

スマートフォン上のアプリケーションにおける 利用者情報の取扱いの現況等に関する調査研究

報告書

平成 26 年 3 月 31 日

目次

第1章. 調査研究の概要	1
1.1 背景.....	1
1.2 本調査の概要.....	3
第2章. スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る取組の現状	5
2.1 プライバシーポリシーの普及状況	5
2.1.1 調査概要.....	5
2.1.2 調査項目 詳細.....	6
2.1.3 アプリプラボリ調査結果.....	8
2.1.4 他の研究事例との比較.....	15
2.1.5 調査結果まとめ.....	19
2.2 関係事業者における取組状況.....	21
2.2.1 調査概要.....	21
2.2.2 アプリ提供者.....	23
2.2.3 業界団体.....	25
2.2.4 第三者検証事業者.....	30
2.2.5 広告配信事業者.....	36
2.2.6 アプリマーケット運営事業者.....	42
2.3 諸外国における取組状況.....	50
2.3.1 政府における取組.....	50
2.3.2 業界団体における取組.....	56
2.3.3 その他関係しうる事業者における取組.....	57
第3章. 利用者情報の適切な取扱いに向けた課題と提言	59
3.1 提言に向けた検討実施体制について.....	59
3.2 アプリケーションのプライバシーポリシー普及および第三者検証の在り方に関する課題について	60
3.2.1 広告検討 WG の検討内容について.....	60
3.2.2 技術検討 WG の検討内容について.....	61
3.2.3 課題.....	62
3.3 アプリケーションのプライバシーポリシー普及および第三者検証の在り方に関する提言について	66
3.3.1 アプリケーションのプライバシーポリシー普及および第三者検証実証実験に向けて	66
3.3.2 第三者検証における検証基準、検証結果の表示方法について.....	67
Appendix1 : 自治体提供のスマートフォンアプリのアプリプラボリ作成状況	69
Appendix2 : 第三者検証事業者リスト	70

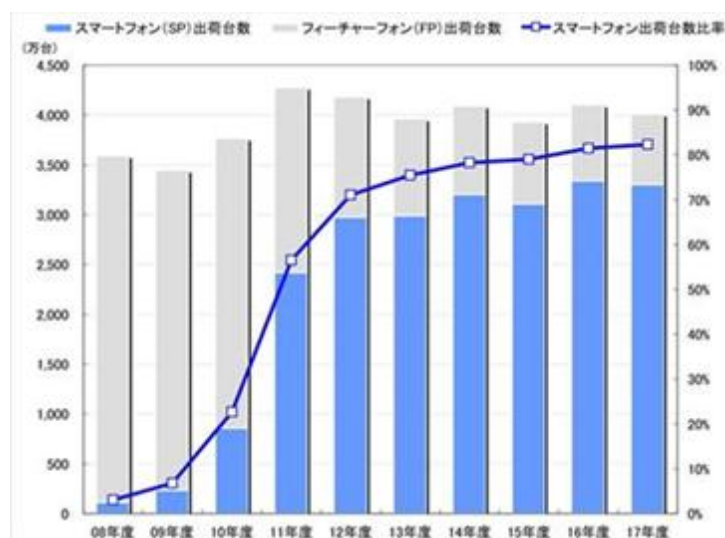
第1章. 調査研究の概要

1.1 背景

我が国において、近年スマートフォン市場が急速に成長している。株式会社MM総研が2013年10月に発表した「スマートフォン市場規模の推移・予測」では、2011年時点で携帯電話の単年の出荷台数の過半数がスマートフォンとなっており、今後も出荷台数におけるスマートフォンの比率は高まると予想されている。契約数では、2013年9月末でのスマートフォン契約数は5,015万件、フィーチャーフォンの契約数は6,862万件となり、携帯電話端末合計で1億1,877万件となった。見通しとしては、2014年度中にはスマートフォン契約数が過半数に到達する見込みである。

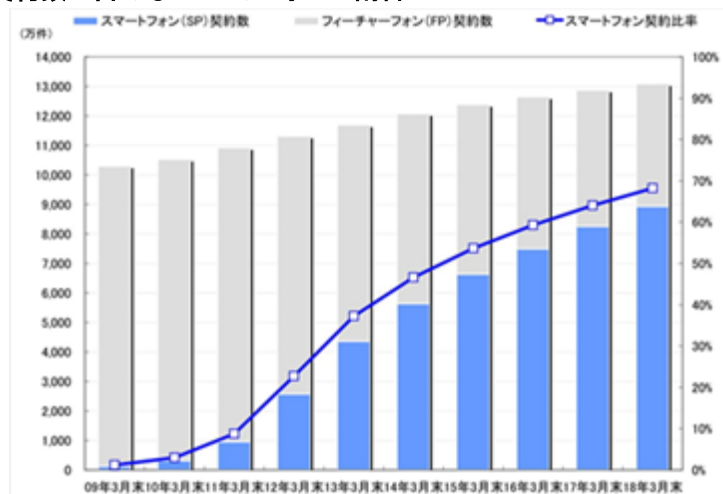
上記の背景に伴い、スマートフォンアプリケーション市場も成長を示しており、米調査会社のアップニーによれば、日本のアプリ売上高は2013年10月に前年同月の3倍強に急拡大し、米国を抜き世界1位の市場規模になった。3位の韓国と比較すると約3倍、4位の英国の5倍以上の規模になっている。

【図表 1.1.1】 携帯電話の出荷台数に占めるスマートフォンの割合



(出所)MM総研「スマートフォン市場規模の推移・予測」(2013年10月)

【図表 1.1.2】 携帯電話の契約数に占めるスマートフォンの割合

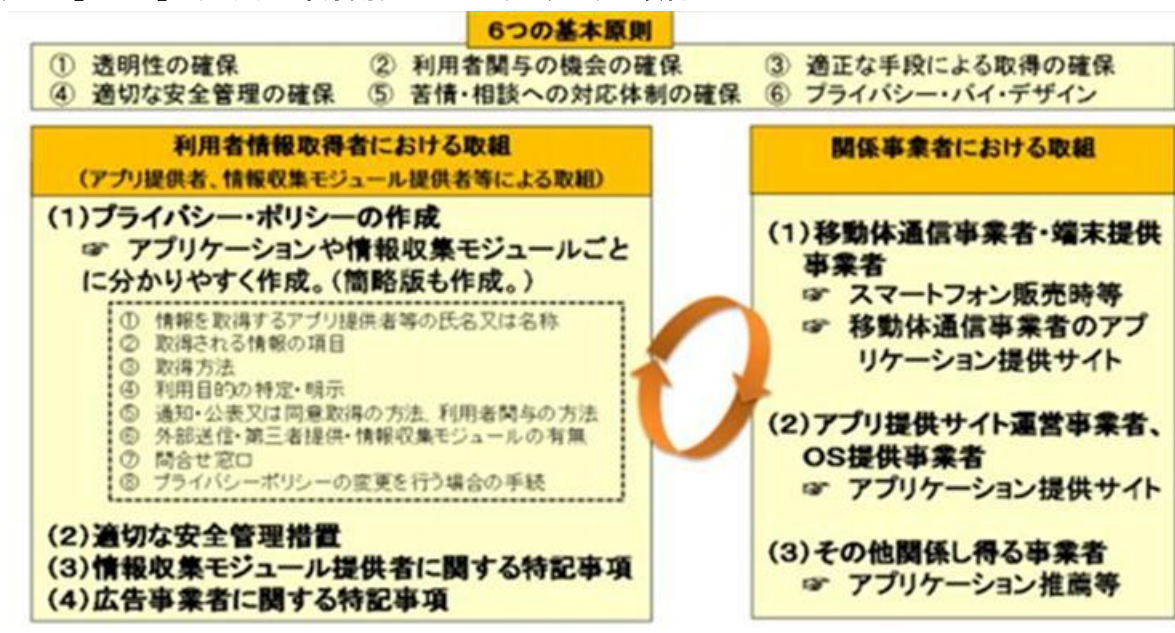


(出所)MM総研「スマートフォン市場規模の推移・予測」(2013年10月)

スマートフォンが普及し、利用者がアプリケーション配信プラットフォーム上からボーダレスにアプリケーションをダウンロード・インストールする利用環境は急速に定着している。ただし、その弊害として、スマートフォンにおいて取得・蓄積された行動履歴や通信履歴等を含む様々な利用者情報が、利用者への十分な説明がないままアプリケーション等により外部送信され、利用者が不安を覚えるケースも見られた。

総務省では、このような状況に対応すべく、「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」において、2012 年 8 月にはスマートフォンにおける利用者情報の適正な取扱いに関する「スマートフォン利用者情報取扱指針」（以下「指針」とする。）を示した「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～」(以下「SPI」とする。)を取りまとめ、公表した。SPI では、図表 1.1.3 に示すように、基本原則 6 項目およびアプリケーションごとのプライバシーポリシー（以下「アプリプラポリ」とする。）の 8 項目を明確にし、指針として関係事業者・団体に広く示し、指針に基づく取組の推進を行っている。

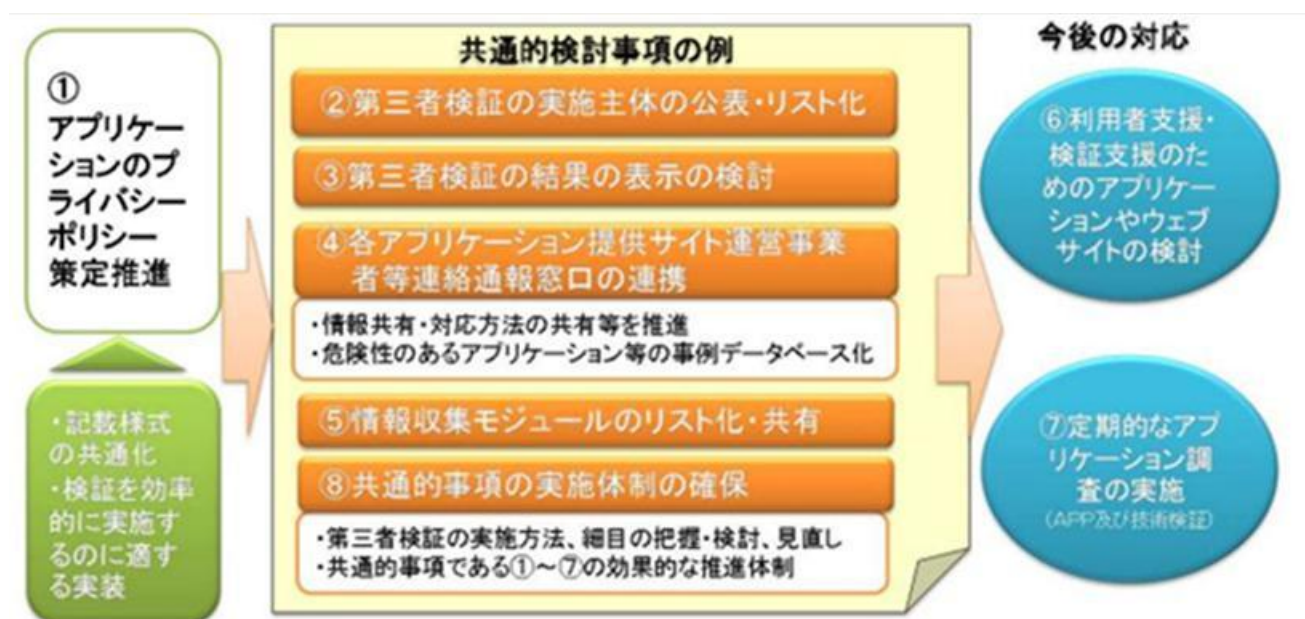
【図表 1.1.3】「SPI」における基本原則およびアプリプラポリ 8 項目



(出所)総務省「SPIⅡ」から抜粋

さらに、総務省では、2013 年 9 月にはアプリケーションの利用者情報の取扱いに関する第三者検証の在り方について提言した「スマートフォン プライバシー イニシアティブⅡ～アプリケーションの第三者検証の在り方～」(以下「SPIⅡ」とする。)を取りまとめ、図表 1.1.4 に示すとおり、今後の具体的措置となる 8 項目を示し、取組を推進している。

【図表 1.1.4】SPIⅡにおける今後の具体的措置



(出所)総務省「SPIⅡ」から抜粋

一方、関係者の取組としては、2011年5月に「日本スマートフォンセキュリティ協会」(JSSEC)が組成され、ICTの各レイヤーに係る事業者、セキュリティ会社、大学等、多様なステークホルダーが参加し、積極的に研究や民間ガイドライン作成などの活動が行われている。2012年4月より一般社団法人として活動しており、SPIおよびSPIⅡに基づき、様々な技術的な調査研究、普及啓発活動及び政策提言を実施している。

加えて、SPIを受けて、2012年10月には「スマートフォンの利用者情報等に関する連絡協議会」(SPSC)が設立され、スマートフォンのアプリケーションに関係する各種団体・企業が参画し、SPIおよびSPIⅡに基づき、各業界が作成するガイドラインやプライバシーポリシーのモデル、利用者情報の取扱いに関する検討、情報共有を行っている。

本調査では、SPIおよびSPIⅡを受けてスマートフォンアプリケーションに係る各種団体・企業等の関係者が取組を進めている状況をリアルタイムに把握することで、共通の検討が可能な項目を抽出するとともに、それぞれ官民の取組の実効性を確保するため、アプリケーションの実態を把握し、アプリケーション調査の基準や追加的に取るべき措置について検討を行うことを目的とする。

1.2 本調査の概要

本調査実施の項目は、SPIおよびSPIⅡの内容を踏まえ、以下の4つの調査項目の調査を行うものとする。

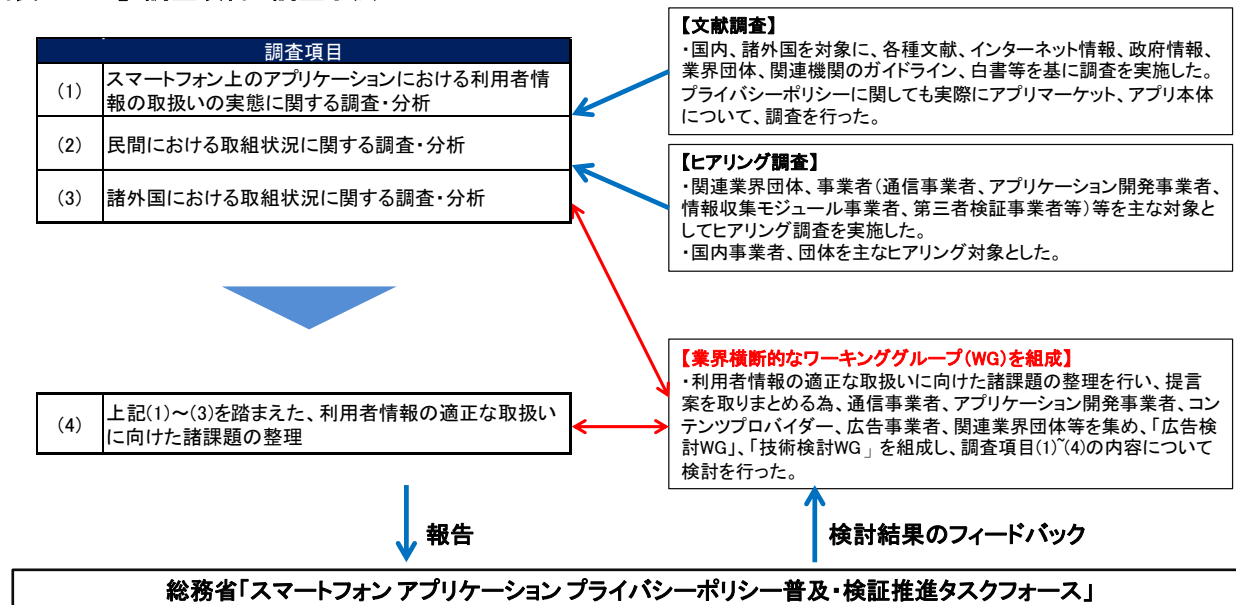
- (1) スマートフォン上のアプリケーションにおける利用者情報の取扱いの実態に関する調査・分析
- (2) 関係事業者・団体等における取組状況に関する調査・分析
- (3) 諸外国における取組状況に関する調査・分析
- (4) 上記(1)～(3)を踏まえた、利用者情報の適正な取扱いに向けた諸課題の整理

