Vol.2013-CSEC-62 No.62
Vol.2013-SPT-6 No.62
2013/7/19

アプリ/コンテンツ向けプライバシーポリシーの第三者検証フレームワーク

竹森敬祐[†1]　磯原隆将[†1]　川端秀明[†1]　窪田歩[†1]　高野智秋[†2]
可児潤也[†3]　西垣正勝[†3]
[†1] KDDI 研究所　[†2] KDDI　[†3] 静岡大学

情報収集モジュールなどを組み込んだスマホアプリからの勝手な情報送信が問題となる中、利用者に送信情報を説明するアプリ向けのプライバシーポリシー（以後、アプリプラポリ）の策定が求められている。我々は、情報送信を伴うアプリとアプリプラポリの実態調査を行い、63%のアプリが情報送信を行い、うち 9 割がアプリプラポリを持たないか、持っていたとしても送信情報を正しく記載していないことがわかった。

そこで本研究では、Market がアプリの第三者検証機関として審査役を担い、正確で解りやすいアプリプラポリを生成・提示することで、利用者判断を仰ぐフレームワークを提案する。特徴として、アプリ解析力のある技術検証機構を持つことで、誤った申告とアプリプラポリの生成を予防できる。ここで、アプリのダウンロードや利用実績に応じた報酬を支払うレベニューシェアを適用する。これにより、過剰な情報送信や目的が判然としないアプリは利用者から倦厭され、報酬が低下する経済論を働かせる。本手法をアプリ Market に実装・運用した結果、16%のアプリしか情報送信を行わないこと、アプリの趣旨に沿った必要最低限の情報送信に限られることを確認する。

Third party review framework for privacy policy of application/contents

Keisuke TAKEMORI[†1]　Takamasa ISOHARA[†1]　Hideaki KAWABATA[†1]
Ayumu KUBOTA[†1]　Tomoaki TAKANO[†2]
Junya KANI[†3]　Masakatsu NISHIGAKI[†3]
[†1]KDDI R&D Laboratories　[†2]KDDI　[†3]Shizuoka University

Applications in a smartphone include data collecting libraries and send user data without notifications. A privacy policy for the smartphone application, which explains “what data are sent,” “why the data are sent,” and “who uses the data,” is recommended to be written. In our investigation, 63% of applications send user data. However, about 90% of applications do not notify users of “what data are sent” or notify users incorrectly.

In this research, we propose the third party review framework for privacy policy of smartphone application to a market place. A market’s reviewer compares the application behavior with the declaration from application developer. The application privacy policy is generated by the market place and is presented to the user. The revenue share is rewarded to the application developer according to the activation records. As the suspicious data sending application is not welcomed by the users, the revenue share become decreasing. We apply the proposed scheme to the market place and investigate the application behavior. As a result, only 16% of applications send user data, which is only used for the application function.

1. はじめに

スマホアプリによる勝手な情報送信がプライバシーの観点から問題視される中で、2012 年 8 月に総務省から、利用者のプライバシー保護の目指すべき姿として、スマホ向けアプリの透明性の向上や、アプリ事業者／Market 運営者の果すべき役割などを記載した、「スマートフォン プライバシー イニシアティブ（以後、SPI）」がリリースされた[1]。特に、送信される情報・その目的・送信先などに関して、解りやすく説明するアプリのプライバシーポリシーを策定し、利用者から承諾を得ることが推奨されている。また、2012 年 10 月には、モバイルコンテンツフォーラム（MCF）から、SPI を参考にしたアプリプラポリの執筆例が公開された[2]。EU では忘れられる権利[3]、米国では Do Not Track[4]が提唱され、ネット上でのプライバシー保護の取り組みと利用者関与の機会が推進されている。こうした流れを受け、日本国内の関係者が情報共有を図る連絡協議会も設けられた[5]。

我々は、アプリから実際に送信される情報の解析とアプリプラポリ中に送信される情報に関する記載の有無について、3 回／3 年間の調査を実施してきた。直近の調査では、63%のアプリが端末や SIM に付随する固定の ID（以後、グローバル ID）もしくはプライバシー情報を送信することが解り、うち 11%のアプリしかアプリプラポリで送信情報を正しく説明していないことが解った。送信される情報の多くは、アプリ本来の趣旨に沿わない、過剰な情報送信が目立ち、これらについてアプリプラポリに正しく記載されないことが原因である。また、SPI が推奨する 8 項目の記載状況や、他社が調査した結果と照合を行い、多くのアプリプラポリにおいて、SPI 8 項目を満たさないこと、用語や文章が曖昧で読み解き者によって判断がばらつく問題が明らかになった。そもそも、アプリプラポリではなく、個人情

