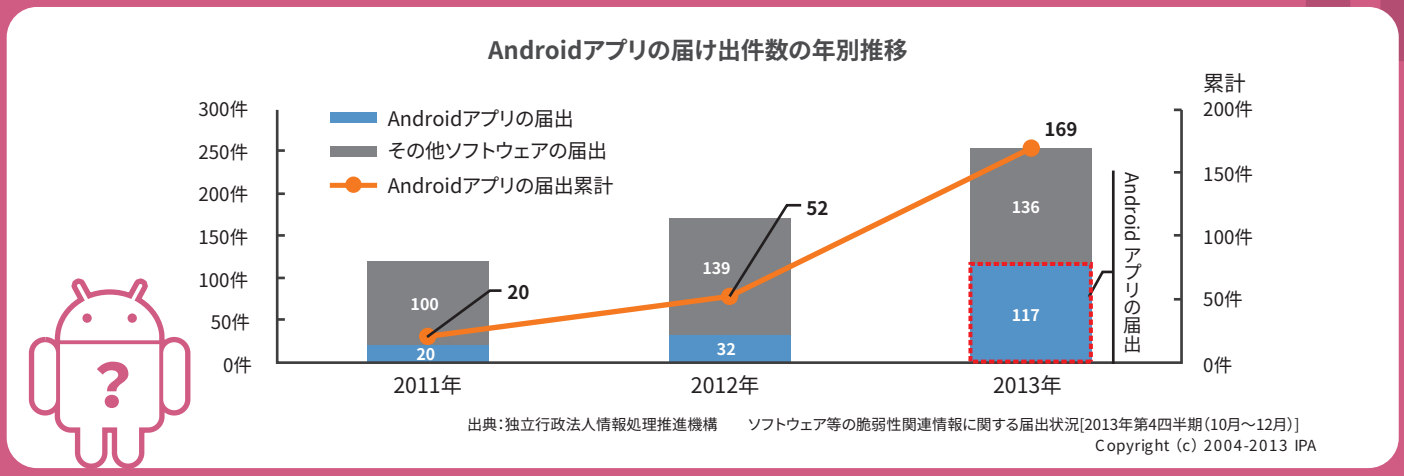
Risk Finder

そのAndroidアプリは安全ですか？

Risk Finder

そのAndroidアプリは安全ですか？

Androidスマートフォンが急速に普及するとともに、Androidアプリの脆弱性の報告も急増しています。
アプリの脆弱性を悪用された場合、利用者の個人情報が漏えいしたり、データが改ざんされたりする可能性があります。
2013年12月の時点で、IPAに寄せられている脆弱性関連情報に関する届け出の約半分がAndroidアプリの脆弱性によるものになっています。



出典：独立行政法人情報処理推進機構　ソフトウェア等の脆弱性関連情報に関する届出状況[2013年第4四半期（10月～12月）]

※ http://www.ipa.go.jp/security/vuln/report/vuln2013q4.html

RiskFinderの特徴

ブラウザでファイルをアップロードするだけなので、誰でも使用できます

事前準備は必要ありません。アプリ開発の知識も不要です。診断したいアプリのファイルとブラウザがあれば、誰でも簡単に脆弱性診断を行うことができます。

アプリファイルのみで診断可能。ソースコードは不要です

ソースコードが入手できないアプリでも診断できます。
アプリが使用しているライブラリ（広告モジュール等）についても同時に診断できます。

脆弱性を指摘するだけでなく対処方法も提示します

診断結果には、検出された問題に対する具体的な対処方法まで記載されています。レポートを参照すれば解決のために何をすれば良いかが簡単に理解できます。

「脆弱性」に加え「マルウェアと間違えられやすい項目」や「品質に関する項目」も検出します

無駄なPermissionや、不要な機能が含まれていることで、マルウェアと誤解されてしまうアプリも多く存在します。RiskFinderは、このようなアプリの品質に関するチェックも行います。

総務省の「スマートフォン プライバシー イニシアティブ」に準拠するための情報を出力します

総務省の「スマートフォン プライバシー イニシアティブ」に準拠したアプリを作成するための情報を出力します。開発者が、利用者のプライバシーポリシ保護を意識したアプリを作成できるように支援します。

Androidアプリのセキュリティについて現時点で発信されている情報を網羅しています

RiskFinderの診断項目は、リスクファインダー株式会社のノウハウに加え、IPA（情報処理推進機構）、JSSEC（日本スマートフォンセキュリティ協会）から発行されている情報を網羅しています。

