デベロッパー プログラム ポリシー

（別段の記載がない限り、2023 年 4 月 26 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。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 プログラム ポリシーとデベロッパー販売 / 配布契約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 にふさわしいものであるか、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

児童の搾取または虐待を助長するコンテンツの作成、アップロード、配布を禁止していないアプリは、Google Play から即時に削除されることがあります。これには、すべての児童性的虐待のコンテンツが含まれます。Google サービス上で児童搾取の疑いがあるコンテンツを報告するには、[**不正行為を報告**] をクリックしてください。インターネット上の Google サービス以外の場所で見つけたコンテンツについては、お住まいの国の適切な管轄当局 に直接通報してください。

Google は、児童を危険にさらすアプリの使用を禁止しています。これには、児童に対する以下のような搾取行為を助長するアプリの使用が含まれますが、これらに限定されません。

- 児童を対象とした不適切な行為（触る、愛撫するなど）。
- チャイルド グルーミング（例: オンラインで児童に取り入って、オンラインまたはオフラインでの性的接触や性的な画像の交換などに誘い込むこと）。
- 未成年の性的対象化（例: 児童の性的虐待を描写、奨励、または助長する画像、あるいは、児童の性的搾取につながる可能性のある方法で児童を描写すること）。
- セクストーション（例: 児童の公開されたくない画像を入手したと主張して児童を脅迫すること）。
- 児童の人身売買（例: 商業的な性的搾取を目的として児童の広告や勧誘を行うこと）。

児童性的虐待のコンテンツの使用が判明した場合、Google は全米行方不明・被搾取児童センターへの報告などの適切な措置を講じます。児童が虐待、搾取、人身売買の危険にさらされている、または実際にその被害に遭っていると思われる場合は、地域の警察や、こちら に掲載されている児童の安全を守る組織に通報してください。

また、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は認められません。次に例を示しますが、これらに限定されません。

- 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な行為を描写または助長するアプリ。

また、身体や自己に否定的なイメージを持たせることで、美容整形、減量など、身体の外観を整える美容上の矯正を推奨するアプリは許可されません。

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。報酬を目的とした性行為を助長または勧誘していると解釈されるおそれのあるアプリやアプリ コンテンツは認められません。性的搾取行為に関連するコンテンツを含む、または行うアプリ、または同意のない性的なコンテンツを配信するアプリは認められません。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。

また、このポリシーに違反するコンテンツがアプリに含まれていても、そのコンテツが適切とされる地域のユーザーは、アプリを利用できる場合があります。その他の地域のユーザーはアプリを利用できません。

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。

- 性的なヌードの描写のほか、裸の人物（全身や局部をぼかした場合も含む）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。
- 獣姦を描写、表現、奨励するコンテンツ。
- 報酬を目的とした性行為を助長または勧誘していると解釈されるおそれのある性関連のエンターテイメント、エスコート サービス、またはその他のサービスを宣伝するアプリ。こうしたサービスには、一方の参加者が他方の参加者に金銭、贈り物、または経済的支援を提供することが想定または暗示される援助交際もしくは性的な取り決め（いわゆる「シュガーデート」）が含まれますが、これらに限定されません。
- 人を辱める、または物と見なすアプリ（人の衣服を脱がせる、または衣服が透けて見えると謳うアプリなど）。いたずらアプリやエンタメアプリと明記されていても同様。
- 盗撮、隠しカメラ、相手の同意を得ていない性的コンテンツ（ディープフェイクまたは類似の技術を利用して作成されたもの）、暴行コンテンツなど、性的な内容でユーザーを脅迫または搾取しようとするコンテンツまたは行動。

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、社会的階層、在留資格など、組織的な人種差別や疎外に結び付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。

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。

- 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、堕落している、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

暴力や他者を危険にさらす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。

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。

- 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、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。

テロに関するコンテンツ

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、芸術（EDSA）を目的としてテロ関連のコンテンツを投稿する場合は、EDSA 分野の関連情報を提供するよう心掛けてください。

危険な団体および運動

民間人に対する暴力行為について関与、準備、または犯行声明を出した運動や団体は、人員募集を含むいかなる目的においても Google Play にアプリを公開することは認められません。

民間人に対する暴力行為の計画、準備、または賛美に関連するコンテンツを含むアプリは認められません。こうしたコンテンツを EDSA を目的としてアプリに含める場合は、関連する EDSA コンテンツの近くに配置する必要があります。

配慮が求められる事象

社会的、文化的、政治的な影響が大きく配慮が求められる事象（国家の非常事態、自然災害、公衆衛生上の緊急事態、紛争、死、その他の悲劇的な事象など）を利用する、またはそのような事象に対する配慮を欠く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。

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。

- 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。
- 文書で十分に裏付けられた大規模な悲劇的事象の発生を否定する。
- 配慮が求められる事象に便乗して利益を得ているように見える（被害者への恩恵が確認できない）。
- 新型コロナウイルス感染症 2019（COVID-19）アプリの要件　に違反しているアプリ。

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。

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。

- 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。

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。

- 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。

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。

- 未成年によるアルコールやタバコの使用や売買の描写または奨励。
- 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、金銭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（ユーザーの状況に合わせたアドバイスを含む）をいいます。

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

バイナリー 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

デバイス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使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。

- 個人ローンに含まれる例: 個人ローン、ペイデイローン、P2P ローン、タイトルローン
- 個人ローンに含まれない例: 住宅ローン、自動車ローン、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、見込み顧客獲得のためのアプリ、消費者と第三者の融資元を仲介するアプリが含まれますが、これらに限定されません。こうしたアプリについては、Google Play Console でアプリのカテゴリを「ファイナンス」に設定し、アプリの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
- 最大年利（実質年率）。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。
- 元金と適用されるすべての手数料を含む、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）。

年利の高い個人ローン

Google Play において、米国では年利が 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年利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。

インド、インドネシア、フィリピン、ナイジェリア、ケニアの個人ローンアプリに関する追加要件

個人ローンアプリをインド、インドネシア、フィリピン、ナイジェリア、ケニアで公開する場合は、さらに下記の資格要件を満たしていることを証明する必要があります。

1. **インド**
   - インド向けの個人ローンアプリ申告　を作成し、申告内容の裏付けに必要な書類を提出します。次に例を示します。
     - インド準備銀行（RBI）から個人ローンを提供するライセンスを供与されている場合は、Google の審査を受けるためにライセンスのコピーを提出する必要があります。
     - 融資活動に直接関与しておらず、登録済みのノンバンク金融会社（NBFC）または銀行によるユーザーへの融資を簡易化するプラットフォームを提供しているだけの場合は、そのことを正確に申告に反映する必要があります。
       - また、登録済みのすべての NBFC と銀行の名称を、アプリの説明文において認識しやすい形で開示する必要があります。
   - デベロッパー アカウント名が、当該の申告で対象としている登録済みの企業名に一致していることを確認します。
2. **インドネシア**
   - インドネシア向けの個人ローンアプリ申告　を作成し、申告内容の裏付けに必要な書類を提出します。次に例を示します。
     - 提供するアプリが、OJK 規制番号 77/POJK.01/2016（随時修正の可能性あり）に規定された「Information Technology-Based Money Lending Services（情報技術に基づく融資サービス）」の活動に関与している場合は、Google の審査を受けるためにライセンスのコピーを提出する必要があります。

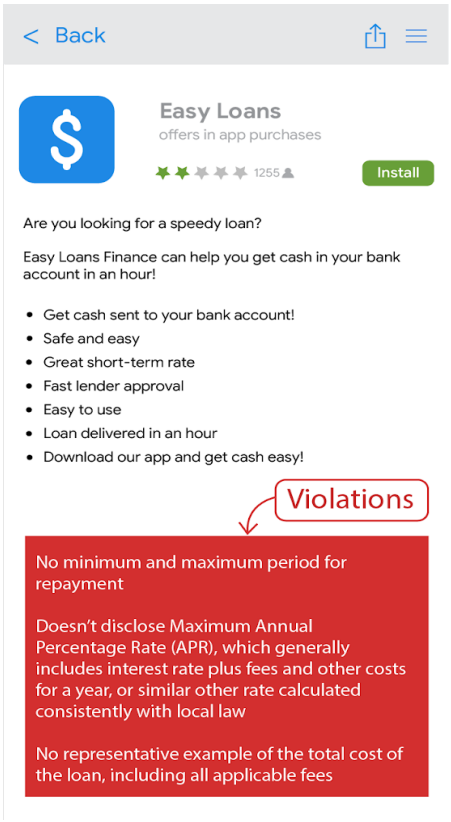
- デベロッパー アカウント名が、当該の申告で対象としている登録済みの企業名に一致していることを確認します。

3. **フィリピン**
   - フィリピン向けの個人ローンアプリ申告　を作成し、申告内容の裏付けに必要な書類を提出します。
     - オンライン融資プラットフォーム（OLP）を通じて融資を提供するすべての金融会社および融資会社は、フィリピン証券取引委員会（PSEC）から SEC 登録番号と認証局（CA）番号を取得する必要があります。
       - さらに、アプリの説明文において、法人名、商号、PSEC 登録番号、金融 / 融資会社を営むための認証局（CA）番号を開示する必要があります。
     - アプリが、融資に基づくクラウドファンディング活動（たとえば P2P レンディング）や、「クラウドファンディングに適用されるルールと規制（CF ルール）」に規定されている活動に関与している場合は、PSEC に登録している CF 仲介者を通じて取引を処理する必要があります。

4. **ナイジェリア**
   - ナイジェリア向けの個人ローンアプリ申告　を作成し、申告内容の裏付けに必要な書類を提出します。
     - デジタルマネーの融資元（DML）は、ナイジェリアの連邦競争消費者保護委員会（FCCPC）が策定した LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING, 2022（随時修正の可能性あり）を遵守して条件を満たし、FCCPC から検証可能な承認状を取得する必要があります。
     - ローン アグリゲーターは、デジタル融資サービスに関する書類および / または証明書と、提携しているすべての DML の連絡先情報を提供する必要があります。
     - Google Play から要請があった場合には、適用される規制やライセンス要件に関する追加の情報または書類を提供する必要があります。

5. **ケニア**
   - ケニア向けの個人ローンアプリ申告　に記入し、申告内容の裏付けに必要な書類を提出します。
     - デジタル クレジット プロバイダ（DCP）は DCP 登録プロセスを完了して、ケニア中央銀行（CBK）からライセンスを取得する必要があります。申告の際には、CBK から取得したライセンスのコピーを提出しなければなりません。
     - 融資活動に直接関与しておらず、登録済みの DCP によるユーザーへの融資を簡易化するプラットフォームを提供しているだけの場合は、そのことを正確に申告に反映させ、各パートナーの DCP ライセンスのコピーを提出する必要があります。
     - 現在 Google Play は、CBK の公式ウェブサイトにあるデジタル クレジット プロバイダのディレクトリに記載されている法人からのみ、申告およびライセンス提出を受け付けています。

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。



現金を伴うギャンブル、ゲーム、コンテスト

現金賭博アプリ、現金賭博に関する広告、ゲーム性のあるポイント プログラム、デイリー ファンタジー スポーツ アプリは、特定の要件を遵守する場合に限り、許可されます。

ギャンブル アプリ

Google は、デベロッパーが、Google Play で配信するギャンブル アプリの申し込み手続きを完了　し、認可を受けた公営の運営者であるか、指定国のギャンブルに関わる適切な行政機関にライセンスを持つ運営者として登録され、提供しようとしている種類のオンライン ギャンブル サービスについて指定国で有効な運営ライセンスを提示している場合に限り、制限および Google Play のすべてのポリシーを遵守することを条件として、特定の国でオンライン ギャンブルを行えるまたは促進するアプリを許可します。

許可されるのは、以下の種類のオンライン ギャンブル サービスを提供する、有効なライセンスが付与されているか承認を受けているギャンブル アプリのみです。

- オンライン カジノゲーム
- スポーツ ギャンブル
- 競馬（スポーツ ギャンブルとは別に規制され、許可が下りているもの）
- 宝くじ
- デイリー ファンタジー スポーツ

対象となるアプリは、以下の要件を遵守する必要があります。

- デベロッパーは、Google Play でアプリを配信するために、申し込み手続きを完了する必要があります。
- アプリは、配信対象国で適用される法律および業界基準をすべて遵守する必要があります。
- デベロッパーは、アプリの配信対象国や州 / 地域ごとに有効なギャンブル ライセンスを取得する必要があります。

- デベロッパーは、ギャンブル ライセンスの範囲を超える種類のギャンブル サービスを提供してはなりません。
- 未成年のユーザーに対しては、アプリを使用できないようにする必要があります。
- デベロッパーがギャンブル ライセンスを取得した国、州、地域以外では、アプリにアクセスして使用することが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、Google Play ストアからのダウンロードとインストールを無料にする必要があります。
- 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必要があります。
- 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。

他のリアルマネー ベースのゲーム、コンテスト、トーナメント用のアプリ

上記のギャンブル アプリに関する資格要件を満たさず、下記の「その他の現金を伴うゲームのパイロット プログラム」に含まれていないその他のすべてのアプリについては、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、参加費を払ったりすることによって、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、オンライン カジノ、スポーツ ギャンブル、宝くじのほか、ユーザーが金銭を支払って現金やその他の実世界で価値のある賞品を獲得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（後述のゲーム性のあるポイント プログラムの要件で認められているプログラムは除きます）。

違反の例

- ユーザーが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。
- 現金を伴うゲーム、コンテスト、トーナメントに賭けたり、参加したりするなどの「行動を促すフレーズ」を提示するナビゲーション要素や機能（メニュー項目、タブ、ボタン、WebView など）があるアプリ（たとえば、賞金獲得のチャンスがあるトーナメントで「賭けよう」、「登録しよう」、「挑戦しよう」とユーザーを誘うアプリ）。
- 賭け金、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に賭けるまたはそれを獲得す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。

その他の現金を伴うゲームのパイロット プログラム

一部の地域では、現金を伴う特定のゲームに関するパイロット プログラムを期間限定で実施することがあります。詳しくは、こちらのヘルプセンターのページ をご覧ください。

ゲーム性のあるポイント プログラム

法律で許可されており、ギャンブルやゲームに関する追加のライセンス要件が適用されない場合は、以下の Play ストア資格要件を条件として、実世界の賞品または金銭的に同等のものをユーザーに提供するポイント プログラムを許可します。

すべてのアプリ（ゲーム およびゲーム以外）：

- ポイント プログラムの特典は、アプリ内の対象となる金銭取引に明確に付加および従属するものでなければなりません（対象となる金銭取引は、ポイント プログラムとは関係のない、商品またはサービスを提供するための完全に別個の取引である必要があります）。また、特典の購入方法を別途提供したり、「現金を伴うギャンブル、ゲーム、コンテンツに関するポリシー」で禁止されている交換方法に結び付けたりしてはなりません。
  - たとえば、対象となる金銭取引のいかなる部分も、ポイント プログラムに参加するための料金または賭け金を表すものであってはなりません。また、対象となる金銭取引により、通常価格を上回る金額で商品またはサービスを購入する結果になってはいけません。

ゲーム アプリ:

- ポイントまたは特典（対象となる金銭取引に関連する特典も含む）の付与およびユーザーによる利用は、一定の比率でのみ行い、その比率はアプリ内の目立つ場所のほか、一般公開されているプログラム公式ルール内にも明記しなければなりません。また、特典や換金額を、ゲームの成績や偶然ベースの結果に対して賭けられる、あるいは結果により獲得 / 増加できることは**許可されていません**。

ゲーム以外のアプリ:

- ポイントや特典は、下記の要件を遵守している場合、コンテストや偶然ベースの結果に結び付けることができます。対象となる金銭取引に関連する特典を含むポイント プログラムは、以下の条件を満たす必要があります。
  - アプリ内でプログラムの正式なルールを公開する。
  - プログラムにおいて、変数、偶然ベース、またはランダム化されたポイント システムを使用している場合: 1）一定の確率に基づいてポイントを決定するポイント プログラムの場合はその確率、2）それ以外のポイント プログラムの場合はその選択方法（例: 変数に基づいてポイントを決定する）を、プログラムの公式利用規約内で開示する。
  - 抽選、懸賞、またはその他の類似するスタイルのプロモーションを提供するプログラムの正式な利用規約内で、プロモーションごとに、一定の当選者数、申し込み締切日、および授与日を指定する。
  - ポイントや特典が一定の比率で発生し利用できる場合は、アプリ内の目立つ場所のほか、プログラムの正式な利用規約内にもその比率を文書化する。

ポイント プログラムを伴うアプリの種類	**ポイント プログラムのゲーム性、特典の変動**	**一定の比率 / スケジュールに基づくポイント特典**	**ポイント プログラムの利用規約が必須**	**偶然ベースのポイント プログラムの確率と選択方法を利用規約で開示する必要がある**
ゲーム	許可しない	許可	必須	なし（ゲームアプリはポイント プログラム内に偶然ベースの要素を含めることが認められない）
ゲーム以外	許可	許可	必須	必須

Play 配信アプリ内でのギャンブルやリアルマネー ベースのゲーム、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広告が表示されるアプリは、以下の要件を遵守する場合に限り許可されます。

- 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および業界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、対象地域で適用される広告のライセンス要件を遵守する必要があります。
- アプリは、18 歳未満であることが明らかになった個人にはギャンブルの広告を表示できません。
- アプリは、ファミリー向けプログラムには登録できません。
- アプリは、18 歳未満の個人を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）。
- ギャンブルや現金を伴うゲーム、宝くじ、トーナメントをサポートする機能やコンパニオン機能（賭博、支払い、スポーツのスコア、オッズ、成績の追跡、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。
- アプリのコンテンツで、ギャンブルや現金を伴うゲーム、宝くじ、トーナメントに関するサービスを宣伝したり、そのようなサービスにユーザーを誘導したりしてはなりません。

ギャンブルや現金を伴うゲーム、宝くじ、トーナメントに関する広告を掲載できるのは、上記の要件をすべて遵守するアプリに限られます。承認されたギャンブル アプリ（上記に定義されるアプリ）、または上記 1～6 の要件を遵守する承認済みのデイリー ファンタジー スポーツ アプリ（下記に定義されるアプリ）には、ギャンブルや現金を伴うゲーム、宝くじ、トーナメントに関する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一体化された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
- ボタンやアイコンといった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、「虚偽広告に関するポリシー」に違反してい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（配信対象地域で適用される法律で定義されるもの）は、以下の要件を遵守する場合に限り許可されます。

- アプリは、1）米国内でのみ配布されるか、2）米国以外の国では上記のギャンブル アプリの要件と申し込み手続きを遵守するものとします。
- デベロッパーは、Play 上でアプリを配信するには、DFS 申し込み　手続きを完了し、承認を受ける必要があります。
- アプリは、配信対象国で適用される法律および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、アプリ内で賭博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、Play ストアからのダウンロードとインストールを無料にする必要があります。
- 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必要があります。
- 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。
- 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。
- デベロッパーは、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。
- デベロッパーはデイリー 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る米国の州または準州以外の地域で、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内の州や準州では、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。

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。

- 違法薬物の売買の推進。
- 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 が含まれるアプリや UGC を提供するアプリ（ユーザーを UGC プラットフォームに誘導するための特殊なブラウザまたはクライアントを備えたアプリを含む）では、以下に示す UGC モデレーションを着実かつ効果的に継続して実施する必要があります。

- 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。
- Google Play デベロッパー プログラム ポリシーを基準として不適切なコンテンツや行為を定義し、アプリの利用規約やユーザー ポリシーでそれらを禁止します。
- アプリでホストされる UGC の種類に合わせて、妥当かつ一貫性のある形で UGC モデレーションを実施します。
  - 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 やユーザーについて報告するためのアプリ内システムを提供し、報告された UGC やユーザーに対して適切な措置を講じます。
- UGC やユーザーをブロックするためのアプリ内システムを提供します。
- 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。