(1)～(3)の調査に関しては、図表1.2.1に示すとおり、主に文献調査及びヒアリング調査を基に調査分析を実施し、それらの結果に基づき、(4)の利用者情報の適正な取扱いに向けた諸課題の整理を行った。

本調査実施にあたっては、総務省が2013年12月に設置した「スマートフォン アプリケーション プライバシーポリシー普及・検証推進タスクフォース」と緊密に連携した。

また(1)～(4)の検討に関しては、業界横断的なワーキンググループ(WG)として、「広告検討WG」、「技術検討WG」の2つを設置し、内容について検討を行った。

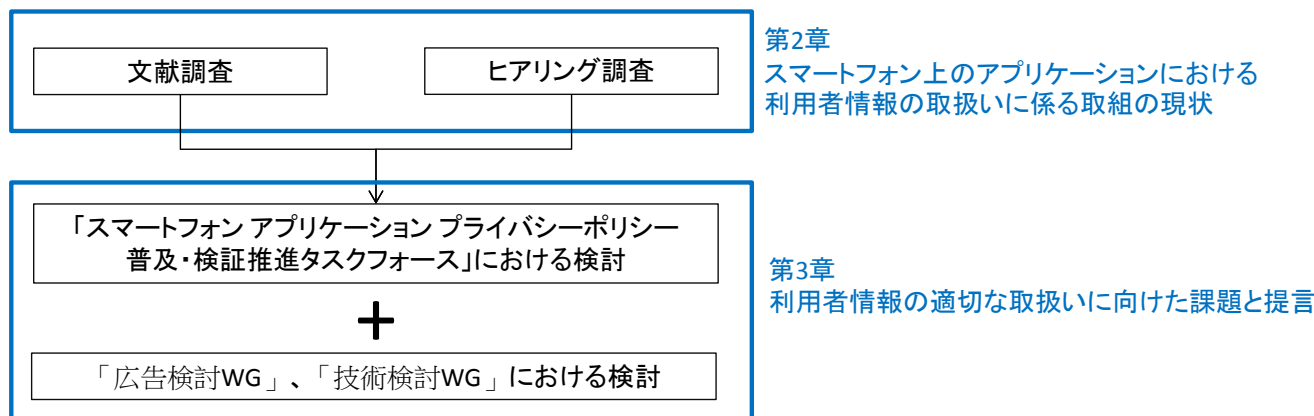
【図表 1.2.1】 調査項目と調査手法



(出所) 日本総合研究所作成

本報告書の構成として、第2章において、文献調査、ヒアリング調査を基に、調査項目(1)～(3)の内容について記述し、上記のタスクフォース、ワーキンググループの内容を踏まえ、第3章において(4)の結果について記述した(図表1.2.2)。

【図表 1.2.2】 本報告書の構成



(出所) 日本総合研究所作成

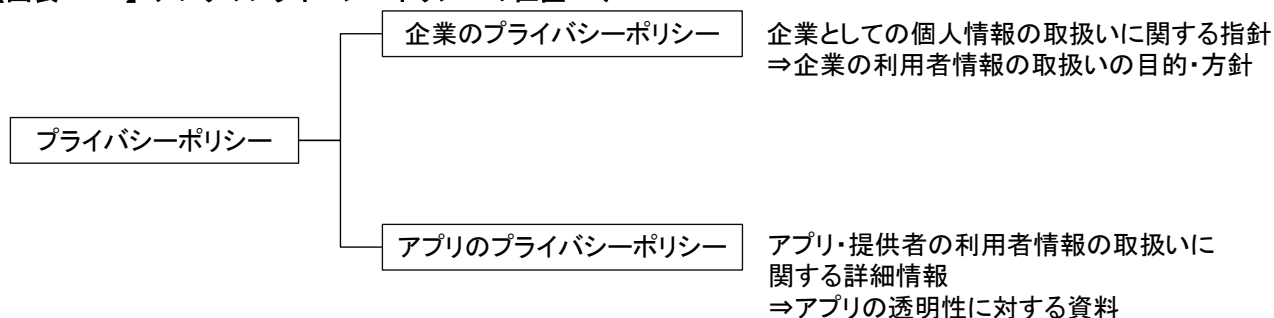
第2章. スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る取組の現状

2.1 プライバシーポリシーの普及状況

2.1.1 調査概要

利用者情報の取扱いに係る取組の現状調査として、アプリケーションのプライバシーポリシーについて調査を行う。本調査の目的は、第一にアプリケーションのプライバシーポリシーの普及状況を調査することである。プライバシーポリシーと一言で言っても、アプリごとのプライバシーポリシー（アプリプラポリ）だけでなく、企業に関するプライバシーポリシー等、対象によってその意味合いは大きく異なる。企業のプライバシーポリシーは、その企業の個人情報の取得・取扱いに関する全体の指針を示すものである。一方でアプリプラポリは、アプリが利用者の利用者情報を取得し適切に取り扱うために、当該企業がアプリやアプリ提供者の利用者情報の取得・取扱いに関する詳細を説明して、アプリの透明性を高めることが最大の目的である（図表 2.1.1）。したがって同一のポリシーであっても、企業とアプリ、どちらのプライバシーポリシーとして提示されているかによって、受け取り方も異なる。本調査では、「アプリのプライバシーポリシー（アプリプラポリ）」の観点に絞って、プライバシーポリシーの調査を行う。

【図表 2.1.1】アプリのプライバシーポリシーの位置づけ



(出所) 日本総合研究所作成

また本調査の第二の目的は、アプリプラポリの検証を通じて、今後アプリプラポリの検証の自動化を試みる場合に、技術的に検証が可能または検証が容易な部分と、困難である部分とを区別することである。本調査では目視によりアプリプラポリの検証を行っているが、今後第三者検証の実施を検討し、検証するアプリ数を拡大させる上で、自動で分析を行う手法が必要となる。したがって、本調査を通じ、今後アプリプラポリの検証を自動で行う仕組みについて検討し、機械による検証が容易な項目と困難な項目、また各項目の評価基準について整理する。

本調査の調査対象となるアプリとして、OS は Android、iOS の 2 つの OS を対象とし、各 OS のアプリマーケット（GooglePlay、AppStore）における、人気上位 100 位を調査対象とした¹。また、国によってアプリの人気が異なるため、今回国際比較を目的として、日本、米国、英国の 3 か国を対象として、上記のプライバシーポリシー調査を行った。また、上位 100 位の内、アプリによっては対象地域の設定によりダウンロードできないアプリや、調査期間中にマーケットより削除されダウンロードできないアプリが存在した。それらのアプリを今回対象外とした結果、最終的な調査対象のアプリの数は図表 2.1.2 となった。

¹ 各国の OS 別のアプリマーケットのランキングは、App Annie (<http://www.appannie.com/>) の 2014 年 2 月 8 日、2 月 9 日時点の各国・各 OS ランキングを引用した。

【図表 2.1.2】国・OS 調査対象アプリ数

	日本	米国	英国
Android	n=100	n=71	n=71
iOS	n=96	n=85	n=91

(出所) 日本総合研究所作成

調査内容は、下記の 4 つとなる。

- ① アプリプラポリの作成・掲載状況
- ② 「スマートフォン プライバシー イニシアティブ」で示される 8 項目の記載
- ③ 利用者情報の取得に関する利用者への同意取得方法
- ④ プライバシーポリシーの概要版作成・掲載状況

調査項目の詳細に関しては次節で説明する。ⁱ

2.1.2 調査項目 詳細

①「アプリプラポリの作成・掲載状況」に関しては、具体的にプライバシーポリシーを作成しているアプリが、どの程度存在するかについて調査を行った（調査項目の詳細は図表 2.1.3）。またプライバシーポリシーの有無だけでなく、プライバシーポリシーの作成・掲載状況の基準として、独立行政法人産業技術総合研究所高木浩光主任研究員の過去調査基準（図表 2.1.4）を採用し、プライバシーポリシーを A~F の 6 段階に分けて、プライバシーポリシーの内容に関しても調査を行った。

【図表 2.1.3】調査項目① アプリプラポリの作成・掲載状況 詳細

調査項目	調査内容	
マーケットのアプリ紹介ページにおけるプライバシーポリシーの作成・掲載状況	プライバシーポリシーへのリンクの状況	❖ アプリの紹介ページにおけるプライバシーポリシーのリンクの有無
	ディベロッパーページにおけるプライバシーポリシーの状況	❖ 紹介ページにリンクのあるディベロッパーページ内のプライバシーポリシーの有無
	アプリ紹介文におけるプライバシーポリシーの状況	❖ アプリ紹介文中のプライバシーポリシーの記載の有無
アプリ内におけるプライバシーポリシーの作成・掲載状況	アプリ内のプライバシーポリシーの状況	❖ アプリ内のプライバシーポリシーの有無
	アプリ初回起動時のプライバシーポリシーの公表	❖ アプリ初回起動時におけるプライバシーポリシー表示の有無
	プライバシーポリシーの記載されている階層	❖ アプリのトップ画面からプライバシーポリシー画面に遷移するまでの操作回数(タッチ回数)

(出所) 日本総合研究所作成

【図表 2.1.4】プライバシーポリシーの作成・掲載状況の基準

分類	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ある
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ない

分類	判断基準
D	❖ 一般的な Web サイトのプライバシーポリシーがあるだけ
E	❖ 会社としての抽象的なポリシー(個人情報保護方針)があるだけ
F	❖ プライバシーポリシーへのリンクがない

(出所)一瀬 小夜、高木 浩光、渡辺 創「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国際比較調査」より抜粋

調査項目②の「『スマートフォン プライバシー イニシアティブ』で示される 8 項目の記載」では、SPI8 項目について、各項目を満たしている比率を調査した。詳細は図表 2.1.5 となり、特定の項目に関しては、更に細分化して調査を行った。

【図表 2.1.5】調査項目②「SPI」で示される 8 項目の記載 詳細

調査項目	調査内容	特に重要と考えられる項目	
1.情報を取得するアプリケーション提供者等の氏名または名称	❖ アプリ提供事業者の名称の記載有無	○	
2.取得される情報の項目	取得される項目の記載状況	○	
	取得される項目の詳細		❖ ユーザー情報の各項目(ex.OS 生成 ID、デバイス固有 ID、位置情報)の記載有無
3.取得方法	❖ アプリが利用者情報を取得する方法(自動、手動)の記載状況		
4.利用目的の特定・明示	❖ 取得される利用者情報に対する利用目的の記載状況	○	
5.通知・公表又は同意取得の方法、利用者関与の方法	送信停止の手順の記載状況		
	利用者情報の削除手順の記載状況		❖ 取得される利用者情報に対する削除手順の記載状況
6.外部送信・第三者提供・情報収集モジュールの有無	利用者情報の第三者への送信の有無の記載状況	○	
	利用者情報の送信先の記載状況		❖ 取得される利用者情報の送信先の記載の有無
	情報収集モジュールに関する記載状況		❖ 情報収集モジュールに関する記載の有無
7.問合せ窓口	❖ 問合せ窓口の記載状況		
8.プライバシーポリシーの変更を行う場合の手続	❖ プライバシーポリシーに変更がある場合の手続の記載状況		

(出所)日本総合研究所作成

また利用者情報の取扱いにおいて、「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の 4 点は、最低限必要な情報であると考え、上記 8 項目の中でも、特に 1、2、4、6 はプライバシーポリシーにおいて最低限記載が必要かつ重要な項目と考えられる。

③に関しては、SPIにおいてプライバシー性が高い情報とされた電話番号、電話帳帳、位置情報、メールアドレスに関して、アプリがその情報を取得する際に、個別の同意を取得しているかについて確認を行った（図表 2.1.6）。最後に調査項目④プライバシーポリシーの概要版作成・掲載状況に関しては、各アプリにおいて、通常のプライバシーポリシーと併せてその概要版の有無について調査を行った。

【図表 2.1.6】調査項目③ 利用者情報の取得に関する利用者への同意取得方法 詳細

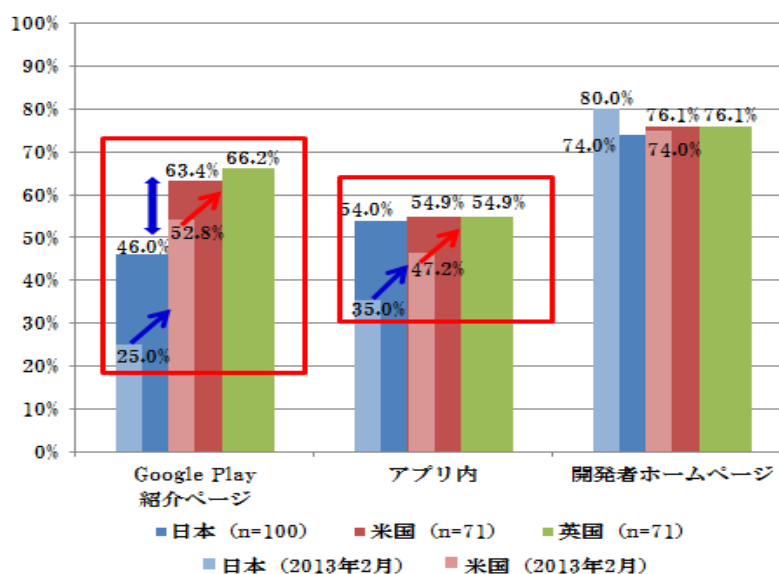
調査項目	判断基準
電話番号	❖ アプリケーションの電話番号の取得の有無。取得する場合、取得時における同意取得の有無。
電話帳情報	❖ アプリケーションの電話帳情報の取得の有無。取得する場合、取得時における同意取得の有無。
位置情報	❖ アプリケーションの位置情報の取得の有無。取得する場合、取得時における同意取得の有無。
メールアドレス	❖ アプリケーションのメールアドレスの取得の有無。取得する場合、取得時における同意取得の有無。

(出所) 日本総合研究所作成

2.1.3 アプリプラポリ調査結果

「① アプリプラポリの作成・掲載状況」の結果に関して、日本、米国、英国における Android アプリのプライバシーポリシーの作成・掲載状況は図表 2.1.7 となる。特徴として、日本は米国、英国と比較して、プライバシーポリシーが GooglePlay 紹介ページに掲載されている比率が低く、プラポリの普及が相対的に進んでいないと言える。一方で 2013 年 2 月に日本総研が日本、米国を対象として行ったアプリプラポリの調査結果²と比較すると、日本、米国共に、GooglePlay 紹介ページ、アプリ内にプラポリが作成されている割合が増加していることから、各国でアプリプラポリに対する意識は高まっていると言える。

