

利用者情報に関する取り組み

タオソフトウェア株式会社



タオソフトウェアについて

- ▶ 2005年創業(9期目)の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
- ▶ 日経BP社主催 Android Application Award 2010 Winter にて tWakeupCallMaker が大賞を受賞。
- ▶ 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、講演など多数

年齢早見

年齢早見

About「年齢早見」



「年齢早見」は、システム手帳の最後に付いているような、西暦と暦変換、年齢早見表を、Android上で見ることが出来るソフトウェアです。

推奨 OS

- Android 1.1 以上

価格

- FREE

Version 1.6.3

- 高解像度、低解像度アイコン追加

機能



今日 2009/7/10

年号、年数、西暦、年齢のいずれかの数字を変更する事が可能です。年齢を30歳に変更すると、自動的に「昭和」「53」「1978」に変更されます。明治元年からの変換が可能です。年齢は、選択された年の1月1日の年齢を表示します。

- ▶ 2008年11月:アンドロイドマーケットが使用可能になると同時に公開
- ▶ 日本法人でアンドロイドマーケットに最初に公開されたソフトウェア

アンドロイド開発者ブログ



- ▶ 英語情報も少ない時期に技術情報の発信開始
- ▶ Android技術者が見るブログとして定着

Android Application Award 2010 Spring

大賞受賞




Androidでめざまし時計をつくろう
tWakeUpCallMaker

めざまし時計作成ソフト(tWakeUpCallMaker)は、Android上であなたの声が埋め込まれためざまし時計ソフト(tWakeUpCall)を作ります。作成した世界に一つの目覚ましソフトはメールにて友人に送る事ができます。



作成方法

- 名前を入力**
作成者の名前を入力します。空欄でも可能です。
- アラーム音を吹き込む**
録音する他、Androidに入っている音楽ファイルを選択する事も可能です。
- メールで送る**
作成した目覚まし時計ソフトは、SDカードに保存されます。メールは別の方法で配布したり、自分で使用する事も可能です。
※ Gmailで送けるとは、iAttachAppInstallerを使用すると簡単にインストールできます。



タオソフトウェア株式会社

本社 〒110-0036
東京都台東区台東2-22-11 アポロビル3階

E-MAIL android.dev@taosoftware.co.jp

URL <http://www.taosoftware.co.jp/>

紹介ページ <http://www.taosoftware.co.jp/android/wakeupcallmaker/>

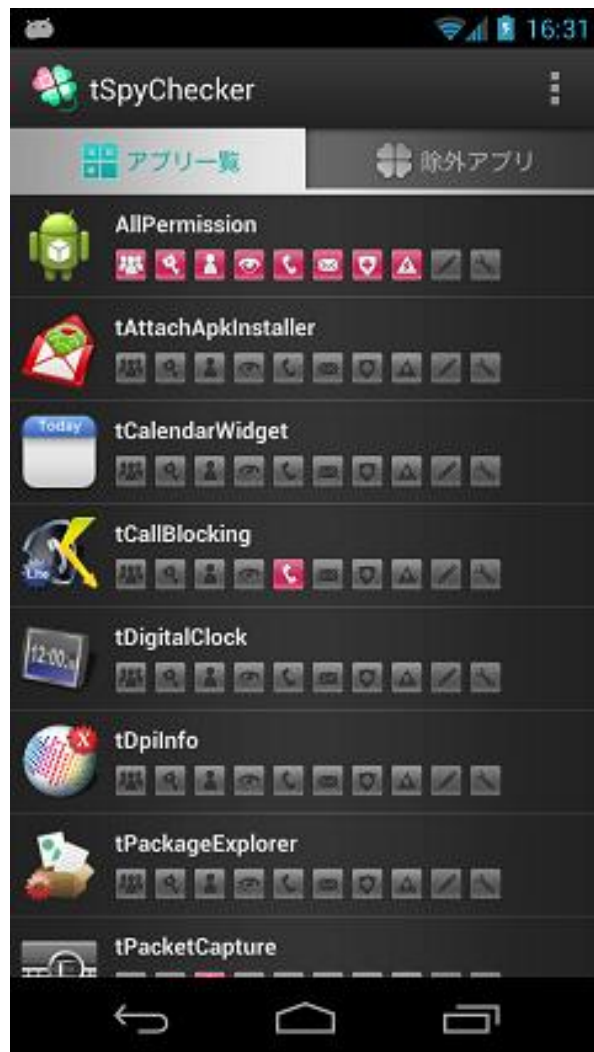
マーケットURL [market://search?q=taosoft.android.wakeupcallmaker](http://market.android.com/details?id=com.taosoft.twakeupcallmaker)





