Vol.2013-CSEC-62 No.61
Vol.2013-SPT-6 No.61
2013/7/19

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

一瀬小夜[†1]　高木浩光[†1]　山口利恵[†2]　渡辺創[†1]

スマートフォン用アプリケーション・プログラム（アプリ）では、どのような情報が自動的に取得・送信されるのかが明らかでないため、アプリケーション・プライバシーポリシーとしてこれら情報を明確にユーザへ提示することが重要である。本稿では、Google Play の無料アプリトップ 500 中 100 アプリ、有料アプリ中 50 アプリ、無作為に抽出した 50 アプリの計 200 アプリについて、そのアプリケーション・プライバシーポリシーの記述状況を調査した。その結果、現状の達成度が 2 割程度であることがわかった。

A Survey of Application Privacy Policies in Mobile Applications

SAYO ICHINOSE[†1]　HIROMITSU TAKAGI[†1]
RIE SHIGETOMI YAMAGUCHI[†2]　HAJIME WATANABE[†1]

Since it is not clear which personal/non-personal data are automatically collected and sent to servers by mobile applications, it is very important to show those information in their application privacy policies to consumers. In this paper, we summarize the current situation of application privacy policies by investigating 200 policies where 100 are from Top Free 500, 50 are from Top Paid 500, and 50 are from a randomly chosen list in Google Play site. Accordingly, those information are clearly written only in about 20% policies.

1. はじめに

近年のスマートフォン（スマホ）の急速な普及により、スマホ用のアプリケーション・プログラム（アプリ）が、利用者のプライバシーに関わる新たな問題を引き起こしている。例えば、2012 年 2 月には、米国企業が運営するソーシャル・ネットワーキング・サービス（SNS）用のアプリが、利用者に無断でスマホ内の電話帳データをアップロードしている事実が発覚して非難の声が上がり、経営者が謝罪してアプリを修正するという事態があった [1)]。また、悪意あるアプリによる被害も報告されるようになり、日本においても、「電池が長持ちする」などと機能を偽って、密かに利用者の電話帳データを盗むアプリが出回り、アプリの配布者が検挙され、地裁で有罪判決[i]を受けるという事件があった。

悪意ある者が利用者を騙してアプリを実行させる行為は犯罪[ii]として摘発していくほかないであろうが、前記の SNS 用のアプリの事例のように、正当な事業者がサービス実現のために善かれと利用者から情報を取得した場合については、利用者に断りなく取得したことが非難の対象となることはあるにせよ、そうしたケースに対してまで直接に刑事罰をもって対処するのが適切とは言えないであろう。

アプリによるスマホからの情報取得が、利用者にとって許容できるものであるか否かは、各々利用者の価値観によって異なるものであり、例えば、GPS による位置情報を使うアプリで、位置情報を無断で収集されることが平気な利用者もいれば許せない利用者もいるであろう。したがって、どのような情報取得が許されるのかを一律に定めることはできず、利用者各自の判断に委ねるほかない。そうした利用者の判断を可能にするには、まず、各アプリがどのような情報を送信するものであるかを、利用者に対して説明することが不可欠である。

このような状況の中、米国では、2012 年 2 月、カリフォルニア州の司法長官が、Google や Apple などアプリ配布を事業とする主要 6 社と、プライバシー保護策の改善で合意したと発表した [2)]。これは、カリフォルニア州法「Online Privacy Protection Act」に基づき、アプリ配布サイトの分かりやすい場所にプライバシーポリシーを表示することなどを求めたものである。この合意により、Google や Apple のアプリ配布サイトには、各アプリの説明ページ内に、「プライバシーポリシー」との見出しのリンクを掲載する専用の場所が設置されることとなった。

時を同じくして、日本でも、同様の問題意識に基づき、総務省が、「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」の下に、「スマートフォンを経由した利用者情報の取扱いに関する WG」を組織し、2012 年 8 月に、「スマートフォン プライバシー イニシアティブ」という報告書 [3)]（以下、総務省報告書）を発表した。総務省報告書は、「関係事業者等や業界団体のイニシアティブによる

†1 独立行政法人産業技術総合研究所
†2 東京大学ソーシャル ICT 研究センター

[i] 京都地裁平成 25 年 5 月 24 日判決

[ii] 刑法第 168 条の 2 及び第 168 条の 3 の不正指令電磁的記録に関する罪に当たる場合がある。

Vol.2013-CSEC-62 No.61
Vol.2013-SPT-6 No.61
2013/7/19

自主的な取組の推進が期待されるもの」として、「スマートフォン利用者情報取扱指針」（以下、総務省指針と言う。）を示している。

総務省指針がアプリ提供者に対して推奨しているのは、アプリケーションごとにプライバシーポリシーを策定して表示することと、一部の情報については取得に際して個別の情報の取得について利用者の同意を求めるものとすることの 2 点[iii]である。

我々は、このような指針が提案されている日本において、アプリ提供者らが実際にどれほどそれを達成しているのかの現状を調査する必要性があると考えた。特に、前者の達成状況については、前記カリフォルニア州司法長官の発表文の参考資料にも調査結果が紹介されており、2011 年 2 月の時点で、米国で配布されていた無料トップ 340 のアプリのうち 19%にしかプライバシーポリシーへのリンクが示されていなかったという調査結果 [4]がある。こうした調査は継続して行うことで改善の状況を評価することができるため、調査の手段と評価の基準を明確にして、誰でも追調査できるようにしておくことが有用である。

本稿は、このような問題意識の下、総務省指針が求める 2 点のうち、前者の「アプリケーションごとにプライバシーポリシーを策定して表示すること」の達成度について、Android 用アプリの配布サイトである「Google Play」を対象として、調査方法と評価基準を明確にするとともに、2013 年 4 月の時点で配布されていたアプリを対象に調査を行った結果を示すものである。

2. 調査方針

総務省指針を受けて、2012 年 11 月、携帯電話向けサービスの業界団体である一般社団法人モバイル・コンテンツ・フォーラムが、「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」[5]を発表した。そこでは、「アプリケーション・プライバシーポリシー」という用語が用いられており、この語を用いることについて次のように説明されている。

> 本ガイドラインでは、アプリケーションごとに利用者情報の取扱い方針を記載したものを「アプリケーション・プライバシーポリシー」と表記しています。
>
> 個人情報保護マネジメントシステム規格である日本工業規格の JIS Q 15001:2006 における「個人情報保護方針」は、事業者の代表者が個人情報の収集、利用、提供等に関する保護方針としてさだめるものであり、原則として 1 社に一つ作成されていることが一般的ですが、名称としてプライバシーポリシーという文言が用いられ、広く普及しています。
>
> 既に作成されている個人情報保護方針と本ガイドラインにおけるアプリケーションごとのプライバシーポリシーは記載内容や位置づけが異なるため、実装にあたっては「個人情報保護方針」と混同されないように、「アプリケーション・プライバシーポリシー」という表記を採用する事を推奨します。【文献 5）より引用】

本稿の調査でも、この考え方に倣い、JIS Q 15001:2006 の「個人情報保護方針」に類するポリシーは、適切なアプリケーション・プライバシーポリシーに当たらないものとして集計することにする。