【図表 2.1.7】 Android アプリのプライバシーポリシーの作成・掲載状況



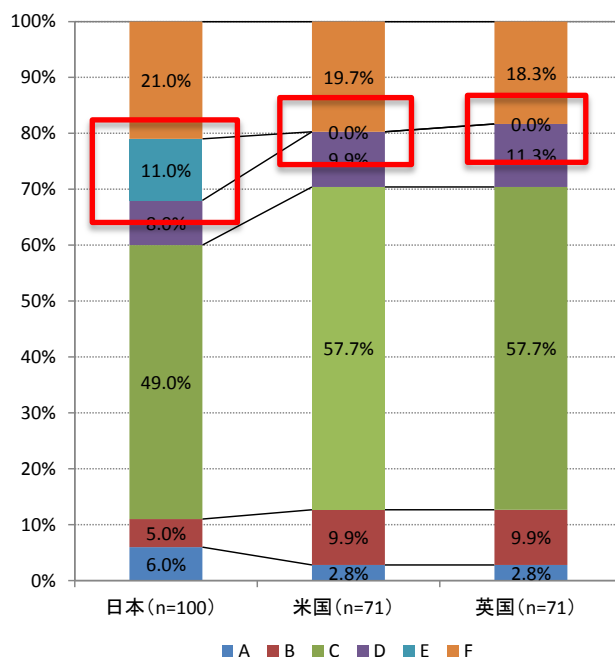
(出所) 日本総合研究所作成

次に、作成・掲載されているプライバシーポリシーの内容について分類を行うと、図表 2.1.8 となる。

² 本調査では、Android における日本、米国のランキング 40 位までのアプリを対象として、プラポリの掲載状況、プラポリの内容等について調査を行った。

結果として、日本のアプリの方が、D～Fのポリシーを記載している比率が高い結果となった。

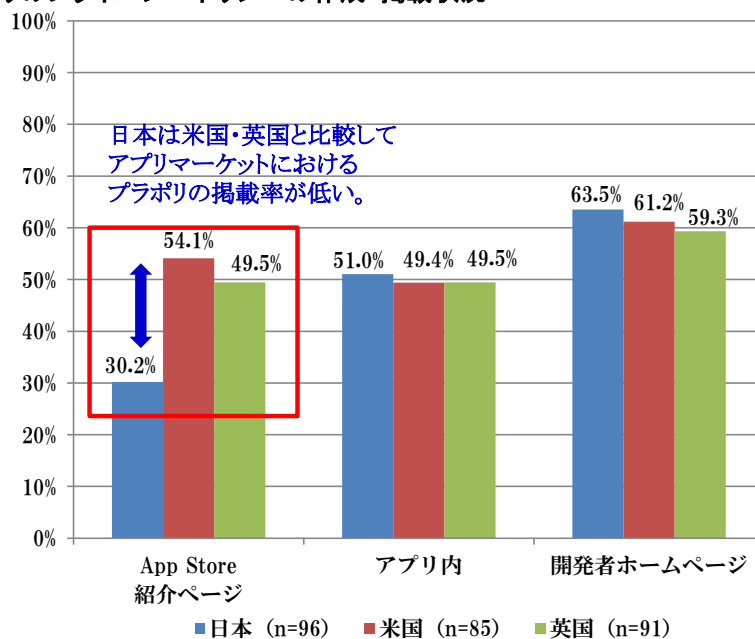
【図表 2.1.8】 Android アプリのプライバシーポリシーの内容分類



(出所) 日本総合研究所作成

同様の調査を iOS において行った結果は図表 2.1.9 となる。Android 同様、マーケット紹介ページにおいて、日本は米国、英国と比較して掲載率が低い。

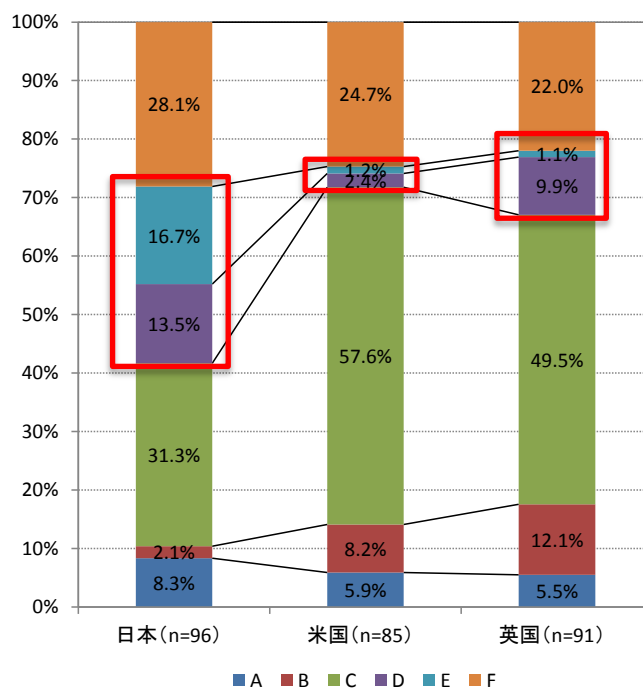
【図表 2.1.9】 iOS アプリのプライバシーポリシーの作成・掲載状況



(出所) 日本総合研究所作成

プライバシーポリシーの内容に関しても、日本のアプリの方が、D～Fのポリシーを記載している比率が高い結果となった (図表 2.1.10)。

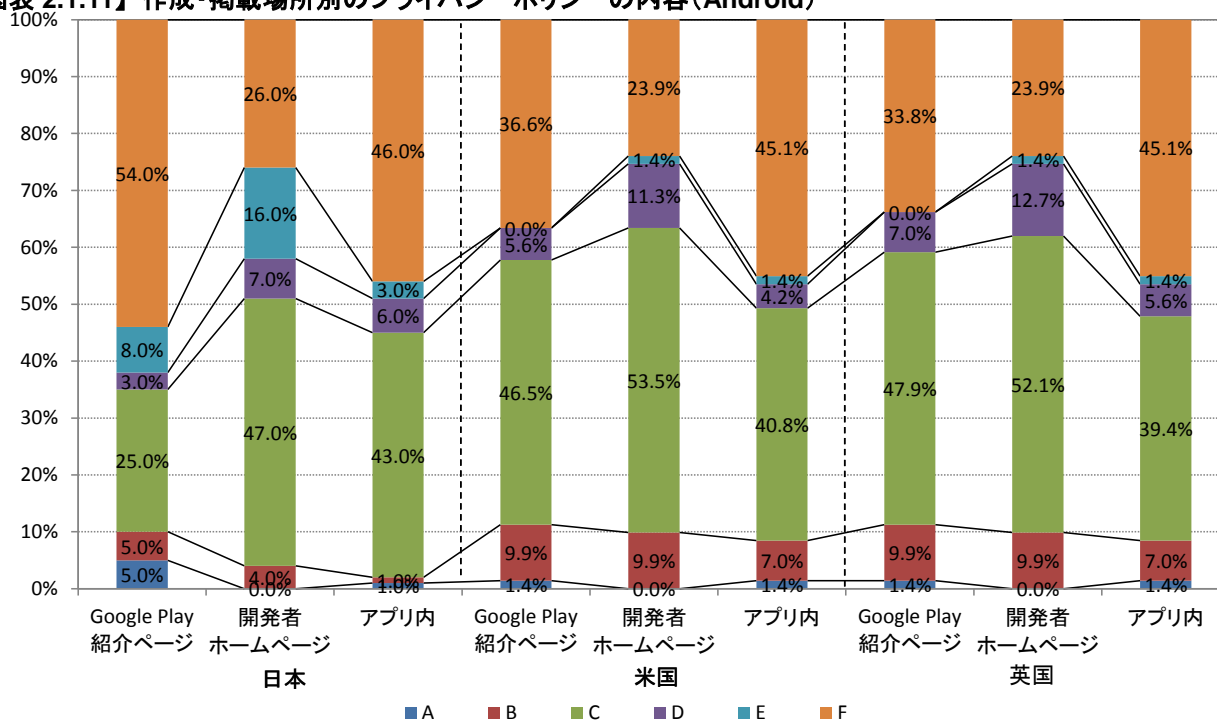
【図表 2.1.10】iOS アプリのプライバシーポリシーの内容分類



(出所) 日本総合研究所作成

次に、作成・掲載場所におけるプライバシーポリシーの内容の違いを分析した。Android における結果は、図表 2.1.11 となる。「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ある」に分類されるプラポリは、GooglePlay の紹介ページで作成・掲載されている場合が多い。一方で開発者ホームページに関しては、「D：一般的な Web サイトのプライバシーポリシーがあるだけ」、「E：会社としての抽象的なポリシー（個人情報保護方針）があるだけ」の割合が、他の場所と比較して高まる傾向が見られる。

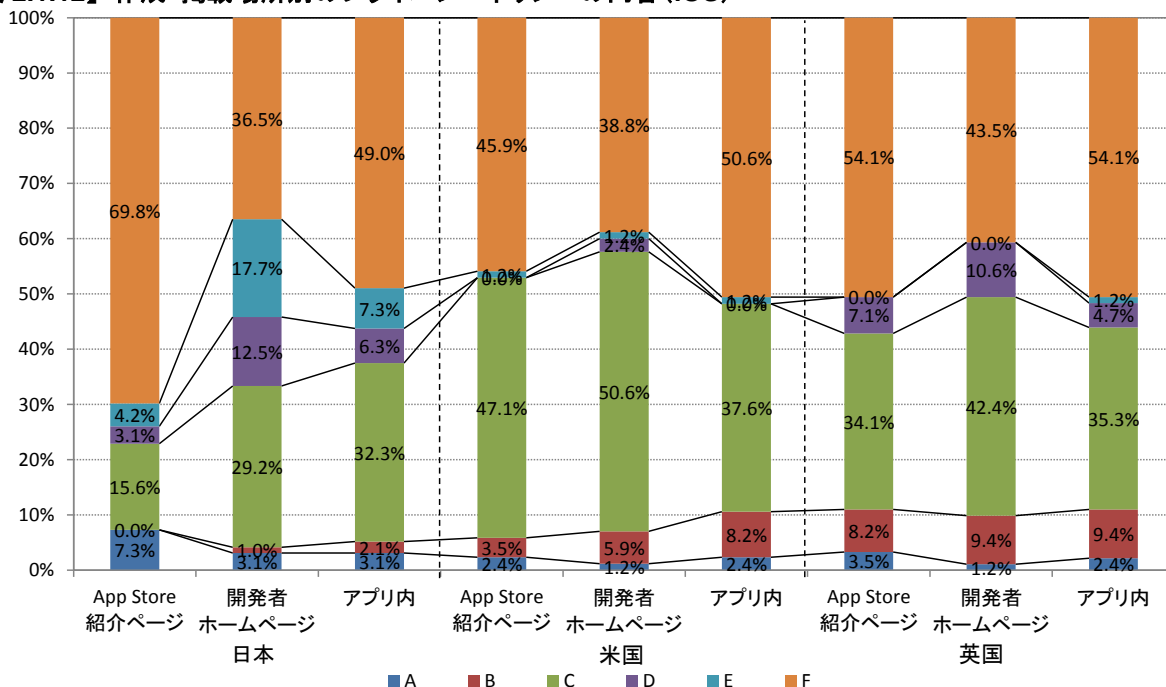
【図表 2.1.11】作成・掲載場所別のプライバシーポリシーの内容(Android)



(出所) 日本総合研究所作成

同様の調査を iOS について行った結果は、図表 2.1.12 となる。マーケット (App Store) の紹介ページにおけるプラポリの掲載率が、日本は他国と比較して低い傾向が見られる。

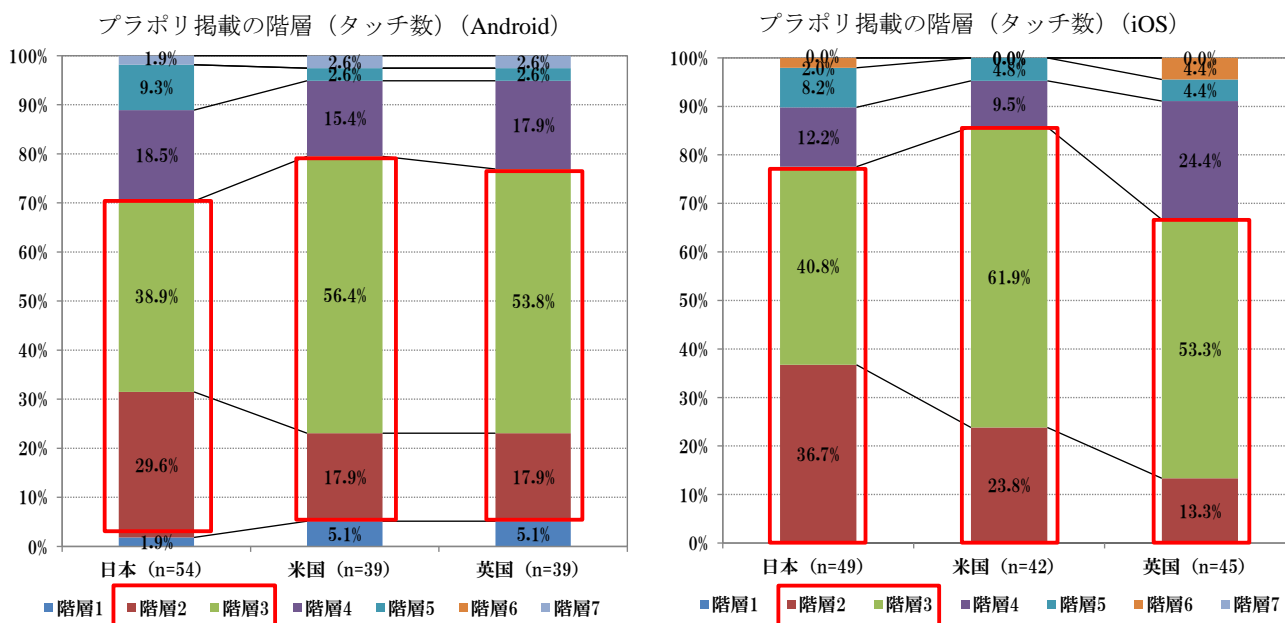
【図表 2.1.12】作成・掲載場所別のプライバシーポリシーの内容 (iOS)



(出所) 日本総合研究所作成

また、アプリの作成・掲載状況に加えて、プラポリの階層として、アプリ内部にプラポリが存在する場合に、アプリのトップ画面からプライバシーポリシーに到達するまでのタッチ回数について調査を行った (図表 2.1.13)。その結果、Android アプリ、iOS アプリ共に、2~3 回のタッチによって閲覧可能な場所に到達するものが多数を占めた。

【図表 2.1.13】アプリのトップ画面からプライバシーポリシーに到達するまでのタッチ回数



(出所) 日本総合研究所作成

次に、項目②『スマートフォン プライバシー イニシアティブ』で示される8項目の記載状況の結果として、Androidのアプリケーションにおける日本、米国、英国の3か国の状況は図表2.1.14となる。

【図表2.1.14】Androidアプリにおける8項目の記載状況

番号	項目	日本(n=79)		米国(n=57)		英国(n=58)		
		アプリ数	比率	アプリ数	比率	アプリ数	比率	
①	情報を取得するアプリケーション提供者等の氏名または住所	74	93.7%	57	100%	58	100%	
②	取得される情報の項目	60	75.9%	53	93.0%	54	93.1%	
③	取得方法	49	62.0%	48	84.2%	48	82.8%	
④	利用目的の特定・明示	56	70.9%	54	94.7%	55	94.8%	
⑤	通知・公表又は同意取得の方法	送信停止の手順の記載状況	42	53.2%	40	70.2%	40	69.0%
		利用者情報の削除手順の記載状況	39	49.4%	25	43.9%	24	41.4%
⑥	外部送信・第三者提供の有無	利用者情報の第三者への送信の有無の記載状況	59	74.7%	49	86.0%	49	84.5%
		利用者情報の送信先の記載状況	13	16.5%	20	35.1%	19	32.8%
		情報収集モジュールに関する記載状況	26	32.9%	36	63.2%	33	56.9%
⑦	問合せ窓口	66	83.5%	51	89.5%	52	89.7%	
⑧	プライバシーポリシーの変更を行う場合の手続	50	63.3%	48	84.2%	48	82.8%	

(出所) 日本総合研究所作成

結果として、「②取得される情報の項目」、「③取得方法」、「④利用目的の特定・明示」等の項目において、日本は米国、英国と比較して、内容が記載されている割合が低い。したがって、SPIの8項目すべてを記載したプライバシーポリシーが、あまり作成されていない可能性が考えられる。

同様の調査をiOSのアプリケーションについて行った結果が、図表2.1.15である。

【図表2.1.15】iOSアプリにおける8項目の記載状況

番号	項目	日本(n=69)		米国(n=66)		英国(n=71)		
		アプリ数	比率	アプリ数	比率	アプリ数	比率	
①	情報を取得するアプリケーション提供者等の氏名または住所	69	100%	66	100%	70	98.6%	
②	取得される情報の項目	52	75.4%	65	98.5%	69	97.2%	
③	取得方法	35	50.7%	58	87.9%	59	83.1%	
④	利用目的の特定・明示	52	75.4%	62	93.9%	66	93.0%	
⑤	通知・公表又は同意取得の方法	送信停止の手順の記載状況	26	37.7%	42	63.6%	43	60.6%
		利用者情報の削除手順の記載状況	27	39.1%	29	43.9%	22	31.0%
⑥	外部送信・第三者提供の有無	利用者情報の第三者への送信の有無の記載状況	53	76.8%	56	84.8%	59	83.1%
		利用者情報の送信先の記載状況	10	14.5%	18	27.3%	20	28.2%
		情報収集モジュールに関する記載状況	22	31.9%	33	50.0%	33	46.5%
⑦	問合せ窓口	58	84.1%	58	87.9%	57	80.3%	
⑧	プライバシーポリシーの変更を行う場合の手続	38	55.1%	58	87.9%	63	88.7%	

