Android アンドロイド Smartphone スマートフォン プライバシーガイドライン

by タオソフトウェア

安心なアプリケーションを提供するために

---------- スマートフォンの利用者情報取扱いに関する総務省指針 ----------

総務省「スマートフォン プライバシー イニシアティブ」の

アンドロイド開発向け解説と具体的手順

Version 2.0

タオソフトウェア株式会社

目次

1. はじめに

本ドキュメントは、総務省のスマートフォンプライバシー指針※1 に沿って、アンドロイドのアプリケーションプログラマ（アプリケーション提供者）が、利用者（ユーザ）が安心して利用できるアプリケーションを効率的に設計し、公開が行えるように支援することを目的としています。総務省のスマートフォンプライバシー指針からアプリケーション提供者に必要な事項をピックアップし、アンドロイド特有の要件を追加して再構成しています。また、プライバシーポリシーの記載方法など、開発者が実際に作業を行う際に役立つように記載しています。

※１　総務省スマートフォンプライバシー指針とは、総務省のスマートフォンを経由した利用者情報の取扱いに関するＷＧにおいて、最終とりまとめとして、平成２４年８月に公開された「スマートフォン　プライバシー　イニシアティブ　- 利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション」を言います。

「スマートフォン　プライバシー　イニシアティブ」ダウンロード先
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

＜読者の皆様へ＞

- 本ドキュメントに、不十分な個所や、理解不足、間違い等がありましたら、ご指摘頂ければ幸いです。
- 本ドキュメントの内容は、弊社出版済みの「Android Security一安全なアプリケーションを作成するために」の第２章セキュリティ要件を補足する内容となっております。
- 多くの方に利用して頂けるよう、本ドキュメントは Apache License 2.0 として無償にて公開いたします。

※ 「Android Security一安全なアプリケーションを作成するために」は、2012 年１月に発刊されました。執筆を行ったのは１年以上前となります。執筆時、利用者情報をどのように取り扱うべきなのかについて記載すべきか非常に迷いました。利用者保護を強めに書くのか、実情に合わせた形で書くのか...。 その結果、具体的な内容に踏み込んだ記述ができず一般的な内容となってしまいました。
「Android Security ー 安全なアプリケーションを作成するために」
http://www.taosoftware.co.jp/android/android_security/

<V2.0 について>

本ドキュメント(V.1.1)公開後、11 月 13 日に、モバイルコンテンツフォーラム（ＭＣＦ）から「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」

（以降ＭＣＦ版）が公開されました。本ドキュメントはアンドロイドスマートフォンのみを対象としておりますが、ＭＣＦ版はスマートフォン全てを対象としています。アンドロイド向けとしても参考になる部分が多くありましたので、その部分を本ドキュメントに内容を加えさせて頂きました。また、自社アプリケーションのプライバシーポリシーを見直す過程で、本ドキュメントを変更した方が良い点、加筆した方が良い点などがありましたので合わせて記載を加えました。変更点の概要についてはドキュメント最後の変更履歴を参照ください。

モバイルコンテンツフォーラム
「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」
http://www.mcf.to/temp/sppv/mcf_spappp_guidline.pdf

2. 「スマートフォン　プライバシー　イニシアティブ」ドキュメント

2.1. 総務省のスマートフォンプライバシー指針の概要

スマートフォンには行動履歴や通信履歴等の様々な利用者情報が蓄積されています。アプリケーションによっては、それらの情報に対してアクセスを行い、外部へ送信しているものもあります。一方、情報の利用目的が不明瞭で、十分な説明が無いまま利用者情報を取得・利用するアプリケーションが増加しており、利用者の不安が高まっています。

このような社会情勢を受けて、総務省のスマートフォンを経由した利用者情報の取扱いに関するWGにおいて、最終とりまとめとして、平成 24 年 8 月に「スマートフォン　プライバシー　イニシアティブ　- 利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション」（以降、総務省のスマートフォンプライバシー指針）(116 ページ)及びその概要(15 ページ)が公開されました。

尚、総務省のスマートフォンプライバシー指針は、あくまでも「指針」であり、法的な拘束力はありません。

総務省のスマートフォンプライバシー指針は、日本国内だけでなく、諸外国でのプライバシー問題、プライバシー保護の取り組み状況も踏まえた上でまとまられています。

スマートフォン市場は、グローバル化が急速に進んでいることから、海外の利用者に対してアプリを配布し、サービスを提供する場合は、諸外国のプライバシー保護に関する規制に従う必要があります。
一方、日本国内では、現在、プライバシー保護に関する規制がなく、スマートフォンでのプライバシー保護に関する指針等が存在しなかったため、アプリケーション提供者が各自で判断して対処する必要がありました。
総務省のスマートフォンプライバシー指針が示されたことにより、アプリケーション提供者はこの課題に対処するための何をすべきかが明確に示されたことになります。アンドロイドのアプリケーション設計、公開について検討する際の論点、開発方針の目安として、是非活用されることをお奨めします。

2.2. 総務省のスマートフォンプライバシー指針の構成

総務省のスマートフォンプライバシー指針の構成は、次のようになっています。

総務省のスマートフォンプライバシー指針では、スマートフォンのプラットフォームとして以下の３つのプラットフォームについて記載されています。

- iOS 搭載端末
- アンドロイド搭載端末
- ウインドウズフォン搭載端末

また、以下の事業者が対象となる事項についてまとめられています。

- アプリケーション提供者
- 情報収集モジュール提供者
- アプリケーション提供サイト運営事業者
- アプリケーション紹介サイト
- OS 提供事業者
- 移動体通信事業者

章の構成は第１部と第２部に大きく分けられています。

- 第１部　スマートフォンと利用者情報に関する現状
  スマートフォンの利用者情報がどのように扱われているか、具体的事例や諸外国の動向、制度的な現状に関して述べられています。
- 第２部　課題認識と具体的な対応
  具体的にどのような対応が求められているのかについてまとめられています。アプリケーション提供者が認識すべき点としては、４章スマートフォンにおける利用者情報の性質・分類、５章スマートフォンにおける利用者情報の取扱いのあり方にまとめられています。
  本ドキュメントは、４章、５章を中心にまとめられています。

2.3.　利用者情報

総務省のスマートフォンプライバシー指針の P.58 には、スマートフォンの利用者情報を以下のように定義しています。

スマートフォンにおける利用者情報:
利用者の識別に係る情報、電話帳等の第三者に関する情報、利用者の通信サービス上の行動履歴、利用者の状態に関する情報など、スマートフォンにおいてスマートフォンの利用者と結びついた形で生成、利用、蓄積されている情報の総称。

具体的な例としては、P.10 に、電話帳データ、通話履歴、メール内容、ネット観覧履歴、位置情報、契約者・端末固有ＩＤ、映像・写真、ＳＮＳの利用履歴等が挙げられています。

2.4. プライバシー

総務省のスマートフォンプライバシー指針の P.51 では、プライバシーについては、「一般的に規定した法律はないが、判例法上プライバシーは法的に保護されるべき人格的権利」として認証されてきていると記載されています。

また、プライバシー権とは、一般人の感受性を基準にして公表されたくない個人に関する情報を、みだりに第三者に開示又は公表されたくない権利であり、これを踏まえると、以下はプライバシー権の侵害に当たる可能性があると記載されています。

アプリケーション提供者が、スマートフォン内の利用情報のうち、

1. 一般人の感受性を基準にして公表されたくない情報を
2. 本人の同意又は正当な目的なしに
3. アプリケーション提供者自身または情報収集モジュール提供者が取得・外部送信する事あるいは、その他第三者に提供する事

「一般人の感受性を基準にして公表されたくない情報」とは、個人識別性がない情報も含まれます。「感受性」は社会の変化、発展と共に変化するものです。したがって、現在プライバシーをどのように守るかについて策定したとしても、将来に渡って追従するのは不可能です。このため、アプリケーション提供者が守るべき基本原則が示されています。

2.5. スマートフォン利用者情報取得指針　基本原則

総務省のスマートフォンプライバシー指針の P.56 では、スマートフォンにおける利用者情報の取扱いについて、関係事業者は下記の通りの基本原則に従う事が望ましいと記載されています。

①透明性の確保

関係事業者等は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

②利用者関与の機会の確保

関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③適正な手段による取得の確保

関係事業者等は、対象情報を適正な手段により取得するものとする。

④適切な安全管理の確保
関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤苦情・相談への対応体制の確保
関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥プライバシー・バイ・デザイン
関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。 利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

2.6. 利用者情報の取扱い

総務省のスマートフォンプライバシー指針の P.54 では、スマートフォンにおける利用者情報を活用する関係事業者等は、利用者が個人情報やプライバシーの観点から安全・安心にサービスを活用できるように、利用者情報を適切に取り扱うとともに、利用者に対して分かりやすく透明性が高い説明を行い、その理解と有効な選択を促す事が求められているとされ、その基本アプローチとして以下が記載されています。

アプリケーションごとに**プライバシーポリシー**を策定すると共に、一定の情報の取得については、個別の情報の取得について、**同意取得**を求める。

利用者情報をどのように扱うのかを「**通知又は公表**」するために**プライバシーポリシー**を作成することが求められています。また**特に重要なデータ**に関しては、アプリケーション内で取得や取扱いについて独立した形で**利用者に同意を求める必要があります**。
アンドロイドのアプリケーションで利用者に注意を促す方法としては、ポップアップダイアログ、通知バー、バイブレーション、サウンド、ＬＥＤ等が挙げられます。

タオソフトウェアでは、以下の理由から、アンドロイドで動作するアプリケーションにおいては、ポップアップダイアログによる同意取得を求めるべきであると考えています。

・ 利用者本人の明確な同意を確認するために、「はい」「いいえ」といった選択肢を用意する必要があること。
・ また、ポップアップダイアログによる表示以外は利用者が見逃すおそれがあること。

なお、総務省のスマートフォンプライバシー指針 P.57 の「本指針の適用対象」には以下の記載があります。

なお、これら事業者であっても、スマートフォン上の利用者情報を、外部送信や蓄積を伴わない形で、スマートフォン内において一時的に取得・利用するのみの場合には、本指針の適用対象として想定していない。

したがって、電話帳データを取得するアプリであっても、外部通信や蓄積をしなければ、同意取得、プライバシーポリシー自体を作成する必要がない事になります。しかし、指針では続けて利用者の理解や透明性を高めるために、

「端末内部で〇〇の目的のための一時的に使用し、蓄積や外部送信をしない」等を利用者に通知又は公表することも有用である。

と記載されています。

つまり、指針を最低限遵守することに加え、基本原則に従い、利用者にとってよりよい方法を選択することが重要であるということです。
プライバシーポリシーの作成が必要のないアプリケーションなのか、プライバシーポリシーを作成していないアプリケーションなのか、利用者には区別が付かないということを踏まえ、全てのアプリケーションについてプライバシーポリシーを作成することを推奨します。