偶発的な性的コンテンツ

UGC アプリに性的なコンテンツが表示されている場合でも、(1) 主に性的でないコンテンツへのアクセスを提供しており、(2) 性的なコンテンツを積極的に宣伝または推奨していない場合は、「偶発的」な性的コンテンツと見なされます。ただし、適用される法律で違法と定義されている性的なコンテンツや、児童を危険にさらす　コンテンツは、「偶発的」とは見なされず許可されません。

以下のすべての要件を満たしている場合、その UGC アプリには偶発的な性的コンテンツが含まれている可能性があります。

- 該当するコンテンツがデフォルトではフィルタされて非表示になり、フィルタを完全に無効にするには 2 つ以上のユーザー操作が必要となる（例: 表示遮断フィルタによって難読化されている、「セーフサーチ」が有効になっているとデフォルトで表示されない）。
- ファミリー ポリシー　に定義されている「子供」が、年齢確認システム（年齢詐称を予防する年齢確認　、適用される法律で定義されている適切なシステムなど）を使用してアプリにアクセスすることが明示的に禁止されている。
- コンテンツのレーティングに関するポリシー　の要件に沿って、UGC に関するコンテンツ レーティング質問票に対して正確な回答を提出している。

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。

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。

健康に関するコンテンツおよびサービス

健康関連の有害なコンテンツおよびサービスをユーザーに提供または紹介するアプリは認められません。

健康に関するコンテンツやサービスを含むまたは宣伝するアプリについては、適用される法律および規制を遵守しなければなりません。

処方薬

処方箋なしでの処方薬の売買を推進するアプリは認められません。

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。

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。

- 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。

健康に関する誤った情報

医学的な統一見解に矛盾する、またはユーザーに害を及ぼす可能性がある、誤解を与えるような効果効能をうたうアプリは認められません。

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。

- ワクチンについて誤解を与える表現（ワクチンは DNA を変化させる可能性があるなど）。
- 承認されていない有害な治療法の擁護。
- 転向療法など、健康に有害なその他の行為の擁護。

COVID-19（新型コロナウイルス感染症）に関する制限

アプリは新型コロナウイルス感染症 2019（COVID-19）アプリの要件 を遵守する必要があります。

医療関連の機能

誤解を招く、もしくは有害となる可能性がある医療や健康関連の機能を提供するアプリは認められません。たとえば、アプリの機能のみで酸素濃度を測定できると申告するアプリは許可されません。酸素濃

度測定アプリには、酸素濃度測定機能をサポートできるように設計された外部ハードウェア、ウェアラブル、またはスマートフォンの専用センサーによる支援が必要です。また、これらの支援を必要とするアプリはメタデータに免責条項を含め、医療用の用途は想定されていないこと、一般的なフィットネスと健康維持のみを目的として設計されていること、医療用デバイスではないことを明記し、互換性のあるハードウェアまたはデバイスのモデルを正しく開示する必要があります。

お支払い - 臨床サービス

法規制の対象となる臨床サービスに関係するお支払いの場合、Google Play の課金システムを利用することはできません。詳しくは、Google Play のお支払いに関するポリシーについて をご覧ください。

ヘルスコネクトのデータ

ヘルスコネクト権限を通じてアクセスされたデータは、ユーザーの個人情報および機密情報と見なされ、ユーザーデータ に関するポリシーおよび追加要件 が適用されます。

知的財産権

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、偽造品の報告 を行ってください。

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、画像および映像など）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承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。オリジナルのものを作成することが、通常は最も安全な方法です。

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。

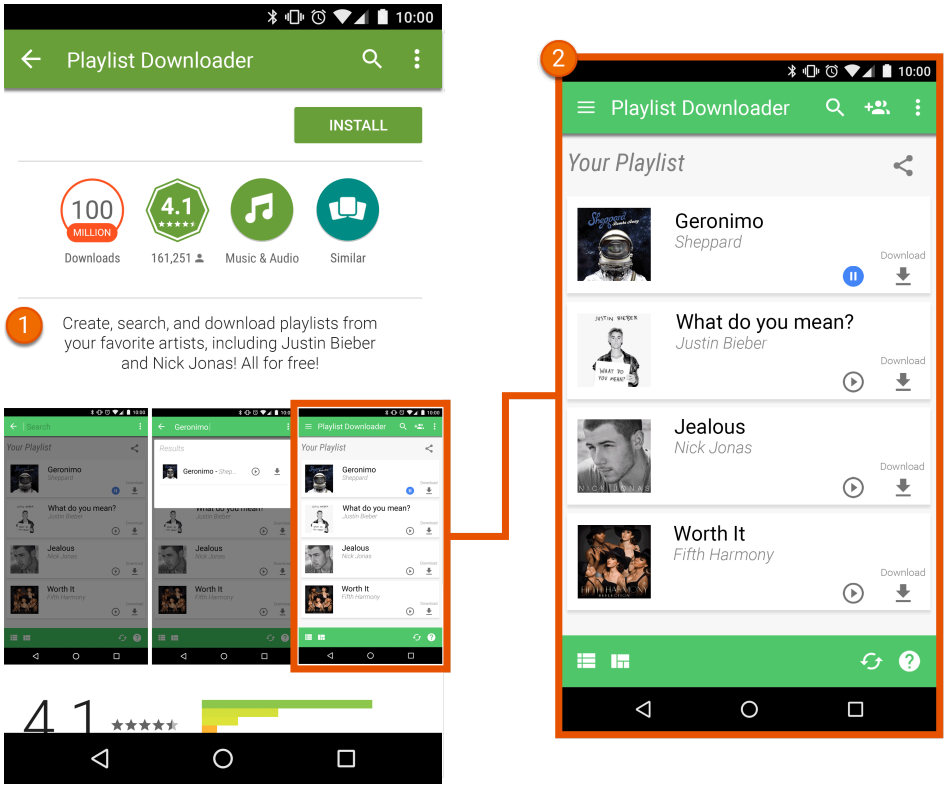
- 音楽のアルバム、ビデオゲーム、書籍のカバーアート
- 映画、テレビ、ビデオゲームのマーケティング画像
- マンガ、アニメ、映画、ミュージック ビデオ、テレビのアートワークや画像
- 大学やプロのスポーツチームのロゴ
- 有名人のソーシャル メディア アカウントから取得した写真
- 有名人のプロによる画像
- 著作権で保護されているオリジナル作品と区別がつきにくい複製または「ファンアート」
- 著作権で保護されているコンテンツの音声クリップを再生するサウンドボードを持つアプリ
- パブリック ドメイン以外の書籍の完全な複製や翻訳

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。

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。

- 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 この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。

偽造品

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、真正品と偽って販売するために、対象商品のブランドの特徴を模倣したものです。

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、ユーザーにとって安全な環境を実現するよう力を尽くしています。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。それには、アプリによるユーザー データのアクセス、収集、使用、処理、共有の方法を示すとともに、データの使用をポリシーに準拠した目的に制限することが求められます。ユーザーの個人情報と機密情報の扱いについては、さらに下記の「ユーザーの個人情報と機密情報」に示す要件も適用されることにご注意ください。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。

サードパーティのコード（SDK など）をアプリに含める場合には、アプリ内で使用するサードパーティのコードと、アプリでのサードパーティによるユーザーデータの扱いが、使用と開示に関する要件を含め、Google Play デベロッパー プログラム ポリシーに準拠していることを確認する必要があります。たとえば、SDK プロバイダがアプリを通じてユーザーの個人情報や機密情報を販売しないようにする必要があります。この要件は、ユーザーデータがサーバーに送信された後で転送される場合にも、サードパーティのコードをアプリに埋め込むことで転送される場合にも適用されます。

ユーザーの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、健康に関するデータ、Health Connect のデータ、デバイス上の他のアプリの一覧、マイクや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個人情報や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のアクセス、収集、使用、および共有を、ユーザーが合理的に予期する目的に適合するアプリとサービスの機能、およびポリシーにのみ許可すること。
  - ユーザーの個人情報や機密情報を使用して広告を配信するアプリは、Google Play の広告ポリシーに準拠する必要があります。
  - サービス プロバイダが必要とする場合、あるいは政府機関による有効な要請や適用される法律を遵守するため、もしくは合併または買収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。
- 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や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、可能な限り実行時の権限をリクエストすること。
- ユーザーの個人情報や機密情報を販売しないこと。
  - 「販売」とは、金銭的対価を目的に第三者との間でユーザーの個人情報や機密情報の交換または転送を行うことを意味します。
    - ユーザーの個人情報や機密情報をユーザーが転送すること（たとえば、ユーザーがアプリの機能を使用して特定のファイルを第三者に転送したり、調査研究専用のアプリを使用したりすること）は、販売とは見なされません。

認識しやすい開示と同意の要件

アプリによるユーザーの個人情報や機密情報のアクセス、収集、使用、共有が、対象のプロダクトや機能のユーザーが合理的に予測できる範囲を超えている場合（たとえばユーザーがアプリを操作していないときに、データの収集がバックグラウンドで行われるなど）には、以下の要件を満たす必要があります。

認識しやすい開示: 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次のとおりです。

- 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。

同意およびランタイム権限: アプリ内でのユーザーによる同意のリクエストや、ランタイム権限のリクエストを行う場合は、その直前にこのポリシーの要件に沿ってアプリ内で開示される必要があります。同意を求める場合は、以下のようにする必要があります。

- 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。
- アプリがユーザーの個人情報と機密情報の収集やアクセスを開始するには、事前にユーザーの許可を得る必要があります。

他の法的根拠（EU の GDPR における正当な利益など）に基づいてユーザーの同意なく個人情報と機密情報を処理するアプリは、適用されるすべての法的要件を遵守するとともに、ユーザーに対して、このポリシーで要求されるアプリ内開示を含む適切な開示を行う必要があります。

ポリシーの要件に準拠するには、認識しやすい開示に関する以下のサンプル フォーマットを必要に応じて参照することをおすすめします。

- 「[このアプリ] は、[機能] を可能にするために、[想定される状況]、[データの種類] を [収集 / 転送 / 同期 / 保存] します。」
- *例: 「Fitness Funds は、フィットネスの記録を可能にするために、アプリが閉じているときや使用されていないときでも、位置情報を収集します。また、位置情報は広告をサポートするためにも使用されます。」*
- *例: 「Call buddy は、組織への連絡を可能にするために、アプリが使用されていないときでも、通話履歴の書き込みと読み込みのデータを収集します。」*

デフォルトでユーザーの個人情報と機密情報を収集するように設計されているサードパーティのコード（SDK など）がアプリに統合されている場合は、Google Play による要請を受けてから 2 週間以内に（Google Play によってそれより長い期間が与えられている場合はその期間内に）、アプリがこのポリシーの認識しやすい開示と同意の要件（サードパーティのコードを通じたデータのアクセス、収集、使用、共有に関する要件を含む）を満たしていることを示す、十分な根拠を提示する必要があります。

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。

- デバイスの位置情報を収集するにもかかわらず、このデータを使用する機能と、バックグラウンドでのアプリの使用について、認識しやすい開示で説明していないアプリ。
- データの使用目的を説明する認識しやすい開示が提示される前に、データへのアクセスを要求する実行時の権限が付与されているアプリ。
- 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。
- ユーザーの個人情報と機密情報を収集し、そのデータをこのユーザーデータ ポリシーや、アクセス、データ処理（許可されていない販売を含む）、認識しやすい開示と同意の要件に沿って処理しない SDK を使用するアプリ。

認識しやすい開示と同意の要件について詳しくは、この記事をご覧ください。

個人情報と機密情報へのアクセスに関する制限

上記の要件に加えて、特定の操作における要件を下表に記載します。

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。
アプリが子供を対象とする場合	子供向けサービスで使用が承認されていない SDK をアプリに含めてはなりません。ポリシーのすべての文言と要件については、子供向けやファミリー向けにアプリを設計する をご覧ください。
永続的なデバイス識別子（IMEI、IMSI、SIM のシリアル番号など）を収集またはリンクするアプリの場合	永続的なデバイス識別子を、他の個人情報と機密情報、またはリセット可能なデバイス識別子にリンクしてはなりません。ただし、以下を目的とする場合を除きます。 • SIM 識別子にリンクされた通話機能（例: 携帯通信会社アカウントにリンクされた Wi-Fi 通話機能） • デバイス所有者モードを使用するエンタープライズ デバイス管理アプリ これらの使用方法は、ユーザーデータに関するポリシー の規定に沿って、ユーザーが認識しやすいように開示する必要があります。 その他の一意の識別子については、こちらのリソース をご覧ください。 Android 広告 ID に関する追加のガイドラインについては、広告ポリシー をお読みください。

データ セーフティ セクション

すべてのデベロッパーは、すべてのアプリについて、ユーザーデータの収集、使用、共有に関する詳細な説明を、データ セーフティ セクションに明瞭かつ正確に記載する必要があります。デベロッパーには、ラベルを正確に記載し、ラベルの情報を最新の状態に保つ責任があります。データ セーフティ セクションは、該当箇所において、アプリのプライバシー ポリシーで開示されている内容と一致する必要があります。

データ セーフティ セクションへの入力に関する追加情報については、こちらの記事 をご覧ください。

プライバシー ポリシー

すべてのアプリで、プライバシー ポリシーのリンクを Google Play Console 内の所定の欄に掲載し、アプリ内にはプライバシー ポリシーのリンクまたはテキストを掲載する必要があります。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、当該アプリでユーザーデータ（データ セーフティ セクションで開示されているデータに限定されない）がどのようにアクセス、収集、使用、共有されるかを包括的に開示する必要があります。これには以下の情報が含まれます。

- デベロッパー情報、およびプライバシーに関する連絡先または問い合わせを行う方法。
- アプリがアクセス、収集、使用、共有するユーザーの個人情報や機密情報の種類、およびユーザーの個人情報や機密情報の共有先の開示。
- ユーザーの個人情報や機密情報を安全に処理するための手順。
- デベロッパーのデータ保持ポリシーおよびデータ削除ポリシー。
- プライバシー ポリシーであることが明瞭にわかるラベル付け（たとえば、タイトルに「プライバシー ポリシー」と記載する）。

アプリの Google Play ストアの掲載情報に記載されている主体（デベロッパーや会社等）がプライバシー ポリシーに明記されている、もしくはアプリ名がプライバシー ポリシーに明記されている必要があります。ユーザーの個人情報や機密情報にアクセスしないアプリであっても、プライバシー ポリシーを掲載する必要があります。

プライバシー ポリシーは必ず、どの国からもアクセスできるよう、アクセス制限のない一般公開の有効な URL（PDF は不可）で参照可能、かつ編集不可にしてください。

アプリセット ID の使用

Android では、分析や不正防止などの重要なユースケースに対応するために、新しい ID が導入されます。この ID を使用するための規約は以下のとおりです。

- **使用**: アプリセット ID を広告のパーソナライズと広告の測定に使用することはできません。
- **個人を特定できる情報またはその他の識別子との関連付け:** 広告を目的として、アプリセット ID を Android の識別子（例: AAID）または個人情報や機密情報に関連付けることはできません。
- **透明性と同意:** アプリセット ID を収集および使用することと、この規約を遵守していることを、法的に適切なプライバシーに関するお知らせ（デベロッパー独自のプライバシー ポリシーを含む）を通じてユーザーに開示する必要があります。必要に応じて、ユーザーから法的に有効な同意を得る必要があります。Google のプライバシー基準について詳しくは、ユーザーデータに関するポリシー をご確認ください。

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

Google が公開している、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、以下の義務があります。

- 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、不正または違法アクセス、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、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 情報の処理を停止するか、適切な水準の保護を確保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。

2020 年 7 月 16 日をもって、Google では、欧州経済領域または英国から米国へのデータ転送において EU-U.S. Privacy Shield（EU-US プライバシー シールド）の利用を終了しました（詳細）。詳しくは、デベロッパー販売 / 配布契約の第 9 条をご覧ください。

機密情報にアクセスする権限または API

機密情報にアクセスする権限や API 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、機密情報にアクセスする権限や API をリクエストできるのは、アプリで現在提供している機能やサービスの実装に必要で、それらが Google Play ストアの掲載情報に掲載されている場合に限られます。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、機密情報にアクセスする権限や API は利用できません。機密情報にアクセスする権限または API を通じてアクセスした個人情報や機密情報を販売したり、販売を促進する目的で共有したりすることは禁止されています。

データにアクセスするために、機密情報にアクセスする権限または API をリクエストする場合は、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（段階的にリクエストする形で）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って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出てきた場合は、その追加の用途に関して、あらためて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」、「Signature」と指定される権限、または下記のような権限です。これらの権限には、以下に示す追加の要件と制限が適用されます。

- 制限付きの権限を通じてアクセスされたユーザーデータやデバイスデータは、ユーザーの個人情報および機密情報と見なされ、ユーザーデータに関するポリシー の要件が適用されます。
- 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。
- Google Play のマルウェアに関するポリシー （昇格させた権限の悪用 を含む）に違反する権限の使用は、明示的に禁止されています。

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と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
通話履歴に関する権限グループ（例: READ_CALL_LOG、WRITE_CALL_LOG、PROCESS_OUTGOING_CALLS）	ユーザーのデバイスで、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。
SMS に関する権限グループ（例: READ_SMS、SEND_SMS、WRITE_SMS、RECEIVE_SMS、RECEIVE_WAP_PUSH、RECEIVE_MMS）	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 ハンドラとして能動的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権限は、承認済みの重要なアプリの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である場合もあり、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「壊れている」、使用できない、と見なされるような機能が「重要な機能」にあたります。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。

位置情報の利用許可

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、バックグラウンドでの位置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利用許可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 を遵守してい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。

ポリシー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。

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 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には、MANAGE_EXTERNL_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。

パッケージ（アプリ）の公開設定権限

デバイスにクエリして入手したインストール済みアプリのインベントリは、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。

デバイス上の他のアプリを起動、検索、相互運用することが主要な目的であるアプリは、以下で概説するように、デバイス上の他のインストール済みアプリに対して、スコープに応じた可視性を得ることができます。

- **広範なアプリの可視性:** 広範な可視性とは、アプリがデバイス上のインストール済みアプリ（「パッケージ」）を幅広く（「広範に」）見渡せる（可視性が与えられている）ことを指します。
  - API レベル 30 以降 をターゲットとするアプリの場合、QUERY_ALL_PACKAGES 権限によってインストール済みアプリについて広範な可視性が得られるのは、特定のユースケース（当該アプリが機能するためにデバイス上のすべてのアプリを認識するか、それらのアプリと相互運用する必要がある）に制限されます。
    - スコープを絞ったパッケージの可視性を宣言 （広範な可視性をリクエストせず、特定のパッケージをクエリしてやり取りするなど）して動作させることが可能なアプリでは、QUERY_ALL_PACKAGES を使用しないでください。
  - QUERY_ALL_PACKAGES 権限に関連する広範な可視性レベルに近い別の方法の使用も同様に、ユーザー向けの主要なアプリ機能と、その別の方法によって検出されたアプリとの相互運用に制限されます。
  - QUERY_ALL_PACKAGES 権限を使用できるユースケースについては、こちらのヘルプセンター記事 をご覧ください。
- **限定的なアプリ公開設定**: 限定的な公開設定とは、アプリが、よりターゲットを絞った（「広範」ではない）方法を使って特定のアプリのクエリを行うことによりデータへのアクセスを最小限に抑える場合（アプリのマニフェスト宣言を満たす特定のアプリのクエリを行う場合など）を指します。アプリが相互運用性に関するポリシーを遵守している場合や他のアプリの管理を担っている場合は、この方法でそれらのアプリのクエリを行えます。
- デバイス上のインストール済みアプリのインベントリに対する公開設定は、アプリの主要な目的やユーザーがアプリ内でアクセスする主要な機能に直接関連する必要があります。

Play で配信中のアプリにクエリして入手したアプリ インベントリのデータを、分析や広告収益化の目的で販売、共有することは禁止されています。

Accessibility API

Accessibility API を次の目的で使用することはできません。

- ユーザーの許可なくユーザー設定を変更したり、ユーザーがアプリまたはサービスを無効化またはアンインストールできないようにしたりする。ただし、保護者による使用制限を使用するアプリを通じて親権者または保護者の許可を得るか、エンタープライズ マネジメント ソフトウェアを通じて認定済み管理者の許可を得た場合を除きます。
- Android の組み込みのプライバシー管理とプライバシー通知を回避する。
- 不正な方法または Google Play デベロッパー ポリシーに違反するその他の方法で、ユーザー インターフェースを変更または利用する。

