モバイルアプリケーションが取得している プライバシー情報の調査

細谷 竜平[1]　角田 裕太[1]　森 達哉[2]　齋藤 孝道[3]

概要：モバイルアプリケーションは，利用者の同意のもと様々な情報を端末から収集している．しかしながら，収集する情報の詳細を開示しないケースが多いため，利用者の想像を超えたデータを収集している可能性がある．本論文では，Android 公式マーケットでリリースされている 1,704 個の無料アプリケーションを調査し，アプリケーションが取得している利用者のプライバシー情報を API レベルで解析した．調査の結果，アプリケーションの 97.54%が何らかの情報を端末から取得していることがわかった．特に，683 個 (全体の 40.08%) は端末のシリアル番号を，1,211 個 (全体の 71.06%) は位置情報を，669 個 (全体の 39.26%) はインストール済みアプリケーション名を取得していることが判明した．

キーワード：Android アプリケーション, アクセス許可，端末情報，Android API

Measurement Study of the Privacy Information Collected by Mobile Apps

Ryohei Hosoya[1]　Yuta Tsunoda[1]　Tatsuya Mori[2]　Takamichi Saito[3]

Abstract: Mobile apps collect various personal information under the consent of users. However, as such apps could fail to present the details of the information they collect, they may be collecting data, which goes beyond the users' expectations. In this work, we study how mobile apps collect user's privacy data. To this end, we analyze 1,704 apps released on the official Android market using API analysis. We revealed that 97.54% apps collect some information from devices. Especially, 683 apps (40.08%) collect serial numbers of devices, 1,211 apps (71.06%) collect the location information of the devices, and 669 apps (39.26 %) collect information about the previously installed applications on the devices.

Keywords: Android Application, Access Permission, Device Information, Android API

1. はじめに

スマートフォンの普及率は年々増加しており，発売当初である 2010 年からわずか 5 年で約 60%も増加している [1]．それに伴い，Google Play ストア [2] を筆頭にモバイルアプリケーションのマーケットが広がりを見せている．AppBrain[3] によると，Google Play ストアでリリースされているアプリケーションの数は 2017 年 8 月時点で 317 万を超えている．この普及率の高さから，モバイルアプリケーションのセキュリティやプライバシーの確保は常に求められている．その中でも，アプリケーションによる利用者のプライバシーに関わる情報の取得に関する議論は多く行われている．

モバイルアプリケーションは，容易に利用者の端末情報を取得することができる．この情報を取得するには，モバイルアプリケーションは OS が独自に定めた API を用いる．これらの情報は利用者の許可 （以降，アクセス許可と呼ぶ）のもとアプリケーション内で利用されている．しか

[1] 明治大学大学院
Graduate School of Meiji University
[2] 早稲田大学
Waseda University
[3] 明治大学
Meiji University

し，利用者がアクセス許可を行う際に，その情報の概要は表示されるが，具体的な情報は表示されない．例えば，利用者がアプリケーションに対し「端末のステータスと ID の読み取り」を許可すると，アプリケーションは利用者の電話番号や通話相手の電話番号などへのアクセスが可能となる．これは，利用者の意図していない情報にアプリケーションがアクセスするという状況を引き起こす可能性がある．また，アプリケーションをインストールする際にアプリケーションが取得する情報を確認していない利用者は多い．IPA の調査 [4] によると，「スマートフォンにおいてデータが盗難・漏えいする不安がある」と答えた利用者が全体の 70.6%であった．しかし，「Android アプリケーションをインストールする際にアクセス許可を確認する」と答えた利用者は全体の 19.3%のみであった．これらのことから，アプリケーションの利用者はプライバシー情報の流出に関する不安を抱えながらも，アクセス許可を確認せずにアプリケーションをインストールしていることが分かる．以上より，我々は，アプリケーションが利用者の端末より取得している情報を把握することが重要であると考えた．

