スマートフォン　プライバシー　イニシアティブ解説

ICT ERA + ABC 2012東北
2012年10月20日(土)
13:00～13:30 (30分)
開発　D会場（B棟 B202）
タオソフトウェア株式会社　谷口岳
@tao_gaku

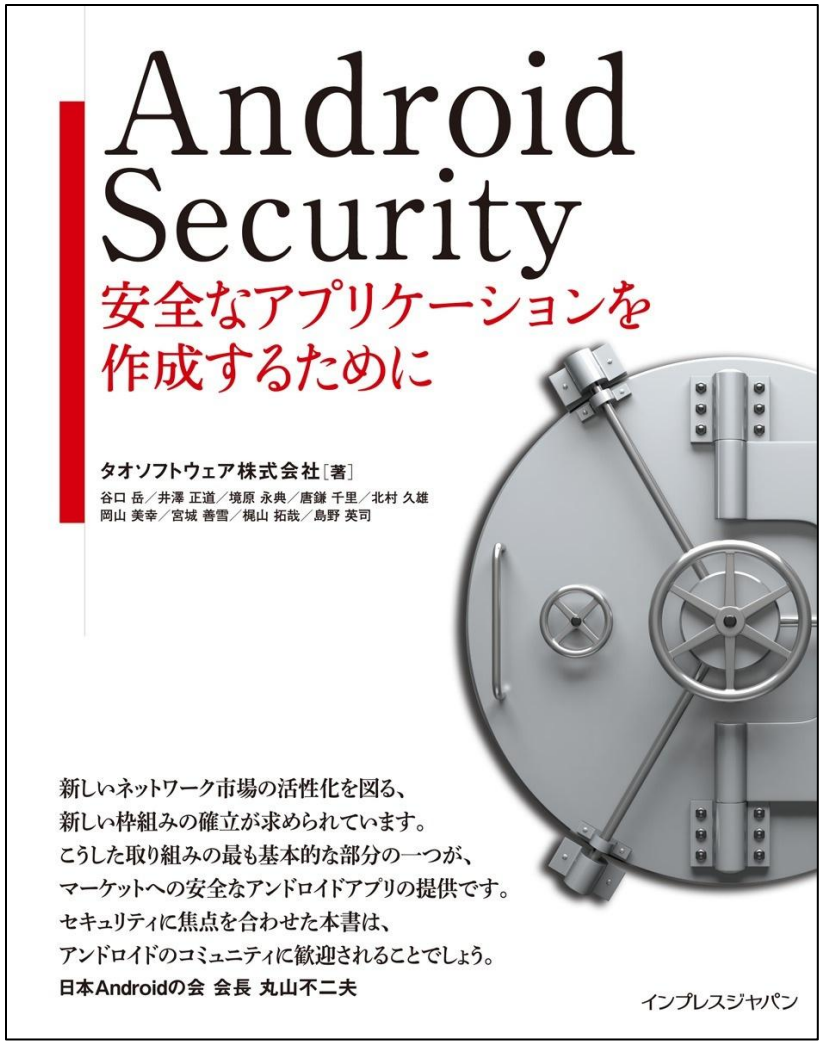
アプリケーション開発者/提供者向けです。

- 2012年8月に、総務省から「スマートフォン　プライバシー　イニシアティブ」が発表され、スマートフォンにおける、利用者情報の適切な取り扱い指針が示された。このドキュメントの解説と、アンドロイドアプリケーション提供者がこの指針に準拠するにはどうしたら良いのかをお話します。

タオソフトウェア株式会社

- 日本の会社（Android専業）
- 独立系ソフトハウス
- Android発表と共に研究開発を開始
- 現在Android専業（受託開発）
- Androidマーケットにアプリを多数公開
- ブログにて開発者向け情報を発信
  - http://www.taosoftware.co.jp/blog/
- 雑誌他執筆、講演
- Twitter @tao_gaku

Android Security
安全なアプリケーションを作成するために



- 2012年1月1日発刊
- プログラマ向け
- アンドロイドのセキュリティに関してプログラマが注意すべき点が多くあるが、あまり認知されていなかったので本の執筆を行った。

- 資料
  - http://www.taosoftware.co.jp/android/android_security/
  - パワポ資料及びビデオ
- Think IT
  - 1章、2章、3章を掲載
  - http://thinkit.co.jp/book/2012/03/05/3463
- Amazon
  - http://www.amazon.co.jp/dp/4844331345/
- 電子版(DRMフリー)
  - http://www.impressjapan.jp/books/3134
  - Google Play Books,達人出版