Accessibility API は、リモート通話の音声録音用には設計されておらず、そのようなリクエストを受けることもできません。

Accessibility API を使用する場合は、Google Play のストアの掲載情報に記載する必要があります。

IsAccessibilityTool に関するガイドライン

障がいのあるユーザーを直接サポートする機能が主体になっているアプリは、**IsAccessibilityTool** を使用して、ユーザー補助アプリとして公式に表明できます。

IsAccessibilityTool の対象とならないアプリはこのフラグを使用できませんが、ユーザー補助に関連する機能をユーザーが認識しにくいため、ユーザーデータに関するポリシー に規定されている「認識しやすい開示と同意」の要件を遵守する必要があります。詳しくは、AccessibilityService API のヘルプセンター記事をご覧ください。

Accessibility API を使用しなくても必要な機能を提供できるのであれば、より限定された範囲の API と権限 をアプリで使用してください。

パッケージ インストールのリクエスト（REQUEST_INSTALL_PACKAGES）権限

REQUEST_INSTALL_PACKAGES 権限を使用すると、アプリからアプリ パッケージのインストールをリクエストできます。この権限を使用するには、アプリのコア機能に以下が含まれている必要があります。

- アプリ パッケージを送信または受信する機能、および
- ユーザーが自発的にアプリ パッケージのインストールを開始する機能

たとえば次のような機能が許可されています。

- ウェブのブラウジングまたは検索
- 添付ファイルをサポートするコミュニケーション サービス
- ファイルの共有、転送、管理
- 企業向けデバイスの管理
- バックアップと復元
- デバイスの移行または電話の転送

コア機能とは、アプリの主要な目的を果たすために必要不可欠な機能を指し、そのすべてがアプリの説明文に認識しやすい形で明記されている必要があります。

REQUEST_INSTALL_PACKAGES 権限は、デバイス管理を目的とする場合を除き、自動更新、修正、アセット ファイル内での他の APK のビルドには使用できません。パッケージの更新とインストールにおいては、常に Google Play のデバイスやネットワークでの不正行為 に関するポリシーに準拠しなければならず、ユーザーが自発的に操作する必要があります。

Android の権限によるヘルスコネクト

ヘルスコネクト権限を通じてアクセスされたデータは、ユーザーの個人情報および機密情報と見なされ、ユーザーデータに関するポリシーおよび以下の追加要件が適用されます。

ヘルスコネクトのアクセス方法と使用方法

ヘルスコネクトを通じてデータにアクセスするためのリクエストは、明確にわかりやすく記述してください。ヘルスコネクトは、該当するポリシーと利用規約を遵守したうえで、このポリシーによって規定されている承認された用途に限り使用できます。これはつまり、権限へのアクセスをリクエストできるのは、アプリまたはサービスの用途が、承認されているいずれかの用途に該当する場合に限られることを意味します。

ヘルスコネクト権限へのアクセスを承認される用途は次のとおりです。

- ユーザーの健康とフィットネスにとって有益な 1 つ以上の機能をユーザー インターフェースを通じて利用できるアプリまたはサービス。ユーザーが自分の身体活動、睡眠、心身の健康、栄養、健康状態の測定値、身体的特徴、および / または健康とフィットネスに関連するその他の記述や測定値を直接**記録、レポート、モニタリング、および / または分析**できる。
- ユーザーの健康とフィットネスにとって有益な 1 つ以上の機能をユーザー インターフェースを通じて利用できるアプリまたはサービス。ユーザーが自分の身体活動、睡眠、心身の健康、栄養、健康状態の測定値、身体的特徴、および / または健康とフィットネスに関連するその他の記述や測定値をスマ

ートフォンおよび / またはウェアラブルに**保存**して、用途に適合するその他のオンデバイス アプリとデータを共有できる。

ヘルスコネクトは、ユーザーが Android デバイス内のさまざまなソースから健康とフィットネスに関するデータを集めて、特定の第三者と共有できる、汎用のデータ ストレージおよびデータ共有プラットフォームです。データは、ユーザーが任意に選択したソースから集めることができます。デベロッパーは、ヘルスコネクトが意図する用途に適しているかを評価するとともに、特定の目的に関連して、また特に調査、健康、または医療上の用途について、ヘルスコネクトからのデータのソースと質を精査する必要があります。

- ヘルスコネクトを通じて取得したデータを使用して、健康関連の被験者調査を実施するアプリは、被験者（未成年者の場合は保護者）の同意を得る必要があります。そのような同意事項には、(a) 調査の性質、目的、期間、(b) 調査手順、被験者に対するリスクおよび利点、(c) データの機密性および取り扱い（第三者との共有を含む）に関する情報、(d) 被験者の質問に対応する問い合わせ先、(e) 取り消し手順が含まれるものとします。ヘルスコネクトを通じて取得したデータを使用して、健康関連の被験者調査を実施するアプリは、(1) 被験者の権利、安全、心身の健康を保護する目的を持ち、(2) 被験者調査を精査、変更、承認する権限を有する、独立した委員会による承認を得る必要があります。要請があった場合には、そのような承認の証明を提出しなければなりません。
- デベロッパーは、ヘルスコネクトの用途、およびヘルスコネクトを通じて得られたデータの用途に基づいて適用される、規制または法律上の要件を遵守する責任があります。Google の特定のプロダクトまたはサービスについて、Google が提供するラベルまたは情報に明示的に記載されていない限り、Google は、特に調査、健康、医療用途に限らず、いかなる用途または目的でも、ヘルスコネクトに含まれるデータの使用を推奨し、その正確性を保証することはありません。Google は、ヘルスコネクトを通じて取得されたデータの使用に関連する、いかなる責任も負いません。

限定的な使用

適切な用途でヘルスコネクトを使用する際には、ヘルスコネクトを通じてアクセスするデータも、以下の要件を遵守して使用する必要があります。これらの要件は、ヘルスコネクトから取得した元データと、元データから集計、匿名化、または取得されたデータに適用されます。

- ヘルスコネクトのデータの使用は、リクエスト元アプリのユーザー インターフェースに明確に表示される、適切な用途または機能の提供もしくは改善に限定されます。
- 以下の目的がある場合を除き、ユーザーデータを第三者に譲渡してはなりません。
  - ユーザーの同意に基づき、リクエスト元アプリのユーザー インターフェースに明確に表示される、適切な用途または機能を提供もしくは改善する場合。
  - セキュリティ上の目的で必要な場合（不正使用の調査など）。
  - 適用される法律および / または規制を遵守するために必要な場合。
  - ユーザーから事前に明示的な同意を得た後で、デベロッパーの合併、買収、または資産売買の一環として行う場合。
- 以下の場合を除き、人にユーザーデータが読まれないようにする必要があります。
  - 特定のデータを読まれることに、ユーザーが明示的に同意している場合。
  - セキュリティ上の目的で必要な場合（不正使用の調査など）。
  - 適用される法律を遵守するために必要な場合。
  - データ（派生データを含む）を集計し、適用されるプライバシー要件および地域のその他の法的要件を遵守した、内部オペレーションのために使用する場合。

ヘルスコネクト データのその他の譲渡、使用、または販売は、以下の行為を含めてすべて禁止されています。

- 広告プラットフォーム、データ ブローカー、または情報リセラーなどの第三者にユーザーデータを譲渡または販売すること。
- パーソナライズ広告やインタレスト ベース広告など、広告の配信を目的としてユーザーデータを譲渡、販売、または使用すること。
- 信用力を判断するため、または貸与目的でユーザーデータを譲渡、販売、または使用すること。

- 連邦食品・医薬品・化粧品法のセクション 201(h) に基づく医療機器と見なされるプロダクトまたはサービスを使用して、規制対象の機能を実行するために、ユーザーデータを譲渡、販売、または使用すること。
- Google から書面による事前の承認を得ている場合を除き、（HIPAA によって定義される）保護対象保健情報に関連する目的で、方法を問わず、ユーザーデータを譲渡、販売、または使用すること。

このポリシー、またはヘルスコネクトについて適用されるその他の利用規約またはポリシーに違反する形で、ヘルスコネクトにアクセスしてはなりません。これには以下を目的とする場合が含まれます。

- ヘルスコネクトの使用または障害によって、死亡、人身傷害、もしくは環境上または財産上の損害に至ることが合理的に予想されるようなアプリ、環境、またはアクティビティ（核施設、航空管制システム、生命維持装置、兵器の作成または操作など）については、その開発、あるいはそれらに組み込む目的で、ヘルスコネクトを使用してはなりません。
- ヘルスコネクトを通じて取得したデータに、ヘッドレス アプリを使用してアクセスしてはなりません。アプリでは、アプリトレイ、デバイスのアプリ設定、通知アイコンなどに、明確に特定できるアイコンを表示する必要があります。
- 対応していないデバイスまたはプラットフォーム間でデータを同期するアプリで、ヘルスコネクトを使用してはなりません。
- 子供だけを対象としているアプリ、サービス、または機能にヘルスコネクトを接続することはできません。主に子供を対象としているサービスでヘルスコネクトを使用することは承認されていません。

ヘルスコネクトのデータの使用が、限定的な使用に関する制限を遵守していることを示す確認的陳述書を、アプリ内、あるいはウェブサービスまたはアプリに関連するウェブサイト上で開示する必要があります。たとえばホームページで、専用ページまたはプライバシー ポリシーに関する注記へのリンクを示し、「ヘルスコネクトから受け取った情報の使用については、限定的な使用に関する要件を含む、ヘルスコネクト権限ポリシーを遵守してください」などと記載します。

最小範囲

アクセス権限をリクエストできるのは、アプリまたはサービスの機能を実装するために不可欠な場合に限ります。

これは次のことを意味します。

- 必要のない情報へのアクセス権限はリクエストしないでください。プロダクトの機能またはサービスの実装に必要なアクセス権限のみリクエストできます。プロダクトで特定のアクセス権限を必要としない場合、そのアクセス権限はリクエストしないでください。

通知と管理の透明性と正確性

ヘルスコネクトは健康とフィットネスに関するデータを扱いますが、それには個人情報と機密情報が含まれます。すべてのアプリとサービスについてプライバシー ポリシーを規定し、アプリまたはサービスがユーザーデータを収集、使用、共有する方法を包括的に開示する必要があります。開示する情報には、ユーザーデータを共有する当事者の種類、データの使用方法、データの保存と保護の方法、アカウントが無効になるか削除された場合のデータの扱いが含まれるものとします。

適用される法律で規定されている要件に加えて、デベロッパーは以下の要件を遵守する必要があります。

- データのアクセス、収集、使用、共有について開示する必要があります。開示については次のことが求められます。
  - ユーザーデータへのアクセスを求めるアプリまたはサービスの識別情報を正確に示す。
  - アクセス、リクエスト、および / または収集するデータの種類に関して、明確かつ正確な情報を提供する。
  - データを使用、共有する方法を示す。1 つの目的でデータをリクエストしながら、別の目的でもデータを使用する場合には、ユーザーに両方の用途を通知する必要があります。
- ユーザーがアプリ上で個人データを管理または削除する方法を示すヘルプ ドキュメントを提供する。

安全なデータ処理

ユーザーデータはすべて安全に扱う必要があります。デベロッパーは合理的かつ適切な手順に沿って、ヘルスコネクトを使用するすべてのアプリケーションまたはシステムを、不正または違法なアクセス、使用、破壊、紛失、改変、開示から保護する必要があります。

推奨されるセキュリティ対策としては、たとえば ISO/IEC 27001 などで規定されている情報セキュリティ管理システムを実装して維持することで、アプリまたはウェブサービスを堅牢にし、OWASP トップ 10 に示されているセキュリティ上の一般的な問題がない状態を確保することが挙げられます。

デベロッパーのプロダクトによってユーザーが所有するデバイスからデータが転送される場合には、使用している API、ユーザーによる権限付与の数、またはユーザー数に応じて、アプリまたはサービスについて定期的なセキュリティ評価を受け、指定した第三者による評価文書を取得する必要があります。

ヘルスコネクトに接続するアプリに関する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。

VPN サービス

VpnService は、アプリが独自の VPN ソリューションを拡張、構築できるようにするための基本クラスです。VPN がコア機能であり、VpnService を使用するアプリのみが、リモート サーバーへのデバイスレベルのセキュアなトンネルを作成できます。ただし、次のようなコア機能を実装するためリモート サーバーを必要とするアプリは例外となります。

- 保護者による使用制限や企業による管理を実装するアプリ。
- アプリの使用状況をトラッキングするアプリ。
- デバイス保護アプリ（ウイルス対策、モバイル デバイス管理、ファイアウォールなど）。
- ネットワーク関連ツール（リモート アクセスなど）。
- ウェブ ブラウジング用アプリ。
- テレフォニーサービスまたは接続サービスを提供するために VPN 機能の使用を必要とする携帯通信会社のアプリ。

VpnService を次の目的で使用することはできません。

- 認識しやすい開示および同意機能を実装せずに、ユーザーの個人情報や機密情報を収集する。
- 収益化を目的として、デバイスでの他のアプリからのユーザー トラフィックをリダイレクトまたは操作する（ユーザーの国とは異なる国から広告トラフィックをリダイレクトするなど）。
- アプリの収益化に影響を与えられるように広告を操作する。

VpnService を使用するアプリは、次のすべての要件を満たす必要があります。

- VpnService を使用することを Google Play の掲載情報に記載する。
- デバイスから VPN トンネル エンドポイントに送信されるデータを暗号化する。
- 広告の不正行為 、権限 、マルウェア に関するポリシーを含む、すべてのデベロッパー プログラム ポリシー に準拠する。

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やその他のデバイス、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）、サービスなど（デバイス上の他のアプリ、Google サービス、許可された携帯通信会社のネットワークを含む）を妨害、阻害、破損する、またはそれらに無断で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している必要があります。

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。この制限は、Android

API への間接アクセスを提供する仮想マシンまたはインタープリタ（WebView またはブラウザ内の JavaScript など）で実行されるコードには適用されません。

アプリまたはサードパーティのコード（SDK など）でインタープリタ言語（JavaScript、Python、Lua など）が実行時に読み込まれる場合（たとえば、アプリにパッケージされていない場合）、それらが Google Play ポリシーに違反する可能性があってはなりません。

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。

FLAG_SECURE の要件

FLAG_SECURE は、アプリのコードで宣言される表示関連のフラグです。アプリの使用中、UI に含まれるセンシティブ データの表示場所をセキュアなサーフェスに限定することを示せます。このフラグは、センシティブ データがスクリーンショットに表示されたり、セキュアでないディスプレイで閲覧されたりするのを防ぐために設計されています。デベロッパーは、アプリのコンテンツがアプリやユーザーのデバイスの外部で閲覧されたり、外部にブロードキャストまたは送信されたりできないようにする場合に、このフラグを宣言します。

セキュリティおよびプライバシー保護のため、Google Play で配信されるすべてのアプリが、他のアプリの FLAG_SECURE 宣言を尊重しなければなりません。つまり、他のアプリでの FLAG_SECURE の設定を回避する手段を作成または促進してはいけません。

ユーザー補助ツール として認められるアプリは、FLAG_SECURE で保護されたコンテンツをユーザーのデバイスの外部でアクセスするために転送、保存、またはキャッシュに保存しない限り、この要件の対象外となります。

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。

- 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方法や、セキュリティ保護の回避方法を推進または説明するアプリ。
- 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許可リストへの登録 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。
- アプリまたはサードパーティのコード（SDK など）のうち、信頼できないウェブ コンテンツ（http:// URL）、または信頼できないソースから取得された未検証の URL（信頼できないインテントで取得された URLなど）を読み込む JavaScript インターフェースが追加された WebView を含むもの。

虚偽の振る舞い

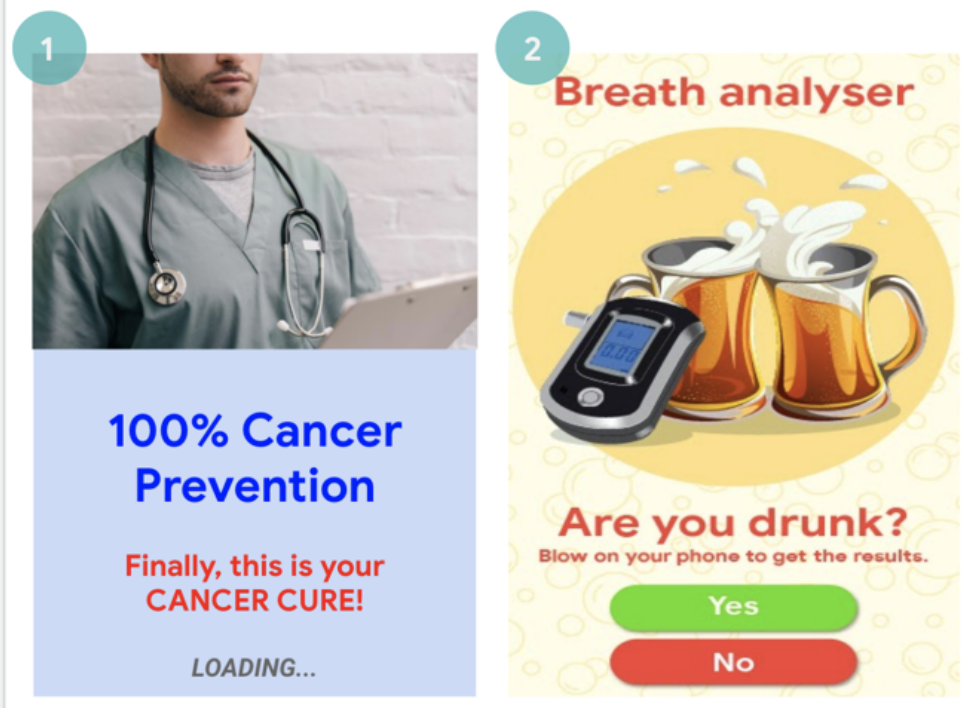
ユーザーを欺こうとするアプリや不正行為を助長するアプリは認められません。たとえば、機能的に不可能だと判断されるアプリが含まれますが、これに限定されません。アプリは、メタデータのあらゆる部分で、アプリの機能に関する説明、画像または動画を正確に開示しなければなりません。オペレーティング システムや他のアプリの機能または警告であるかのように装うことも認められません。デバイスの設定を変更する場合は、ユーザーに通知して同意を得ること、およびユーザーが簡単に元に戻せることが必要です。

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ていません。

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。

- 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。
- 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デバイス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。

不正行為を助長する

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、銀行口座、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。

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。

- 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、またはその作成に役立つ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。

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。

- 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

以下のようなアプリやデベロッパー アカウントは許可されません。

- 他の人や組織になりすましたり、オーナーや主目的を偽装、隠ぺいしたりしている。
- ユーザーに誤解を与えるような組織的行為に関与している。たとえば、配信元の国を偽装、隠ぺいしたり、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。
- 政治や社会問題、公衆の関心事に関連するコンテンツを扱っている場合に、他のアプリやサイト、デベロッパー、アカウントと連携して、デベロッパーやアプリの重要情報（身元など）を隠ぺい、偽装している。

Google Play の対象 API レベルに関するポリシー

ユーザーに安全で保護されたエクスペリエンスを提供するため、Google Play では**すべてのアプリ**に対し、以下の API レベルを対象とすることを義務付けます。

新規アプリとアプリ アップデートは、Android の最新のメジャー バージョンのリリースから 1 年以内にその Android API レベルをターゲットにする必要があります。この要件を満たさない新規アプリとアプリ アップデートは、Google Play Console からのアプリの送信ができなくなります。

アップデートのない既存の Google Play アプリ: Android の最新のメジャー バージョンのリリースから 2 年を過ぎてもその Android API レベルをターゲットにしていないアプリは、それ以降のバージョンの Android OS を搭載したデバイスの新規ユーザーからアクセスできなくなります。そのアプリを以前に Google Play からインストールしたユーザーは、アプリでサポートされていればどのバージョンの Android OS でも、引き続きアプリを検索、再インストール、使用できます。