適切なアプリケーション・プライバシーポリシーと呼ぶに相応しいのは、ポリシーを掲示すべきとされるその趣旨に照らせば、そのアプリがどのような挙動をするものであるか、特に、どのような利用者情報を外部に送信するものであるかを記述したものと言える。調査の集計にあたっては、そのような形態での記述をしているものを、適切なアプリケーション・プライバシーポリシーとみなすことにする。

また、アプリケーション・プライバシーポリシーの掲載場所について、前記のカリフォルニア州と主要 6 社との合意に基づいて設置された、アプリ配布ページ上の専用のリンク場所に掲示するのが望ましい形であるとして、集計することにする。

3. 調査方法

調査対象アプリとして、Google Play で公開されている Android 向けアプリから、以下の方法により、合計 200 個を抽出した。

① 2013 年 4 月 4 日時点の無料アプリトップ 500[iv]から、5 番飛びに 100 個
② 2013 年 4 月 10 日時点の有料アプリトップ 500[v]から、10 番飛びに 50 個
③ 人気順ではなく無作為抽出したアプリも調査するために、2013 年 4 月 9 日時点でキーワード「あ」でアプリを検索した結果の上から 50 個

これらのアプリについて、プライバシーポリシーを探す方法を以下の手順とした。

Google Play の各アプリのページに用意されている「デベロッパー」との見出しのある部分（図 1）からリンクされているものを対象とする。

[iii] 総務省報告書 p.54 より。

[iv] Google Play 上で「人気（無料）」との見出しで上位 500 個までのアプリが一覧表示される場所。

[v] Google Play 上で「人気（有料）」との見出しで上位 500 個までのアプリが一覧表示される場所。

Vol.2013-CSEC-62 No.61
Vol.2013-SPT-6 No.61
2013/7/19

図 1 プライバシーポリシーの掲載場所

まず、「プライバシーポリシー」の見出しで示されるリンクの有無を確認する。リンクが存在する場合には、リンク先のページのスクリーンショットを撮って記録する。(この場合を以下、掲載場所は「X」であると言う。)

このリンクが存在しない場合には、「ウェブページにアクセス」の見出しで示されるリンクの有無を確認し、リンクが存在する場合は、リンク先に示された開発者の Web サイトを訪れ、訪れた先のサイトで、ページのフッタ部分のリンク先を含めて辿って、プライバシーポリシーらしきものを探す。それが見つかった場合には、該当ページのスクリーンショットを撮って記録する。(この場合を以下、掲載場所は「Y」であると言う。)

以上の 2 つの方法で見つからない場合には、プライバシーポリシーの掲載はないとして扱う。

実際には、プライバシーポリシーが、アプリの内容を説明する自由記述欄に記載されている場合や、アプリを実行したときにアプリ上で表示される場合もあると考えられるが、本調査ではそれらを対象にしていない。その理由は、前記調査方針の通り、アプリケーション・プライバシーポリシーはこの所定の場所「X」に記載されることが期待されているものであること、また、アプリ上でポリシーを表示する仕組みができているのであれば、同時に同じものをここに掲載することは容易であるはずであるから、アプリ上に表示するがここに記載のないアプリは少数と予想できる[vi]からである。

今回の調査では、掲載場所が「X」であったアプリは 44 個、「Y」は 58 個、掲載のないアプリが 98 個であった。

プライバシーポリシーの掲載がないものが半数近くに及ぶが、その原因として、アプリが利用者情報を送信しないものであり、プライバシーポリシーを掲載する必要がないためである可能性もある。そのようなアプリをできるだけ除外して集計することにした。

アプリが利用者情報を送信するものであるか否かを判別することはそもそも容易でないが、Android では、利用者情報を参照するアプリは、Permission 機構によってダウンロード時に利用者に警告が表示される仕組みになっているので、これを利用することにし、不完全な方法ではあるが、各アプリが利用者情報に係る Permission を要求しているかを調べ、これを元に、プライバシーポリシーを掲載する必要のないアプリを集計から排除することにした。

利用者情報に係る Permission の一覧を表 1 に示す[vii]。アプリがこれらの Permission を要求する場合、アプリが利用者情報を送信している可能性があるものとする。調査では、Google Play でアプリをインストールしようとした際に表示される Permission の一覧のスクリーンショットを撮り、表 1 の Permission を要求しているかを記録した。

表 1 利用者情報に係る Permission 一覧

Permission	概要
READ_PROFILE	プロフィール情報の読み取り
GET_ACCOUNTS	端末内のアカウントの検索
USER_CREDENTIALS	アカウントの認証情報を使用
READ_PHONE_STATES	端末 ID の読み取り
READ_SMS	SMS の読み取り
READ_CONTACTS	連絡先の読み取り
READ_HISTORY_BOOKMARKS	ブラウザの履歴とブックマークの読み取り
GET_TASKS	実行中のアプリケーションの取得
READ_LOGS	機密ログデータの読み取り
ACCESS_FINE_LOCATION	精細な位置情報
ACCESS_COARSE_LOCATION	おおよその位置情報

また、Android には、表 1 の Permission を要求しなくても取得可能な「Android_ID」と呼ばれる Android OS が生成する端末固有の ID が存在する。この調査では、Android_ID も利用者情報として取り扱うことにし、各アプリが Android_ID を使用するコードを含むか否か、「secroid」[8]の情報を参照して確認した。

[vi] 実際、文献 6)にアプリケーション・プライバシーポリシーの掲載状況の調査結果が掲載されている（p.16）が、その中で、ポリシーがアプリ内に掲載されているのに、「Google Play 紹介ページ」及び「開発者ホームページ」には記載がないというケースは、40 個中 1 個のアプリのみ（同文献図表 1-2-1 より）と、例外的であったことが報告されている。

[vii] 文献 7)の表 1 を参考に作成した。

No.	順位	名称	開発会社	更新日	ポリシーの場所	ポリシーランク	プロフィール情報の読み取り	この端末上でのアカウントの検索	この端末上のアカウントの使用	携帯のステータスとIDの読み取り	連絡先の読み取り	SMSの読み取り	ブラウザの履歴とブックマークを読み取る	実行中のアプリケーションの取得	機密ログデータの読み取り	緯細な位置情報（GPS）	おおよその位置情報（ネットワーク基地局）	Android_ID	日・日英・英
57	281			2013/4/5	Y	A有+				無							有	×	英
58	286			2013/4/3	Y	C有0							有			有	有	×	日
59	291			2013/1/31	Y													×	
60	296			2013/3/4	Y	E		○		○						○		×	日
61	301			2013/3/30														×	
62	306			2013/3/31														×	
63	311			2013/4/4	X	A有0		無										有	日英
64	316			2013/3/28	X	B有-				有								有	英
65	321			2012/6/23		F												○	日
66	326			2013/4/1	X													×	