2.6.1. 通知又は公表（包括的な確認）

総務省のスマートフォンプライバシー指針の P.58 では、スマートフォンの場合の「通知」と「公表」は以下のように想定されています。

- 「**通知**」　書面（郵送等）、電子メール、アプリケーションによるポップアップ等の方法で伝える事
- 「**公表**」　アプリケーション上あるいはウェブサイト等へのリンクを示す事

「通知又は公表」となっているため、方法としてはどちらを選択しても良く、通常はより

簡便な「公表」を選択する事になります。具体的には、上記で述べた”ポップアップによる通知（表示）“ではなく、アプリケーション上かウェブサイト上で公表することを選択する事になります。

「通知又は公表」とは、プライバシーポリシーを作成しアプリケーション上かウェブサイト等へのリンクを示す事を表します。

2.6.2. 個別の情報に関する同意取得（都度確認）

総務省のスマートフォンプライバシー指針の P.58 では、「個別の情報に関する同意取得」（以後「個別同意取得」）とは、アプリケーション等により取得される個別の情報(電話帳、位置情報等)について、取得や取扱いについて独立した形で同意を取得することと記載されています。
また同指針の P.61 では、OS による利用許諾はアプリケーションがどのような情報にアクセスするかを示しているが、利用目的や外部送信・第三者提供の有無等の項目の記載がない場合には、OS による利用許諾単体のみでは本項に示す通知又は同意取得として十分ではないと記載されています。

具体例として、アンドロイドの OS ではどのようにアプリケーションの個別の情報に関する同意取得が行われているのかをみてみましょう。

アンドロイドの OS では、OS はアプリケーションをインストールする時にのみ、アプリケーションが OS のどのような機能を使用し、どのような利用者情報にアクセスする可能性があるのかに関する情報（権限、あるいは、パーミッションといいます）の確認画面を自動的に表示します。
（したがってアンドロイド OS の利用規約は通知又は同意取得としては十分ではありません。）

[アンドロイド OS のアプリケーション・インストール時の確認画面]

アンドロイドでは、アプリケーションが、都度確認をするべき機能を使用する際、あるいは、利用者情報にアクセスする際に、従来のフィーチャーフォンのように OS が強制的に確認画面を表示してくれないため、アプリケーション側で通知又は同意取得を行う必要があります。
尚、従来のフィーチャーフォンでも、アプリケーションの“利用目的や外部送信・第三者提供の有無”については、アプリケーション側で利用許諾画面を実装し、通知又は同意取得を行う必要があります。

よって、本ドキュメントでは、個別の情報に関する同意の取得とは、アプリケーション内でポップアップダイアログ表示をし、「はい・いいえ」ボタン等による「個別同意取得」を行う事とします。

このように、「個別同意取得」が必要なプライバシーデータがある場合、アプリケーションにポップアップ表示させるコードを実装する必要があります。したがって、アプリケーションが取り扱うプライバシーデータを、「通知又は公表」だけで良いものと、「個別同意取

得」を必要とする物を区別する必要があります。

「通知又は公表」か「個別同意取得」かは、「利用者情報の性質と種類」と、「利用目的による分類」を元に判断します。

2.7. 利用者情報の性質と種類

総務省のスマートフォンプライバシー指針の P.44 では、利用者情報に関して、３つの区分に分類をし、それらのデータの個人識別性の高さについてまとめています。

P.44 図表 4-2: スマートフォンにおける利用者情報の性質と種類

区分	情報の種類	含まれる情報	利用者による変更可能性	個人識別性等
第三者の情報	電話帳で管理されるデータ	氏名、電話番号、メールアドレス等	×～△	電話帳には一般に氏名、電話番号等が登録されることが多く、個人識別性を有している場合が多い。
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等	×～△	契約者情報には一般に氏名、住所等が含まれており、個人識別性を有している場合が多い。
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	・ログインのための識別情報は変更可能な場合も有り。 ・ログインのための識別情報は、氏名等個人識別性を有する場合もあり、単なる数字や記号等で単体では個人識別性を有さない場合もある。
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ウェブブラウザを通じ一時的にPCに書込み記録されたデータ等	○ 利用者が必要に応じて変更・修正を行うことが可能	・利用者がウェブブラウザ上で削除やオプトアウトを行うことが可能。 ・単体では個人識別性を有しないが、発行元等において他情報と照合し個人識別性を有する場合がある。
	契約者・端末固有ID	OS が生成するID（Android ID）、 独自端末識別番号（UDID）、 加入者識別ID（IMSI）、 IC カード識別番号（ICCID）、	× 端末交換や契約変更をしない限り変更が困難	・スマートフォンのOS やシステムプログラム、SIM カード、端末そのもの等に割り振られ管理される。利用者は端末交換や契約変更をしない限り変更困難。

		端末識別ID（IMEI）、MACアドレス等		・単体では個人識別性を有しない。他の情報と容易に照合できる場合、個人識別性を獲得する。 ・同一 ID に紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が指摘される。
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴	×～△ 端末や電気通信事業者のサーバーにおいて管理	・通信相手等により個人識別性を有する場合がある。 ・電気通信事業者の取扱い中のものは通信の秘密の保護の対象。 ・通信履歴はプライバシー上の懸念が指摘される。
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、検索履歴等の行動履歴	×～△ 端末やウェブページ管理者、アプリケーション提供者等のサーバーにおいて管理	・利用者の行動履歴や状態に関する情報については、内容・利用目的等によりプライバシー上の懸念が指摘される。 ・相当程度長期間にわたり時系列に蓄積された場合等、態様によって個人が推定可能になる可能性がある。
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等		
	位置情報	GPS 機器によって計測される位置情報、基地局に送信される位置登録情報		
	写真・動画等	スマートフォン等で撮影された写真、動画		・内容、利用目的等によりプライバシー上の懸念がある。 ・顔認識技術等が進むと、個人識別性に結びつく可能性が高まるとの指摘がある。

「区分」

- 「第三者の情報」は、利用者だけでなく、利用者以外（第三者）の情報が含まれている事を示します。このデータは、利用者データに加えて、家族、友人、会社等の情報が含まれ**利用者情報以外の第三者のプライバシーデータを含む事となり、より丁寧な取扱いが必要となります。**
- 「利用者の識別に係る情報」は、個人情報そのもの、もしくは個人情報になりうる情報を

示します。変更可能性も考慮した上でどの程度丁寧に取り扱うかを決める必要があります。

- 「通信サービス上の行動履歴や利用者の状態に関する情報」は、GPSデータやアプリケーションの利用履歴等、直ぐには個人情報になりにくいが、長期的に収集される場合は個人識別性が可能になる場合もあります。

「利用者による変更可能性」

ユーザーがその情報をどの程度変更しやすいかを表しています。容易に変更できる場合、情報が他者に渡ったとしても利用者が情報を変更することによって自衛する事ができます。逆に、変更が不可能な場合、関係事業者により名寄せ処理が可能になり、特定のIDに基づく個人識別性を持つ可能性があります。したがって、変更可能性が低い情報ほど個人情報に近いものとなり丁寧な取扱いが必要となります。

個人情報及び個人識別性が高い利用者情報を用いるときは、「個別同意取得」を求める。

2.8. 利用者情報の利用目的による分類

総務省のスマートフォンプライバシー指針の P.41 では、アプリケーションによる利用者情報の利用目的には大きくわけて４つあると記載されています。

利用目的	利用者の反応	必要な対応
１．アプリケーション等がそれ自体のサービス提供のために用いる場合。	利用者が直感的に理解しやすい。	従来通りの対応。
２．アプリケーション提供者が、アプリケーションの利用状況等を把握することにより、今後のサービス開発や市場調査のために用いる場合。	利用者が認知しにくいので、利用者のために丁寧な説明が必要。	「通知又は公表」及び「同意取得」が必須になる。
３．スマートフォンの位置情報あるいは契約者・端末固有 ID 等の利用者情報を情報収集事業者等が取得し、広告サービス等に活用する場合又はその他の市場調査等の情報分析等に活用する場合。		
４．現段階では目的が明確で	問題外、マルウェアと見なさ	NG

はないが将来的な利用可能性等を見込んで取得する場合。	れる可能性が高い。	

１の「アプリケーション等がそれ自体のサービスの提供のために用いる場合」とは、例えば電話帳アプリケーションが氏名や電話番号を使用する場合です。この場合は利用者情報の取得は、利用者に直感的に理解しやすいと言えます。
アプリケーション機能以外の目的に使用する、２、３の場合は、利用者がそのような情報が取得されるのを認知しにくいため、利用者のために丁寧な説明が必要です。
４の目的が明確でない物は、「通知又は公表」及び「個別同意取得」以前に情報取得すべきではありません。マルウェアとされる危険性が非常に高くなります。

アプリケーション自体のサービス以外に利用者情報を用いるときは、「個別同意取得」を求める。

3. アプリケーションの実装（個別同意取得ダイアログ）

本章では、総務省のスマートフォンプライバシーの指針に基づいた、アンドロイドのアプリケーションの実装例（個別同意取得ダイアログ）について解説します。

尚、本アプリケーションの実装方法については、あくまで、タオソフトウェアの独自の解釈に基づく一提案であり、総務省のスマートフォンプライバシーの指針において具体的な実装方法が示されているわけではありません。必ず、原文を参照する必要があります。

3.1. 個別同意取得ダイアログの作成要件

個別の情報に関する同意取得（都度確認）に従い、アプリケーションの実装要件については、本ドキュメントでは、個別同意取得ダイアログの作成要否の要件は、アプリケーションの外部通信の有無により決定されるとします。

アプリケーションの外部通信	個別同意が必要な利用者情報取得	個別表示取得ダイアログ
外部通信不可能	（1）しない	必要なし
	（2）する	必要なし
外部通信可能	（3）しない	必要なし
	（4）する	必要 or 推奨

（1）外部通信不可能、利用者情報を取得しない場合

利用者情報を取得しないので同意取得ダイアログを表示する必要性はありません。

（2）外部通信不可能、利用者情報を取得する場合

利用者情報を取得したとしても、外部に通信不可能なので個別同意取得ダイアログは必要ありません。プライバシーポリシーに取得情報及び収集していない事を明記する事を本ドキュメントでは推奨します。

（3）外部通信可能、利用者情報を取得しない場合

利用者情報を取得しないので同意取得ダイアログを表示する必要はありません。

（4）外部通信可能、利用者情報を取得する場合

＜個別同意が必要な利用者情報をサーバーに送っていない場合＞

総務省のスマートフォンプライバシーの指針では、個別同意取得の必要がないとされ

ています。しかし、アプリケーションが INTERNET パーミッションを持っている場合は、ユーザーへ明確なメッセージを伝え安心してもらうようにするべきです。「端末内部で〇〇目的のために××を一時的に使用します。蓄積や外部送信は致しません。」のようなメッセージを表示することを本ドキュメントでは推奨します。この場合「はい」「いいえ」ボタンのダイアログではなく「ＯＫ」のみのダイアログで十分です。

