安心安全なモバイルアプリを公開するために

～DevOps and Mobile　2013/8/1～

C5

#devsumiC

谷口岳

@tao_gaku

17:15分～18:00（45分）

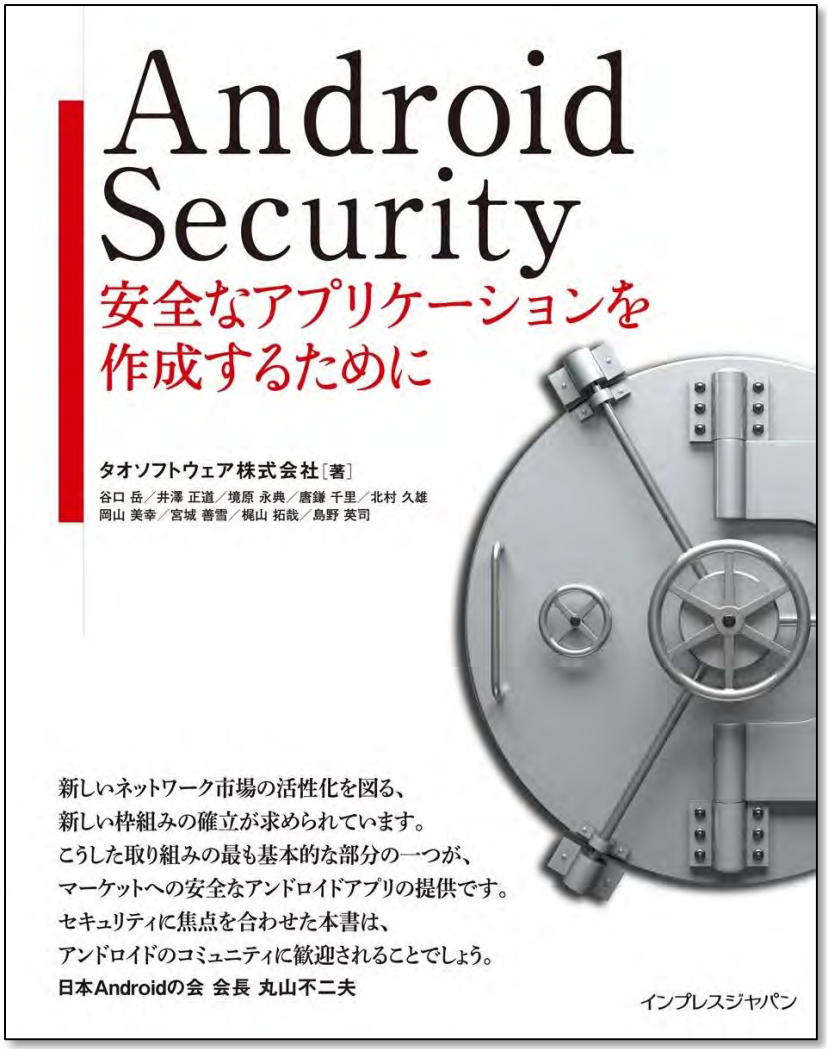
タオソフトウェア株式会社

代表取締役

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



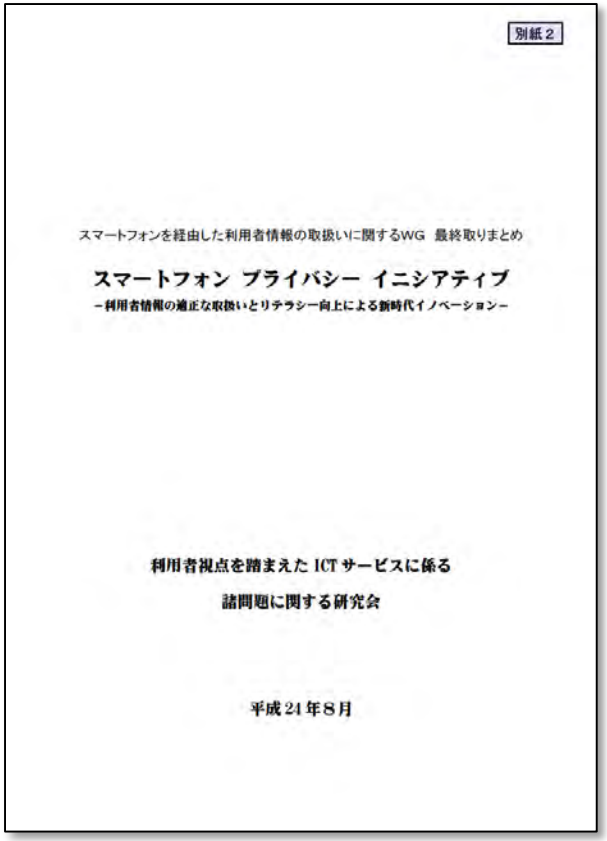
- 2012年1月1日発刊
- 開発者向け
- アンドロイドのセキュリティに関して開発者が注意すべき点が多くあるが、あまり認知されていなかったので本の執筆を行う。
- 資料
  - http://www.taosoftware.co.jp/android/android_security/
  - パワポ資料及びビデオ
- Think IT
  - 1章、2章、3章を掲載
  - http://thinkit.co.jp/book/2012/03/05/3463
- Amazon
  - http://www.amazon.co.jp/dp/4844331345/
- 電子版(DRMフリー)
  - http://www.impressjapan.jp/books/3134