写真提供: 日経BP社(撮影: 菊池くらげ)

日本で初めてのアンドロイドアプリコンテスト
日経BP主催: NTTドコモ協賛

 tSpyChecker

▶ 端末内のアプリケーションそれぞれに対して、利用者情報の流出の可能性を検知

- 当初は開発者向けにパーミッションの危険性を知らせるために作成
- パーミッション説明の日本語が非常に分かりにくかったので、分かりやすい表示で解説

▶ 2011年2月リリース

tSpyChecker

アプリが取得可能な情報



外部通信方法



▶ パーミッションや機能を複数のカテゴリに分類し、外部通信方法と組み合わせる危険な可能性を表示

<http://www.taosoftware.co.jp/android/spychecker/>

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な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



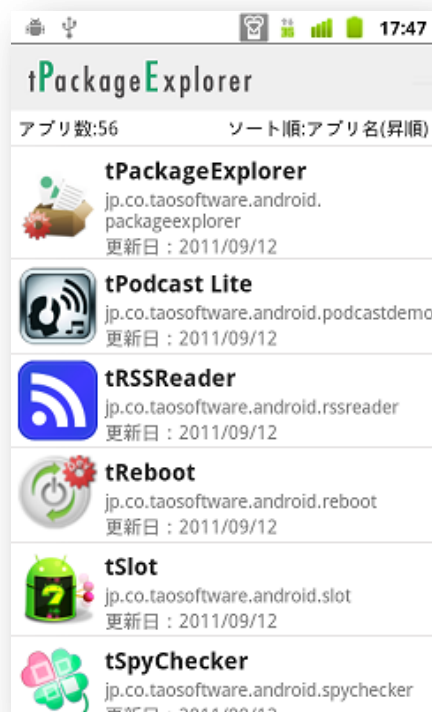
- ▶ 2012年06月11日
 - 第1版の作成に深く関わる
 - ドキュメント
 - http://www.jssec.org/dl/android_securecoding.pdf
 - サンプルコード
 - http://www.jssec.org/dl/android_securecoding.zip
- ▶ JSSEC
 - 日本のキャリアやハードメーカ等が集まって作成されたセキュリティに関する団体



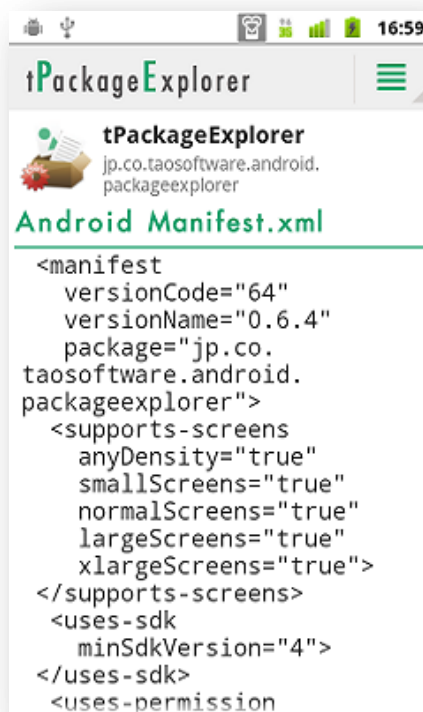
tPackageExplorer

- ▶ アンドロイドアプリケーションのリソース情報(内部情報)を確認するアプリケーション
- ▶ アプリ内のデータは公開APIのみで抜き取り可能な事を実証する事が目的
 - <https://market.android.com/details?id=jp.co.taosoftware.android.packageexplorer>