図 2　調査結果の集計表（一部抜粋）

調査の過程で作成した集計表の一部を図 2 に示す。各行が一つ一つのアプリであり、「名称」と「開発会社」はここでは伏せて表示した。各列には、プライバシーポリシーの掲載場所、表 1 の各 Permission 要求の有無、Android_ID 利用コードの有無のほか、「A」～「F」、「有」「無」、「＋」「0」「－」といったプライバシーポリシーのランク評価の結果、プライバシーポリシーの言語（「日」「日英」「英」）について記載している。

背景が灰色の行は、表 1 の Permission の要求と Android_ID 利用コードのいずれもない場合であり、アプリケーション・プライバシーポリシーを記述する必要がない場合と判断したものであり、評価から除外したアプリである。

今回の調査では、除外したアプリは 52 個であった。残りの 148 個のアプリ（内訳：無料アプリ 85 個、有料アプリ 28 個、「あ」検索結果 34 個）について、次節に示す基準でランク評価を行った。

4. 評価基準

評価は、スクリーンショットを撮って記録した各アプリのプライバシーポリシーを読んで行った。

全体を通して読むと、アプリが送信する情報が何かを記述している「アプリケーション・プライバシーポリシー」と呼ぶに相応しいものがある他に、開発会社が提供しているサービス全体について書かれたものや、利用者が Web サイトで自ら入力する情報（ユーザ登録、アンケートなど）について書かれたものなど、いくつかの様式が混在していることが分かった。

そこで、まず、各アプリのプライバシーポリシーの様式について、表 2 の基準でランク付けすることにした。以下、このランクを「様式ランク」と呼ぶ。

ランク「E」は、前記調査方針で示した、JIS Q 15001:2006 の「個人情報保護方針」に類するものが該当する。前記調査方針で適切なアプリケーション・プライバシーポリシーと呼ぶに相応しいものは、ランク「A」「B」が該当する。

ランク「C」は、利用者情報の取得に関する記述があっても、各アプリによる送信で取得するものなのかが書かれていない場合が該当し、例えば、「端末 ID を取得する場合がある」と書かれていても、何によって送信されるのか明らかにされていない場合は、ランク「C」と判定する。

なお、アプリの機能や開発会社が提供しているサービスの内容から、ポリシーの内容がアプリについて書かれた記述であることを推察できる場合もあるが、あくまでポリシーの記述の様式でランク評価をすることにし、アプリの機能や開発会社の事情については考慮しないことにした。

表 2　プライバシーポリシーの様式によるランク

ランク	判断基準
A	個々のスマホアプリ専用のプライバシーポリシーが用意されている
B	サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述が有る
C	サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述が無い
D	サービスのプライバシーポリシーとは言えない一般的な Web サイトのプライバシーポリシーが有るだけ
E	会社としての抽象的なポリシー（個人情報保護方針）が有るだけ
F	プライバシーポリシーへのリンクが無いまたはリンク先にそれらしきものが見当たらない

次に、様式ランクが「A」「B」「C」であるアプリのプライバシーポリシーについて、利用者情報の取得に関する記述の有無を評価することにした。

これは次の方法で行う。まず、アプリが要求している各 Permission に対応する利用者情報のそれぞれについて、取

Vol.2013-CSEC-62 No.61
Vol.2013-SPT-6 No.61
2013/7/19

得に関するポリシーでの記述の有無を確認し、集計表（図1）に記載する。そして、対応する利用者情報についての記述がポリシーに書かれているPermissionが1つ以上あれば、アプリにおける利用者情報取得の記述の有無を「有」と判定し、1つも記述がないもののみ「無」と判定した[ix]。今回の調査では、「無」と判定したアプリは3個のみであった。

そして次に、これを「有」と判定したアプリを対象に、プライバシーポリシーの内容の優劣を評価することにした。優劣の評価は、標準を「0」とし、どちらかといえば優れているものを「+」、どちらかといえば優れていないものを「－」とし、表 3 の基準で評価を行った。以下、このランクを「内容ランク」と呼ぶ。

表 3 プライバシーポリシーの内容によるランク

ランク	判断基準
＋	取得情報ごとにその利用目的が書かれている
0	「＋」でも「－」でもない
－	取得情報の範囲や利用目的があいまいに書かれている[x]

5. 調査結果

今回の調査の結果を以下に示す。図 3 は、無料アプリトップ 500 と有料アプリトップ 500 の様式ランクの分布である。グラフ内の数字はそのランクを付けられたアプリの数を表す。ランク「A」および「B」を直線パターンの寒色、「C」～「E」をドットパターンの暖色、「F」を単色の赤で示している。

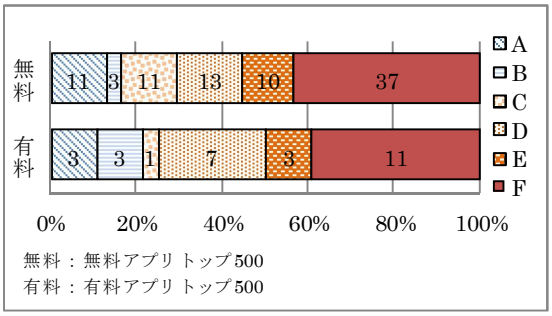

図 3 無料アプリトップ 500 と
有料アプリトップ 500 の様式ランク分布

無料アプリトップ 500、有料アプリトップ 500 ともに、様式ランク「D」「E」「F」であったものが 7 割以上を占めており、サービスやアプリについてのプライバシーポリシーを公開している場合が少ないことがわかる。また、無料アプリトップ 500 と有料アプリトップ 500 では、有意な違いは認められなかった。

無料アプリトップ 500 では、抽出したアプリについて、人気ランキング上位において開発会社の重複が多く、偏りが見られた。そこで、その偏りの影響の有無を確認するため、人気ランキング 1 位～250 位と 251 位～500 位の前後半に分けたものと、キーワード「あ」で検索して抽出したアプリ（無作為抽出と同等と想定して選んだ抽出法）について、様式ランクの分布を比較した。結果を図 4 に示す。

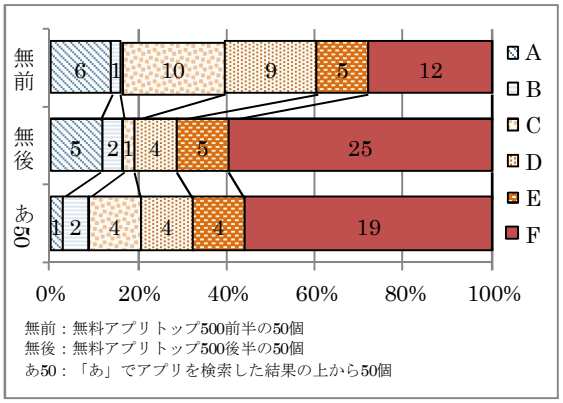

図 4 無料トップアプリ 500 の前・後半と
「あ」の検索結果 50 の様式ランク

無料アプリトップ500の前半／後半では、様式ランク「D」「E」「F」となったアプリの数に明らかな差があり、無料アプリトップ 500 の後半とキーワード「あ」で検索した結果から抽出したアプリを比較すると、様式ランク「D」「E」「F」の分布が類似していると観測できる。

