



「スマートフォン時代における 安心・安全な利用環境の在り方に関するWG」

資料7

スマートフォンセキュリティ時代！ 「アンドロイダー」の取り組み

2012年12月21日
アンドロイダー（株）

会社概要



■ 商号 : (株) ルクレ (2011.10.1社名変更)

■ 設立 : 1995年9月20日

富士通（株）の社内ベンチャー制度から創業

■ 主要サービス



会員数35万人の「デジカメ写真」交歓サイト



会員数120万人のデコレメサービス



業界トップシェアを誇る工事写真管理ソフト



国内実績No.1を誇る監視カメラソフトウェア



アンドロイダーとは

国内最大級のAndroid情報サイト!!



◆サービス開始日	2010.2. 1 (Open)
◆公認アプリ数	3,602 アプリ
◆公認デベロッパー数	1,220(法人/個人)
◆隊員数	1,126人
◆フォロワー数	18,732人

※2012年12月17日 時点

圧倒的な更新頻度と情報量、ユーザー目線のコンテンツでAndroid端末エントリーユーザーからアプリ開発者様からも篤い支持をいただいている弊社運営サイトです。

2012年10月1日 安全なアプリのみを紹介するプラットフォームに大幅リニューアル

アンドロイダーの業務領域



- サイト企画/運営/広告/コンテンツ提供
- アプリ/システム開発/端末検証
- 講演/研修イベント支援
- コンサルタント/アグリゲート

レビューサイトを運営する開発会社の特徴を活かし
アンドロイドに関する幅広い業務領域をカバー
セキュリティの啓蒙においても広範囲な発信が可能です

セキュリティに関する悩み



スマートフォン利用者の急増により不正アプリのリスクも顕在化
デベロッパー、ユーザー、各種媒体それぞれがアプリに関する悩みを抱えている

誰が解決するのか？

デベロッパー

不正アプリの疑いがかけられる。



各種媒体

アプリの安全性を証明できない。

ユーザー

安全なアプリを知る方法がない。

セキュリティ時代のアン드로이드



セキュリティリスクが顕在化した今、端末利用者、メーカー、デベロッパー、各種媒体など幅広いパートナーとの事業領域を持つ「アン드로이드」が最優先で取り組むべきはセキュリティ！