対象 API レベルの要件を満たす方法についての技術的なアドバイスについては、移行ガイド　をご覧ください。

具体的なスケジュールや例外については、こちらのヘルプセンター記事　でご確認ください。

SDK に関する要件

アプリ デベロッパーが重要な機能やサービスをアプリに統合する際に、サードパーティのコード（SDK など）を使用することが多くなっています。アプリに SDK を含める場合は、ユーザーの安全を確保できること、あらゆる脆弱性からアプリを保護できることを確認する必要があります。ここでは、プライバシーとセキュリティに関する Google の既存の要件が、SDK との関連でアプリにどのように適用されるかについて説明し、これらの要件を満たすことで SDK を安全かつ確実にアプリに統合できることを示します。

アプリに SDK を含める場合、そのサードパーティのコードと実行に起因して、アプリが Google Play デベロッパー プログラム ポリシーに違反しないことを確認する責任はアプリ デベロッパーにあります。アプリ内の SDK がユーザーデータをどう扱っているかを理解し、SDK が使用する権限、収集するデータ、それらの使用目的を把握することが重要です。SDK によるユーザーデータの収集と処理が、アプリでのポリシー準拠のデータ使用と一貫していなければなりません。

SDK の使用がポリシー要件に違反していないことを確認するには、以下に挙げるポリシーの全文を読んで理解し、SDK に関連する既存の要件に注意を払ってください。

ユーザーデータに関するポリシー

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。それには、アプリによるユーザーデータのアクセス、収集、使用、処理、共有について開示するとともに、ポリシーに準拠した開示している目的にのみデータを使用することが求められます。

サードパーティのコード（SDK など）をアプリに含める場合には、アプリ内で使用するサードパーティのコードと、アプリでのサードパーティによるユーザーデータの扱いが、使用と開示に関する要件を含め、Google Play デベロッパー プログラム ポリシーに準拠していることを確認する必要があります。たとえば、SDK プロバイダがアプリを通じてユーザーの個人情報や機密情報を販売しないようにする必要があります。この要件は、ユーザーデータがサーバーに送信された後で転送される場合にも、サードパーティのコードをアプリに埋め込むことで転送される場合にも適用されます。

ユーザーの個人情報と機密情報

- アプリを通じて取得した個人情報や機密情報のアクセス、収集、使用、および共有を、ユーザーが合理的に予期する目的に適合するアプリとサービスの機能、およびポリシーにのみ許可すること。
  - ユーザーの個人情報や機密情報を使用して広告を配信するアプリは、Google Play の広告ポリシーに準拠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や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、可能な限り実行時の権限をリクエストすること。

ユーザーの個人情報や機密情報の販売

ユーザーの個人情報や機密情報を販売しないこと。

- 「販売」とは、金銭的対価を目的に第三者との間でユーザーの個人情報や機密情報の交換または転送を行うことを意味します。
  - ユーザーの個人情報や機密情報をユーザーが転送すること（たとえば、ユーザーがアプリの機能を使用して特定のファイルを第三者に転送したり、調査研究専用のアプリを使用したりすること）は、販売とは見なされません。

認識しやすい開示と同意の要件

アプリによるユーザーの個人情報や機密情報のアクセス、収集、使用、共有が、対象のプロダクトや機能のユーザーが合理的に予測できる範囲を超えている場合は、ユーザーデータに関するポリシーの認識しやすい開示と同意の要件を満たす必要があります。

デフォルトでユーザーの個人情報と機密情報を収集するように設計されているサードパーティのコード（SDK など）がアプリに統合されている場合は、Google Play による要請を受けてから 2 週間以内に（Google Play によってそれより長い期間が与えられている場合はその期間内に）、アプリがこのポリシーの認識しやすい開示と同意の要件（サードパーティのコードを通じたデータのアクセス、収集、使用、共有に関する要件を含む）を満たしていることを示す、十分な根拠を提示する必要があります。

サードパーティのコード（SDK など）を使用したことによって、アプリがユーザーデータに関するポリシーに違反することのないよう注意してください。

認識しやすい開示と同意の要件について詳しくは、こちらのヘルプセンター記事をご覧ください。

SDK に起因する違反の例

- ユーザーの個人情報と機密情報を収集し、そのデータをこのユーザーデータ ポリシーや、アクセス、データ処理（許可されていない販売を含む）、認識しやすい開示と同意の要件に沿って処理しない SDK を使用するアプリ。
- このポリシーのユーザーの同意に関する要件と認識しやすい開示に関わる要件に違反して、デフォルトでユーザーの個人情報と機密情報を収集する SDK を統合したアプリ。
- ユーザーの個人情報や機密情報を、不正対策のみを目的として収集すると主張しているにも関わらず、収集したデータを広告や分析のためにサードパーティと共有する SDK を使用するアプリ。
- 認識しやすい開示のガイドラインやプライバシー ポリシーのガイドラインに違反する形で、ユーザーのインストール済みパッケージの情報を転送する SDK を含むアプリ。
  - モバイルの望ましくないソフトウェアに関するポリシーも参照してください。

個人情報と機密情報へのアクセスに関する追加要件

次の表に、特定の操作における要件を示します。

操作	要件
永続的なデバイス識別子（IMEI、IMSI、SIM のシリアル番号など）を収集またはリンクするアプリの場合	永続的なデバイス識別子を、他の個人情報と機密情報、またはリセット可能なデバイス識別子にリンクしてはなりません。ただし、以下を目的とする場合を除きます。 • SIM 識別子にリンクされた通話機能（例: 携帯通信会社アカウントにリンクされた Wi-Fi 通話機能） • デバイス所有者モードを使用するエンタープライズ デバイス管理アプリ これらの使用方法は、ユーザーデータに関するポリシー の規定に沿って、ユーザーが認識しやすいように開示する必要があります。 その他の一意の識別子については、こちらのリソース をご覧ください。 Android 広告 ID に関する追加のガイドラインについては、広告ポリシー をお読みください。
アプリが子どもを対象とする場合	アプリに含めることができる SDK は、子ども向けサービスでの使用が自己認定されているもののみです。ポリシーのすべての文言と要件については、ファミリー向け自己認定広告 SDK プログラムをご覧ください。

SDK に起因する違反の例

- Android ID や位置情報にリンクする SDK を使用するアプリ
- 広告または分析を目的として AAID を永続的なデバイス識別子に関連付ける SDK を使用するアプリ
- 分析を目的として AAID とメールアドレスを関連付ける SDK を使用するアプリ

データ セーフティ セクション

すべてのデベロッパーは、すべてのアプリについて、ユーザーデータの収集、使用、共有に関する詳細な説明を、データ セーフティ セクションに明瞭かつ正確に記載する必要があります。これには、アプリで使用されるサードパーティのライブラリまたは SDK を通じて収集、処理されるデータも含まれます。デベロッパーには、ラベルを正確に記載し、ラベルの情報を最新の状態に保つ責任があります。データ セーフティ セクションは、該当箇所において、アプリのプライバシー ポリシーで開示されている内容と一致する必要があります。

データ セーフティ セクションへの入力に関する追加情報については、こちらのヘルプセンター記事をご覧ください。

ユーザーデータに関するポリシーの全文をご覧ください。

機密情報にアクセスする権限と API に関するポリシー

機密情報にアクセスする権限や API 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、機密情報にアクセスする権限や API をリクエストできるのは、アプリで現在提供している機能やサービスの実装に必要で、それらが Google Play ストアの掲載情報に掲載されている場合に限られます。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、機密情報にアクセスする権限や API は利用できません。機密情報にアクセスする権限または API を通じてアクセスした個人情報や機密情報を販売したり、販売を促進する目的で共有したりすることは禁止されています。

機密情報にアクセスする権限と API に関するポリシーの全文をご覧ください。

SDK に起因する違反の例

- 承認されていない目的や開示されていない目的で、バックグラウンドで位置情報をリクエストする SDK を含むアプリ
- Android の read_phone_state 権限から派生した IMEI を、ユーザーの同意なく転送する SDK を含むアプリ

マルウェアに関するポリシー

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おそ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。

マルウェアに関するポリシーの全文をご覧ください。

SDK に起因する違反の例

- 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（OAuth トークンなど）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。
- 開示されていない目的のためにデバイスデータにアクセスして昇格権限を取得することにより、Android の権限モデルに違反している SDK を含むアプリ。
- 携帯電話料金の請求を通じ、ユーザーをだましてコンテンツの購入や定期購入を行わせるコードを含む SDK を使用するアプリ。

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。

モバイルの望ましくないソフトウェアに関するポリシー

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に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。

違反の例:

- 広告の不正行為
- ソーシャル エンジニアリング

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 ポリシーに準拠し、データ保護の予防措置をすべて講じる必要があります。

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

モバイルの望ましくないソフトウェアに関するポリシーの全文をご覧ください。

デバイスやネットワークでの不正行為に関するポリシー

ユーザーのデバイスやその他のデバイス、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）、サービスなど（デバイス上の他のアプリ、Google サービス、許可された携帯通信会社のネットワークを含む）を妨害、阻害、破損する、またはそれらに無断でアクセスするアプリは認められません。

アプリまたはサードパーティのコード（SDK など）でインタープリタ言語（JavaScript、Python、Lua など）が実行時に読み込まれる場合（たとえば、アプリにパッケージされていない場合）、それらが Google Play ポリシーに違反する可能性があってはなりません。

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。

デバイスやネットワークでの不正行為に関するポリシーの全文をご覧ください。

SDK に起因する違反の例

- 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。
- Google Play 以外の提供元から実行コード（dex ファイルやネイティブ コードなど）をダウンロードする SDK を含むアプリ。
- 信頼できないウェブ コンテンツ（http:// URL）、または信頼できない提供元から取得された未検証の URL（信頼できないインテントで取得された URL など）を読み込む JavaScript インターフェースが追加された WebView を含む SDK を使用するアプリ。
- APK 自体を更新するためのコードを含む SDK を使用するアプリ。
- 安全でない接続を介してファイルをダウンロードすることにより、ユーザーにセキュリティ脆弱性をもたらす SDK を含むアプリ。
- Google Play 以外の不明な提供元からアプリをダウンロードまたはインストールするコードを含む SDK を使用するアプリ。

SDK に起因する違反との関連性が高い Google Play デベロッパー ポリシー

アプリで使用しているサードパーティのコードが Google Play のデベロッパー プログラム ポリシーに準拠していることを確認するには、以下のポリシーの全文に目を通してください。

- ユーザーデータに関するポリシー
- 機密情報へのアクセスに関する権限と API
- デバイスやネットワークでの不正行為
- マルウェア
- モバイルの望ましくないソフトウェア
- ファミリー向け自己認定広告 SDK プログラム
- 広告ポリシー
- Google Play デベロッパー プログラム ポリシー

一般に問題となることが多いのは上記のポリシーですが、粗悪な SDK コードが原因で上記以外のポリシーに違反する恐れがある点も重要です。SDK がポリシーに準拠してアプリデータを扱っていることを確

認する責任はアプリ デベロッパーにあります。すべてのポリシーの全文を確認し、最新の更新について常に把握するようにしてください。

詳細につきましては、ヘルプセンターをご覧ください。

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おそれのあるすべてのコードを指します。マルウェアには、有害な可能性のあるアプリ（PHA）、バイナリ、フレームワーク変更などがあり、そのカテゴリは、トロイの木馬、フィッシング、スパイウェア アプリなどに分類されます。ただし、これらに限定されるものではなく、Google は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。これは、アプリ、バイナリ、フレームワーク変更の動作が環境に応じて変わるためです。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 プロテクトについての説明　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が含まれる場合があります。通常、バックドアは有害な可能性のある操作をデバイス上で発生させることができる方法で、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 詐欺、通話料詐欺、電話料金詐欺などがあります。

SMS 詐欺
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 詐欺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。

通話料詐欺
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。

電話料金詐欺
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。

電話料金詐欺には、有料の SMS 詐欺や通話料詐欺を除く、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

モニタリング目的で、デバイス上の個人情報や機密性の高いユーザーデータを収集して第三者（企業または特定の個人）に送信するコード。

アプリは、ユーザーデータに関するポリシー　に定められているとおり、認識しやすい開示を適切に行いユーザーの同意を得る必要があります。

モニタリング アプリに関するガイドライン

モニタリング アプリとして承認を受けるためには、特定の個人のモニタリング（保護者による子供のモニタリングなど）や企業管理（従業員のモニタリング）のみを目的として設計、販売しており、以下に示す要件を完全に満たしている必要があります。これらのアプリを、目的以外の人（たとえば配偶者）の追跡に使用することはできません。永続的な通知が表示されるかどうかに関係なく、たとえ追跡される人がそのことを認識し許可している場合でも使用できません。これらのアプリは、マニフェスト ファイルで IsMonitoringTool メタデータ フラグを使用して、モニタリング アプリであることを適切に表明する必要があります。

モニタリング アプリは、最低限、以下の要件を満たす必要があります。

- 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。
- アプリの実行中は常に永続的な通知を表示し、アプリを明確に識別できる固有のアイコンを示す必要があります。
- モニタリング機能または追跡機能について Google Play ストアのアプリの掲載情報で開示する必要があります。
- アプリや Google Play のアプリ掲載情報では、利用規約に違反する機能（Google Play 以外でホストされていてポリシーを遵守していない APK へのリンクなど）を有効にする手段や、そうした機能にアクセスする手段を提供してはなりません。
- 適用されるすべての法律を遵守する必要があります。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。

詳しくは、ヘルプセンター記事 IsMonitoringTool フラグの使用　をご覧ください。

サービス拒否攻撃（DoS）

ユーザーが気付かないうちにサービス拒否攻撃（DoS）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る）。

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であ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おそ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請求情報を要求して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、昇格させた権限の取得、セキュリティ関連のコア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わせるコード。

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全部を制御不能にし、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の実行を要求するコード。

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していれば、ランサムウェアのカテゴリ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、悪意のあるものとないものがあります。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、ユーザーへの開示なく、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る場合があります。

- 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、音声や通話音声の録音、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

一見すると無害だが（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なる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は、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 マルウェアと分類されます。

ただし、アプリが任意のコード実行を許可しており、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。

なりすまし

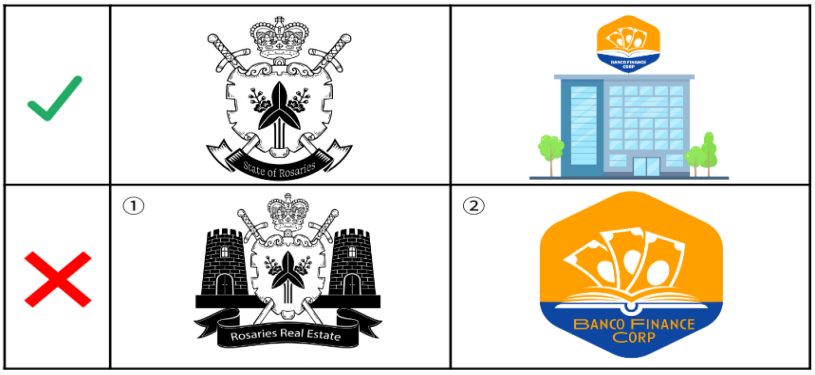
他者（別のデベロッパー、会社、組織など）または別のアプリになりまして、ユーザーを誤解させるようなアプリは認められません。アプリが無関係の誰かに関係がある、または承認されているとほのめかしてはなりません。アプリのアイコン、説明、タイトル、アプリ内要素についても、他者や他のアプリとの関係を誤解させるようなものは使用しないようご注意ください。

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。

- 別の会社 / デベロッパー / 法人 / 組織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。

- 別の会社 / デベロッパー / 法人 / 組織に関係があるかのような虚偽をほのめかすアイコンやタイトルを使用しているアプリ。



①このアプリは国章を使用して、政府と関係があるアプリだとユーザーに誤認させています。
②このアプリは特定の企業のロゴをコピーして、その企業の公式アプリであるかのような虚偽を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。

①このアプリは、有名な暗号通貨ウェブサイトのロゴをアプリアイコンに使用して、公式ウェブサイトであるかのようにほのめかしています。
②このアプリは、人気テレビ番組のキャラクターとタイトルをコピーして、テレビ番組と関係があるとユーザーに誤認させています。

- 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。「Justin Bieber Official」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。
- Android ブランドの取り扱いガイドライン　に違反しているアプリ。

Mobile Unwanted Software

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、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。
- ユーザーが気付かな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に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のめかしてはなりません。

違反の例:

- 広告の不正行為
- ソーシャル エンジニアリング

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

悪意のあるダウンローダ

モバイルの望ましくないソフトウェア（MUwS）をダウンロードするコード（コード自体は望ましくないソフトウェア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。

- MUwS 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 MUwS 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 MUwS 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 MUwS 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。
- すべてのソフトウェアの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。

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。

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。

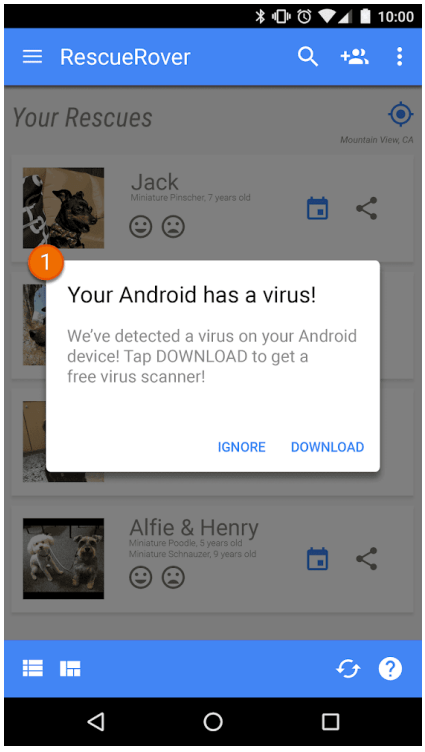
- ユーザーに表示されない広告を掲載するアプリ。
- ユーザーの意図に反して広告のクリックを自動的に生成する、またはクリック件数を不正に付与できるネットワーク トラフィックを生成するアプリ。
- インストール アトリビューション クリックを偽造して送信し、送信元のネットワークからではないインストールに対して報酬を得るアプリ。
- ユーザーがアプリ インターフェース内にいないときに広告をポップアップ表示するアプリ。
- アプリによる広告枠の虚偽の表示や表明。たとえば、実際には Android デバイスで実行されているのに iOS デバイスで実行されていると広告ネットワークに通知するアプリや、収益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

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。

- 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。

広告に関するその他の例については、広告ポリシーの説明をご覧ください。

Social Engineering

We do not allow apps that pretend to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

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に準拠している必要があります。賭博行為の広告に関するポリシーは、こちらをクリックしてご覧ください。

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 で提供するアプリのダウンロードに課金する場合は、それらの取引の支払い方法として Google Play の課金システムを使用しなければなりません。
2. Google Play で配信しているアプリにおいて、アプリ内の機能やサービスへのアクセス（すべてのアプリ機能、デジタル コンテンツ、デジタル商品を含み、「アプリ内購入」と総称する）に対する支払いを必要とする、または受け付けている場合は、第 3 項または第 8 項に該当する場合を除き、それらの取引には Google Play の課金システムを使用する必要があります。

   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、サービスのアップグレード、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）

3. 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。
   a. 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）に関する支払い
   b. 個人間送金、オンライン オークション、非課税寄付に関する支払い
   c. 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
   d. 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

      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 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。

4. 第 3 項および第 8 項に記載の条件に該当する場合を除き、アプリは 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、アプリ内ユーザー インターフェース フローで、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

5. アプリ内仮想通貨の使用は、その通貨を購入したアプリまたはゲーム内のみに限定しなければなりません。

6. デベロッパーは、購入対象となるアプリ、アプリ内機能および定期購入の利用規約や価格について、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、Play 請求サービスのユーザー 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。Google Play でのプロダクトの説明をする中で、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言及する場合、アプリの掲載情報に、その機能の利用には支払いが必要と明記する必要があります。

