

Be Bold!



アンドロイドアプリを公開する上でセキュリティ的に注意する事

～日本Androidの会 × CEDEC
(ショートセッション3連発)～

谷口岳

@tao_gaku

11:20分～12:20 (20分)

タオソフトウェア株式会社

代表取締役

#262

レギュラーセッション

2013:8:22

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




Tao software

HOME SERVICES ANDROID ABOUT

Welcome.

豊かな未来と高度情報社会の実現に貢献

私たちタオソフトウェアは、ソフトウェア開発において優れた開発手法を創出し、品質の優れたソフトウェアを短期間・低価格で作り出すことのできる開発基盤を提供することによって、世界の人々ひとりひとりが実感できる、豊かな未来と高度情報社会の実現に貢献します。

DOROKURI

Android 自動生成サービス「ドロクリ」

ドロクリは、あらかじめ用意されたフレームワークにユーザが持っているコンテンツを組み合わせてアプリケーションを生成する Web サービスです。

ドロクリの利用にあたってはプログラミングの知識は必要なく、ドロクリにデータを入力するだけで Android アプリケーションを制作できます。

BLOG

タオソフトウェア社員によるブログです。1年半以上に渡り Android 関連の技術情報や記事を毎日掲載しております。

HOME SERVICES ANDROID ABOUT

Sitemap Privacy policy Copyright (C) 2005-2011 Taosoftware Co., Ltd. All Rights Reserved.

アンドロイドのセキュリティ本

Android Security

安全なアプリケーションを
作成するために

タオソフトウェア株式会社 [著]

谷口 岳 / 井澤 正道 / 境原 永典 / 唐鎌 千里 / 北村 久雄
岡山 美幸 / 宮城 善雪 / 梶山 拓哉 / 鳥野 英司



新しいネットワーク市場の活性化を図る、
新しい枠組みの確立が求められています。
こうした取り組みの最も基本的な部分の一つが、
マーケットへの安全なアンドロイドアプリの提供です。
セキュリティに焦点を合わせた本書は、
アンドロイドのコミュニティに歓迎されることでしょう。
日本Androidの会 会長 丸山不二夫

インプレスジャパン



Android アプリのセキュア設計 セキュアコーディングガイド

【みんなでスマホが安全に使える世界へ!】



2012年6月1日版

日本スマートフォンセキュリティ協会 (JSSEC)

セキュアコーディンググループ

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. ウェブサービス型
4. 脆弱性以外も検出

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

The screenshot displays the Tao RiskFinder web interface. The top navigation bar includes 'Risk', 'Analyze', 'Results', and 'Help'. The main content area is titled 'Summary' and shows a report for 'VariousRisks1'. It features two large icons: a red octagon with an exclamation mark and the word 'ERROR' next to the number '28', and a yellow triangle with an exclamation mark and the word 'WARNING' next to the number '27'. Below this, there is an 'Analyze' section with a table of metadata:

Field	Value
RiskFinder Version	10
Analyzed Date	2013/04/24 21:46
Filename	VariousRisks1.apk
Size	1,130,608byte
SHA1	3124f29b5edbb4fe89f26823e2044c8fc73762d8
MD5	651444a864679885b61e4b60f1647fff

Below the metadata table is a 'Risk Summary' table:

No.	Level	Message
1	ERROR	デバッグモードのアプリケーション
2	ERROR	アプリケーション設定誤り (persistent=true)
3	ERROR	デバッグ用設定による脆弱性

アンドロイドアプリを公開する上でセキュリティ的に注意する事



アンドロイドアプリを公開する上でセキュリティ的に注意する事

1. 安全なアプリを作る方法
2. リバースエンジニアリングの仕方
3. 利用者情報の取り扱い

安全なアプリケーションを作る方法



本を読むといい

Android Security

安全なアプリケーションを
作成するために

タオソフトウェア株式会社 [著]

谷口 岳 / 井澤 正道 / 境原 永典 / 唐鎌 千里 / 北村 久雄
岡山 美幸 / 宮城 善雪 / 梶山 拓哉 / 鳥野 英司



新しいネットワーク市場の活性化を図る、
新しい枠組みの確立が求められています。
こうした取り組みの最も基本的な部分の一つが、
マーケットへの安全なアンドロイドアプリの提供です。
セキュリティに焦点を合わせた本書は、
アンドロイドのコミュニティに歓迎されることでしょう。
日本Androidの会 会長 丸山不二夫

インプレスジャパン



Android アプリのセキュア設計 セキュアコーディングガイド

【みんなでスマホが安全に使える世界へ!】



2012年6月1日版

日本スマートフォンセキュリティ協会 (JSSEC)