バザールやってます。アルテミスforNexusQ(ゲーム)
C棟　萩ホール　C-104

スマートフォン　プライバシー　イニシアティブ背景

スマートフォン　プライバシー　イニシアティブ

- 2012年8月　総務省よりリリースされたドキュメント
  - 概要(14ページ)
  - 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(119ページ)
  - http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

- 読者対象
  - 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

- 対象プラットフォーム
  - iOS搭載端末
  - アンドロイド搭載端末
  - 移動体通信事業者

2012/10/9公開
「アンドロイド　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」
Apache license2 無料

スマートフォン　プライバシー　イニシアティブのポイント

■ **スマートフォンの急速な普及**

平成23年度においてスマートフォンの国内出荷台数は2,417万台（携帯電話端末の総出荷台数の約57%）となり、平成23年度末の世帯普及率は約3割と1年前（約1割）の3倍となるなど急速に普及。

■ **アプリケーションによる端末内の利用者情報へのアクセス**

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。それらに対してアプリケーションがアクセスを行い、外部へ送信している場合があり、当該利用者情報の利用目的等が不明瞭な場合もある。

■ **利用者情報を十分な説明がないまま取得・活用するアプリも多く、利用者の不安が高まっている。**

「スマートフォン　プライバシー　イニシアティブ」の取りまとめ

■ **利用者情報の適正な取扱いとリテラシー向上による、スマートフォン市場の中長期的発展**

■ **利用者が安全安心にサービスを活用できるように、下記のようなスマートフォン・プライバシーに関する包括的な対策を提案する**

①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を中心に、アプリケーション提供サイト運営事業者・OS提供事業者、移動体通信事業者等のスマートフォンの関係事業者に広く適用可能な「スマートフォン利用者情報取扱指針」を示す

②第三者によるアプリ検証の仕組み等、指針の実効性を上げるための方策を提案

③利用者リテラシー向上のための情報提供・周知啓発方策

④国際連携の推進

総務省が言いたい事

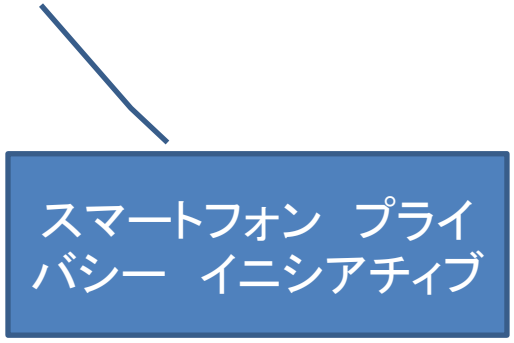
「個人情報の取扱いなど、スマートフォンの安心・安全な利用環境の確保のために事業者や業界団体自身による自主ガイドライン作成などを推進する活動を実施し、その取り組み状況を**フォローアップ**する」

1. 情報収集モジュールを組み込んだアプリケーションが、プライバシー問題があると指摘されていると認識した。

2. 現在問題があるが、禁止してしまうと、「市場が大きくなると予想される利用者情報に関するサービス」ができなくなってしまうので指針を示した。

3. 業界関係者できちんとしなさい。

4. きちんとしないと(~_~メ)



業界団体発足

- スマートフォンの利用者情報等に関する連絡協議会　(2012/10/4発足)
- 協議会メンバー
  - 日本スマートフォンセキュリティ協会
  - モバイルコンテンツフォーラム(MCF)
  - 電気通信事業者協会(TCA)
  - 日本Androidの会
  - インターネット広告推進協議会(JIAA)
  - 情報処理推進機構(IPA)
  - JPCERTコーディネーションセンター(JPCERT/CC)
  - 日本インターネットプロバイダー協会
  - オブザーバー（ドコモ、KDDI、ソフトバンク、電通、博報堂、経済産業省、消費者長、総務省等）
  - など、36の業界団体
- 第一回会議
  - 議長：慶應義塾大学総合政策学部准教授の新保史生氏
  - 副議長：英知法律事務所弁護士の森亮二氏
- 「これからスマートフォン関連の事業領域は中長期的に発展していく。このタイミングでは法規制ではなく民間の自主的な取り組みによって、安心安全な利用環境を整備していくことが望ましい」
- 年内に残り2回の会合を開く予定