次に、様式ランク「A」「B」「C」と判断されたアプリのうち、「有」と判断されたアプリの、様式ランクと内容ランクの相関を図 5 に示す。

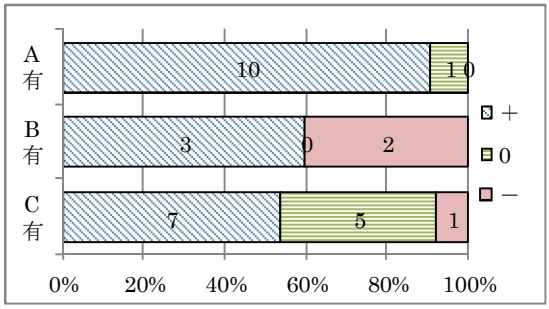

図 5 「A 有」「B 有」「C 有」と
「＋」「0」「－」の相関

[ix] 1つでも記述されていれば「有」としたのは、Permissionを要求していても、対応する利用者情報を送信しているとは限らないためである。もとより、Permission要求の有無から利用者情報の送信の有無を判断することはできないのであり、これは妥協した方法である。

[x] 例えば、取得する利用者情報の列挙において、“including …, but not limited to …” あるいは、“such as …, for example” の定型句で例示し、例示した他に何を送信するかを明らかにしていない場合がこれに該当する。

Vol.2013-CSEC-62 No.61
Vol.2013-SPT-6 No.61
2013/7/19

今回の調査では、そもそも「A」「B」「C」に判定されたアプリの数が少ないという結果であったため、内容ランクでの評価に優位な傾向を見出すことはできなかった。

次に、様式ランク「A」～「E」と掲載場所「X」「Y」の相関を図 6 に示す。

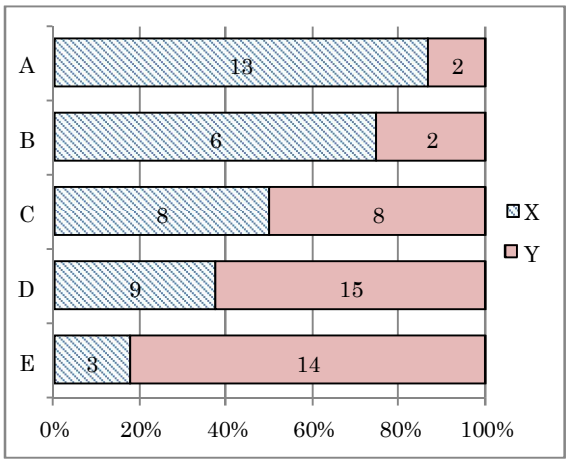

図 6 様式ランク「A」～「E」と
掲載場所「X」「Y」の相関

様式ランクが「A」に近いほど、プライバシーポリシーが、本来あるべき掲載場所である「X」に掲載される傾向が表れている。

最後に、ポリシーの言語と様式ランクとの相関を図 7 に示す。ポリシーの言語は、見つかったポリシーの記述言語が日本語のみであった場合を「日」、日本語と英語の両方があった場合を「日英」、英語のみであった場合を「英」とした。

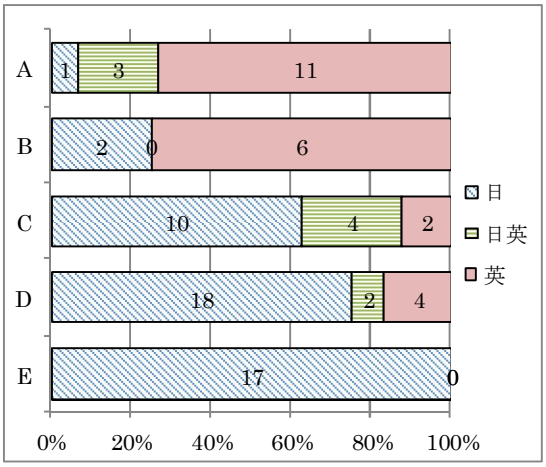

図 7 様式ランク「A」～「E」と
プライバシーポリシーの言語の相関

様式ランクが「A」に近いほど、ポリシーの言語が「日」である場合が少ないという傾向が見て取れる。

6. 考察

今回の調査結果で、

7. おわりに

参考文献

1) Path, We are sorry., http://blog.path.com/post/17274932484/we-are-sorry（2013 年 6 月閲覧）, 2012 年 2 月
2) 米国カリフォルニア州プレスリリース, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy（2013 年 6 月閲覧）, 2012 年 2 月
3) 総務省, スマートフォン プライバシー イニシアティブ ― 利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション ―, 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 スマートフォンを経由した利用者情報の取扱いに関する WG, 2012 年 8 月
4) TRUSTe, More Consumers Say Privacy Over Security is Biggest Concern on Smartphones, http://www.truste.com/about-TRUSTe/press-room/news_truste_mobile_privacy_survey_results_2011（2013 年 6 月閲覧）, 2011 年 4 月
5) 一般社団法人モバイル・コンテンツ・フォーラム, 「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」, 2012 年 11 月
6) 総務省, 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 中間取りまとめ, 2013 年 4 月
7) 下野恵実子, 山口利恵, 高木浩光, 小川貴英: Android アプリケーションにおけるパーミッションの有効性調査, SCIS 2013 講演論文集 1C2-4, (2013)
8) ネットエージェント株式会社, Android アプリの潜在リスクチェックは secroid（セキュロイド）, http://secroid.jp/

正誤表	
誤: 1頁1行～7頁最終行	正: 以下の通り

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

一瀬小夜[†1]　高木浩光[†1]　山口利恵[†2]　渡辺創[†1]

スマートフォン用アプリケーション・プログラム（アプリ）では、どのような情報が自動的に取得・送信されるのかが明らかでないため、アプリケーション・プライバシーポリシーとしてこれら情報を明確にユーザへ提示することが重要である。本稿では、Google Play の無料アプリトップ 500 中 100 アプリ、有料アプリ中 50 アプリ、無作為に抽出した 50 アプリの計 200 アプリについて、そのアプリケーション・プライバシーポリシーの記述状況を調査した。その結果、現状の達成度が 2 割程度であることがわかった。

A Survey of Application Privacy Policies in Mobile Applications

SAYO ICHINOSE[†1]　HIROMITSU TAKAGI[†1]
RIE SHIGETOMI YAMAGUCHI[†2]　HAJIME WATANABE[†1]

Since it is not clear which personal/non-personal data are automatically collected and sent to servers by mobile applications, it is very important to show those information in their application privacy policies to consumers. In this paper, we summarize the current situation of application privacy policies by investigating 200 policies where 100 are from Top Free 500, 50 are from Top Paid 500, and 50 are from a randomly chosen list in Google Play site. Accordingly, those information are clearly written only in about 20% policies.