(出所) 日本総合研究所作成

全体の傾向は、Android アプリの場合と同様で、「②取得される情報の項目」、「③取得方法」、「④利用目的の特定・明示」等において、日本においては記載されている割合が低い。また iOS の場合は、「⑧プライバシーポリシーの変更を行う場合の手続き」においても、日本と他の二か国で割合に差が見られた。

調査項目③「利用者情報の取得に関する利用者への同意取得方法」に関しては、第一に株式会社 KDDI 研究所の協力の下、静的解析を行い、各アプリが取得し得る利用者情報について調査を行った³。本調査では利用者にとってプライバシー性の高いと考えられる、「電話番号」、「電話帳情報」、「位置情報」、「メールアドレス (Gmail アドレス)」の 4 つを対象としたが、その結果は図表 2.1.16 となる。米国、英国に関しては、日本からインストールできないアプリを調査対象外としているため、アプリの種類に偏りが生じている場合があるが、全体の傾向として、位置情報、次いで電話帳情報を取得する仕組みが最も多く組み込まれている結果となった⁴。

【図表 2.1.16】利用者情報取得に関する静的解析結果(Android)

調査項目	日本	米国	英国
電話番号	18%(18/100)	10%(7/71)	11%(8/71)
電話帳情報	20%(20/100)	23%(16/71)	24%(17/71)
位置情報	30%(30/100)	32%(23/71)	32%(23/71)
メールアドレス(Gmail アドレス)	10%(10/100)	4%(3/71)	6%(4/71)

(出所) 日本総合研究所作成

また、上記の 4 つの情報を取得する際、アプリが利用者から同意を取得するかどうかについても、実際にアプリを動作させることで検証した。その結果は図表 2.1.17 となる。結果として、上記 4 つの利用者情報のいずれかを取得する見込みのあるアプリは、日本、米国、英国の 3 か国とも、全体の 40% 前後である。また、その中で、利用者情報取得時に同意取得が行われないものは、日本で 67% と、同意取得が確認できないアプリが多い。また米国、英国は同意取得が行われないアプリの割合が 81%、84% と、日本よりも高い。

【図表 2.1.17】利用者情報取得時の同意取得状況(Android)

調査項目	日本	米国	英国
4 つの利用者情報(電話番号、アドレス帳、位置情報、メールアドレス)のいずれかを取得する	39%(39/100)	44%(31/71)	44%(31/71)
上記情報の取得時に同意取得が見られない。	67%(26/39)	81%(25/31)	84%(26/31)

(出所) 日本総合研究所作成

³ 調査項目③に関しては、今回利用した解析ツールが Android のみを対象としており、iOS アプリの解析が技術的に困難なことから、Android アプリのみを対象とした。

⁴ 本調査の留意点として、静的解析に基づいた結果であるため、プログラム上から利用者情報を取得するコードの有無を判断したものであり、実際にそのアプリが利用者情報を取得するかどうかは、判断できない部分があることに留意が必要である。

項目④「プライバシーポリシーの概要版作成・掲載状況」に関して、概要版の作成状況は図表 2.1.18 となり、国、OS 問わず、現状プライバシーポリシーの概要版を作成しているアプリは極めて少ない状況である。

【図表 2.1.18】プライバシーポリシーの概要版作成・掲載状況

	日本	米国	英国
Android	5.0% (5/100)	1.4% (1/71)	0.0% (0/71)
iOS	0.0% (0/96)	2.4%(2/85)	0.0%(0/91)

(出所) 日本総合研究所作成

現在概要版を作成している事業者の例としては、国内事業者では株式会社ディー・エヌ・エーが挙げられる。同社は各アプリに対して個別にプライバシーポリシーを作成しており、かつ概要版において、SPI の 8 項目について簡易に記載されている。詳細版に関しては、概要版のリンクから、閲覧することが出来る (図表 2.1.19)。

【図表 2.1.19】プライバシーポリシーの概要版の事例(株式会社ディー・エヌ・エー)

mobage by DeNA 概要版	mobage by DeNA 詳細
<p>アプリ提供者プライバシーポリシー</p> <p>情報を取得するアプリ提供者等の氏名又は名称</p> <p>株式会社ディー・エヌ・エー</p> <p>取得される情報の項目</p> <p>IMEI・MACアドレス</p> <p>取得方法</p> <p>自動取得：IMEI・MACアドレス</p> <p>利用目的の特定・明示</p> <p>サービス・マーケティング提供目的：IMEI・MACアドレス</p> <p>通知・公表又は同意取得の方法、利用者関与の方法</p> <p>アプリマーケットの当該スマートフォンアプリのプライバシーポリシーリンクに掲示</p> <p>外部送信・第三者提供・情報収集モジュールの有無</p> <p>外部送信、第三者提供、情報収集モジュールあり ※ 詳細はMobageプライバシーポリシーをご参照ください</p> <p>問合せ窓口</p>	<p>プライバシーポリシー</p> <p>1.個人情報の収集</p> <p>個人情報とは、個人に関する情報であり、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)を指します。当社(株式会社ディー・エヌ・エー 所在地:〒150-8510 東京都渋谷区渋谷2-21-1 渋谷ヒカリエ)は、個人情報を収集することがあります。当社は、個人情報の利用目的を公表します。</p> <p>2.個人情報の利用目的</p> <p>当社は、収集した個人情報を以下の目的で利用することができるものとします。</p> <ul style="list-style-type: none"> ・オークション、ショッピングモール、コンテンツその他の情報提供サービス、システム利用サービスの提供のため ・当社及び第三者の商品等(旅行、保険その他の金融商品を含む。以下同じ。)の販売、販売の勧誘、発送、サービス提供のため ・当社及び第三者の商品等の広告または宣伝(ダイレクトメールの送付、電子メールの送信を含む。)のため ・料金請求、課金計算のため

(出所) 株式会社ディー・エヌ・エーのウェブページから抜粋

概要版における海外事業者の例としては、米国の eBay Inc. が挙げられる。同社も「Summary of Privacy Policy」としてプライバシーポリシーの概要版を作成しており、概要版の中では、取得する情報、目的、利用目的、第三者提供及び問合せ先を中心に説明している。詳細版に関しては、ディー・エヌ・エーと同様にリンクが掲載されており、各項目の詳細や、モバイル版の利用者情報の取扱いに関して記載されている (図表 2.1.20)。

【図表 2.1.20】海外におけるプライバシーポリシーの概要版の事例(eBay Inc.)

Summary of our Privacy Policy

In this article

- Collection
- Information use
- Disclosure
- Communication preferences
- Other information
- Contact us

This summary provides the key concepts of the full eBay Privacy Policy and applies to the eBay Web site and services. If you have questions, please refer to the full text version of the eBay Privacy Policy.

Collection

- When you register or enter information on our site, we collect your personal information.
- We may combine the information you provide with information from other companies and eBay entities.
- We use cookies and other technology to keep track of your online interaction with our site.

Information use

We use information to:

- Provide the requested services.
- Personalize the site for you, communicate with you, and offer you special eBay promotions.
- Help enforce our terms and conditions, prevent fraud, and keep our Web site safe.

Privacy Policy

Posted and effective for new users: September 11, 2013

Effective for current users: October 26, 2013

Previous version: February 4, 2013

Effective for new users immediately and for current users on October 26, 2013 and superseding all previous versions of the Privacy Policy.

Your Privacy Rights

This Privacy Policy describes your privacy rights regarding our collection, use, storage, sharing, and protection of your personal information. It applies to the eBay.com website and all related sites, applications, services and tools where this policy is referenced, regardless of how you access or use them, including mobile devices.

You can view a summary of this Privacy Policy at our Privacy Summary Page. More detailed information about our privacy practices is available at our eBay Privacy Center.

The eBay website is a licensee of the TRUSTe Web Privacy Program. If Customer Support cannot answer your privacy-related questions, please use the TRUSTe Watchdog Dispute Resolution Process.

TRUSTe Certified Privacy

Contents

- Scope and Consent

(出所) eBay Inc.ウェブページから抜粋

2.1.4 他の研究事例との比較

他のプライバシーポリシーの現状に関する調査としては、株式会社 KDDI 研究所竹森敬祐ネットワークセキュリティグループ研究マネージャによる調査と、独立行政法人産業技術総合研究所高木浩光セキュアシステム研究部門主任研究員による調査が、代表例として挙げられる。本節では、その両者の調査結果と、本調査の結果の比較を行う。

(1) 株式会社 KDDI 研究所調査結果との比較

同社は、2013年2月と12月において、Android マーケットでの無料人気アプリと、無料新着アプリのプライバシーポリシーの掲載状況を調査した。その結果は図表 2.1.21 となる。

【図表 2.1.21】プライバシーポリシーの作成・掲載状況(株式会社 KDDI 研究所調査)

	無料人気アプリ100		無料新着アプリ155
	2013年2月	2013年12月	2013年12月
マーケットにプラポリを掲載しているアプリ	25.0%	46.0%	26.5%
企業のプラポリ	10.0%	32.0%	25.2%
アプリのプラポリ	15.0%	14.0%	1.3%

(出所) KDDI 研究所調査結果より抜粋

図表 2.1.7 の結果と比較したところ、2013年12月時点でのプライバシーポリシーの掲載率は、本調査結果と一致している。同様に図表 2.1.8 の結果と比較すると、本調査結果においてアプリプラポリと考えられるのは、「A：個々のスマホアプリ専用のプライバシーポリシー」または「B：サービス全体のプライバ

シーポリシーと個々のスマホアプリに関する記述」を備えていると分類された 11%となり、KDDI 研究所によるアプリプラポリの比率は 2013 年 12 月時点で 14%となっていることから、本調査結果と KDDI 研究所による調査結果は一致していると言える。

また、KDDI 研究所の調査結果より得られた情報として、2013 年 2 月時点での調査と、2013 年 12 月時点で、マーケットにプラポリを掲載しているアプリの比率が顕著に高まっていることから、この期間中に、事業者の多くがマーケット上にプラポリを公表するようになったものと考えられる。一方で、同社の調査では人気アプリだけでなく、新着アプリの上位 155 位も対象として、プラポリの公表状況を調査しているが、新着アプリ群におけるプラポリの公表の割合は、人気アプリ群のものと比較して顕著に低い結果が得られた。この背景として、人気アプリの上位は特定の大手事業者が開発・提供するアプリが占める割合が高いため、プラポリについても対応されている場合が多くみられるが、新着アプリは企業規模に関係なく、中小企業によるアプリが占める割合が人気アプリよりも高いため、結果としてプラポリの公表比率は低い。したがって、プラポリの普及状況としては、現状大手事業者が対応を開始したところであり、中小企業に対しては今後普及に向けた取組が求められると考える。

また同社の調査では、利用者情報の送信を行うアプリにおけるプライバシーポリシーの掲載状況についても調査しており、結果は図表 2.1.22 となる。

【図表 2.1.22】 利用者情報の送信を行うアプリにおけるプライバシーポリシーの掲載状況

調査時期	2012年4月	2013年2月
上位人気アプリ	100アプリ	100アプリ
利用者情報を送信するアプリ	81%(81/100)	63%(63/100)
プラポリを公表	19%(15/81)	57%(36/63)
アプリのプラポリを公表	—	25%(16/63)
送信情報を正しく説明	3%(2/81)	11%(7/63)
説明が正しく、SPI準拠	—	0%(0/63)

(出所) KDDI 研究所調査結果より抜粋

結果として、上位アプリのうち、利用者情報を送信するものの比率は、2012 年 4 月から 2013 年 2 月の間で減少が見られる。一方、その中でプラポリを掲載しているアプリの比率は増加しており、アプリの利用者情報の取扱いに関する対応が進んでいると考えられる。

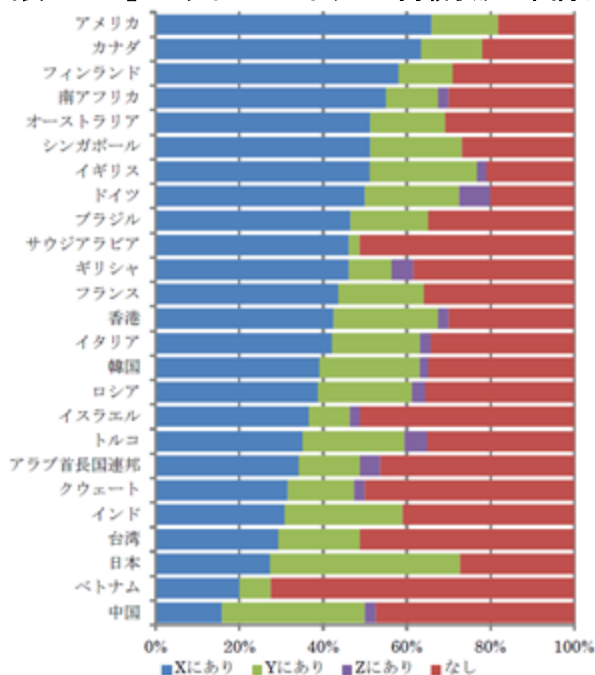
ただし、アプリプラポリを掲載しているものは利用者情報を送信するアプリの 25%、送信情報を正しく説明しているアプリは 11%と、利用者に対して十分な説明を行っているアプリは限られていると言える。

(2) 独立行政法人産業技術総合研究所調査結果との比較

産業技術総合研究所は、「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国際比較調査⁵」において、日本を含む 49 か国における、2013 年 9 月～11 月時点の Android アプリにおけるプライバシーポリシーの掲載状況を調査した。主要国において、トップ 500 からアプリを 10 番飛びに 50 個抽出し、プライバシーポリシーの状況を調査した結果は、図表 2.1.23 となる。

⁵ <https://staff.aist.go.jp/takagi.hiromitsu/paper/ipsj-csec62-62-ichinose-dist.pdf>

【図表 2.1.23】 プライバシーポリシー掲載状況の国際比較の結果



(出所) 産業技術総合研究所調査結果から抜粋



結果として、マーケット紹介ページにプライバシーポリシーのリンクを掲載している比率⁶は、米国では65%程度、日本では30%程度と大きく差があり、本調査と同様の傾向が見られた。なお、本調査の結果と比較して値が低い背景として、産業技術総合研究所の調査では、アプリ人気ランキング下位のアプリを調査対象に含めているため、プライバシーポリシーの対応が不十分なアプリの比率が高まるものと推察される。

また、上記の調査において、主要国におけるプライバシーポリシーの記載内容を抽出して比較した結果は、図表 2.1.24 となる。

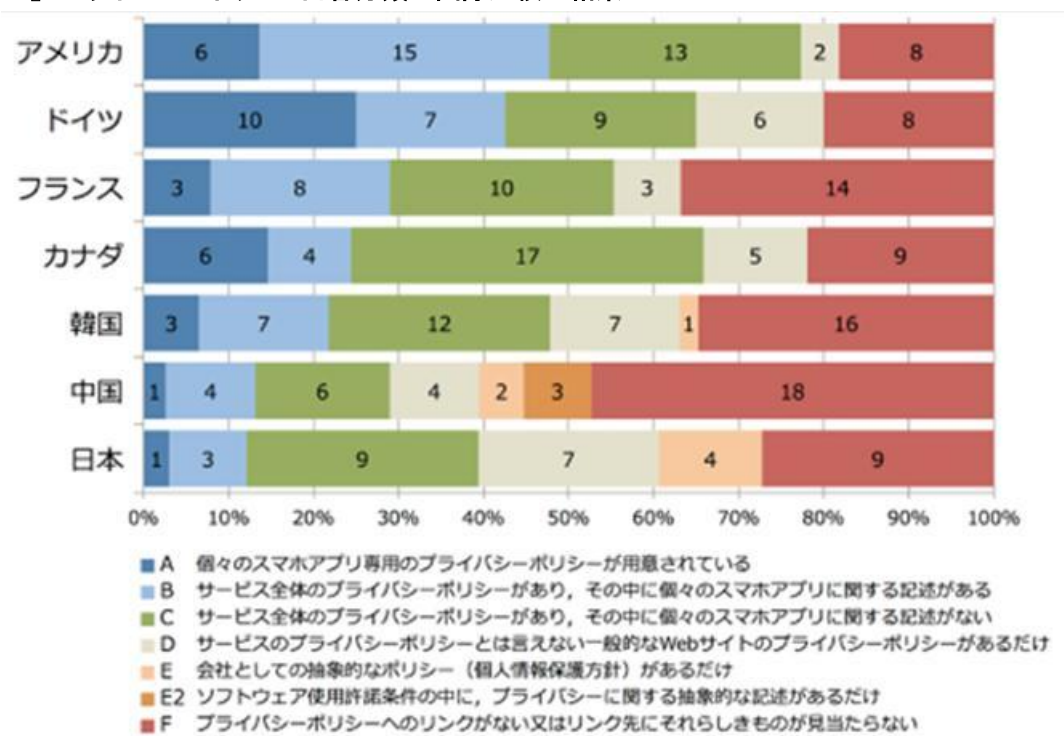
調査の結果として、A、B の比率は日本では10%程度であり、D、E の比率が他国と比べて高い点は、本調査結果と一致している。一方で、産業技術総合研究所の調査では、米国における A、B の比率は日本よりも明らかに高く、この点で一部本調査結果とは違いが生じている。原因としては、B と C の分類の部分で、判断の差が生じたものと考えられる。