JSSEC セキュアコーディングガイド

- 2012年06月11日
  - 第1版の作成に深く関わる
  - ドキュメント
    - http://www.jssec.org/dl/android_securecoding.pdf
  - サンプルコード
    - http://www.jssec.org/dl/android_securecoding.zip
- JSSEC
  - 日本のキャリアやハードメーカ等が集まって作成されたセキュリティに関する団体

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

- 2012年8月 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」が公開された
- これをアンドロイドアプリ用に再編集して独自のプライバシーガイドラインを作成・公開


別紙２

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 最終取りまとめ

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－

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

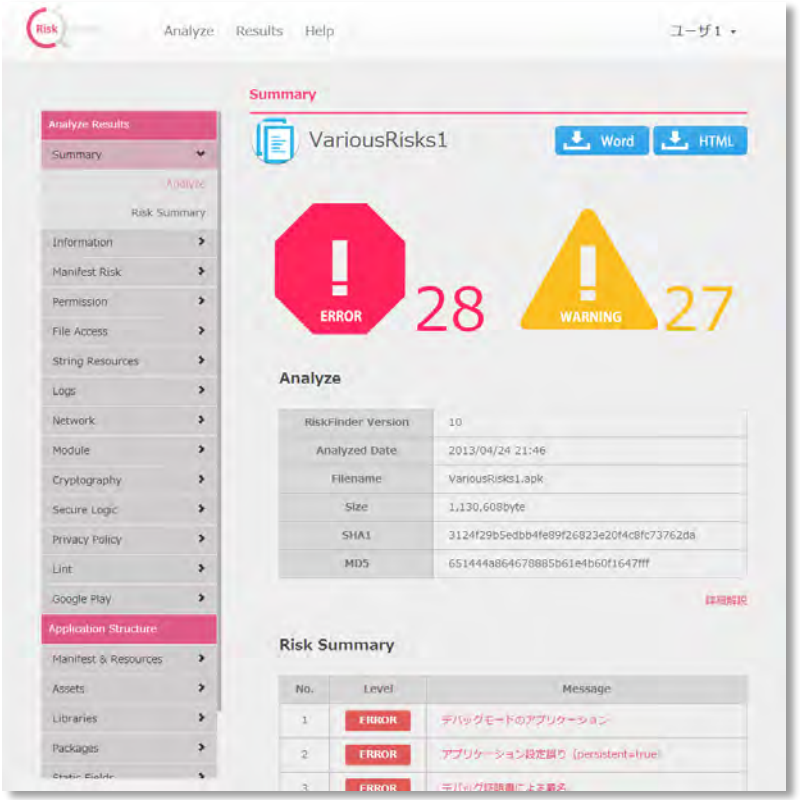
平成24年8月

アンドロイドアプリ開発者が
わかりやすいように
再編集

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://www.taosoftware.co.jp/services/riskfinder/

安心安全なモバイルアプリを公開するために

安心安全なモバイルアプリを公開するために

- スマートフォンの利用者情報を盗むようなアプリがある一方、正当な理由により利用者情報を取得するアプリもあります。しかしながらユーザにとっては区別がつかず非常に不安を与えているのが現状です。