Androidの最新情報に素早く対応します

リスクファインダー株式会社のグループ企業であるタオソフトウェアは、AndroidがGoogleより発表された当時から研究開発を行っている、日本において老舗のAndroidアプリ開発会社です。受託開発、研究開発と並行して、常にAndroidの最新の情報を追いかけています。RiskFinderにも最新の情報、ノウハウが反映されます。

RiskFinderはアプリの安全性をチェックします。

RiskFinderはAndroidアプリの脆弱性診断WEBサービスです。
RiskFinderを使用することにより簡単に脆弱性を診断できるようになり、アプリの品質を一定に保つ事が可能になります。

apkファイルを選択してアップロード

診断結果表示

RiskFinderの利用シーン

RiskFinderは誰でも簡単に利用できるので、様々な場面で活用できます。

アプリ開発時の品質担保

開発担当者の意識や経験に依存してセキュリティやプライバシー保護に関する実装をしていては、アプリの品質を維持することはできません。
RiskFinderを使用してアプリを診断する事で、技術者のレベルに左右されない、安定した品質のアプリを作成できます。また、RiskFinderが出力したレポートは、脆弱性やプライバシー保護に関する検査記録として納品することもできます。

開発委託したアプリの受け入れ検査

アプリ開発を外部に委託した場合、委託側は納品されたアプリを検査することになります。
委託側には通常、専門知識をもった技術者がいないため、脆弱性や利用者のプライバシー保護等について検査することは困難です。
RiskFinderが出力する診断レポートを使用すれば、委託側と開発側が的確なコミュニケーションをとれるようになり、利用者が安心して利用できるアプリをリリースできます。

脆弱性診断業務・テスト業務支援

脆弱性診断担当者・テスト担当者は、まずアプリ全体を解析して構造を把握し、重点的に調査すべきポイントを明らかにする必要があります。RiskFinderは短時間でアプリ全体をもれなく解析し、レポートを作成します。担当者はこのレポートを元にすることで、より高度な分析作業に注力できるようになります。結果として、高品質で競争力のあるサービスを顧客に提供する事が可能になります。

社内導入アプリの決定（MDM）

社内導入するアプリを選定する場合、そのアプリがマルウェアでないことや、脆弱性がないことを確認する必要があります。
RiskFinderを使用してアプリを診断することで、マルウェアやグレーゾーン（利用者の個人情報を使用するが目的が不明）のアプリを検出でき、アプリの採用／不採用の判断材料を得ることができます。

掲載アプリの選定（アプリ紹介サイト・書籍）

アプリの紹介サイトや書籍で紹介されたアプリは優良なアプリとして推薦されたものとして、多くの利用者が使用します。サイトの運営者や書籍の編集者は、掲載するアプリが安心、安全なものであることを確認することが必要です。RiskFinderを使ってアプリを診断する事でアプリの問題を把握できるので、マルウェアや不適切なアプリを誤って紹介してしまうような事態を未然に防ぐことができます。