1. はじめに

近年のスマートフォン（スマホ）の急速な普及により、スマホ用のアプリケーション・プログラム（アプリ）が、利用者のプライバシーに関わる新たな問題を引き起こしている。例えば、2012 年 2 月には、米国企業が運営するソーシャル・ネットワーキング・サービス（SNS）用のアプリが、利用者に無断でスマホ内の電話帳データをアップロードしている事実が発覚して非難の声が上がり、経営者が謝罪してアプリを修正するという事態があった [1)]。また、悪意あるアプリによる被害も報告されるようになり、日本においても、「電池が長持ちする」などと機能を偽って、密かに利用者の電話帳データを盗むアプリが出回り、アプリの配布者が検挙され、地裁で有罪判決[i]を受けるという事件があった。

悪意ある者が利用者を騙してアプリを実行させる行為は犯罪[ii]として摘発していくほかないであろうが、前記の SNS 用のアプリの事例のように、正当な事業者がサービス実現のために善かれと利用者から情報を取得した場合については、利用者に断りなく取得したことが非難の対象となることはあるにせよ、そうしたケースに対してまで直接に刑事罰をもって対処するのが適切とは言えないであろう。

アプリによるスマホからの情報取得が、利用者にとって許容できるものであるか否かは、各々利用者の価値観によって異なるものであり、例えば、GPS による位置情報を使うアプリで、位置情報を無断で収集されることが平気な利用者もいれば許せない利用者もいるであろう。したがって、どのような情報取得が許されるのかを一律に定めることはできず、利用者各自の判断に委ねるほかない。そうした利用者の判断を可能にするには、まず、各アプリがどのような情報を送信するものであるかを、利用者に対して説明することが不可欠である。

このような状況の中、米国では、2012 年 2 月、カリフォルニア州の司法長官が、Google や Apple などアプリ配布を事業とする主要 6 社と、プライバシー保護策の改善で合意したと発表した [2)]。これは、カリフォルニア州法「Online Privacy Protection Act」に基づき、アプリ配布サイトの分かりやすい場所にプライバシーポリシーを表示することなどを求めたものである。この合意により、Google や Apple のアプリ配布サイトには、各アプリの説明ページ内に、「プライバシーポリシー」との見出しのリンクを掲載する専用の場所が設置されることとなった。

時を同じくして、日本でも、同様の問題意識に基づき、総務省が、「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」の下に、「スマートフォンを経由した利用者情報の取扱いに関する WG」を組織し、2012 年 8 月に、「スマートフォン プライバシー イニシアティブ」という報告書 [3)]（以下、総務省報告書）を発表した。総務省報告書は、「関係事業者等や業界団体のイニシアティブによる

†1 独立行政法人産業技術総合研究所
†2 東京大学ソーシャル ICT 研究センター

[i] 京都地裁平成 25 年 5 月 24 日判決

[ii] 刑法第 168 条の 2 及び第 168 条の 3 の不正指令電磁的記録に関する罪に当たる場合がある。

自主的な取組の推進が期待されるもの」として、「スマートフォン利用者情報取扱指針」（以下、総務省指針と言う。）を示している。

総務省指針がアプリ提供者に対して推奨しているのは、アプリケーションごとにプライバシーポリシーを策定して表示することと、一部の情報については取得に際して個別の情報の取得について利用者の同意を求めるものとすることの 2 点[iii]である。

我々は、このような指針が提案されている日本において、アプリ提供者らが実際にどれほどそれを達成しているのかの現状を調査する必要性があると考えた。特に、前者の達成状況については、前記カリフォルニア州司法長官の発表文の参考資料にも調査結果が紹介されており、2011 年 2 月の時点で、米国で配布されていた無料トップ 340 のアプリのうち 19%にしかプライバシーポリシーへのリンクが示されていなかったという調査結果 [4]がある。こうした調査は継続して行うことで改善の状況を評価することができるため、調査の手段と評価の基準を明確にして、誰でも追調査できるようにしておくことが有益である。

本稿は、このような問題意識の下、総務省指針が求める 2 点のうち、前者の「アプリケーションごとにプライバシーポリシーを策定して表示すること」の達成度について、Android 用アプリの配布サイトである「Google Play」を対象として、調査方法と評価基準を明確にするとともに、2013 年 4 月の時点で配布されていたアプリを対象に調査を行った結果を示すものである。

2. 調査方針

総務省指針を受けて、2012 年 11 月、携帯電話向けサービスの業界団体である一般社団法人モバイル・コンテンツ・フォーラムが、「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」[5]を発表した。そこでは、「アプリケーション・プライバシーポリシー」という用語が用いられており、この語を用いることについて次のように説明されている。

> 本ガイドラインでは、アプリケーションごとに利用者情報の取扱い方針を記載したものを「アプリケーション・プライバシーポリシー」と表記しています。
>
> 個人情報保護マネジメントシステム規格である日本工業規格の JIS Q 15001:2006 における「個人情報保護方針」は、事業者の代表者が個人情報の収集、利用、提供等に関する保護方針としてさだめるものであり、原則として 1 社に一つ作成されていることが一般的ですが、名称としてプライバシーポリシーという文言が用いられ、広く普及しています。
>
> 既に作成されている個人情報保護方針と本ガイドラインにおけるアプリケーションごとのプライバシーポリシーは記載内容や位置づけが異なるため、実装にあたっては「個人情報保護方針」と混同されないように、「アプリケーション・プライバシーポリシー」という表記を採用する事を推奨します。【文献 5)より引用】

本稿の調査でも、この考え方に倣い、個人情報保護マネジメントシステムの「個人情報保護方針」に類するポリシーは、適切なアプリケーション・プライバシーポリシーに当たらないものとして集計することにする。

適切なアプリケーション・プライバシーポリシーと呼ぶに相応しいのは、ポリシーを掲示すべきとされるその趣旨に照らせば、そのアプリがどのような挙動をするものであるか、特に、どのような利用者情報を外部に送信するものであるかを記述したものと言える。調査の集計にあたっては、そのような形態での記述をしているものを、適切なアプリケーション・プライバシーポリシーとみなすことにする。

また、アプリケーション・プライバシーポリシーの掲載場所について、前記のカリフォルニア州と主要 6 社との合意に基づいて設置された、アプリ配布ページ上の専用のリンク場所に掲示するのが望ましい形であるとして、集計することにする。

3. 調査方法

調査対象アプリとして、Google Play で公開されている Android 向けアプリから、以下の方法[iv]により、合計 200 個を抽出した。

① 2013 年 4 月 4 日時点の無料アプリトップ 500[v]から、5 番飛びに 100 個
② 2013 年 4 月 10 日時点の有料アプリトップ 500[vi]から、10 番飛びに 50 個
③ 人気順ではなく無作為抽出したアプリも調査するために、2013 年 4 月 9 日時点でキーワード「あ」でアプリを検索した結果の上から 50 個

これらのアプリについて、プライバシーポリシーを探す方法を以下の手順とした。

Google Play の各アプリのページに用意されている「デベロッパー」との見出しのある部分（図 1）からリンクされているものを対象とする。

[iii] 総務省報告書 p.54 より。

[iv] Google Play へのアクセスは、日本語の言語設定で、日本から行った。

[v] Google Play 上で「人気（無料）」との見出しで上位 500 個までのアプリが一覧表示される場所。

[vi] Google Play 上で「人気（有料）」との見出しで上位 500 個までのアプリが一覧表示される場所。

図 1 プライバシーポリシーの掲載場所

まず、「プライバシーポリシー」の見出しで示されるリンクの有無を確認する。リンクが存在する場合には、リンク先のページのスクリーンショットを撮って記録する。(この場合を以下、掲載場所は「X」であると言う。)

