Risk Finder
Powered by Taosoftware.

アプリを公開する前に、最低限知っておきたいセキュリティ事項

2015/4/25(土)
15:30-16:25 (55分)ROOM A

タオソフトウェア株式会社
代表取締役　谷口岳

@tao_gaku

Tao software

自己紹介：タオソフトウェアについて

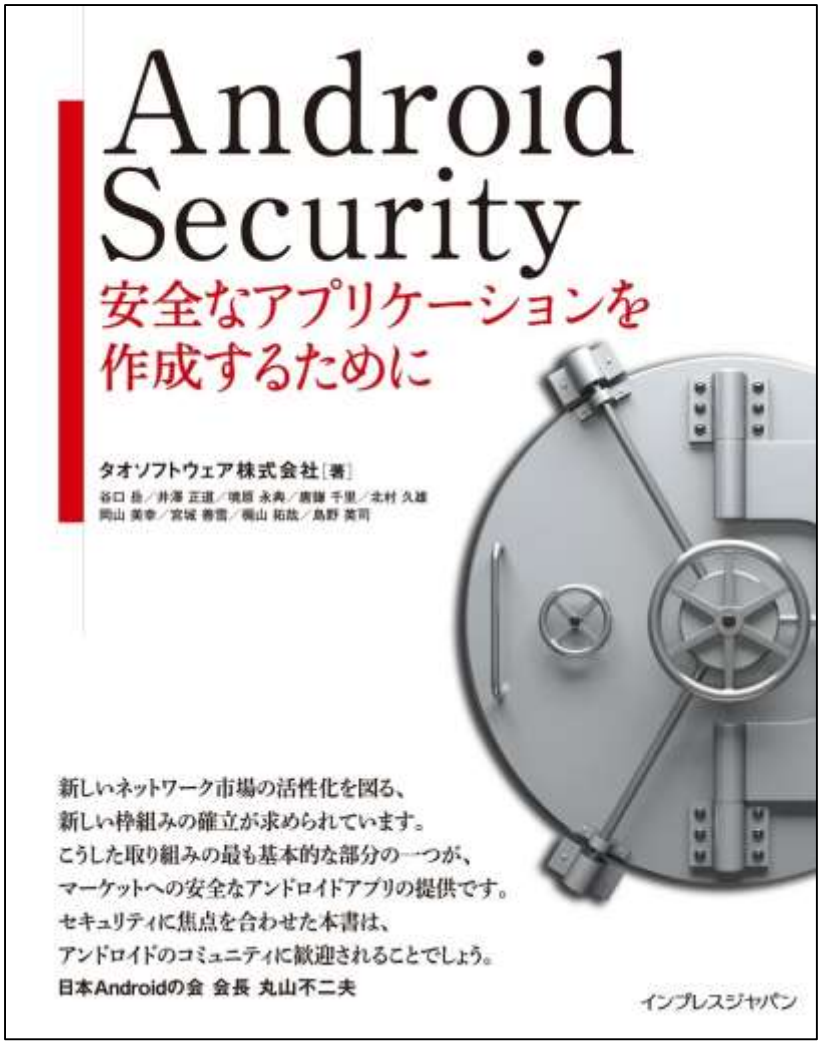
- 2005年創業　独立系ソフトハウス
- 代表取締役　谷口 岳
- Webアプリケーション開発会社としてスタート。Google社のAndroidに発表当初より着目し、研究開発を開始
- 現在Android専業（受託開発）
- Google Playにアプリを多数公開
- ブログにて開発者向け情報を発信
  - http://www.taosoftware.co.jp/blog/
- 雑誌他執筆、講演など