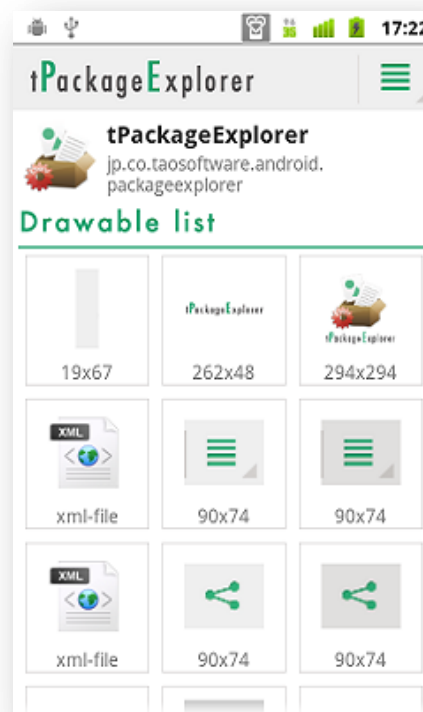
アプリ一覧



AndroidManifest.xml



アプリ内画像の表示



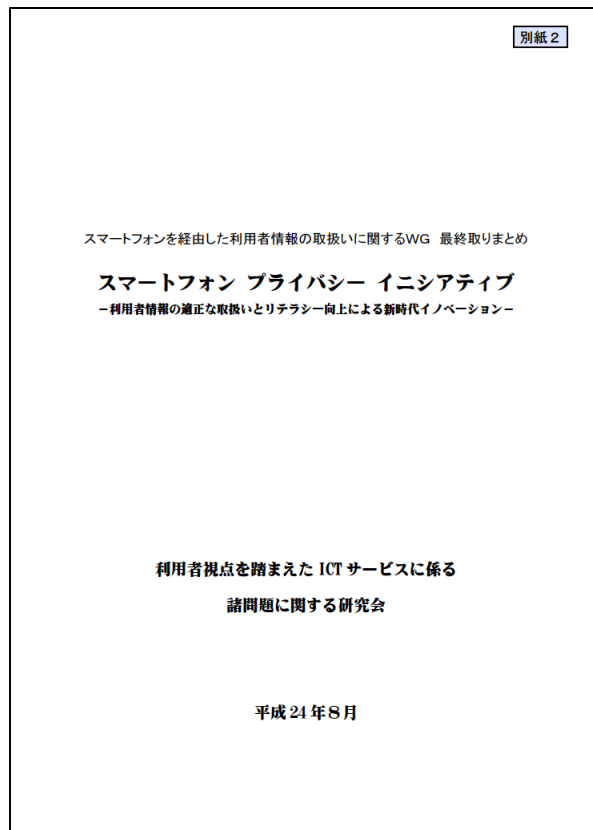
tPacketCapture/ Pro



- ▶ ルート化なしで動作するパケットキャプチャソフト(世界初)
- ▶ 端末をルート化する理由を一つ減らすのが目的
- ▶ 4.0の新機能のVpnServiceを使用し、正規の方法でパケットキャプチャを実現。
- ▶ 危険な可能性があるソフトながらセキュリティ会社で使われる等の実績を持つ
- ▶ <https://play.google.com/store/apps/details?id=jp.co.taosoftware.android.packetcapture>

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



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



講演実績(一部)

