この資料の目的

Android 6.0 は 2015 年の 12月にリリースされ、ユーザー体験を影響するパーミッションの仕様変更がありました。この資料に実行時パーミッション（Runtime Permissions）の実装についての補足点をまとめております。

Android 6.0 (API Level 23) より、Dangerous パーミッションへのアクセス権限は自動的に許可されないため、アプリ実行中に権限を要求する必要があります。Dangerous パーミッションとは、ユーザーの個人情報に関連するデータのアクセス、ユーザーが保有しているデータへのアクセス、その他のアプリの動作に影響する権限を含みます。これらのパーミッションは Calendar, Camera, Phone, Location, SMS, などの 9 つのグループに分かれており、1 つのグループの権限が付与された場合そのグループのすべての権限が許可されます（参考資料 Normal and Dangerous Permissions をご参照ください）。そして、権限を要求するためのデフォルトダイアログ (例 1.2) はシステムが提供する一般的な説明しかありませんので、新たにデベロッパーが設定したタイミングでパーミッションを要求し、例1.2 のようなダイアログと連動できた直感的でわかりやすいご案内が必要と考えます。

また、Android 6.0 からはひとつひとつのパーミッション グループを任意なタイミングで要求できるため、デベロッパーは様々な体験を想像することができますが、Android 5.0 以前の端末のユーザーはすべてのパーミッションを確認してから、インストールする仕様には変更ありません。こちらの資料は主に新たな パーミッション モデルに対応する際の参考資料として作成しておりますが、Android 5.0 以前の仕様も考慮しております。本資料は新たなパーミッソンモデルを実装する際の参考となりましたら幸いです。

作成日: 20/02/2017
Google Play Techops 川端

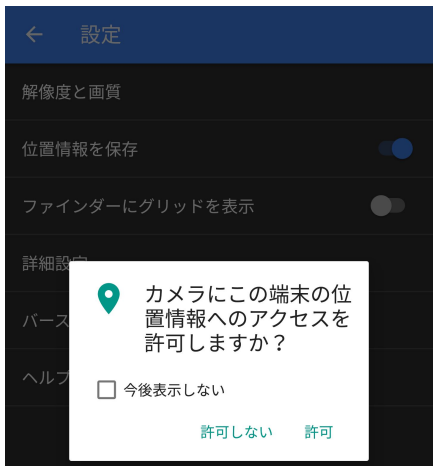
※本資料の情報は作成日時点のものであり、最新の Android や Google Play の仕様やガイドラインとは異なる場合がありますのでご了承ください。

実行時パーミッションの実装

実装をご検討いただく前に**もう一度かならずご確認いただきたい点として、アプリがユーザーにアクセスを要求しているパーミッションや情報は、本当にユーザー向けの機能に必要なのかという事です。**ユーザーに不信感を与えないためにも、提供している機能で必要なパーミッション以外は削除し、最小限のパーミッションのみを要求できるよう実装の調整をお勧めいたします。とくにユーザーの個人情報にアクセスする場合は注意が必要です（インテントで実装が可能な機能もありますので使用をご検討ください）。

例 1.1 Gmail : 連絡先を提案する機能

例 1.2 カメラ: 位置情報を利用した機能



上記の例 1.1 と例 1.2 は両方とも二次的なパーミッションのリクエストです。それぞれは異なったUXを実装していますが、ユーザーには直感的で自然なフローを提供できています。

実行時パーミッションの必要性をユーザー視点から見ると、大きく二種類にわけることができます。ユーザー向けの機能に必要であり、許可がなければアプリ自体の使用を困難にしてしまうパーミッションをこのドキュメントでは「必要不可欠なパーミッション」と呼びます。そして、アプリをより便利にするための二次的な拡張機能に必要なパーミッションを「二次的なパーミッション」と呼びます。

本資料の最後にはユーザーファーストで考えた基本的なユーザーフローを掲載しましたが UX を作る際の参考程度に活用ください。また、補足点もあわせて最後に残してありますのでご確認ください。