タオバイザー

3DVRゴーグル

- クラウドファンディングで資金調達
- アマゾンで絶賛販売中
- http://taovisor.com

Android Security 安全なアプリケーションを作成するために

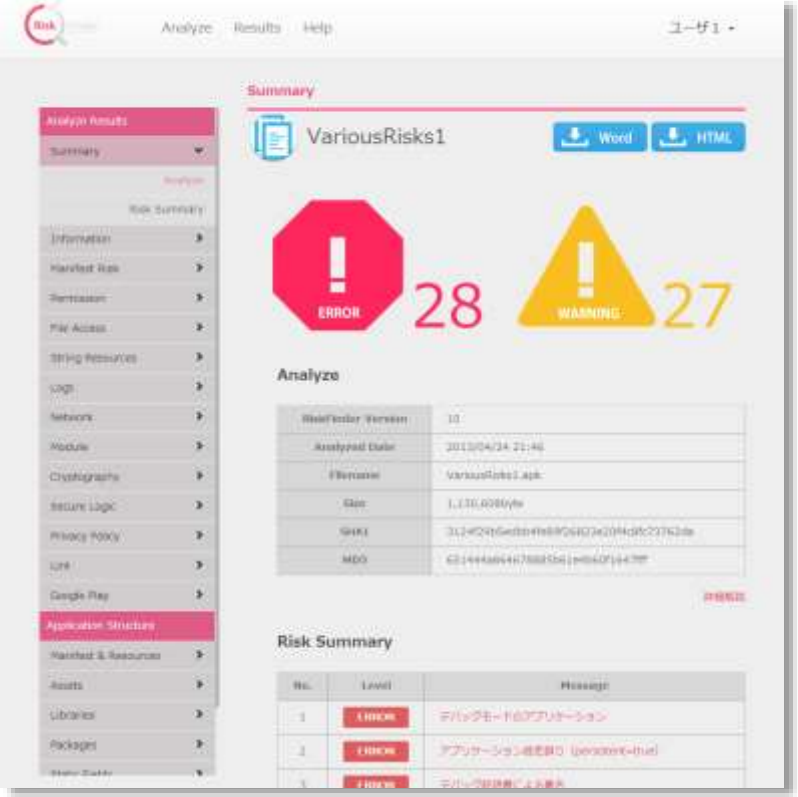


- 2012年1月1日発刊
- 開発者向け
- 出版社：インプレスジャパン
- Amazonにて絶賛販売中

Tao RiskFinder（脆弱性発見ツール）

APKファイルをアップロードするだけで脆弱性レポートが作成されます。

講演をする中で、
「気を付ける事が沢山あるのは分かった。
でも全てのプログラマが理解するのは
難しい
何かいい方法はないか？」
という声があったので作ってみました。