そこで，本論文では，Google Play ストアでリリースされているカテゴリ別ダウンロード数ランキング上位 60 のアプリケーションを収集し，合計 1,704 個を解析した．そして，アプリケーションが取得している端末の情報を調査した．調査にあたって，取得される情報を API レベルで分類することで，既存研究 [6][7] よりも詳細な取得情報の調査を実現した．

調査の結果，調査対象のアプリケーション 1,704 個の 97.54%が端末の何らかの情報を取得していた．特に，以下の事実が判明した．

(1) 683 個 (全体の 40.08%) は，ハードウェアのシリアル番号を取得していた
(2) 1,211 個 (全体の 71.06%) は，端末の位置情報を取得していた
(3) 669 個 (全体の 39.26 %) は，インストール済みアプリケーション名の情報を取得していた

さらに，カテゴリごとの売上がトップのアプリケーションの中には，電話番号や International Mobile Equipment Identity（IMEI）を取得していることが分かった．また，1 つのアプリケーションが多種類の情報を取得していることも分かった．

2. 関連研究

モバイルアプリケーションに関する研究は，マーケット立ち上げ当時から現在に至るまで盛んにされている．Martin[5] らは，2015 年までに行われたモバイルアプリケーションやマーケットに関する研究論文を調査した．その結果，Google Play ストアと App Store の 2 つの大型マーケットの立ち上げからわずか 7 年で，既に 180 以上の論文が発表されていることが分かった．

その研究の中には，モバイルアプリケーションによる利用者の情報取得に関するものもある．Grace ら [6] は，広告ライブラリに関連するプライバシーリスクを特定する静的分析ツールである AdRisk を提案した．このツールを用いて Google Play ストアでリリースされている 100,000 個のアプリケーションを調査し，52,067 個のアプリケーションが広告ライブラリを使用していることを示した．また，その 31 %が複数の広告ライブラリを使用していることも示した．さらに，彼らは調査した 100 の広告ライブラリの大部分が利用者の端末情報を収集していることを示した．

Senevirante ら [7] は，無料のアプリケーションが利用者の情報を取得していると言われているが，同様に，有料のアプリケーションも利用者の情報を収集していることを示した．有料アプリケーションの 60%が利用者の情報を収集したのに対し，無料アプリケーションでは 85%であった．また，彼らは収集された 3,605 個の Android アプリケーションの 20%が 3 つ以上の広告ライブラリやアナリティクスライブラリに接続されていることを示した．

いずれの研究も，アプリケーションに組み込まれているサードパーティライブラリによる情報の取得に関するものである．しかし，これらの研究では取得される情報が具体的に掲載されていない．例えば，取得されている情報の中に“電話帳情報の取得”という表現があるが，それは電話帳に載っている名前のみを表すのか，あるいは電話番号や通話時刻も表しているのかが分からない．プライバシーを気にする利用者のためにも，取得されている情報の細かい分類が必要である．

3. 情報の取得について

3.1 Android アプリケーションによる情報取得

モバイルアプリケーションなどのシステムは，利用者の端末情報を取得することで，サービスの向上に役立てている．端末情報の取得はあらかじめ利用者から情報利用の許可を得るという前提のもとで行われている．その中でも，Android では，配布されるアプリケーションパッケージ (APK) 内の AndroidManifext.xml というファイルの中で利用者に対する許可 (パーミッション) の情報を定義する．利用者の許可が降りると，アプリケーションは OS が独自に定めた API を使用することで，利用者の端末情報を取得できる．

端末情報を取得する API は，アプリケーションに組み込まれている広告ライブラリでも使用されている．広告ライブラリは，開発者が収益を得る目的でアプリケーションに組み込まれている．この広告ライブラリによって，アプリケーションは，開発者の意図とは別に利用者の端末から情報を取得している可能性がある．

