ネットワークに通知するアプリや、収益化対象のパッケージ名を偽るアプリ。

システム機能の不正使用または模倣

通知や警告のようなシステム機能を装う、または阻害するアプリや広告は認められません。システムレベルの通知は、アプリの重要な機能でのみ使用できます。たとえば、航空会社のアプリがユーザーに特典を知らせる場合や、ゲームがユーザーにゲーム内のプロモーションを知らせる場合です。

一般的な違反の例:

- システムの通知や警告を通じて配信されるアプリや広告:



- ① このアプリで表示されるシステム通知は、広告の配信に使用されています。

広告でのその他の例については、[広告に関するポリシー](#)をご覧ください。

なりすまし

デベロッパーが他者や他者のアプリであるかのように装う行為は、ユーザーを誤解させるだけでなく、デベロッパー コミュニティの信頼を損なうことにもなります。他者になりすましてユーザーを誤解させるようなアプリは禁止されています。

なりすまし

他者（別のデベロッパー、会社、組織など）または別のアプリになりまして、ユーザーを誤解させるようなアプリは認められません。アプリが無関係の誰かに関係がある、または承認されているとほのめかしてはなりません。アプリのアイコン、説明、タイトル、アプリ内要素についても、他者や他のアプリとの関係を誤解させるようなものは使用しないようご注意ください。

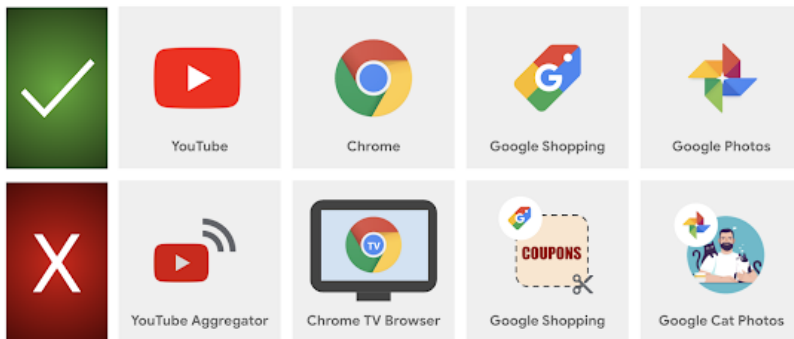
一般的な違反の例:

- 別の会社やデベロッパーに関係があるかのような虚偽をほのめかすデベロッパー:



① このアプリに表示されるデベロッパー名は、実際には存在しない **Google** との正式な関係があるかのようにほのめかしています。

- 既存のプロダクトやサービスのものとユーザーが混同しかねない、アプリのタイトルやアイコン:



収益化と広告

Google Play では、有料配布、アプリ内アイテム、定期購入、広告ベースモデルなど、デベロッパーとユーザーにメリットのあるさまざまな収益化戦略がサポートされています。ユーザーに最適な利便性を実現するために、デベロッパーはこうしたポリシーを遵守する必要があります。

支払い

1. Google Play で提供するアプリやダウンロードに課金する場合、Google Play の課金システムを決済方法として使用しなければなりません。

2. Play で配信するアプリにおいて、アプリの機能、デジタル コンテンツ、商品などの機能やサービスへのアクセスに対する支払いを必要とする、または受け取る場合は、Google Play の課金システムを決済方法として使用しなければなりません。

(i) Google Play の課金システムの使用を必要とするアプリの機能やサービスの例としては、以下のもののアプリ内購入が挙げられますが、これらに限定されません。

- アイテム (仮想通貨、ライフの追加、プレイ時間の追加、アドオン アイテム、キャラクター、アバターなど)
- 定期購入サービス (フィットネス、ゲーム、出会い、教育、音楽、動画、その他のコンテンツの定期購入サービス)
- アプリの機能やコンテンツ (アプリの広告のないバージョン、無料バージョンでは使用できない新機能など)

- ・クラウドソフトウェア、クラウドサービス（データストレージサービス、ビジネス効率化ソフトウェア、会計管理ソフトウェアなど）

(ii) 以下の場合は **Google Play** の課金システムを使用しないでください。

- ・主に以下に対する支払いの場合:
 - ・物理的な商品（食料品、衣料品、家庭用品、電子機器など）の購入またはレンタル
 - ・物理的なサービス（運賃、清掃サービス、航空運賃、ジムの会費、食品の配達、ライブイベントのチケットなど）の購入
 - ・クレジットカードの請求、公共料金（有線通信サービス、電気通信サービスなど）に関する送金

注: 一部の市場では、物理的な商品やサービスを販売するアプリにも **Google Pay** を提供しています。詳しくは、[Google Pay デベロッパー ページ](#) をご覧ください。

- ・ピアツーピア支払い、オンラインオークション、非課税寄付に関する支払い
- ・[現金を伴うギャンブル、ゲーム、コンテスト](#)に関するポリシーの[ギャンブル アプリ](#)のセクションに記載されているようなオンラインギャンブルを推進するコンテンツやサービスに対する支払い
- ・**Google** の[ペイメントセンターのコンテンツ ポリシー](#)で許可されない商品カテゴリに関する支払い

3. 上記の 2 (ii) に該当しないアプリは、**Google Play** の課金システム以外の支払い方法に、直接または間接を問わず、ユーザーを誘導することはできません。この禁止事項には、以下を介してユーザーを別の支払い方法に誘導することが含まれますが、これらに限定されません。

- ・**Google Play** でのアプリの掲載情報
- ・購入可能なコンテンツに関連するアプリ内プロモーション
- ・アプリ内ウェブ表示、ボタン、リンク、メッセージ、広告、その他の行動を促すフレーズ
- ・アカウントの作成フローや登録フローなどで、アプリから **Google Play** の課金システム以外の支払い方法にユーザーを誘導するアプリ内ユーザー インターフェース フロー

4. アプリ内仮想通貨の使用は、その通貨が購入されたアプリやゲーム内のみに限定しなければなりません。

5. デベロッパーは、アプリの利用規約や価格、および購入のために提供されるアプリ内の機能や定期購入について、ユーザーに明確かつ正確に伝える必要があります。アプリ内の価格設定は、ユーザー向けの **Play** 課金インターフェースに表示される価格と一致している必要があります。個別課金または追加課金が必要になるアプリ内機能について、**Google Play** の説明で言及する場合、特定機能の利用には支払いが必要になるとアプリの掲載情報に明記する必要があります。

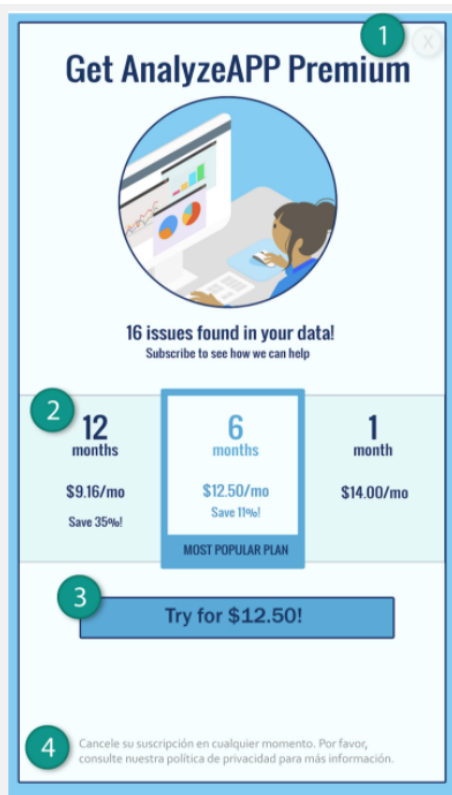
6. 仮想アイテムをランダムに受け取る購入メカニズム（ルートボックス、ガチャが該当しますが、これらに限定されません）をアプリやゲームで提供する場合は、アイテムを取得できる確率を、購入直前にタイミングよく明確に開示する必要があります。

定期購入

デベロッパーは、アプリ内で提供する定期購入によるサービスまたはコンテンツについて、ユーザーの誤解を招かないようにしなければなりません。どのアプリ内プロモーションまたはスプラッシュ画面でも明確に伝えることが重要です。

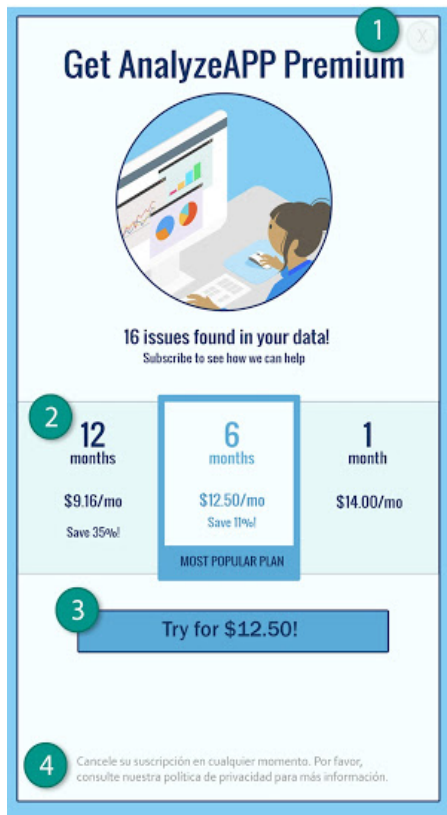
アプリ内で: 提供する内容について透明性の高い情報を提供する必要があります。これには、提供に関する条件、定期購入にかかる費用、請求の期間と頻度、アプリを利用するうえで定期購入が必須かどうかを明示することも含まれます。ユーザーが追加の操作を行わなくても、これらの情報を確認できるようにしてください。

一般的な違反の例:



- ① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.
- ② Offer only displays pricing in terms of monthly cost and users may not understand that they will be charged a six month price at the time they subscribe.
- ③ Offer only shows the introductory price and users may not understand what they will automatically be charged at the end of the introductory period.
- ④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

- 月単位の定期購入において、毎月自動的に更新されて請求が発生することをユーザーに知らせていない。
- 年単位の定期購入において、月単位の価格が最も目立つように表示されている。
- 定期購入の価格設定や条件のローカライズが不完全である。
- 定期購入しなくてもコンテンツを利用できるのに、そのことがアプリ内プロモーションに明示されていない。
- SKU 名が定期購入の本質を正確に表していない（たとえば「無料試用」とあるのに請求が繰り返し自動発生する）。