1. プログラマでなくても使える
2. ソースコード不要
3. ウエブサービス型
4. 脆弱性以外も検出

http://riskfinder.com/

Doroid Kaigi 講演内容

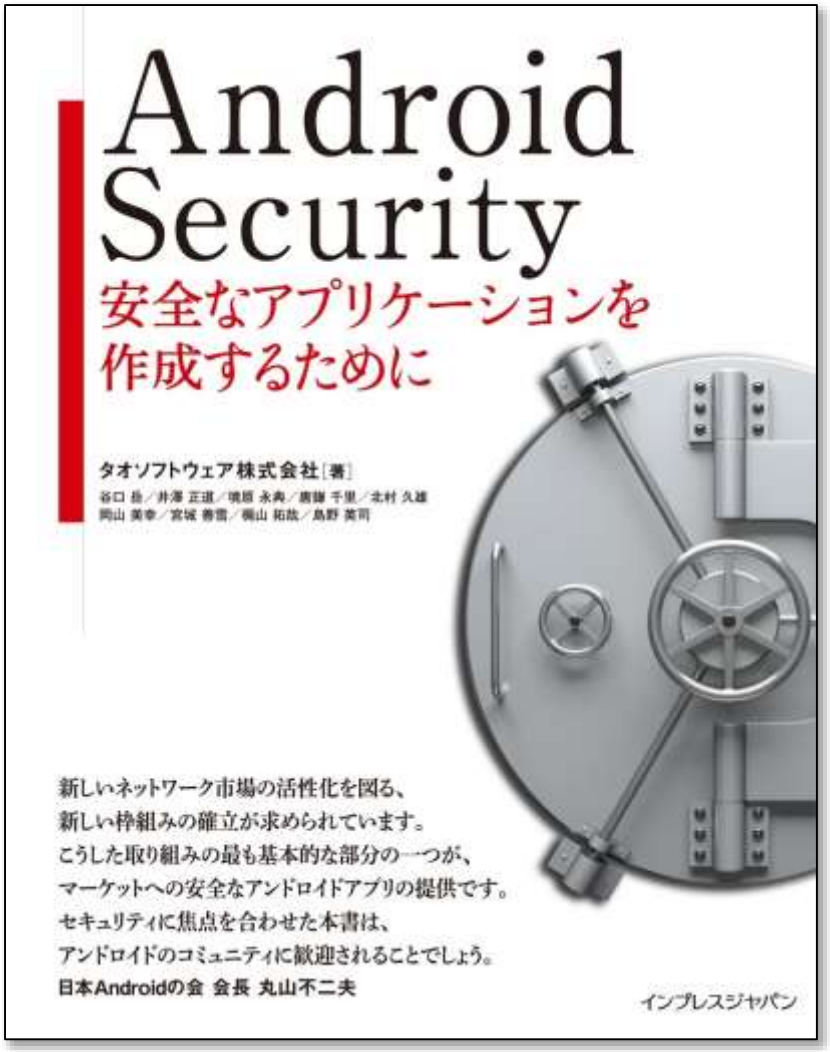
- セキュリティホールがあるアプリケーションをを作らないようにするために、やりがちな例をあげながら、その対応策について解説致します。また、不正のないアプリがマルウェアに間違われる事、他人の作成したライブラリを使用したために、意図せずマルウェアになってしまう事もあります。個人情報の取扱い等、知っているだけで防げる例が数多く存在します。アプリを公開する人に最低限知ってもらいセキュリティに関する事項をお話します。

目次

- セキュリティの学習方法
  - 2冊のセキュリティ本
  - AnCole
- 最低限知っておきたい事
  - ファイルアクセス
  - コンポーネントアクセス
  - HTTPS通信
  - 不必要なパミッション
- 第三者モジュールに注意
  - ライセンス、脆弱性、マルウェア、プライバシー
- プライバシポリシ
  - プライバシーポリシーを作成
  - 何の情報を何の目的で取得するのか、また第三者提供について
  - ダイアログによる同意取得

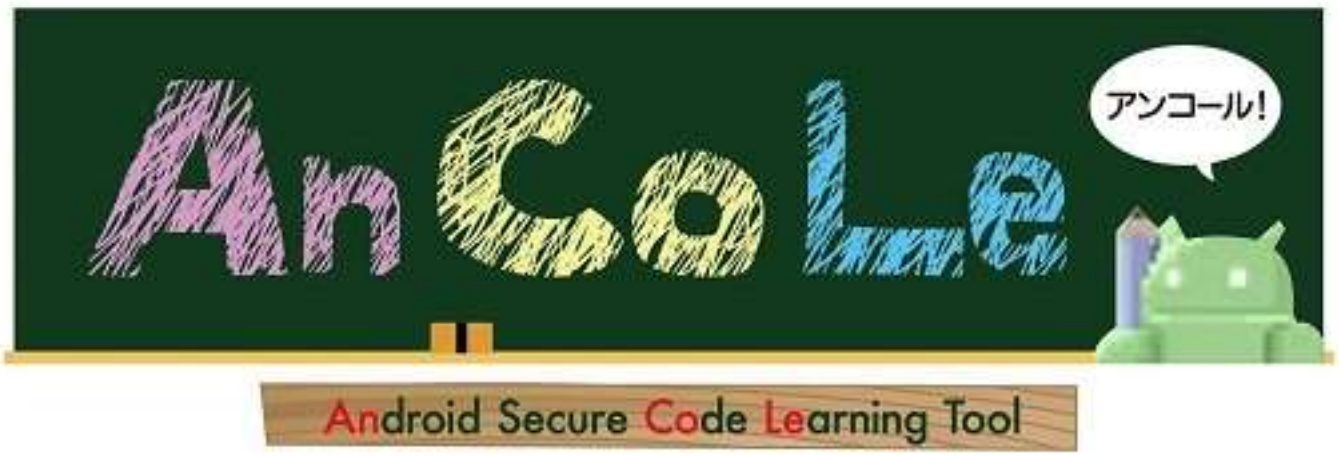
セキュリティの学習方法

日本語で読める本



About AnCoLe

- Androidアプリの開発者を対象とした、脆弱性が作り込まれてしまう原因や対策について実習形式で学べるツール
- IPA提供　無料
- ダウンロード
  - http://www.ipa.go.jp/security/vuln/ancole/index.html