＜個別同意が必要な利用者情報をサーバーに送っている場合＞

個別同意ダイアログを表示してユーザーの同意を取る必要性があります。

3.2. 個別同意取得が必要な利用者情報

利用者情報の性質と種類に記載したように、「個別同意取得」の必要性は、「利用目的の分類」と「利用者情報の種類」を元に、利用者が簡単に判断できるかどうか（利用目的との一致）と取得する利用者情報が個人識別性をどの程度持つのか、プライバシー特性といった観点で分類されています。

よって本ドキュメントでは、スマートフォンに蓄積され、アプリケーションを通じて外部に自動送信され得る利用者情報で、かつプライバシー性の高い情報については原則「個別同意取得」が必要であるとします。
また、それ以外のデータに関しては、プライバシーポリシーへの記載で問題なく対応できるとします。

総務省のスマートフォンプライバシー指針の P.61 に「個別同意取得」代表的な事例が挙げられています。以下の場合は「個別同意取得」が必要となります。

1. 個人情報を含む電話帳などについては、目的に応じ必要とされる範囲（フィールド）を限定するとともに、プライバシー侵害を回避する観点から個別の情報を取得する事について同意を取得する
2. アプリケーションが提供するサービスへの利用以外の目的で、個人と結びつきうる形で GPS の位置情報等を取得する場合については、プライバシー侵害につながらないよう原則として個別の情報を取得する事について同意を取得する。
3. 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得については、通信相手等の個人識別性を有する場合があること、通信の内容を含むプライバシー上の懸念が想定されることから、個別の情報を取得することについて同意を取得する。
4. スマートフォンのアプリケーションの利用履歴やスマートフォンに保存された写真・動画については、アプリケーションによるサービス提供のために必要な範囲で用いられる場合を除き、プライバシー上の懸念が想定されるため、その取得に当たっては個

別の情報に関する同意を取得する。

5. 契約者・端末ＩＤなど、契約や端末に対して一義的に指定・作成され、利用者側で変更が困難であるが、幅広い主体により利用される可能性がある物が取得者において個人識別性を有する情報と結びつきうる形で利用される場合、同一ＩＤの上に様々な情報が時系列的に蓄積し得る事、取得者又は第三者において個人識別性を有する可能性があることから、個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱う事が適切と考えられる。具体的には、取得される項目及び利用目的を明確に記載し、その目的の範囲内で適正に扱う事とする。

以上をまとめると、

- （個別識別性が高い利用者情報）
  １、３，５より個人識別性が高く、個人情報とされる情報を利用する場合は、「個別同意取得」が必要となる。
- （利用者情報の目的外利用）
  ２、４より、アプリケーションのサービスへの利用以外の目的で利用者情報を取得する場合は、個人識別性が低い情報であってもプライバシーの観点から「個別同意取得」が必要となる。
- （第三者の利用者情報の扱い）
  ３より、利用する情報が利用者以外の第三者の個人識別性を有する可能性がある時は、「個別同意取得」が必要となる。
- （利用者の識別に関わる情報の変更容易性）
  ５より、利用者による変更が困難な情報を取得する場合は、名寄せの可能性があるため「個別同意取得」が必要となる。

となります。

よって、本ドキュメントでは、アプリケーションのサービスへの利用以外の目的で利用者情報を取得する時（利用者情報の目的外利用）は、「個別同意取得」が必要となり、アプリケーションのサービスへの利用目的で使用する場合は、個人識別性に応じて「同意取得」が必要かを決定するとします。

「通知又は公表」と「個別同意取得」

	（目的内利用） (1)アプリケーション自体のサービスに使用される時	（目的外利用） (2),(3)アプリケーション自体のサービスに使用されない時
第三者情報	個別同意取得	個別同意取得
個人情報	個別同意取得	個別同意取得

利用者で変更が困難な情報	個別同意取得	個別同意取得
利用者の識別に関わる情報	下表参照	個別同意取得
通信サービス上の行動履歴や利用者の状態に関する情報	個別同意取得、あるいは、通知又は公表（通知）	個別同意取得
それ以外のプライバシーデータ（環境による）	通知又は公表	個別同意取得

※利用者の識別に係る情報についての個別同意取得については、情報の種類によって「個別同意取得」要不要の判断が異なると解釈されるため、別表としました。

利用者の識別に係る情報についての「通知又は公表」と「個別同意取得」

区分	情報の種類	含まれる情報	利用者による変更可能性	個人識別性等
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等	×～△	個別同意取得 明らかに個人情報のため
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	通知又は公表 （自分のサービスで振り出したログインID） 個別同意取得 （他社サービスのログインIDやパスワード,Twitter,Facebook等）
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ウェブブラウザを通じ一時的にPCに書込み記録されたデータ等	○ 利用者が必要に応じて変更・修正を行うことが可能	通知又は公表
	契約者・端末固有ID	OS が生成するID（Android ID）、 独自端末識別番号（UDID）、 加入者識別ID（IMSI）、 IC カード識別番号（ICCID）、 端末識別ID（IMEI）、 MACアドレス等	× 端末交換や契約変更をしない限り変更が困難	個別同意取得 （変更が困難なため）

3.3. 個別同意取得のタイミング

個別同意取得ダイアログを出すタイミングとしては、「アプリケーション起動時」、「データを初めて取得する前」の２つが考えられます。

本ドキュメントでは、アプリケーション起動時での同意取得ダイアログは、利用者が読まずに同意する事が多いと思われるため、「データを初めて取得する前」に表示する事を推奨します。

しかし、広告モジュールが利用者情報取得している場合や、その情報がなければアプリケーションが成り立たないような場合は、アプリケーションの起動時に個別同意取得をするのが自然であると考えます。特にバックグラウンドで利用者情報を収集するアプリケーションでは、個別同意取得を得ていないのに情報を収集してしまう事のないように注意して頂きたいと思います。

4. プライバシーポリシー作成（ドキュメントワーク）

4.1. プライバシーポリシー作成要件

総務省のスマートフォンプライバシー指針に基づき、本ドキュメントでは、プライバシーポリシーの作成要否の要件は、アプリケーションが外部通信の有無と利用者情報を取得しているかにより決定されるとします。

アプリケーションの外部通信	利用者情報取得	プライバシーポリシーの作成要否
外部通信不可能	（1）しない	推奨
	（2）する	推奨
外部通信可能	（3）しない	推奨
	（4）する	必須

（1）外部通信不可能、利用者情報を取得しない場合

総務省のスマートフォンプライバシー指針では、利用者情報を取得しない場合は、ドキュメント作成の対象外となっています。しかし、利用者に対して利用者情報は取得しておらず、外部通信機能もない事を明示する事は、アプリケーション利用者に安心感を与えるのと同時に、アプリケーションがダウンロードされやすくなる効果も期待できるため、本ドキュメントではプライバシーポリシーの作成を推奨します。

（2）外部通信不可能、利用者情報を取得する場合

アンドロイドのアプリケーションでは、利用者がアプリの要求するパーミッション（INTERNET パーミッション）を確認することで、アプリケーションが外部通信を可能であるかを判断できます。このため外部通信をしていない場合、必ずしもプライバシーポリシーの作成は必要ではないと考えられますが、パーミッションの意味を全ての利用者が理解していることを期待するのは難しいと思われるため、全ての利用者が安心してアプリケーションを使用できるよう、本ドキュメントではプライバシーポリシーの作成を推奨します。

（3）外部通信可能、利用者情報を取得しない場合

総務省のスマートフォンプライバシー指針では、利用者情報を取得しない場合はドキュメント作成の対象外となっています。しかし、利用者に対して利用者情報は取得しておらず、外部通信機能もない事を明示する事は、アプリケーション利用者に安心感を与えるのと同時に、アプリケーションがダウンロードされやすくなる効果も期待できるため、本ドキュメントではプライバシーポリシーの作成を推奨します。

（4）外部通信可能、利用者情報を取得する場合

INTERNET パーミッションが付いており、利用者情報をサーバーに送信はしていないものの、外部通信が可能なアプリケーションは多くあります。

総務省の指針ではプライバシーポリシーの記載は必要ないようですが、利用者の視点では、プライバシーポリシーを通知又は公表していない不透明な（怪しい）アプリケーションなのか、利用者情報を外部通信していないため、プライバシーポリシーを記載する必要のないアプリケーションなのかの区別がつきません。

利用者情報をサーバーに送信していない場合でも、データを送信していない事を明示するためにプライバシーポリシーを作成し、通知又は公表する事で、利用者はアプリケーションに対する不安を解消することができ、安心してアプリケーションを使用することができます。

本ドキュメントでは、全てのアプリケーションが、プライバシーポリシーの作成を行うことを推奨します。

4.2. プライバシーポリシーの記載内容

総務省のスマートフォンプライバシーポリシー指針 P59 には、プライバシーポリシーに記載すべき情報について記載されています。

プライバシーポリシーに記載する内容

項目	説明
1. 情報を収集するアプリ提供者等の指名又は名称	アプリケーション提供者の名称、連絡先等を記載する。
2. 取得される情報の項目	取得される利用者情報の項目・内容を列挙する
3. 取得方法	利用者の入力によるものか、アプリケーションがスマートフォンの内部の情報を自動取得する物なのか等を示す。
4. 利用目的の特定・明示	● 利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるか、それ以外の目的のために用いるかを記載する。 ● 広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。
5. 通知・公表又は「同意取得」の方法、利用者関与の方法	● 通知・公表の方法、同意取得の方法 ● 利用者関与の方法
6. 外部送信・第三者提供・情報モジ	外部送信・第三者提供・情報収集モジュールの組

ュールの有無	み込みの有無を記載する。
7. 問い合わせ窓口	問い合わせ窓口の連絡先等を記載する。
8. プライバシーポリシーの変更を行う場合の手順	プライバシーポリシーの変更を行った場合の通知方法を記載する。

総務省のスマートフォンプライバシー指針の P.54 には､「アプリケーションごとにプライバシーポリシーを策定するとともに、一定の情報の取得については、個別の情報の取得につて...」という記載があります。

個々のアプリケーション毎にプライバシーポリシーを作成するのは手間がかかるため、最大公約数的なプライバシーポリシーを使用して全てのアプリケーションに適用させている例が見受けられます。利用者情報を取得しないアプリケーションに対しても、利用者情報を取得するプライバシーポリシーを適用する事は利用者が混乱する可能性があり、これは利用者への透明性が良いとは言えません。
プライバシーポリシーはアプリケーション毎に作成する事を推奨します。