このリンクが存在しない場合には、「ウェブページにアクセス」の見出しで示されるリンクの有無を確認し、リンクが存在する場合は、リンク先に示された開発者の Web サイトを訪れ、訪れた先のサイトで、ページのフッタ部分のリンク先を含めて辿って、プライバシーポリシーらしきものを探す。それが見つかった場合には、該当ページのスクリーンショットを撮って記録する。(この場合を以下、掲載場所は「Y」であると言う。)

以上の 2 つの方法で見つからない場合には、プライバシーポリシーの掲載はないとして扱う。

実際には、プライバシーポリシーが、アプリの内容を説明する自由記述欄に記載されている場合や、アプリを実行したときにアプリ上で表示される場合もあると考えられるが、本調査ではそれらを対象にしていない。その理由は、前記調査方針の通り、アプリケーション・プライバシーポリシーはこの所定の場所「X」に記載されることが期待されているものであること、また、アプリ上でポリシーを表示する仕組みができているのであれば、同時に同じものをここに掲載することは容易であるはずであるから、アプリ上に表示するがここに記載のないアプリは少数と予想できる[vii]からである。

今回の調査では、掲載場所が「X」であったアプリは 44 個、「Y」は 58 個、掲載のないアプリが 98 個であった。

プライバシーポリシーの掲載がないものが半数近くに及ぶが、その原因として、アプリが利用者情報を送信しないものであり、プライバシーポリシーを掲載する必要がないためである可能性もある。そのようなアプリをできるだけ除外して集計することにした。

アプリが利用者情報を送信するものであるか否かを判別することはそもそも容易でないが、Android では、利用者情報を参照するアプリは、Permission 機構によってダウンロード時に利用者に警告が表示される仕組みになっているので、これを利用することにし、不完全な方法ではあるが、各アプリが利用者情報に係る Permission を要求しているかを調べ、これを元に、プライバシーポリシーを掲載する必要のないアプリを集計から排除することにした。

利用者情報に係る Permission の一覧を表 1 に示す[viii]。アプリがこれらの Permission を要求する場合、アプリが利用者情報を送信している可能性があるものとする。調査では、Google Play でアプリをインストールしようとした際に表示される Permission の一覧のスクリーンショットを撮り、表 1 の Permission を要求しているかを記録した。

表 1 利用者情報に係る Permission 一覧

Permission	概要
READ_PROFILE	プロフィール情報の読み取り
GET_ACCOUNTS	端末内のアカウントの検索
USER_CREDENTIALS	アカウントの認証情報を使用
READ_PHONE_STATES	端末 ID の読み取り
READ_SMS	SMS の読み取り
READ_CONTACTS	連絡先の読み取り
READ_HISTORY_BOOKMARKS	ブラウザの履歴とブックマークの読み取り
GET_TASKS	実行中のアプリケーションの取得
READ_LOGS	機密ログデータの読み取り
ACCESS_FINE_LOCATION	精細な位置情報
ACCESS_COARSE_LOCATION	おおよその位置情報

また、Android には、表 1 の Permission を要求しなくても取得可能な「Android_ID」と呼ばれる Android OS が生成する端末固有の ID が存在する。この調査では、Android_ID も利用者情報として取り扱うことにし、各アプリが Android_ID を使用するコードを含むか否か、「secroid」[8]の情報を参照して確認した。

[vii] 実際、文献 6)にアプリケーション・プライバシーポリシーの掲載状況の調査結果が掲載されている（p.16）が、その中で、ポリシーがアプリ内に掲載されているのに、「Google Play 紹介ページ」及び「開発者ホームページ」には記載がないというケースは、40 個中 1 個のアプリのみ（同文献図表 1-2-1 より）と、例外的であったことが報告されている。

[viii] 文献 7)の表 1 を参考に作成した。

No.	順位	名称	開発会社	更新日	ポリシーの場所	ポリシーランク	プロフィール情報の読み取り	この端末上でのアカウントの検索	この端末上のアカウントの使用	携帯のステータスとIDの読み取り	連絡先の読み取り	SMSの読み取り	ブラウザの履歴とブックマークを読み取る	実行中のアプリケーションの取得	機密ログデータの読み取り	精細な位置情報(GPS)	おおよその位置情報(ネットワーク基地局)	Android_ID	日・日英・英
57	281			2013/4/5	Y	A有+				無							有	×	英
58	286			2013/4/3	Y	C有0							有			有	有	×	日
59	291			2013/1/31	Y													×	
60	296			2013/3/4	Y	E		○		○						○		×	日
61	301			2013/3/30														×	
62	306			2013/3/31														×	
63	311			2013/4/4	X	A有0		無										有	日英
64	316			2013/3/28	X	B有-				有								有	英
65	321			2012/6/23		F												○	日
66	326			2013/4/1	X													×	

図 2　調査結果の集計表（一部抜粋）

調査の過程で作成した集計表の一部を図 2 に示す。各行が一つ一つのアプリであり、「名称」と「開発会社」はここでは伏せて表示した。各列には、プライバシーポリシーの掲載場所、表 1 の各 Permission に関する調査結果[ix]、Android_ID 利用コードの有無のほか、「A」～「F」、「有」「無」、「＋」「0」「－」といったプライバシーポリシーのランク評価の結果、プライバシーポリシーの言語（「日」「日英」「英」）について記載している。

背景が灰色の行は、表 1 の Permission の要求と Android_ID 利用コードのいずれもない場合であり、アプリケーション・プライバシーポリシーを記述する必要がない場合と判断して評価から除外したアプリである。

今回の調査では、除外したアプリは 52 個であった。残りの 148 個のアプリ（内訳：無料アプリ 85 個、有料アプリ 28 個、「あ」検索結果 34 個）について、次節に示す基準でランク評価を行った。

4. 評価基準

評価は、スクリーンショットを撮って記録した各アプリのプライバシーポリシーを読んで行った。

全体を通して読むと、アプリが送信する情報が何かを記述している「アプリケーション・プライバシーポリシー」と呼ぶに相応しいものがある他に、開発会社が提供しているサービス全体について書かれたものや、利用者が Web サイトで自ら入力する情報（ユーザ登録、アンケートなど）について書かれたものなど、いくつかの様式が混在していることが分かった。

そこで、まず、各アプリのプライバシーポリシーの様式について、表 2 の基準でランク付けすることにした。以下、このランクを「様式ランク」と呼ぶ。

表 2　プライバシーポリシーの様式によるランク

ランク	判断基準
A	個々のスマホアプリ専用のプライバシーポリシーが用意されている
B	サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述が有る
C	サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述が無い
D	サービスのプライバシーポリシーとは言えない一般的な Web サイトのプライバシーポリシーが有るだけ
E	会社としての抽象的なポリシー（個人情報保護方針）が有るだけ
F	プライバシーポリシーへのリンクが無いまたはリンク先にそれらしきものが見当たらない