  このような状況の中、アプリケーションの開発者は、どのようにしたら、「安心安全なアプリケーション」をユーザに届けられるでしょうか。

  本公演では、アンドロイドの話が主体となりますが、他のモバイルプラットフォームでも参考になるようにお話をしたいと思っております。

1. 安心できるアプリケーションを公開する方法

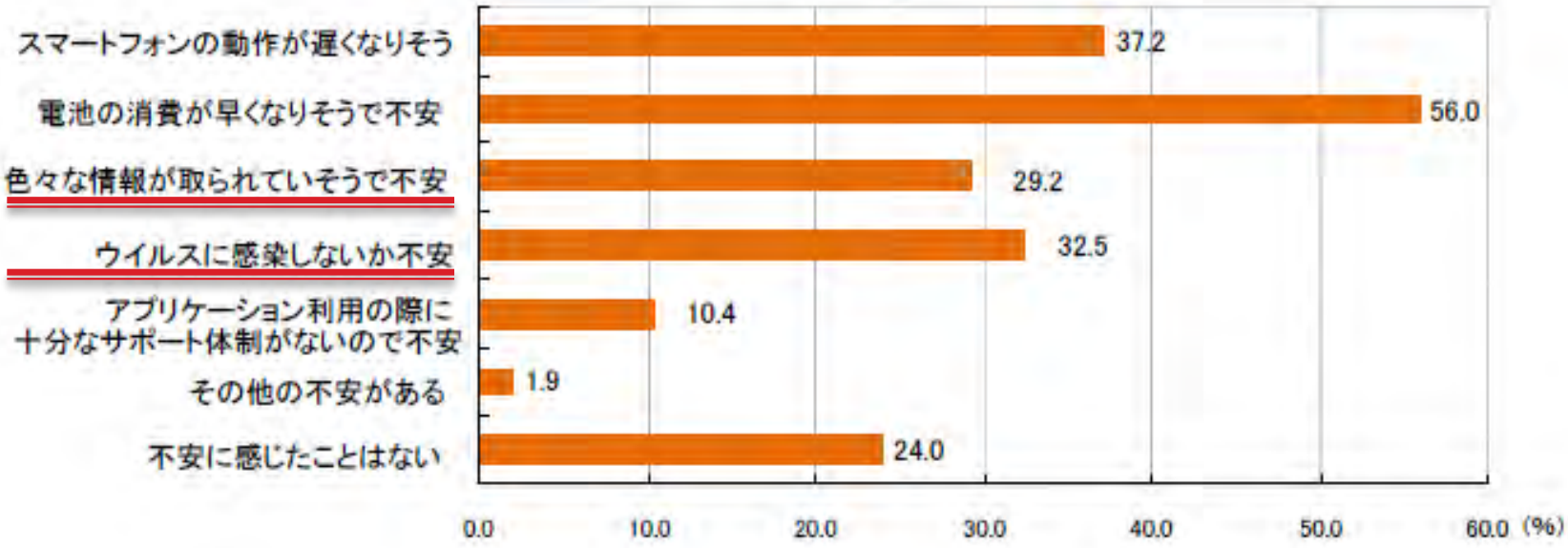
2. 安全なアプリケーションを作る方法

安心できるアプリケーションを公開する方法

【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

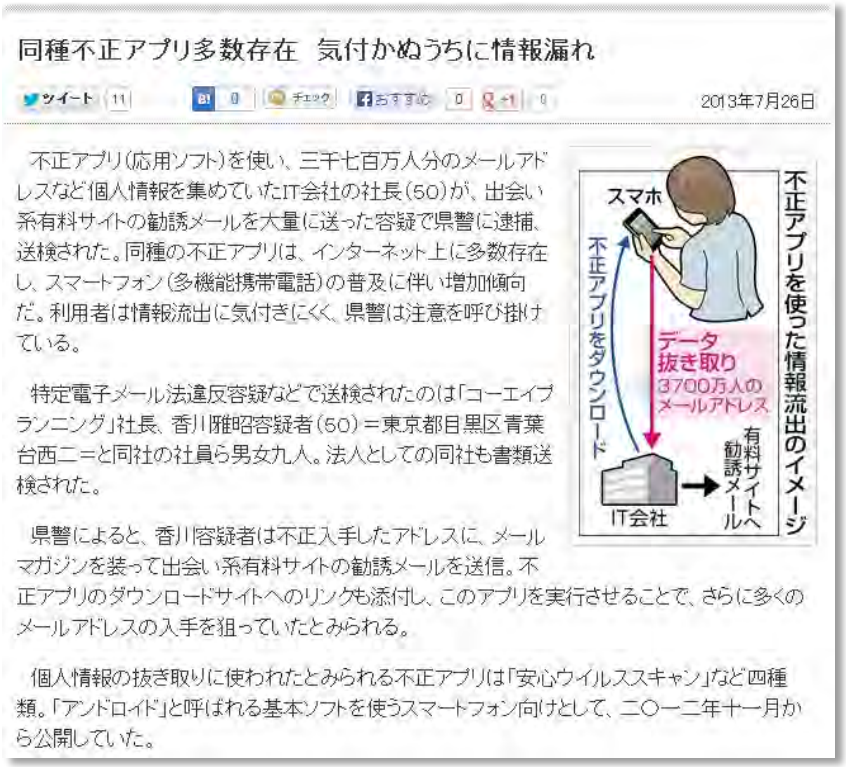
アプリケーション利用に対する不安
スマートフォン上でダウンロードしたアプリケーションを利用して不安と感じたことがありますか
ある場合、どのような不安を感じたことがありますか（不安に感じた場合のみ複数回答）