基本機能

1. アプリケーション脆弱性検出機能

アプリの脆弱性や、プライバシー、品質に関する問題を検出します。また、アプリ内の情報を一覧できるようにします。

RiskFinderは脆弱性検出するだけのツールではありません。
利用者が安心して利用できるアプリを作成するために必要となる項目を検出します。

検出された項目は以下の３つの視点で分類されます。

１. カテゴリ
検出された問題が、アプリのどの部分で検出されたのかを示す情報です。

２. 種別
検出された問題が、脆弱性なのか品質の問題なのかといった種類を示す情報です。

３. リスクレベル
検出された問題が、必ず対処しなければいけない問題なのかといった重要度を示す情報です。

問題に対処する際には、これらの情報を使って項目を整理する事で、対処しやすくできます。

検出項目のカテゴリ

RiskFinderが検出した情報は、以下のカテゴリに分類されて一覧され、情報を簡単に把握できるようになっています。

カテゴリ名	内容
Information	アプリ名、パッケージ名、バージョンコード等アプリの基本的な情報を確認できます。
Manifest Risk	AndroidManifest.xml内の脆弱な設定や、誤った設定等を確認できます。
Permission	誤ったPermission定義や不要なPermission、利用者から危険なアプリに見えるPermissionの組み合わせの存在等を確認できます。
File Access	外部ストレージの誤った利用や、他のアプリからアクセス可能なファイルを作成している処理の存在等を確認できます。
String Resources	ここに一覧された情報を使用して、パスワード等の重要な情報がハードコードされていないか、コメントに不適切なものがないか確認できます。
Logs	ログ出力メソッド、printStackTraceメソッドの使用の一覧です。この一覧を使用して重要な情報がログ出力されていないかどうか確認することができます 。
Network	どこと通信を行っているか、WebViewの脆弱性の影響を受けないか、通信時の例外を無視していないか等、通信に関連する問題点を確認できます 。
Module	アプリが内蔵している第三者モジュールが危険なものでないか、ライセンス契約が必要なものでないか等を確認できます。
Cryptography	推奨されないHash関数、強度が十分でない暗号化ロジック等がないか確認できます。
Secure Logic	外部のdexファイルの読み込み、リフレクションの使用等、セキュリティ上注意が必要な実装の存在、OSバージョンに強く依存した実装の存在を確認できます 。
Privacy Policy	利用者のプライバシーに配慮が必要な処理の存在を確認できます。
Power Saving	バッテリーに負荷をかける処理の存在を確認できます。

種別

RiskFinderは、検出された項目を以下の４種類の種別で分類します。

- **脆弱性に関する項目**
- **センシティブな情報に関する項目**
- **品質に関する項目**
- **バッテリーに影響を与える項目**

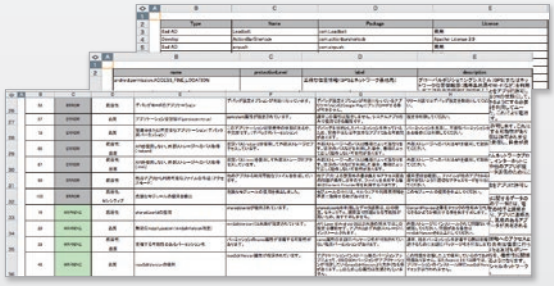
リスクレベル

RiskFinderが検出した情報は、重要度に応じて「ERROR」、WARNING」、「CONFIRM」、「INFO」の４つのレベルに分かれており、
優先的に対応すべき項目が一目で分かるようになっています。
また、検出結果は、「検出内容」、「検出理由」、「対処方法」の３ブロックで表現されており、具体的な対処方法まで記載しています。レポートを参照すれば解決のために何をすれば良いか簡単に理解できます。

レベル	表示例
ERROR	明らかな誤りであり、修正が必要なものです。
WARNING	脆弱性と考えられる項目ですが、アプリの仕様上そうならざるを得ない場合があるため、設計通りであるか確認が必要なものです。 例えば、不特定多数のアプリからインテントを受け取るように設計された公開Activity等があります。
CONFIRM	この項目だけでは脆弱性とはなりませんが、他の処理との関連によっては脆弱性となりうるものです。 例えば、SDカードへの書き込み権限を持つアプリの場合、脆弱性となるかどうかは書き込む内容に依存するため、SDカードへ出力される内容の確認が必要となります。
INFO	直接脆弱性につながるものではありませんが、アプリの使用状況を踏まえて対策することを検討してもよいと思われるものです。

2. 解析結果のダウンロード機能

診断結果をHTML形式、Excel形式でダウンロードすることができます。
会議等での使用、RiskFinderのアカウントを持っていない方との
情報共有が可能になります。
Excelデータは、「リスクレベル」と「種別」でフィルタリングできるため、
対処が必要な項目を絞り込んで表示させることができます。



利用形態

RiskFinderの利用方法には以下の3タイプがあります。

1．パブリッククラウド

リスクファインダー株式会社がクラウド上に構築しているサーバを複数のお客様で共用していただく形式です。

2．プライベートクラウド

リスクファインダー株式会社がお客様専用のサーバをクラウド上に構築します。

※サーバ構築費用が発生します。詳細はお問い合わせ下さい。

3．オンプレミス

お客様が所有するネットワーク上にサーバを構築して利用していただく形式です。

※ サーバ構築費用が発生する場合があります。利用状況確認のため、サーバと弊社の間に通信が必要となります。
詳細はお問い合わせ下さい。

課金形式・価格

RiskFinderには以下の2タイプの課金形式があります。
初回契約時にどちらかの種別のチケットを、１年間の予想使用回数分ご購入ください。
チケットの有効期限は１年となります。