産業技術総合研究所では、アプリケーションの利用者情報の取得状況とプライバシーポリシーの掲載状況についても調査を行っている。具体的に図表 2.1.25 の調査では、各国のアプリランキングにおいて、「READ_PHONE_STATE」のパーミッションを取得しているアプリの割合を調査している⁷。結果、日本は同パーミッションを要求しているアプリの割合が最も低く、センシティブな利用者情報を取得している割合が、他国と比較して低いものと考えられる。

⁶ 産業技術総合研究所の調査の定義では、X にプライバシーポリシーがある比率になる。

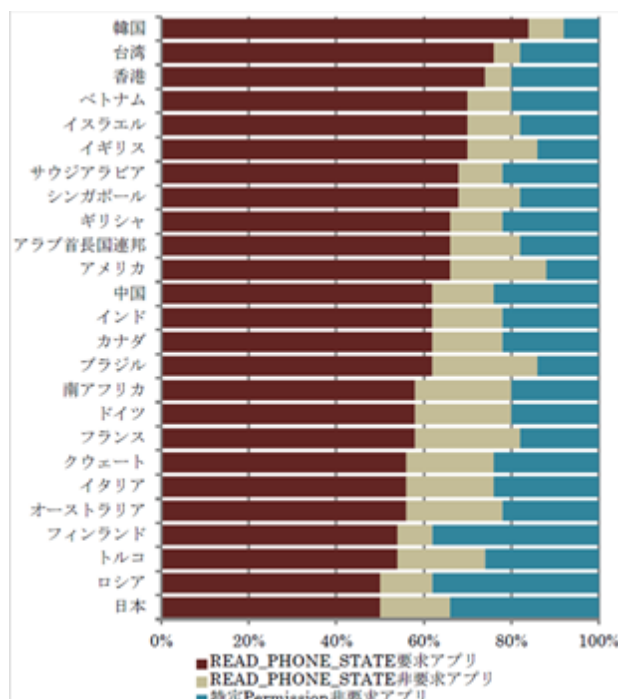
⁷ 「READ_PHONE_STATE」は、端末識別番号を取得するために用いられるパーミッションで、利用者を識別する目的で用いられることから、プライバシー面で懸念がある。

【図表 2.1.24】 プライバシーポリシー内容分類の国際比較の結果



(出所) 産業技術総合研究所調査結果から抜粋

【図表 2.1.25】 アプリの「READ_PHONE_STATE」取得状況の国際比較

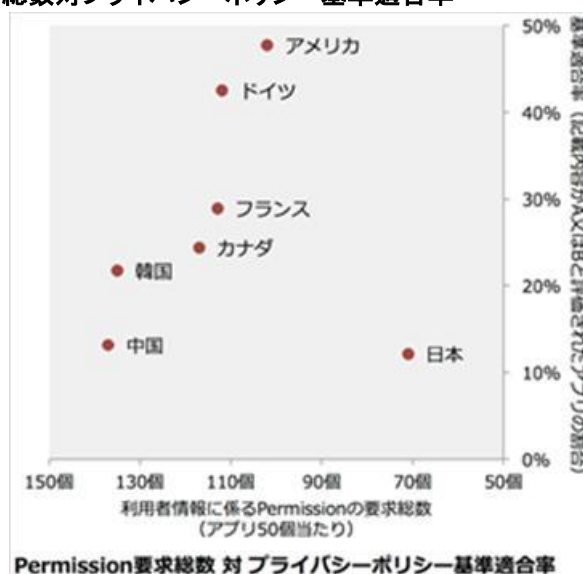


(出所) 産業技術総合研究所調査結果から抜粋

同様に、図表 2.1.26 では、各国のアプリランキングにおける、アプリ 50 個当たりののパーミッション

要求総数と、プライバシーポリシーの基準適合率⁸のマトリクスを評価した。その結果、日本は他国と比較して基準適合率が低いことから、適切なプライバシーポリシーが掲載されている割合が低いと考えられるが、一方でアプリのパーミッション要求総数は他国と比べて低い。このことから、日本のアプリの傾向として、利用者情報は多く取らないものの、プライバシーポリシーによる説明は不十分な状況であると言える。

【図表 2.1.26】 パーミッション要求総数対プライバシーポリシー基準適合率



(出所) 産業技術総合研究所高木浩光氏の調査結果から抜粋

2.1.5 調査結果まとめ

本調査結果のまとめとして、以下の4つの基準を設置し、それぞれを満たすアプリの比率を国・OS別で、図表 2.1.27 に示した。

- 基準①：プライバシーポリシーが作成・掲載されている
- 基準②：SPI8項目の内、重要度の高い項目が記載されている
- 基準③：SPI8項目の全項目について記載されている
- 基準④：基準③に加えて、概要版のポリシーを作成している

上記の分析結果として、基準①のプライバシーポリシーの作成・掲載では日本、米国、英国に大きな差は見られないが、基準②、③において、日本は米国、英国と比較して基準を満たすプライバシーポリシーの割合が低い。8項目のうち重要度の高い項目の記載状況について、日本と他国において差が生じている。したがって、今後の取組として重視すべきは、②の基準を満たすよう、重要度の高い項目についてプラポリに記載することを推奨する取組である。その上で、その他の項目についても、アプリの透明性を高めるという観点から記載を促していくことが必要になる。

また、基準④まで満たすアプリは、3か国全てにおいて、現状ほぼ存在していないため、長期的には、

⁸ 基準適合率とは、プライバシーポリシーにおいて、記載内容が「A：個々のスマホアプリ専用のプライバシーポリシー」または「B：サービス全体のプライバシーポリシーと個々のスマホアプリに関する記述」と評価されたアプリの比率

プラポリの概要版作成の普及に向けた取組が重要になると考えられる。また、プラポリとは異なる別の形式により、利用者に分かり易い説明を行うことも検討する必要がある。

【図表 2.1.27】 アプリプライバシーポリシー調査結果まとめ

		基準①	基準②	基準③	基準④
		プライバシーポリシーが作成・掲載されている	SPI8項目の内、重要度の高い項目を記載している 「①提供者名」、「②取得される情報」、「④利用目的」、「⑥外部送信・第三者提供、情報収集モジュール」	SPI8項目の全項目について記載している。 基準②に加えて、「③取得方法」、「⑤利用者関与」、「⑦問合せ窓口」、「⑧変更の手続き」を記載	基準③に加えて、概要版のプライバシーポリシーを作成している(※)
Android	日本	79.0%	46.0%	34.0%	5.0%
	米国	80.3%	62.0%	53.5%	1.4%
	英国	81.7%	62.0%	53.5%	0.0%
iOS	日本	71.9%	43.8%	24.0%	0.0%
	米国	75.3%	57.6%	34.1%	2.4%
	英国	78.0%	61.5%	46.2%	0.0%

(出所) 日本総合研究所作成

これまでの調査結果から、「プラポリの作成・掲載手法」と「プラポリの内容」に対する考察として、まず前者に関しては、掲載場所として、第一に利用者がアプリをダウンロードする前に、利用者がアプリの利用者情報の取扱い状況を把握できるような仕組みを提供することが望ましい。具体的には、アプリマーケット（Google Play, App Store）のアプリ紹介ページにおいて、プラポリへのリンクの掲載を促進すべきである。特に日本は他国よりも掲載比率が低いため、今後の促進が特に重要と考えられる。また掲載場所に関しては、利用者がトップ画面より2、3タッチで閲覧できる場所に作成する等、利用者に分かり易い場所に掲載することが望ましい。

次にプラポリの内容に関しては、アプリプラポリを作成していない事業者は、最低限説明することが望ましい重要な項目を記載したポリシーを提示することが望ましい。具体的には、「誰が」、「何の情報を」、「どのような目的で取得し」、「どこに（外部に）送信するのか」の4項目を優先的に説明する概要版を作成すべきである。特にサービス全体のプラポリを掲載する事業者は、上記の項目に関しては、別途ポリシーを作成することが望ましいと考えられる。重要な項目について記載した上で、その他の項目についても長期的に記載を進め、アプリの透明性を高める必要がある。

また、本章の冒頭でも説明したが、本章の調査で対象としたアプリプラポリは、アプリにおける利用者情報の取扱いの透明性を高めることを目的としており、一方で企業のプラポリは、組織としての個人情報の取扱い体制・指針を示すことが目的である。アプリの透明性に加え、組織としての個人情報の取扱い体制・指針の検討・整備の両方が最終的に必要であると考えられる。

2.2 関係事業者における取組状況

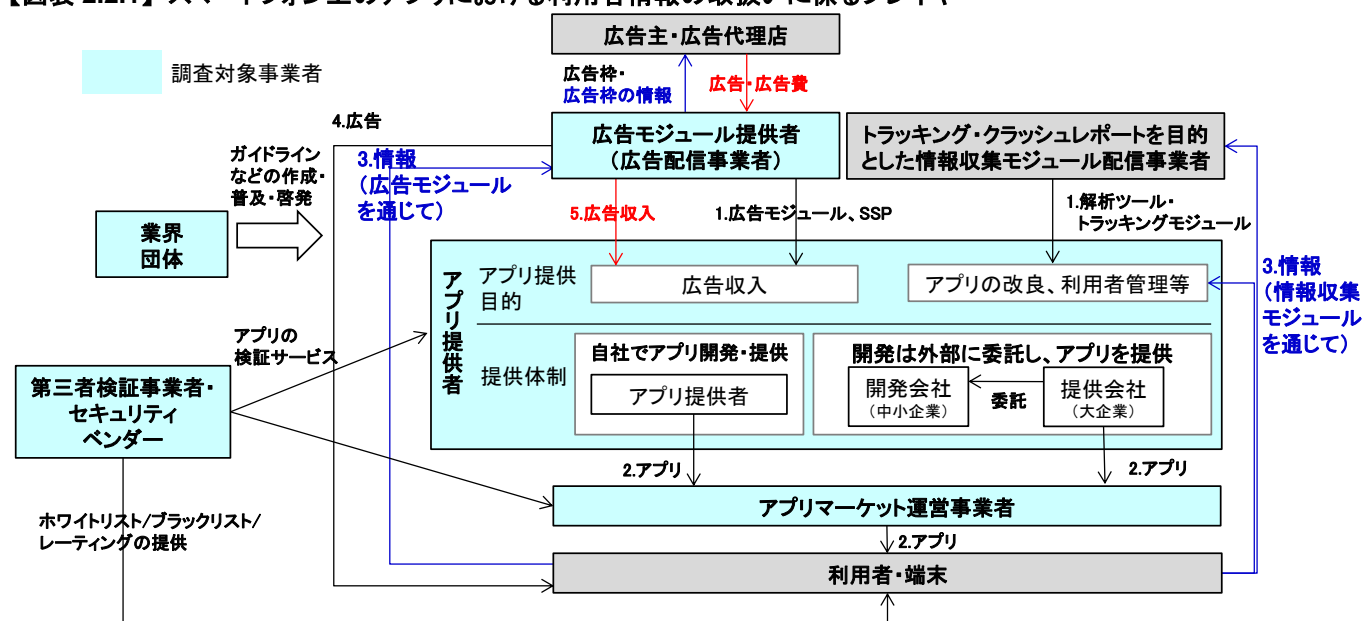
2.2.1 調査概要

スマートフォン上のアプリにおける利用者情報の取扱いに係るプレイヤー整理を行った上で、調査対象、取りまとめの観点について説明する。

(1) プレイヤー整理

スマートフォン上のアプリにおける利用者情報の取扱いに係るプレイヤーは図表 2.2.1 のように整理できる。

【図表 2.2.1】スマートフォン上のアプリにおける利用者情報の取扱いに係るプレイヤー



(出所) 日本総合研究所作成

アプリの開発・配信における主要なプレイヤーは「アプリ提供者」、「情報収集モジュール⁹提供者」、「アプリマーケット運営事業者」である。

「アプリ提供者」はアプリを開発し、有料又は無料で利用者に提供している。アプリ提供の目的は広告収入やアプリ・コンテンツ販売、企業の情報発信・マーケティングなど様々であるが、多くのアプリが広告収入を収入源として無料で提供されている。また、多くのアプリでは、アプリの品質・ユーザビリティの改善、収益向上を目的として利用者の利用状況の収集・分析が行われている。これらのアプリへの広告掲載や利用者の利用状況収集・分析の機能をアプリ提供者に提供しているのが、「情報収集モジュール提供者」である。

広告用の情報収集モジュール（広告モジュール）提供者（広告配信事業者）は、アプリ提供者からアプリの広告枠を獲得し、広告主・広告代理店に広告枠を販売している。広告モジュールは、アプリ提供者の手により、アプリに組み込まれて、利用者の手に届く。アプリが起動され、広告掲載のタイミングで、広

⁹情報収集モジュールは、「SPIII」では、「(情報収集モジュールは) アプリケーション本体以外のモジュールで、何らかの情報を外部送信するプログラムである。広告配信、アプリケーションの利用解析、クラッシュレポート等のための使われていることが多い」とされている。

告モジュールは広告配信事業者のサーバーと通信を行い、広告を取得し、利用者に配信する。広告配信の際に、広告の効果測定、不正の防止、効果的な広告配信（ターゲティング広告など）のために、広告モジュールは利用者情報を取得し、サーバーに送信している。

利用状況収集、分析の機能、プログラムであるトラッキング用の情報収集モジュール（トラッキングモジュール）も、アプリ提供者のアプリに組み込まれる形で利用される。トラッキングモジュールは定期的に事業者のサーバーに端末情報、アプリの動作状況などを送信し、事業者は送信された情報を統計化、可視化し、アプリ提供者に提供している。

スマートフォンではアプリマーケットを介さずにアプリを提供することが難しい状況にあるため、アプリ配信において「アプリマーケット運営事業者」の果たす役割は非常に大きい。一般的に「アプリマーケット運営事業者」は、自社のマーケットにアプリを公開する前あるいは公開後にアプリの審査やチェック等を行った上で、不適切だと判断したアプリの排除を行うなどの対応を行っている。そのため、主要なアプリマーケット運営事業者の運営・審査方針やその体制が、市場に流通するアプリの健全性に大きな影響を与える状況にある。

また、アプリの利用者情報に係る主要なプレイヤーとして、先ほど挙げた3つの主体以外に、「業界団体」、「第三者検証事業者」が挙げられる。

(2) 調査対象

本調査では、アプリの開発・配信、利用者情報に係る主要なプレイヤーである「アプリ提供者」、「広告モジュール提供者」（以下「広告配信事業者」とする。）、「アプリマーケット運営事業者」、「業界団体」、「第三者検証事業者」を調査対象とし、図表 2.2.2 に示す企業に対する公開情報リサーチ、ヒアリングの実施などを行った。

【図表 2.2.2】リサーチ対象企業

事業者・団体	ヒアリング実施企業
アプリ提供者	● 複数社にヒアリング（事業者名は非公開）
業界団体	● SPSC（スマートフォンの利用者情報等に関する連絡協議会） ¹⁰ ● JSSEC（一般社団法人日本スマートフォンセキュリティ協会） ● JIAA（一般社団法人インターネット広告推進協議会）
広告配信事業者	● 株式会社 AMoAd ● インモビ ジャパン株式会社 ● 株式会社ファンコミュニケーションズ ● 株式会社 VOYAGE GROUP ● 株式会社マイクロアド ● 株式会社 mediba
第三者検証主体	● アンドロイダー株式会社 ● 株式会社カスペルスキー ● トレンドマイクロ株式会社