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

事例:安心ウイルススキャン

- 2013/7/26:不正アプリ(応用ソフト)を使い、三千七百万人分のメールアドレスなど個人情報を集めていたIT会社の社長(50)が、出会い系有料サイトの勧誘メールを大量に送った容疑で県警に逮捕、送検された



同種不正アプリ多数存在　気付かぬうちに情報漏れ

ツイート 11　B! 0　チェック　おすすめ 0　+1 0　2013年7月26日

不正アプリ(応用ソフト)を使い、三千七百万人分のメールアドレスなど個人情報を集めていたIT会社の社長(50)が、出会い系有料サイトの勧誘メールを大量に送った容疑で県警に逮捕、送検された。同種の不正アプリは、インターネット上に多数存在し、スマートフォン(多機能携帯電話)の普及に伴い増加傾向だ。利用者は情報流出に気付きにくく、県警は注意を呼び掛けている。

特定電子メール法違反容疑などで送検されたのは「コーエイプランニング」社長、香川雅昭容疑者(50)＝東京都目黒区青葉台西二＝と同社の社員ら男女九人。法人としての同社も書類送検された。

県警によると、香川容疑者は不正入手したアドレスに、メールマガジンを装って出会い系有料サイトの勧誘メールを送信。不正アプリのダウンロードサイトへのリンクも添付し、このアプリを実行させることで、さらに多くのメールアドレスの入手を狙っていたとみられる。

個人情報の抜き取りに使われたとみられる不正アプリは「安心ウイルススキャン」など四種類。「アンドロイド」と呼ばれる基本ソフトを使うスマートフォン向けとして、二〇一二年十一月から公開していた。