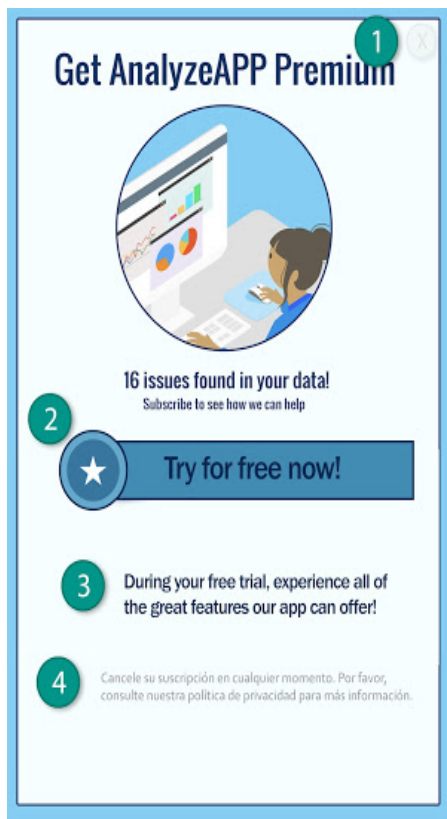
- ① 閉じるボタンがはっきり表示されておらず、機能を利用するには定期購入しなければならないとユーザーが誤解する恐れがあります。
- ② 月単位の料金しか示されておらず、定期購入する際に 6 か月分の料金が請求されることをユーザーが認識できない恐れがあります。
- ③ お試し価格しか示されておらず、お試し期間終了後に自動的に請求される料金をユーザーが把握できない恐れがあります。
- ④ ユーザーが提供される内容を完全に理解できるよう、利用規約と同じ言語にローカライズする必要があります。

無料試用とお試し特典

ユーザーが定期購入に登録する前に: 特典の条件（期間、価格設定、利用できるコンテンツやサービスなど）について明確かつ正確に説明する必要があります。無料試用から有料定期購入にいつどのような方法で移行するのか、有料の定期購入はいくらかかるか、有料の定期購入に移行したくない場合は解約できることについて、ユーザーにわかりやすく説明してください。

一般的な違反の例:

- ・ 無料試用またはお試し価格がいつまで続くかが明確に説明されていない特典。
- ・ 特典期間が終了すると有料定期購入に自動的に登録される場合に、そのことが明確に説明されていない特典。
- ・ 試用しなくてもコンテンツを利用できる場合に、そのことを明示していない特典。
- ・ 価格設定と条件のローカライズが不完全な特典。



- ① 閉じるボタンがはっきり表示されておらず、機能を利用するには無料試用に登録しなければならないとユーザーが誤解する恐れがあります。
- ② 無料試用が強調されており、試用期間終了後に料金が自動的に請求されることをユーザーが認識できない恐れがあります。
- ③ 試用期間が明記されておらず、いつまで定期購入コンテンツに無料でアクセスできるかをユーザーが認識できない恐れがあります。
- ④ ユーザーが提供される内容を完全に理解できるよう、利用規約と同じ言語にローカライズする必要があります。

定期購入の管理と解約

ユーザーが定期購入をどのような方法で管理または解約できるかについて、アプリで明確に開示しておく必要があります。

デベロッパーの責任で、定期購入、解約、払い戻しのポリシーを変更する際はユーザーに通知し、それらのポリシーが適用される法律を遵守していることを確認します。

広告

ユーザーを欺いたり、混乱させたりするような広告を含むアプリは認められません。広告は、その広告を配信するアプリ内でのみ表示できます。アプリ内で配信される広告もアプリの一部と見なされます。アプリ内で表示される広告は Google のすべてのポリシーを遵守している必要があります。ギャンブルの広告に関するポリシーについては、[こちら](#)をクリックしてください。

広告目的での位置情報の使用

権限に基づくデバイスの位置情報を広告配信にも利用するアプリは、[個人情報と機密情報](#)に関するポリシーの対象となり、以下の要件も遵守する必要があります。

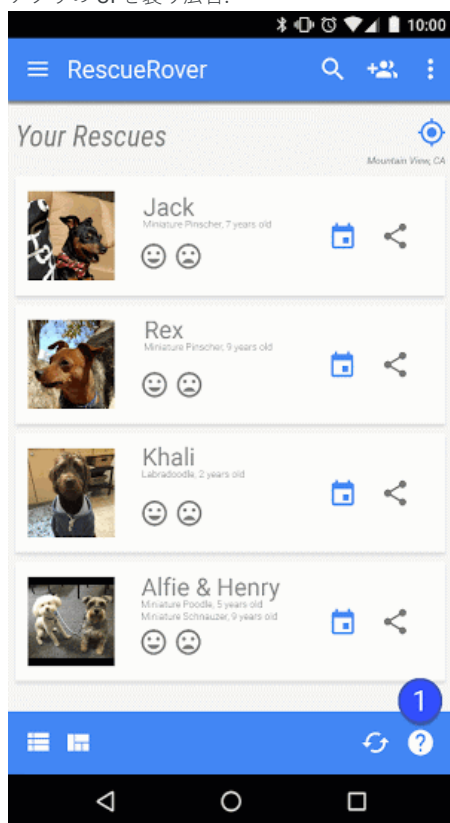
- 権限に基づくデバイスの位置情報を広告目的で利用または収集するには、その旨をユーザーに対して明確にし、アプリに義務付けられているプライバシー ポリシーに明記する必要があります。該当する広告ネットワークのプライバシー ポリシーで位置情報の使用について定められている場合にそれにリンクすることも含まれます。
- [位置情報の権限](#)に関する要件のとおり、位置情報の権限は、アプリ内で現在提供している機能やサービスを実装する場合にのみリクエストできます。広告利用のみを目的としてデバイスの位置情報の権限をリクエストすることは認められません。

虚偽の広告

アプリのユーザー インターフェイスまたはオペレーティング システムからの通知や警告を装う広告は認められません。各広告をどのアプリが配信しているかをユーザーに明示する必要があります。

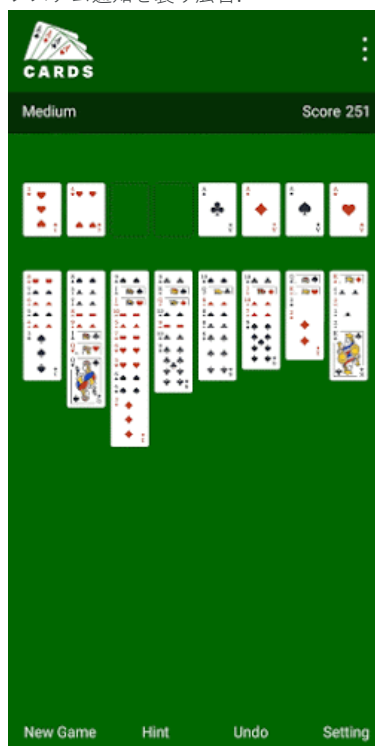
一般的な違反の例:

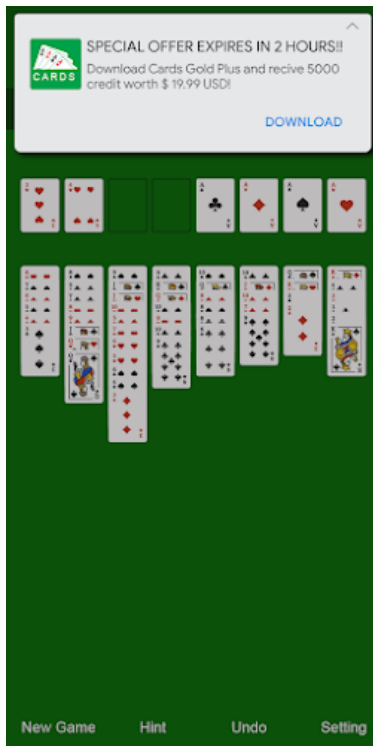
- アプリの UI を装う広告:



① このアプリの疑問符アイコンは、外部のランディング ページにユーザーを移動させる広告です。

- システム通知を装う広告:





さまざまなシステム通知を装う広告の例を上記に示します。

ロック画面の収益化

ロック画面自体がアプリの唯一の目的である場合を除いて、ロック中のデバイスの表示を収益化する広告や機能をアプリに導入することは認められません。

混乱させる広告

混乱させる広告とは、予期しない方法でユーザーに表示され、意図しないクリックや、デバイス機能のユーザビリティの低下を招くものを指します。

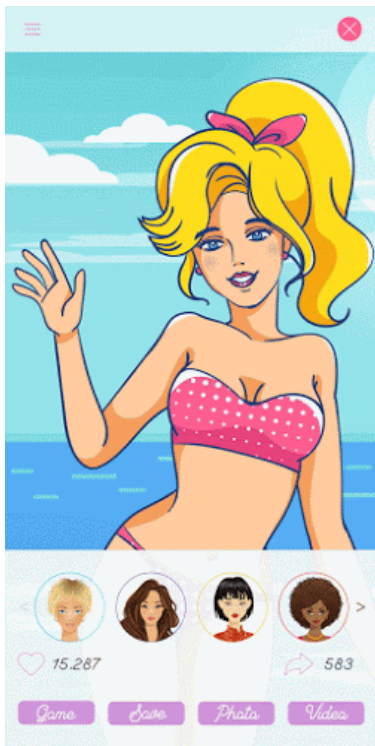
アプリの全機能の利用と引き換えに広告のクリックや個人情報の提供をユーザーに強制することはできません。インタースティシャル広告は、その広告を配信するアプリ内でのみ表示できます。アプリの通常の利用を妨げるようなインタースティシャル広告などを表示する場合、そういった広告は無条件で簡単に閉じられるようにする必要があります。

一般的な違反の例:

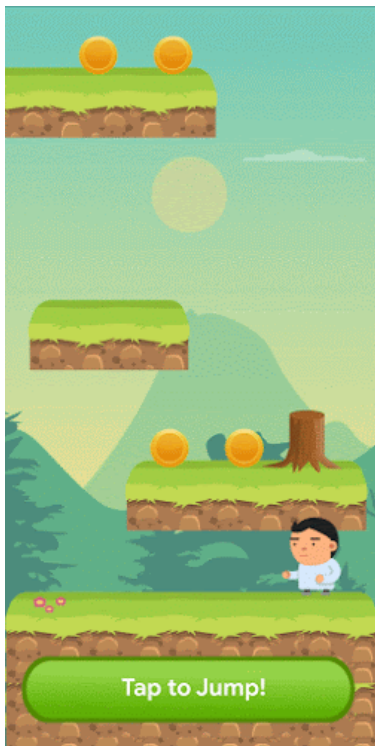
- 画面全体を占拠する、または通常の使用を妨げるうえに、閉じる手段をわかりやすく提示しない広告:



- ① この広告には閉じるボタンがありません。
- 偽りの閉じるボタンを使用したり、別の機能のためにユーザーが通常タップするアプリの領域に急に広告を表示したりして、ユーザーにクリックさせようとする広告。



偽りの閉じるボタンを使用している広告



ユーザーがアプリ内の機能を使用するために通常タップする領域に突然表示される広告

アプリ、サードパーティの広告、デバイスの機能に対する妨害

アプリで広告を表示する場合は、他のアプリ、広告、デバイスの操作（システムやデバイスのボタン、端子を含む）の邪魔にならないようにする必要があります。これには、オーバーレイ、コンパニオン機能、広告ユニットのウィジェット化も含まれます。広告は、その広告を配信するアプリ内でのみ表示する必要があります。

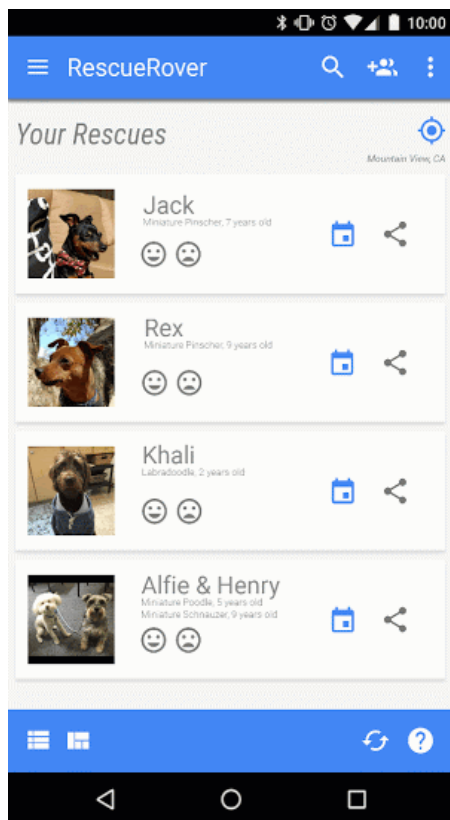
一般的な違反の例:

- 広告を配信するアプリの外に表示される広告:



説明: ユーザーがこのアプリからホーム画面に移動すると、ホーム画面に突然広告が表示されます。

- ホームボタンのほか、明らかにアプリの終了のために設計された機能によって表示される広告:

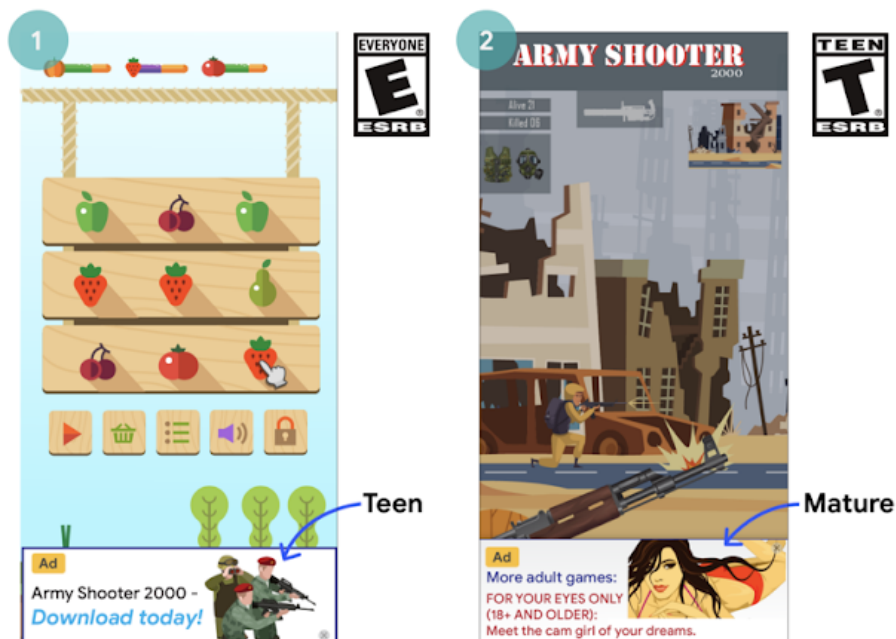


説明: ユーザーがアプリを終了してホーム画面に移動しようとしたところを広告が妨げています。

不適切な広告

アプリ内の広告は、コンテンツそのものが Google のポリシーを遵守しているだけでなく、アプリの対象ユーザーにとって適切である必要もあります。

一般的な違反の例:



- ① この広告（13 歳以上）はアプリの対象ユーザー（7 歳以上）に不適切です
- ② この広告（成人向け）はアプリの対象ユーザー（12 歳以上）に不適切です

Android 広告 ID の使用

Google Play 開発者サービス バージョン 4.0 では、広告と分析のプロバイダが使用する新しい API と ID が導入されました。この ID を使用するための規約は以下のとおりです。

- **用途:** Android 広告 ID は広告とユーザーの分析以外で使用してはなりません。ID の各アクセスについて [インタレスト ベース広告をオプトアウト] または [広告のパーソナライズをオプトアウトする] の設定のステータスを確認する必要があります。
- **個人を特定できる情報またはその他の ID との関連付け:**
 - 広告での使用: 広告 ID を永続的なデバイス ID（SSAID、MAC アドレス、IMEI など）に関連付けることはできません。広告 ID は、ユーザーの明示的な同意がある場合にのみ、個人を特定できる情報に関連付けることができます。
 - 分析での使用: 広告 ID は、ユーザーの明示的な同意がある場合のみ、個人を特定できる情報、または永続的なデバイス ID（SSAID、MAC アドレス、IMEI など）に関連付けることができます。
- **ユーザーの選択を優先:** ユーザーの明示的な同意なしに、リセットの際に新しい広告 ID を以前の広告 ID や以前の広告 ID からのデータにリンクしてはなりません。さらに、ユーザーが指定した [インタレスト ベース広告をオプトアウト] または [広告のカスタマイズをオプトアウトする] の設定を遵守する必要があります。ユーザーがこの設定を有効にした場合は、広告目的でユーザーのプロフィールを作成したり、ユーザーをパーソナライズド広告のターゲットに設定したりするために広告 ID を使用してはなりません。ただし、コンテンツ ターゲット広告、フリークエンシー キャップ、コンバージョン トラッキング、レポート、セキュリティや不正行為の検出などに使用することはできます。
- **ユーザーに対する透明性:** 広告 ID の収集と使用、およびこうした規約の遵守について、法的に適切なプライバシーに関するお知らせでユーザーに開示する必要があります。Google が掲げるプライバシーの基準については、[ユーザーデータ](#)に関するポリシーをご覧ください。
- **利用規約の遵守:** 広告 ID は、こうした利用規約を遵守する場合にのみ使用できます。ビジネスにおいてこの ID が第三者と共有された場合の使用についても同様です。Google Play にアップロードまたは公開されるすべてのアプリでは、広告 ID（デバイスで利用可能な場合）を使用する必要があります。この広告 ID は、広告を目的とした他のあらゆるデバイス ID に取って代わるものです。

ファミリー向け広告プログラム

[ファミリー ポリシー](#)に記載されているとおり、子供のみをターゲット ユーザーとするアプリで広告を配信する場合は、下記の広告 SDK 認定の要件を含め、Google Play ポリシーの遵守を自己認定している広告 SDK を使用しなければなりません。アプリのターゲット ユーザーに子供と大人の両方が含まれる場合は、ユーザーを年齢層別に分ける手段を実装し、子供に配信される広告がこれらの自己認定広告 SDK からのみ配信されるようにする必要があります。ファミリー向けプログラムのアプリでの広告配信には、必ず自己認定広告 SDK を使用する必要があります。

Google Play 認定広告 SDK の使用が必須なのは、広告 SDK を使用して子供に広告を配信する場合のみです。以下については、広告 SDK による Google Play での自己認定がなくても許可されます。ただし、広告コンテンツとデータ収集行為が Google Play の[ユーザーデータに関するポリシー](#)と[ファミリー ポリシー](#)を遵守しているかどうかについては責任を持って確認する必要があります。

- 自社による広告配信（SDK を使用して自社アプリまたは自社のその他のメディアや商品の相互プロモーションを管理するなど）
- 広告主との直接取引（SDK を使用して広告枠を管理する）

広告 SDK 認定の要件

- どのような広告コンテンツや行動が好ましくないとされるのかを定義し、そのようなコンテンツや行動を広告 SDK の規約やポリシーで禁止していること。定義の内容は Play のデベロッパー プログラム ポリシーを遵守するものである必要があります。
- 対象年齢別区分に沿って広告クリエイティブをレーティングする方法を整備していること。対象年齢別区分には、少なくとも「全ユーザー対象」と「15 歳以上推奨」を含める必要があります。レーティング手法は、下のお問い合わせフォームへご記入いただいた後、Google が SDK に提供する手法に整合させる必要があります。
- サイト運営者が広告配信に関して子供向け取り扱いを求めるリクエストを（リクエストごと、またはアプリごとに）行えるようにしていること。そうした取り扱いは、米国の[児童オンライン プライバシー保護法（COPPA）](#)や EU の[一般データ保護規則（GDPR）](#)など、適用される法律と規制を遵守していなければなりません。Google Play では子供向け取り扱いの一環として、広告 SDK でパーソナライズド広告、インタレスト ベース広告、リマーケティングを無効にする必要があります。
- [Play のファミリー向け広告と収益化ポリシー](#)を遵守し、[教師承認済みプログラム](#)の要件を満たしている広告フォーマットを、サイト運営者が選択できるようにすること。
- 子供向けの広告配信にリアルタイム ビッドダーが使用されている場合は、クリエイティブが審査済みで、プライバシーインジケータがビッドダーに反映されていることを確認すること。