ⓒ 2013 Information Processing Society of Japan

Vol.2013-CSEC-62 No.62
Vol.2013-SPT-6 No.62
2013/7/19

報保護法に基づく事業者としてのプラポリ（以後、事業者プラポリ）を流用しているものも多く、アプリから送信される情報を適切に説明できていない[6]。

本研究で解決すべき課題を纏めると、(i)第三者検証機関として、実際に送信される情報とアプリプラポリの整合性を確認すること、(ii)正確で解りやすいアプリプラポリを利用者に提示すること、(iii)アプリから必要最低限の情報送信に抑えることに取り組む。

本研究では、課題(i)から(iii)を解決するために、アプリ提供者となる Market 運営者が、アプリの第三者検証機関としてアプリの審査役を担い、適切なアプリプラポリを Market 側で生成し、利用者が送信される情報に納得した上で、アプリをダウンロードするフレームワークを提案する。具体的には、アプリ事業者がアプリを Market にアップロードする際に、アプリから送信される情報について申告し、申告内容とアプリの解析結果を突き合わせる。申告内容に矛盾が無ければ、用語と様式が定型化されたアプリプラポリが生成される。あくまで、アプリ事業者からの申告に基づき生成することで、内容はアプリ事業者の責任になっている。利用者は、スマホ画面 1 ページ程度に集約されたアプリプラポリを参考に、ダウンロードの判断を行う。Market 側は、アプリ事業者にアプリのダウンロードや利用実績に応じた報酬を支払う。アプリの趣旨に沿わない過剰な情報送信を行うものは、利用者に倦厭されダウンロード数が減ることになり、報酬額が減る。これにより、アプリの趣旨に沿った必要最低限の情報送信に抑え込むことができる。我々は本フレームワークをアプリ Market に実装・運用した。評価として、アプリから送信される利用者情報が 16%に抑えられていることを確認し、課題(i)と(ii)に取り組んだことで、課題(iii)をも解決できた実績を示す。

2. 実態調査

2.1 利用者情報

表 1 に、本研究で注目する利用者情報を纏めておく[1]。スマホ特有のグローバル ID とプライバシー情報であり、利用者に直接結び付かず、利用者側で取替えが可能な cookie やアプリ独自の ID を含めていない。

表 1　スマホにおける利用者情報

グローバル ID	International Mobile Equipment Identity (IMEI)、International Mobile Subscriber Identity (IMSI)、SIM serial number (ICCID)、OS 生成 ID、電話番号、MAC アドレス
プライバシー情報	メールアドレス、電話帳、位置、インストールアプリ名、アプリ実行ログ（含：実行アプリ名、通話履歴など）

2.2 3 回／3 年の実態調査

我々は、3 回／3 年に渡り、スマホ向け無料アプリから送信される利用者情報に関する実態調査を行ってきた。アプリは、日本のドメインから参照した際の人気順にダウンロードしている。結果を表 2 に示す。プラポリとの整合性に関する調査結果も示しているが、対象にしたプラポリとして、アプリプラポリと事業者プラポリの両者を読み解いた結果であることに注意されたい。図 1 に、プラポリ記載の正誤関係を示しておく。実際に送信された情報が全てプラポリ内に記載がある場合を「白」とし、一部でもプラポリに記載が足りない場合を「灰」、そもそもプラポリを持たない場合を「黒」としている。プラポリには、実際に送信されない情報を広く記載されていても良いとしている。

表 2　スマホアプリからの利用者情報の送信状況

	2011.8–2012.1 調査(400件)	2012.4–2012.5 調査(100件)	2013.2–2013.3 調査(100件)
情報収集ﾓｼﾞｭｰﾙを組み込んだｱﾌﾟﾘ	56.9%*1 (558件)	82% (82件)	63% (63件)
利用者情報を送信するｱﾌﾟﾘ	45.3%*2 (181件)	81% (81件)	63% (63件)
ﾌﾟﾗﾎﾟﾘに送信情報が正しく記載のｱﾌﾟﾘ(白)	17/181件=9% 17/400件=4%	2/81件=3% 2/100件=2%	7/63件=11% 7/100件=7%
ﾌﾟﾗﾎﾟﾘに送信情報が誤って記載のｱﾌﾟﾘ(灰)	7/181件=4% 7/400件=2%	13/81件=16% 13/100件=13%	29/63件=46% 29/100件=29%
ﾌﾟﾗﾎﾟﾘが無く利用者情報を送信するｱﾌﾟﾘ(黒)	157/181件=87% 157/400件=39%	66/81件=81% 66/100件=66%	27/63件=43% 27/100件=27%

*1 この調査のみ980件のｱﾌﾟﾘを対象としている。
*2 2011.8–2012.1の調査ではSSL通信で送信される利用者情報を対象外。

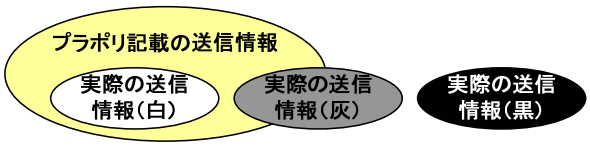


図 1　プラポリ記載内容の正誤関係

SPI は 2012 年 8 月に公開された。表 2 の 2011、2012、2013 年の 3 列は、それぞれ空白期、SPI 公開前、SPI 公開後の状態であることを勘案して参照すると解りやすい。