東京新聞 http://www.tokyo-np.co.jp/article/chiba/20130726/CK2013072602000146.html

PCと異なり携帯電話は個人情報の宝庫

- 電話帳をサーバに送る人
  - 名簿屋さん
  - ソーシャル電話アプリ

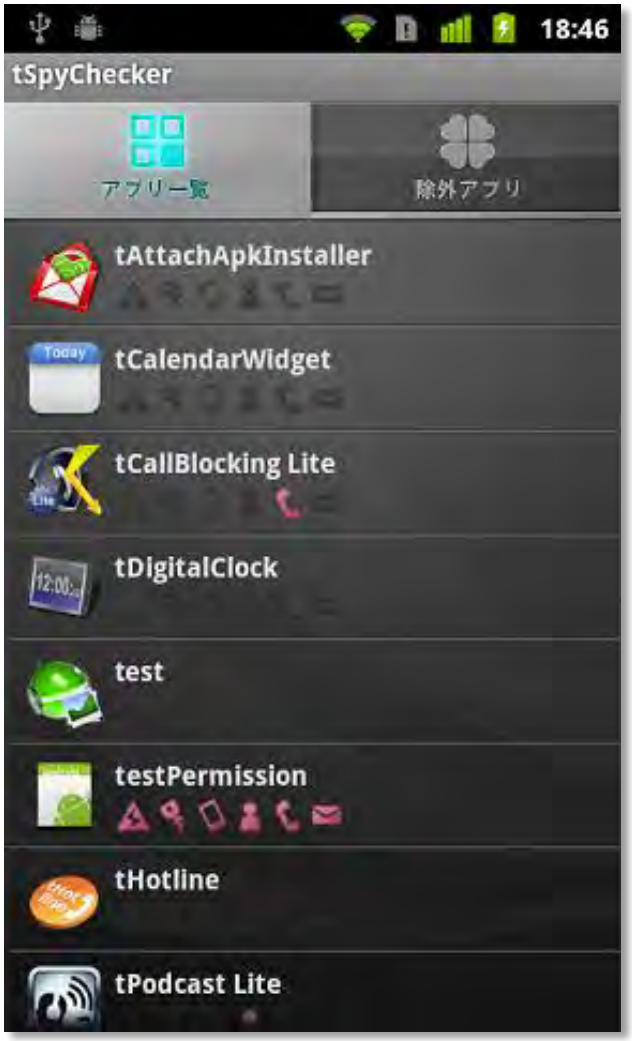
危険か区別しずらい。

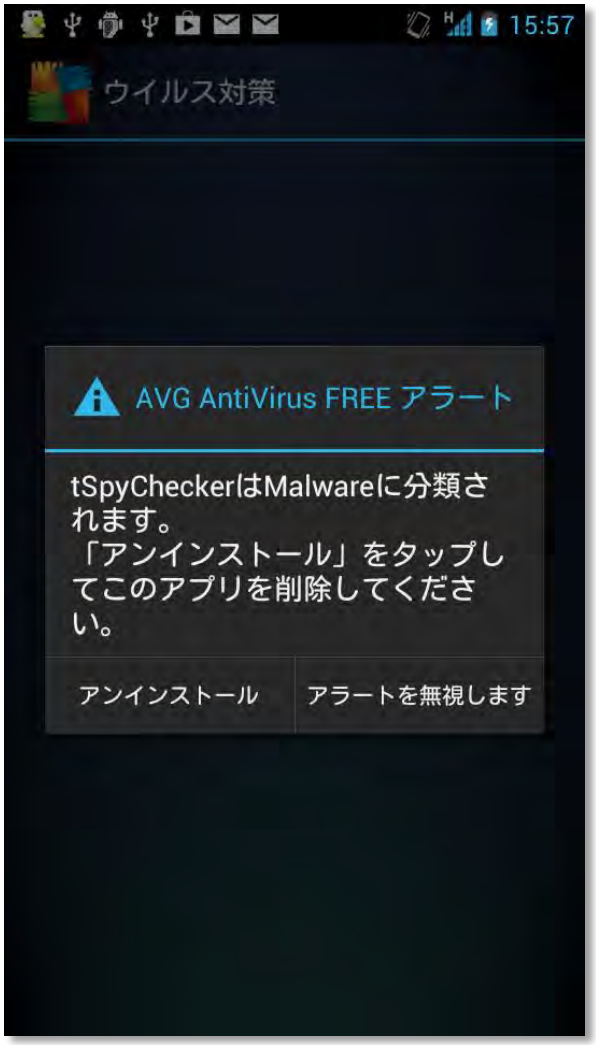
- 広告屋さん
  - 個人に特化した広告を出すことができる
  - 渋谷にいるなら、渋谷近辺の広告を出す
  - 女性には女性向けの広告を出す
  - 年齢別の広告を出す
  - 子供がいる家庭には子供向け広告を出す

現在問題になってます。
現在進行中…

- PCアプリの時はウイルスチェックアプリに任せておけばよかったが、怪しそうなグレーのアプリが多いため、判断が難しい

事例:間違えられました！？





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間違える

間違えられないようにするには、
どうしたらいいのか？！

スマートフォン　プライバシー　イニシアティブ

- 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」（SPI)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。
  - http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

スマートフォンの利用者情報等に関する連絡協議会（SPSC）が設立された。

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)

スマートフォン　プライバシー　イニシアチィブ

スマートフォンイニシアティブII

- 2013年7月3日に、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提言「スマートフォン安心安全強化戦略」（案）に対する意見募集が開始された。
- 8月2日まで
- その後、募集した意見を踏まえて正式公開

国が出した資料ということは、説得力があるので社内でうまく使える

何をやれば良いか

- 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告知

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：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

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

1. 同意取得

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

同意取得ダイアログ

- 以下の2点から同意取得ダイアログを出すかを決める
- 「利用者情報の性質と種類」
  - 個人情報になりうるもの
  - 個人識別性が高い物
  - 利用者による変更が困難な物（IMEI,Android ID…）
- 「利用者情報の利用目的」
  - アプリケーションの主目的以外の情報に関しては同意取得をする。

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

- 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。

2. プライバシーポリシーの作成

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

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。

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。
5. 通知・公表又は「同意取得」の方法、利用者関与の方法	1. 同意取得の対象、タイミング 2. 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。