スマートフォンの利用者情報等に関する連絡協議会設立案内
http://www.mcf.to/press_comment/pdf/spsc_press_20121004.pdf
「スマートフォンの利用者情報等に関する連絡協議会」が発足、業界ガイドラインの策定を促進
http://itpro.nikkeibp.co.jp/article/NEWS/20121004/427621/?top_tl1

アンドロイド的
スマートフォン　プライバシー　イニシアティブ内容

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

- 第一部
  - スマートフォンで利用者情報がどのように扱われているのか、具体事例や諸外国の動向、制度的な現状を述べている
- 第二部
  - 課題認識と具体的な対応
    - アプリケーション提供者は
      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り扱いのあり方」

利用者情報？

利用者情報とは

- スマートフォンにおける利用者情報とは、
  - 利用者の識別に係る情報
  - 電話帳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
  - 等の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

- 結局全ての情報
  - 電話帳データ、通話履歴、メールの内容、ネット観覧履歴、位置情報、IMEI，氏名、年齢、映像、写真、SNS利用履歴　.....

個人情報保護法

- 個人情報保護法
  - 間違った個人情報の概念
  - 5000件以下ならいいんじゃない？
  - 法人じゃなければいいんじゃない？
- プライバシー侵害について考える必要が出てきた

- お勧め、「個人情報」という言葉を使うと、法律があーだこーだという話にすぐになるので、「個人情報」という言葉を使わないのが吉
- 総務省ドキュメントでは「利用者情報」という言葉を使っている。

プライバシー侵害

- プライバシーに関して一般的に規定した法律はない
- プライバシー侵害にあたる可能性
  1. 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
  2. 一般人の**感受性**を基準にして公表されたくない情報を
  3. 本人の同意又は正当な目的なしに
  4. 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

感受性？？

スマートフォン利用者情報取得指針　基本原則

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。

利用者情報の取り扱い方法

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。

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。

個別同意取得

同意取得ダメな例

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表しているが
利用目的、外部送信・第三者提供の有無等の項目の記載がない

個別同意取得は、ポップアップダイアログを出す

個別同意取得が必要な一定の情報とは

- 個別の同意取得が必要な利用者情報かは以下から判断する。
  1. 利用者情報の性質と種類
  2. 利用者情報の利用目的による分類

利用者情報の性質と種類

- 個人情報そのもの、個人情報になりうる情報、個人識別性が高い情報
  - 氏名、年齢、電話帳、
- 利用者による変更が困難な情報
  - IMEI,Android_ID

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。

利用者情報の利用目的による分類

- アプリケーションのサービスのために情報を用いる時は、利用者にわかり易い
- 広告、利用状況把握等のために利用者情報を用いるのは、利用者にわかりにくい

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。

個別同意取得まとめ

	サービス目的内使用	サービス目的外使用
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
利用者の識別にかかわる情報	個別同意取得・通知又は公表	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・通知又は公表	個別同意取得
それ以外のプライバシーデータ	通知又は公表	個別同意取得

注）利用者情報を保存、外部通信する場合

プライバシーポリシー

プライバシーポリシーの作成要件

- 利用者情報を取得するしないにかかわらず、全てのアプリケーションで作成するのをおすすめ
- 総務省ドキュメントで必須とされていないパターンでも作成する理由
  - 利用者情報取得していない、外部通信していない事は、アプリケーションのアピールポイントとなる。
  - 利用者情報を取得、外部通信機能はあるが、利用者情報を外部に送信していない場合
    - 安心できるアプリなのにユーザにはわからず、もったいない

プライバシーポリシーの8つの記載内容

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	1. プライバシーポリシーの掲示場所、掲示方法 2. プライバシーポリシー概要 3. 同意取得の対象、タイミング 4. 利用者関与の方法
6. 外部送信・第三者提供・情報モジュールの有無	1. 第三者提供する場合の取り扱い 2. 情報収集モジュールを組み込む場合の取り扱い
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。

書きやすいように整理してみました

項目	例
① アプリケーション提供者名	1 アプリケーション提供者名
② アプリケーションで取り扱う利用者情報	2 取得される情報の項目 3 取得方法 4 利用目的の特定・明示 5-3 同意取得の対象、タイミング
③ パーミッションと利用目的	独自に追加
④ プライバシーポリシーの掲示場所	5-1 プライバシーポリシーの提示場所 5-2 プライバシーポリシー概要
⑤ 利用者関与の方法	5-4 利用者関与の方法
⑥ 外部送信・第三者提供・情報モジュールの有無	6-1 第三者提供する場合の取り扱い 6-2 情報収集モジュールを組み込む場合の取り扱い
⑦ 問い合わせ窓口	7 連絡先
⑧ プライバシーポリシーの変更について	8 プライバシーポリシーの変更を行う場合の手順