Android 端末においてアプリケーションが取得可能な情

表 1　コード解析によって得られる結果の例

出力される情報	説明	例
アプリ名	アプリケーションを表す識別子	com.facebook.katana
パーミッション	アプリケーションが端末に求めるアクセス許可の情報	android.permission.READ_PHONE_STATE
クラス	アプリケーションの実装に使用されている Java のクラス名	com.facebook.widget.tiles.AutoGeneratedBindings.java
メソッド	アプリケーションのコードにて呼び出されているすべてのメソッド	android.hardware.Camera.getNumberOfCameras()

報は多岐にわたる．例えば，ハードウェアに関する情報であれば機種名や GPU の種類，センサーの有無，メモリやストレージの容量などがある．ネットワークに関する情報であれば，IP アドレスや Wi-Fi の SSID，登録済みの Wi-Fi アクセスポイントなどが挙げられる．また，電話に関する情報であれば電話番号や SIM のプロバイダ名，連絡先の情報が挙げられる．その他にも，インストール済みアプリケーションや IMEI と呼ばれる端末の識別子，端末のルート証明書の一覧，利用者の位置する座標 (位置情報) などがあり，アプリケーションは様々な情報を取得することが可能である．

3.2　プライバシーに関わる情報

本論文では，調査を行うにあたって，利用者が取得されることに嫌悪感を抱く情報（以降，プライバシー情報と呼ぶ）がアプリケーションによって取得されているか確認する．本論文では，メールアドレス，電話番号，位置情報，写真の情報，いずれか，または，これらの組み合わせをプライバシー情報と定義する．これらの情報は，前述した IPA の調査 [4] の「インターネット上に漏洩したら困る情報」というアンケートにて 50%以上の回答があり，かつ，Android で取得できる情報をもとに我々が選定した．この調査によると，メールアドレス，電話番号，住所または氏名といった情報を取得されることに嫌悪感を抱く利用者が最も多く，75%も存在した．また，その他にも利用者の位置情報や写真を取得されることに嫌悪感を抱く利用者は 50%近く存在した．このうち，Android アプリケーションでは，メールアドレス，電話番号，位置情報または写真の情報を取得することができる．

4.　調査方法

我々は、アプリケーションのコード解析を行い，API の呼び出し状況を確認することによってモバイルアプリケーションが取得している情報を調査した．今回は Android アプリケーションを対象に調査を行った．

4.1　調査対象

我々が調査対象としたアプリケーションは，Google Play ストアから収集した 1,704 個のアプリケーションである．これらの APK ファイルは，Google Play ストアの無料アプリケーションの日本国内のダウンロード数ランキング (2017/08/04 現在) において，全 35 カテゴリからそれぞれ上位 60 のアプリケーションを収集し，重複を除いたものである．

4.2　API と取得できる情報の対応表

我々は，Android 公式のリファレンス [10] に記載されている API，及び，それにより取得可能な情報の組みにした表（以降，API 対応表と呼ぶ）を作成した．この表には，183 個の API と取得可能な情報との対応が示されている．この API 対応表の一部を表 2 に示す．例えば，コード内で android.content.pm.PackageManager.getInstalledApplications() という API が呼び出されていた場合，そのアプリケーションは，端末にインストールされているアプリを取得していることになる（表 2 参照）．

表 2　API 対応表の一部

API	取得情報
android.content.pm.PackageManager .getInstalledApplications()	インストール済みアプリ
android.telephony.TelephonyManager. getDeviceId()	IMEI

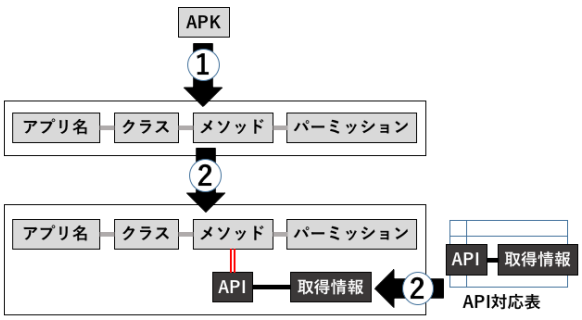

図 1　アプリケーション調査の概念図

4.3　解析の仕組み

我々の行った解析の概念図を図 1 に示す．本論文では，対象の APK ファイルに対して以下の 2 つの過程（図 1 の “1”，“2” に対応している）を通して解析を行った．本節では，それぞれの過程について説明する．

