

Androidセキュリティの今・昔

2017/2/28(水) JSSECセキュリティフォーラム2017
ベルサール神田 2階 イベントホール
15:00～15:45 T3<技術部セッション3>



タオソフトウェア株式会社
代表取締役
谷口岳
@tao_gaku





タオソフトウェア株式会社

- 代表取締役 谷口岳
- 2005年創業、Android関連システム受託開発
- 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（昔）
- 雑誌執筆、講演
- セキュリティ色々





3DVRがスマホで手軽に楽しめる!

話題の3Dバーチャルリアリティーを体験しませんか?
TaoVisorにAndroidスマホをセットすれば
すぐに手軽に3DVRの世界が体験できます!



3DVR ゴーグル タオバイザー
TaoVisor

3DVRは体験しないと、その面白さがわかりません。
様々な3Dアプリを多くの人に手軽に観てもらいたい、
作ってもらいたいとの想いから、スマートフォンをセットして、
3DVRを体験できるゴーグル「タオバイザー」を作りました。

ご支援ありがとうございました!

タオバイザーはクラウドファンディング
を利用して制作されました。
583人の方から、目標金額250%以上の
1,374,500円のご支援を頂きました。

眼鏡をかけたままでも使える
子供も楽しい組み立てキット
軽くて壊れにくい素材
持ち運びに便利
目の間隔調整ができる
Google Cardboard互換

YouTube等の
side by side形式の
3D動画も楽しめます

⚠ 本製品の対象年齢は13歳以上です。対象年齢以下のお子様を使用する場合は、必ず保護者監督のもとで行ってください。

TaoVisor ホームアプリ

タオバイザーホームアプリは、タオバイザーと一緒に
使用する事で、より便利にタオバイザーを使用できる
ようにするアプリです。
Google CardboardやDive など他の3DVR用ゴーグル
でも使用できます。

★ サンプルコンテンツが楽しい!
★ アプリランチャーでカンタン!

ANDROID アプリ
Google play

Google Playにて無料でダウンロードできます
動作環境: Android OS 4.1.2以上

タオバイザーについての詳しい情報はホームページをご覧ください。
<http://www.taovisor.com/>

Tao software タオソフトウェア株式会社
〒110-0015 東京都台東区東上野 2-1-1 フリーアネックスビル8F
TEL.03-6802-8247 FAX.03-6802-8347 <http://www.taosoftware.co.jp>

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
- <http://taovisor.com>





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

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



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

The screenshot shows the RiskFinder web interface. The top navigation bar includes 'Analyze', 'Results', and 'Help'. The main content area is titled 'Summary' and displays the filename 'VariousRisks1' with download options for 'Word' and 'HTML'. It features two large icons: a red octagon with an exclamation mark labeled 'ERROR' with the number '28', and a yellow triangle with an exclamation mark labeled 'WARNING' with the number '27'. Below this 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	3124f29b5eddb4fe89f26823e20f4c8fc73762da
MD5	651444a864678885b61e4b60f1647fff

Below the metadata 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	デバッグ詳細書による署名



アンドロイドセキュリティの 今・昔



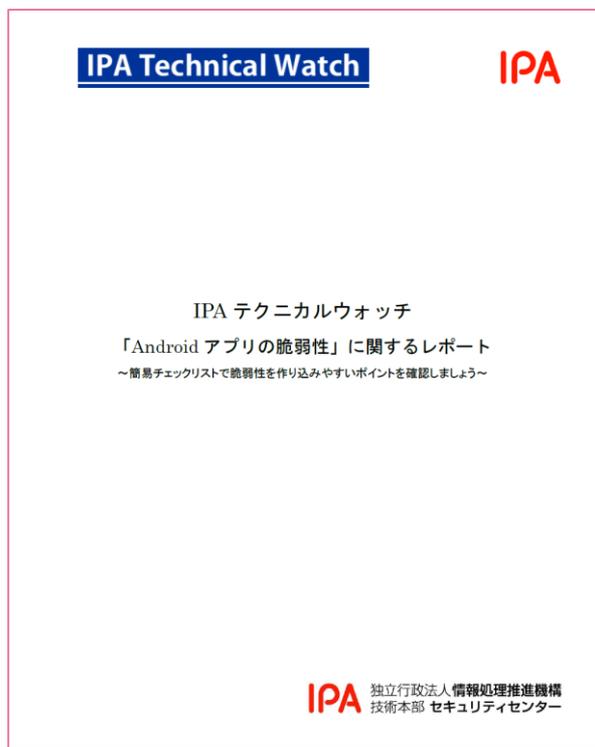


Androidセキュリティの今・昔

Androidアプリは、セキュリティ的に問題が多いと言われ2012年には**IPAテクニカルウォッチ**「Androidアプリの脆弱性」に関するレポートが公開されました。Androidは毎年バージョンアップされ、色々な問題が解決されてきました。Androidアプリが陥りやすかった過去の問題は最新のOSではどのようなになっているのか、どのように解決されているかを解説し、また小粒な新しいセキュリティに関する機能に関する説明も致します。