7. 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。

8. 第 3 項に記載の条件に該当する場合を除き、スマートフォンおよびタブレット向けに Google Play で配信しているアプリで、インドおよび / または韓国のユーザーからのアプリ内購入に対する支払いを必要とする、または受け付けている場合は、デベロッパーとして各プログラムの課金システムの申告フォーム（インド、韓国）の提出を完了し、それに含まれている追加規約とプログラム要件に同意することにより、それらの取引に Google Play の課金システムに加えて代替の課金システムを提供することができます。

注: このポリシーに関するスケジュールやよくある質問については、ヘルプセンターをご覧ください。

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およびそれに関連付けられているオファーは、アプリの一部と見なされます。アプリに表示される広告は、Google Play のすべてのポリシーを遵守する必要があります。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の利用を広告配信にも適用するアプリは、個人情報や機密情報に関するポリシーの適用を受けるとともに、以下の要件も遵守する必要があります。

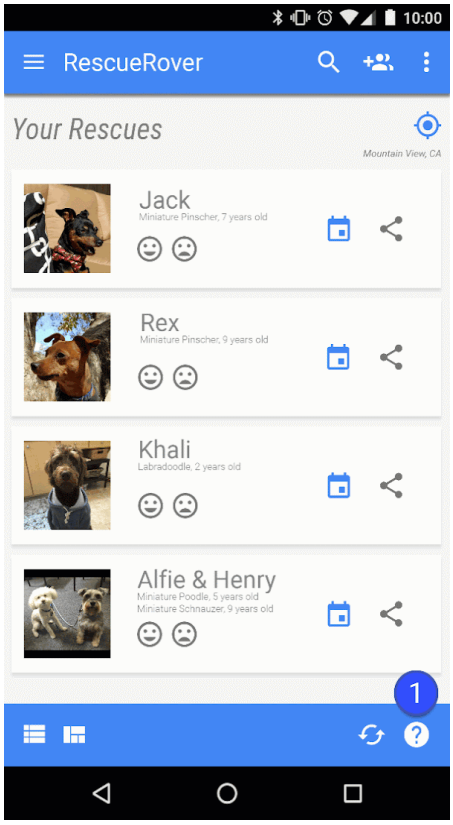
- 権限に基づくデバイスの位置情報を広告目的で利用または収集する旨をユーザーに対して明確にし、アプリに義務づけられているプライバシー ポリシーに明記する必要があります。これには位置情報の使用について定めている該当する広告ネットワークのプライバシー ポリシーがあればそれにリンクすることも含まれます。
- 位置情報の利用許可に関する要件に従い、位置情報の利用許可は、アプリ内で現在提供している機能やサービスを実装するためにのみリクエストでき、広告利用のみを目的としてデバイスの位置情報の利用許可をリクエストすることは認められません。

虚偽の広告

オペレーティング システムからの通知や警告など、アプリの機能のユーザー インターフェース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。

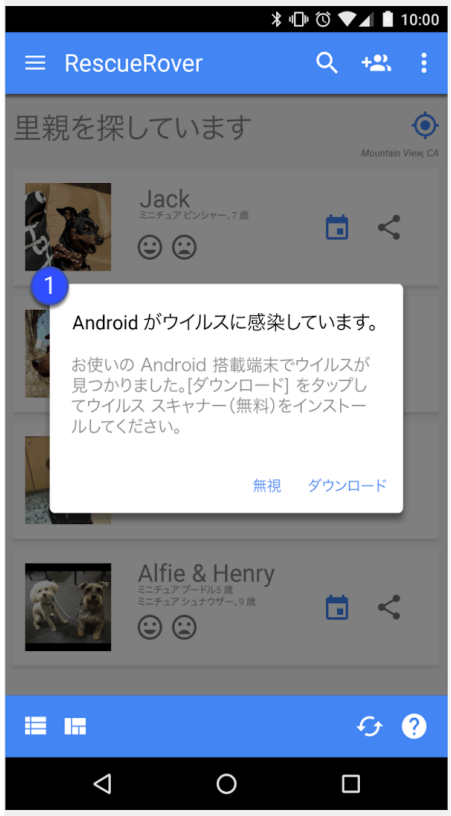
Google Play をこれからも信頼できる安全なプラットフォームとしてご利用いただけるようにするため、ユーザーにとって有害または不適切なコンテンツを定義し、禁止する基準を作成しました。

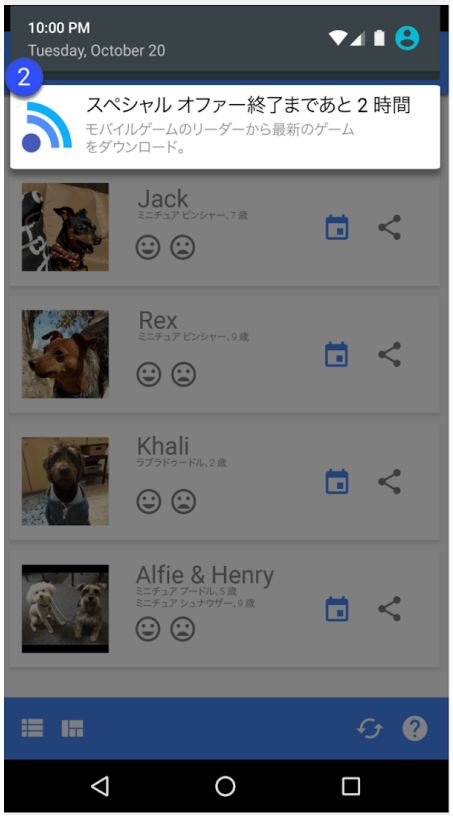
- アプリのユーザー インターフェースを装う広告:



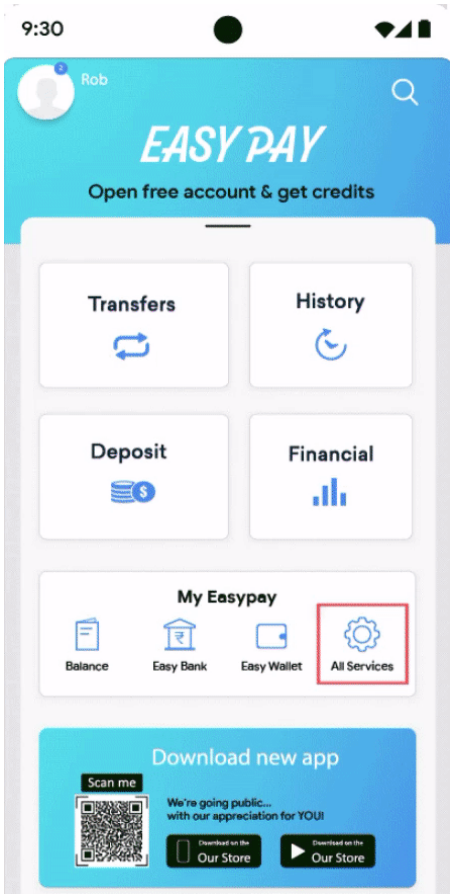
① このアプリの疑問符アイコンは、外部のリンク先ページにユーザーを移動させる広告です。

- システム通知を装う広告:





① ② 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。



① さまざまな機能を装いつつ、実際にはユーザーを広告に誘導するだけの機能セクションの例を上記に示します。

ロック画面の収益化

アプリの唯一の目的がロック画面で機能することである場合を除き、ロック中のデバイスのディスプレイを収益化する広告や機能をアプリが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る広告であり、意図しないクリックや、デバイス機能のユーザビリティを損ねるまたは妨げることにつながる恐れがあります。

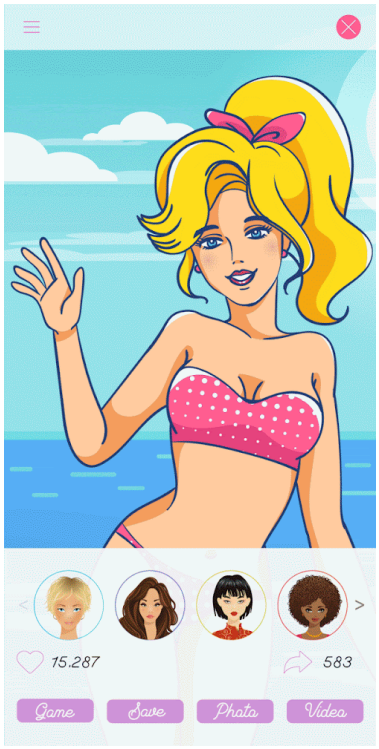
アプリの全機能の利用と引き換えに広告のクリックや個人情報の提供をユーザーに強制することはできません。インタースティシャル広告は、その広告を配信するアプリ内でのみ表示できます。アプリの通常の利用を妨げるようなインタースティシャル広告などを表示する場合、そういった広告は無条件で簡単に閉じられるようにする必要があります。

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。

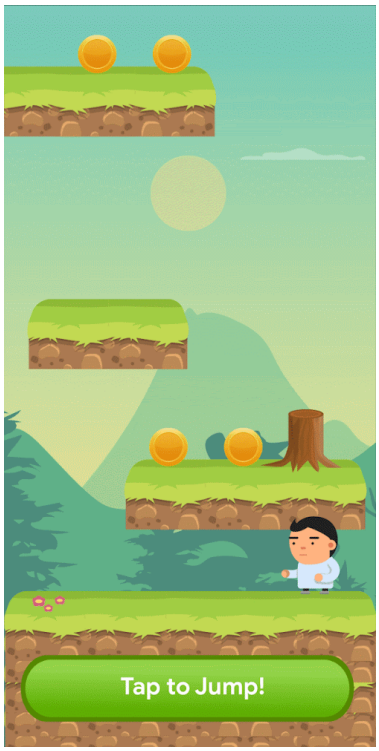
- 画面全体に表示されて画面を占拠するか通常の使用を妨げ、非表示にする明確な手段を提供しない広告:

① この種の広告には非表示にす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



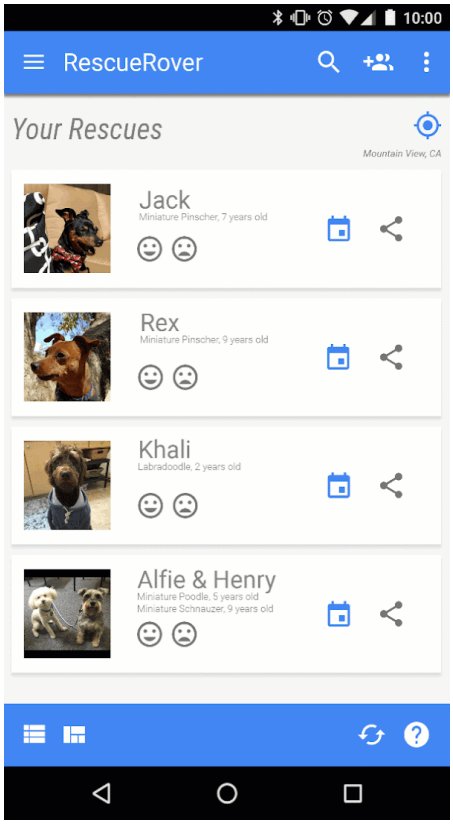
ユーザーがアプリ内の機能を使用するために通常タップする領域に突然表示される広告

アプリ、サードパーティの広告、またはデバイスの機能の妨害

アプリに関連付けられた広告が、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）を妨げてはなりません。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。

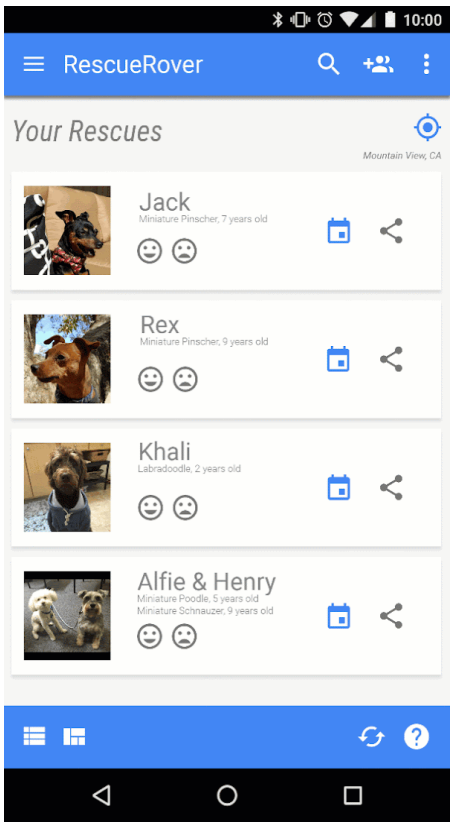
Google Play をこれからも信頼できる安全なプラットフォームとしてご利用いただけるようにするため、ユーザーにとって有害または不適切なコンテンツを定義し、禁止する基準を作成しました。

- 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:

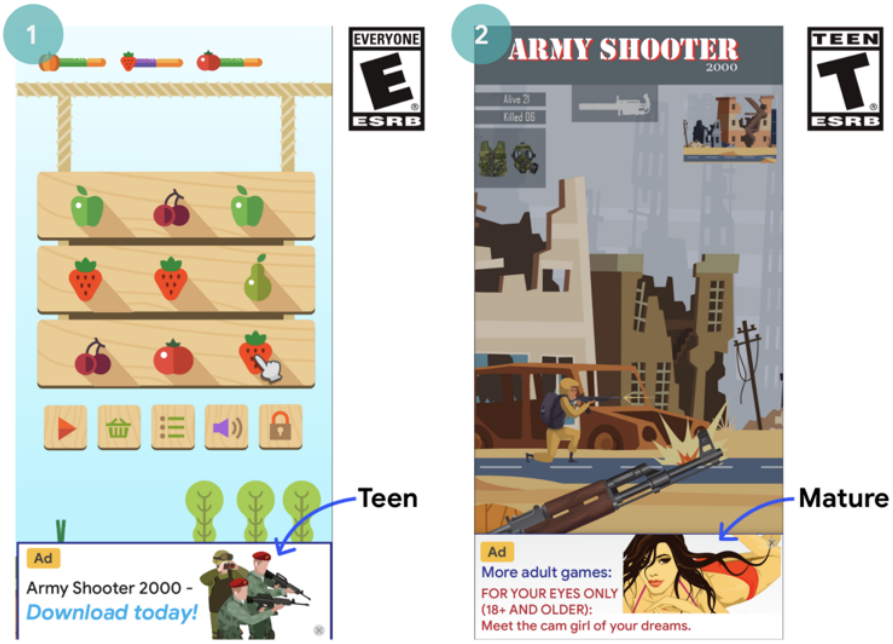


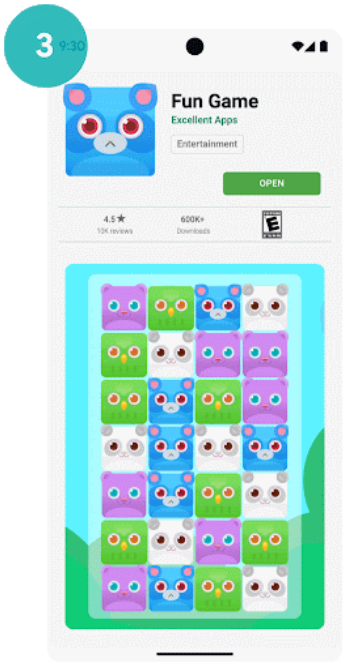
説明: ユーザーがアプリを終了してホーム画面に移動しようとしたところを広告が妨げています。

不適切な広告

アプリ内に表示される広告およびそれに関連付けられているオファー（広告が別のアプリのダウンロードを宣伝している場合など）は、アプリのコンテンツのレーティング　に適したものでなければなりません。コンテンツ自体が Google Play のポリシーを遵守している場合も同様です。

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。





① この広告（13 歳以上）はアプリのコンテンツのレーティング（全ユーザー対象）に対し不適切です
② この広告（成人向け）はアプリのコンテンツのレーティング（13 歳以上）に対し不適切です
③ この広告のオファー（成人向けアプリのダウンロード）は、広告が表示されたゲームアプリのコンテンツのレーティング（全ユーザー対象）に対し不適切です

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 [広告のカスタマ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、広告目的で永続的なデバイス識別子（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 を、分析目的で、個人を特定できる情報または永続的なデバイス識別子（SSAID、MAC アドレス、IMEI など）に関連付けることはできません。永続的なデバイス識別子に関するその他のガイドラインについては、ユーザーデータに関するポリシー をお読みください。
- **ユーザーの選択の尊重**。
  - 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。
  - 最近のデバイスでは、ユーザーが Android 広告 ID を削除すると、その ID は消去されます。消去された ID にアクセスしようとすると、ゼロからなる文字列が返されます。広告 ID がないデバイスは、以前の広告 ID にリンクされているデータまたは以前の広告 ID から取得されたデータに関連付けてはなりません。
- **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通知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詳しくは、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、Google Play デベロッパー プログラム ポリシー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識別子に取って代わるものです。

質の高い広告エクスペリエンス

デベロッパーは、Google Play アプリを使用するユーザーに質の高い体験を提供するために、広告に関する以下のガイドラインを遵守する必要があります。広告が次のような予期しない方法でユーザーに表示されることは認められません。

- 一般にユーザーがなんらかの操作を選択したときに突然表示される、あらゆるフォーマット（動画、GIF、静止画像など）の全画面インタースティシャル広告は認められません。
  - ゲームをプレイ中、レベルの冒頭やコンテンツ セグメントの開始中に表示される広告は認められません。
  - アプリの読み込み画面（スプラッシュ画面）の前に表示される全画面動画インタースティシャル広告は認められません。
- 15 秒経過後に閉じることができない全画面インタースティシャル広告は認められません。オプトインの全画面インタースティシャル、またはユーザーのアクションを妨げない全画面インタースティシャル（ゲームアプリのスコア画面の後に表示される場合など）は、15 秒以上表示することが可能です。

このポリシーは、ユーザーが明示的にオプトインするリワード広告（例: 広告を視聴したユーザーには特定のゲーム内機能やコンテンツを提供することをデベロッパーが明示している広告）には適用されません。また、通常のアプリの使用やゲームのプレイを妨げない収益化要素や広告（動画コンテンツに組み込まれた広告、全画面表示ではないバナー広告など）にも適用されません。

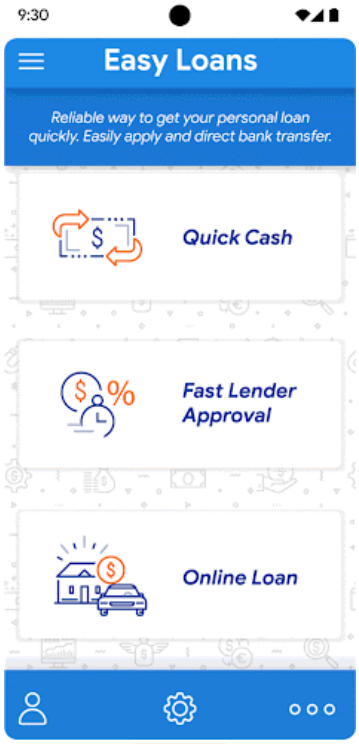
これらのガイドラインは、Better Ads Standards - Mobile Apps Experiences のガイドラインを参考にしています。Better Ads Standards について詳しくは、Coalition of Better Ads のページをご覧くださ

い。

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。

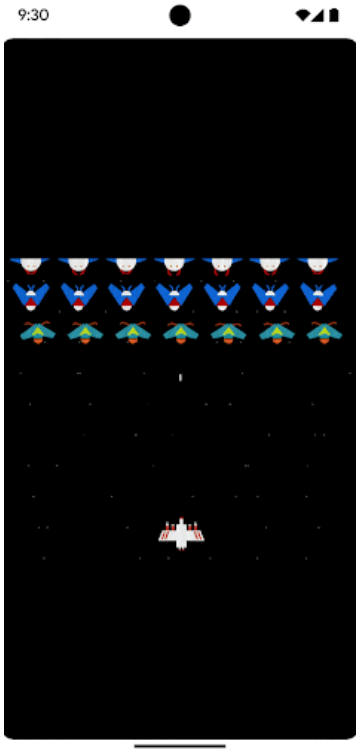
- ゲームのプレイ中やコンテンツ セグメントの開始中（例: ユーザーがボタンをクリックした後、このボタンクリックにより意図されるアクションが有効になる前）に突然表示される広告。このような広告は、ゲームが始まったりコンテンツを使用したりするつもりでいるユーザーにとって予期しないものです。