② アプリケーションで取り扱う利用者情報

個々の取得項目について以下をわかり易く記載する。

- 取得される情報の項目
  - パーミッション主体ではなく、メールアドレス、電話番号等具体的に記載する。
- 取得方法
  - 自動的にアプリが取得するのか、利用者入力によるかを記載する
- 利用目的の特定・明示
  - アプリ自体の目的に使用するか、アプリ以外の目的（広告等）に使用するかを記載する。
  - 取得したデータを第三者提供する場合はその旨記載する。
- 同意取得の対象、タイミング
  - アプリケーション内で個別同意取得ダイアログを出すのか出さないかを記載

③　パーミッションと利用目的

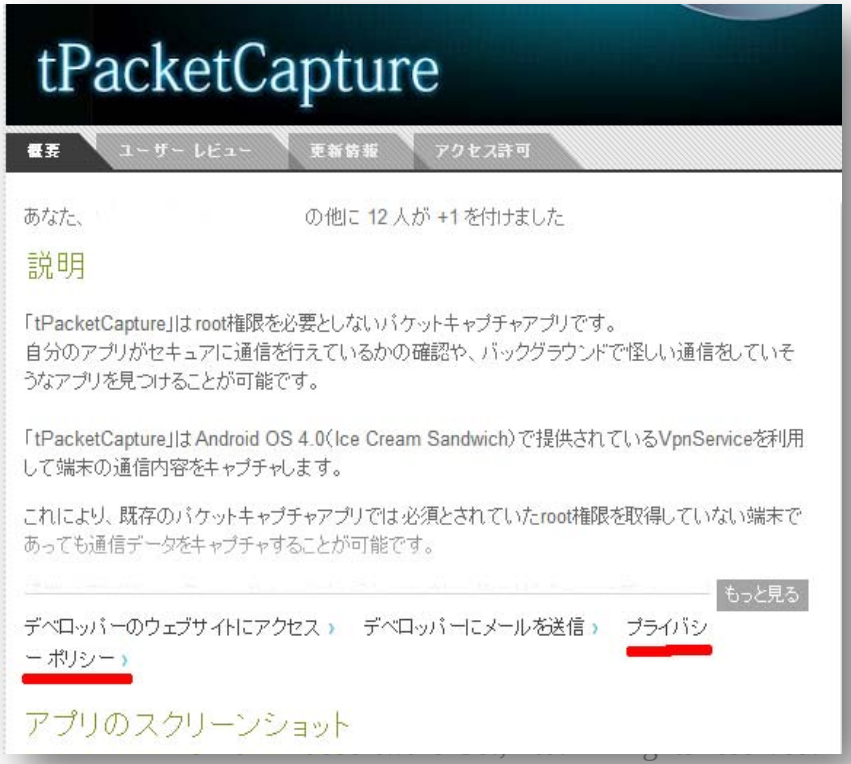
- 総務省のドキュメントには記載はないが、アンドロイドでは、パミッション情報はアプリケーションの特性を判断する重要な情報なので記載を行う。

- プロテクションレベルdangerousなパミッションについては必須
- プロテクションレベルnormalのパミッションについては推奨

④ プライバシーポリシーの掲示場所（1）

Google Play Developer Consoleの入力画面

Google Play Web上のプライバシーポリシーリンク（ブラウザで見た場合)

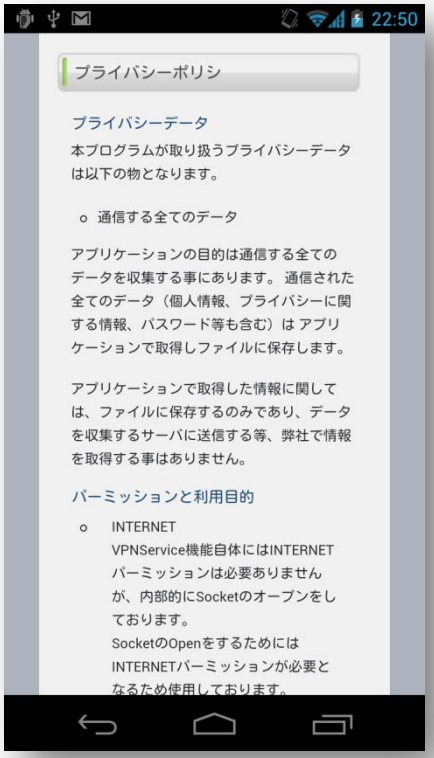


④ プライバシーポリシーの掲示場所（2）

GooglePlayアプリケーション上のプライバシーポリシー

プライバシーポリシーリンク画面

クリック後のプライバシーポリシー表示画面



④ プライバシーポリシー概要

- プライバシーポリシーを簡潔にまとめた文を、Google Playのアプリ説明に追加する。

例:

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 利用者関与の方法

- 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。
  - アプリケーションのアンインストール
  - サーバーにログインしてアカウント削除等
- 注意
  - 利用や取得の停止が出来ない物は作らない
  - アプリケーションを削除しても、情報の利用停止ができないものは作らない

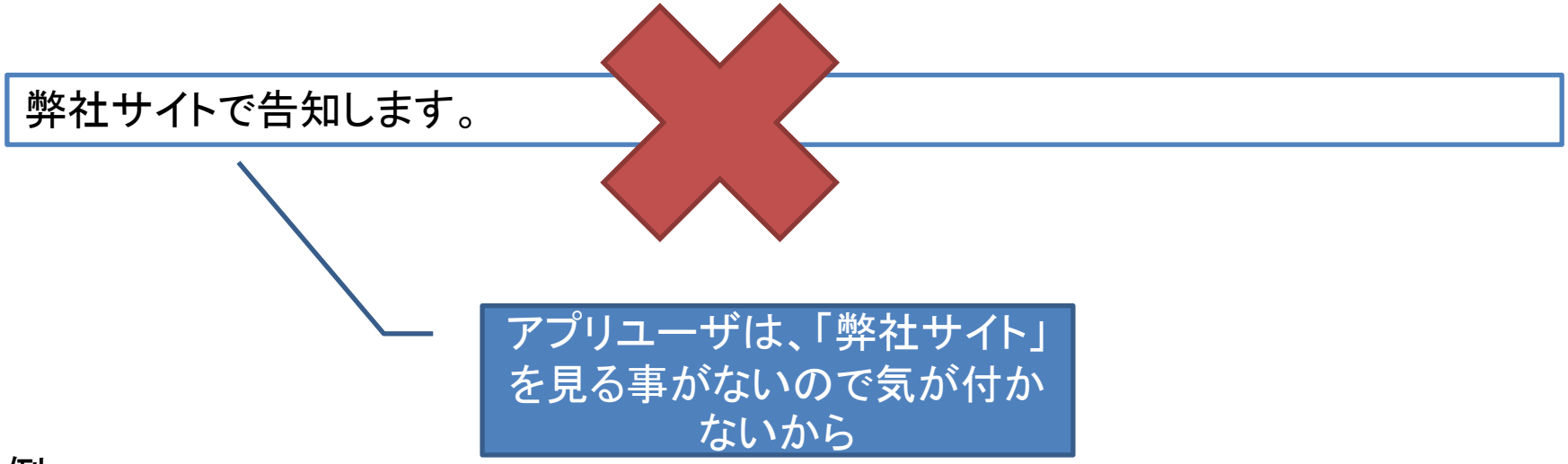
⑥ 外部送信・第三者提供・情報モジュールの有無

- 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。
  - 広告会社
  - 情報収集会社

- 第三者提供する場合の取り扱い
  - 第三者に提供する場合は、その記載を行う。

- 情報収集モジュール（広告等）を組み込む場合の取り扱い
  - モジュールに関して下記を記載する。
  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

⑧ プライバシーポリシーの変更について



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。

アンドロイド　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

- 本講演の内容は、このドキュメントに詳しく記載されています。
- 「アンドロイド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」は、総務省のスマートフォンプライバシーイニシアティブに沿って、アンドロイドのアプリケーションプログラマが、利用者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、公開が行えるよう支援することを目的として、アンドロイドのアプリケーションプライバシーガイドラインとしてまとめたものです。

- 多くの方に利用して頂けたらと思いApatch License2として無償にて公開致しております。
- 一つでも多くのアプリケーションがプリバシーポリシーを作成してもらえたらと思っております。
- 置き場所
  - http://www.taosoftware.co.jp/android/android_privacy_policy/

ありがとうございました。

ICT ERA + ABC 2012東北
2012年10月20日(土)
13:00～13:30 (30分)
開発　D会場（B棟 B202）
タオソフトウェア株式会社　谷口岳