セキュアコーディンググループ

Androidアプリ脆弱性の内訳

IPAに届け出られた Androidアプリの脆弱性の内訳

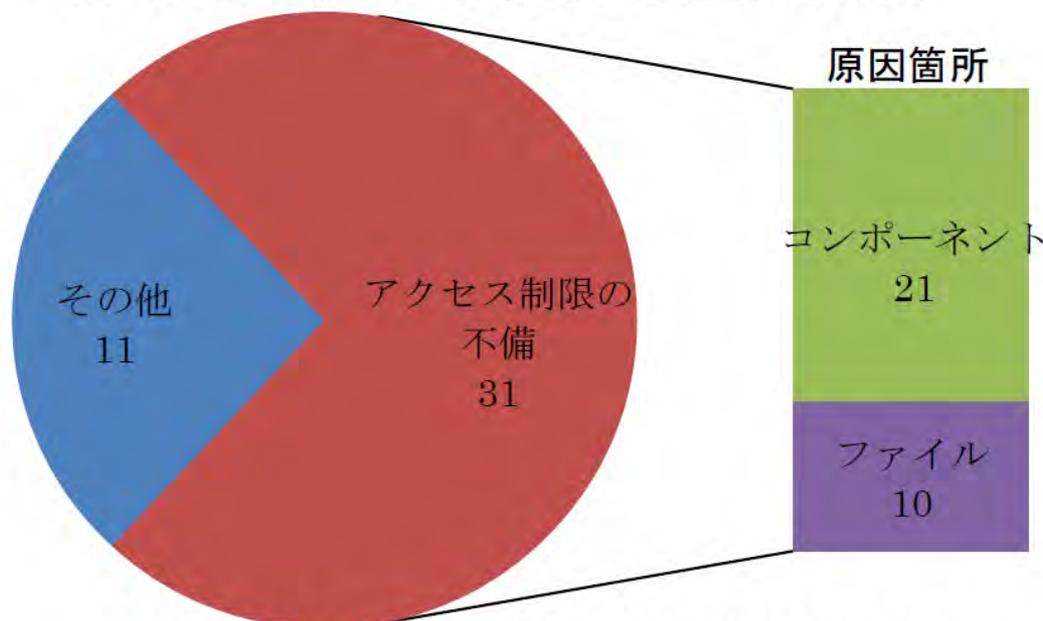


図 3-1 IPA に届け出られた Android アプリの脆弱性の内訳

- ▶ 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

NEC製品
セキュリティ情報

お知らせ

セキュリティ情報

影響のある製品

カテゴリ順

アルファベット順

日付順

掲載番号:NV12-008

脆弱性情報識別番号:JVN#05102851

Android版 嫁コレにおける端末識別番号の管理不備の脆弱性

■ 概要

Android版 嫁コレには、IMEI(端末識別番号)をSDカードに保存する問題が存在します。不正な他のAndroidアプリケーションを使用した場合、IMEIを取得される可能性があります。

■ 対象製品

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ー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

リバースエンジニアリングの仕方



リバースは簡単な事を知る

▶ 守る必要のある物

- アプリケーション内の著作物データ
 - 画像、動画、音声、文字列
- アプリケーションロジック
 - 特殊なアルゴリズム、暗号化キー

アプリ内の著作権データ

- ▶ アプリケーション内のデータは総て**簡単に**抜き取り可能
- 1. PCと接続してAPKファイルの吸出し
- 2. Android端末上でAndroidアプリによるリソースの吸出し



タイトル: ブラックジャックによろしく
著作者名: 佐藤秀峰
サイト名: Manga on Web
URL: <http://mangaonweb.com>



tPackageExplorer

- ▶ Androidアプリケーションのリソース情報を確認するアプリ
 - <https://market.android.com/details?id=jp.co.taosoftware.android.packageexplorer>
 - Google Playで「**taosoftware**」で検索