また、アプリケーションの利用許諾内にプライバシーポリシーを入れてしまうと、分かりにくくなる可能性が高く、利用者に確認してもらえない可能性が高くなるため、利用許諾とプライバシーポリシーは分けて作成する事を本ドキュメントでは推奨します。

4.3. 日本語以外のプライバシーポリシー

Google Play を利用してアプリケーションを公開している場合、アプリケーションは海外でも利用されることが考えられます。
しかし、全ての言語に対して翻訳したプライバシーポリシーを作成するのは、ほぼ不可能です。機械翻訳をする事も考えられますが、誤訳される可能性もあります。許諾に関する事項のためアプリケーション提供者が正確に理解できない物を使用するのは非常に危険です。また国により法律が異なる点にも注意が必要です。

日本で作成されるアプリケーションは、英語と日本語に対応しているものがほとんどです。この場合の現実的な対応策としては

- アプリケーションをローカライズした言語のみプライバシーポリシーを記載する。プライバシーポリシーの翻訳は信頼できる専門家に依頼する。
- 日本語と英語のみプライバシーポリシーを記載する。プライバシーポリシーの翻訳は信頼できる専門家に依頼する。
- 日本語のプライバシーポリシーと機械翻訳をベースとしたある程度正しい英語のプライバシーポリシーを用意する。英語のプライバシーポリシーに、翻訳文であり正式な

プライバシーポリシーは日本語である事を明記する。

- 日本語のプライバシーポリシーのみを用意する。英語のプライバシーポリシーを記載すべき場所に日本語のプライバシーポリシーへのリンクを張る（読む人に機械翻訳をお願いする）

予算やアプリケーションの性質によって最適な方法を選択することになりますが、安易な翻訳をすると法的な問題が発生する事がありますので、注意してください。

5. プライバシーポリシーの記載方法

次に、アンドロイドアプリケーションを Google Play を通して公開する時に、プライバシーポリシーをどのように記載すれば良いのかについて、具体的に解説します。

5.1. 情報を収集するアプリケーション提供者等の氏名又は名称

解説：

アプリケーション提供者の名称を記載します。

対応策：

会社名、屋号、個人名を記載します。

記載例：

提供者名 タオソフトウェア株式会社

5.2. 取得される情報の項目

5.2.1. 取得項目

解説：

取得される利用者情報の項目・内容を列挙する。

対応策：

アンドロイドの場合、パーミッションを要求する理由を記載するケースが多く見られますが、パーミッションの情報から、一般利用者がどのような利用者情報が取得されるか想像することは困難であると考えられます。

また、一つのパーミッションで複数の利用者情報が取得可能なためメールアドレス、電話番号等、取得する具体的な項目を記載する必要があります。

センシティブな内容となるので、記載をすると利用者が使用しなくなるのではと心配される声も聞きますが、センシティブな内容だからこそ、記載しなければいけません。できるだけ丁寧に記載する事で利用者からの信頼を得る事ができますので、わかり易い記載を心がけてください。

後述する、「利用目的」や「同意取得」等の記載事項は、アプリケーション単位ではなく、取得情報単位で異なる記載となるので、本ドキュメントでは、取得項目毎に記載することを推奨します。

また本ドキュメントでは、外部通信をしていない場合、利用者情報を取得していない場合も、取得する項目として記載する事を推奨します。

記載例：通常

取得する情報項目：電話番号 内容：電話帳データから電話番号を取得します。

記載例：外部通信していない場合

取得する情報項目：電話番号 内容：電話帳データから電話番号を取得する 補足：蓄積や外部送信は致しません。

記載例：取得される情報の項目がない場合

取得する情報項目: 利用者情報は一切取得しておりません。

5.2.2. パーミッションと利用目的

解説：

アンドロイドにおいては、アプリケーションが要求するパーミッションの情報も重要です。

アンドロイドの OS がアプリケーションのインストール時に表示する、アプリケーションが要求するパーミッション情報は、利用目的の説明ではありません。またパーミッションには、利用者情報の取得以外にも、利用者に対して様々なリスクが伴うパーミッションが存在します。（電話や SMS を送信する等金銭が発生するパーミッション等）

本ドキュメントでは、これらの情報についても利用者に適切に通知（説明や警告を表示するなど）をするのが望ましいと考え、以下の指針に従って記載することを推奨します。

対応策

利用者にリスクが伴うプロテクションレベルが dangerous なパーミッションについては、利用目的を記載します。それ以外の物であっても記載することにより、利用者に対してより安心感を与えることができます。

記載例：パーミッションと利用目的

WRITE_EXTERNAL_STORAGE 作成した QR コード画像を外部記憶装置にファイルとして保存するのに使用しております。

5.3. 取得方法

解説：

利用者情報の取得方法が、利用者の入力による方法なのか、アプリケーションがスマートフォン内部の情報を自動的に取得する方法なのかを示します。

対応策：

利用者が自分自身で入力する場合と比べ、スマートフォンに保存されている利用者情報を自動的に取得する場合は、情報が取得されている事を利用者が認知しにくいと言えます。情報が取得されている事を明確にするために取得方法の記載をします。

「２．取得される情報の項目」毎に、利用者入力（ユーザー名をテキストボックスに直接入力する等）によるものなのか、あるいは、アプリケーションがスマートフォンに保存されている利用者情報を自動的に取得するのか、を記載します。項目により取得方法は異なるので、取得される情報の項目各々について記載する必要があります。

記載例：自動取得

取得方法：アプリケーションが自動的に取得する。

記載例：利用者入力

取得方法：利用者入力による

5.4. 利用目的の特定・明示

解説：

- 2.8.利用者情報の利用目的による分類に基づき、利用情報をアプリケーション自体の利用者に対するサービス提供のため（利用目的１）に用いるのか、それ以外の目的のため（利用目的２と３）に用いるのかを明確に記載する。
- アプリケーション自体が利用者に提供するサービス以外の目的に使用する場合（利用目的２と３）は、利用目的と取得される情報の項目の関係について丁寧な説明を行う。
- （利用目的３）広告配信・表示やマーケティング（ターゲティング広告等含む）目的のために取得する場合はその旨明示する。
- （利用目的３）利用者に対してターゲッティング広告等の配信を行う場合にはその旨明示する。
- （利用目的３）取得したデータを第三者に情報提供する場合はその旨を明示する。

対応策：

アプリケーションの目的に沿った利用者情報を取得するのであれば、その内容を詳しく、

かつわかりやすく説明します。
特に、アプリケーション自体の利用に対するサービス提供以外で利用者情報を取得する場合（利用目的２と３は、個別同意取得が必要な項目となる）は注意が必要です。
この情報の説明を怠るとマルウェアと誤解されたり利用者に不信感を与えてしまったりするおそれがあります。

アンドロイドの場合であれば、自アプリケーション内の利用者の操作ログを取得しているアプリケーション(例えばゲームオーバーした場所をサーバーに送り統計を取ることでゲームバランスを調整するケース等があります)、広告等の情報収集モジュールを組み込んだアプリケーションなどが主に該当します。

「２．取得される情報の項目」毎に、アプリケーション自体の利用に対するサービス提供に使うのか、それ以外の目的に使うのか異なるため取得される情報の項目各々に記載する必要があります。

広告等の情報収集モジュールを組み込む場合は、利用目的に「広告を利用するため」などように情報収集目的を記載します。

情報収集モジュールが第三者のものである場合、第三者（広告会社などの情報収集事業者）にデータが渡る事になるため、第三者提供項目に、「広告会社に情報が送られる」と記載します。

広告会社などの情報収集事業者から、さらに第三者にデータが渡る事がありますが、これ以上の情報については、「６．外部送信・第三者提供・情報モジュールの有無」に記載を行います。

情報収集モジュールによっては、どのような情報を取得するか明確でないことが多く、「スマートフォン　プライバシー　イニシアティブ」を受けて、日本の広告等の情報収集事業者はプライバシーポリシーや取得する利用者情報を明確にする事が予想されます。

本ドキュメントでは、アプリケーション開発者が、広告等の情報収集事業者が公開する情報を良く吟味し、広告等の情報収集モジュールの選定を行うことを推奨します。広告等の情報収集モジュールがマルウェア機能を持っているケースもあります。信頼できる会社の情報収集モジュールを使用してください。

記載例：アプリケーション自体の利用に対するサービス提供に使用する場合

利用目的：アプリケーション自体の機能として使用する。

記載例：アプリケーションの利用状況を把握するために使用する場合

利用目的：ゲームオーバーした場所の統計を取る事でゲームバランスを改善するため

記載例：広告モジュールを使用している場合

利用目的：広告を利用するため 第三者提供：広告会社に情報が送られる。

5.5. 通知・公表又は同意取得の方法、利用者関与の方法

解説：

- プライバシーポリシーの掲示場所や掲示方法、「個別同意取得」の対象、タイミング等について記載します。
  プライバシー性の高い低いによって以下の２つの取扱いをします。
  - 一般的な取扱い
    - プライバシーポリシーはダウンロードする前に掲示又はリンクを配置する
    - プライバシーポリシー概要を作成し表示する
    - ダウンロード、インストール前に提示が難しい場合は起動時にプライバシーポリシーの表示を行う
  - 「個別同意取得」等を要する利用者情報の取扱い
    - 情報取得処理が行われる前に「個別同意取得」を行うこと
    - 現在アンドロイド OS が表示する、パーミッションを軸とした利用許諾は内容が十分でないため「個別同意取得」としては十分ではない

- 利用者関与の方法については利用者情報の利用を中止する方法を記載します

プライバシーポリシーは、利用規約のように長文で何が書いてあるのか分からないので、利用者が読み飛ばしてしまう事を防ぐために分かりやすく記載すると共に、簡潔な概要を作成しインストール前に見られるようにする、概要から詳細にリンクを張ります。

5.5.1. プライバシーポリシーの提示場所、掲示方法

対策：

プライバシーポリシーの文章の置き場所は、ウェブページ、アプリケーション内部の２種類が考えられます。

アプリケーション内でしかプライバシーポリシーを確認できない場合、利用者がアプリケーションをインストールしてからでないとプライバシーポリシーを確認できなくなります。プライバシーポリシーは、利用者がいつでも自由に参照できるようにしておくことが望ましいとされています。アプリケーション内部に持っている場合も、ウェブページに記載をしてください。

プリインストールアプリケーションや、アプリ配布時に利用者がプライバシーポリシーを参照できる機会がない場合もあります。この場合は初回起動時にダイアログを出してプライバシーポリシーを表示してください。

アプリケーション内部に置く場合は、メニューからプライバシーポリシーの表示を利用者が選択すると、ブラウザを開いてプライバシーポリシーのページを開く実装が簡単でお勧めです。