① ゲームのプレイ中、レベルの冒頭に静的広告が突然表示される。



② コンテンツ セグメントの開始中に動画広告が突然表示される。

- ゲームのプレイ中に表示され、15 秒経過しても閉じることができない全画面広告。



① インタースティシャル広告がゲームのプレイ中に表示され、15 秒以内にスキップするオプションがユーザーに提供されない。

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。ユーザーをだまして購入させたり、言葉巧みに購入させたりするアプリは認められません（これにはアプリ内購入や定期購入も含まれます）。

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。

定期購入では、その有効期間を通じて持続的または繰り返し利用可能な価値を提供する必要があり、効果が 1 回限りの特典（たとえば、アプリ内クレジット / 通貨を一括で提供する SKU、1 回しか使用できないゲーム内ブースターなど）を提供するために定期購入を使用することはできません。定期購入において、動機付けやプロモーションを目的としてボーナスを提供することは可能ですが、定期購入の有効期間を通じて提供する持続的または繰り返し利用可能な価値を補完するものでなければなりません。持続的または繰り返し利用可能な価値を提供しないアイテムは、定期購入アイテムではなくアプリ内アイテムとして提供する必要があります。

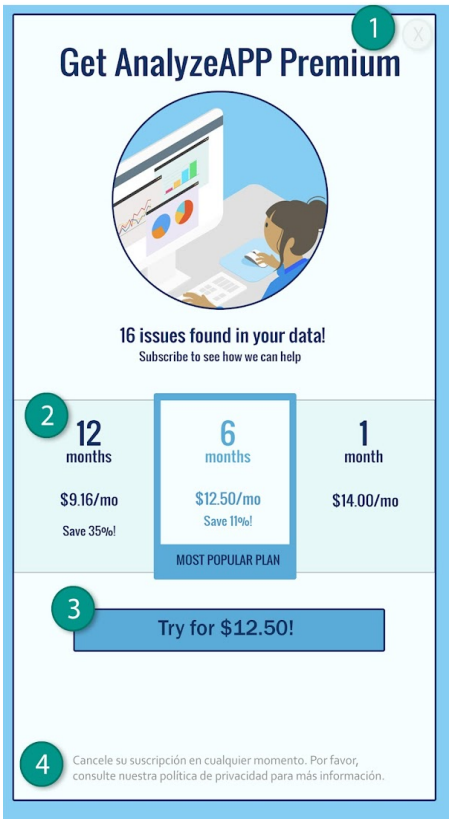
1 回限りの特典を定期購入と偽装したり、ユーザーが定期購入と誤認するような方法で提示したりすることはできません。これには、ユーザーが定期購入した後に、定期購入を 1 回限りの特典に変更する行為（たとえば、繰り返し利用できる価値を取り消し、廃止、最小化することなど）も含まれます。

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。

- 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」、「有料会員を 3 日間無料お試し」などと記載されているのに請求が繰り返し自動発生する）。
- 購入フローが複数の画面に分かれており、ユーザーが誤って定期購入ボタンをクリックしてしまう恐れがある。
- 定期購入において、持続的または繰り返し利用可能な価値を提供していない（たとえば、最初の月は 1,000 ジェムを提供するのに、次の月からは定期購入を継続していても 1 ジェムずつしか提供しない場合）。
- 定期購入を自動更新するためにはユーザーが登録して 1 回限りの特典を受け取る必要があり、購入後にユーザーからのリクエストがなければ定期購入が解約される。

例 1:



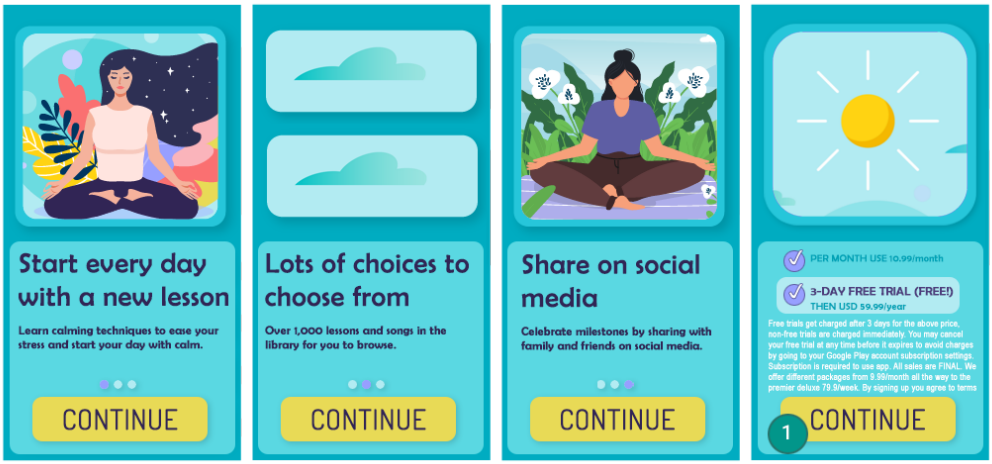
① 閉じるボタンがはっきり表示されておらず、機能を利用するには定期購入しなければならないとユーザーが誤解する恐れがあります。

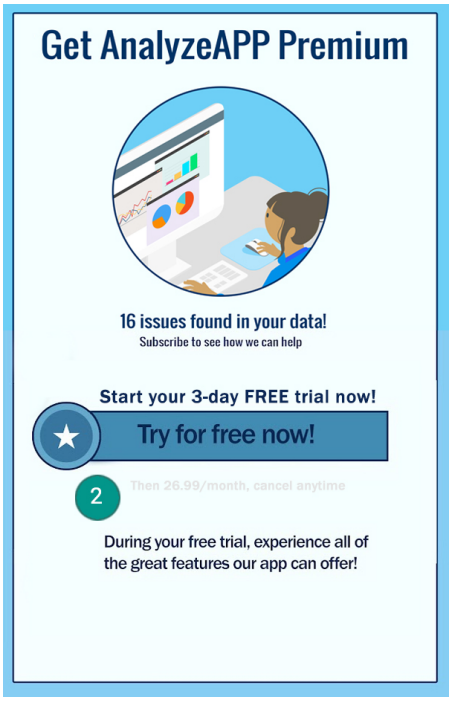
② 月単位の料金しか示されておらず、定期購入する際に 6 か月分の料金が請求されることをユーザーが認識できない恐れがあります。

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。

例 2:





① 同じボタン領域を繰り返しクリックする仕組みになっているため、ユーザーが最後の [CONTINUE（続行）] ボタンをうっかりクリックし、意に反して定期購入してしまう恐れがあります。

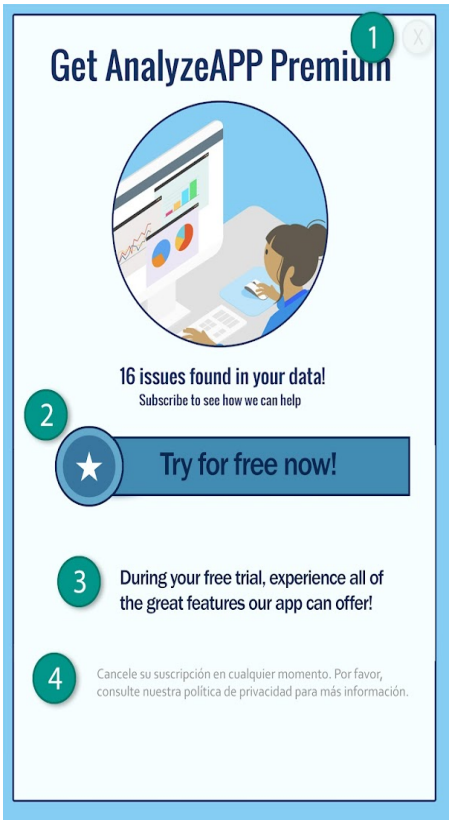
② お試し期間終了後の請求額が目立たないように記載されているため、ユーザーが無料プランだと勘違いする恐れがあります。

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。

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。

- 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いないため、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いるため、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いないため、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、解約、払い戻し

アプリで定期購入アイテムを販売する場合、ユーザーが定期購入を管理または解約する方法を明確に開示しなければなりません。また、定期購入をオンラインで簡単に解約できる手段にアプリ内からアクセスできるようにすることも必要です。この要件を満たすには、アプリのアカウント設定（または同等のページ）に次の項目を追加します。

- Google Play の定期購入センターへのリンク（Google Play の課金システムを使用するアプリの場合）
- 解約手続きに直接アクセスできるリンク

Google Play の課金システムから行った定期購入をユーザーが解約する場合、解約日にかかわらず、ユーザーは原則として現在の請求期間についての払い戻しは受けられませんが、請求期間の残りの期間中、該当するコンテンツを引き続き受け取れます。ユーザーの解約が有効になるのは、現在の請求対象期間が終了した後です。

コンテンツ プロバイダまたはアクセス プロバイダは、ユーザーに対して直接、より柔軟な払い戻しポリシーを実施することもできます。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。

ファミリー向けプログラム用の自己認定広告 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、ファミリー向け自己認定広告 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、子供には（年齢詐称を予防する年齢確認を使用するなどの手段により）これらの自己認定広告 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。

自己認定広告 SDK を含め、アプリで実装する SDK の全バージョンが、適用されるすべてのポリシー、現地の法律および規制を遵守していることを保証する責任はデベロッパーにあります。Google は、広告 SDK が自己認定手続きにおいて提供する情報の正確性に関する表明や保証を一切行いません。

ファミリー向け自己認定広告 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 に準拠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）

ファミリー向け自己認定広告 SDK 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 Google Play デベロッパー プログラム ポリシーに準拠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。
- パブリッシャー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。
- Google Play のファミリー向け広告と収益化ポリシー に準拠し、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、パブリッシャー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ダーに反映されていることを確認すること。
- 広告 SDK のポリシーがすべての自己認定要件に準拠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の情報など）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（広告 SDK バージョンがすべての自己認定要件に準拠していることを検証できるよう新しいバージョンのリリースを送信する、テストアプリを提供するなど）。
- 新しいバージョンのすべてのリリースが、ファミリー ポリシー要件を含む、最新の Google Play デベロッパー プログラム ポリシーに準拠していると自己認定 すること。

注: ファミリー向け自己認定広告 SDK は、パブリッシャー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。

広告クリエイティブの透かしやテストアプリの提供について詳しくは、こちら をご覧ください。

子供に広告を配信する際の、配信プラットフォームのメディエーションの要件は次のとおりです。

- ファミリー向け自己認定広告 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に準拠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。

ファミリー向け自己認定広告 SDK の一覧についてはこちら 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（広告など）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。広告などによるプロモーションが Google Play のデベロッパー プログラム ポリシーに違反する場合、虚偽、または有害なプロモーションとみなされます。

一般的な違反の例:

- ウェブサイト、アプリ、またはその他のプロパティに虚偽 の広告（システムの通知やアラートに似た通知を含む）を掲載する。
- 露骨な性的表現を含む 広告を使用して、アプリをダウンロードさせるためにユーザーをアプリの Google Play 掲載情報に誘導する。
- 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 サービスを通じて未承諾のプロモーションを行う。

デベロッパーは自身の責任において、アプリと関連付けた広告ネットワーク、アフィリエイト、広告がこのポリシーを遵守していることを確認してください。

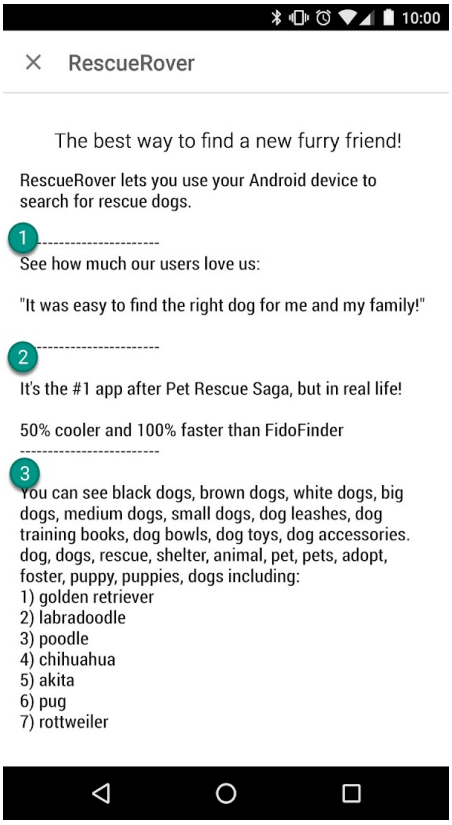
メタデータ

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、過多なメタデータ、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、アプリについて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。

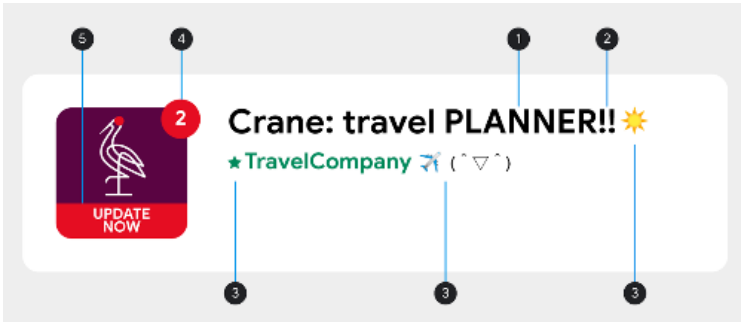
アプリのタイトル、アイコン、デベロッパー名は、ユーザーがアプリを見つけて詳細を確認するうえで特に役立ちます。これらのメタデータ要素では、絵文字、顔文字、または特殊文字の繰り返しを使用しないでください。ブランド名の一部でない限り、すべて大文字の表記は避けてください。アプリアイコンに誤解を招く記号を使用することは許可されません。たとえば、新しいメッセージがない場合に新規メッセージのドット インジケーターを表示したり、アプリがコンテンツのダウンロードと無関係な場合にダウンロード / インストール記号を表示したりしてはなりません。アプリのタイトルは 30 文字以内にしてください。

ここに記載の要件に加えて、特定の Google Play デベロッパー ポリシーにより、追加のメタデータ情報の提供が必要となる場合があります。

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。



① 出典不明または匿名のユーザーからの賞賛や推薦の言葉
② アプリまたは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



① すべて大文字（ブランド名の一部である場合を除く）
② アプリに関係しない連続した特殊文字
③ 絵文字、顔文字、特殊文字の使用
④ 誤解を招く記号
⑤ 誤解を招くテキスト

ストアの掲載情報での不適切なテキスト、画像、動画の例を次に示します。

- 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をなど、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。

以下に、おすすめの方法を紹介します。

- 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。
- スト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。

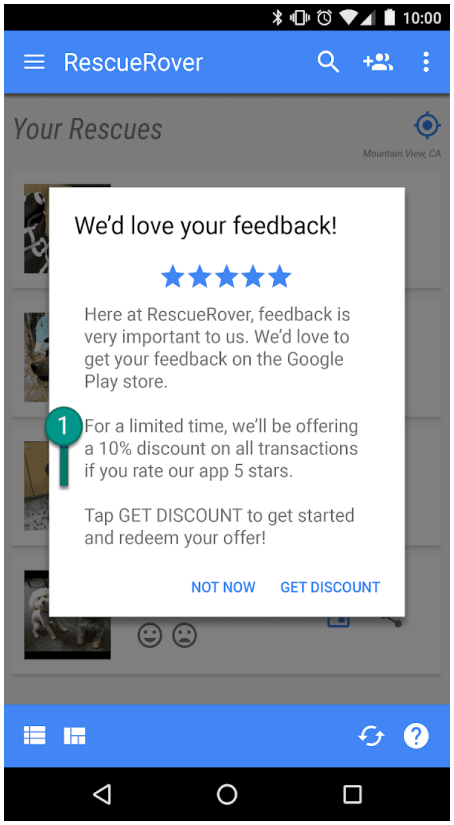
ユーザーの評価、レビュー、インストール

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。報酬付きのインストール、レビュー、評価には、アプリのタイトル、アイコン、デベロッパー名において価格や他のプロモーション情報を示すテキストまたは画像を使用することも含まれます。

デベロッパーは、アプリのタイトル、アイコン、デベロッパー名に、ストアのパフォーマンスまたはランキングを示すテキストまたは画像、既存の Google Play プログラムとの関連を示唆するテキストまたは画像を追加してはなりません。

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。

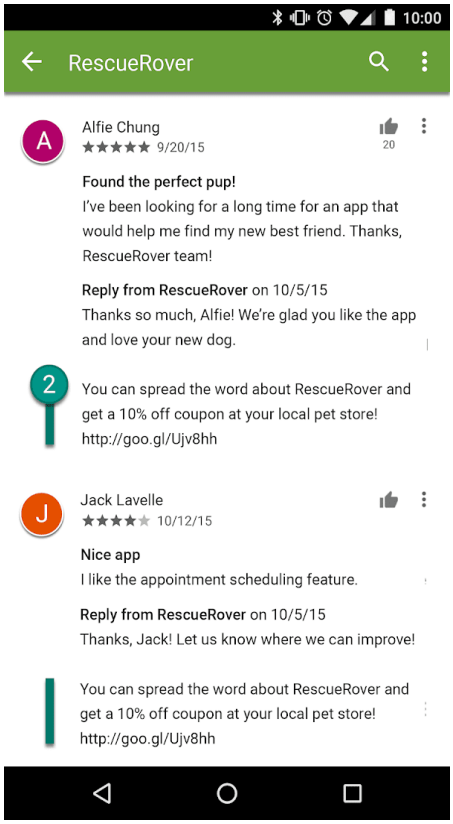
- 報酬付きでアプリの評価をユーザーに依頼する。



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。



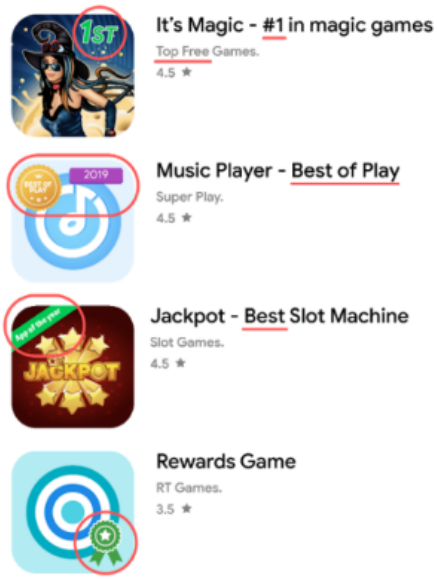
② このレビューでは、クーポンを提供して、RescueRover アプリを宣伝するようにユーザーに奨励しています。

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。

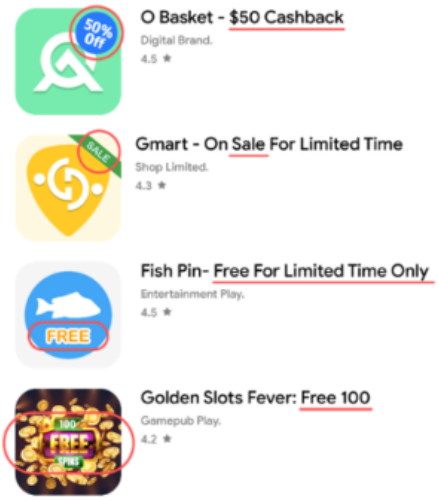
- ユーザーから指摘された問題に的を絞って返信しましょう。高く評価するようユーザーに求めてはなりません。
- サポート アドレスやよくある質問のページなど、参考となるリソースへの参照は記載できます。