安全な「アプリデータベース」を構築
情報提供と啓蒙を推進



セキュリティの取り組み



公認制度とは

アンドロイダーでは、安全性の確認がとれた公認アプリのみを掲載
安全性を高めるため「公認認定制度」を策定、運用

公認デベロッパー

デベロッパーの実在性

アンドロイダーに登録されるアプリの開発者が、物理的、運用的に
実在していること。



公認アプリ

パーミッションの正当性

アプリが、正当なパーミッションを使用していること。

ウイルスのスキャン

アプリが、不正なデータ、Webサイトへアクセスしない。
また不正な動作をしないこと。



公認アプリ掲載までの手順

開発者の
実在性を確認

公認開発者申込み

公認開発者審査

アプリの
安全性を確認

セキュリティチェック

掲載審査

公認アプリとして掲載

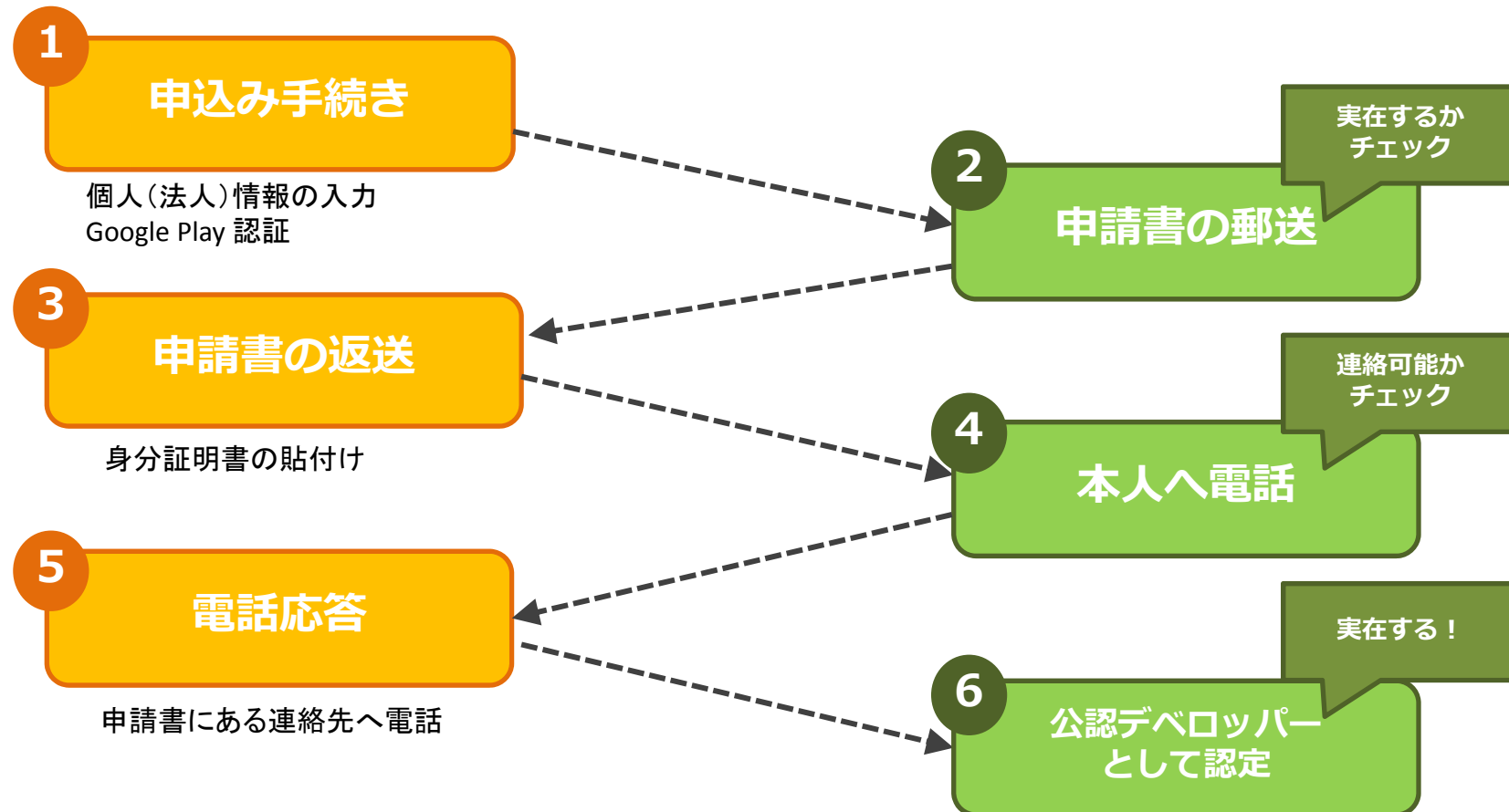
外部メディアへの情報提供



公認デベロッパー登録の流れ

デベロッパー

運営事務局



公認アプリ登録の流れ

デベロッパー

運営事務局

専門パートナー

1 アプリ情報の
投稿

3 使用目的の
説明

※不要なパーミッションを
使われている場合のみ、
説明が求められる。

2 セキュリティチェック

APKの解析

パーミッションの確認
・リスクコンビネーション
・使用目的の正当性を確認

ウィルスチェック
・ウィルス／マルウェア／
フィッシング／アプリの動作

4 公認確定

NEXT ACTION

プライバシーポリシー組
込済の場合は機能との
差異確認。未掲出の場
合は組込を促す！

(Taosoftware)
リスクの調査
アドバイス

(TrendMicro)
アドバイス

デベロッパーへの啓蒙

デベロッパーに対してセミナーを開催。
セキュリティの重要性を直接啓蒙、公認制度への参加を働きかけている。





まとめ

端末利用者の安全性を図り、業界全体に情報提供、啓蒙することで
オープンプラットフォームの健全な発展に寄与

アプリ制作者を
集め

なぜ集められるのか？

- これまでの関係性
- アンドロイダーは多数の
露出先を持っている
- 作り手にとって露出は恒
常的な課題
- 安全性の証明が可能

アプリの安全性を
確認して

どの様に安全性確認
啓蒙を行うのか？

- 独自のセキュリティポリ
シー
- 身元確認を前提とした
公認ベンダー制度
- 識者連携によるセキュア
チェック
- チェック結果のフィード
バックとアドバイス