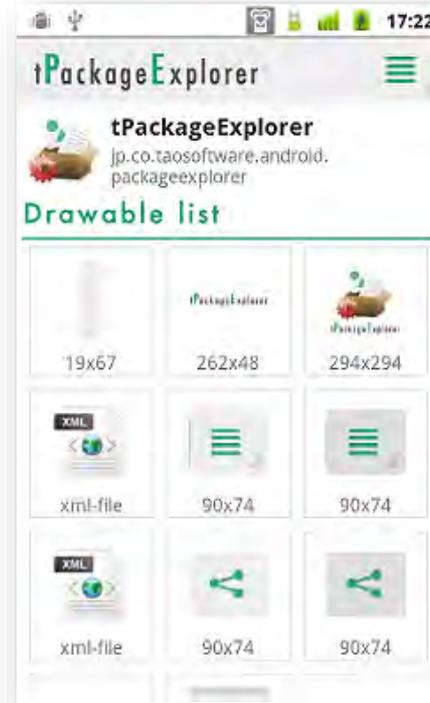
アプリ一覧



AndroidManifest.xml



アプリ内画像の表示



PCと接続してAPKファイル吸出し

- ▶ APKファイルはZIPファイル
 - 拡張子を変えて解凍すると構成ファイルを取り出すことができる。
- ▶ APKファイルの構造

```
/trssreader.apk
└─AndroidManifest.xml ー Androidのマニフェストファイル
└─resources.arsc ー res ディレクトリの内 values ディレクトリをまとめたもの
└─classes.dex ー プログラムコードをまとめたもの
└─META-INF ー 署名関連のファイルが含まれている
└─/assets ー 開発時の assets ディレクトリがそのまま含まれている
  └─┬─test.png
  └─┬─index.html
└─/res ー 開発時の values ディレクトリ以外の res ディレクトリがそのまま含まれている
  └─┬─/drawable
  └─┬─┬─icon.png
  └─┬─/layout
  └─┬─┬─main.xml
```

2. アプリケーションロジック

- ▶ Javaで書かれているAndroidアプリケーションはソースコード解析が簡単
 - ツールも出回っており、解析を防ぐ事はできない
 - 簡単な手順で解析が可能
 1. APKファイル取得
 2. Dex2jar classes.dex
 3. JavaDecompiler
 - root化などの特殊な処理は必要ない
 - Proguard等の難読化ツールで時間稼ぎ
 - NDKにコードを移動(完全ではない)

利用者情報の取り扱い

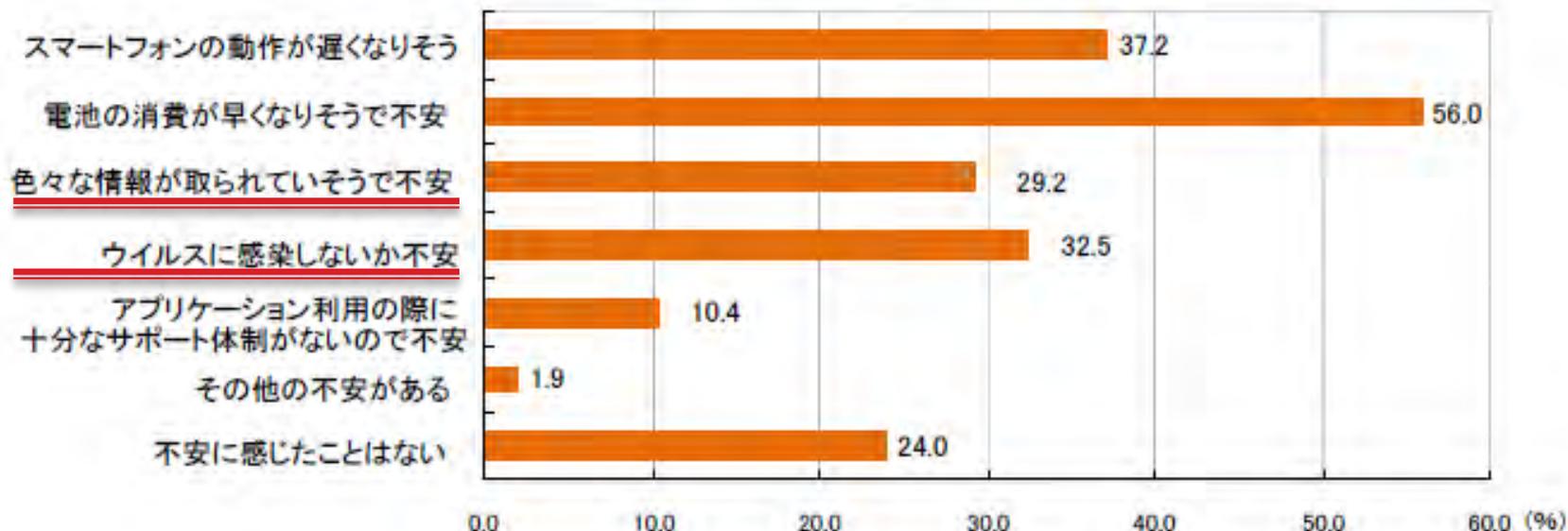


【図表2-11: アプリケーション利用に関する不安】

- ・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を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(不安を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

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がつきにくく、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「コーエイブランニング」社長、香川雅昭容疑者(50)＝東京都目黒区青葉台西二＝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。

The diagram illustrates the flow of information. A person is shown using a smartphone. A red arrow labeled '不正アプリをダウンロード' (Download malicious app) points from the smartphone to an 'IT会社' (IT company). A red arrow labeled 'データ抜き取り (3700万人のメールアドレス)' (Data extraction (37 million email addresses)) points from the smartphone to the IT company. A red arrow labeled '有料サイトへ勧誘メール' (Promotional email to paid site) points from the IT company to a '有料サイト' (Paid site). A vertical label on the right reads '不正アプリを使った情報流出のイメージ' (Image of information leakage using malicious app).