2012 年 4-5 月の情報収集モジュール[7]-[13]の組み込み率と利用者情報の送信率が 8 割を超えているのに対して、2013 年 2-3 月では、6 割程度になっており、SPI のリリースによって、素行が良く解らない外部の情報収集モジュールの組み込みや、不必要な利用者情報の収集を控えるアプリ事業者が現れてきたことが伺える。また、アプリもしくは事業者プラポリを持たずに勝手な情報送信をするアプリ(黒)が、87%→81%→43% へと減少している。送信情報が誤って記載されているものの、プラポリを通じて利用者に説明しようと努力が伺えるアプリ(灰)が、4%→16%→43% へと増加している。特に、SPI 公開前後で減少と増加の変化量が著しい。これより、SPI[1]や MCF ガイド[2]を参考にプラポリを書く流れが起きていることが伺える。

ⓒ 2013 Information Processing Society of Japan

ここで、正しく送信情報を記載できているアプリは、9%→3%→11%と、2013 年現在も 1 割程に留まっており、プラポリを正しく書けない現状がある。主な理由は、外部の情報収集モジュールを組み込むことに起因している。

2.3 2013 年 4-5 月(100 件)の詳解

プラポリとして、サービスを含めたアプリプラポリと、Web サイトを含めた事業者プラポリのいずれが、アプリの説明に適用されているかの調査を実施した。結果を表 3 に示す。

アプリプラポリを持つアプリは、利用者情報の送信の有無に関わらず 25%程であることが解る。また、事業者プラポリを代用したアプリが 30%程あることも解る。ちなみに、アプリプラポリ 16 件のうち、送信情報を正しく記載していたものは 5/16 件=31%であり、事業者プラポリ 20 件のうち、送信情報を正しく記載していたのは 2/20 件=10%であった。これより、事業者プラポリではアプリから送信される利用者情報を適切に説明しきれていないことが解る。また、たとえアプリプラポリを持っていたとしても、送信情報を正しく説明できているアプリが少ないこともわかる。

表 3 プラポリに関する詳解（2013 年 4-5 月）

	全ｱﾌﾟﾘ(100件)	利用者情報を送信するｱﾌﾟﾘ(63件)
アプリプラポリを持つアプリ	24/100件=24%	16/63件=25% (正確5/16件=31%)
事業者プラポリを持つアプリ	29/100件=29%	20/63件=32% (正確2/20件=10%)
プラポリを持たないアプリ	47/100件=47%	27/63件=43%

次に、表 3 に示したアプリプラポリ 24 件と事業者プラポリ 29 件の計 53 件について、SPI 8 項目の記載状況を表 4 に纏める。ここで我々は、プライバシー懸念の主要因である情報収集モジュールがアプリに組み込まれていることを利用者に明確に伝えるべきと考え、SPI ⑥の第三者提供と情報収集モジュールの記載の有無について分けて調査を進めた。

結果として、①のアプリ事業者に関する説明は、100%のプラポリに記載があった。しかし、⑥-2 の情報収集モジュールの有無については、23%のプラポリにしか記載がない。アプリに組み込まれた情報収集モジュールについて、アプリ事業者から利用者へ説明責任があるにも関わらず、その意識が薄い様子が伺える。これに起因して、②の送信情報に関する説明が 92%のプラポリに記載がるにも関わらず、前記の通り約 9 割のアプリが、送信情報についての記載漏れが生じている。

ちなみに、SPI 8 項目の全てを記載しているアプリは 4/100 件=4%あり、うち送信情報を正しく記載できていたものは 0/4 件=0%であった。形式論も必要であるが、そもそも送信情報を正しく説明するために、アプリの挙動を技術検証し、アプリプラポリの記載内容が正しいことを第三者が客観的に検証するスキームが望まれる。

表 4 SPI の 8 項目と 53 件のアプリへの記載状況

①	情報を取得するアプリ提供者等の氏名又は名称	53/53 件=100%
②	取得される情報の項目	49/53 件=92%
③	取得方法の記載の有無（自動送信、手入力、Web 側での閲覧履歴）	39/53 件=74%
④	利用目的の特定・明示	52/52 件=98%
⑤	通知・公表又は同意取得の方法、利用者関与の方法（送信の停止、情報削除）	32/53 件=60%
⑥	1)外部送信・第三者提供の有無 2)情報収集モジュールの有無	47/53 件=89% 12/53 件=23%
⑦	問い合わせ窓口の情報	36/53 件=68%
⑧	プライバシーポリシー変更の手続きの説明	32/53 件=60%