(1) **APK ファイルに対するコード解析**

調査対象の APK ファイルに対してコード解析を行う．Androguard[8] はアプリケーションのコード内で使用されているクラスやメソッドを抽出することができる．我々は，この Androguard によって抽出された値（表 1 参照）を用いた

(2) **コード解析の結果と API 対応表の対応付け**

上記 1 の解析によって出力された情報と，4.2 節で紹介した API 対応表を紐付けることで，アプリケーションが取得している情報を推察する．具体的には，表 1 で示している “メソッド” と，API 対応表 (表 2) が示す “API” を紐付ける．こうすることで，“アプリ名” と “取得情報” の対応関係を得ることができる (図 1 参照)．

我々は，以上の調査を 1,704 個のアプリケーション全てに対して行い，アプリケーションごとに取得している情報を集計した．

5. 調査結果

5.1 取得情報の集計

表 3 に，取得情報とそれに対応するアプリケーションの数および割合を示す．“取得情報” の欄にはアプリケーションが取得している情報を示し，それに対応する “アプリ数” の欄はその情報を取得しているアプリケーションの数を示している．“割合 (%)” の欄には全体のアプリケーションの個数 (1,704 個) に対する “アプリ数” の割合を示している．

調査結果により，最も取得されている情報は，Wi-Fi 関連の機能の対応有無，カメラの搭載台数，GPS の対応有無であることが分かった．これらの情報を取得しているアプリケーションの数は 1,662 個であり，調査対象のアプリケーションの 97.54%にあたる．また，その他にもインストール済みのアプリケーションやハードウェアのシリアル番号，IMEI といった情報が 30%から 40%のアプリケーションによって取得されていることが分かった．

プライバシー情報に着目すると，位置情報が見られるが，電話番号やメールアドレスといったプライバシー情報は上位には見られない．

5.2 カテゴリ別トップのアプリにおける取得情報の分布

表 4 に，それぞれのカテゴリ別ランキングのトップに位置する 20 アプリにおける取得情報の分布を示す．残りの 15 アプリは付録の表 A·2 に示している．表 4 中の番号は，付録の表 A·1 にてアプリ名と対応している．例えば，表 4 の最上行の “1” は，jp.co.yahoo.android.news というアプリケーションを示している．アプリケーションが取得している情報である場合は “o”，取得していない情報は空白で示されている．