- 広告 SDK がすべての認定要件を遵守しているかどうかを検証するために十分な情報（下記のお問い合わせフォームに示す情報など）を Google に提供し、その後も情報提供を求められた場合は適時に対応すること。

注: 広告 SDK は、サイト運営者に適用される可能性のあるすべての児童関連法令を遵守した広告配信をサポートしなければなりません。

配信プラットフォームから子供に広告を配信する際のメディエーションの要件:

- Play 認定広告 SDK のみを使用するか、メディエーションから配信されるすべての広告が上記の要件を遵守したものとなるように必要な対策を講じること。
- 広告コンテンツのレーティングと、適用される子供向け取り扱いを示すために必要な情報をメディエーション プラットフォームに渡すこと。

[こちらの自己認定広告 SDK の一覧](#)をご覧ください。

また、自己認定を希望する広告 SDK があればこちらの[お問い合わせフォーム](#)をご紹介ください。

ストアの掲載情報とプロモーション

アプリのプロモーションや掲載順位はストアの質に大きな影響を及ぼします。Google Play では、スパムにあたるようなストアの掲載情報、質の低いプロモーション、アプリの掲載順位を人為的に高めようとする行為は避けてください。

アプリのプロモーション

ユーザーやデベロッパー エコシステムに対して虚偽のまたは有害なプロモーションに直接間接を問わず関与するようなアプリや、そうしたプロモーションから利益を得るようなアプリは認められません。これには、以下の行為に関与するアプリも含まれます。

- システムの通知や警告に類似した通知を行うほか、ウェブサイト、アプリ、または他のプロパティに虚偽の広告を掲載する。
- ユーザーに通知して操作させることなく、Google Play へのリダイレクトやアプリのダウンロードを開始する手法でプロモーションやインストールを行う。
- SMS サービス経由の未承諾のプロモーション。

アプリと関連付けた広告ネットワークやアフィリエイトがこのポリシーを遵守し、禁止されたプロモーションを実施することのないよう、デベロッパーが責任を持って管理してください。

メタデータ

誤解を招くメタデータ、誤った形式のメタデータ、非記述的なメタデータ、無関係なメタデータ、過大なメタデータ、不適切なメタデータをアプリに設定することは認められません。メタデータには、アプリの説明、デベロッパー名、タイトル、アイコン、スクリーンショット、プロモーション画像などがあります（ただしこれらに限定されません）。デベロッパーはアプリに、わかりやすく的確な説明を提供しなければなりません。また、アプリの説明に、出典不明または匿名のユーザーからの称賛や推薦の言葉を含めることは認められません。

ここに記載の要件に加えて、特定の Play サービスのデベロッパー ポリシーで追加のメタデータ情報の提供を求めることがあります。

一般的な違反の例:



- ① 出典不明または匿名のユーザーからの称賛や推薦の言葉
- ② アプリやブランドの比較データ
- ③ 単語を寄せ集めたもの、カテゴリが狭すぎる / 広すぎる単語リスト

ストアの掲載情報での不適切なテキスト、画像、動画の例:

- ・ 性的なものを暗示する画像や動画。胸部、でん部、性器のほか、フェティシズムの対象となる身体部位など、性的なものを暗示する画像の掲載は写実性を問わず避けてください。
- ・ アプリのストアの掲載情報における、冒とく的表現、下品な表現など、一般ユーザーに不適切な表現の使用。
- ・ アプリのアイコン、プロモーション画像、動画での露骨な暴力の描写。
- ・ 違法薬物の使用に関する描写。教育、ドキュメンタリー、科学、芸術（EDSA）に該当するコンテンツの場合でも、ストアの掲載情報に含める内容は、すべてのユーザーに適したものにする必要があります。

おすすめの方法:

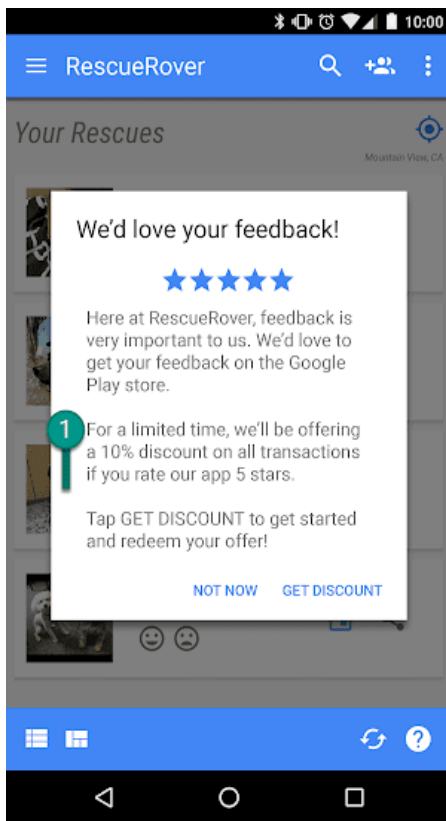
- ・ アプリの優れている点を強調します。アプリについて興味深い、注目すべき事実を紹介し、アプリの特長をユーザーに伝えるようにします。
- ・ アプリのタイトルと説明が、アプリの機能を正確に表すようにします。
- ・ キーワードや関連情報を繰り返したり、無関係なものを含めたりしないようにします。
- ・ アプリの説明は簡潔でわかりやすくします。説明が短くなるほど、特に画面の小さいデバイスでは、ユーザーの利便性が高まります。長すぎる、詳しくすぎる、形式が不正、反復が多すぎるなどの場合、このポリシーへの違反となります。
- ・ スタアの掲載情報は一般ユーザーに適した内容にする必要があります。不適切なテキスト、画像、動画を掲載情報に含めることは避け、上記のガイドラインを遵守してください。

ユーザーの評価、レビュー、インストール

デベロッパーは、いかなるアプリについても、Google Play での掲載順位を操作しようとしてはなりません。これには、プロダクトに対する良い評価、レビュー、インストール数を不正な手段（捏造、報酬付与など）でつり上げることが含まれますが、これらに限定されません。

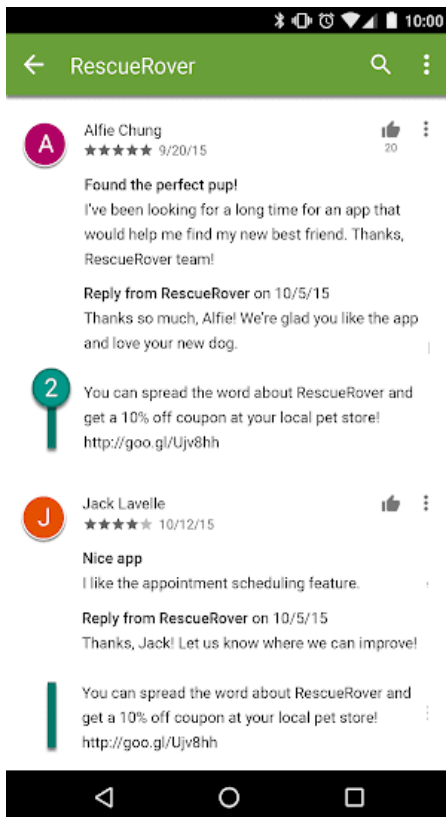
一般的な違反の例:

- ・ 報酬付きでアプリの評価をユーザーに依頼する。



① このお知らせでは、高い評価の見返りとして割引をユーザーに持ちかけています。

- アプリの評価を繰り返し送信することで、Google Play での掲載順位を操作する。
- 不適切なコンテンツ（アフィリエイト、クーポン、ゲームのコード、メールアドレス、ウェブサイトや他のアプリへのリンクなど）を含むレビューを送信する、またはユーザーにその送信を奨励する。



② このレビューでは、クーポンを提供して、RescueRover アプリを宣伝するようにユーザーに奨励しています。

評価やレビューはアプリの品質を測る指標となるものです。ユーザーはそれらが真実で妥当なものと信頼しています。ユーザーのレビューに返信する際のポイントを紹介します。

- ・ ユーザーから指摘された問題に的を絞って返信しましょう。高く評価するようユーザーに求めてはなりません。
- ・ サポート アドレスやよくある質問のページなど、参考となるリソースへの参照は記載できます。

コンテンツのレーティング

Google Play のコンテンツのレーティング システムは IARC（International Age Rating Coalition）を採用しており、デベロッパーはユーザーの各国に応じたレーティングをユーザーに示すことができます。地域の IARC 機関は、アプリ内のコンテンツの対象年齢を判断するためのガイドラインを管理しています。Google Play では、コンテンツのレーティングが指定されていないアプリは認められません。

コンテンツのレーティングの用途

コンテンツのレーティングを使って、ユーザー（特に保護者）に、不快に感じる可能性のあるコンテンツがアプリに含まれていることを伝えることができます。また、法律上義務付けられている特定の地域やユーザーに対してコンテンツを除外またはブロックしたり、特別なデベロッパー プログラムに対するアプリの資格を判断したりする役割もあります。

コンテンツのレーティングが割り当てられる仕組み

コンテンツのレーティングを取得するには、[Play Console のレーティング質問票](#)でアプリのコンテンツの性質について回答する必要があります。この質問票の回答に基づいて、複数のレーティング機関のコンテンツのレーティングがアプリに割り当てられます。アプリのコンテンツについて偽った場合は、アプリの削除や公開停止の措置が取られることがあるため、コンテンツ レーティング質問票には正確に回答してください。

アプリが「レーティングなし」に分類されないように、Google Play で配信中の既存のすべてのアプリに加え、Play Console に新しいアプリを送信するたびにコンテンツ レーティング質問票に回答する必要があります。

レーティング質問票の回答に影響するアプリのコンテンツや機能を変更した場合は、Play Console で改めてコンテンツ レーティング質問票に回答して送信する必要があります。

各種[レーティング機関](#)やコンテンツ レーティング質問票への回答方法について詳しくは、[ヘルプセンター記事](#)をご覧ください。

レーティングへの異議申し立て

アプリに割り当てられたレーティングに同意しない場合は、証明書の通知メールに記載されたリンクを使用して IARC レーティング機関に直接申し立てることができます。

ニュース

「ニュース」カテゴリを選択したアプリに、以下の要件を満たさないコンテンツが表示される場合は、Play ストアでニュース カテゴリのアプリとは認められません。ユーザーが購読会員となる必要があるニュースアプリは、購入前にユーザーにコンテンツのプレビューを提供する必要があります。