アンドロイドの場合は、Google Play Developer Console でアプリケーション毎にプライバシーポリシー情報へのリンクを入力する箇所がありますので、プライバシーポリシーをウェブサイトに置き URL を記載するのが一般的です。

Google Play のようにプライバシーポリシーへのリンクがないマーケットサイトで配布する場合は、マーケットサイトのアプリ紹介画面にリンクを記述し、加えて、アプリケーション内に保持し、アプリケーション起動時に表示します。この時は、「アプリケーション内に掲示しアプリケーション起動時に表示」と記載します。

記載例：

プライバシーポリシーの掲示方法：
ホームページに掲示
http://www.taosoftware.co.jp/android/packetcapture/#privacy_policy

プライバシーポリシー概要提示場所：
アプリケーションの説明画面に記載

プライバシーポリシーの提示場所：
アプリケーション内に掲示しアプリケーション起動時に表示

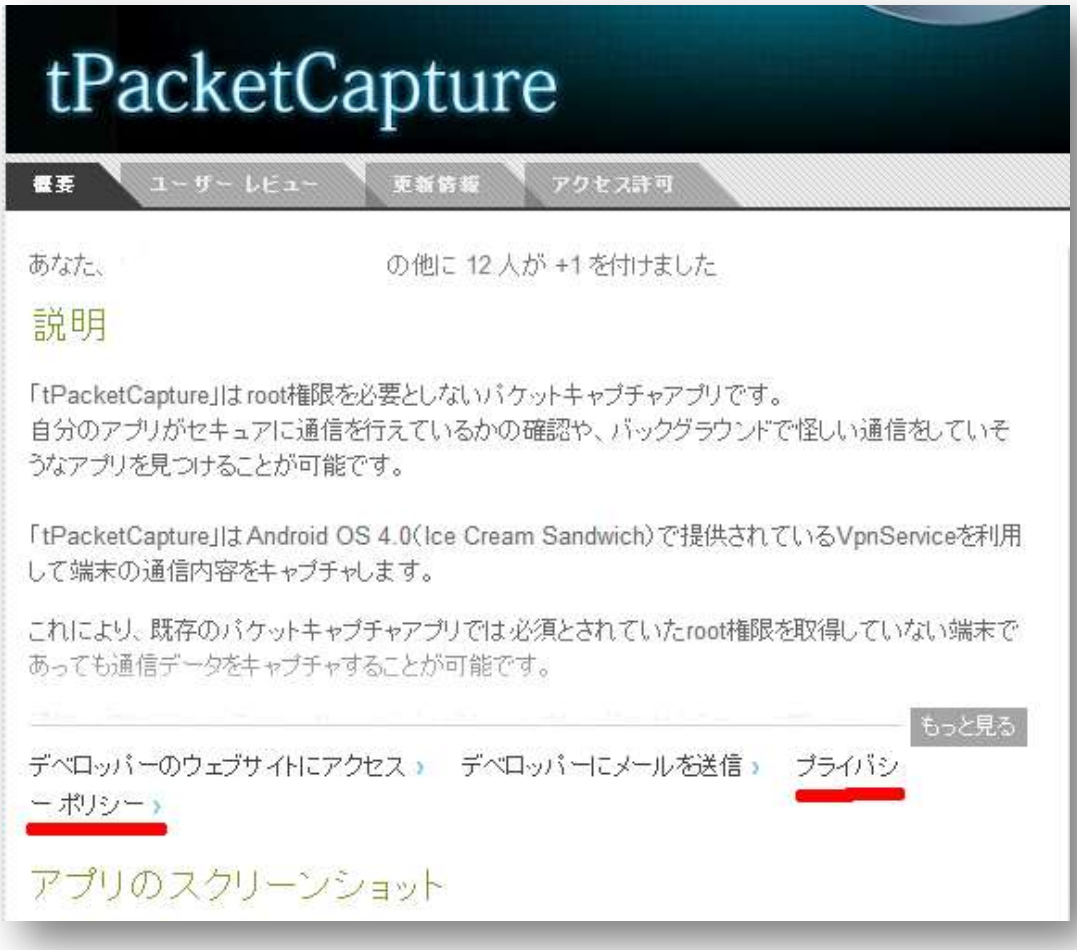
プライバシーポリシー概要提示場所：
アプリケーションの説明画面に記載

Google Play のプライバシーポリシー表示について
アプリケーションを公開するときに、プライバシーポリシー情報のリンクを設定する項目が存在します。

[Google Play Developer Console の入力画面]

ここに作成したプライバシーポリシーの URL を記載することで、利用者はダウンロード前にプライバシーポリシーを参照することができます。プライバシーポリシーの文章自体をアップロードする事はできません。(「今回はプライバシーポリシーの URL を送信しないチェックボックス」をオンにする事でプライバシーポリシーを設定しない事もできます)

[Google Play Web 上のプライバシーポリシーリンク]



プライバシーポリシーの URL を設定したアプリケーションを、Google Play の Web 版で表示すると、プライバシーポリシーのリンクが表示されます。このリンクをクリックすると、ブラウザは設定された URL へ遷移します。

[Google Play アプリケーション上のプライバシーポリシーリンク画面（左）とクリック後のプライバシーポリシー表示画面（右）]

Google Play にはこのようなプライバシーポリシーの URL を記載する画面があるが、残念ながら、プライバシーポリシーの URL を記載しているアプリケーションは多いとは言えないのが現状です。

5.5.2. プライバシーポリシー概要

対策：
長文かつ複雑で難解に書かれたプライバシーポリシーは利用者が詳細を読むことなく同意してしまう事が考えられます。
本ドキュメントでは、プライバシーポリシー概要を作成し、ダウンロード前に表示されるアプリケーション説明文に記載することを推奨します。

また、プライバシーポリシー原文の参照先を URL で記載しますが、Google Play ではアプリケーション説明部分には記載された URL はハイパーリンクとして認識されないので、利用者が直ぐにプライバシーポリシーの原文が掲載されているウェブページに移動ができません。

本ドキュメントでは、利用者の観点から、URL をテキストとして記載しつつ「上記ＵＲＬへは、デベロッパー情報のプライバシーポリシーリンクから移動可能です。」と記載することを推奨します。

記載例：Google Play アプリケーション概要内

プライバシーポリシー概要 本アプリケーションは、電話帳に含まれる全てを取得し弊社サーバーに送信します。 これらのデータは本アプリケーションが提供するサービス以外の目的には使用しません。 アプリケーションには広告が含まれますが、広告会社には電話帳データは送信されません。 プライバシーポリシーの詳細につきましては、 http://www.taosoftware.co.jp/android/packetcapture/#privacy_policy を参照ください。 上記ＵＲＬへは、デベロッパー情報のプライバシーポリシーリンクから移動可能です。

5.5.3. 同意取得の対象、タイミング

対策：
「２．取得される情報の項目」毎に、「同意取得」を行うのか、プライバシーポリシーへの記載のみで「個別同意取得」を行わないのか異なるので、取得される情報の項目各々に記載します。

「個別同意取得」のタイミングは、以下の２つに分けられるので実装に応じて記載します。

- 「アプリケーション初回起動時」
- 「初回情報取得時」

記載例：

同意取得：有：初回情報取得時

記載例：

同意取得：なし

5.5.4. 利用者関与の方法

解説：
利用者がアプリケーションによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載します。

＜オプトアウトできる場合＞

- アプリケーションを使用しながら、情報の取得が中止される方法がある場合は記載する
- アプリケーションを使用しながら、情報の取得は継続されるが、その利用が中止される方法がある場合には記載をする（※）
- 一度利用者が同意を行った後に、後から同意撤回などの変更が可能となる機会についてもできるだけ提供するように努める

※総務省の原文がわかりにくいため本ドキュメントで補足しました。本ドキュメントでは、例えば、端末から取得された情報がサーバーに送信され続けるが、サーバーが受信した情報は使用されない、のように解釈いたしました。

＜オプトアウトできない場合＞
- 利用者がアプリケーションによる利用者情報の利用や取得を中止したい場合に、アプリケーションそのものをアンインストールする以外に方法がない場合はその旨記載する。

※利用者に関する情報が、プライバシーに反して収集され、取り扱われている事が明確である場合などについては、利用者からの申し出を受け利用の停止又は消去を行うものとする。

ＭＦＣ版のアプリケーションプライバシーポリシーＰ18 の「6. 取得した利用者情報の取扱いについて」では、利用者情報の保存期間を記載しておくことが有用だと記載されています。
利用者関与をするためには、他の利用者の情報と区別するために本人確認が必要となります。しかしながら、端末の買い替えをした場合、退会手続きをせずにアプリケーションをアンインストールした場合等、利用者関与ができなくなってしまいます。このような場合を想定して、一定の期間利用がなかった場合に利用者情報を削除する事を推奨します。またその旨をプライバシーポリシーに記載します。
なお、MFC 版アプリケーションプライバシーポリシーでは、サンプルとして「２年」を保存期間としています。

対応策：
利用者情報の利用や取得の停止方法

＜オプトアウト方法を記載する＞
- 利用や取得の停止が、アプリケーションの設定画面等から可能な時はその手順を記載

する。

- 利用や取得の停止が、サーバーのコンソールから可能な時はその手順を記載する
- 電話、メールや Web 上のフォームから連絡する事で可能な場合は、その旨記載をする

＜オプトアウト方法がない場合はアプリケーションの利用中止を記載する＞

- アプリケーションのアンインストールしかない場合はその旨を記載する

本ドキュメントでは、以下のようなオプトアウト手段がないアプリ／サービスは、利用者保護の観点から提供すべきではないと考えます。

＜提供してはいけないアプリ＞

- 利用や取得の停止ができないものは提供しない。
- アプリケーションを削除しても、情報の利用の停止ができないものは提供しない

アプリケーション自体が取り扱う利用者情報の取得停止方法にくわえ、広告等の情報収集モジュールを使用しており、利用者情報がそのモジュールで使用されている場合についても記載する必要があります。

利用者データの取得に関しては、アプリケーションをアンインストールすることで、収集を停止することが可能ですが、既に取得されたデータはサーバーに残っています。

本ドキュメントでは、利用者データの利用停止（使用しない事やデータをサーバーから削除する事）に関しては、そのような機能が実装されていない物も多く存在するため、利用者情報を取得する第三者モジュールは組み込まないように注意する必要があると考えています。