「Androidアプリの脆弱性」



2012年6月13日

IPAに届け出られるAndroidアプリの脆弱性関連情報が2011年後半から増加していることを踏まえ、それらを分析して脆弱性を作り込みやすいポイントをまとめ、技術レポート「IPAテクニカルウォッチ」として公開しました。

20ページと少ないが重要な事項を抽出している。

IPAテクニカルウォッチ「Androidアプリの脆弱性」

<https://www.ipa.go.jp/about/technicalwatch/20120613.html>



2012年～

2012/1/1

- Android Security安全なアプリケーションを作成するために発刊(タオソフトウェア)

2012/6/1

- Androidアプリのセキュア設計・セキュアコーディングガイド (JSSEC)

2012/6/13

- **IPAテクニカルウォッチ**

2015/5/25

- IPA Androidアプリの脆弱性の学習・点検ツールAnCoLe
- <https://www.ipa.go.jp/security/vuln/ancole/>

2017/2/8

- 今日



Androidは大きく変化

2011年02月 Android 3.0 端末リリース

2011年11月 Android 4.0 端末リリース

2012年07月 Android 4.1 端末リリース

...

2016年10月 Android 7.0 端末リリース

現在 Android 7.1.1

IPAテクニカルウォッチの 振り返り





簡易チェックリスト

■ Android アプリのセキュリティ実装 簡易チェックリスト

No	項目	対策内容	チェック	解説
1	ファイルのアクセス制限	○ SDカードに機微な情報を保存しない	※1 <input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.1(1)
		○ 必要に応じて、SDカードに保存するデータを暗号化する		
2		○ ファイル作成時に、ファイルへのアクセス許可を適切に設定する	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.1(2)
3	コンポーネントのアクセス制限	○ アクティビティやサービスに対してアクセス制限をかける	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.2(1)
4		○ コンテンツプロバイダに適切なアクセス制限をかける	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.2(2)
5	ログ出力の内容	○ デバッグログに機微な情報を含めない	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.3(1)
6		○ インテントを送信する際のパラメータに機微な情報を含めない	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	4.3(1)
7	アプリの権限	○ 必要以上に権限を要求しない※2	<input type="checkbox"/> 対応済 <input type="checkbox"/> 未対応 <input type="checkbox"/> 対応不要	2.2

※1 このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックする

※2 脆弱性の直接の原因ではないが、Androidの仕組みを適切に使用する上で必要な対策である



簡易チェックリスト

1. ファイルのアクセス制限

- SDカードに機微な情報を保存しない
- 必要に応じて、SDカードに保存するデータを暗号化する
- ファイル作成時に、ファイルのアクセス許可を適切に設定する。

2. コンポーネントのアクセス制限

- アクティビティやサービスに対してアクセス制限をかける
- コンテントプロバイダに適切なアクセス制限をかける

3. ログ出力の内容

- デバックログに機微な情報を含めない
- インテントを送信する際のパラメータに機微な情報を含めない

4. アプリの権限

- 必要以上に権限を要求しない



1. ファイルのアクセス制限





ファイルのアクセス制限

要求と問題点

- 連携するアプリとデータのやり取りがしたい
他のアプリから参照可能になる
- 良くわからないのでソースコードをコピペ
そのまま動いてしまうので脆弱性となる
- サイズの大きなファイルをSDカードに置きたい。
他のアプリから参照可能になる
- 端末の写真データをアプリで使いたい。
外部ストレージ全アクセス権限が必要で怪しくなる



ファイルでのデータ連携は禁止

Android OS 4.2 (API level 17)

- `openFileOutput()`, `getSharedPreferences()`等のファイル作成メソッド引数変更
- `MODE_WORLD_WRITEABLE`, `MODE_WORLD_READABLE` 非推奨
- `SharedPreferences Class`

名前はShareだけどShare機能はなくなった。



連携するアプリとのデータのやり取り 2

Android 7.0 (API level 24)

- **MODE_WORLD系使用時は、SecurityExceptionとなる。**

ファイルでは、データの連携できなくなった。

ContentProvider,FileProviderを利用するというルール



ディレクトリ移動も制限

従来

- パッケージディレクトリのアクセス許可:

751

所有ユーザ : rwx、所属グループ : r-x、その他のユーザ : --x

Android 7.0 (API Level 24)

- パッケージディレクトリのアクセス許可

700

所有ユーザ : rwx、所属グループ : ---、その他のユーザ : ---



外部ストレージの仕様変更

WRITE_EXTERNAL_STORAGEの問題

Android 1.5(API Level 3)

- アプリから外部ストレージアクセスし放題
- ユーザの写真、データが改変、読み取り可能

Android 1.6(API Level 4)

- WRITE_EXTERNAL_STORAGE追加、この権限がないと外部ストレージに書き込みできない。
- 読み込みは権限関係なく可能→ユーザの写真が自由に読み取り可能

Android 4.1(API Level 16)

- READ_EXTERNAL_STORAGE仮追加

多くのアプリがWRITE_EXTERNAL_STORAGEを持つようになり意味がなくなってきた



サイズの大きなファイルをSDカードにおきたい

アプリ専用外部ストレージエリア導入（権限なく特定の領域は外部ストレージアクセス可能）

Android 4.4(API Level 19)