プライバシポリシの配置

プライバシーポリシー設定

Google Play Developer Consoleの入力画面

プライバシーポリシーの表示

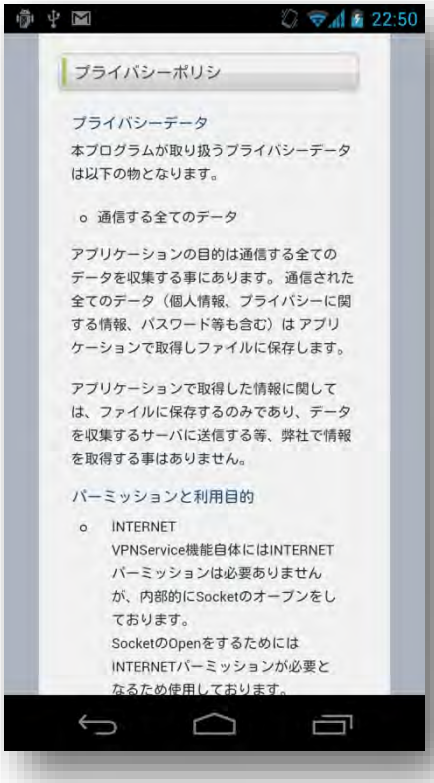
Google Play Web上のプライバシーポリシーリンク(ブラウザで見た場合)

プライバシーポリシーの表示

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

プライバシーポリシー表示画面



プライバシーポリシー概要

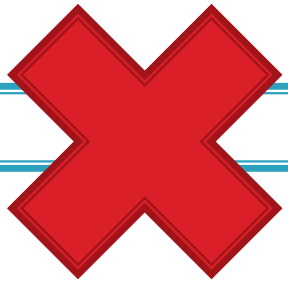
- プライバシーポリシーを簡潔にまとめた文を、Google Playのアプリ説明に追加する。

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。

プライバシーポリシーの変更について

弊社サイトで告知します。



アプリユーザは、「弊社サイト」を見る事がないので気が付かないから

例：

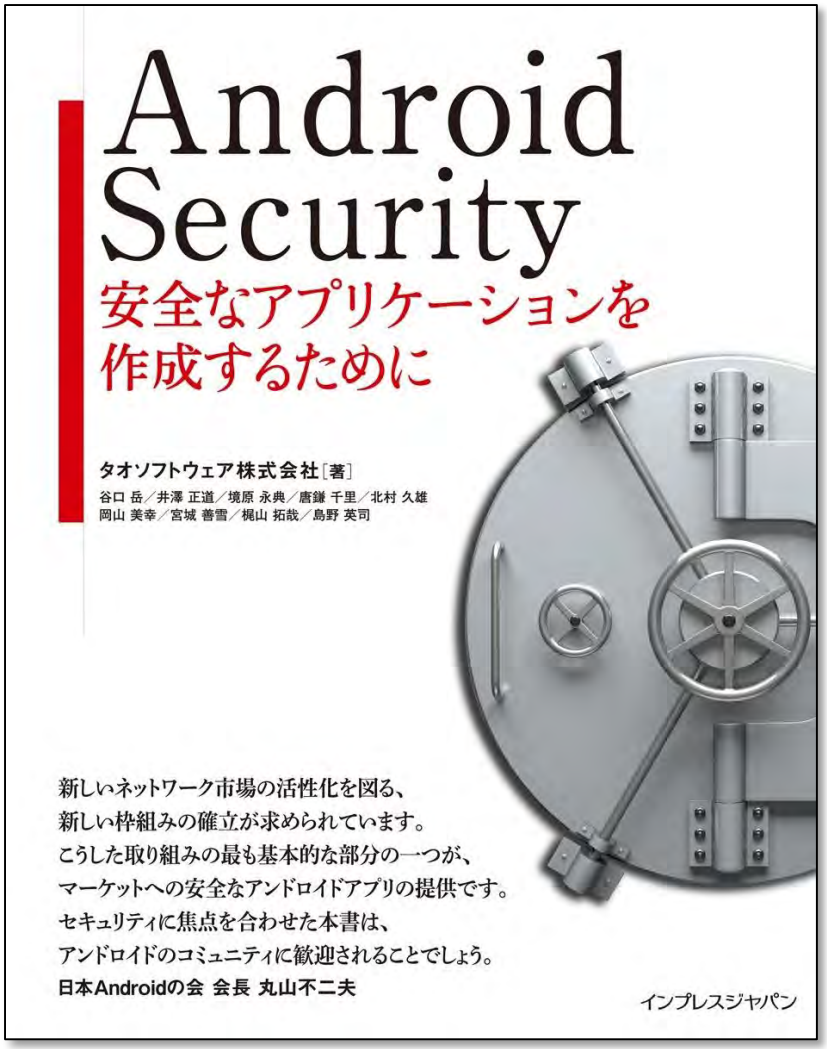
プライバシーポリシーの変更を行う場合の手順：

「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。

安全なアプリケーションを作る方法

アンドロイドのセキュリティ本は2冊



Tao RiskFinder アンドロイドアプリの脆弱性を診断するウエブサービス。

APKファイルをアップロードするだけでレポートが作成されます。

1. 解析結果はダウンロードできます
2. アイコンでエラー数、警告数を表示します
3. リスク
示し

- アプリケーションファイルのみでレポートを出力します。(ソースコードは必要ありません)
- 静的解析のみ行います。動的解析(アプリケーションを実行しての解析)は行いません