ニュースアプリの要件:

- ・ 明確な所有権など、ニュース メディアと寄稿者に関する十分な情報を提供すること、かつ
- ・ ニュース メディアの有効な連絡先情報を提供するウェブサイトまたはアプリ内ページを設けること

ニュースアプリの禁止条項:

- ・ 誤字、脱字、文法の誤りがある
- ・ 静的コンテンツしかない
- ・ アフィリエイト マーケティングや広告収益を主な目的とする

ニュース アグリゲータ アプリの場合、アプリ内のコンテンツの提供元について透明性を確保し、提供元がそれぞれニュース ポリシー要件を満たしている必要があります。

スパムと最低限の機能

アプリは最低限、基本的な機能を備えるとともに、ユーザーに対し失礼にならないようなエクスペリエンスを提供する必要があります。頻繁にクラッシュするアプリや、使い勝手の非常に悪いアプリ、またはユーザーや Google Play に対するスパム行為をするアプリは、ストアに追加する意義のあるアプリとはいえません。

スパム

ユーザーに迷惑メールを送信するアプリや、別のアプリを複製したアプリ、低品質のアプリなど、ユーザーや Google Play に対してスパム行為を働くアプリは認められません。

メッセージ スпам

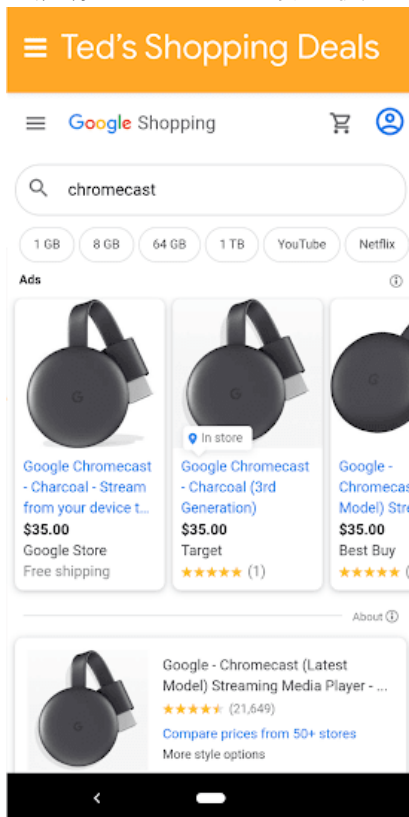
ユーザーの代わりに、SMS やメールなどのメッセージを、ユーザーがその内容や送信先を確認できない状態で送信するアプリは認められません。

ウェブ表示スパムやアフィリエイト スпам

ウェブサイトへのアフィリエイトトラフィックを誘導する、またはウェブサイトの所有者や管理者に無断でそのウェブサイトの表示を提供することを主な目的とするアプリは認められません。

一般的な違反の例:

- ウェブサイトの参照トラフィックを誘導して、そのウェブサイトでのユーザーの登録や購入に対してクレジットを受け取ることを主な目的とするアプリ。
- 無断で特定のウェブサイトの表示を提供することを主な目的とするアプリ:



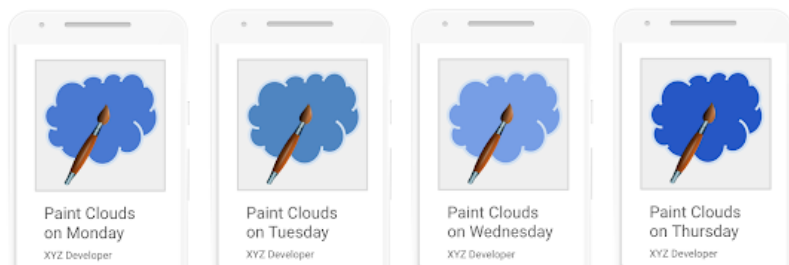
「Ted's Shopping Deals」というこのアプリには、Google ショッピングのウェブサイトを表示する機能しかありません。

コンテンツの繰り返し

Google Play 上の既存のアプリと同じユーザー エクスペリエンスを提供するだけのアプリは認められません。アプリは、独自のコンテンツやサービスを生み出すことによって、ユーザーに価値を提供する必要があります。

一般的な違反の例:

- 独自のコンテンツや価値を追加せず、他のアプリのコンテンツをコピーしている。
- コンテンツやユーザー エクスペリエンスがほとんど同じである複数のアプリを作成する。このようなアプリのコンテンツがどれも少量である場合は、1 つのアプリにすべてのコンテンツを集約することを検討してください。



広告目的

広告表示を主目的とするアプリは認められません。

一般的な違反の例:

- ユーザーがクリックやスワイプなどの操作を行うたびにインタースティシャル広告を表示するアプリ。

最低限の機能

ユーザーにとって魅力的で、動作の安定性と応答性があるアプリを提供してください。

一般的な違反の例:

- 何もしない、または何の機能も提供しないアプリ

不完全な機能

クラッシュ、強制終了、フリーズ、その他正常でない動作をするアプリは認められません。

一般的な違反の例:

- インストールできないアプリ
- インストールできるが読み込まれないアプリ
- 読み込まれるが応答しないアプリ

その他のプログラム

このポリシー センターで定められたコンテンツ ポリシーの遵守に加え、他の **Android** エクスペリエンス向けに作成され **Google Play** で配信されるアプリには、プログラム固有のポリシー要件も適用されることがあります。下記のリストで、こうしたポリシーがアプリに適用されるかどうかをご確認ください。

Android Instant Apps

Android Instant Apps の目標は、魅力的で、滑らかなユーザー エクスペリエンスを創出すると同時に、プライバシーとセキュリティの厳しい標準にも準拠することです。Google のポリシーはこの目標に沿って設計されています。

Google Play で **Android Instant Apps** を配信するデベロッパーは、以下のポリシーとその他すべての [Google Play デベロッパー プログラム ポリシー](#) を遵守する必要があります。

ID

ログイン機能がある **Instant Apps** には、[Smart Lock for Passwords](#) を統合する必要があります。

リンクのサポート

Android Instant Apps のデベロッパーは、他のアプリのリンクを適切にサポートする必要があります。デベロッパーの **Instant App** やインストール済みのアプリに、**Instant App** に解決される可能性があるリンクが含まれる場合、デベロッパーは、たとえば、[WebView](#) でリンクをキャプチャするのではなく、ユーザーをその **Instant App** に誘導する必要があります。

技術仕様

デベロッパーは、Google が定める **Android Instant Apps** の技術仕様と技術要件を遵守する必要があります。この仕様と要件は、Google の[一般公開ドキュメント](#)に記載されているものを含め、随時修正される可能性があります。

アプリのインストールの提供

Instant App はユーザーにインストール可能なアプリを提供できますが、これを **Instant App** の主な目的にしないでください。インストールを促す場合、デベロッパーは次の要件を満たす必要があります。

- インストール ボタンに、[マテリアル デザインの「アプリをダウンロード」アイコン](#)と「インストール」というラベルを使用する。
- Instant App での暗黙的なインストール メッセージは 2〜3 回に抑える。
- ユーザーにインストール メッセージを表示するためにバナーなどの広告のような手法を使用しない。

Instant App の詳細やユーザー エクスペリエンスのガイドラインについては、[Google Play Instant 版アプリの UX に関するおすすめの方法](#)をご覧ください。

デバイス状態の変更

Instant Apps は、Instant App のセッションより長く持続する変更をユーザーの端末に加えてはいけません。たとえば、Instant Apps がユーザーの壁紙を変更したり、ホーム画面のウィジェットを作成したりすることは認められません。

アプリの表示

デベロッパーは、Instant App が端末で実行されていることをユーザーが常にわかるように、Instant Apps をユーザーに表示する必要があります。

端末の ID

Instant Apps は、（1）Instant App が実行を停止した後も持続し、かつ（2）ユーザーが再設定できない端末の ID にアクセスすることはできません。次に例を示しますが、これらに限定されません。

- ビルドのシリアル
- ネットワーク チップの MAC アドレス
- IMEI、IMSI

Instant Apps は、実行時の権限を使って電話番号を取得している場合、その電話番号にアクセスできます。デベロッパーは、こうした ID やその他の手段を使ってユーザーのフィンガープリントを入手しようとしてはなりません。

ネットワーク トラフィック

Instant App 内部からのネットワーク トラフィックは、HTTPS などの TLS プロトコルを使って暗号化する必要があります。

ファミリー

Google Play では、家族みんながそれぞれの年齢に応じて楽しめる高品質のコンテンツをデベロッパーが公開できるように、高機能なプラットフォームを提供しています。ファミリー向けプログラムにアプリを送信する場合や、子供向けのアプリを Google Play ストアに送信する場合は、アプリが子供に適していて、かつ関連するすべての法律に準拠していることをデベロッパーの責任で確認します。

アプリ アカデミーで、ファミリー ポリシーの詳細とインタラクティブ チェックリストをご確認ください。

子供向けやファミリー向けにアプリを設計する

家族の生活を豊かにするためのツールとしてテクノロジーを活用する機会が増える中、保護者は、子供と安全に共有できる高品質のコンテンツを探し求めています。子供に向けたアプリや、子供の注目を集めるアプリを開発しているデベロッパーは、Google Play を利用することで、ファミリーを含むあらゆるユーザーにとって安全なアプリを提供できるようになります。

「子供」という言葉は、地域や文脈によって意味が異なる場合があります。アプリに対してどのような義務や年齢制限が適用されるのかを判断する際は、弁護士に相談することをおすすめします。アプリがどのように機能するのか最もよく知っているのは、デベロッパーの皆様ご自身です。そのため、Google Play 上で提供するアプリをファミリー向けの安全なものにするには、デベロッパーの皆様のご協力が欠かせません。

子供を主な対象とするアプリは、ファミリー向けプログラムに参加する必要があります。子供とそれ以外のユーザーの両方を対象とするアプリでも、ファミリー向けプログラムに参加できます。ファミリー向けプログラムにオプトインするアプリはすべて、[教師承認済みプログラム](#)の審査対象となります。ただし、アプリが教師承認済みプログラムに含まれると保証することはできません。ファミリー向けプログラムに参加しない場合でも、他のすべての [Google Play デベロッパー プログラム ポリシー](#)、[デベロッパー販売 / 配布契約](#)に加えて、下記の Google Play のファミリー ポリシー要件を遵守する必要があります。