アプリの実行にパーミッションが必要不可欠な場合

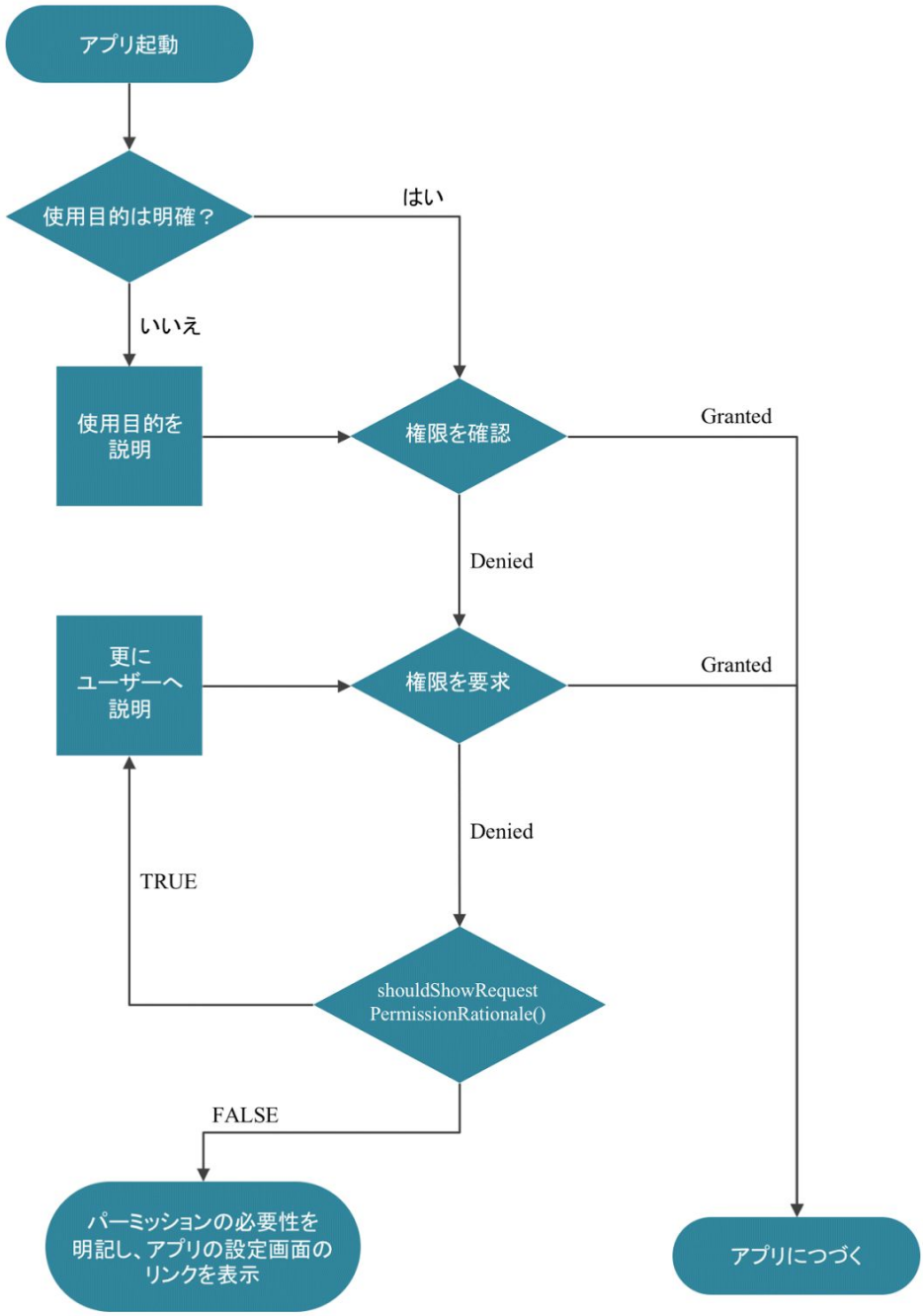
- 利用目的がユーザーに分かりにくい場合、初期起動時にパーミッションが必要な理由を案内し、その後にパーミッションの要求をする。
- 利用目的が明確な場合、アプリの初期起動時に直接ユーザーにパーミッションを要求する。

パーミッションが拒否されても

- すぐにユーザーをアプリ設定画面に案内しない。
- そのパーミッションの利用目的をユーザーに伝え、必要であれば再度アプリの中でパーミッションを要求する。
- 「今後は確認しない」にチェックしたまま「許可しない」を選択すると、アプリ内のパーミッション要求ダイアログが表示されません。この場合にのみユーザーにパーミッションの理由を説明しアプリの設定画面に直接遷移できるリンクを掲載する。