日付	主催	タイトル
2010 /07/13	ワイヤレスジャパン	アンドロイドの復習とこれから (S-2-1 Androidセッション)
2010/11/24	Mobidec(MCF)	アンドロイドアプリビジネス
2011/07/14	ワイヤレス技術セミナー (リックテレコム主催)	Android向け開発プロジェクトの成功パターン分析
2011/12/05	Androidの会	安全なアプリを作成するために
2012/03/24	ABC 2012 Spring	Android Security 安全にアンドロイドを使用するために
2012/04/27	Android テスト祭り	Androidのセキュリティと品質保証の問題について
2012/06/21	石川県工業試験場	安全なAndroidアプリを作成するために
2012/07/09	パナソニックAVC	セキュアなAndroidアプリケーション開発法
2012/10/08	NTTドコモ	AROツール活用方法（消費電力問題）
2013/01/18	岐阜ソフトピアジャパン	AROツール活用方法（消費電力問題） Androidプライバシーガイドライン
2013/02/01	ワイヤレス技術セミナー (リックテレコム主催)	「スマートフォンプライバシーイニシアティブ」への理解とAndroidアプリへの実装方法

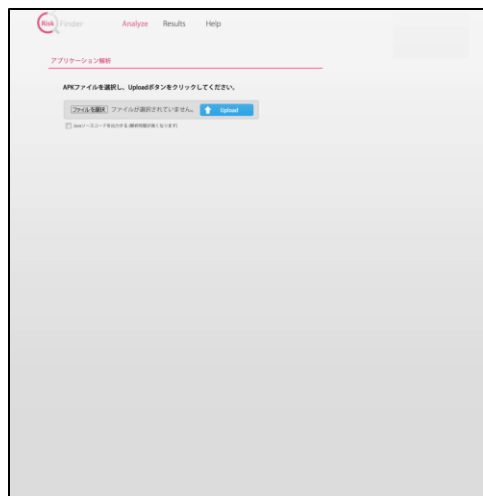


アンドロイドアプリの脆弱性を診断するウェブサービス。

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

サマリ画面

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。



解析結果はダウンロードできます



アイコンでエラー数、警告数を表示します



- 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



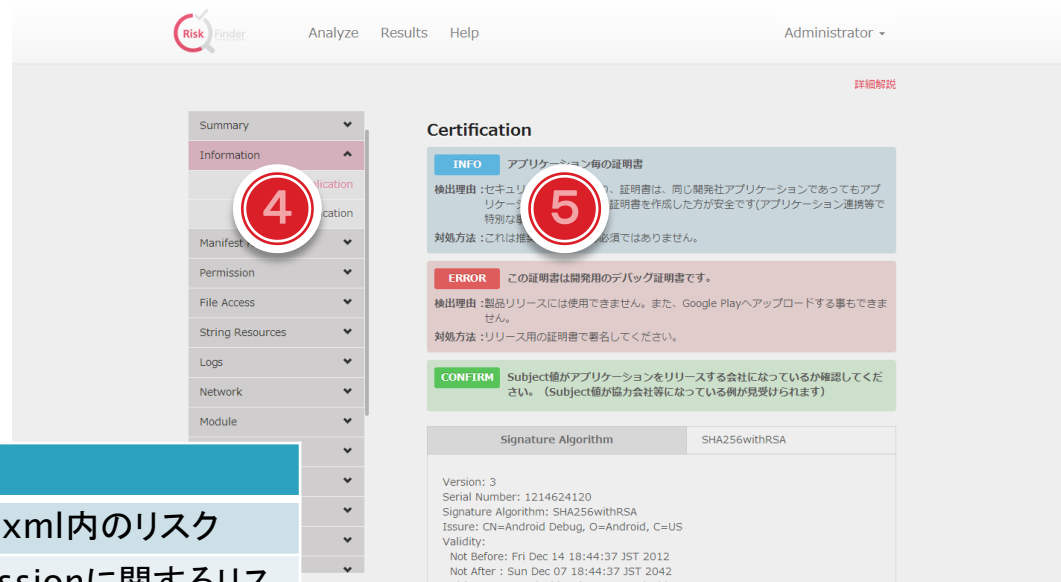
リスクレベル付きの解析結果を一覧表示します。

リスクレベル	説明
ERROR	以上レベル
WARNING	警告レベル
CONFIRM	確認レベル
INFO	情報レベル

詳細画面

4

左メニュー	説明
ManifestRisk	AndroidManifest.xml内のリスク
Permission	使用しているPermissionに関するリスク
FileAccess	使用しているファイルに関するリスク
String Resource	使用している文字列リソース
Logs	ログ出力APIの使用箇所
Network	アクセスしているURL、プロトコル
Module	使用している外部モジュールのリスク
Cryptography	使用している暗号化アルゴリズムのリスク
Security Logic	外部DEXの使用、リフレクションの使用等
Privacy Policy	プライバシーポリシーに関する情報