Play Console 要件

[ターゲットユーザーおよびコンテンツ](#)

アプリを公開する前に、Google Play Console の [[ターゲット ユーザーおよびコンテンツ](#)] でアプリのターゲット ユーザーを指定する必要があります。表示される年齢層のリストから選択してください。Google Play Console での指定にかかわらず、子供を対象にしていると考えられる画像や言葉がアプリ内に含まれていると、指定されたターゲット ユーザーに関する Google Play による審査に影響を与える場合があります。Google Play は、デベロッパーが指定したターゲットユーザーが妥当かどうかを判断するため、デベロッパーが提供したアプリ情報を独自に審査する権限を有します。

大人だけをターゲット ユーザーとして選択したアプリが、Google によって「子供と大人の両方を対象にしており、ターゲット ユーザーの指定が不正確である」と判断された場合は、警告ラベルの表示に同意することで、アプリが子供を対象にしていないことをユーザーに明示できます。

アプリのターゲット ユーザーとして複数の年齢層を選択できるのは、選択した年齢層のユーザー向けにアプリが設計されていて、選択した年齢層のユーザーに適したアプリであることが確実である場合に限られます。たとえば、乳児、幼児、就学前の子供を対象とするアプリの場合に限り、アプリの対象年齢層として **[5 歳以下]** を選択できます。具体的な学年を対象としているアプリの場合は、その学年に最も合った年齢層を選択してください。大人と子供の両方を含む年齢層を選択できるのは、全年齢を対象としているアプリの場合に限られます。

[ターゲット ユーザーおよびコンテンツ] の更新

Google Play Console の [[ターゲット ユーザーおよびコンテンツ](#)] では、いつでもアプリの情報を更新できます。この情報を Google Play ストア上で反映させるには、[アプリのアップデート](#)が必要です。ただし、Google Play Console のこのセクションで変更した場合、アプリのアップデートを送信する前であっても、ポリシーを遵守しているかどうか審査されることがあります。

アプリの対象年齢層を変更した場合や、広告やアプリ内購入の使用を開始した場合は、アプリのストア掲載情報ページの **[新機能]** やアプリ内通知を使用して、既存のユーザーに知らせることを強くおすすめします。

Play Console 内の不実表示

[[ターゲット ユーザーおよびコンテンツ](#)] を含め、Play Console 内でアプリに関する情報に不実表示があった場合は、アプリの削除や公開停止の措置がとられることがあるため、正確な情報を提供するようにしてください。

ファミリー ポリシー要件

アプリのターゲット ユーザーに子供が含まれる場合は、以下の要件を満たす必要があります。要件を満たしていない場合、アプリの削除や公開停止の対象となることがあります。

- 1. アプリのコンテンツ:** 子供がアクセスできるアプリのコンテンツは、子供に適したものにする必要があります。
- 2. Google Play Console 内の回答:** Google Play Console 内では、アプリに関する質問に対して正確に回答する必要があります。また、アプリを変更した場合は回答を更新して変更内容を正確に反映させる必要があります。
- 3. 広告:** 子供や年齢不明のユーザーに対してアプリ内で広告を表示する場合は、以下の要件を満たす必要があります。
 - このようなユーザーに広告を表示するには、必ず [Google Play 認定広告 SDK](#) を使用すること。
 - このようなユーザーに対して、インタレスト ベース広告（オンライン ブラウジング行動に基づき特定の特徴のある個々のユーザーをターゲットとする広告）や、リマーケティング（アプリやウェブサイトでの以前の操作に基づき個々のユーザーをターゲットとする広告）が表示されないこと。
 - このようなユーザーに対して表示される広告が、子供に適したコンテンツを表示すること。
 - このようなユーザーに対して表示される広告が、ファミリー向け広告フォーマットの要件を満たしていること。
 - 子供への広告掲載に関して適用されるすべての法規制および業界基準を遵守していること。
- 4. データ収集:** アプリ内で、API や SDK を呼び出すまたは使用する場合なども含めて、子供の **個人情報や機密情報** を収集する場合は、データを収集することに関して情報を開示する必要があります。子供の機密情報には、認証情報、マイクやカメラのセンサーデータ、デバイスのデータ、**Android ID**、使用状況データ、広告 ID などが含まれますが、これらに限定されません。
- 5. API と SDK:** アプリで API や SDK を利用する場合、すべて正しく実装している必要があります。
 - 子供だけを対象としているアプリの場合、子供向けサービスでの使用が承認されていない API や SDK を利用することはできません。これには、Google ログイン（および、Google アカウントに関連付けられたデータにアクセスする各種 Google API サービス）や、Google Play ゲームサービス、OAuth テクノロジーを使用して認証や承認を行う各種 API サービスなどが含まれます。
 - 子供と大人の両方を対象としているアプリの場合、子供向けサービスでの使用が承認されていない API や SDK は、**年齢詐称を予防する年齢確認**後に使用するか、子供からのデータ収集につながらない方法で実装している場合（例: Google ログインがオプション機能として提供されている場合）を除き、実装することはできません。子供と大人の両方を対象とするアプリでは、子供向けサービスでの使用が承認されていない API または SDK を介したログインや、アプリ コンテンツへのアクセスを必須とはなりません。

6. **プライバシー ポリシー:** アプリのストアの掲載情報ページには、アプリのプライバシー ポリシーへのリンクを記載する必要があります。このリンクは、アプリがストア上で利用可能である間は常に維持されていなければならない、特に、アプリによるデータ収集とデータ使用について正確に説明するプライバシー ポリシーにリンクしている必要があります。
7. **特別な制限:**
- ・ 拡張現実 (AR) を使用するアプリの場合、AR 機能を起動する際に、安全に関する警告を表示する必要があります。この警告には、以下の内容を含める必要があります。
 - ・ 保護者による管理の重要性に関する適切なメッセージ。
 - ・ 現実の世界における物理的な危険性 (例: 周囲の状況) に関する注意喚起。
 - ・ 子供による使用が推奨されていないデバイス (例: Daydream、Oculus) の使用をアプリの要件とすることはできません。
8. **法規制の遵守:** アプリは、そのアプリで呼び出す、または使用するすべての API および SDK を含め、[米国の児童オンライン プライバシー保護法 \(COPPA\)](#)、[EU の一般データ保護規則 \(GDPR\)](#)、その他適用されるすべての法規制を遵守する必要があります。

一般的な違反の例:

- ・ ストアの掲載情報では子供向けと説明しているが、実際のコンテンツは大人向けになっているアプリ。
- ・ 子供向けアプリでの使用が利用規約によって禁止されている API を実装しているアプリ。
- ・ アルコールや、タバコ、規制薬物の使用を美化するアプリ。
- ・ ギャンブルそのものやギャンブルのシミュレーションを含むアプリ。
- ・ 暴力や殺人など、子供に適さない衝撃的なコンテンツを含むアプリ。
- ・ 出会い系サービスを提供するアプリ、または性的なアドバイスや夫婦生活のアドバイスを提供するアプリ。
- ・ Google Play の[デベロッパー プログラム ポリシー](#)に違反するコンテンツを表示するウェブサイトへのリンクを含むアプリ。
- ・ 成人向けの広告 (暴力的なコンテンツ、性的なコンテンツ、ギャンブルに関するコンテンツなど) を子供に表示するアプリ。子供向けの広告、アプリ内購入、商用コンテンツに関する Google Play のポリシーについて詳しくは、[ファミリー向けの広告と収益化に関するポリシー](#)をご覧ください。

ファミリー向けプログラム

子供を主な対象とするアプリは、ファミリー向けプログラムに参加する必要があります。また、子供やファミリーを含め、すべてのユーザー向けに設計されているアプリの場合も、プログラムへの参加を申し込むことができます。

アプリがこのプログラムの認定を受けるには、[Google Play デベロッパー プログラム ポリシー](#)と[デベロッパー販売 / 配布契約](#)に記載されている要件に加えて、ファミリー ポリシー要件とファミリー向けプログラム参加要件をすべて満たす必要があります。

プログラムに参加するためのアプリの提出プロセスについて詳しくは、[こちら](#)をクリックしてください。

プログラム参加要件

ファミリー向けプログラムに参加するアプリは、アプリと広告の両方のコンテンツが子供に適していて、かつ以下の要件をすべて満たしている必要があります。ファミリー向けプログラムに承認されたアプリは、すべてのプログラム要件を遵守し続ける必要があります。Google Play は、ファミリー向けプログラムに適していないと判断されるアプリを拒否、削除、または停止することがあります。

ファミリー向けの要件

1. アプリの ESRB レーティングが「Everyone」、「Everyone 10+」、または同等のレーティングである必要があります。
2. Google Play Console のコンテンツ レーティング質問票で、アプリのインタラクティブ要素に関して正確な情報を開示する必要があります。たとえば、以下の点について正確に記載してください。
 - ・ ユーザー間で交流や情報の交換ができるかどうか。
 - ・ ユーザーから提供された個人情報を第三者と共有するかどうか。
 - ・ ユーザーの物理的位置情報を他のユーザーと共有するかどうか。
3. [Android Speech API](#) を使用するアプリの場合は、アプリの RecognizerIntent.EXTRA_CALLING_PACKAGE を PackageName に設定する必要があります。
4. 広告の表示には、必ず [Google Play 認定広告 SDK](#) を使用する必要があります。
5. 子供専用のアプリの場合、位置情報のアクセス権限をリクエストすることできません。
6. アプリで Bluetooth をリクエストする際は、[コンパニオン デバイス マネージャー \(CDM\)](#) を使用する必要があります。ただし、CDM に対応していないオペレーティングシステム (OS) バージョンのみを対象としている場合を除きます。

プログラムの参加要件を満たしていないアプリの例:

- ・ ESRB レーティングが「Everyone」であるが、ギャンブル コンテンツの広告を含むアプリ
- ・ 保護者向けのアプリ（例: 授乳記録アプリ、育児ガイド）
- ・ 保護者のみが使用することを目的としたガイドやデバイス管理アプリ
- ・ 子供に不適切なアプリアイコンやランチャー アイコンを使用しているアプリ