表 3 上位の取得情報とその情報を取得しているアプリの数の対応表

取得情報	アプリ数	割合 (%)
Wifi の 5GHz 対の対応有無	1662	97.54
ラウンドトリップタイムのサポート有無	1662	97.54
Wifi のパフォーマンスカウンタのサポート有無	1662	97.54
WifiP2pManager(WiFi Direct) のサポート有無	1662	97.54
オフロード接続スキャンのサポート有無	1662	97.54
TDLS のサポート有無	1662	97.54
カメラの搭載台数	1662	97.54
GPS の対応有無	1662	97.54
ピクセル密度の相対値 (mdpi=1.0)	1648	96.71
機種名	1623	95.25
画面サイズ (幅)	1611	94.54
画面解像度の幅	1611	94.54
画面サイズ (高さ)	1603	94.07
画面解像度の高さ	1603	94.07
ビルド ID	1589	93.25
VR 対応 (パフォーマンス維持モード)	1562	91.67
ディスプレイの高さ	1555	91.26
ディスプレイのサイズや濃度	1529	89.73
Wifi の対応有無	1522	89.32
Wifi Direct の対応有無	1522	89.32
Bluetooth デバイスの有無	1522	89.32
Bluetooth Low Energy サポート有無	1522	89.32
カメラのオートフォーカスの対応有無	1522	89.32
カメラのフラッシュの対応有無	1522	89.32
VR 対応	1522	89.32
VR 対応 (高品質)	1522	89.32
タッチパネルのデバイス有無	1522	89.32
マルチタッチの対応有無	1522	89.32
2 箇所以上のタッチ操作の対応有無	1522	89.32
5 箇所以上のタッチ操作の対応有無	1522	89.32
2 箇所以上の画面タッチイベント有無	1522	89.32
5 箇所以上の画面タッチイベント有無	1522	89.32
製造社名	1515	88.91
デバイス名	1425	83.63
SUPL の対応有無	1202	70.54
位置情報	1196	70.19
ディスプレイの ID	1128	66.20
低 RAM デバイス判定	1109	65.08
WebView のデフォルトの UserAgent	1078	63.26
ストレージ (/data) の容量	1077	63.20
製品名	1015	59.57
ブランド名（キャリア、メーカー名など）	1006	59.04
ディスプレイの状態	965	56.63
ヒープの最大サイズ	950	55.75
Android キーストアプロバイダの対応の有無	832	48.83
システム時刻	812	47.65
メモリの容量	772	45.31
ネイティブコードの命令セット	724	42.49
シリアル番号	683	40.08
インストール済みアプリ	669	39.26
IMEI 番号	601	35.27
フォントの相対値 (mdpi=1.0)	581	34.10
画面サイズ	520	30.52
ピクセル密度	520	30.52
ボード (基盤) の名称 (SoC)	479	28.11

表 4 売上トップのアプリケーションにおける取得情報の分布 (1-20)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
インストール済みアプリ	o	o		o	o							o		o				o		o
位置情報	o	o	o	o		o	o	o	o	o	o		o	o			o	o	o	o
IMSI 番号			o																	
シリアル番号	o	o	o	o	o	o		o			o	o					o		o	
IMEI 番号			o		o			o	o		o								o	
ボード (基盤) の名称 (SoC)	o		o		o	o					o			o					o	o
ブートローダのバージョン番号																			o	
ブランド名	o	o	o		o	o	o	o	o		o			o					o	o
ネイティブコードの命令セット	o		o	o	o						o			o					o	o
ネイティブコードの第 2 命令セット	o				o						o			o					o	o
デバイス名	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o
ハードウェア名			o		o													o	o	
製造社名	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
システム時刻	o	o	o		o	o	o	o	o	o		o		o	o				o	
接続されている音声機器の情報										o									o	
メモリの容量	o		o	o	o	o	o		o	o	o			o	o					o
ヒープの最大サイズ	o	o	o		o	o	o	o	o		o	o					o			o
ビルド ID	o	o	o		o		o	o			o	o	o	o	o		o	o		o
機種名	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o
製品名	o	o	o	o	o	o	o		o	o	o	o	o	o					o	
ベースバンドバージョン																			o	
電話番号					o														o	
対応暗号スイート		o		o	o	o		o		o		o								
インストール済みルート証明書	o													o						o
接続している Wi-Fi の SSID		o				o		o				o								
Wi-Fi 上での IP アドレス					o															
検知している Wi-Fi スポット		o			o	o														o
登録済みのアクセスポイント					o															
SIM の国コード		o						o						o					o	o
サービスプロバイダの名前			o								o		o	o						o
SIM のシリアル番号 (ICCID)			o					o											o	
Bluetooth デバイスの名前								o												o
ストレージ (/data) の容量		o	o	o	o	o	o	o	o	o	o	o	o	o	o		o	o		o
Web サービスのアカウント情報			o		o			o												
アカウントのトークン取得			o		o		o					o	o							
アカウントのパスワード取得																				
WebView の UserAgent	o	o				o			o		o	o	o		o		o			o
カメラの搭載台数	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o
ディスプレイ名									o	o								o	o	
ディスプレイの ID				o	o	o			o	o		o	o		o		o	o	o	
画面解像度の高さ	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o
ピクセル密度 (xdpi)					o				o		o	o						o		o