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。

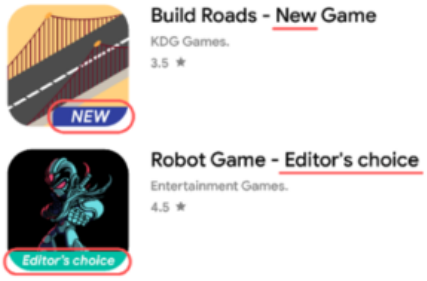
- ストアのパフォーマンスまたはランキングを示す画像またはテキスト（「App of the Year」、「No.1」、「20XX 年のベストオブ Play」、「人気」、受賞アイコンなど）



- 価格、プロモーションの情報を示す画像またはテキスト（「10% オフ」、「$50 キャッシュバック」、「期間限定で無料」など）



- Google Play プログラムを示す画像またはテキスト（「エディターのおすすめ」、「新着」など）



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　　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は、特定のアプリについて、不快感を与える可能性のあるコンテンツがそのアプリに含まれていることをユーザー（特に保護者）に知らせるために使用いたします。また、法律の規定に沿って特定の地域やユーザーに対してアプリのコンテンツを除外またはブロックしたり、アプリが特別なデベロッパー プログラムの対象となるかどうかを判断したりする際にも、コンテンツのレーティングが利用されます。

コンテンツのレーティングはどのように割り当てられるか

コンテンツのレーティングを取得するには、アプリのコンテンツの性質について、Play Console でレーティング質問票　に回答します。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を偽った場合は、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するには、Google Play で現在配信されているすべてのアプリだけでなく、新たに Play Console に送信するアプリに関してもそれぞれ、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。コンテンツのレーティングが割り当てられていないアプリは Play ストアから削除されます。

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に変更を加えた場合は、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。

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　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を行うことができます。

ニュース

ニュースアプリとは、以下のいずれかに該当するアプリです。

- Google Play Console で「ニュース」アプリとして申告している。
- Google Play ストアで「ニュース＆雑誌」カテゴリに掲載されており、アプリのタイトル、アイコン、デベロッパー名、または説明文で「ニュース」に関するアプリであることが示されている。

たとえば、「ニュース＆雑誌」カテゴリ内の以下のようなアプリはニュースアプリと判断されます。

- アプリの説明文で「ニュース」に関するアプリであることが示されている（以下のような記載を含みますが、これらに限定されません）。
  - 最新のニュース
  - 新聞
  - 速報
  - ローカル ニュース
  - 今日のニュース
- アプリのタイトル、アイコン、またはデベロッパー名に「ニュース」という言葉が含まれている。

ただし、ユーザー作成コンテンツがメインとなるアプリ（たとえばソーシャル メディア アプリ）は、ニュースアプリとして申告すべきではなく、ニュースアプリと判断されることもありません。

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アプリ内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:

- アプリとニュース記事の提供元に関する所有権情報を提供すること（これには、各記事の配信元や執筆者が含まれますが、これらに限定されません）。記事の個別の執筆者を記載する慣習がない場合は、ニュースアプリ自体を記事の配信元とする必要があります。なお、ソーシャル メディア アカウントへのリンクは、執筆者や配信元の情報の形式としては十分ではありません。
- 連絡先情報が記載されていることを目立つように明示した、専用のウェブサイトまたはアプリ内ページを見つけやすい場所に設けて（たとえば、ホームページの下部やサイトのナビゲーション バーにリンクを設置する）、ニュース メディアの有効な連絡先情報（連絡先のメールアドレスまたは電話番号のいずれか）を提供すること。なお、ソーシャル メディア アカウントへのリンクは、ニュースメディアの連絡先情報の形式としては十分ではありません。

ニュースアプリの禁止条項:

- 誤字、脱字、文法の著しい誤りがある
- 静的コンテンツ（3 か月以上前のコンテンツなど）のみである
- 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している

なお、ニュースアプリが商品やサービスの販売または広告収益の獲得を主な目的としていない限り、そのアプリで広告を配信したり、その他の形式のマーケティングを実施したりすることは可能です。

さまざまな提供元のコンテンツを集約するニュースアプリは、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。

必要な情報を提供する最適な方法については、こちらの記事をご確認ください　。

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できる必要があります。クラッシュするアプリ、その他機能的とはいえない動作を示すアプリ、あるいはユーザーまたは Google Play に対するスパム行為を行うだけのアプリは、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

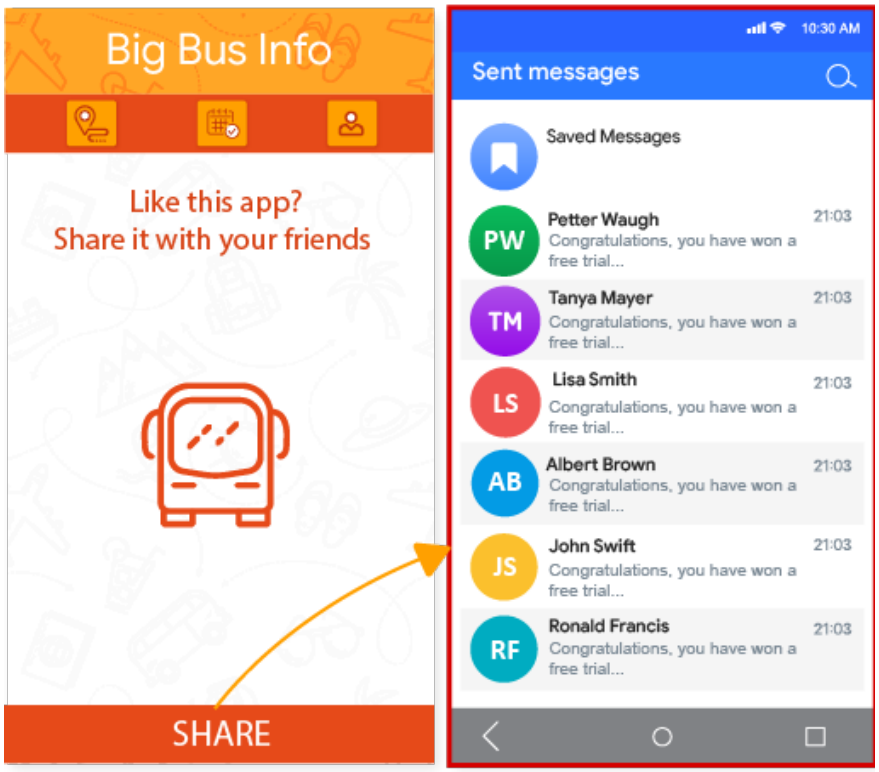
ユーザーに迷惑メールを送信するアプリや、別のアプリを複製したアプリ、低品質のアプリなど、ユーザーや Google Play に対してスパム行為を働くアプリは認められません。

メッセージ スパム

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。

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。

- ユーザーが [共有] ボタンを押すと、このアプリがユーザーに代わってメッセージを送信します。その際、内容や送信先をユーザーが確認することはできません。

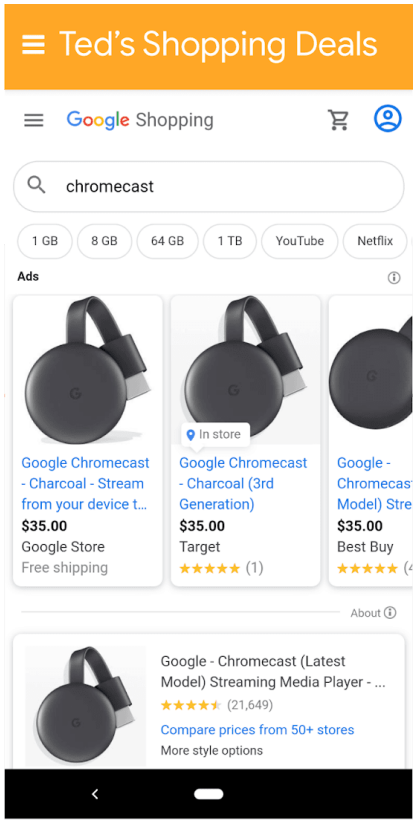


ウェブ表示スパムやアフィリエイト スパム

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。

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。

- 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の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ウェブ表示を提供することを主な目的とするアプリ:



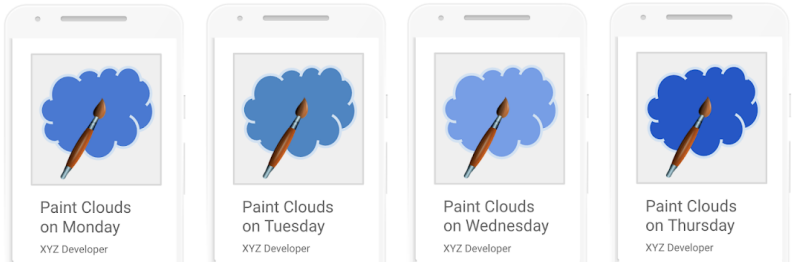
① 「Ted's Shopping Deals」というこのアプリには、Google ショッピングのウェブサイトを表示する機能しかありません。

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。

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。

- 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。
- 機能、コンテンツ、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。

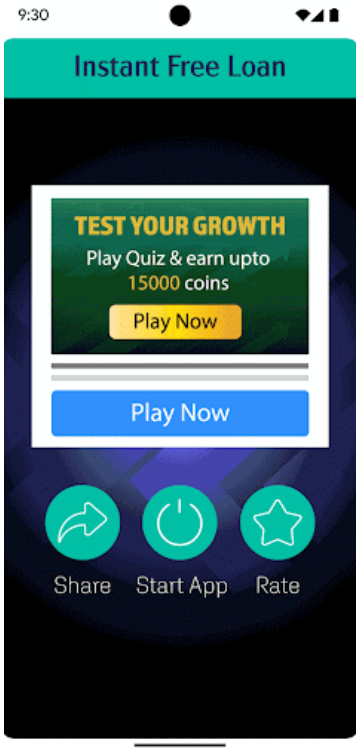


広告目的

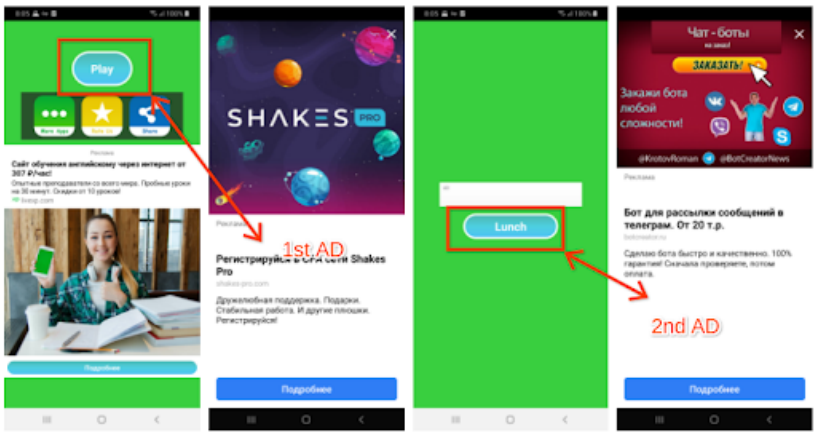
インタースティシャル広告を繰り返し表示することで、ユーザーがアプリを操作したりアプリ内タスクを実行したりするのを妨げるアプリは認められません。

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。

- ユーザーがなんらかの操作（クリック、スワイプなど）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。



最初のアプリ内ページに、操作用のボタンが複数用意されています。ユーザーがアプリを使用するために [**Start App**] をクリックすると、インタースティシャル広告がポップアップ表示されます。この広告が閉じた後、ユーザーはアプリに戻ってサービスを使用するため [**Service**] をクリックしますが、別のインタースティシャル広告が表示されます。



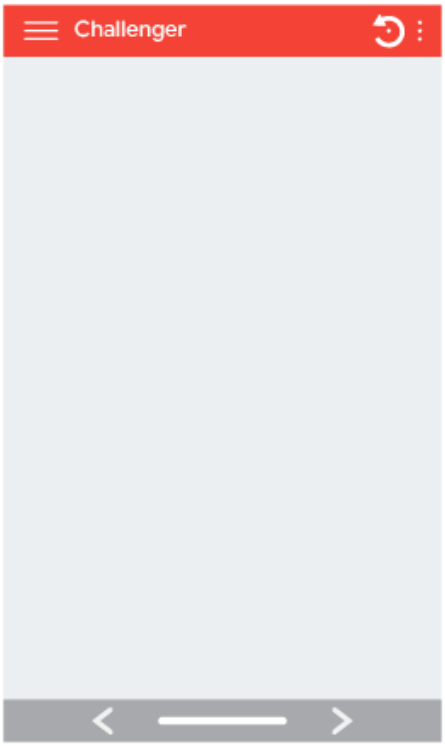
ユーザーは最初のページで、アプリで使用できる唯一のボタンである [**Play**] をクリックするよう誘導されます。ユーザーがクリックすると、インタースティシャル広告が表示されます。この広告が閉じた後、ユーザーは唯一操作できる [**Launch**] ボタンをクリックします。すると、別のインタースティシャル広告がポップアップ表示されます。

最低限の機能

ユーザーの興味を引き、操作に反応し、安定して動作するアプリにしてください。

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。

- 何もしない、または何の機能も提供しないアプリ



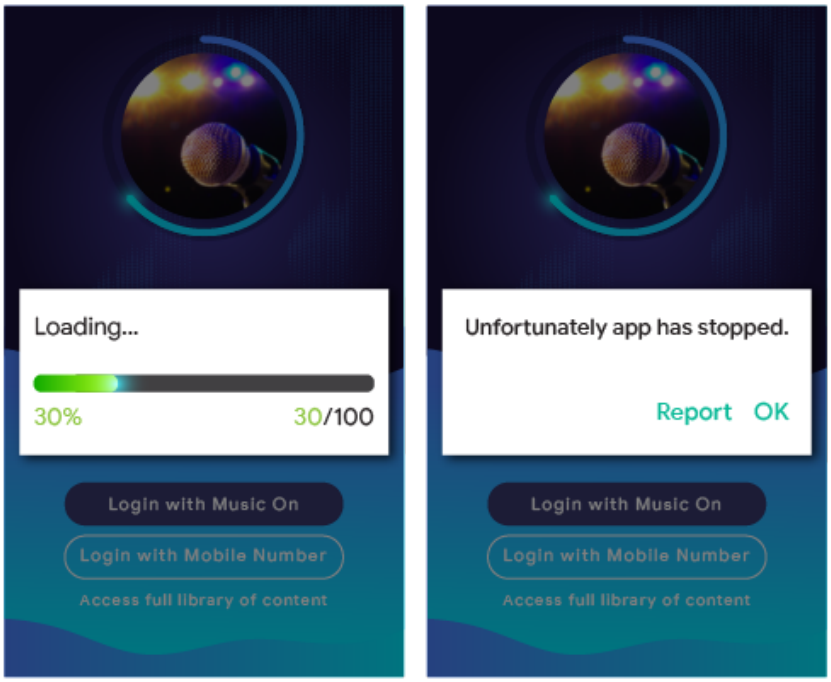
不完全な機能

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。

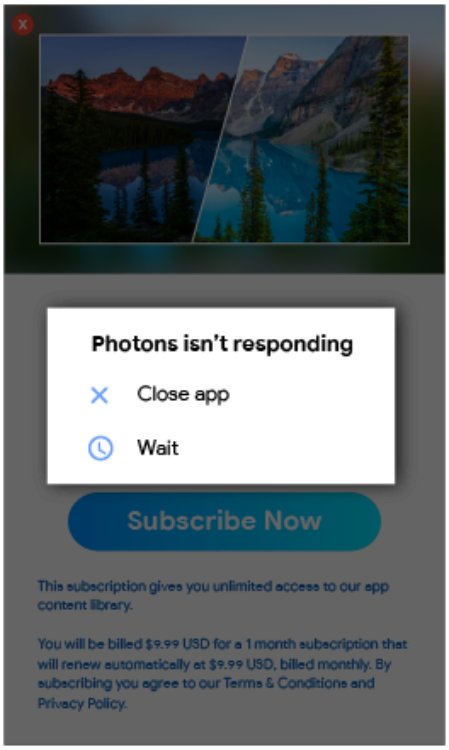
Google Play をこれからも信頼できる安全なプラットフォームとしてご利用いただけるようにするため、ユーザーにとって有害または不適切なコンテンツを定義し、禁止する基準を作成しました。

- **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基準も遵守することです。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 を通じて 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ている場合、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 の技術仕様および技術要件を遵守する必要があります。この仕様および要件は、Google の一般公開文書 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を促す

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。

デバイスの状態を変更する

Instant Apps が Instant App セッション以外でユーザーのデバイスを変更することは許可されていません。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してはなりません。

アプリの表示

デベロッパーは、Instant App がデバイス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。

デバイス 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デバイスの ID にアクセスすることはできません。これには次のものが含まれますが、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。

Android 絵文字ポリシー

Android 絵文字ポリシーは、一貫したインクルーシブなユーザー エクスペリエンスを促進できるように設計されています。これを実現するためには、すべてのアプリが Android 12 以上での実行時に Unicode 絵文字　の最新バージョンをサポートしている必要があります。

デフォルトの Android 絵文字をカスタム実装なしで使用しているアプリは、Android 12 以上での実行時にはすでに Unicode 絵文字の最新バージョンを使用しています。

カスタム絵文字（サードパーティ ライブラリ提供の絵文字を含む）を実装しているアプリは、新しい Unicode 絵文字のリリース後 4 か月以内に、Android 12 以上での実行時に最新の Unicode バージョンを完全にサポートする必要があります。

最新の絵文字をサポートする方法については、こちらのガイド　を参照してください。

アプリが最新の Unicode バージョンに準拠しているかどうかは、以下に示す絵文字の例が表示されるかどうかで確認できます。

例	Unicode バージョン
🩷🤳🦃	15.0
🫠🫱🏽🫲🏾	14.0
😶‍🌫️👩🏻‍❤️‍👩🏻	13.1
🥲🧑🏿‍🦲🐻‍❄️	13.0
🧑‍🦰🚶‍♀️‍➡️👫	12.1
🦩🫜🧑‍🤝‍🧑	12.0

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。デベロッパーは、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おり、関連するすべての法律に準拠していることを確認する責務を負います。

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。

Google Play ファミリー ポリシー

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。

Google Play のファミリー ポリシーに準拠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になるようオプトインできます。ただし、教師承認済みプログラムにアプリが含まれることは保証されません。

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。表示された年齢層のリストの中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] を選択することができます。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場合があります。

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。アプリに含まれているコンテンツが全世界向けとしては適切でない場合でも、特定の地域の子供ユーザーに適していると判断されれば、その地域（限定された地域 ）ではアプリを利用できる場合があります（それ以外の地域では引き続き利用できません）。
2. **アプリの機能:** ウェブサイトの所有権に関係なく、アプリでウェブサイトのウェブ表示を提供するアプリ、および特定の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ことを主な目的とするアプリは認められません。
   - Google は、子供向けアプリのデベロッパー向けに新たなエクスペリエンスを提供する方法を常に模索しています。Google の教育アプリ向け Trusted Web App パイロットへの参加にご関心をお持ち