5

3ブロックで表示される検出結果
メッセージ

「検出内容」

「検出理由」

「対処方法」

具体的な対処方法まで記載していますので、レポートを参照すれば解決のための方法が分かる

カバレッジ



その他の脆弱性



パーミッションとAPI関連

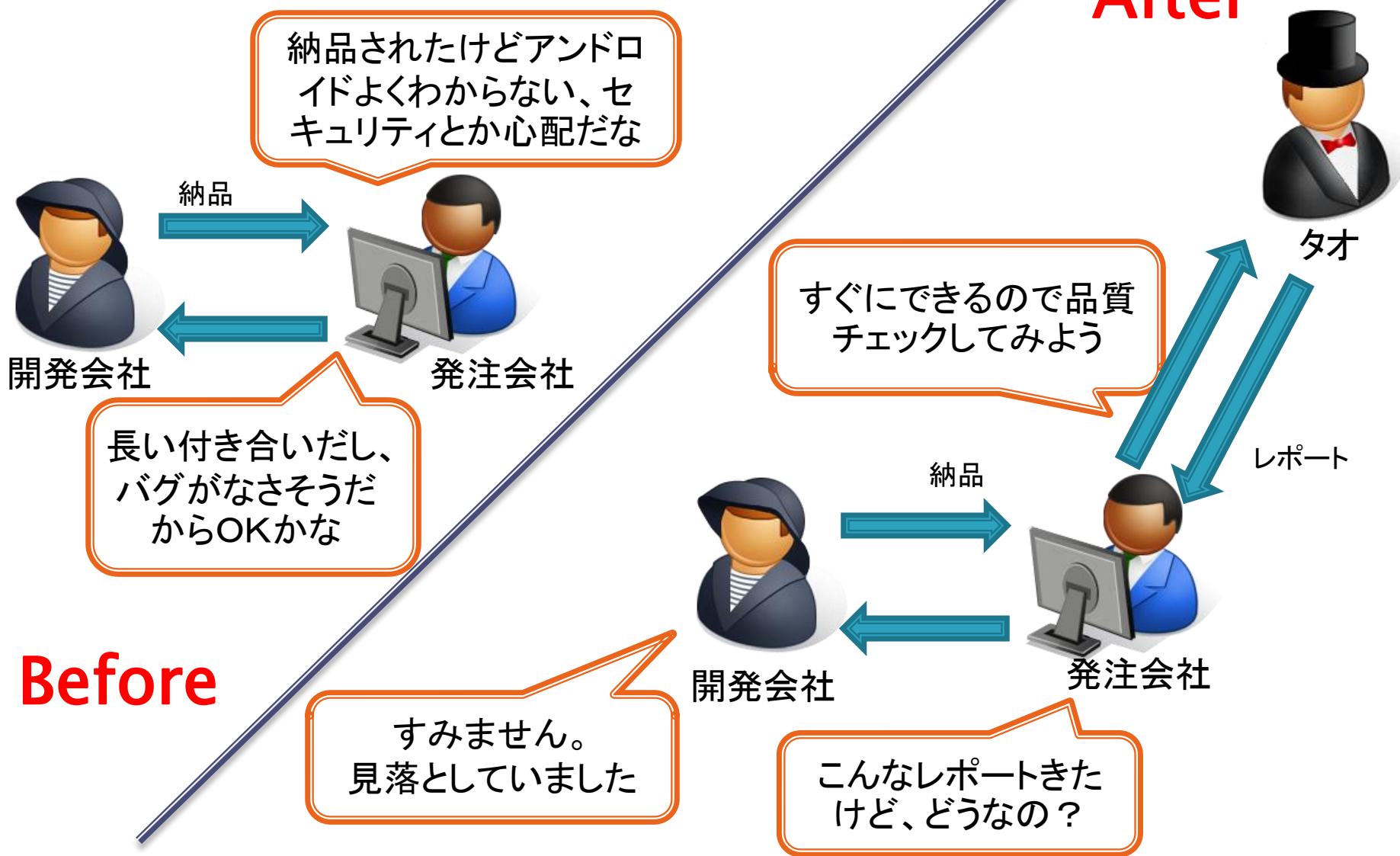


Android OSのバージョンによる差異



第三者モジュール

利用シーン: 発注者の場合



Tao RiskFinderの利用者

- ▶ A: アプリケーション開発会社
 - 作製したアプリの脆弱性チェック
- ▶ B: アプリケーション販売会社
 - 受け入れテスト等における一定の評価基準として利用
- ▶ C: 複数のアプリを集めて提供する会社
 - MDM、ソフトウェア紹介サイト
 - アプリケーションが一定の品質を持っているか、マルウェア（リスクウェア）の可能性がチェックできます。
- ▶ D: テスト会社、脆弱性検査会社
 - 従来のテストに加え脆弱性検査を加える
 - サーバの脆弱性検査に加え、クライアントの脆弱性検査をおこなう

利用者情報に関する機能

Permissionメニュー

- ▶ パーミッションに関する情報を分析
 - 使用パーミッションを表示
 - パーミッションの組み合わせによる危険性を報告
 - (電話帳取得+Internet,NFC,Bluetooth等)
 - 必要のないパーミッションを検知
 - 特定のパーミッションに対して使用せずに機能を実現する方法を提示