安全なアプリ情報
のみ提供する

誰にどの様に情報を
提供するのか？

- 端末利用者だけでなく
企業、媒体各社等に広く
情報提供
- 自社媒体、一般媒体、
キャリア、メーカー、
コンサル、セミナーなど
を通じて情報を提供



デベロッパーのセキュリティ意識



セキュリティチェック結果サマリー

セキュリティチェック 実施数	約 3,000本
セキュリティに関する デベロッパー 問い合わせ件数	約 2,600本
広告モジュールに関する 問い合わせ	約 2,000本
公認アプリ「リジェクト数」	約50本

- 法人、個人制作に関わらず予想以上に不要な権限取得を行っているアプリが多い
- 後日実装する等を理由に事前に取得している権限が多い。



傾向

- ・ **セキュリティに関するデベロッパーの意識は総じて低い。**
⇒アプリの不正コピー防止など制作者利益に関わる内容には敏感だが、利用者利益に関わるパーミッション取得への意識は低い
- ・ **パーミッションに関する理解・知識不足**
⇒問い合わせに対する回答から理解、知識不足が伺える
また弊社側が指摘をしないと気付かないケースも散見
- ・ **不要なパーミッションを外すことに積極的ではない**
⇒実作業は該当箇所の文字列を削除するだけだが、企業等では申請等も必要になるため対応を避ける傾向がある
- ・ **アプリ提供企業側の理解、意識の低さ**
⇒企業名義で提供されているアプリは外注制作が多く、リスクに関してノーチェックでリリースされているケースが多い
(問い合わせをしても要領を得ず対応が困難)

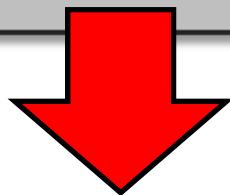


【今後の取り組み】 「ホワイトアプリ」情報の外部提供

オープンマーケットでの 「グレーアプリ」とは



アプリ制作者の意図に関わらず
利用者に不利益を与える
恐れがあるアプリ



オープンマーケットでは
大量の「グレーアプリ」が流通

「グレーアプリ」の問題点



Google play

総数 70 万強のアプリが玉石混合の状態

ブラックアプリ
(明らかに危険)

グレーアプリ
(危険/安全判別困難)

ホワイトアプリ
(安全)