なお，取得情報は種類が膨大ため，“対応有無”などを除き，情報の相関が無くなるように我々が選定したものを示している．

調査結果により，トップの人気を誇るアプリケーションでも，多くの情報を取得していることが分かった．

プライバシー情報に着目すると，位置情報以外にも，わずかであるが電話番号が取得されていることが分かる．

6. 考察

6.1 位置情報の取得について

調査結果より，1,196 個 (70.18%) ものアプリケーションが端末の位置情報を取得していることが分かった．位置情報の取得は利用者の許可が必要であるが，地図アプリ以外にも位置情報を取得しているアプリケーションが多いことが分かった．

最近では端末が検知している Wi-Fi のアクセスポイントの情報から位置推定を行う手法が発表され，主に地図アプリの補助機能として使用されている [11]．今回の調査結果より，234 個 (13.73%) のアプリケーションが，端末が検知している Wi-Fi のスポットを取得していることが分かった．また，位置情報と Wi-Fi のアクセスポイントのどちらかを取得しているアプリケーションは 1,211 個 (71.06%) であることから，大半の利用者の位置情報がアプリケーションによって取得されていることが推測できる．

6.2 ユーザトラッキングの脅威

調査結果より，683 個 (40.08%) のアプリケーションでは，ハードウェアのシリアル番号を取得していることが分かった．また，その他にも一部のアプリケーションは IMEI や International Mobile Subscriber Identity (IMSI) を取得していることが分かった．これらの情報は端末ごとに一意に割り当てられているので，これらを取得するアプリケーションは端末を識別することができ，端末のトラッキングをすることが可能となる．しかし，これらの情報は事前に利用者の許可を必要とすることから，利用者は未然にトラッキングを防ぐことができる．

ところが，IMEI などの端末識別情報を取得しなくても，アプリケーションはその他に収集した情報を複数組み合わせることによって端末を識別することができる．Kurtz ら [12] は，自作のアプリケーションをインストールさせ，そのアプリケーションから収集した情報を用いて端末のトラッキングを行い，100%の端末が識別可能，97%の端末が時間経過を伴う識別，つまりトラッキングが可能であることを示した．Kurtz らは，ハードウェアに関する情報など，様々な情報を収集したが，特にインストール済みアプリケーションがトラッキングに十分な情報量を持っていることを示している．我々の調査結果より，669 個 (40.08%) のアプリケーションがインストール済みのアプリケーションを取得しており，その他にも端末に関する様々な情報を取得していることが分かっている．このことから，調査したアプリケーションの大半が，識別番号を用いずに端末をトラッキングするには十分な情報を取得している可能性があると考えられる．

これらの情報は，アプリケーションに組み込まれた広告ライブラリによって収集されている可能性がある．AppBrain[3] によると，Google Play ストアでリリースされているアプリケーションの 52.01%が AdMob[13] という広告ライブラリを組み込んでおり，その他にも多数の広告ライブラリを組み込んでいるアプリケーションが存在する．広告ライブラリは利用者に最適な広告を提供するために，利用者をトラッキングしている可能性がある．広告ライブラリによるトラッキングには Google が推奨している広告 ID を用いてトラッキングを行う必要がある．これは，トラッキングをされたくない利用者が設定によって広告 ID を変更・消去できるためである．本節で紹介した，IMEI などの識別情報や複数の情報の組み合わせを用いた方法では，利用者の意図に反してトラッキングを行うことができてしまう．

7. 今後の課題

7.1 検知精度の向上

本論文ではプライバシー情報の取得状況を API 対応表を用いて確認した．しかし，API 対応表は Android 公式のリファレンスの API のみで作成されているので，それ以外の API を用いて取得されている情報は今回の結果に反映していない．実際に我々が調査した中には baidu などの API を用いてプライバシー情報を取得していると思われるアプリケーションが複数存在した．プライバシー情報の取得状況をより正確に把握するには API 対応表を Android 公式のリファレンスの API 以外にも対応させたい．