2.4 他社の調査結果との照合

ほぼ同じ時期に、日本総研(株)によって SPI 8 項目に注目した 40 件のプラポリの記載状況の確認が行われた。我々が対象にしていた 100 件のうち、33 件が同じアプリを調査していた。そこで、両社の結果を持ち寄り、SPI 8 項目への適合性について確認したところ、17/32 件＝52% のアプリのプラポリにおいて、いずれかの項目で読み解きの判断が分かれた。この様子を図 2 の左側（黄色）に示しておく。この原因は、プラポリの説明文や用語が曖昧なために、判断が分かれたのが主原因である。尚、図 2 の右側には、プラポリに記載のあった送信情報について、我々が列挙した状況を示しておく。この送信情報の記載内容と、アプリから実際に送信される情報を検証することが望まれる。

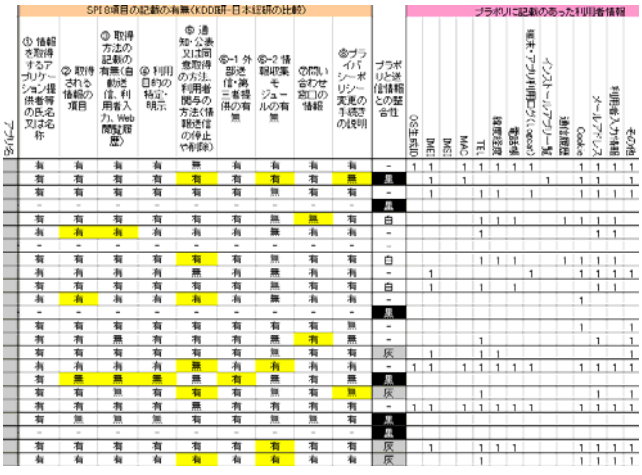


図 2 SPI の準拠性調査の様子と判断が分かれた状態
(黄色い箇所が判断の分かれた箇所)

2.5 情報収集モジュールから送信される利用者情報

図 3 に、2013 年 4-5 月調査の 100 件のアプリを 5 分間実行した際に、情報収集モジュールから送信された利用者情報の様子を示しておく。複数のグローバル ID を送信する情報収集モジュールも多い。中には、グローバル ID と位置情報を合わせて送信するものもあり、利用者の位置を活かした広告コンテンツの提供の様子が伺える。尚、Web 向け広告で利用されているような cookie を使った利用者追跡を行っているものは見当たらなかった。スマホアプリ向け情報収集モジュールで実現できる cookie 方式が 2012 年 12 月に提案されている中で[14]、広告のために忘れられる権利が侵されかねないグローバル ID を用いる理由は成り立たない。利用者のプライバシー保護の観点から、利用者に直接結びつかず、利用者によって消去や取替えが可能な cookie 方式の普及が望まれる。



図 3　情報収集モジュールから送信された利用者情報

2.6 情報収集モジュールが扱う情報に関する説明

情報収集モジュールが扱う情報についてアプリ事業者への説明の事例を 2 つ紹介する。

【良い事例】

アプリの利用統計を調査するモジュールとして Flurry がある[7]。我々が調べた Android アプリ向け Flurry Agent は、Android ID と位置情報を送信する機能を持っていた。Flurry Agent をアプリに組み込むまでの設定に関する説明として、アプリの Manifest ファイルに、以下のパーミッションを書くよう述べられている。

<Required Permission>

android.permission.INTERNET

<Optional Permission>

android.permission.ACCESS_COARSE_LOCATION or
android.permission.ACCESS_FINE_LOCATION

また、Flurry Agent に位置情報を取得させたい場合には、

FlurryAgent.setReportLocation(false/true)

の API を true に設定して利用するよう説明がある。さらに、事業者のホームページ（HP）にアプリプラポリが掲載されており、Android ID と位置情報を利用する旨が記されている。アプリ事業者が本モジュールから送信される利用者情報を把握することは可能であり、透明性が確保された情報収集モジュールと言える。

【悪い事例】

我々の動的解析で、Android ID、IMEI、IMSI を送信することを確認したある広告モジュールについて、アプリへ組み込むまでの設定・解説書の状況を紹介する。まず、アプリのマニフェストファイルに、以下のパーミッションを書くよう述べられている。

android.permission.INTERNET
android.permission.READ_PHONE_STATE

しかし、本広告モジュールから送信される利用者情報を設定する機能は提供されておらず、デフォルトで Android ID、IMEI、IMSI のグローバル ID を多重送信するようになっている。また、本事業者の HP を確認したところ、広告モジュールに関するアプリプラポリは見当たらなかった。この広告モジュールをアプリ事業者が組み込む場合、正しくアプリポリシーを書くことは難しい状況にある。

3. アプリ Market が担う第三者検証フレームワークの提案

利用者がアプリプラポリを参照・承諾する主なタイミングは、Market からアプリをダウンロードする前とアプリの利用時である。我々は、アプリのセキュリティ品質に一定の役割が期待される Market に注目し、アプリを利用者に届ける Market 運営者が第三者検証役を担うプライバシー審査のフレームワークを提案する。