記載例：複数モジュールがある場合

利用者関与の方法：
サービス自体に利用される情報の利用者関与：

- 取得の中止：アプリケーションをアンインストールすることで可能
- 利用の中止：本サービスのウェブサービスにログインして、アカウントの削除を行ってください。

広告に利用される情報の利用者関与：

- 取得の中止：アプリケーションをアンインストールすることで可能

利用の中止：XXX 社のサービスを利用しております。利用中止の方法に関しては、XXX 社

（リンク等）にお問い合わせください。

5.6. 外部送信・第三者提供・情報モジュールの有無

5.6.1. 第三者提供する場合の取扱い

解説：

- アプリケーション提供者や情報収集モジュール提供者等が取得した利用者情報を第三者に提供する場合、あらかじめ本人の同意を取得する
- この場合、以下の項目に関してそれぞれ明確にプライバシーポリシーに記載すること
  1. 第三者への提供を利用目的とすること
  2. 第三者に提供される利用者情報の項目
  3. 第三者への提供の手段または方法
- この場合、個別同意取得を行う事

第三者とは、アプリケーション提供者、あるいは、サービスを提供している会社以外の人を言います。

第三者提供とは、アプリケーションが取得した利用者情報を上記の第三者に無償、あるいは、有償で提供することを言います。また、利用者情報の提供を受けた第三者は、提供条件の範囲内において、提供された利用者情報を自由に利用することができます。
尚、委譲する場合は、第三者提供には該当しません。
利用者情報の取得者が、利用目的の達成に必要な範囲内において、利用者情報の取扱いの全部または一部を外部委託する事は第三者提供に該当しません。ただしこの場合は、委託先における利用者情報の取扱いの安全管理についてもアプリケーション提供者が監査責任を負います。

第三者に提供する場合でも、個人識別性を獲得し得ない匿名化された情報を統計処理した結果等を第三者に提供する場合は、あらかじめ本人の同意を取得する必要はありません。

対応策：

サービス自体が取得した利用者情報を第三者に提供する場合は、以下の３つの項目に関してプライバシーポリシーに記載し、個別同意取得を取る事が必要です。

記載例：利用者情報を取得しない場合

利用者情報は取り扱っておりません。したがって、利用者情報を外部送信したり第三者提供することはありません。

記載例：第三者提供しない場合

本サービスは取得した利用者情報を、第三者に提供する事はありません。

記載例:第三者に渡す場合

利用目的：注文された商品を住所に配送するため運送会社に提供を行う 利用者情報項目：氏名、住所、電話番号 提供の手段または方法：書面、電話

除外事項

本プライバシーポリシーに記載されている第三者以外への情報の提供は行いません。ただし次のいずれかに該当する場合を除きます。 1. 法令上の義務により開示を求められた場合。 2. 人の生命、身体または財産等の重大な利益を保護するために緊急に必要がある場合。 3. 公衆衛生の向上又は児童の健全な育成の推進のために必要がある場合。 4. 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する場合。

5.6.2. 情報収集モジュールを組み込む場合の取扱い

解説：

- アプリケーション提供者が情報収集モジュールを組み込む場合、アプリケーションを通じた情報収集の詳細について明らかにする上で、アプリケーション提供者は、自らが組み込んでいる情報収集モジュールの数、名称、提供者等の基本的な情報について、利用者に対して説明する必要があります。
- 具体的には、アプリケーション提供者は、アプリケーションのプライバシーポリシーに、以下の情報を情報収集モジュールごとに記載するとともに、各種情報収集モジュール提供者のプライバシーポリシーにリンクを張るなどして容易に見られるようにする必要があります。
    1. 組み込んでいる情報収集モジュールの名称
    2. 情報収集モジュール提供者の名称
    3. 取得される情報の項目

4. 利用目的
5. 第三者提供の有無等

対応策：
情報収集モジュールには、広告モジュールも含まれます。解説に従って記載を行います。

記載例：

広告モジュール名： ＹＹＹ広告モジュール 広告モジュール提供者名： 株式会社ＸＸＸ 広告モジュールのプライバシーポリシー： http://xxx.xxx.co.jp/policy/ 取得される項目： 広告を表示する毎に位置情報を取得します。 利用目的： 利用者にとって価値のある広告を配信するため 第三者提供の有無： 広告モジュールの説明に第三者への提供はないと記載されています。

5.6.3. 海外モジュールの取扱い

海外で作成されたモジュール（特に広告モジュール）は現在日本語でのプライバシーポリシーの提供は殆どありません。翻訳して記載する事も可能ですが、国によりプライバシーの取扱いが異なるため、意味を取り違える場合もあります。安易な翻訳は止めて専門家に相談する事をお勧めします。
また、マルウェア的性質を持った広告モジュールは多く存在します。そのようなモジュールをアプリケーションに入れてしまうと、アプリケーション自体マルウェアとして認定されてしまいます。良くわからないモジュールはアプリケーションに入れないように注意してください。

5.7. 問い合わせ窓口

解説：
利用者情報を取得する者は、利用者情報の取扱いに関する苦情や相談の適切かつ迅速な処理に努めなければなりません。具体的には、苦情相談窓口・連絡先を設置するなど必要な体制の整備に努めなければなりません。

対応策
問い合わせ窓口の連絡先を、電話番号やメールアドレスで記載します。

記載例：

問い合わせ窓口： info@taosoftware.co.jp

5.8. プライバシーポリシーの変更を行う場合の手順

解説：
プライバシーポリシーの変更を行う場合の手順に関しては、「スマートフォン　プライバシー　イニシアティブ」には記載されていません。

Web サービスでのプライバシーポリシーでは、「弊社サイトで告知」と記載されているものが多いのですが、アプリケーションの場合、利用者が再度プライバシーポリシーの記載ページに来る事はまれであり、変更を認知することは困難と考えられます。

したがって、スマートフォンアプリケーションの場合は、ＰＣ上で動作するソフトウェアのように、プライバシーポリシーが変更となった際には、アプリケーション起動時やポリシー変更による影響を受けるデータ取得時に「個別同意取得」するなどの工夫を行うことが望ましいといえます。

対応策：
「個別同意取得」が必要なプライバシーポリシーの場合はアプリケーション上で同意を求めます。
「個別同意取得」が必要ないプライバシーポリシーの変更の場合は、「弊社サイトで告知」等の記載で良いと思われます。

記載例：

プライバシーポリシーの変更を行う場合の手順： 「個別同意取得」が必要な、重要なプライバシーポリシーの変更はアプリケーション内でポップアップ表示させ再度「個別同意取得」致します。 「個別同意取得」が必要ないプライバシーポリシーの変更に関しては、弊社サイトで告知を致します。

6. プライバシーポリシーサンプル

「5 プライバシーポリシーの記載方法」を踏まえて、アンドロイドアプリケーションの場合どのような記載が良いのかを以下にサンプルとして記載します。

本ドキュメントが定義するプライバシーポリシーのテンプレートについて説明します。

１．アプリケーション概要
２．プライバシーポリシー概要
３．プライバシーポリシー（本体）

＜アプリケーション概要の記載事項＞

項目	説明
アプリケーション名	サンプルアプリケーション名
機能概要	サンプルアプリケーションがどのような機能を持っているのか簡単に説明します。

＜プライバシーポリシー概要の記載事項＞

項目	説明
取得する利用者情報の概要	複数ある場合は個人識別性の高い項目を中心に簡潔に記載します。
外部送信の有無と目的	利用者情報を外部送信するかとその目的について記載します。
情報収集モジュールの有無	使用している情報収集モジュールと収集している利用者情報について簡潔に記載します。
プライバシーポリシーの場所	概要ではなく、プライバシーポリシー本体の掲載場所を記載します。

＜プライバシーポリシー（本体）の記載事項＞

大項目	中項目
①　アプリケーション提供者名	（参照：5.1.情報を収集するアプリケーション提供者等の氏名又は名称）
②　アプリケーションで取り扱う利用者情報	（参照:5.2. 取得される情報の項目、5.3. 取得方法、5.4 利用目的の特定・明示、5.5.3 同意取得の対象、タイミング） ＜中項目＞

	・項目名 ・内容 ・取得方法 ・利用目的 ・同意取得の方法
③　パーミッションと利用目的	(参照：5.2.2 パーミッションと利用目的)
④　プライバシーポリシーの掲示場所	(参照：5.5.1 プライバシーポリシーの提示場所、5.5.2 プライバシーポリシー概要) ＜中項目＞ ・プライバシーポリシーの掲示方法 ・プライバシーポリシー概要提示場所
⑤　利用者関与の方法	（参照：5.5.4 利用者関与の方法） ＜中項目＞ ・サービス自体に利用される情報の利用者関与： –取得の中止 –利用の中止 ・広告に利用される情報の利用者関与 –取得の中止 –利用の中止
⑥　外部送信・第三者提供・情報モジュールの有無	（参照：5.6.1 第三者提供する場合の取扱い、5.6.2 情報収集モジュールを組み込む場合の取扱い） ＜中項目＞ ・サービス自体による利用者情報の第三者提供 ・情報収集モジュール（広告等）
⑦　問い合わせ窓口	（参照：5.7 問い合わせ窓口）
⑧　プライバシーポリシーの変更について	（参照：5.8 プライバシーポリシーの変更を行う場合の手順） ＜中項目＞ ・プライバシーポリシーの変更を行う場合の手順

6.1. プライバシーポリシーのサンプル（情報収集モジュールを組み込まない）

6.1.1. 利用者情報を外部送信しないアプリケーション

6.1.1.1. アプリケーション概要

QR コードを作成するアプリケーション

機能概要：

- ユーザーが入力した電話番号を QR コードとして画面に表示します。
- 電話帳から連絡先を 1 件選択して QR コードとして画面に表示します。
- 作成した QR コードはファイルとして外部メモリ（microSD 等）に保存する事ができます。

QR コードファイルを選択して表示する機能や、ご利用者の名前を QR コードに入れる機能は含まれておりません。

6.1.1.2. プライバシーポリシー概要

本アプリケーションは、QR コードを作成するために、ご利用者自身の入力及び電話帳から氏名、電話番号を取得しますが、これらのデータは一切サーバーに転送されません。
アプリケーションには広告等の情報収集モジュールは含んでいません。
プライバシーポリシーの詳細につきましては、
http://www.taosoftware.co.jp/android/qrcode/#privacy_policy を参照ください。
上記ＵＲＬへは、デベロッパー情報のプライバシーポリシーリンクから移動可能です。

6.1.1.3. プライバシーポリシー

①　アプリケーション提供者名

（参照：5.1.アプリケーションを収集するアプリケーション提供者等の氏名又は名称）

タオソフトウェア株式会社

②　アプリケーションで取り扱う利用者情報

（参照：5.2.取得される情報の項目、5.3 取得方法、5.4 利用目的の特定・明示、5.5.3 同意取得の対象、タイミング）

項目１：電話番号
内容：電話番号
取得方法：アプリケーションがご利用者からの操作により電話帳から取得する。

利用目的：アプリケーションの機能として
同意取得の方法：アプリケーション内での同意は行わない。プライバシーポリシーに記載。
（※１：連絡帳にアクセスしているが、 外部送信していないのでプライバシーポリシーに記載のみ）
その他：電話番号をアプリケーション内部で取り扱っておりますが、サーバーに送信する等、弊社で情報を取得する事はありません