7.2 データセットの拡大

今回の調査では国内のランキングに掲載されていた 1,704 個のアプリケーションを対象としたが，この数を増加させることでより幅広い調査が可能となる．Google Play ストアには 317 万を超えるアプリケーションが存在している [3] 上に，世界中には他にも多くのマーケットが存在している．調査の規模を大きくするためにも世界中のアプリケーションを対象とした調査を行いたい．

8. まとめ

調査の結果，Google Play ストアから収集した 1,704 個の無料アプリケーションの 97.54%が端末のなんらかの情報を取得していた．特に，以下の事実が判明した．

(1) 683 個 (全体の 40.08%) は，ハードウェアのシリアル番号を取得していた

(2) 1,211 個 (全体の 71.06%) は，端末の位置情報を取得していた

(3) 669 個 (全体の 39.26 %) は，インストール済みアプリケーション名の情報を取得していた

さらに，電話番号を取得しているアプリケーションが 138 個 (全体の 8.10%) もあった．また，iOS4 以降では取得が禁止されている IMEI を取得している Andoroid アプリケーションも 669 個 (全体の 39.26%) あることが分かった．

これらの事実から，モバイルアプリケーションは，利用者のプライバシー情報を取得していると言える．そもそも利用者はアクセス許可の情報を確認していないと言われているが，確認をしている利用者でさえも想定外の情報が取得されていることが推定できる．このことから，利用者と開発者がプライバシー上の合意を確実にするためにも，開発者やマーケットは，モバイルアプリケーションが取得する情報を利用者に明示する仕組みを推し進めていく必要があると言える．

参考文献

[1] “総務省 平成 28 年度 情報通信白書”. http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc252110.html ,(参照 2017-08-10)

[2] “Google Play ストア”. https://play.google.com/store/ ,(参照 2017-08-03)

[3] “AppBrain”. https://www.appbrain.com/stats , (参照 2017-08-10)

[4] “IPA 2016 年度情報セキュリティの脅威に対する意識調査”. http://www.ipa.go.jp/files/000056568.pdf , (参照 2017-08-03)

[5] Martin, W. Sarro, F. Jia,Y. Zhang, Y and Harman, M., A Survey of App Store Analysis for Software Engineering. IEEE Transactions on Software Engineering, 2016,

[6] Grace, M. Wu, Z. and Xuxian, J. Sadeghi, A.R., Unsafe Exposure Analysis of Mobile In-App Advertisements. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec2012)

[7] Senevirante, S. Kolamunna, H. Seneviratne, A., A Measurement Study of Tracking in Paid Mobile Applications. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec2015)

[8] “Androguard”. http://androguard.blogspot.jp , (参照 2017-07-31).

[9] ”Java Platform API”. https://docs.oracle.com/javase/jp/8/docs/api/, (参照 2017-07-31)

[10] ”Android Developers API Reference”. https:// developer.android.com/reference/packages. html , (参照 2017-07-31)

[11] “Google の位置情報サービスでアクセスポイントを設定する”. https://support.google.com/maps/answer/1725632?hl=ja , (参照 2017-08-10)

[12] Kurtz, A. Gascon, H. Becker, T. Rieck, K. Freiling, F., Fingerprinting Mobile Devices Using Personalized Configurations, in Proc. of Privacy Enhancing Technologies (PoPETS), pp.419, 2016.