リスクレベ	
ERROR	
WORNING	
CONFIRM	
INFO	情報レベル

広告！

http://www.taosoftware.co.jp/services/riskfinder/

Androidアプリ脆弱性の内訳

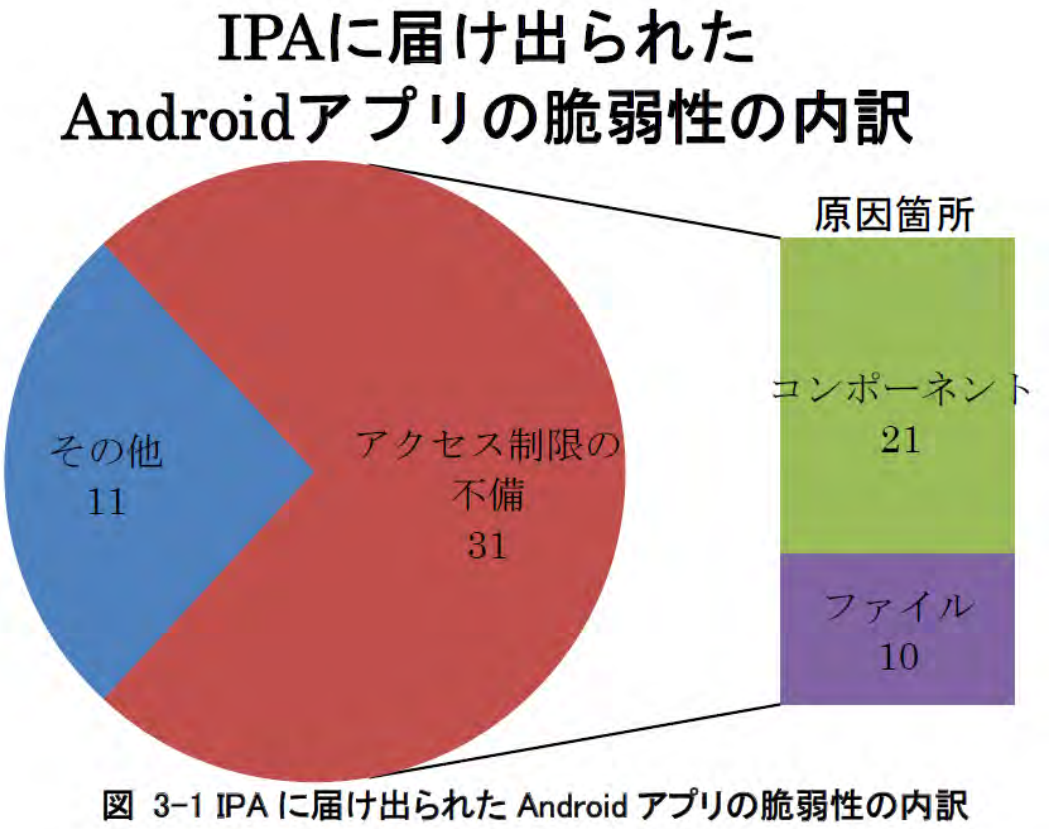


図 3-1 IPA に届け出られた Android アプリの脆弱性の内訳

- IPAに届け出られるAndroidアプリの脆弱性関連情報も増加傾向にある。届け出られた脆弱性は、アクセス制限の不備に関するものが7割以上であった。さらに分析した結果、これらはAndroidの仕組みを理解し、適切にアクセス制限の設定をしていれば防ぐことのできる脆弱性であることがわかった。(2012/6)