カテゴリ

ファミリー向けプログラムへの参加が認められた場合、アプリを説明する 2 つ目のカテゴリとして、ファミリー向け専用カテゴリを選択することができます。ファミリー向けプログラムに参加しているアプリが利用できるカテゴリは次のとおりです。

アクション&アドベンチャー: アクション中心のアプリやゲーム（シンプルなレースゲームやファンタジー アドベンチャーなど、ユーザーをワクワクさせるように設計されたアプリやゲーム）。

脳トレ系: ユーザーに考えさせるゲーム（パズルや、絵合わせゲーム、クイズなど、記憶力や知能、論理的思考力を試すゲーム）。

クリエイティブ系: 創造性を刺激するアプリやゲーム（図形描画アプリや、ペイントアプリ、コーディング アプリなど、さまざまなコンテンツを作成できるアプリやゲーム）。

教育: 学習促進を目的として、教育専門家（教師、教育評論家、研究者など）の意見に基づいて設計されたアプリやゲーム（学業、社会感情、運動、創造的学習、基本的ライフスキル、批判的思考、問題解決に関する学習など）。

音楽と動画: 音楽コンポーネントや動画コンポーネントを含むアプリやゲーム（楽器シミュレーション アプリ、動画やオーディオ コンテンツを提供するアプリなど）。

ごっこ遊び: ユーザーが役を演じて遊べるアプリやゲーム（コック、医者、王子さま / お姫さま、消防士、警官、架空の人物など）。

広告と収益化

ファミリー ポリシー要件やファミリー向け要件の対象となるアプリのユーザーに配信される広告（個々のアプリ向け、サードパーティ製アプリ向け）、アプリ内購入用クーポン、その他営利目的のコンテンツ（有料プロダクト プレースメントなど）のすべてに、下記のポリシーが適用されます。アプリ内のすべての広告、アプリ内購入用クーポン、営利目的のコンテンツは、適用されるすべての法規制（関連する自主規制や業界ガイドラインを含む）を遵守している必要があります。

Google Play は、過度に攻撃的な営業手法を採るアプリに対して、必要な措置を講じる権限を有します。

広告フォーマットの要件

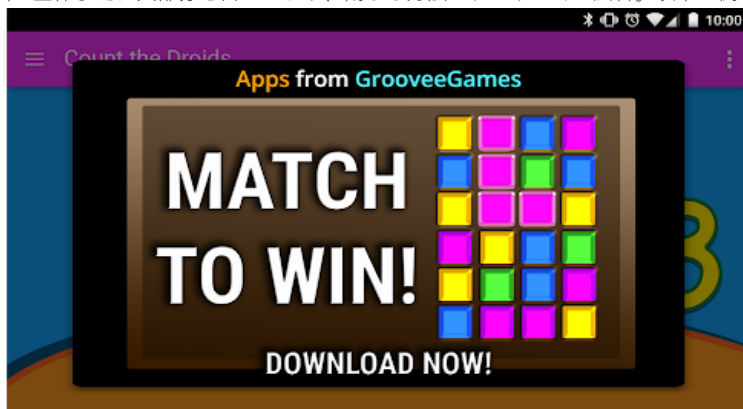
広告やアプリ内購入用クーポンは、虚偽的なコンテンツを含まず、子供のユーザーが誤ってクリックすることのないように設計されている必要があります。以下は禁止されています。

- ・ 画面全体を占拠したり通常の使用を妨げたりして、閉じる手段をわかりやすく提示しない広告など、混乱させる広告（例: [非表示にできない広告](#)）
- ・ 5 秒経過しても閉じることができない広告を、アプリの通常の使用を妨げる形で配置すること。通常のアプリの使用やゲームのプレイを妨げない広告（動画コンテンツに組み込まれた広告など）は 5 秒以上表示できます。
- ・ アプリの起動の直後にインタースティシャル広告やアプリ内購入用クーポンを表示すること
- ・ 1 ページに複数の広告を配置すること（1 つのプレースメントに複数のクーポンを表示するバナー広告、複数のバナー広告や動画広告の表示は許可されません）。
- ・ アプリのコンテンツと明確に区別できないような形で広告やアプリ内購入用クーポンを配置すること
- ・ 広告の表示やアプリ内購入を促す目的で、衝撃的な手法や巧妙に感情を操る策略を使うこと
- ・ アプリ内購入に関して、仮想のゲームコインの使用と実際のお金の使用を明確に区別しないこと

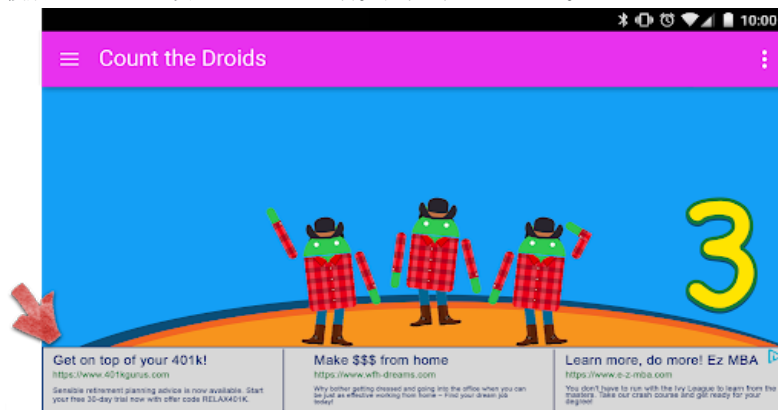
広告フォーマットの違反の例:

- ・ ユーザーが閉じようすると動いて逃れる広告。

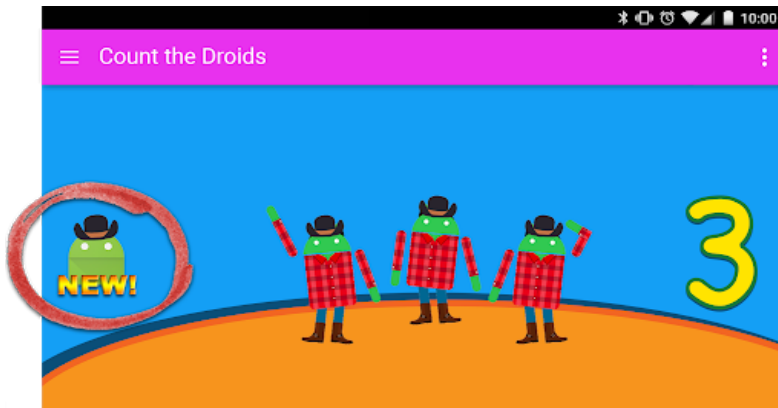
- 画面の全体または大部分を占めており、閉じる方法がわかりにくい広告。以下に例を示します。



- 複数のクーポンを表示するパナー広告。以下に例を示します。

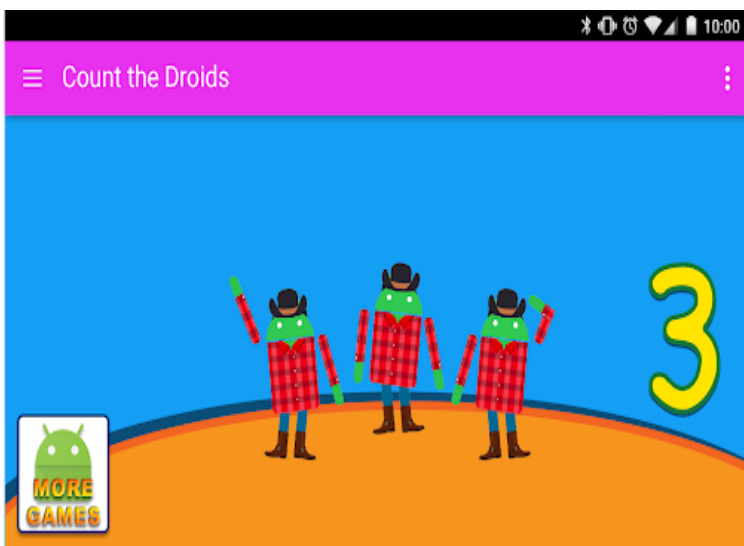


- アプリのコンテンツとして誤認される恐れのある広告。以下に例を示します。



- デベロッパーは、ボタンや広告を使用して、自分が開発した他の Google Play ストア掲載情報について宣伝することができますが、そのボタンや広告は、アプリのコンテンツと明確に区別できる必要があります。以下に例を示しま

す。



子供に対して表示すべきではない不適切な広告コンテンツの例:

- **不適切なメディア コンテンツ:** 子供には適していないテレビ番組、映画、音楽アルバム、その他各種メディアに関する広告。
- **不適切なビデオゲームやダウンロード可能なソフトウェア:** 子供に適さないダウンロード可能なソフトウェアや電子ビデオゲームに関する広告。
- **規制薬物や有害物質:** アルコール、タバコ、規制薬物、その他の各種有害物質に関する広告。
- **ギャンブル:** 擬似ギャンブル、コンテスト、懸賞の宣伝に関する広告（参加無料のものも含む）。
- **成人向けコンテンツおよび性的なものを暗示するコンテンツ:** 性的コンテンツや、性的なものを暗示するコンテンツ、成人向けコンテンツを含む広告。
- **出会い系や交流サイト:** 出会い系サイトや成人向け交流サイトに関する広告。
- **暴力的なコンテンツ:** 子供には適していない、暴力的で刺激の強いコンテンツを含む広告。

広告 SDK

子供だけをターゲット ユーザーとするアプリで広告を配信する場合、[Google Play 認定広告 SDK](#) を使用しなければなりません。アプリのターゲット ユーザーに子供と大人の両方が含まれる場合は、ユーザーを年齢層別に分ける手段（[年齢詐称を予防する年齢確認](#)など）を実装し、子供には [Google Play 認定広告 SDK](#) からのみ広告が配信されるようにする必要があります。ファミリー向けプログラムのアプリでの広告配信には、必ず自己認定広告 SDK を使用する必要があります。

各要件の詳細と現時点で承認されている広告 SDK のリストについては、[ファミリー向け広告プログラムのポリシー](#)をご覧ください。

AdMob を使用している場合は、そのサービスの詳細を [AdMob のヘルプセンター](#)でご確認ください。

デベロッパーは、自分のアプリが広告、アプリ内購入、営利目的コンテンツに関する要件をすべて満たすようにする責任を負います。広告 SDK のコンテンツ ポリシーと広告手法の詳細については、各 SDK の提供元にお問い合わせください。