[13] ”AdMob”.https://www.google.co.jp/admob/ , (参照 2017-08-10)

付　　録

A.1 表 4 と表 A·2 における番号とアプリ名の対応表

表 A·1 表 4 と表 A·2 における番号とアプリ名の対応表

番号	アプリ名
1	jp.co.yahoo.android.news
2	jp.ne.ibis.ibispaintx.app
3	jp.co.rakuten.carlifeapp
4	jp.hotpepper.android.beauty.hair
5	com.amazon.kindle
6	com.mobisystems.office
7	jp.kakao.piccoma
8	jp.naver.line.android
9	jp.co.i_bec.suteki_happy
10	com.aoizemi.android_client
11	com.ss.android.article.topbuzzvideo
12	com.disney.cars3_goo
13	jp.co.rakuten.kc.rakutencardapp.android
14	com.kurashiru
15	com.bandainamcoent.taikogp
16	com.woodses.denma
17	jp.co.recruit.android.suumo
18	com.google.samples.apps.cardboarddemo
19	jp.ne.goo.oshiete.app
20	jp.co.yahoo.android.apps.navi
21	com.tokyotsushin.rougan
22	jp.linecorp.linemusic.android
23	jp.co.yahoo.android.yjtop
24	com.amanefactory.totsukitoka
25	com.buzzpia.aqua.launcher.buzzhome
26	com.campmobile.snow
27	jp.co.yahoo.android.yfiler
28	com.kouzoh.mercari
29	com.instagram.android
30	jp.co.yahoo.android.sports.npb.textlive
31	com.antivirus.boost.clean.defender
32	jp.co.yahoo.android.apps.map
33	tv.abema
34	jp.co.yahoo.android.weather.type1
35	com.peatix.android.Azuki

A.2 売上トップのアプリケーションにおける取得情報の分布 (21-35)

表 A·2　売上トップのアプリケーションにおける取得情報の分布 (21-35)

	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
インストール済みアプリ	o		o		o		o		o	o	o			o	
位置情報			o	o	o	o	o	o	o		o		o	o	o
IMSI 番号											o				o
シリアル番号		o	o			o			o		o				o
IMEI 番号					o	o			o		o			o	o
ボード (基盤) の名称 (SoC)		o	o	o		o	o			o		o		o	
ブートローダのバージョン番号		o													
ブランド名		o	o	o	o	o	o	o	o	o	o	o	o	o	o
ネイティブコードの命令セット		o	o	o		o	o	o	o	o	o	o	o	o	o
ネイティブコードの第 2 命令セット			o				o		o	o		o		o	
デバイス名	o	o	o	o	o	o	o	o	o	o		o	o	o	o
ハードウェア名			o						o						o
製造社名	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
システム時刻			o				o		o	o	o		o	o	
接続されている音声機器の情報															
メモリの容量		o	o		o	o	o		o	o	o	o	o	o	o
ヒープの最大サイズ		o	o		o	o	o	o	o	o		o	o	o	o
ビルド ID	o		o	o		o	o		o	o	o		o	o	o
機種名	o	o	o	o	o	o	o	o	o	o		o	o	o	o
製品名	o	o	o	o	o	o		o	o				o	o	o
ベースバンドバージョン															
電話番号						o					o				o
対応暗号スイート									o						o
インストール済みルート証明書			o				o			o			o		o
接続している Wi-Fi の SSID								o							o
Wi-Fi 上での IP アドレス	o							o							
検知している Wi-Fi スポット								o							o
登録済みのアクセスポイント															
SIM の国コード	o					o					o			o	
サービスプロバイダの名前			o			o								o	o
SIM のシリアル番号 (ICCID)															o
Bluetooth デバイスの名前															
ストレージ (/data) の容量	o	o	o		o	o	o	o	o	o	o		o	o	o
Web サービスのアカウント情報					o	o		o							o
アカウントのトークン取得								o							o
アカウントのパスワード取得								o							
WebView の UserAgent	o	o	o	o			o			o	o	o	o	o	
カメラの搭載台数	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
ディスプレイ名									o				o		
ディスプレイの ID	o	o		o	o						o		o		
画面解像度の高さ	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
ピクセル密度 (xdpi)	o							o	o			o			