『Androidアプリの脆弱性』に関するレポート
http://www.ipa.go.jp/about/technicalwatch/20120613.html

最低限覚えておきたいこと

- 1. コンポーネントの脆弱性
- 2. ファイルの脆弱性
- 3. 広告モジュール

見つかりやすい脆弱性
かつ
知って入れば簡単回避できるもの

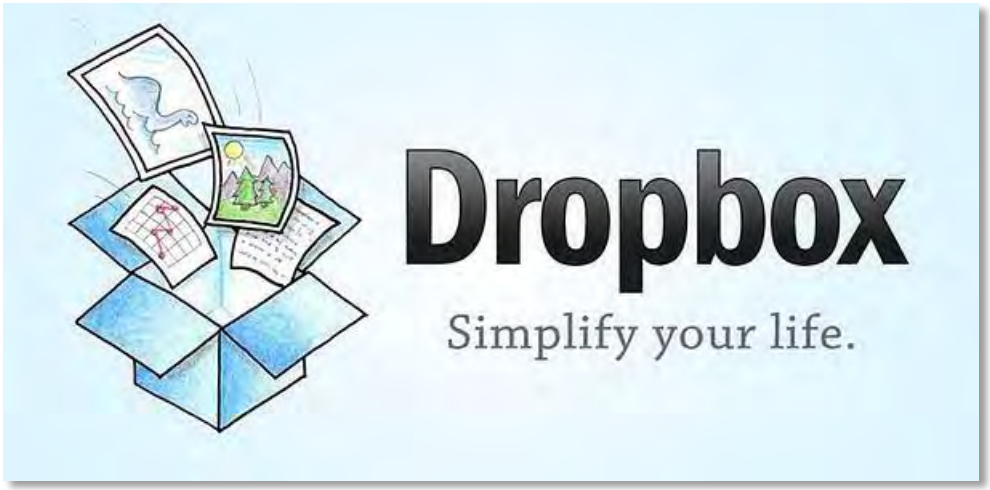
1. コンポーネントの脆弱性

コンポーネントとは

- コンポーネントが複数集まってアプリケーションとなる

- ４つのコンポーネント
  - Activity （画面表示やユーザ入力を受け持つ）
  - Service （見えない場所動いて何かをする。例：データ収集）
  - Receiver （見えない場所で、外部からメッセージを受け取る。）
  - Content Provider (外部からデータ(DB等)をアクセス可能にする）

- コンポーネントは外部アプリから呼び出し可能なので適切なアクセス制限をかけないと脆弱性を生む。
- 基本デフォルトで外部からアクセス不可となっている。



やっちゃった例

- 事件の概要
  - 他のアプリケーションからデータベースに変更を加え、Dropboxの公開用フォルダである「Public」フォルダにDropboxのアカウント情報が含まれている設定ファイルをアップロードさせたりすることが可能。
- 原因
  - ContentProviderは外部にデータを公開する仕組みなので、みんなに「公開する」がデフォルト値
  - android:exported=“false”を指定する必要があった。
- 詳しくは
  - ContentProviderのアクセス範囲 – Dropboxにおける脆弱性の修正
    - http://codezine.jp/article/detail/6286

AndroidManifest.xml セキュリティ設定

- コンポーネントのアクセス制限方法

- android:exported＝false
  - falseを設定した場合、他のアプリケーションから使用不可能になる
  - 自分自身かsharedUserId指定によって、同じユーザIDを持っているアプリケーションのみアクセス可能となる
- IntentFilterに注意
  - IntentFilterは外部公開する仕組み
  - IntentFilterが設定されている場合で、指定しない場合はtrue
  - IntentFilterが設定されていない場合で、指定しない場合はfalse

2. ファイルの脆弱性

Androidのファイル

✓他のアプリからファイルが読める→重要なデータを読み取られる

✓他のアプリからファイルが書き込める→ハングアップ、アプリデータの改変

注意する事

- ファイルの作成方法
  - MODE_WORLD_READABLE
  - MODE_WORLD_WRITEABLE
- ファイルの作成場所
  - アプリケーションデータディレクトリ
  - 外部記憶装置（SDカード）

SDカードに重要なデータを保存

やっちゃった例

- IMEIをユーザ識別に使っていた
- テスト時にユーザ切り替えしやすいようにSDカードに書いていた
- http://www.nec.co.jp/security-info/secinfo/nv12-008.html

外部記憶装置(SD)

外部記憶装置のファイルは全てのアプリケーションがアクセス可能

- どのアプリケーションがファイル出力を行ってもオーナとグループは同じ値となる
- アプリケーション毎にファイルやディレクトリのアクセス制御を行うことはできない
- 外部記憶装置のファイルやディレクトリは全てのアプリケーションがアクセス可能であることを意味する

3. 広告モジュールに注意

使用している広告モジュールがマルウェア！？

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です。

- 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
- 海外モジュールに特に注意

まとめ

まとめ

- 安心できるプリケーションを公開する方法
  - スマートフォンプライバシーイニシアティブ
  - 同意取得ダイアログ
  - プライバシーポリシの作成
- 安全なアプリケーションを作る方法
  - コンポーネントの脆弱性
  - ファイルの脆弱性
  - 広告モジュールに注意

ありがとうございました。

安心安全なモバイルアプリを公開するために

谷口岳

@tao_gaku

17:15分～18:00（45分）

タオソフトウェア株式会社

代表取締役