特徴

- 必要な物
  - Windows OS
  - Eclipse（Eclipseのプラグインとして提供）
  - Android SDK等アプリ開発に必要な物
- 何ができるか
  - 学習コンテンツ
    - 読み物
    - 脆弱性アプリに対する攻撃実習
  - 点検機能
    - 自分のアプリに脆弱性がないか点検ができる

デモ

7つの学習テーマ

1. ファイルアクセス制限の不備
2. コンポーネントのアクセス制限不備
3. 暗黙的Intentの不適切な使用
4. 不適切なログ出力
5. WebViewの実装不備
6. SSL通信の実装不備
7. 不必要な権限の取得

上記テーマに複数のシナリオが入っており
計11の項目について学習できる

最低限知っておきたい事

今回説明する物

1. ファイルアクセス制限の不備
2. コンポーネントのアクセス制限不備
3. ~~暗黙的Intentの不適切な使用~~
4. ~~不適切なログ出力~~
5. ~~WebViewの実装不備~~
6. SSL通信の実装不備
7. 不必要な権限の取得

1. ファイルアクセス制限の不備

1. 内部ストレージのアクセス制限不備
2. Preferenceファイルのアクセス制限不備
3. SDカードのファイルアクセス制限の理解不足

問題点

- セキュアデータの漏えい
- 不正な外部コードの読出し(LoadDex)

解決方法

ファイルを作成する時にファイルのアクセス権限を指定しない（デフォルトでOK）

外部記憶装置（SDカード）は、他のアプリから読み取れるので、セキュアな情報はおかない。

2.コンポーネントのアクセス制限不備

1. 非公開コンポーネントのアクセス制限不備
2. 公開コンポーネントのアクセス制限不備
3. CotentProviderのアクセス制限不備

問題点

- Activityの乗っ取り
- ContentProviderからのデータ読み込み

解決方法

- コンポーネントは、外部非公開(export=false)にする

6.SSL通信の実装不備

1. セキュリティ例外の無視

問題点

- サーバの正当性が保証できなく、偽装サーバのアクセス、中間者攻撃が防げない

原因：開発時にテストサーバ（オレオレ証明サーバ）を使うと、例外を無視するように実装しないと動かない→リリース版でもそのまま

解決方法

- 例外無視コードは最後に削除
- なるべく早くに本番サーバーを立てる

くわしくはこちら

- デブサミ2015 事例から学ぶAndroidアプリのセキュアコーディング「SSL/TLS証明書検証の現状と対策」
  http://www.slideshare.net/jpcert_securecoding/androidssltls

7.不必要な権限の取得

- マルウェアと誤解される可能性のあるPermissionの使用

問題点

- マルウェアと間違えられる。
- 第三者モジュールにパミッションを使われる
- プライバシーポリシーとの矛盾

解決方法

- パミッションは最低限にする

第三者モジュール

第三者モジュールとは

- 他者が作成したライブラリで、アプリに組み込んで使用をする。
- 通信ライブラリ、パーサ、広告モジュール等様々な物が存在する。
- Gitでソースコードが公開されているものから、企業の製品まで様々な物がある。

使用上の注意

1. ライセンス感染
2. 脆弱性感染（造語）
3. マルウェア感染（造語）
4. プライバシー情報感染（造語）

ライセンス感染

- **ライセンス感染**
  - コピーレフトな著作物、主にソフトウェアを利用する場合において、原著作物のライセンスがその二次的著作物にも適用されることを比喩的に表現したスラングである。
- GPL汚染
  - GPL由来のソースコードが何らかの理由によって他のライセンスのソフトウェアに混ざることにより、ソフトウェア全体にGPLが適用されてしまう事