1．アプリケーション単位課金

検査対象となるアプリケーションに対して課金が発生する形式です
検査期間（初回検査から３０日間）中は検査回数の制限はありません。
検査回数が多く、かつ検査対象アプリの本数が少ない場合に向いています。

	価格
1本（３０日間有効）	￥100,000

※ 別途、初期費、アカウント維持費が必要となります。詳細はお問い合わせ下さい。

2．検査回数課金

検査1回単位に課金が発生する形式です。
検査対象、または検査回数の大きな増減が見込まれる場合に向いています。
（多数のアプリを頻繁に検査するような場合は、ご相談ください。）

	価格
1回	￥50,000

※ 別途、初期費、アカウント維持費が必要となります。詳細はお問い合わせ下さい。

その他

お客様の運用形態に合わせてRiskFinderをカスタマイズする事も可能です。
課金形式についても運用に合わせて柔軟に調整させていただきます。お気軽にご相談ください。

RiskFinder

リスクファインダー株式会社

〒110-0015
東京都台東区東上野2-1-1 フリーアネックスビル8階
Phone：080-8873-8243 ／ FAX：03-6802-8347
E-mail：info@riskfinder.co.jp ／ Homepage：http://www.riskfinder.co.jp/

検出項目について

RiskFinderは、アプリに対して500項目以上のチェックを行い、脆弱性や問題点を検出します。
Androidアプリのセキュリティについて現時点で発信されている情報を網羅しています。

① 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　インプレスジャパン株式会社発行）
② 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（独立行政法人情報処理推進機構）
③ Android アプリのセキュア設計・セキュアコーディングガイド（一般社団法人日本スマートフォンセキュリティ協会 セキュアコーディンググループ）
④ スマートフォン プライバシー イニシアティブ（総務省 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）
⑤ Androidアプリの脆弱性の学習・点検ツール「AnCoLe」（独立行政法人情報処理推進機構 開発協力 タオソフトウェア株式会社）

独自のチェック項目

これらの項目に、さらにRiskFinder独自のチェック項目を追加しています。

1. アプリが内蔵している第三者のライブラリの問題を検出

アプリの開発担当者も内部を把握していない、第三者のライブラリも診断し、問題を検出します。
一般的なライブラリはRiskFinderに登録されているので、ライブラリの機能、ライセンス形態等の情報を確認できます。

2. APIとPermissionの関連付けによるチェック

RiskFinderはPermissionとAPIの依存関係の情報を内蔵しているため、以下のようなチェックが可能です。
・Permissionを必要とするAPIを使用しているが、Permissionの利用が宣言されていない
・Permissionの利用が宣言されているが、これを必要とするAPIを使用していない

3. バッテリーに負荷をかける処理を検出

バッテリーに負荷をかける処理を検出し、改善策を提案します。

4. Android OSのバージョンに応じた不具合の検出

特定のバージョンのOSにのみ存在する問題も検出します。アプリがサポート対象とするOSバージョンに応じたチェックにより問題を検出し、改善策を提案します。

5. Android推奨ルールからの逸脱を検出

Googleが提供しているデベロッパーズガイドに準拠していない点を検出し、改善策を提案します。

検出項目一覧

脆弱性に関する項目

・Activityの脆弱性
・Serviceの脆弱性
・ContentProviderの脆弱性
・BroadcastReceiverの脆弱性
・AndroidManifest.xmlの脆弱性
・使用できないPermission
・不要なPermission
・外部記憶装置へのアクセス
・ファイルのアクセス制限不備
・Log出力メソッドの使用
・JavaScriptが使用可能なWebView
・JavaScriptを使用しているAsset内HTMLファイル
・SSL通信時の証明書検証不備
・アプリ内に含まれているURL
・安全性の低い暗号化ロジック
・プログラム内に組み込まれているライブラリの問題　等

品質に関する項目

・誤った証明書の使用
・AndroidManifest.xml内の不要な項目
・デバッグモードの設定
・OSバージョン固有の問題
・廃止されたAPIの使用
・プライバシーに配慮が必要な処理
・Android推奨ルールからの逸脱
・実行時エラーとなる可能性　等

マルウェアと疑われる可能性のある項目

・グレーゾーンアプリの疑いのあるPermissionの使用
・危険なPermissionの使用
・広告ライブラリの使用
・危険なライブラリの使用
・グレーゾーンのライブラリ使用　等