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？！

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。



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)
- ▶ 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

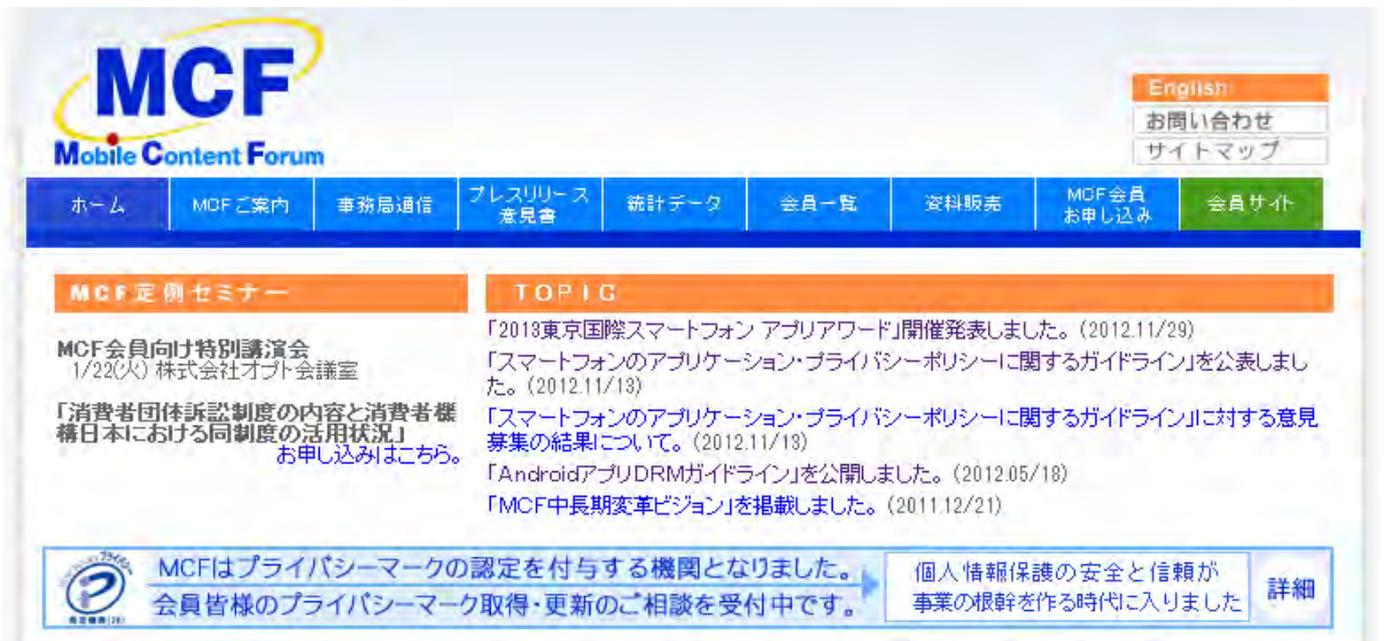


Androidスマートフォンプライバシーガイドライン作り
ました。無料公開(ApacheLicense2)

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_spapppp_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



The screenshot shows the homepage of the Mobile Content Forum (MCF). The header includes the MCF logo and a navigation menu with items like 'ホーム', 'MCFご案内', '事務局通信', 'プレスリリース 意見書', '統計データ', '会員一覧', '資料販売', 'MCF会員 お申し込み', and '会員サイト'. There are also buttons for 'English', 'お問い合わせ', and 'サイトマップ'. The main content area is divided into two sections: 'MCF定例セミナー' (MCF Regular Seminars) and 'TOPIC' (Topics). The seminar section lists an event for members on 1/22 (Tuesday) at the Opt Co., Ltd. conference room, with a link to learn more. The topic section lists several recent news items, including the announcement of the 'Smartphone Application Privacy Policy Guidelines' on 11/13/2012, and the 'Android App DRM Guidelines' on 05/18/2012. At the bottom, there is a banner announcing that MCF has become an authorized certifying body for the Privacy Mark, with a link for more details.

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

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定める
- ▶ 「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
- ▶ 自分の子供や親が安心して使えるかを考える

- ▶ 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。

まとめ



まとめ

1. 安全なアプリを作る方法
 - 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
2. リバースエンジニアリングの仕方
 - リバースエンジニアリングは簡単
 - アプリ内に重要な情報を入れる時は注意
3. 利用者情報の取り扱い
 - プライバシーポリシーを書く
 - 同意取得ダイアログを出す

Be Bold!



ありがとうございました。

アンドロイドアプリを公開する上でセ
キュリティ的に注意する事