3.1 課題の整理

2 章の議論から本研究で解決すべき課題を以下に纏める。

(i) 第三者検証機関として、実際に送信される情報とアプリプラポリの整合性を確認すること

(ii) 正確で解りやすいアプリプラポリを利用者に提示すること

(iii) アプリから必要最低限の情報送信に抑えること

3.2 第三者検証フレームワーク

図 4 に、アプリ Market が主体となって課題(i)から(iii)を解決する第三者検証フレームワークを提案する。

ⓒ 2013 Information Processing Society of Japan

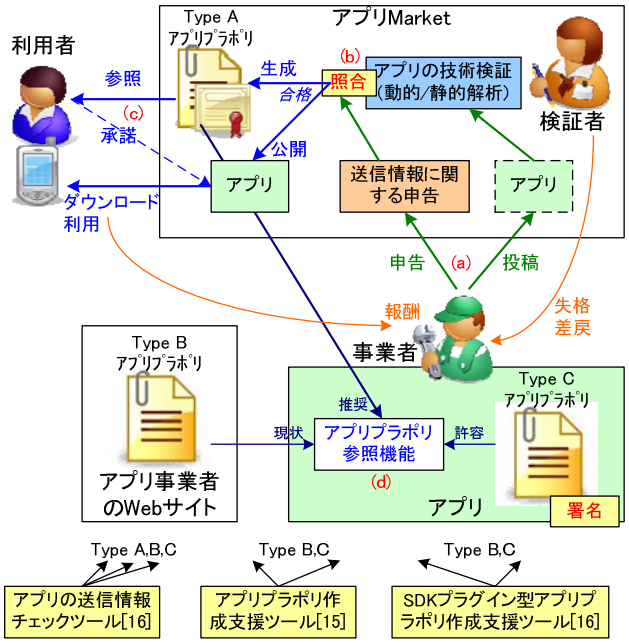


図 4　アプリ Market が担う第三者検証フレームワーク

(a)　アプリ事業者は、Market にアプリを投稿する際に、送信情報、目的、送信先などについて申告する。

(b)　Market 運営者は、アプリについて静的/動的解析を行い、実際の送信情報と申告内容の整合性を確認する。

(c)　Market 側で、申告内容に基づいてアプリプラポリを生成し、アプリのダウンロード前に利用者へ提示する。利用者が承諾してダウンロードした数や利用実績に応じて、Market 運営者はアプリ事業者に報酬を支払う。

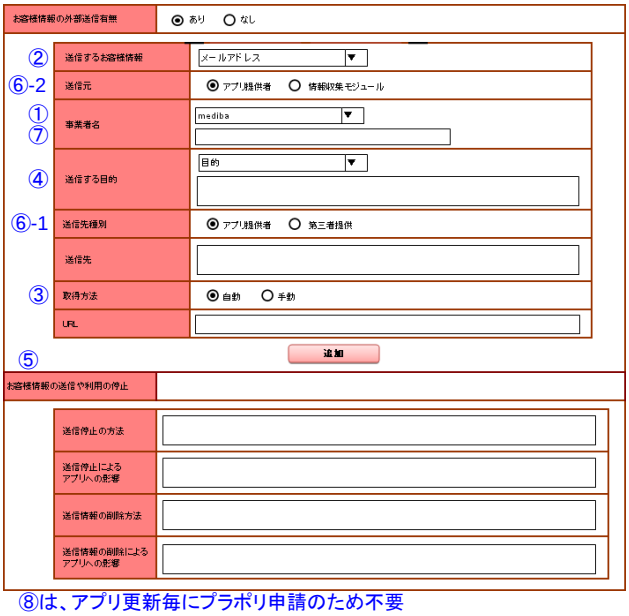
(d)　アプリ側にも、アプリの利用時にアプリプラポリを参照する機能を持たせる。

3.3　(a)アプリ申告

アプリ事業者が Market にアプリを投稿する際に、送信情報に関して申告するための画面を図 5 に示す。表 4 で示した SPI の 8 項目に準拠した設計になっている。ポイントは、②送信情報をキーに、①・⑥・⑦誰（アプリ事業者、情報収集モジュール、その他の第三者）が、④なぜ、③どのように送信するのかを説明する。これを、②送信される利用者情報の数だけ申告する。

ここで、重要事項の一つである「⑤通知・公表又は同意取得の方法、利用者関与の方法（送信の停止、情報削除）」については、これを実現できているアプリや情報収集モジュールが少ない実態がある（参考：表 4）。よって、現時点ではこの記載についてはオプション扱いとして分けている。

尚、「⑧プライバシーポリシー変更の手続きの説明」については、アプリがバージョンアップ・投稿される度に、送信情報を申告し、新アプリプラポリが新アプリとセットで公開されるため、既に⑧を満たしており、記載はない。そもそも、個人情報保護法に基づく事業者プラポリについては、様々な事業を手がける事業者の実態に合わせて柔軟な変更と利用者への通知が必要である。しかし、アプリプラポリは、あるバージョンのアプリ・サービスに特化したもので変更が必要になるケースは少ない。そもそも、送信される利用者情報を規定するアプリの保証書の役割を果すことから、勝手な変更があってはならない。アプリ・バージョンとアプリプラポリが 1 対 1 に結び付くべきであり、アプリがバージョンアップされる度に、アプリの投稿と送信情報の申告を毎回行うモデルでは⑧は不要である。