問題点

- ソフトウェアのソースコードを公開する必要が出てくる等
- そもそも商用不可等

WikiPedia ライセンス感染:
http://ja.wikipedia.org/wiki/%E3%83%A9%E3%82%A4%E3%82%BB%E3%83%B3%E3%82%B9%E6%84%9F%E6%9F%93

脆弱性感染

- もしも第三者モジュールに脆弱性があったら
  アプリケーションにも脆弱性がある事になる。

問題点

第三者モジュールの脆弱性を確認するのは難しい

FacebookSDKの脆弱性 (ログ出力)

- ライブラリがログを出力する事がある。
- 事例
  - 2012年4月 Facebook SDKでログイン時のアクセストークンがログに出力されていた。
  - http://jp.techcrunch.com/archives/20120410security-hole-spotted-in-facebook-android-sdk-long-tail-apps-may-still-be-unpatched/

OpenSSLの脆弱性

- 深刻度 – 高 (Severity: High)
  - OpenSSL 1.0.2 ClientHello sigalgs DoS (CVE-2015-0291)
  - Reclassified: RSA silently downgrades to EXPORT_RSA [Client] (CVE-2015-0204)
- 深刻度 – 中 (Severity: Moderate)
  - Multiblock corrupted pointer (CVE-2015-0290)
  - Segmentation fault in DTLSv1_listen (CVE-2015-0207)
  - Segmentation fault in ASN1_TYPE_cmp (CVE-2015-0286)
  - Segmentation fault for invalid PSS parameters (CVE-2015-0208)
  - ASN.1 structure reuse memory corruption (CVE-2015-0287)
  - PKCS7 NULL pointer dereferences (CVE-2015-0289)
  - Base64 decode (CVE-2015-0292)
  - DoS via reachable assert in SSLv2 servers (CVE-2015-0293)
  - Empty CKE with client auth and DHE (CVE-2015-1787)
- 深刻度 – 低 (Severity: Low)
  - Handshake with unseeded PRNG (CVE-2015-0285)
  - Use After Free following d2i_ECPrivatekey error (CVE-2015-0209)
  - X509_to_X509_REQ NULL pointer deref (CVE-2015-0288)

JVNVU#95877131：OpenSSL に複数の脆弱性
https://jvn.jp/vu/JVNVU95877131/

マルウェア感染

マルウェアと認定される広告モジュールが入っていたら、そのアプリはマルウェア。

- 広告モジュールが電話帳を参照して勝手にサーバに送っていないか？
- 電話帳を送るのは流石に少ないが、以下の物は良く送られている。
  - 電話番号
  - IMEI
  - ANDROID_ID
  - アプリ一覧
- 海外広告モジュールに特に注意

プライバシー問題

- 第三者モジュールがプライバシーデータを勝手に取得して送っている事がある
- アプリケーションのプライバシーポリシーに、第三者モジュールも含めたプライバシーデータの取得、取扱いに記載する必要があるが、第三者モジュールが何のデータを収集している記載されてらず記載できない
- 広告モジュールの営業さんに確認すると、「大丈夫です」と言われる。（何が大丈夫かわからない）

どんな広告モジュールを使えばよいか

- アンドロイダー、広告モジュール認定制度を開始　総務省スマートフォンプライバシーイニシアティブに準拠　国内広告事業社9社が参画
- https://androider.jp/topic/media/history/20140801/