ランク「E」は、前記調査方針で示した、JIS Q 15001:2006 の「個人情報保護方針」に類するものが該当する。前記調査方針で適切なアプリケーション・プライバシーポリシーと呼ぶに相応しいものは、ランク「A」と「B」が該当する。

ランク「C」は、利用者情報の取得に関する記述があっても、そのアプリによる送信で取得するものなのかが書かれていない場合が該当し、例えば、「端末 ID を取得する場合がある」と書かれていても、何によって送信されるのかを明らかにしていない場合は、ランク「C」と判定する。

ランク「B」の典型例としては、サービス全体のプライバシーポリシーが書かれている中に、どのアプリかを明示した上で、「アプリ経由で自動的に取得する」といった記述[x]で取得情報を示しているものが該当する。

[ix] 表中の印「有」は、この Permission の要求があり、かつ、プライバシーポリシーに、対応する利用者情報の送信についての記述があるものを表し、「無」はその記述がないものを表す。「○」は、Permission 要求はあるが、プライバシーポリシーがないため、記述の有無を調べていないものを表す。）

[x] 文献 5)に示されている「アプリケーション・プライバシーポリシーのモデル案」においても、ポリシーに記述すべき表現として、「以下の利用者情報を以下の利用目的のためにアプリケーション経由で自動的に取得いたします。」という例が示されている。

なお、アプリの機能や開発会社が提供しているサービスの内容から、ポリシーの内容がアプリについて書かれた記述であることを推察できる場合もあるが、評価の客観性を確保するため、あくまでポリシーの記述の様式でランク評価をすることにし、アプリの機能や開発会社の事情については考慮しないことにした。

次に、様式ランクが「A」「B」「C」であるアプリのプライバシーポリシーについて、利用者情報の取得に関する記述の有無を調べる。これは次の方法で行う。

まず、アプリが要求している各 Permission に対応する利用者情報のそれぞれについて、取得に関するポリシーでの記述の有無を確認し、集計表（図 2）に記載する。そして、対応する利用者情報についての記述がポリシーに書かれている Permission が 1 つ以上あれば、アプリにおける利用者情報取得の記述の有無を「有」と判定し、1 つも記述がないものを「無」と判定した[xii]。今回の調査では、「無」と判定したアプリは 3 個のみであった。

そして次に、これを「有」と判定したアプリを対象に、プライバシーポリシーの内容の優劣を評価することにした。

優劣の評価は、標準を「0」とし、どちらかといえば優れているものを「+」、どちらかといえば優れていないものを「－」とし、表 3 の基準で評価を行った。以下、このランクを「内容ランク」と呼ぶ。

表 3 プライバシーポリシーの内容によるランク

ランク	判断基準
＋	取得情報ごとにその利用目的が書かれている
0	「＋」でも「－」でもない
－	取得情報の範囲や利用目的があいまいに書かれている

「＋」評価とならない典型例は、複数の取得情報と複数の利用目的がある場合に、それぞれが分離して列挙されていて、各取得情報と各利用目的の対応関係が示されていない場合である。

「－」評価となる典型例は、取得する利用者情報の列挙において、“including …, but not limited to …”、“such as …, for example” の定型句で例示し、例示した他に何を送信するかを明らかにしていない場合である。

5. 調査結果

今回の調査の結果を以下に示す。図 3 は、無料アプリトップ 500 と有料アプリトップ 500 の様式ランクの分布である。グラフ内の数字はそのランクを付けられたアプリの数を表す。ランク「A」および「B」を直線パターンの寒色、「C」～「E」をドットパターンの暖色、「F」を単色の赤で示している。

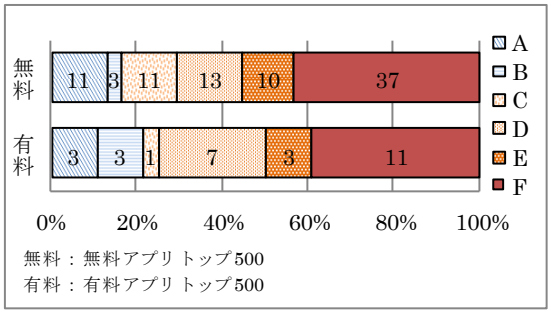

図 3 無料アプリトップ 500 と
有料アプリトップ 500 の様式ランク分布

無料アプリトップ 500、有料アプリトップ 500 ともに、様式ランク「D」「E」「F」であったものが 7 割以上を占めており、サービスやアプリについてのプライバシーポリシーを公開している場合が少ないことがわかる。また、無料アプリトップ 500 と有料アプリトップ 500 では、有意な違いは認められなかった。

無料アプリトップ 500 では、抽出したアプリについて、人気ランキング上位において開発会社の重複が多く、偏りが見られた。そこで、その偏りの影響の有無を確認するため、人気ランキング 1 位～250 位と 251 位～500 位の前後半に分けたものと、キーワード「あ」で検索して抽出したアプリ（無作為抽出と同等と想定して選んだ抽出法）について、様式ランクの分布を比較した結果を図 4 に示す。

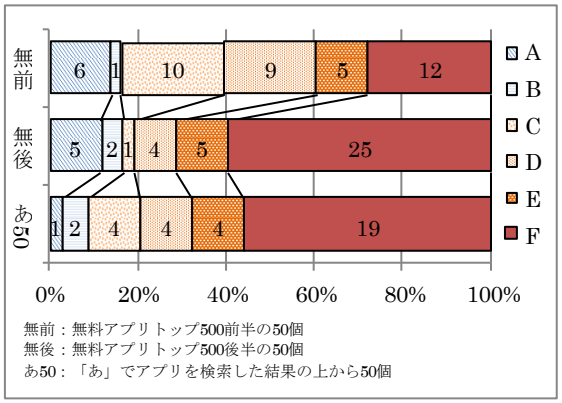

図 4 無料トップアプリ 500 の前・後半と
「あ」の検索結果 50 の様式ランク

無料アプリトップ500の前半／後半では、様式ランク「D」「E」「F」となったアプリの数に明らかな差があり、無料アプリトップ 500 の後半とキーワード「あ」で検索した結

[xii] 1 つでも記述されていれば「有」としたのは、Permission を要求していても、対応する利用者情報を送信しているとは限らないためである。もとより、Permission 要求の有無から利用者情報の送信の有無を判断することはできないのであり、これは妥協した方法である。