¹⁰ <http://jssec.org/spsc/>

	<ul style="list-style-type: none"> ● ネットエージェント株式会社 ● 一般社団法人モバイル・コンテンツ・フォーラム (MCF) ● 一般財団法人日本情報経済社会推進協会 (JIPDEC)
アプリマーケット運営事業者	<ul style="list-style-type: none"> ● Apple ● グーグル株式会社 ● 株式会社 NTT ドコモ ● KDDI 株式会社

2.2.2 アプリ提供者

アプリ提供者においては、アプリが取得している利用者情報、アプリプラポリに関する取組状況、利用者・開発者に対する普及・啓蒙活動の状況に関する下記の項目について、ヒアリング調査を行った。

- アプリが取得している利用者情報
 - ◇ 各アプリが取得する利用者情報の管理体制、開発者との役割分担
 - ◇ アプリの利用者情報の取得に対する貴社内ルールの有無
 - ◇ 貴社アプリの情報収集モジュールの導入の現状
 - ◇ 貴社アプリの取得した利用者情報の第三者提供の現状
- アプリプラポリに関する取組
 - ◇ 作成における貴社内の体制、役割分担
 - ◇ 記載に関する貴社内のルールの有無
 - ◇ アプリプラポリ概要版の作成に対する貴社での認識
- 利用者・開発者に対する普及・啓蒙活動
 - ◇ アプリの利用者情報の取扱いに関する貴社の取組の有無

複数の大手アプリ提供者にヒアリングを行った結果は、図表 2.2.3 となる。結果として、今回ヒアリングを行った大手事業者に関しては、開発するアプリの利用者情報、アプリプラポリ共に、企画部門と法務部門が中心となって定めていた。ただし事業者によって検討対象となる情報のレベルが異なっており、個人情報のみを対象としているケースも存在した。

また、アプリプラポリの概要版に対しては、SPI で言及されていることは認識しているが、法的拘束力もなく、必要性に対する理解不足から、アプリ提供者としてはその作成に対して様子を見ているという側面もある。

アプリプラポリ普及のための課題として、アプリ提供者は実際にアプリプラポリを見ている利用者は少数だと考えており、アプリプラポリに対する利用者ニーズが十分に認識できていないことが挙げられた。アプリ提供者に対して、アプリプラポリの必要性に対する周知啓発を行うとともに、アプリプラポリの作成と利用者にとって見やすい掲載を促す取組を導入することが必要となる。

【図表 2.2.3】アプリ提供者の取組

大項目	小項目	概要
アプリの利用者情報の取扱いにおける取組	管理体制	<p>事業部がアプリの企画書を作成した段階で、法務側で審査し、プライバシーなどに関して問題がなければ、アプリ開発が行われる</p> <ul style="list-style-type: none"> ❖ 事業部の企画担当者が作成したアプリの企画書を、法務側でアプリの意図、プライバシーインパクト、世論の流れの視点でチェックし、問題がなければ、実際の開発が行われる。プライバシーバイデザインの考え方に則って、アプリの企画・開発を行っている。 ❖ 企業により利用者情報に関する対応のレベルが異なり、個人情報の取得においてのみ配慮する場合や、それ以外の利用者情報まで含めて対応を検討する場合がある。
	社内ルールの有無	<p>アプリ企画・開発に関するマニュアル・社内ルールが存在し、利用者情報・個人情報の取扱いなどについて記載している</p> <ul style="list-style-type: none"> ❖ 利用者情報・個人情報の取扱いに関して、社内用のマニュアルが存在する。 ❖ アプリでは UI が非常に重要になるため、同意の取り方において画一的なルールは決めにくい。
	情報収集モジュールの導入状況	<p>自社が出稿した広告の効果測定やユーザーのアクションを測定するために情報収集モジュールを導入しており、第三者に情報を送信する場合には、法務側の同意を得る必要がある</p>
プライバシーポリシーに関する取組	アプリプラポリの作成体制	<p>事業部側と、法務部が連携しながらアプリプラポリを作成している</p> <ul style="list-style-type: none"> ❖ アプリプラポリ作成は、事業部側が作成したアプリの取得情報・利用目的の申告書類をベースに作成している(法務側で、申告書類が本当に正しいかの技術検証は基本的にしていない)。 ❖ 法務部が入力用のフォーマットを作成した上で、事業部がそれに則った上でアプリプラポリを作成するケースも存在している。
	アプリプラポリ概要版	<p>概要版の作成は様子見の状況</p> <ul style="list-style-type: none"> ❖ 概要版の作成に関しては、今後の動向を見てからの対応として、様子見の状況である。 ❖ また、各文章が短い概要版では、逆に誤解を招くリスクを懸念しているアプリ提供者も存在している。
	アプリプラポリに関する課題	<p>消費者がアプリプラポリを読まないこと、アプリプラポリの掲載が逆に消費者の不安を煽ることになりやすいことは課題 アプリプラポリを準備することのメリットが不明</p> <ul style="list-style-type: none"> ❖ 利用者ニーズの観点から、アプリプラポリやアプリの検証が必要となっているならば、取組を促進したい。
利用者・開発者に対する普及・啓蒙活動	アプリプラポリ掲載以外の活動	<p>消費者に対しては、青少年向けの安心・安全活動を普及している</p> <ul style="list-style-type: none"> ❖ 消費者に対しては、青少年利用の観点での安心・安全について、アプリプラポリとは別に告知を行っている。

また、スマートフォンの利用者情報等に関する連絡協議会（SPSC）¹¹が、2013年12月から2014年2月にSPSC参加団体の加盟及び会員企業に対して実施したアプリプラポリに関するアンケートを基に全体的

¹¹ SPSCは2012年10月に、35以上の業界団体や企業・団体等が参加し、設置された。SPSCの活動目的は、様々な団体・事業者の緊密な情報交換及び相互の知見の集結により、スマートフォンのプライバシーに関する業界ガイドラインの策定を促進し、利用者情報等の適正な取扱いを通じて安心安全なスマートフォンの利用環境を整備することである。

な傾向を俯瞰する（図表 2.2.4）。

アプリ提供者のアプリプラポリ作成状況として、回答者の3割強がアプリ毎にアプリプラポリを作成している。利用者情報を外部に送信している事業者は、全体の7割弱であり、アプリプラポリを提供しているのはその中の約半数である（図表 2.2.5）。

【図表 2.2.4】アプリプラポリに関する事業者アンケート調査概要

- 調査対象
SPSC参加団体の加盟及び会員企業。
加盟団体より個別企業に依頼、サイト内のアンケートフォームを通じて回収。
- 実施期間
2013年12月20日（金）～2014年2月14日（金）
- 回収状況
28件

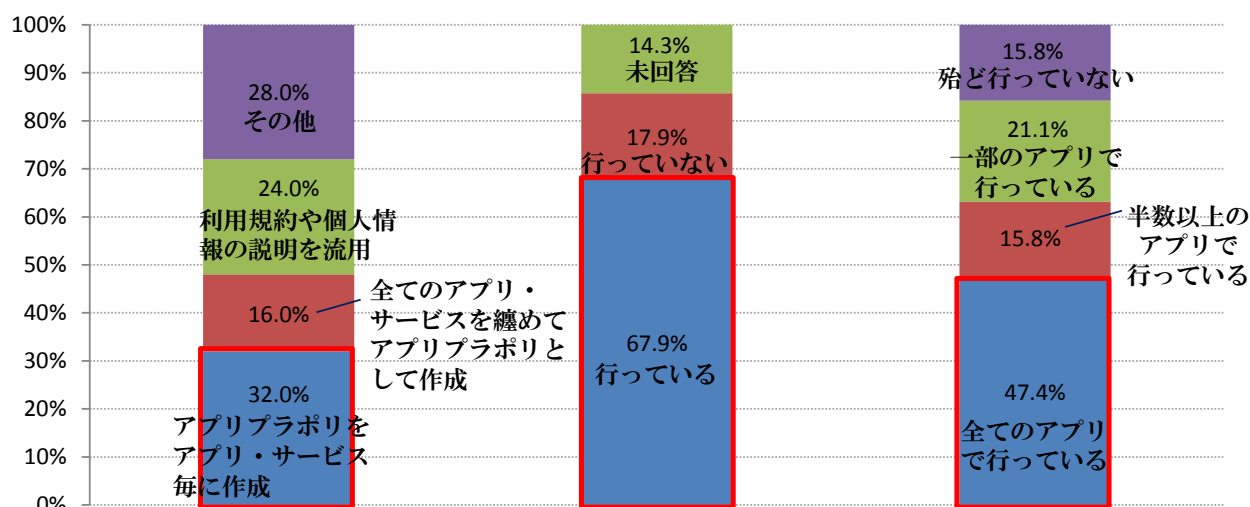
（出所）SPSC 資料を基に日本総合研究所作成

【図表 2.2.5】情報の送信状況およびアプリプラポリの掲載状況

アプリの利用規約や事業者の個人情報保護の説明とは独立して、アプリ・プラポリをアプリ個別に策定していますか（n=25）

利用者情報を取得し自社のサーバや外部に送信していますか（n=25）

自社のサーバや外部に利用者情報の送信をしている場合、自社アプリケーションでアプリ・プラポリを策定し、利用者に通知・公表を行っていますか（n=19）



（出所）SPSC 資料を基に日本総合研究所作成

2.2.3 業界団体

(1) 利用者情報取扱いに関する指針・ガイドラインの対応状況

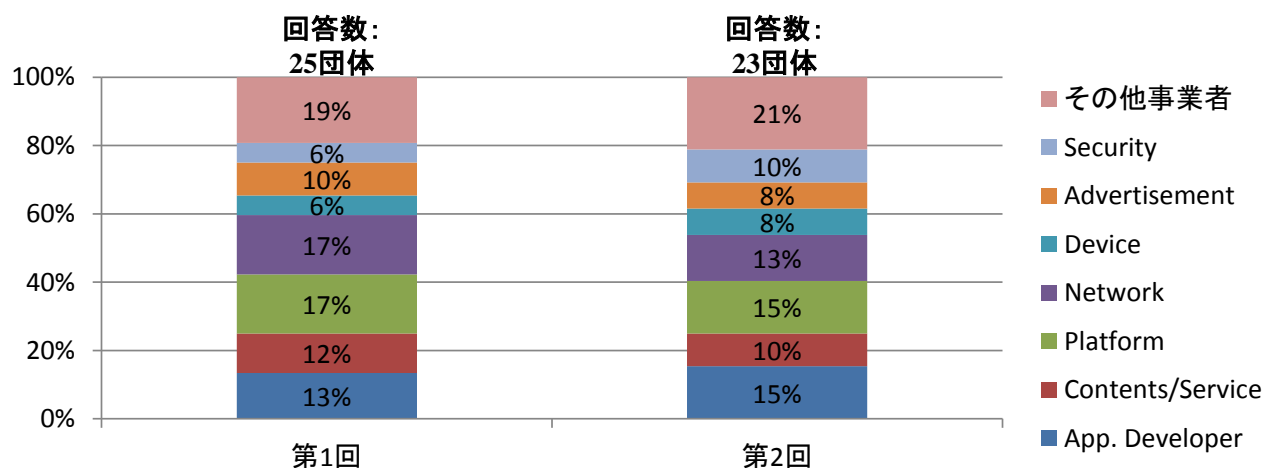
利用者情報取扱いに関する指針・ガイドラインの対応状況については、SPSCが、SPSCに加盟している業界団体に実施したアンケートを基に全体的な傾向を俯瞰する。同アンケートは、2012年（第1回）、2013年（第2回）に実施されており、各団体の利用者情報の取扱いに関する指針・ガイドラインの周知の状況を調査している。アンケートの概要および回答団体の活動・事業領域は図表 2.2.6、2.2.7のとおりである。

【図表 2.2.6】アンケートの概要および回答団体の活動・事業領域

項目	内容
調査対象	スマートフォンの利用者情報等に関する連絡協議会参加団体、企業
調査内容	業界団体から会員企業への利用者情報取扱いに関する指針・ガイドライン （「SPI」など）の周知の状況
実施期間	第1回:2012年10月4日～2012年10月24日 第2回:2013年11月29日～2013年12月18日

(出所)SPSC 資料を基に日本総合研究所作成

【図表 2.2.7】回答団体の活動・事業領域



※業界団体の会員構成によって、複数回答を行っているケースも存在

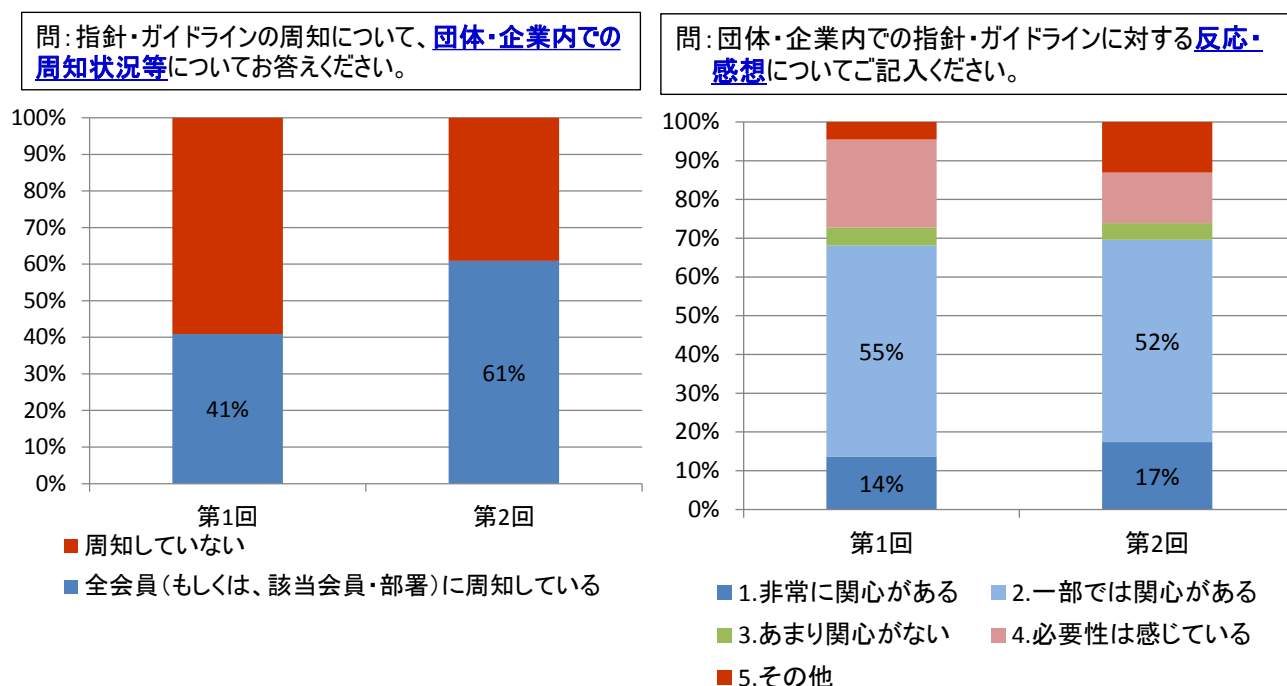
(出所)SPSC 資料を基に日本総合研究所作成

「指針・ガイドラインの団体・企業内での会員への周知状況」は、第2回のアンケートでは全体の61%の団体が「全会員（もしくは該当会員・部署）に周知している」という結果になっており、第1回アンケートと比較して約50%増となっている（図表 2.2.8）。

「団体・企業内での指針・ガイドラインに対する反応・感想」では、「非常に興味がある」、「一部では興味がある」と回答している割合は第1回、第2回共に69%であり、横ばいで推移している（図表 2.2.8）。

第2回アンケートにおける「会員企業等のアプリプラポリに対する対応状況」では、全体の5割弱の団体が、会員企業が「具体的な対応を既に開始」、「対応の検討開始段階」のステータスにあると認識しており、アプリプラポリの作成の必要性が一定程度認知・理解されてきているといえる（図表 2.2.9）。