⑧は、アプリ更新毎にプラポリ申請のため不要

図 5　送信情報に関する申告画面

3.4　(b)アプリの技術検証

アプリから送信される利用者情報を技術的に解析し、申告内容が正しいことを検査する。解析には、アプリパッケージに対する静的解析や、実行させたときの挙動に注目する動的解析などを適用する。これにより、アプリから送信される情報、送信先、送信元プロセス（アプリ本体、情報収集モジュール）などの証拠を取る。また、アプリの趣旨や、機能を把握することで、情報利用の目的や送信手段を推定する。尚、アプリプラポリを参照する機能の有無についても検証する。これらの証拠を積み上げた上で、申告内容との整合性を確認する。

もし申告内容に不備があれば、アプリを不合格として、アプリ事業者に再申告を促す。ここでのポイントとして、アプリプラポリの様式／枠を Market 運営者が用意したとしても、申告やその修正を全てアプリ事業者が主体となって行うことで、内容の責任元がアプリ事業者になっていることである。

3.5　(c)Market で生成されるアプリプラポリ

技術検証で合格した場合は、アプリプラポリの概要版（図 6）と詳細版（図 7）が生成され、アプリが公開される。利用者がアプリをダウンロードする前に、送信される利用

ⓒ 2013 Information Processing Society of Japan

者情報を確認できるようになっている。

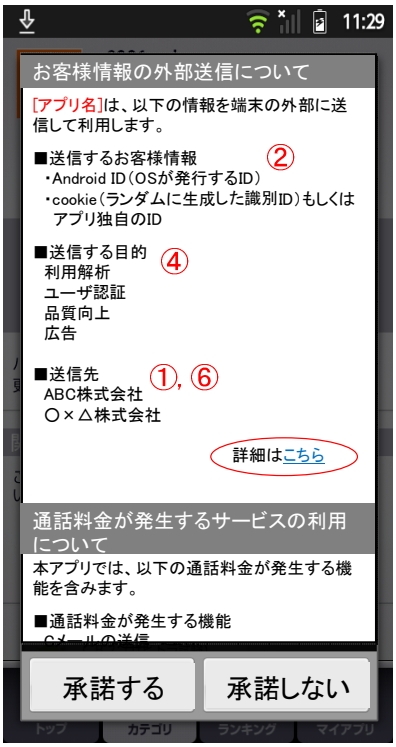


図 6　概要版アプリプラポリ

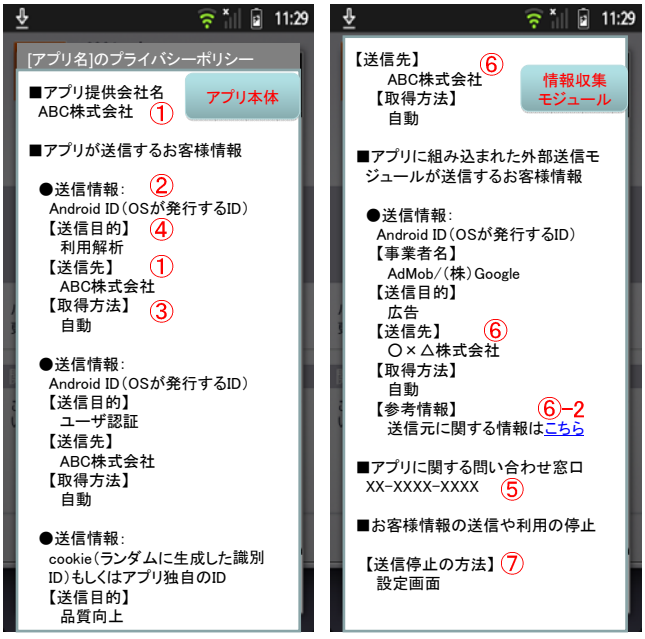


図 7　詳細版アプリプラポリ

図 6 の概要版アプリプラポリでは、SPI 8 項目のうち、②送信される情報、④目的、①,⑥送信先を、箇条書することで、判断に欠かせない重要事項をスマホ画面の 1 ページ程度で参照できるようになっている。

図 7 の詳細版アプリプラポリでは、①アプリ本体に関する説明部と、⑥第三者提供（含：情報収集モジュール）の説明部に分けた構成になっている。両者とも、②送信される情報ごとに、④目的・①,⑥送信先、③自動/手動を結び付けて説明する。ここで、④目的や①,⑥送信先が複数に分かれる場合には、全ての組み合わせを②送信される情報を主語にして列挙する。尚、⑥-2 情報収集モジュールに関してアプリプラポリがある場合には、その URL を記載する欄を設けている。