の場合は、こちら　からお申し込みください。

3. **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。これには、[ターゲット ユーザーおよびコンテンツ] セクション、データ セーフティ セクション、IARC コンテンツ レーティング質問票において、アプリに関する正確な回答を提供することが含まれますが、これに限定されるものではありません。
4. **データの取り扱い:** アプリ内で API や SDK を呼び出すまたは使用するなどの方法で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、広告使用状況データなどが含まれますが、これらに限定されません。また、アプリはデータの取り扱い　に関して以下の要件を遵守している必要があります。
   - 子供のみを対象としているアプリの場合、Android 広告 ID（AAID）、SIM のシリアル、ビルドのシリアル、BSSID、MAC、SSID、IMEI、IMSI の送信を行ってはなりません。
     - 子供のみを対象としているアプリで、Android API 33 以上をターゲットとしている場合は、AD_ID 権限をリクエストすべきではありません。
   - 子供と大人の両方を対象とするアプリの場合、子供または年齢が不明なユーザーの AAID、SIM のシリアル、ビルドのシリアル、BSSID、MAC、SSID、IMEI、IMSI の送信を行ってはなりません。
   - Android API の TelephonyManager からデバイスの電話番号をリクエストしてはなりません。
   - 子供だけを対象としているアプリは位置情報の利用許可をリクエストしたり、正確な位置情報　の収集、使用、送信を行ったりしてはなりません。
   - アプリで Bluetooth を要求する際は、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。
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。
   - 主に子供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 Games 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　とともに使用されるか、子供からデータを収集しない方法で実装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してはなりません。
6. **拡張現実（AR）:** 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（たとえば周囲の状況）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（たとえば Daydream や Oculus）の使用をアプリの要件とすることはできません。
7. **ソーシャル アプリとソーシャル機能:** ユーザーが情報を共有したり交換したりできるアプリの場合は、Google Play Console のコンテンツ レーティング質問票　で、それらの機能について正確に開示する必要があります。
   - ソーシャル アプリ: ソーシャル アプリとは、ユーザーが自由形式のコンテンツを共有したり、大勢の人々が交流したりできるようにすることを主な目的としたアプリです。ターゲット ユーザーに子供が含まれるすべてのソーシャル アプリでは、子供のユーザーが自由形式のメディアや情報を交換できるようにする前に、オンライン環境での安全を確保し、オンラインでの交流が現実世界に影響を及ぼすリスクを認識できるよう、アプリ内でリマインダーを提供する必要があります。また、子供のユーザーが個人情報を交換できるようにする前に、大人による操作が必要となるようにしなければなりません。
   - ソーシャル機能: ソーシャル機能とは、ユーザーが自由形式のコンテンツを共有したり、大勢の人々が交流したりできるようにする追加のアプリ機能です。ターゲット ユーザーに子供を含み、ソーシ

ャル機能を備えるアプリでは、子供のユーザーが自由形式のメディアや情報を交換できるようにする前に、オンライン環境での安全を確保し、オンラインでの交流が現実世界に影響を及ぼすリスクを認識できるよう、アプリ内でリマインダーを提供する必要があります。また、子供のユーザーが使用するソーシャル機能を、大人が管理できるようにするための方法も提供する必要があります。たとえば、ソーシャル機能を有効または無効にできるようにする、機能のレベルを選択できるようにする、などが挙げられますがこれらに限定されません。さらに、子供のユーザーが個人情報を交換できる機能を有効にする前に、大人による操作が必要となるようにしなければなりません。

- 大人による操作とは、操作するユーザーが子供ではないことを確認し、子供が年齢を偽って大人向けのアプリ領域（大人用の PIN、パスワード、誕生日、メール確認、写真付き身分証明書、クレジット カード、SSN など）へのアクセスを得ようとしないようにするための仕組みを意味します。
- 知らない人とチャットをすることを主な目的としたソーシャル アプリでは、ターゲット ユーザーに子供を含めることはできません。たとえば、チャット ルーレット形式のアプリ、出会い系アプリ、子供向けのオープン チャットルームなどがこれに該当します。

8. **法規制の遵守:** アプリは、アプリ内で呼び出すまたは使用するすべての API および SDK も含め、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。

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。

- 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。

広告と収益化

子供を対象とするアプリを Google Play で収益化する場合は、「ファミリー向けの広告と収益化に関するポリシー」の要件を遵守することが重要です。

下記のポリシーは、アプリ内のすべての収益化要素と広告に適用されます。これには、広告、相互プロモーション（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）が含まれます。これらのアプリ内の収益化要素と広告は、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。

広告の要件

子供や年齢不明のユーザーに対してアプリ内で広告が表示される場合は、次の要件を満たす必要があります。

- このようなユーザーに対して広告を表示する場合は、Google Play ファミリー向け自己認定広告 SDK のみを使用すること。
- 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を持つ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。

広告フォーマットの要件

アプリ内の収益化要素と広告は、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デザインされている必要があります。

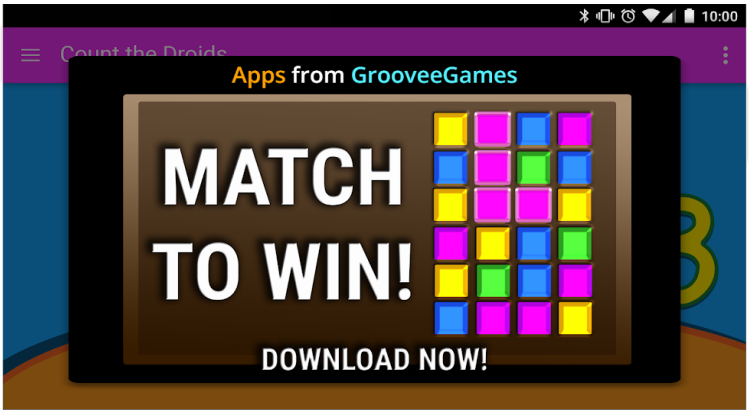
子供のみをターゲット ユーザーとするアプリでは、以下が禁止されています。子供と大人の両方をターゲット ユーザーとするアプリにおいて、子供または年齢不明のユーザーに広告を配信する場合は以下が禁止されています。

- 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、ユーザーを混乱させる恐れのある収益化要素や広告（たとえばウォール型広告）。
- 通常のアプリの使用やゲームのプレイを妨げ、5 秒経過しても閉じることができない収益化要素や広告（リワード広告やオプトイン広告を含む）。
- 通常のアプリの使用やゲームのプレイを妨げない収益化要素や広告（たとえば、動画コンテンツに組み込まれた広告）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などを表示して収益化すること。
- 1 ページに複数の広告を配置すること（たとえば、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のほか、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収益化要素や広告を配置すること。
- 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。

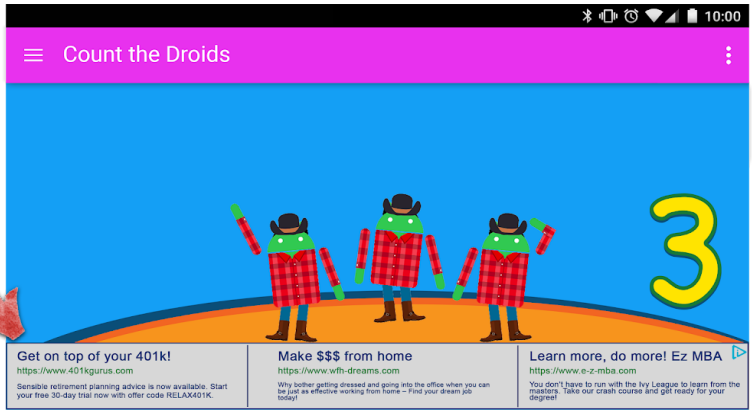
Google Play をこれからも信頼できる安全なプラットフォームとしてご利用いただけるようにするため、ユーザーにとって有害または不適切なコンテンツを定義し、禁止する基準を作成しました。

- ユーザーが閉じようとすると動いて逃れる収益化要素や広告。
- 5 秒以上表示しても閉じる方法が判明しない収益化要素や広告。次に例を示します。

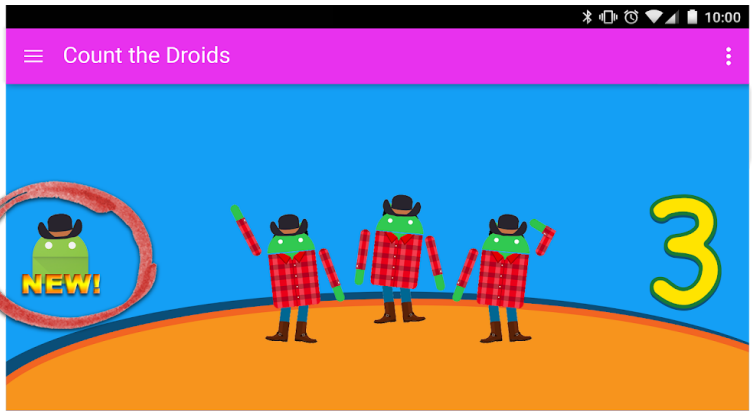
- 画面の全体または大部分を占めており、閉じる方法がわかりにくい収益化要素や広告。次に例を示します。



- 複数のクーポンを表示するバナー広告。次に例を示します。

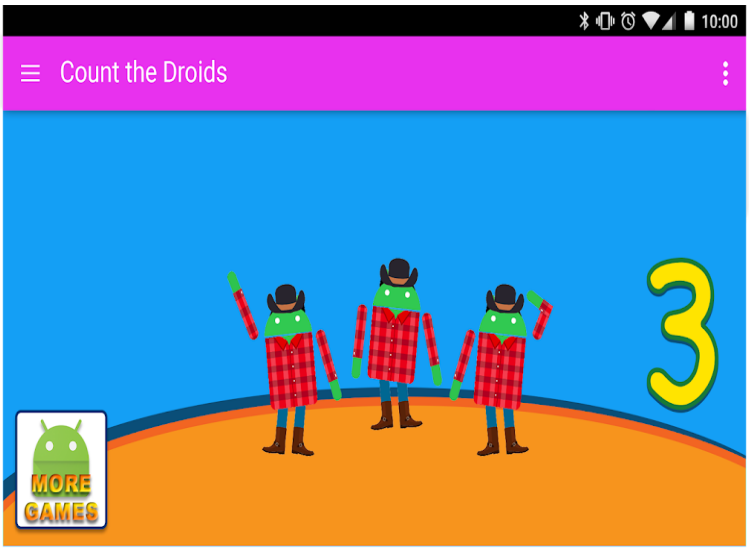


- アプリのコンテンツとして誤認される恐れのある収益化要素や広告。次に例を示します。



- デベロッパーは、ボタン、広告、収益化要素を使用して、自分が開発した他の Google Play ストアの掲載情報について宣伝できますが、そのボタン、広告、収益化要素は、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。次に例を示します。



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**: 子供には適してい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。

アプリ内購入

子供だけを対象と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。

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、ファミリー向け自己認定広告 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 自己認定広告 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。

各要件の詳細については、ファミリー向け自己認定広告 SDK プログラムに関するポリシー のページをご覧ください。現時点でのファミリー向け自己認定広告 SDK のリストについては、こちら 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。

ファミリー向け自己認定広告 SDK に関するポリシー

Google Play では、子供やファミリー層のお客様に安全にご利用いただける環境の構築に取り組んでいます。そのためには、ユーザーの年齢に合った適切な広告のみを表示することや、子供のデータを適切に扱うことが重要であると考えています。この目標を実現するため、SDK やメディエーション プラットフォームが子供向けに適しており、Google Play デベロッパー プログラム ポリシー と Google Play ファミリー ポリシー （ファミリー向け自己認定広告 SDK プログラムの要件 を含む）に準拠しているかどうかを自己認定することを求めています。

Google Play ファミリー向け自己認定広告 SDK プログラムは、どの広告 SDK やメディエーション プラットフォームが自己認定済みで、子供向けに設計されたアプリの開発に適しているかを判断するための重要な手段の 1 つです。

SDK に関する情報（お問い合わせフォーム での申請内容を含む）に不実記載があった場合は、ファミリー向け自己認定広告 SDK プログラムからの SDK の削除または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。

ポリシーに関する要件

SDK プロバイダとして、Google Play のファミリー向けプログラムの一部となっているアプリを配信できる SDK またはメディエーション プラットフォームを提供する場合は、以下の要件を含むすべての Google Play デベロッパー ポリシーに準拠する必要があります。ポリシー要件を満たしていない場合は、ファミリー向け自己認定広告 SDK プログラムからの削除または停止の措置が講じられる可能性があります。

SDK またはメディエーション プラットフォームがポリシー要件を満たしていることを確認する責任は SDK プロバイダにあります。Google Play デベロッパー プログラム ポリシー 、Google Play ファミリー ポリシー 、およびファミリー向け自己認定広告 SDK プログラムの要件 を必ず確認してください。

1. **広告コンテンツ:** 子供がアクセスできる広告コンテンツは、子供に適したものにする必要があります。
   - SDK プロバイダは、(i) 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、(ii) それらを規約やポリシーで禁止する必要があります。定義の内容は Google Play デベロッパー プログラム ポリシー に準拠するものである必要があります。
   - また、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する必要があります。対象年齢別区分には、少なくとも「全ユーザー対象」と「16 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、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。
   - 子供向けの広告配信にリアルタイム ビッ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、上記の要件を満たしていることを確認する必要があります。
   - さらに、クリエイティブの配信元が自社の広告枠であることを視覚的に識別する仕組み （広告クリエイティブにブランドロゴの透かしを入れる機能、またはそれに相当する機能）を提供する必要があります。
2. **広告フォーマット:** 子供のユーザーに表示されるすべての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を確認し、デベロッパーが Google Play ファミリー ポリシー に準拠した広告フォーマットを選択できるようにする必要があります。
   - 広告は、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デザインする必要があります。
   - 画面全体を占拠する広告、通常のアプリの使用を妨げる広告、閉じ方がわかりにくい広告など、ユーザーを混乱させる恐れのある広告（たとえばウォール型広告 ）は許可されません。
   - 通常のアプリの使用やゲームのプレイを妨げる広告（リワード広告やオプトイン広告を含む）は、5 秒経過したら閉じられるようにする必要があります。
   - 1 つのページに複数の広告を配置することはできません。たとえば、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や、複数のバナー広告または動画広告を表示することは許可されません。
   - 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。

- 広告の表示を促す目的で、広告において衝撃的な手法や巧妙に感情を操る策略を用いることはできません。

3. **IBA / リマーケティング:** 子供のユーザーに対して、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を持つ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）が表示されないようにする必要があります。
4. **データの取り扱い:** SDK プロバイダとして、ユーザーデータ（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。デバイス情報もこれに含まれます）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、SDK 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。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。子供の個人情報や機密情報 （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、広告使用状況データなどが含まれますが、これらに限定されません）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。
   - デベロッパー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）行えるようにする必要があります。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る必要があります。
     - 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。
   - 子供向けの広告配信にリアルタイム ビッダーが使用されている場合は、プライバシー インジケータがビッダーに反映されていることを確認する必要があります。
   - ユーザーが子供または年齢が不明である場合には、AAID、SIM のシリアル、ビルドのシリアル、BSSID、MAC、SSID、IMEI、IMSI の送信を行うことはできません。

5. **メディエーション プラットフォーム**: 子供に広告を配信する場合は、以下の要件を満たす必要があります。
   - ファミリー向け自己認定広告 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満た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。

6. **自己認定とコンプライアンス:** 広告 SDK のポリシーがすべての自己認定要件を満たしているかどうかを検証するために、お問い合わせフォーム の情報をはじめ、十分な情報を Google に提供する必要があります。こうした情報には以下が含まれますが、これらに限定されません。
   - SDK またはメディエーション プラットフォームの利用規約、プライバシー ポリシー、パブリッシャー向け統合ガイドの英語版を提供してください。
   - 要件を満たしている最新バージョンの広告 SDK を使用したサンプル テストアプリ を送信してください。このサンプル テストアプリは、ビルドが完了した実行可能な Android APK で、SDK のすべての機能が使用されている必要があります。テストアプリの要件:
     - スマートフォンのフォーム ファクタで実行することを目的とする、ビルドが完了した実行可能な Android APK として送信する必要があります。
     - Google Play のポリシーに準拠した、最新リリース バージョンまたは近日リリース予定のバージョンの広告 SDK を使用する必要があります。
     - 広告 SDK を呼び出して広告を取得、表示するなど、広告 SDK のすべての機能を使用する必要があります。
     - テストアプリからリクエストされたクリエイティブを介してネットワーク上のすべての公開中 / 配信中の広告枠にフルアクセスできる必要があります。
     - 位置情報による制限を設けることはできません。
     - 広告枠が複数の年齢層のユーザーを対象とする場合、テストアプリは、広告枠全体の広告クリエイティブのリクエストと、子供またはすべての年齢層に適した広告枠の広告クリエイティブのリクエストを区別できるようにする必要があります。

- 年齢詐称を予防する年齢確認で制御される広告を除き、広告枠内の特定の広告に限定することはできません。

7. その後も情報提供を求められた場合は適時に対応し、新たにリリースするすべてのバージョンが最新の Google Play デベロッパー プログラム ポリシー（ファミリー ポリシーの要件を含む）に準拠していることを自己認定　する必要があります。
8. **法規制の遵守:** ファミリー向け自己認定広告 SDK は、パブリッシャー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する必要があります。
   - SDK またはメディエーション プラットフォームが、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していることを確認する必要があります。

     注:「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。

プログラム要件の詳細については、ファミリー向け自己認定広告 SDK プログラム　のページをご覧ください。

施行

ポリシー違反に後から対処することもできますが、まずは違反を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もらうよう努めます。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リンク先ページなど、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（第三者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がすべての Google Play ポリシーを遵守していることを保証する必要があります。またこうしたアプリは、場合によっては追加のポリシー審査を受ける必要があります。

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 エコシステムに対するユーザーの信頼を傷つけるアプリやアプリのコンテンツは認められません。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、これらに限らず、さまざまな要因を検討します。不正行為については、アプリやデベロッパーに固有の申し立て、ニュース報道、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、これらに限らず、さまざまな項目を判断材料としてその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。

否承認

- 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承認となった場合、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、否承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。
- 否承認が 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: 否承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。
- アプリの否承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、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。

地域の限定

- 特定の地域のユーザーのみが Google Play を通じてアプリをダウンロードできるようにします。
- それ以外の地域のユーザーは、Google Play ストアで当該アプリを見つけることができなくなります。
- すでにアプリをインストール済みのユーザーは、そのデバイスでアプリを使い続けることはできますが、アップデートを受け取ることはできなくなります。

- 地域の限定は、Google Play デベロッパー アカウントの状態には影響しません。

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ないでください。

休眠アカウント

休眠アカウントとは、非アクティブまたは放置状態のデベロッパー アカウントです。休眠アカウントは、デベロッパー販売 / 配布契約　で求められている良好な状態にありません。

Google Play デベロッパー アカウントは、アプリを公開して積極的にメンテナンスしているアクティブなデベロッパーのためのアカウントです。アカウントの不正使用を防ぐために、使用されていないか、重要な作業（アプリの公開と更新、統計へのアクセス、ストア掲載情報の管理など）に利用されていない休眠状態のアカウントは定期的に閉鎖されます。

休眠アカウントが閉鎖されると、アカウントとアカウントに関連するすべてのデータは削除されます。登録料は返金されず、没収されます。Google は、休眠アカウントを閉鎖する前に、当該アカウントに提供された連絡先情報を使用して通知します。

休眠アカウントが閉鎖されても、その後 Google Play で公開することを決めた場合、新しいアカウントの作成が制限されることはありません。ただし、休眠アカウントを再度アクティブ化することはできず、新しいアカウントで以前のアプリまたはデータを利用することはできません。

ポリシー違反の管理と報告

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。

その他の参考リンク

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
- 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

Play Console 要件

Google Play は、ユーザーの皆様が安全かつ快適にアプリを利用できるだけでなく、すべてのデベロッパー様が成功を収めるための機会を得ることができる環境を提供したいと考えており、ユーザーにアプリを提供するまでのプロセスが可能な限りスムーズになるように努めています。

審査プロセスを妨げ、不承認の理由ともなる一般的な違反を回避するために、Google Play Console を通じて情報を送信する場合には、必ず以下のことを行ってください。

アプリを申請する際には次のことを行う必要があります。

- アプリに関するすべての情報とメタデータを正確に提供する
- 連絡先情報が最新であることを確認する
- アプリのプライバシー ポリシーをアップロードし、**データ セーフティ** セクションの要件を記入する
- 有効なデモアカウントやログイン情報など、アプリの審査に必要なすべてのリソース（ログイン認証情報、QR など）を提供する

前提として、申請するアプリは安定性と応答性に優れ、魅力的なユーザー エクスペリエンスを実現するものであるようにしてください。また、広告ネットワーク、アナリティクス サービス、サードパーティ SDK を含むアプリのあらゆる要素が、Google Play デベロッパー プログラム ポリシー を遵守していることを再確認してください。アプリの対象ユーザーに子供が含まれている場合は、Google のファミリー ポリシー も遵守する必要があります。

デベロッパー販売 / 配布契約 とすべてのデベロッパー プログラム ポリシー をお読みになり、アプリがこれらを完全に遵守していることを確認してください。

Developer Distribution Agreement

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