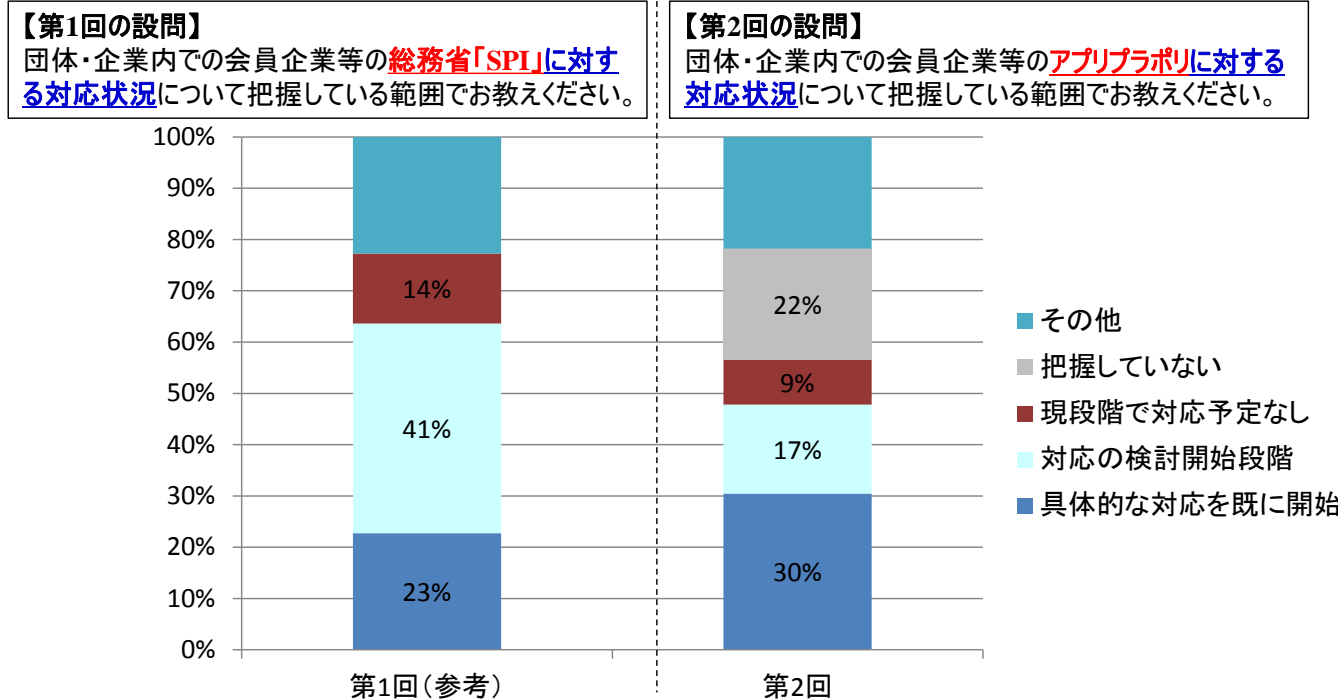
【図表 2.2.8】 指針・ガイドラインの周知の団体・企業内での会員への周知状況および
団体・企業内での指針・ガイドラインに対する反応・感想



(注)* 「周知していない」: 第1回では「問合せに対して周知している」、「あまり周知できていない」「その他」という回答を統合して集計、第2回では「今後周知を予定」、「周知する予定なし」、「その他」という回答を統合して集計。

(出所) SPSC 資料を基に日本総合研究所作成

【図表 2.2.9】 会員企業等のアプリケーション・プライバシーポリシーに対する対応状況



(注)* 「具体的な対応を既に開始」: 第2回における「対象企業では既に APP を作成・周知している」、「一部の企業で APP を作成・周知しており、今後拡がる予定」の回答を統合して集計。

(出所) SPSC 資料を基に日本総合研究所作成

(2) 各団体の利用者情報取扱いに関する取組

1) 一般社団法人日本スマートフォンセキュリティ協会(JSSEC)における取組

JSSECの技術部会は5つのワーキンググループ(WG)で構成されており、そのうちの1つにスマートフォン利用の安全・安心への寄与を目的とした「アプリケーションWG」が存在する。「アプリケーションWG」には、3つのグループ(アプリケーション・プライバシーポリシー作成グループ、情報収集モジュール調査グループ、アプリケーション解析グループ)が存在し、それぞれがアプリプラポリの考察、情報収集モジュールの調査、アプリ解析手法の考察を担当している(図表2.2.10)。

【図表 2.2.10】アプリケーションWGの各グループの研究内容

グループ名	調査・研究内容
アプリケーション・プライバシーポリシー作成	アプリプラポリの実際に開示が求められるケース、開示・承諾の手順、解りやすいフォームの事例などを、技術視点から考察
情報収集モジュール調査	アプリプラポリの作成やアプリの第三者検証を行う際に情報収集モジュールに関する知識が必要になるため、情報収集モジュールの事前調査を実施
アプリケーション解析	アプリ解析技術の普及、解析者に求められる技術レベルや精度について考察

(出所) JSSEC 各種公開資料を基に日本総合研究所作成

2014年2月6日にJSSECが主催した「情報セキュリティシンポジウム」では、アプリケーションWGの3つのグループの取組内容が発表され、それらの発表資料はJSSECウェブサイトで開催されている¹²。「アプリケーション・プライバシーポリシー作成グループ」の発表内容では、アプリプラポリの作成が必要なケース・不要なケースの分類、各ケースにおけるユーザーへの掲示方法について、具体例を示している(図表2.2.11)。

【図表 2.2.11】アプリプラポリの作成・掲示手順の例

アプリ実践	該当情報(例)	作成の要否	対応	アプリにおける対応	アプリマーケット掲載時の対応
1) 利用者情報の送信を行わない場合。	---	不要	①	情報送信が無い旨、入力操作によって情報を送る旨などの説明をアプリの説明書や利用規約に記載する。	情報送信が無い旨、入力操作によって情報を送る旨などの説明を、「アプリの説明」欄に掲載する。
2) 利用者による明示的な操作によって利用者情報を送信する場合(ログイン時のID/PWDの入力やメール送信時の宛先入力等)。	---				
3) 単体では利用者識別性を有さない利用者情報を送信する場合。 ※但し、サーバ側に、これら複数の情報からアクセス元を識別する処理が組み込まれている場合は、包括同意の取得(対応③)が必要。	ブラウザエージェント OS名 バージョン情報など				
利用者による取り換えが容易な利用者情報のみを送信する場合。	cookie UUIDなど +これらで管理される情報	必要	②	ヘルプメニューを入口とする、アプリ・プライバシーポリシーの参照機能を設ける。	アプリプライバシーポリシーへのリンクを、「アプリプライバシーポリシーURL」欄に掲載する。
利用者による取り換えが困難な利用者情報を送信する場合。	IMEI IMSI ICCID MACアドレス OSが生成するIDなど +これらで管理される情報				
慎重な取扱いが求められる利用者情報を送信する場合。	位置情報 アドレス帳 電話番号 メールアドレスなど				
<p>プライバシー不安は、行動・属性などの利用者情報の性質と、これを管理するIDの性質に依存する。 ⇒ cookie、IMEI、電話番号などの識別子(ID)と、そのIDでどのような利用者情報が管理されるのか説明すること。</p>					

(出所) JSSEC「スマホアプリのプライバシーポリシー作成・開示についての考察」(2014年2月)から抜粋

¹² <http://www.jssec.org/event/20140206.html>

2) 一般社団法人インターネット広告推進協議会(JIAA)における取組

インターネット広告（モバイル広告含む）ビジネスに関わる企業 156 社が加盟する JIAA は、主な活動の 1 つとして、消費者保護の観点に基づいた広告掲載に関わる基準についての調査・研究、協議、ガイドラインの策定及び啓発活動を行っている。その活動の一環として、JIAA はインターネット広告において取得・利用されるユーザー情報の取扱いに関する事業者向けの指針として「プライバシーポリシー作成のためのガイドライン」を 2004 年 11 月に、「行動ターゲティング広告ガイドライン」を 2009 年に 3 月に策定¹³した。JIAA は昨今のスマートフォン広告の普及に合わせて、2 つのガイドラインの改定の検討を 2012 年 9 月に開始し、2014 年 3 月に改訂版を公開した¹⁴。

「プライバシーポリシー作成のためのガイドライン」の最も注目すべき改定内容は、ガイドラインの対象とする情報の範囲を、主にユーザーが自ら会員各社に登録を行った「登録情報」から、会員各社が取得し得る「個人関連情報」に変更したことである。「個人関連情報」とは「個人情報¹⁵」および「インフォマティブデータ¹⁶」のうち統計情報等を除いた部分である。インフォマティブデータの具体例として、スマートフォンの契約者・端末固有 ID、行動履歴情報などが含まれる。「プライバシーポリシー作成のためのガイドライン」の主な改定内容は図表 2.2.12 のとおりである。

【図表 2.2.12】「プライバシーポリシー作成のためのガイドライン」の主な改定内容

項目	概要
ガイドラインの対象とする情報の範囲の変更	<ul style="list-style-type: none"> ● ガイドラインの対象とする情報の範囲を<u>会員各社が取得し得る「個人関連情報」</u>に変更。 ● 「個人関連情報」とは「<u>個人情報</u>」および「<u>インフォマティブデータ（スマートフォンの契約者・端末固有 ID、行動履歴情報などが含まれる）</u>」のうち<u>統計情報等を除いた部分</u>。
最も注目すべき変更点	
プライバシーポリシーの構成	● 個人情報保護法に準じてプラポリに含まれていることが望ましい事項を追加し、「個人関連情報」を対象とすべきものはその旨を規定した。
利用目的の明示	● 取得する個人関連情報について、 <u>それぞれの利用目的を可能な限り明確に特定して、プラポリ上にて分かりやすい形で明示するよう規定を改めた。</u>
スマートフォンでの情報の取扱い	● SPI を踏まえ、アプリ向けの広告配信における情報の取扱いに関して、プラポリをアプリからのリンクなどにより消費者が容易に参照できる場所に掲示するよう努めることを規定。

¹³ 「行動ターゲティング広告ガイドライン」は 2010 年 6 月に総務省の配慮原則を踏まえて改定されている。

¹⁴ 「プライバシーポリシー作成のためのガイドライン」：http://www.jiaa.org/download/JIAA_PPguideline2014_02.pdf

「行動ターゲティング広告ガイドライン」：http://www.jiaa.org/download/JIAA_BTAguideline2014_02.pdf

¹⁵ 個人情報とは個人情報保護法に定める個人情報、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）。

¹⁶ インフォマティブデータとは、郵便番号、メールアドレス、性別、職業、趣味などの個人に関する情報、顧客番号、クッキー情報、IP アドレス、契約者・端末固有 ID などの識別子情報および位置情報、閲覧履歴、購買履歴などのインターネットの利用にかかるログ情報など、個人を特定することができないものの、プライバシー上の懸念が生じうる情報ならびにこれらの情報が集積化、統計化された情報であつて、特定の個人と結びつきえない形で使用される情報の総称。

項目	概要
	● 「契約者・端末固有 ID」の取扱いについてプライバシー保護のために考慮すべき要点を提示
消費者への配慮	● <u>青少年や高齢者にも分かりやすい形で適切な説明</u> を行うことに留意すべきとした。
個人関連情報の 第三者提供	● 「オプトアウト」による第三者提供（個人情報保護法第 23 条第 2 項）について「個人情報」だけでなく「 <u>個人関連情報</u> 」にも適用するものとした。

(出所) JIAA ウェブページ、JIAA「プライバシーポリシー作成のためのガイドライン」(2014 年 2 月)を基に日本総合研究所作成

「行動ターゲティング広告ガイドライン」の主な改定内容は、図表 2.2.13 のとおりである。

【図表 2.2.13】「行動ターゲティング広告ガイドライン」の主な改定内容

項目	概要
行動履歴情報を含む個人関連情報の取扱い	● 行動ターゲティング広告に関して個人情報を取り扱う場合には「個人情報保護法」に従うものとし、 <u>行動履歴情報を含む個人関連情報の取扱いについては「プライバシーポリシー作成のためのガイドライン」に従うものとする</u> ことを前提として、規定を整理した。
事業領域の定義と適用範囲	● <u>各行動ターゲティングの事業領域の定義とその事業領域ごとに遵守すべき規定</u> を整理した。 ● 各事業領域のうち <u>複数の事業活動を行っている場合には、該当するすべての規定が適用される</u> ものとした。
インフォメーションアイコン	● 「 <u>インフォメーションアイコン</u> 」(広告内や周辺に表示されたアイコンから情報の取扱いに関する説明やオプトアウトへの導線を設けるもの)の設置に JIAA として取り組むことを明記。

(出所) JIAA ウェブページ、JIAA「行動ターゲティング広告ガイドライン」(2014 年 2 月)を基に日本総合研究所作成

2.2.4 第三者検証事業者

スマートフォンアプリにおける第三者検証では、アプリ自体を検証するアプリ検証と、アプリ提供者の開発体制・利用者情報の取扱いの方針などを検証するアプリ提供者の検証が存在する。

(1) アプリケーションの検証

1) 第三者検証機関のリスト化

アプリ検証の第三者検証機関の調査では、事業者へのヒアリングおよび公開情報を基に、事業者の検証体制を図表 2.2.14 のフォーマットで整理し、アプリ検証の第三者検証機関のリスト化を行った (appendix 参照)。今回の調査では、アプリ提供者から有料でアプリ検証を請け負い、アプリ提供者にのみ検証結果を報告書などの形式で提供する検証サービスは対象外としている。

調査項目の中から、対象 OS、検証体制 (クローリング型 (能動型)¹⁷、申請型 (受動型)¹⁸)、検査手法・

¹⁷ クローリング型 (能動型) とは、第三者検証事業者が自らアプリマーケットなどからアプリをダウンロードし、能動的に検証を行う体制。スマートフォン向けのセキュリティソフトを提供しているセキュリティベンダーの中には、アプリマーケット上のアプリだけでなく、自社のセキュリティソフトがインストールされた端末がアクセス・インストールしたアプリも検証対象にしている場合が存在する。

項目、検証結果の表示方法について、図表 2.2.15 にまとめた。

検証体制では、大部分の第三者検証がクローリング型であり、申請型の第三者検証はほとんど行われていない。技術的なアプリ解析では、全ての事業者が静的解析、動的解析を実施している。ただし、静的解析・動的解析を行う対象・自動化の状況などは各社により異なっている。アプリプラポリ審査をすべてのアプリに対して実施している第三者検証事業者は存在しない（必要に応じて実施している事業者は存在）。その理由として、アプリプラポリは定型化されておらず、アプリ提供者ごとに記載場所・内容・順番・使用する用語が異なるため、機械で自動的に検証することが難しく、すべてのアプリに対して実施するためにはコストがかかるためと推測される。

ただし、アプリマーケット運営事業者である KDDI は、アプリ提供者からの送信情報に関する申請に基づき、アプリプラポリを自動生成する仕組みを用意し、その上で、au スマートパス向けのアプリすべてに対して、手動によるアプリプラポリの第三者検証を実施・運用している。また、アプリプラポリを掲載するためのホスティングサーバーを KDDI が提供することで、アプリ提供者の負担を減らしている。

¹⁸ 申請型とは、アプリ提供者が第三者検証事業者にアプリの検証を申請し、第三者検証事業者は申請されたアプリを検証する体制。

【図表 2.2.14】アプリ検証の第三者検証機関の取りまとめフォーマット

事業者名: _____

商品・サービス名			
事業者URL			
対象OS	<input type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> その他 ()		
対象言語	<input type="checkbox"/> 日本語 <input type="checkbox"/> 英語 <input type="checkbox"/> 中国語 <input type="checkbox"/> 韓国語 <input type="checkbox"/> その他 ()		
検証したアプリケーションの数	件 ()	種類 ()	利用者数 (選択してください)
検証を行うアプリケーションの取得方法・頻度			
検証結果の表示方法			
検証基準			
① アプリケーションのプライバシーポリシー(APP)等の作成・公表の有無や掲載場所について検証している。 <ul style="list-style-type: none"> ● APPを作成しているか ● APPを利用者が容易に参照可能な場所に掲載しているか、アプリケーション内で容易に参照可能であるか 			<input checked="" type="checkbox"/> (必要に応じて)
② アプリケーションのプライバシーポリシーの記載事項・内容について検証している。 <ul style="list-style-type: none"> ● スマートフォンプライバシーイニシアティブ推奨の8つの事項(※)について必要な内容を記載しているか (※)①アプリ提供者の氏名・名称、②取得情報、③取得方法、④利用目的、⑤通知・公表、同意取得、利用者関与、⑥外部送信・第三者提供・情報収集モジュールの有無、⑦問合せ窓口、⑧プライバシーポリシー変更手続 ● 情報収集モジュールの名称、提供者等 			<input checked="" type="checkbox"/> (必要に応じて)
③ 同意取得に関する事項について検証している。 <ul style="list-style-type: none"> ● プライバシー性の高い情報を取得するアプリケーションの場合、個別に同意を取得しているか ● 第三者提供を行う場合、あらかじめ本人の同意取得をしているか 			<input checked="" type="checkbox"/> (必要に応じて)
④ 外部送信される利用者情報の有無等について技術的(動的解析・静的解析)に検証している。 <ul style="list-style-type: none"> ● アプリケーションにより外部送信される利用者情報は何か ● 外部送信される利用者情報の送信先はどこか 			<input checked="" type="checkbox"/> (必要に応じて)
⑤ 技術検証結果とアプリケーションのプライバシーポリシーの記載内容との整合性について検証している。 <ul style="list-style-type: none"> ● APPに記載される利用者情報の項目と、実際に外部送信される利用者情報の項目が合致しているか ● 外部送信される利用者情報の利用目的が明示されているか ● 情報収集モジュールの名称、提供者、送信情報等が合致しているか 			<input checked="" type="checkbox"/> (必要に応じて)