- ▶ パーミッションを必要とするAPIをデータベース化し、APIから必要なパーミッション、パーミッションから必要なAPIを検知可能
- ▶ ユーザによる変更が困難な端末情報取得APIを検出(パーミッションが必要のない物を含む)
 - アプリケーション内全て
 - 第三者モジュール内のみ

Moduleメニュー

- ▶ 第三者モジュール
 - アプリケーション作成者以外が作成したもの
 - 広告モジュールやバグレポートモジュール等
 - パッケージ名で判断。
- ▶ 第三者モジュールを独自に調査してデータベース化
- ▶ 現在500モジュール(広告以外も含む)
- ▶ アプリケーションに含まれるモジュールとマッチング、危険なモジュールは警告。
- ▶ 検査時第三者モジュール内のコード調査(静的解析)
 - アクセス先URL
 - 固有識別子取得(IMEI他)
 - 使用するパーミッションやAPI

PrivacyPolicyメニュー

総務省「スマートフォン プライバシー イニシアティブ」に沿うための情報を表示

- ▶ 外部通信の可能性検出
- ▶ 第三者情報を取得可能なパーミッション検出
- ▶ 個人情報を取得可能なパーミッション検出
- ▶ 利用者で変更が困難な情報を取得するパーミッション検出
- ▶ その他利用者情報を取得可能なパーミッション検出
- ▶ 位置情報の取得検出
- ▶ 固有識別子の取得検出
- ▶ ユニークIDの生成の検出
- ▶ 第三者モジュール上での、通信、プライバシー情報、固有識別子の取得検出

ありがとうございました。
タオソフトウェア株式会社