ここでのポイントとして、情報送信を行うアプリに限って、図 6, 7 の承諾画面がポップアップ形式で利用者に通知されるようにすることである。この理由として、

- 情報送信を伴わないアプリについても承諾画面が表示されると、利用者に慣れが生じてしまい、内容の確認が疎かになることを防ぐためである。狼少年化を避け、情報送信をともなうアプリに絞って、正しく読みやすいアプリプラポリを提示し、利用者の判断を仰ぐことが重要である。
- Market 側の技術検証者は、②送信される情報、④目的、①,⑥送信先について、記載の有無や整合性は確認できるが、その妥当性については判断が難しい。そこに、利用者側の判断が入るよう、概要版プラポリで端的に解りやすく、詳細版プラポリで正確に伝える。不安や不信を感じるアプリはダウンロード数が低下し、Market 運営者からアプリ事業者へ支払われる報酬額が減少する。これにより、もしアプリ本来の機能に利用者情報が不要な場合には、ポップアップの承諾画面が表示されないよう、情報送信を取りやめる判断に至る。必要最低限の情報送信に抑える経済論を働かせるモデルである。

3.6 (d)アプリプラポリ参照機能

SPI では、アプリから任意のタイミングでアプリプラポリを参照できることが推奨されている。そこで、情報送信をともなうアプリについては、アプリ内にアプリプラポリを参照できる機能を持つことを必須化する。

参照先として、Market が生成したアプリプラポリへのリンク、アプリ内に組み込まれたアプリプラポリのファイル、アプリ事業者 HP にあるアプリプラポリへのリンクがある。ポイントとして、第三者検証機関である Market で生成されたアプリプラポリへのリンクを推奨することである。この理由として、

- 整合性が検証されたアプリプラポリであり、一定の正確性が期待できるためである。
- アプリプラポリは、アプリの保証書の役割を果すものであり、アプリ事業者が任意のタイミングで書き換えられる状況は好ましくない。Market 生成のアプリプラポリは勝手な書き換えはできない。アプリ内にファイル形式で持つ場合も、署名によって担保される。
- 正確性が期待される Market 生成のアプリプラポリと、アプリ内ファイルやアプリ事業者 HP のアプリプラポ

ⓒ 2013 Information Processing Society of Japan

リの記載に食い違いがでることで、矛盾を生じる。

- アプリプラポリは、アプリ事業者の法的保護の役割を果す側面を持ち、Market 運営者は、アプリ事業者が自ら作成したアプリプラポリの矛盾や不備に対してコメントし難い。Market 運営者が申告内容に沿って生成したものであれば、Market への投稿ルールとして、コメントバック可能である。

追記として、本 Market で生成されるアプリプラポリは、グローバルに公開されるものである。よって、本 Market から配布されるアプリの参照先として利用できるだけでなく、他の Market に投稿された同じコード・動作のアプリであれば参照先として利用しても良い。

4. 評価

我々は、3 章の提案手法を実際のアプリ配信 Market に適用し、運営してみた。ここで、図 5 の申告内容は、図 6 の概要版アプリプラポリに沿った簡略化されたものを利用し、図 7 の詳細版アプリプラポリは未適用である。この運営で得られた結果を本論文の評価として、以下に述べる。

4.1 利用者情報を送信するアプリ

2013 年 5 月 1 日からさかのぼって投稿された直近 100 件のアプリに注目し、表 1 に示す利用者情報の送信アプリ数を調査した。

結果、16/100 件=16% のアプリが利用者情報を送信していた。表 2 より、2013 年 2-3 月の一般の Market では 63% のアプリが情報送信を行うのに対して、1/4 程度に抑えられていることがわかる。適用された Market には、

a) Market から利用実績に応じて報酬を支払うコース
　→ 利用者情報を送信する広告モジュールを禁止
b) Market からの支払の無いコース
　→ 情報収集モジュールに関する禁止事項なし

が設けられている。多くのアプリが a)に登録されており、広告モジュールによる情報送信が b)に限られることが主因である。但し、b)コースのアプリについても、広告モジュールを組み込まず、ポップアップ・承諾画面がでないものもある。次に、利用統計を把握するモジュールは、a), b)ともに適用できるが、情報送信を伴うアプリは、ポップアップ・承諾画面が入るため、アプリ本体が情報送信をともなわない場合には、極力ポップアップを避けたい傾向があるようである。的確に送信情報を検知する技術検証フェーズを持つ Market においては、アプリプラポリとの整合性を確認し、申告ミスの指摘や利用者承諾を設けることで、アプリ本来の機能に必要な利用者情報の送信に抑制される様子が伺える。

4.2 検証で失格したアプリのその後

2013 年 5 月 1 日からさかのぼって、一旦は申告ミスを指摘され不合格になった後に、合格となって公開されたアプリ 10 件について追跡した。

- 6/10 件が、②送信される情報, ①,⑥-2 送信先のいずれかの申告ミスが修正された。
- 4/10 件が、情報収集モジュールを停止/削除するというアプリ仕様が修正された。