アプリ内購入

ファミリー向けプログラムに参加しているアプリでアプリ内購入が発生する場合、[Google Play](#) はその前に必ずユーザーの再認証を行います。この方法により、子供ではなく、支払い責任を負う当事者が購入を承認しているかどうかを確認できます。

施行

ポリシー違反に後から対処することもできますが、まずは違反しないようにすることが重要です。それでも違反が発生した場合、[Google](#) はアプリにポリシーを遵守させる方法をデベロッパーに十分に理解していただけるよう努めます。[違反を見つけた場合](#)、または[違反の管理](#)に関してご不明な点がある場合は、[Google](#) にお知らせください。

ポリシーの範囲

Google のポリシーはアプリで表示されるコンテンツのほか、アプリからリンクされるコンテンツにも適用されます。これには、ユーザーに表示される広告やアプリがホストするユーザー作成コンテンツ、アプリからリンクするユーザー作成コンテンツも含まれます。さらにこのポリシーは、デベロッパー名や記載されているデベロッパーのウェブサイトのランディング ページなど、Google Play で一般公開されるデベロッパー アカウントのすべてのコンテンツに適用されます。

他のアプリをユーザーのデバイスにインストールできるようにするアプリは認められません。他のアプリ、ゲーム、またはソフトウェア（サードパーティが提供する機能やコンテンツを含む）をインストールすることなく利用できるようにするアプリは、その場合に利用可能になるあらゆるコンテンツについて、Google Play ポリシーの遵守を徹底する必要があります。またこうしたアプリは、追加のポリシー審査の対象となることがあります。

このポリシーで規定される用語は、[デベロッパー販売 / 配布契約（DDA）](#)と同じ意味で使用されています。アプリのコンテンツは、これらのポリシーと DDA を遵守するだけでなく、Google の[コンテンツのレーティングに関するガイドライン](#)に沿ってレーティングを受ける必要があります。

Google Play でアプリの承認または削除の審査をする際、有害な動作パターンや不正行為の危険性の高さなど、これに限らず、さまざまな要因を検討します。不正行為については、違反履歴、ユーザーからのフィードバック、人気のあるブランドやキャラクターなどのアセットの使用状況など、幅広い項目を判断材料として危険性を見極めます。

Google Play プロテクトの仕組み

Google Play プロテクトは、ユーザーがアプリをインストールする際に、そのアプリをチェックします。また、デバイスを定期的にスキャンします。有害な可能性のあるアプリが検出された場合は、次のような処理を行うことがあります。

- ユーザーに通知を送信する。ユーザーは通知をタップして【アンインストール】をタップするとアプリを削除できます。
- アプリがアンインストールされるまで無効にする。
- アプリを自動的に削除する。有害なアプリが検出されると、ほとんどの場合、アプリが削除されたという通知がユーザーに届きます。

マルウェアから保護する仕組み

悪意のあるサードパーティ ソフトウェア、URL、その他のセキュリティ上の問題からユーザーを保護するため、Google は次のような情報を受け取ることがあります。

- デバイスのネットワーク接続
- 有害な可能性のある URL
- オペレーティング システム、および Google Play またはその他の提供元からデバイスにインストールされたアプリ

アプリまたは URL が安全ではない可能性がある場合、Google から警告が表示されることがあります。デバイス、データ、またはユーザーにとって有害であることがわかっているアプリや URL は、削除されるかインストールできないようブロックされることがあります。

この保護機能の一部を、デバイスの設定で無効にできます。ただし、Google Play からインストールされたアプリについては、Google が引き続き情報を受け取る可能性があります。他の提供元からデバイスにインストールされたアプリについては、セキュリティの問題に関して引き続きチェックが行われることがありますが、Google に情報は送信されません。

プライバシー通知の仕組み

ユーザーの個人情報にアクセスする可能性があるアプリが Google Play ストアから削除された場合、Google Play プロテクトから通知が届き、ユーザーは必要に応じてすぐにアプリをアンインストールできます。

施行プロセス

Google のポリシーに違反するアプリには、下記に概説するような適切な措置が取られます。さらに、Google が行った措置に関連する情報と、Google が誤って対処したと思われる場合の再審査請求の手順をメールでお知らせします。

Google からの削除や管理上の通知で、各アプリや広範囲にわたるアプリカタログの個々のポリシー違反をすべて指摘しているとは限らないのでご注意ください。ポリシーに関する問題のすべてに対処し、さらにアプリのその他の部分もポリシーを完全に遵守するよう十分に努めることは、デベロッパーの責任です。すべてのアプリでポリシー違反に対処しないと、追加の措置が取られる可能性があります。

こうしたポリシーまたは[デベロッパー販売 / 配布契約（DDA）](#)への違反の繰り返しや重大な違反のあるアプリ（マルウェア、不正を行うアプリ、ユーザーやデバイスに危害を及ぼす恐れのあるアプリ）は、デベロッパー個人のまたは関連のある Google Play デベロッパー アカウントの停止につながります。

違反措置

さまざまな違反措置がアプリにさまざまな影響を与えることがあります。以下、**Google Play** が行う可能性のあるさまざまな措置と、アプリまたは **Google Play** デベロッパー アカウントに与える影響について説明します。この情報については、[こちらの動画](#)でも説明しています。

否認

- 審査のために送信された新しいアプリまたはアプリのアップデートは、**Google Play** で利用可能になりません。
- 既存のアプリのアップデートが否認となった場合、そのアップデートの前に公開されているバージョンは引き続き **Google Play** で公開されます。
- その場合、否認となったアプリの既存のユーザー インストール、統計情報、評価には影響はありません。
- 否認が **Google Play** デベロッパー アカウントの状態に影響することはありません。

注: 否認となったアプリは、ポリシー違反をすべて修正するまで再送信しないでください。

削除

- アプリは、そのアプリの以前のバージョンとともに **Google Play** から削除され、ユーザーはダウンロードできなくなります。
- アプリが削除されるので、ユーザーはアプリのストアの掲載情報、ユーザー インストール、統計情報、評価を確認できなくなります。これらの情報は、削除されたアプリに対して、ポリシーを遵守したアップデートを送信すると復元されます。
- ポリシーを遵守したバージョンが **Google Play** で承認されるまで、ユーザーはアプリ内購入やアプリ内課金機能を利用できません。
- 削除されても **Google Play** デベロッパー アカウントの状態にすぐには影響はありませんが、複数回削除されるとアカウントが停止される場合があります。

注: ポリシー違反をすべて修正するまで、削除されたアプリを再公開しようとししないでください。

停止

- アプリは、そのアプリのそれまでのバージョンとともに **Google Play** から削除され、ユーザーはダウンロードできなくなります。
- アプリの否認または削除が繰り返された場合だけでなく、重大なポリシー違反や、複数のポリシー違反により停止となることがあります。
- アプリが停止されるので、ユーザーはアプリのストアの掲載情報、既存のユーザー インストール、統計情報、評価を確認できなくなります。これらの情報は、削除されたアプリに対して、ポリシーを遵守したアップデートを送信すると復元されます。
- 停止されたアプリの **APK** や **App Bundle** は使用できなくなります。
- ポリシーを遵守したバージョンが **Google Play** で承認されるまで、ユーザーはアプリ内購入やアプリ内課金機能を利用できません。
- 停止の対象になると、**Google Play** デベロッパー アカウントの状態が良好ではなくなります。違反警告を複数回受けると、個人アカウントや関連する **Google Play** デベロッパー アカウントが停止されることがあります。

注: 停止されたアプリは、**Google Play** からの許可がない限り再公開しようとししないでください。

制限付き公開

- Google Play** でのアプリの表示は制限されています。アプリは引き続き **Google Play** で利用でき、ユーザーはアプリの **Play** ストアの掲載情報を指すリンクから直接アプリを使用できます。
- アプリが制限付き公開の状態になっても、**Google Play** デベロッパー アカウントの状態には影響しません。
- 制限付き公開状態のアプリについて、ユーザーに表示される既存のストアの掲載情報、ユーザー インストール、統計情報、評価には影響はありません。

アカウントの停止

- デベロッパー アカウントが停止されると、そのカタログ内のすべてのアプリが **Google Play** から削除され、新しいアプリを公開できなくなります。また、関連する **Google Play** デベロッパー アカウントも完全に停止されます。
- 複数回の停止措置や重大なポリシー違反による停止措置により、**Play Console** アカウントが停止されることもあります。
- 停止されたアカウント内のアプリは削除されるため、ユーザーはアプリのストアの掲載情報、既存のユーザー インストール、統計情報、評価を確認できなくなります。

注: 新しいアカウントを開設しようとしても同様に停止されます（デベロッパー登録料金の払い戻しはありません）。そのため、アカウントのいずれかが停止されている間、新しい **Play Console** アカウントを登録しようとししないでください。

ポリシー違反の管理と報告

How to handle a policy violation on Go...



違反措置に対する異議申し立て

Google が誤って措置を行い、アプリが **Google Play** プログラム ポリシーとデベロッパー販売 / 配布契約に違反していないと判明した場合は、アプリを元に戻します。ポリシーをよくご確認のうえ、**Google** の判断が誤りだと思われる場合は、違反措置の通知メールに記載の手順に沿ってその判断に対する異議申し立てを行ってください。

参考情報

違反措置やユーザーからの評価、コメントについて詳しくは、下記のリソースをご覧になるか、[Google Play ヘルプセンター](#)からお問い合わせください。ただし、**Google** が法律上の助言をすることはできません。法律上の助言が必要な場合は、弁護士にご相談ください。

- [アプリの確認と異議申し立て](#)
- [ポリシー違反を報告する](#)
- [アカウントの停止またはアプリの削除に関する Google Play への問い合わせ](#)
- [適切な警告](#)
- [不適切なアプリやコメントを報告する](#)
- [アプリが Google Play から削除された](#)
- [Google Play デベロッパー アカウントの停止について](#)



この記事に関するフィードバックをお寄せください

この情報は役に立ちましたか？

はい

いいえ

さらにサポートが必要な場合

次の手順をお試しください。

お問い合わせ

詳しい情報をお知らせください。解決に向けてサポートいたします