アプリの一部の機能に

必要不可欠なパーミッションの基本的なフロー



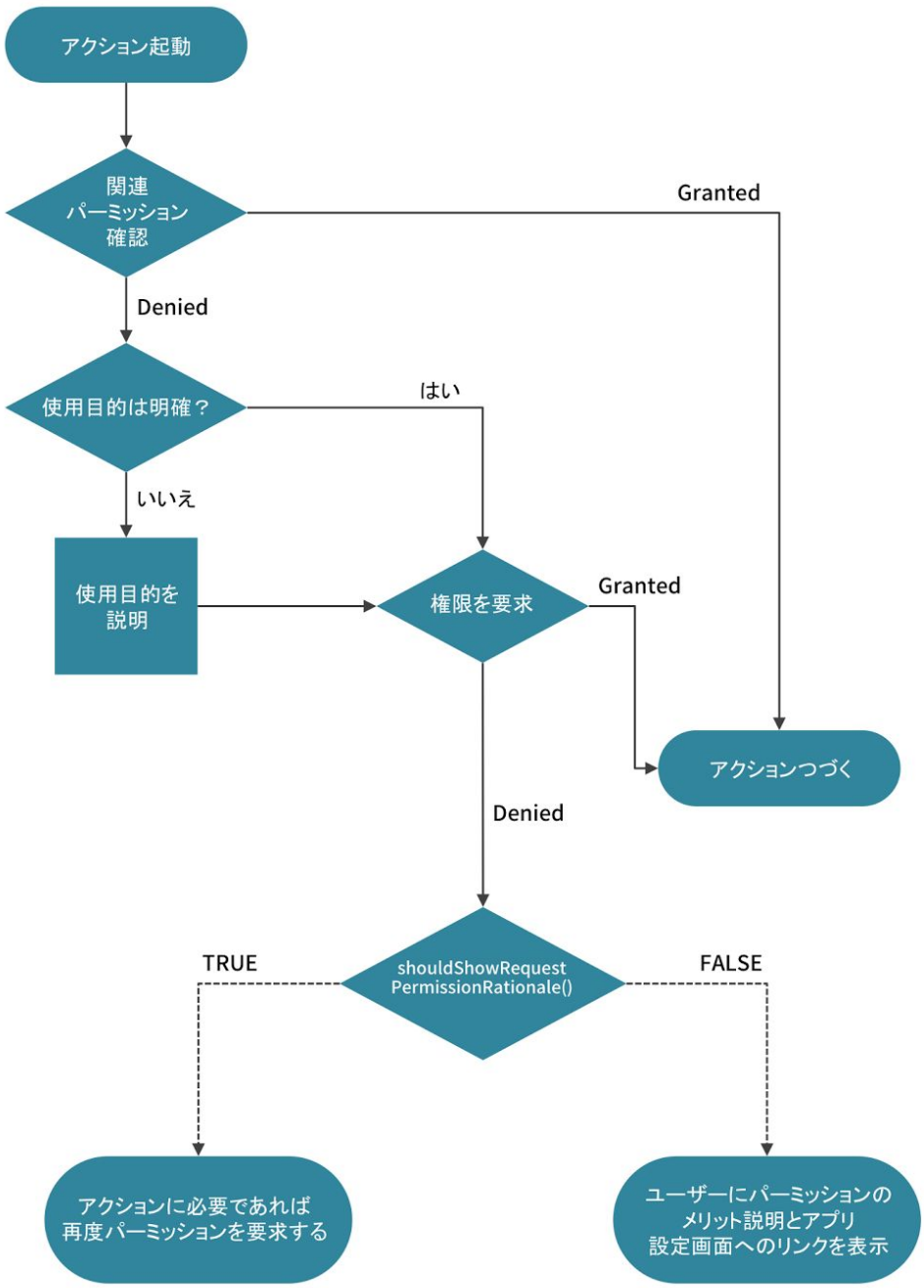
二次的なパーミッションの基本的なフロー

のみパーミッションが必要な場合

- 必要としている機能と関連する画面などで要求する。（例 1.1、例 1.2）
- パーミッションの必要性が明確ではない場合は、パーミッションを要求する前にユーザーに説明する。
- 更に良い体験を提供するには、ユーザーがパーミッションを許可した直後にパーミッションを許可した利益が一目でわかるよう実装する。

パーミッションが拒否された場合

- すぐにユーザーをアプリ設定画面に案内しない。
- パーミッションの利用目的をユーザーに伝え、必要であれば再度アプリの中でパーミッションを要求する。
- 一部の機能にだけ必要なパーミッションに「許可しない」と選択されても、アプリを利用できるように実装する。
- 「今後は確認しない」にチェックしたまま「許可しない」を選択すると、アプリ内のパーミッション要求ダイアログが表示されません。この場合にのみユーザーにパーミッションの理由を説明しアプリの設定画面に直接遷移できるリンクを掲載する。



最後に補足点を箇条書きで記載いたしました。

Android 6.0 のパーミッションモデルでは

- ユーザーが新たなパーミッションを確認しなくともアプリをアップデートできる。（インストール時にパーミッションの許可をもとめない）
- ユーザーは端末の設定から直接、それぞれのアプリパーミッションを管理することが可能。
- Dangerous パーミッションは 9 つのグループに分けられている。一つのグループの権限が付与された場合、そのグループのすべての権限が許可される。
    - また、グループとグループ内にあるパーミッションは更新されることもあるため、必ず Normal and Dangerous Permissions を参考に開発をすすめる。
- ユーザーにわかりやすい UX を提供するためには適切なタイミングでパーミッションを要求する必要がある。
- 以前のモデルと同じく、パーミッションは必要最小限に留める。
- パーミッションのアクセス権限は毎回確認する。
- アプリに対しパーミッションを拒否し、今後も実行時では要求できなくする設定がある。

その他の詳細な実行時パーミッションの参考資料：

- 実行時パーミッションのベスト・プラクティス（日本語）
- ブログ：実行時パーミッションでさらに優れたアプリを構築する（日本語）
- 動画：パーミッション要求の実装（英語）
- 実行時のパーミッション リクエスト（日本語）
- マテリアルデザイン（英語）
- マテリアルデザイン（日本語 PDF）