10 件中 5 件は、アプリの利用統計を収集するモジュールを組み込んだものであり、1 件が前者の申告ミスの修正で、4 件が停止/削除のアプリ仕様の修正の対応であった。このことからも、アプリプラポリの申告ミスの主因は、外部の情報収集モジュールを組み込むことで生じていることがわかる。また、アプリ本来の機能に必要な情報のみ送信されるよう促されている様子がわかる。

5. まとめと期待

スマホアプリからの勝手な利用者情報の送信が問題になる中、アプリ Market が主体となって、正確で解りやすいアプリプラポリを生成・提示し、利用者判断を仰ぐ第三者検証フレームワークを提案した。ここに至るまでに、自らプラポリの実態調査を行い、多大な工数を要する割には的確に読み解けない状況を認識し、現時点でアプリ事業者が書いたアプリプラポリに基づく第三者検証を妥当なコストで運用することは不可能であると結論付けた。そこで、アプリ事業者に SPI 8 項目を申告して貰い、これと実際の送信情報との整合性を確認する検証モデルを考案した。申告に基づき、概要版と詳細版のアプリプラポリを生成し、利用者に内容の妥当性の判断を仰ぐ。ここに、アプリのダウンロードや利用実績に応じて報酬を支払うレベニューシェアを適用する。過剰な情報送信や目的が判然としないアプリについては、利用者から倦厭されるため、必要最低限の情報送信になるような経済論を働かせている。本スキームをアプリ Market に実装・運用した結果、16%のアプリしか情報送信を行わず、送信される情報もアプリの趣旨に沿ったものに限られることがわかった。追記として、今回の Market へ投稿されたプラバシー対策済みのアプリが、世界的なアプリ Market にそのまま投稿されているケースを確認している。本 Market 検証が、グローバル Market 上のアプリにも良い影響を与え始めている現われである。また我々は、情報送信をともなうアプリについては、アプリ内にアプリプラポリを参照する機能を持つことを必須化する。その参照先として一定の正確性が期待される Market 側で生成されるアプリプラポリを推奨している。

経済論を働かせることができる Market に第三者検証機関を担わせる効果は高く、本手法を業界のデファクトへと導くことで、スマホアプリ市場全体の信頼向上が期待される。我々はその期待に応えたいと思う。

謝辞

本研究の 2 章の実態調査を纏めるにあたり、読み解き結

ⓒ 2013 Information Processing Society of Japan

果を共有頂けた日本総研(株) 東氏、前田氏に深謝する。また、アプリプラポリと事業者プラポリの区分をアドバイス頂けた産業総合研究所 高木氏、渡辺氏に深謝する。

参考文献

1) 総務省,“スマートフォン プライバシー イニシアティブ”, http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html http://www.soumu.go.jp/main_content/000171224.pdf
2) MCF,“スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン”, http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf
3) European Commission, April 2010, “A comprehensive approach on personal data protection in the European Union: Right to be Forgotten,” COM(2010) 609 final, Brussels. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
4) Federal Trade Commission (FTC), 2010, “Endorses ‘Do Not Track’ to facilitate consumer choice about online tracking,” http://www.ftc.gov/opa/2010/12/privacyreport.shtm.
5) スマートフォンの利用者情報等に関する連絡協議会(SPSC), http://www.mcf.to/press_comment/pdf/spsc_press_20121004.pdf
6) 一瀬，高木，山口，渡辺，“スマホアプリにおけるアプリケーション・プライバシーポリシー掲載の現状調査”, 情処, CSEC62-61, 2013 年 7 月.
7) FLURRY, http://www.flurry.com/, http://www.flurry.com/privacy-policy.html, http://support.flurry.com/index.php?title=Analytics/GettingStarted/TechnicalQuickStart/Android, http://support.flurry.com/index.php?title=Analytics/Code/Doc/Android.
8) Google Analytics, http://www.google.com/analytics/.
9) AdLantis, http://sp.www.adlantis.jp/.
10) i-mobile, http://i-mobile.co.jp/en/index.aspx.
11) nend, http://nend.net/.
12) Admob by Google, http://www.google.com/ads/admob/.
13) AMoAd, http://www.amoad.com/.
14) 竹森敬祐，他 5 名、“スマートフォンアプリ向け独自 ID の生成・管理”，情処，CSEC59-8，2012 年 12 月.
15) 磯原，川端，竹森，窪田，“XML を用いたモバイルアプリのプライバシーポリシーの運用”，信学，SCIS シンポジウム，2013 年 1 月.
16) 磯原，川端，竹森，窪田，“Android アプリの静的解析を用いた利用 API と外部モジュール検知によるプライバ シーポリシー作成支援機構”，情処，CSEC62-63，2013 年 7 月.

ⓒ 2013 Information Processing Society of Japan