果から抽出したアプリを比較すると、様式ランク「D」「E」「F」の分布が類似していると観測できる。

次に、様式ランク「A」「B」「C」と判断されたアプリのうち、「有」と判断されたアプリの、様式ランクと内容ランクの相関を図 5 に示す。

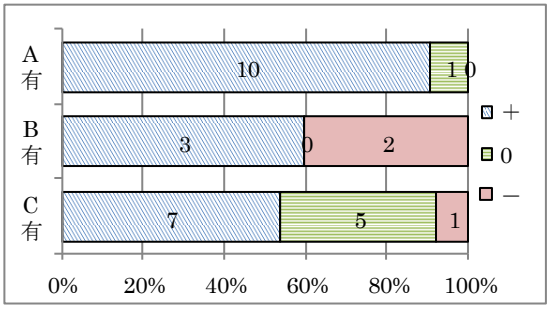

図 5　「A 有」「B 有」「C 有」と
「＋」「0」「－」の相関

今回の調査では、そもそも「A」「B」「C」に判定されたアプリの数が少ないという結果であったため、内容ランクでの評価に優位な傾向を見出すことはできなかった。

次に、様式ランク「A」～「E」と掲載場所「X」「Y」の相関を図 6 に示す。

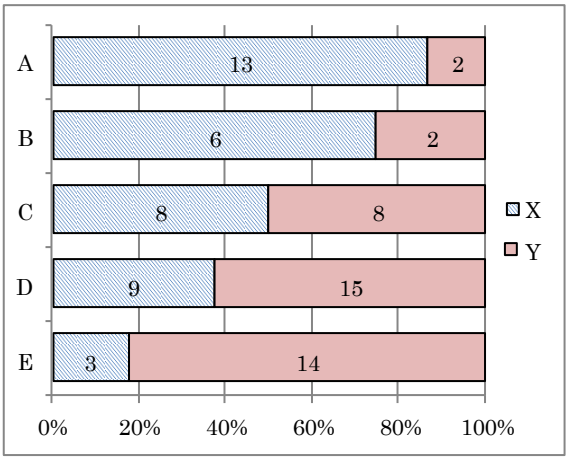

図 6 様式ランク「A」～「E」と
掲載場所「X」「Y」の相関

様式ランクが「A」に近いほど、プライバシーポリシーが、本来あるべき掲載場所である「X」に掲載される傾向が表れている。

最後に、ポリシーの言語と様式ランクとの相関を図 7 に示す。ポリシーの言語は、見つかったポリシーの記述言語が日本語のみであった場合を「日」、日本語と英語の両方があった場合を「日英」、英語のみであった場合を「英」とした。

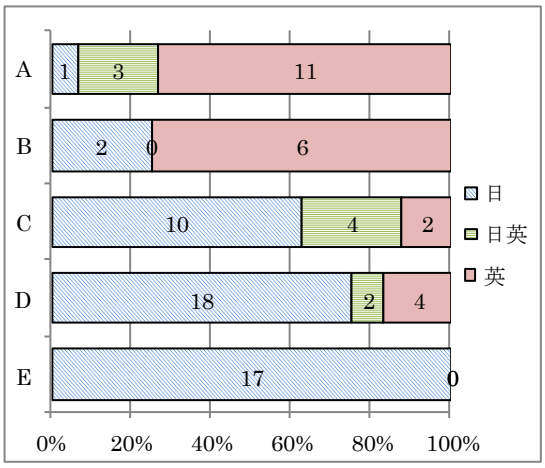

図 7 様式ランク「A」～「E」と
プライバシーポリシーの言語の相関

様式ランクが「A」に近いほど、ポリシーの言語が「日」である場合が少ないという傾向が見て取れる。

6. 考察

今回の調査では、適切なアプリケーション・プライバシーポリシーと言える形でポリシーを掲示していたアプリ（ランク「A」および「B」と評価）の割合は、無料トップ 500 で 16%、有料トップ 500 で 21%程度という結果であった。

図 7 の結果を見ると、日本のアプリ提供者が、アプリケーション・プライバシーポリシー掲載について対応が遅れている様子が窺える[xiv]。

「日英」に分類されたアプリは、外国製のものがポリシーの日本語訳を用意している場合を含んでおり、日本製か外国製かの特定まではしていないが、仮にこれを日本製と仮定しても、日本製のアプリで適切なアプリケーション・プライバシーポリシーを掲載したアプリは、6 件であり、ごく僅かである。

特に、「E」の形態（個人情報保護マネジメントシステムの「個人情報保護方針」に類するポリシー）の傾向は顕著であり、日本独特の形態であると言える。

図 6 の結果を見ると、アプリ配布サイトの「プライバシーポリシー」リンク掲載場所は、ランクが「A」に近いものほど、活用している割合が高いことがわかる。

適切なアプリケーション・プライバシーポリシーを掲示しているアプリでは、この場所を活用している場合が 8 割

[xiv] この結果は日本向けの Google Play に掲載されていたアプリを対象にしたものであるため、例えば、米国製でありながら日本でも人気の高いアプリに限って、適切なアプリケーション・プライバシーポリシーが掲載される傾向があったという可能性を否定できない。正確に日米のアプリを比較するには、米国向けの Google Play に掲載されたアプリとの比較が必要である。

前後であり、この場所の認知はそれなりに進んでいると言える。その一方で、ランク「D」「E」のアプリがこの場所にポリシーを掲載している例もあり、誤用されているケースも少なくないことがわかる。

7. おわりに

スマホの普及により、多様なアプリを自由に選んで利用できる環境が進み、利用者の利便性が高まった一方で、利用者情報を自動的に外部へ送信するアプリも少なくないため、利用者の間に不安が広がっており、米国及び日本の政府機関が、ほぼ同時期に、スマホアプリ利用環境の健全化のため、アプリケーション・プライバシーポリシーの掲示をするよう、アプリ提供者らに促すという状況になっている。日本のアプリ提供者らがこのような政府の施策にどの程度従っているかを継続的に調査することは有益である。

本稿では、そのような継続的な調査が誰にでもできるようにするため、Android 用アプリの配布サイト「Google Play」を対象として、調査方法と評価基準を示した。

この方法と基準に従い、2013 年 4 月の時点での調査を行ったところ、適切なアプリケーション・プライバシーポリシーを掲示していたアプリは、無料トップ 500 で 16%、有料トップ 500 で 21%程度であり、日本製とみられるアプリはごく僅かであった。

今後、一定の間隔をおいて同じ調査を繰り返すことにより、改善が進んでいるか否かを評価できると期待できる。

参考文献

1) Path, We are sorry., http://blog.path.com/post/17274932484/we-are-sorry（2013 年 6 月閲覧）, 2012 年 2 月
2) 米国カリフォルニア州司法省プレスリリース, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy（2013 年 6 月閲覧）, 2012 年 2 月
3) 総務省, スマートフォン プライバシー イニシアティブ ― 利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション ―, 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 スマートフォンを経由した利用者情報の取扱いに関する WG, 2012 年 8 月
4) TRUSTe, More Consumers Say Privacy Over Security is Biggest Concern on Smartphones, http://www.truste.com/about-TRUSTe/press-room/news_truste_mobile_privacy_survey_results_2011（2013 年 6 月閲覧）, 2011 年 4 月
5) 一般社団法人モバイル・コンテンツ・フォーラム, 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, 2012 年 11 月
6) 総務省, 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 中間取りまとめ, 2013 年 4 月
7) 下野恵実子, 山口利恵, 高木浩光, 小川貴英, Android アプリケーションにおけるパーミッションの有効性調査, SCIS 2013 講演論文集 1C2-4, 2013 年 1 月.
8) ネットエージェント株式会社, Android アプリの潜在リスクチェックは secroid（セキュロイド）, http://secroid.jp/