問題点

明らかに危険な「ブラックアプリ」、安全な「ホワイトアプリ」は
セキュリティアプリなどで判別可能

反面 「グレーアプリ」は「危険/安全」の境界が曖昧
セキュリティアプリだけのチェックでは正しい判別が困難

仕分けが困難な「グレーアプリ」

チェック項目

Step①

セキュリティアプリ導入

Step②

要求パーミッションからのリスク予見

Step③

プライバシーポリシーの読み解き/実挙動比較

Step④

広告モジュールの挙動確認

問題点

必ずしもアプリリスクを
「ブラック」「ホワイト」に
仕分けすることができない

一般利用者は理解できない

記述内容、実挙動精査など
リスク予見は困難

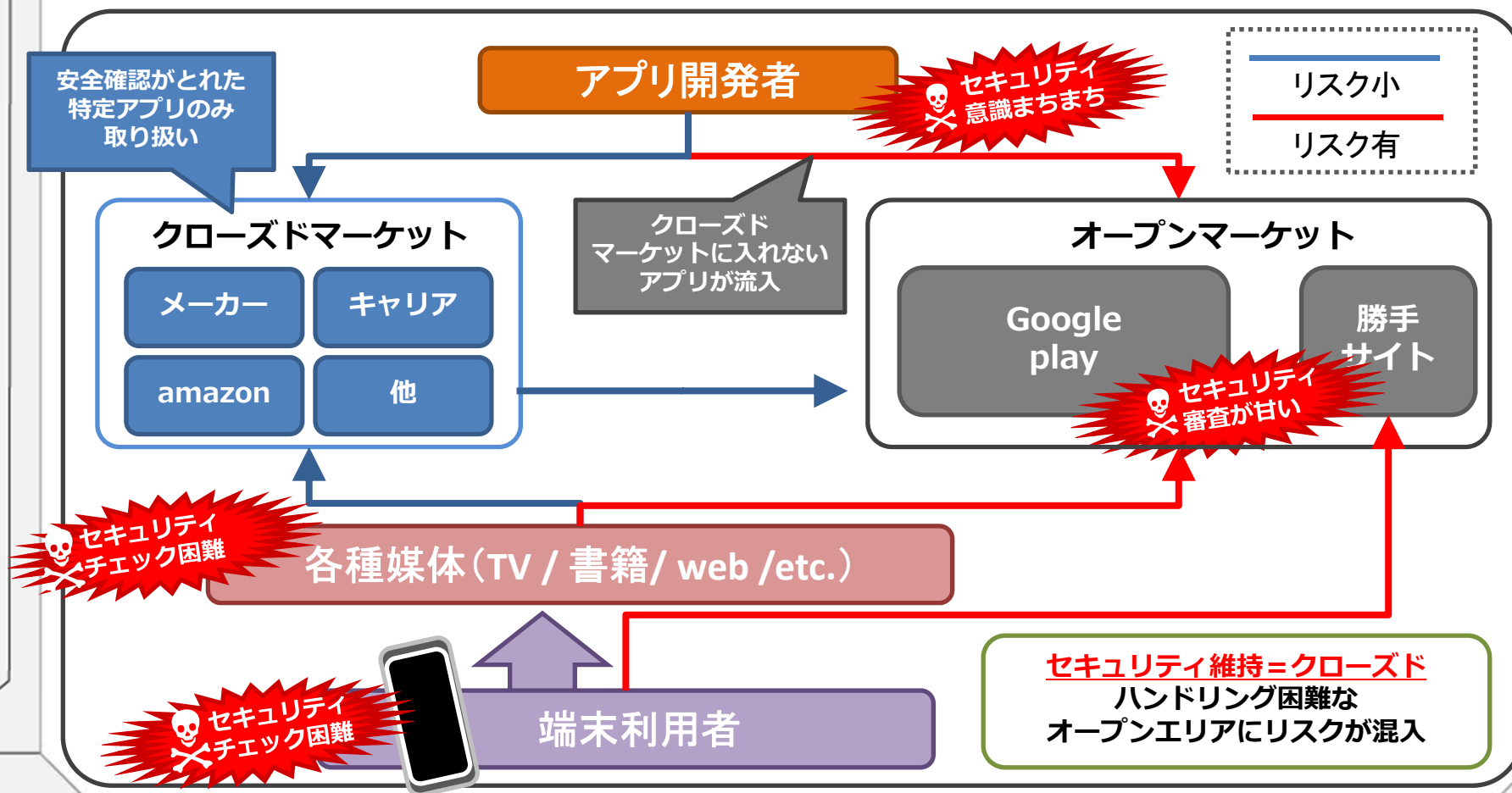
モジュール提供者特定、
挙動精査など
有識者以外の実施困難

※より高い精度を求める場合、脆弱性確認なども必要

有識者が複合的に検証する上記項目を利用者自身が行い
「グレーアプリ」のリスクを推し量ることは困難

「アプリ」の認知経路に潜むリスク

端末の急激な普及が進む中、利用者保護は不十分
オープンマーケットのアプリ検証を行うプレイヤーが必要





近日リリース

Androider[®]API



基本機能は無料提供予定

アンドロイダーの役割



「ホワイトアプリ」情報を積極的に外部へも提供
アンドロイドプラットフォームの発展に貢献いたします