- ExternalAppDirに書き込みを行う際、WRITE権限が不要。
例) `storage/sdcard0/Android/data/com.example/files`
キャッシュや巨大なデータを保存するのにWRITE権限は必要ではなくなつた。
- READ_EXTERNAL_STORAGE追加、この権限がないと外部ストレージの読み込みはできない（WRITEがあればできる）

写真にアクセスしたいだけなのに、
WRITE_EXTERNAL_STORAGEが必要な問題はそのまま



写真データに怪しまれずにアクセスしたい

Android7.0(API Level 24)

- **Scoped Directory Access**
- **従来のパーミッションモデルとは異なるが、実行時にユーザに特定のディレクトリにアクセスしても良いか問い合わせる仕組み**

タイプ	説明
DIRECTORY_MUSIC	一般的な音楽ファイルの標準ディレクトリ
DIRECTORY_PODCASTS	ポッドキャストの標準ディレクトリ
DIRECTORY_RINGTONES	着信音の標準ディレクトリ
DIRECTORY_ALARMS	アラーム音の標準ディレクトリ
DIRECTORY_NOTIFICATIONS	通知音の標準ディレクトリ
DIRECTORY_PICTURES	画像ファイルの標準ディレクトリ
DIRECTORY_MOVIES	動画ファイルの標準ディレクトリ
DIRECTORY_DOWNLOADS	ユーザがダウンロードしたファイルの標準ディレクトリ
DIRECTORY_DCIM	カメラによる画像・動画ファイルの標準ディレクトリ
DIRECTORY_DOCUMENTS	ユーザによって作られたドキュメントの標準ディレクトリ



外部ストレージ問題

外部ストレージの問題は、ほぼ終了

Android 7.0でWRITE_EXTERNAL_STORAGEを利用する必要は殆どなくなった。

2年ほどすれば、WRITE_EXTERNAL_STORAGEを持っているアプリは怪しいと言える環境が出来上がるはず。



2.コンポーネントのアクセス 制限





問題点

- アクティビティやサービスを他のアプリからアクセス可能になることを知らずに、アクセス可能な実装してしまう。
- コンテントプロバイダーを他のアプリからアクセス可能な実装してしまう。



アクティビティ

Acrivityに関するAndroidの仕様変更は特になし。

- **基本export=false**



明示的Intentを使うルール変更

Android 5.0 (API level 21)

Serviceの仕様を変更

- **startService**

intent-filterは利用しない事を推奨

- **bindService**

**Bindサービス時にIntent-Filterを使用すると、
IllegalArgumentExceptionが発生**



コンテンツプロバイダーのアクセス

外部連携のためではなく、自アプリのデータベースへのアクセス手法として実装する例が多い。

デフォルトがtrueになっていたので多くのアプリがContentProvider公開設定になっていた。

Android 4.2 (API Level 17)

- exportのデフォルトがtrueからfalseに変更



3.ログ出力の内容





ログの出力

- デバッグログをそのままにしてしまう問題
- インテント内容がデバッグログに出力される問題

Android 4.1 (API Level 16)

- 自分自身のログのみ参照可能に仕様変更

システムログ、他アプリのログが参照不可能になった



4. アプリの権限





必要以上に権限を要求しない

- 何も考えずにアプリの権限をどんどん付けてしまう。

Android 6.0 (API Level 23)

Runtime Permission

- インストール時ではなく、実行時に権限を確認するため、不必要な権限は使用されない。
- 権限取得ダイアログを実装する必要があるため、権限取得に慎重になる。

まとめ





簡易チェックリスト

ファイルのアクセス制限

- 注意** ● SDカードに機微な情報を保存しない
- 注意** ● 必要に応じて、SDカードに保存するデータを暗号化する
- OK** ● ファイル作成時に、ファイルのアクセス許可を適切に設定する。

コンポーネントのアクセス制限

- OK** ● アクティビティやサービスに対してアクセス制限をかける
- OK** ● コンテントプロバイダに適切なアクセス制限をかける

ログ出力の内容

- OK** ● デバックログに機微な情報を含めない
- OK** ● インテントを送信する際のパラメータに機微な情報を含めない

アプリの権限

- OK** ● 必要以上に権限を要求しない



最近のちょっとした機能





SafetyNet Attestation

- システムがRoot化されている、システム自体が改変されているかをチェックする機能
- Google Play Serviceにて提供
- Googleのサーバと通信してチェックを行う
- <https://developer.android.com/training/safetynet/index.html>



SafetyNet SafeBrowsing

- Googleが常に更新している安全でないウェブサイトのリストに対して、URLを渡し確認できる機能
 - フィッシング詐欺サイト
 - マルウェアサイト
 - 不要なソフトをホストするサイト
- Google Play Serviceにて提供
- Googleのサーバと通信してチェックを行う
- <https://developer.android.com/training/safebrowsing/index.html>



タオソフトウェア株式会社 谷口岳

ありがとうございました。