アンドロイダー公認広告モジュール

i-mobile for SP i-mobile 運営：株式会社アイモバイル	2.0.2	・位置情報(位置情報を利用しているアプリケーションの場合のみ取得) ・インストール済みのアプリ情報(外部送信なし)	準備中
asterisk アスタ 運営：株式会社マルジュ	アイコン型 1.2.1 ウォール型 1.1.1	なし	-
AppVador AppVador 運営：アップベイダー株式会社	1.1.0	・IMEI(端末識別番号)	詳細はこちら
AdLantis AdLantis 運営：Glossom株式会社	1.5.7	なし	-
AppliPromotion AppliPromotion 運営：株式会社AMoAd	-	なし	-
appC cloud appC cloud 運営：カイト株式会社	1.1.6	・Googleアカウント ・インストール済みのアプリ情報(外部送信なし) ・ストレージ等のユーザーコンテンツの読み込み	詳細はこちら
AID AID 運営：ライヴエイド株式会社	1.2.1	なし	-

GAME FEAT GAME FEAT 運営：株式会社フルセイル	3.3.0	・インストール済みのアプリ情報	準備中
nend nend 運営：株式会社ファンコミュニケーションズ	2.4.0	・インストール済みのアプリ情報(外部送信なし)	詳細はこちら
BEAD BEAD 運営：ビヨンド株式会社	1.3.4	・インストール済みのアプリ情報(外部送信なし)	詳細はこちら
goodAD™ goodAD 運営：株式会社レボラボ	20140612	・インストール済みのアプリ情報(※CVしたアプリのパッケージ名のみ送信) ・独自ID、もしくはcookieのストレージへの書き込み(※ハッシュ化した上で送信)	詳細はこちら

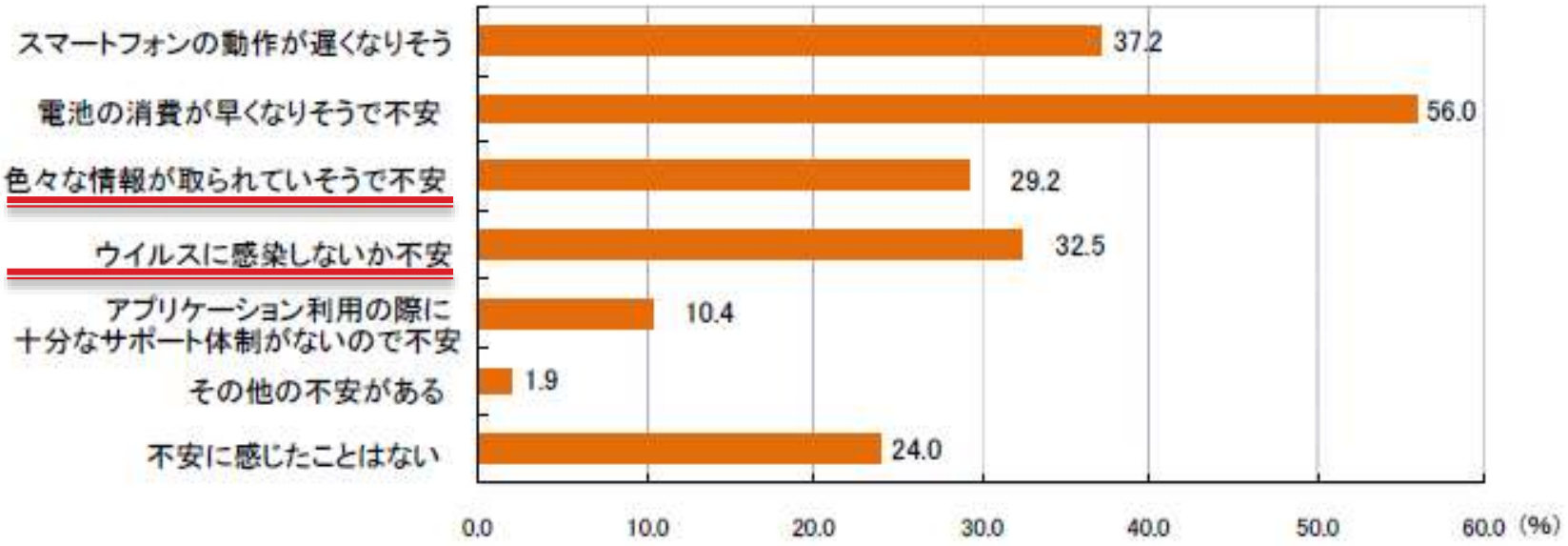
- アンドロイダー公認広告モジュールについて
- http://blog.androider.jp/dev/archives/3087