項目２：電話番号
内容：電話番号
項目名３：ご利用者が入力した電話番号
取得方法：作成する QR コードの情報としてご利用者により入力される。
利用目的：アプリケーションの機能として
同意取得の方法：アプリケーション内での同意は行わない。プライバシーポリシーに記載
その他：電話番号をアプリケーション内部で取り扱っておりますが、サーバーに送信する等、弊社で情報を取得する事はありません

項目４：QR コード画像
内容：電話番号が含まれる QR コードを外部メモリ(microSD カード)に保存する
取得方法：ご利用者が操作した時にファイルとして保存する。
利用目的：アプリケーションの機能として
同意取得：なし
その他：作成した QR コード画像は、サーバーに送信する等、弊社で情報を取得する事はありません。SD カード上の QR コード画像は他のアプリケーションから取得可能です。

③　パーミッションと利用目的
(参照：5.2.2 パーミッションと利用目的)
WRITE_EXTERNAL_STORAGE
作成した QR コード画像を外部記憶装置にファイルとして保存するのに使用しております。
（※注 ご利用者が指示した電話番号を QR コードにするので、READ_CONTACTS は必要ない）

④　プライバシーポリシーの掲示場所
(参照：5.5.1 プライバシーポリシーの提示場所、5.5.2 プライバシーポリシー概要)

プライバシーポリシーの掲示方法：
ホームページに掲示

http://www.taosoftware.co.jp/android/qrcode/#privacy_policy

プライバシーポリシー概要提示場所:
アプリケーションの説明画面に記載

⑤　利用者関与の方法
（参照：5.5.4 利用者関与の方法）

サービス自体に利用される情報の利用者関与：
利用を取りやめるときは、アプリケーションをアンインストールしてください。アプリケーションで作成されたファイルは全て削除されます。
SD カードに保存した QR コードファイルもアプリケーションアンインストール時に自動的に削除されますが、SD カードが使用不可能な状態でアプリケーションをアンインストールした場合は、手動で削除してください。

広告に利用される情報の利用者関与：
広告は表示しておりません。

⑥　外部送信・第三者提供・情報モジュールの有無
（参照：5.6.1 第三者提供する場合の取扱い、5.6.2 情報収集モジュールを組み込む場合の取扱い）

サービス自体による利用者情報の第三者提供：
利用者情報を取得しておりません

情報収集モジュール（広告等）：
広告を含め、情報を収集するモジュールは使用しておりません。

⑦　問い合わせ窓口
（参照：5.7 問い合わせ窓口）

info@taosoftware.co.jp

⑧　プライバシーポリシーの変更について
（参照：5.8 プライバシーの変更を行う場合の手順）

プライバシーポリシーの変更を行う場合の手順：

「個別同意取得」が必要な、重要なプライバシーポリシーの変更はアプリケーション内でポップアップ表示させ再度「個別同意取得」致します。

「個別同意取得」が必要ないプライバシーポリシーの変更に関しては、弊社サイトで告知を致します。

6.1.2. 利用者情報取得するアプリケーション

6.1.2.1. アプリケーション概要

スーパー電話帳預かりサービス

機能概要：

- 携帯電話上の電話帳をサーバーにバックアップします。

携帯電話をなくした場合や機種変更した場合、サーバーに預けた電話番号を取得できます。

6.1.2.2. プライバシーポリシー概要

本アプリケーションは、電話帳に含まれる全てを取得し弊社サーバーに送ります。
これらのデータは本アプリケーション以外の目的には使用せず、第三者にも提供致しません。
アプリケーションには広告は含まれておりません。
プライバシーポリシーの詳細につきましては、http://www.taosoftware.co.jp/android/superphone/#privacy_policy を参照ください。
上記ＵＲＬへは、デベロッパー情報のプライバシーポリシリンクから移動可能です。

6.1.2.3. プライバシーポリシー

① アプリケーション提供者名

タオソフトウェア株式会社

② アプリケーションで取り扱う利用者情報

項目１：電話帳内の全てのデータ（氏名、電話番号、会社名他）
内容：電話帳内の全てのデータをバックアップします。
取得方法：ご利用者がバックアップボタンを押した後に取得する。
利用目的：アプリケーションの機能として
同意取得の方法：初回に電話帳を参照する時にダイアログを表示して同意を得る

項目２：ユーザーID、パスワード
内容：サーバーにユーザーアカウントを作成します。
取得方法：ご利用者の入力による。
利用目的：アプリケーションの機能として
同意取得の方法：アプリケーション内での同意は行わない。インストール前にプライバシ

ーポリシーを参照して同意したものとする。

③　パーミッションと利用目的

INTERNET
電話帳データをサーバーにアップロードするのに必要です。

④　プライバシーポリシーの掲示場所

プライバシーポリシーの掲示方法：
ホームページに掲示
http://www.taosoftware.co.jp/android/superphone/#privacy_policy

プライバシーポリシー概要提示場所：
アプリケーションの説明画面に記載

⑤　利用者関与の方法

サービス自体に利用される情報の利用者関与：

- 取得の中止：アプリケーションをアンインストールすることで可能
- 利用の中止：本サービスのウェブサービスにログインして、アカウントの削除を行ってください。サーバーに保存されているデータは全て削除されます。
- ご利用者が２年以上利用されなかった場合、メールにてご連絡をし、サービス継続の確認が取れなかった場合、利用を停止した物と判断し、本サービスはサーバーに保存されているデータは全て削除されます。

広告に利用される情報の利用者関与：
広告は表示しておりません。

⑥　外部送信・第三者提供・情報モジュールの有無

サービス自体による利用者情報の第三者提供：
取得したデータは第三者に提供する事は致しません。

情報収集モジュール（広告等）：
広告を含め、情報を収集するモジュールは使用しておりません。

本プライバシーポリシーに記載されている第三者以外への情報の提供は行いません。ただし次のいずれかに該当する場合を除きます。

1. 法令上の義務により開示を求められた場合。
2. 人の生命、身体または財産等の重大な利益を保護するために緊急に必要がある場合。
3. 公衆衛生の向上又は児童の健全な育成の推進のために必要がある場合。
4. 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する場合。

⑦　問い合わせ窓口

info@taosoftware.co.jp

⑧　プライバシーポリシーの変更について

プライバシーポリシーの変更を行う場合の手順：
「個別同意取得」が必要な、重要なプライバシーポリシーの変更はアプリケーション内でポップアップ表示させ再度「個別同意取得」致します。
「個別同意取得」が必要ないプライバシーポリシーの変更に関しては、弊社サイトで告知を致します。

6.1.3. 利用者情報を取得しないアプリケーション

6.1.3.1. アプリケーション概要

スーパー電卓

機能概要：

- 電卓アプリ

6.1.3.2. プライバシーポリシー概要

アプリケーションは利用者情報を取扱いません。アプリケーションに広告は表示されません。プライバシーポリシーの詳細につきましては、http://www.taosoftware.co.jp/android/tambourine/#privacy_policy を参照ください。上記 URL へは、デベロッパー情報のプライバシーポリシーリンクから移動可能です。

6.1.3.3. プライバシーポリシー

① アプリケーション提供者名

タオソフトウェア株式会社

② アプリケーションで取り扱う利用者情報

利用者情報は取り扱っておりません。

③ パーミッションと利用目的

パーミッションは利用しておりません。

④ プライバシーポリシーの掲示場所

プライバシーポリシーの掲示方法：

ホームページに掲示

http://www.taosoftware.co.jp/android/calc/#privacy_policy

プライバシーポリシー概要提示場所：

アプリケーションの説明画面に記載

⑤ 利用者関与の方法

サービス自体に利用される情報の利用者関与：
利用者情報は取り扱っておりません。

広告に利用される情報の利用者関与：
広告は表示しておりません。

⑥　外部送信・第三者提供・情報モジュールの有無

サービス自体による利用者情報の第三者提供：
利用者情報は取り扱っておりません。したがって、利用者情報を外部送信したり第三者提供することはありません。

情報収集モジュール（広告等）：
広告を含め、情報を収集するモジュールは使用しておりません。

⑦　問い合わせ窓口

info@taosoftware.co.jp

⑧　プライバシーポリシーの変更について

プライバシーポリシーの変更を行う場合の手順：
「個別同意取得」が必要な、重要なプライバシーポリシーの変更はアプリケーション内でポップアップ表示させ再度「個別同意取得」致します。
「個別同意取得」が必要ないプライバシーポリシーの変更に関しては、弊社サイトで告知を致します。

6.2. プライバシーポリシーのサンプル（情報収集モジュールを組み込む）

広告を扱うアプリケーション

6.2.1.1. アプリケーション概要

前述したサンプル「スーパー電話帳預かりサービス」と機能は同じで広告が含まれるパターン。

6.2.1.2. プライバシーポリシー概要

本アプリケーションは、電話帳に含まれる全てを取得し弊社サーバーに送ります。
これらのデータは本アプリケーション以外の目的には使用せず第三者にも提供致しません。
アプリケーションには広告が含まれますが、広告会社には電話帳データは送信されません。
プライバシーポリシーの詳細につきましては、http://www.taosoftware.co.jp/android/superphone/#privacy_policy を参照ください。
上記ＵＲＬへは、デベロッパー情報のプライバシーポリシーリンクから移動可能です。

6.2.1.3. プライバシーポリシー

（省略)...

④　利用者関与の方法

（参照：5-4 利用者関与の方法）

サービス自体に利用される情報の利用者関与：

- 取得の中止：アプリケーションをアンインストールすることで可能
- 利用の中止：本サービスのウェブサービスにログインして、アカウントの削除を行ってください。

広告に利用される情報の利用者関与：

- 取得の中止：アプリケーションをアンインストールすることで可能
- 利用の中止：XXX 社のサービスを利用しております。利用中止の方法に関しては、XXX 社（リンク記載）にお問い合わせください。

⑤　外部送信・第三者提供・情報モジュールの有無

サービス自体による利用者情報の第三者提供：

取得したデータは第三者に提供する事は致しません。

本プライバシーポリシーに記載されている第三者以外への情報の提供は行いません。ただし次のいずれかに該当する場合を除きます。

5. 法令上の義務により開示を求められた場合。
6. 人の生命、身体または財産等の重大な利益を保護するために緊急に必要がある場合。
7. 公衆衛生の向上又は児童の健全な育成の推進のために必要がある場合。
8. 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する場合。

情報収集モジュール（広告等）：

広告モジュール名：　ＹＹＹ広告モジュール
広告モジュール提供者名：株式会社ＸＸＸ
広告モジュールのプライバシーポリシー：http://xxx.xxx.co.jp/policy/
取得される項目：　広告を表示する毎に位置情報を取得します。
利用目的：　利用者にとって価値のある広告を配信するため
第三者提供の有無：　広告モジュールの説明に第三者への提供はないと記載されています。
（省略）...