プライバシ問題

【図表2-11： アプリケーション利用に関する不安】

・76 %のユーザーがアプリケーションの利用に関して何らかの不安を感じている
・不安を感じる主な理由は、「電池の消費速度への影響」、「端末動作速度への影響」といった端末の性能に係わるものが多い
・ユーザー情報を取得されることやウィルスへの感染に対して不安を感じるユーザーは、約3割である

アプリケーション利用に対する不安
スマートフォン上でダウンロードしたアプリケーションを利用して不安と感じたことがありますか
ある場合、どのような不安を感じたことがありますか（不安に感じた場合のみ複数回答）



参考資料：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
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

安心して使用できるアプリかの判断が難しい

- ユーザの情報を取得しているが、正しい目的のために取得しているのかわからない
- ウイルスチェックツールも検出不能

アプリ提供者は、どうしたらいいのか？！

総務省からの指針

- 総務省の指針に沿って、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。
- 1. プライバシーポリシードキュメントの作成
- 2. 重要な情報を取得する時にダイアログでユーザに同意を求める。

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作りました。無料公開(ApacheLicense2)
http://www.taosoftware.co.jp/android/android_privacy_policy/

参考資料:アプリビジネスで転ばないためのスマートフォンプライバシーの基礎知識

- 印刷書籍版 2520円
- 電子書籍版 1680円
- インプレスR&D
- ISBN:978-4-8443-9536-2
- http://www.amazon.co.jp/gp/product/484439536X/
- 寺田 眞治
  - 一般社団法人モバイル・コンテンツ・フォーラム常務理事

参考資料：一般社団法人モバイル・コンテンツ・フォーラム（MCF）

- 2012年11月13日
  - 「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」策定公開
  - http://www.mcf.to/temp/sppv/mcf_spappp_guidline.pdf
- MFC
  - 約217社コンテンツプロバイダー中心のモバイルコンテンツ業界団体

同意取得ではない例

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以下の項目の記載がない

- 利用目的
- 外部送信
- 第三者提供の有無

個別同意取得は、ポップアップダイアログを出す

総務省の動き

- 2012/8「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～」
  - 個人情報及びプライバシーを保護しつつアプリ提供者等がスマートフォンにおける利用者情報を適切に取り扱うための具体的な指針
- 2013/9「スマートフォン　プライバシー　イニシアティブII」
  - 利用者情報の適切な取扱いがなされているかどうか等を、運用面・技術面から第三者が検討する仕組みの提言
- 2014/5スマートフォン プライバシー アウトルック
  - 第三者検証の仕組みを構築するに当たっての諸課題について具体的な検討
- 2015/4スマートフォン プライバシー アウトルックII
  - プライバシーポリシーの作成・掲載に係る実態調査を行うとともに、第三者検証に係る実証実験
- Next
  - 引き続き第三者検証実運用に向けた検討

参考資料:「スマートフォン プライバシー アウトルックIIの公表
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000168.html

個人情報保護法

- 法に反していなければ問題ないは間違い
- 海外展開にも注意
- プライバシー侵害について考える
- 自分の子供や親が安心して使えるかを考える

- TIPS：
  「個人情報」という言葉を使うと、法律がという話になり進展しないので、「個人情報」という言葉は使用しない
- 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。

注意

- 利用規約と一緒にしない
- 会社のプライバシーポリシーと同じにしない
- 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。

まとめ

まとめ

- セキュリティの学習方法
  - 2冊のセキュリティ本
  - AnCole
- 最低限知っておきたい事
  - ファイルアクセス
  - コンポーネントアクセス
  - HTTPS通信
  - 不必要なパミッション
- 第三者モジュール
  - ライセンス、脆弱性、マルウェア、プライバシー
- プライバシポリシ
  - プライバシーポリシーを作成
  - 何の情報を何の目的で取得するのか、また第三者提供について
  - ダイアログによる同意取得

ありがとうございました。

タオソフトウェア株式会社