7. まとめ

本ドキュメントでは、アプリケーション提供者は、「アプリケーション毎にプライバシーポリシーを策定すると共に、一定の情報の取得については個別の情報の取得について、「個別同意取得」を求める」ことを推奨します。

7.1. アプリケーションに関する事項

- 利用者情報の性質と種類、利用目的に応じて、利用者に対して①通知又は公表、あるいは、②個別同意取得（都度確認）を行うこと。

- プライバシーポリシーを作成して利用者に告知する（①通知又は公表）
  - 利用規約とは別にプライバシーポリシーを作る事
  - プライバシーポリシーはアプリケーション毎に作成すること
  - プライバシーポリシー概要を作る事
  - アプリケーション内からプライバシーポリシーを参照できるようにすること

- 3.2 個別同意取得が必要な利用者情報にある、プライバシー性が高い情報を取得し、サーバーに送る場合は、アプリケーション内でポップアップ許諾すること。
  （②個別同意取得（都度確認））

- 第三者提供の事実を告知すること。
  - 取得したデータを第三者に提供するかを明確にすること。

7.2. サーバーに関する事項

- サーバーでの利用者情報の取扱いについて。
  - 取得した利用者情報の利用期間を定め、使用が終わったら削除すること。
  - 現時点で目的が明らかでないデータは収集しないこと。
  - 利用者から取得し、サーバーで保存している利用者情報は、利用者の要求に基づき速やかに削除できるようにすること。

7.3. 第三者モジュールに関する事項

- 第三者モジュールを使用する時は、不正なモジュールでないかを確認する事
- 第三者モジュール（広告モジュール）が取るデータを明確にすること
- プライバシーポリシーに以下の項目を含める事
  - 組み込んでいる情報収集モジュールの名称
  - 情報収集モジュール提供者の名前
  - 取得される情報の項目

- 利用目的
- 第三者提供の有無等

- 第三者モジュールに利用者情報を送るときは全て、アプリケーション内でポップアップ許諾すること（②個別同意取得（都度確認））

8. Appendix

プライバシーポリシーの作成や「個別同意取得」以外についての情報

1. 適切な安全管理措置。
2. 情報収集モジュール提供者に関する特記事項。
3. 広告配信事業者に関する特記事項。

8.1. 適切な安全管理措置

- 取り扱う利用者情報が漏えい、減失又はき損の危険にさらされないように利用者情報の安全管理のために必要かつ適切な措置を講じる
- 利用目的に必要な期間に限り保存し、目標達成等により不要となった際には、適切に消去等の措置を行う物とする。
- 利用者がアプリケーションをアンインストールした事が判明した後のデータの保存期間、その後の処理等についてあらかじめ定めておくものとする。

対策：

アンドロイドアプリケーションの脆弱性対策については、「Android Security一安全なアプリケーションを作成するために」を参考にしてください。

8.2. 情報収集モジュール提供者に関する特記事項

アプリケーション提供者へ以下の情報を提供する、また変更があった場合はプライバシーポリシーを更新すると共に、重要な変更があった場合にもアプリケーション提供者へ通知するものとする。

1. 取得する情報の項目
2. 利用目的
3. 第三者提供の有無等

店頭でのアフィリエイトで使われているモジュールも該当します。アプリケーション作成者への正確な情報提供を行ってください。

8.3. 広告配信事業者に関する特記事項

アプリケーション提供者へ以下の情報を提供する、また変更があった場合はプライバシーポリシーを更新すると共に、重要な変更があった場合にもアプリケーション提供者へ通知するものとする。

1. 取得する情報の項目
2. 利用目的

3.　第三者提供の有無等

行動ターゲッティング広告を行う場合には、「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」二次提言における「配慮原則」を踏まえてされた自主的なガイドラインを本指針を踏まえて見直す事。

広告モジュールを開発側に提供する場合は、正確な情報提供を行ってください。「必要なパーミッションは特にありません」と情報と、広告モジュールがハングアップしない条件についてのみ情報提供し、実際はアプリケーションにパーミッションが付加されている場合はその範囲で取得できる情報を取得するといったモジュールはマルウェアとみなされます。（情報収集モジュールも同じです）（例えば、READ_CONTACTS パーミッションがアプリケーションに付いている場合だけ、電話帳からデータを収集する等）

8.4.　Google Play のデベロッパープログラムポリシー

2012 年８月１日に Google Play のデベロッパープログラムポリシーが変更になり、従来よりも厳しくなりました。この中で広告モジュールについても記載があります。

広告のポリシー
下記のポリシーは、アプリに実装され組み込まれるすべての広告に適用されます。Google Play で入手した Android アプリをすべてのユーザーに快適にご利用いただける環境を維持するために、下記のルールに従っていただくことが重要です。これらのポリシーは随時変更されますので、定期的にご確認ください。

デベロッパー向け利用規約はアプリ/拡張機能のユーザー エクスペリエンス全体に適用
Google のデベロッパー販売/配布契約とデベロッパー プログラム ポリシー（総称して「デベロッパー向け利用規約」とします）は、各アプリに加え、アプリに組み込まれている、またはアプリ経由で表示される、あらゆる広告やサードパーティ ライブラリにも適用されます。一貫性のある、ポリシーに準拠したわかりやすく公正なユーザー エクスペリエンスをユーザーに提供してください。

通常、コンテンツのレビューとデベロッパー向け利用規約に準拠しているかどうかの審査においては、広告もアプリの一部とみなされます。したがって、違法行為、暴力、露骨な性表現を含むコンテンツ、プライバシーの侵害などに関連するすべてのポリシーが適用されます。これらのポリシーに違反しない広告を利用してください。

また、アプリ自体のコンテンツのレーティングに適合しない広告も、デベロッパー向け利用規約に対する違反となります。

広告のコンテキスト
それぞれの広告がどのアプリに関連付けられているか、どのアプリに組み込まれているかなどを、ユーザーにわかりやすく明示する必要があります。広告が、ユーザーの認識や同意なしでデフォルト設定を変更したり、ショートカット、ブックマーク、アイコンなどをインストールしたりするなどの動作によって、広告外でユーザーの端末の機能を変更してはなりません。広告でそのような変更を行う場合には、どのアプリが変更を行ったのかをユーザーにわかりやすく明示する必要があります。さらに、端末で設定を調整する、アプリ内で広告表示設定を調整する、またはアプリを完全にアンインストールするといった方法のいずれかによって、ユーザーがその変更を簡単に元に戻せる必要があります。

システム通知や警告を装った広告は認められません。

交換条件としての広告表示
アプリの全機能の利用と引き換えに広告のタップや個人情報の送信をユーザーに強制することは、ユーザー エクスペリエンスの低下につながるため禁止されています。ユーザーが無条件に広告を非表示にできるようにしてください。

サードパーティの広告やウェブサイトの妨害
アプリに関連付けられた広告が、サードパーティ アプリの広告を妨害することがあってはなりません。

（引用 http://play.google.com/intl/ALL_jp/about/developer-content-policy.html）

今まで明示されていなかった、通知バーへの広告は禁止とされております。
アプリケーション提供者は、Google Play にアプリケーションを公開する場合が多いので、Google Play の規約を順守する必要があります。その場合広告モジュールもアプリケーションの一部とみなされるため Google Play の規約を順守する必要があります。

8.5. タオソフトウェア株式会社のプライバシーポリシー

弊社でリリースしているアプリケーションのプライバシーポリシーを記載します。参考にしていただけたらと思います。

アプリ名	プライバシーポリシーURL

tCallBlocking	http://www.taosoftware.co.jp/android/callblocking/
tWakeUpCallMaker	http://www.taosoftware.co.jp/android/wakeupcallmaker/
tWakeUpCall	http://www.taosoftware.co.jp/android/wakeupcall/
tGentleBoot	http://www.taosoftware.co.jp/android/gentleboot/
ラブ★タンバリン	http://www.taosoftware.co.jp/android/tambourine/
tSpyChecker	http://www.taosoftware.co.jp/android/spychecker/
tPacketCapture	http://www.taosoftware.co.jp/android/packetcapture/

■会社紹介

タオソフトウェア株式会社

2005 年創業の独立系ソフトハウス（http://www.taosoftware.co.jp）

サーバーサイドアプリケーション開発会社としてスタート。Google 社のアンドロイドに発表当初より着目し、研究開発を開始。現在はアンドロイド専業（受託開発）として、アンドロイド端末上で動作するアプリケーションやアンドロイド端末と連携して動作するサーバー側アプリケーションを数多く手がけている。

日経 BP 社主催 Android Application Award 2010 Spring にて「tWakeUpCallMaker」が大賞を受賞。

2010 年 5 月に、プログラミング不要でアンドロイドアプリを作成できる「DOROKURI」サービスを開始。

2012 年 1 月に、「Android Security 一安全なアプリケーションを作成するために」をインプレス社から出版（ISBN コード：978-4-8443-3134-6）。

記事執筆、講演など多数。

ブログ（開発者向け情報を発信）（http://www.taosoftware.co.jp/blog/）

■協力（テクニカルレビュー）

@typex20

アンドロイド黎明期から" 突然消失するかもしれないブログ"

（http://typex2.wordpress.com/　http://blog.2maru.com/）で、さまざまな端末のセキュリティに関する内容を記事として取り上げている。hack がライフワーク。

■履歴

日付	バージョン	変更点等
2012/10/9	V1.0	公開
2012/10/11	V1.1	タイトルに「アプリケーション」文字が入っていたのを修正、誤字、脱字修正
2012/01/17	V2.0	MCF の「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」（以降 MCF 版）を参照し加筆
		表紙を追加
		4.プライバシーポリシー作成 4.3 日本語以外のプライバシーポリシーを追記
		5-5-1 プライバシーポリシーの掲示場所、掲示方法 プライバシーポリシーの場所は、ウェブ上とアプリ内両方に置く事を推奨していましたが、ウェブ上に置く

		事を推奨に変更しました。
		5-5-1 プライバシーポリシーの掲示場所、掲示方法 プレインストールアプリのプライバシーポリシーの置き場所について記載を追加しました。
		5-5-4 利用者関与の方法 MFC 版に記載されていた、利用者情報の保存期間の記載を追加
		6-2-3 プライバシーポリシー MFC 版に記載されていた、利用者情報の保存期間の記載を追加
		5-5-6 外部送信・第三者提供・情報モジュールの有無 6-3 海外モジュールの取扱いを追記
		5-6-1 第三者提供する場合の取扱い 除外事項を追加（個人情報保護法の除外事項を追加）
		6 プライバシーポリシーサンプル 情報の第三者提供の除外事項を追加
		段付け修正、表現修正、文字校正実施（内容変更なし）