(出所) 日本総合研究所作成

【図表 2.2.15】各社のアプリ検証一覧

事業者名 (サービス名)	対象 OS	検査体制		技術的なアプリ 検証【1】		アプリ プラポリ 検証 【2】	【1】と 【2】の突 合	表示方法		
		申請	クロー リング	静的 解析	動的 解析			ブラック リスト	ホワイト リスト	レーティ ング
アンドロイダー(株) (アンドロイダー)	An	○	×	○	△ (必要に 応じて)	△ (必要に 応じて)	△ (必要に 応じて)	×	○	×
(株)カスペルスキー (プライバシーアドバイザー[開発中])	An	○	○	○	○	×	×	×	○ (利用者による定義)	○
トレンドマイクロ(株) (MAR)	An, Bl	○	○	○	○	△ (必要に 応じて)	△ (必要に 応じて)	×	×	○
ネットエージェント(株) (secroid)	An	×	○	○	○	×	×	×	×	○
KDDI(株) (au スマートパス)※1	An	○	×	○	○	○	○	×	○	×

アプリプラポリ検証の自動化が難しいために、
同検証には一定程度のコストを要する

※1: KDDI は第三者検証事業者ではないが、参考情報として記載。KDDI のアプリマーケットでは、アプリ提供者から送信情報に関する申請に基づき、アプリプラポリを自動生成する仕組みを用意している。その上で、au スマートパス向けアプリの全てに対して、一定のコストを要する手動審査によるプラポリの第三者検証を実施している。また、au Market の au スマートパス以外のアプリに対してはコスト抑制の自動審査による検証を実施。また、アプリプラポリを掲載するためのホスティングサーバーを KDDI が提供しており、ホスティングされたアプリプラポリはアプリからリンクすること推奨している。

※2: An : Android Bl: BlackBerry

(出所) 各種公開情報およびヒアリング内容を基に日本総合研究所作成

2) 第三者検証事業者の特徴的な取組

ネットエージェント株式会社は Android アプリが危険性を持っているかについて客観的に判定するエンジン「secroid」¹⁹を開発・提供している。「secroid」での検証においてアプリの危険性をより正確にかつ詳細に把握するために、情報収集モジュールのデータベースを作成し、活用している。情報収集モジュールデータベースには、2013 年 4 月時点で 750 種類以上に及ぶモジュールの内容認識と送信先が保存されている。ネットエージェントが構築している情報収集モジュールデータベースを用いれば、アプリ解析において、アプリに含まれている情報収集モジュールの解析にかかる時間の大幅な削減につながると考えられる。

アンドロイダー株式会社は、アプリ提供者から申請されたアプリを検証し、パスしたアプリ（公認アプリ）を掲載したアプリ紹介サイト「アンドロイダー²⁰」を提供している。しかし、公認アプリの審査において、アプリに組み込まれた情報収集モジュールの検証が困難という課題に直面し、現在、情報収集モジュールの公認制度化を検討している。同社は公認した情報収集モジュールを「公認広告モジュール」として、アンドロイダーの審査をパスしたアプリのデベロッパー向けに提示することを想定している。また、情報収集モジュールの審査項目としては、図表 2.2.16 のように用途に必要なパーミッションを正当に利用していること、プライバシーポリシーの提出だけでなく、公認デベロッパーの収益的支援要素があることを挙げている。公認デベロッパーの収益的支援要素があることを条件に含めることでデベロッパーが公認

¹⁹ <http://secroid.jp/>

²⁰ <https://androider.jp/>

広告モジュールを利用するインセンティブが安全性だけでなく収益面においても発生する仕組みになっている。つまり、アンドロイダーが検討している情報収集モジュールの公認制度化は、広告事業者、デベロッパー、端末利用者それぞれがメリットを享受できるようになっている（図表 2.2.17）。

また、アンドロイダーは公認アプリのアプリ提供者（公認デベロッパー）向けにセミナーを実施しており、その中で、スマートフォンにおける利用者情報に関する課題、SPI、アプリプラポリの作成例、KDDI 研究所が提供しているアプリプラポリ作成支援ツールなどの紹介を行っている。

【図表 2.2.16】情報収集モジュールの審査項目(案)

- ◆公認アプリの審査基準を満たしていること
 - ・ウイルス、マルウェア等を含んでいないこと
 - ・公序良俗に反していないこと
 - ・**アプリ用途に必要なパーミッションを正当に利用していること**
- ◆プライバシーポリシーの提出（取得パーミッションの提示）
 - ・どんな情報、なぜ、第三者提供の有無などSPI 8項目に準拠

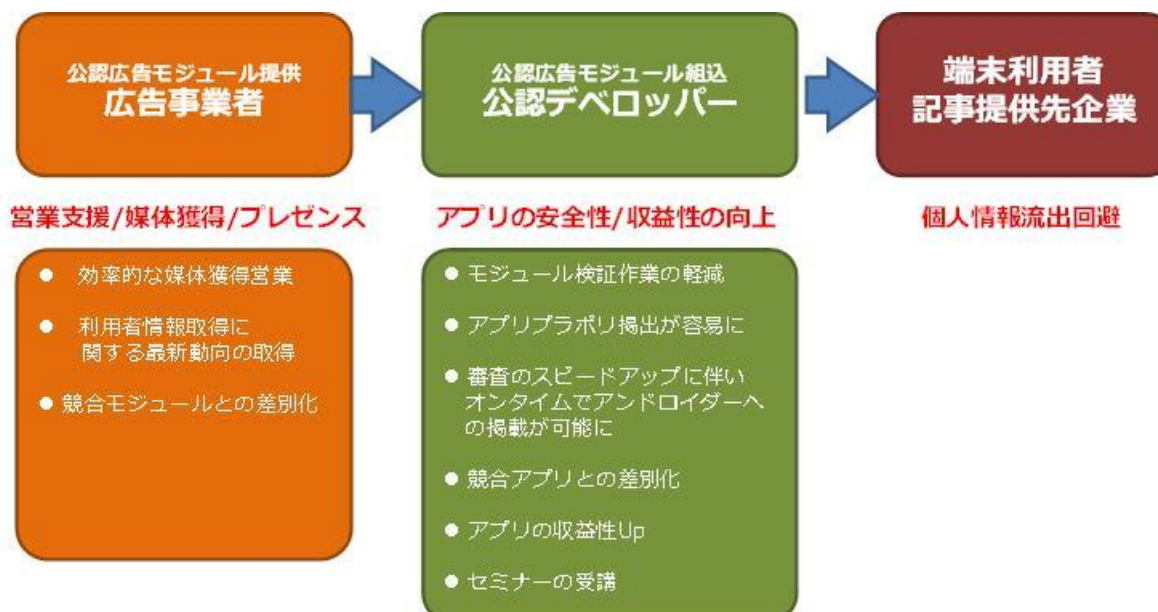


- ◆公認デベロッパーの収益的な支援要素があること
（広告メニューの検討/セミナーの開催など）

利用者情報取得の透明性確保と収益メリットを提供することで
アプリデベロッパーへの「公認広告モジュール」組込を推進、
プライバシーに配慮したアプリ普及を推進

(出所)アンドロイダー資料から抜粋

【図表 2.2.17】情報収集モジュールの公認化制度のメリット



(出所)アンドロイダー資料から抜粋

(2) アプリケーション提供者の検証取組

アプリ提供者の検証取組として、株式会社アイ・エス・レーティング（スマートフォンアプリケーション格付け準備委員会）、一般財団法人日本情報経済社会推進協会（JIPDEC）・一般社団法人モバイル・コンテンツ・フォーラム（MCF）の2つが実施しているものが存在する。

1) アイ・エス・レーティング(スマートフォンアプリケーション格付け準備委員会)の取組

2012年8月にスマートフォンアプリが取得するユーザー情報の取扱いなどについて、一定の信頼性が確保されているかどうかの証明や格付けを実施することを検討している「スマートフォンアプリケーション格付け準備委員会」を立ち上げ、同年11月からアプリ提供事業者に対する第三者証明書の発行を開始した。アイ・エス・レーティングは同委員会事務局を務めており、第三者証明書の発行を担当している。第三者証明書の発行の標準工程は図表 2.2.18 のとおりであり、主にアプリ提供者の利用者情報に関するマネジメント・プロセスを客観的に評価するものになっている。また、同委員会では、スマートフォンアプリの格付サービスの実施も予定しており、同格付ではアプリの安全性評価を含むことが検討されている。

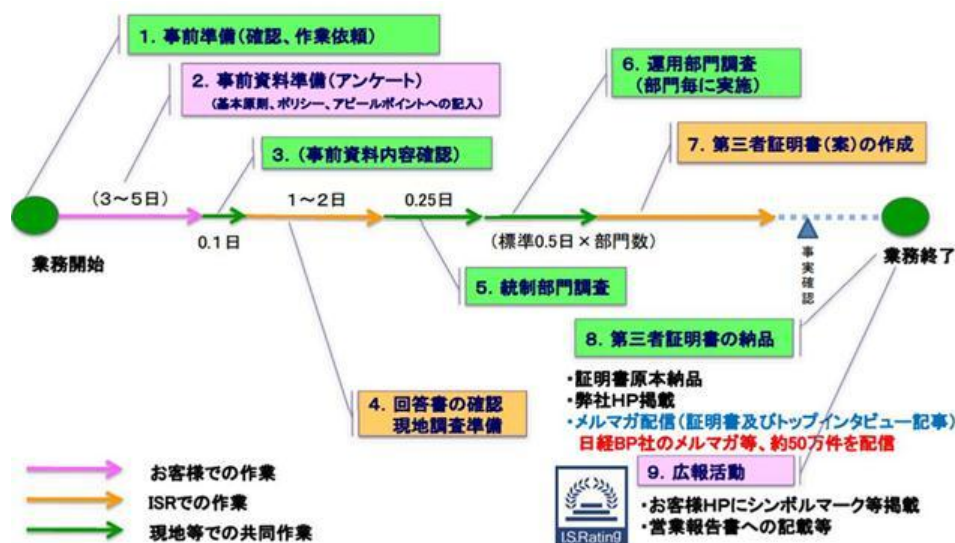
2) JIPDEC・MCF の取組

プライバシーマーク指定審査機関である MCF は 2014 年 1 月に「モバイルコンテンツ関連事業者のための個人情報保護ガイドライン 第 2 版」を公表し、プライバシーマーク付与機関である JIPDEC はプライバシーマーク付与を受けようとするアプリ提供者、情報収集モジュール提供者に対して、同ガイドラインに従って利用者情報を取り扱うことを求めている。同ガイドラインにおけるスマートフォンアプリの利用者情報の取扱いに関する項目は大きく 2 つある。

1 つ目は、契約者・端末固有 ID、位置情報、通話履歴、アプリ利用履歴など特定の個人が識別できる情報ではないが、特定の個人が識別できる可能性があるプライバシー情報を「個人情報と同等に扱う利用者情報」と定義していることである。その上で、「個人情報と同等に扱う利用者情報」については、個人情報と同等に取扱い、管理台帳に「アプリケーションの利用者情報」として 1 つにまとめて登録して、リスク分析を実施することを求めている。

2 つ目は、アプリプラポリについての記載であり、アプリプラポリと個人情報保護方針の目的の違い、アプリプラポリの掲載場所・掲載方法などについて言及している。

【図表 2.2.18】 第三者証明書発行の標準工程



(出所)アイ・エス・レーティング「スマートフォン・アプリケーション格付け準備状況」(2013年1月)

2.2.5 広告配信事業者

広告配信事業者の取組の調査では、次の項目についてヒアリングを行った。

【ヒアリング項目】

- 現状の広告モジュールにおける取組
 - ◇ 広告モジュールの取得情報
 - ◇ 情報取得の目的
 - ◇ 利用者識別・ターゲティング広告の手法
 - ◇ プライバシーポリシーの作成状況
- アプリ提供者・利用者に対する取組
 - ◇ アプリ提供者への取組
 - ◇ 利用者への取組
 - ◇ 現状の取組の課題
- 第三者検証への要望
- 今後の動向・課題
 - ◇ SSP・メディエーションを利用した際の利用者情報の取扱いに対する影響

(1) 広告配信事業者の現状の取組

広告配信事業者の「広告モジュールにおける取組」について、図表 2.2.19 のように取りまとめた。

【図表 2.2.19】 広告モジュールにおける取組

項目	概要
広告モジュールの取得情報	<p>主要な国内事業者の最新の広告モジュールは端末固有 ID を取得していない、一方、多くの海外事業者のモジュールは端末固有 ID を取得している</p> <p>❖ 主要な国内事業者の最新の広告モジュールは、AndroidID、端末 ID などの端末固有 ID は取得していない。</p> <p>◇ 国内事業者の広告モジュールが取得する情報は、IDFA、AdID、各端末に割り当てた独自 ID、UserAgent 情報などである。</p> <p>❖ 多くの海外事業者の広告モジュールは、AndroidID や端末 ID を取得している。</p>
情報取得の目的	<p>一番の目的は利用者を識別し、正確な広告の効果測定を行うため</p> <p>❖ 情報取得の一番の目的は、広告主への広告費の請求・アプリ提供者への報酬の確定のために、利用者を識別し、広告の閲覧数・クリック数などの広告効果を正確に測定することである。</p> <p>❖ ただし、取得した情報を利用したターゲティング広告も行われている。</p>
利用者識別手法	<p>端末固有 ID を利用しない識別方法も存在する。最近では、端末固有 ID を利用しない手法を採用するモジュールが増加している</p> <p>❖ ユーザー識別の方法は、①端末固有 ID、②OS 事業者が提供する広告 ID、③広告配信事業者による独自 ID(端末に保存される)、④デバイスフィンガープリンティングの 4 つの手法が存在するが、主要な国内事業者は端末固有 ID は利用していない(図表 2.2.20、2.2.21)。</p>
ターゲティング広告の手法	<p>利用者の属性情報などを利用したターゲティング広告は一定程度利用されている</p> <p>❖ アプリをインストールしていないユーザーに対するリターゲティング広告やグループ会社のユーザーの属性情報を用いたターゲティング広告は既に一定程度利用されている(アプリ広告におけるターゲティング広告の普及率は全体の 10~30%程度ではないか)。</p> <p>❖ 日本では位置情報を利用した広告はほぼ利用されていないが、将来的に普及する可能性が存在。</p>
プライバシーポリシーの作成状況	<p>広告モジュールのプライバシーポリシーが提供されていないケースも存在</p> <p>❖ 端末固有 ID を取得していないが、独自 ID や AdID などにより利用者識別・ターゲティングは行っている広告モジュールにおいて、プライバシーポリシーが存在しないケースも見られる。</p>

(出所) 広告配信事業者へのヒアリング内容(2014 年 2 月~3 月)を基に日本総合研究所作成

「広告モジュールの取得情報」では、主要な国内事業者が提供する最新のモジュールは端末固有 ID を取得していないが、海外事業者が提供するモジュールの多くは端末固有 ID を取得しており、国内と海外で大きな違いがある。詳細はアプリマーケット運営事業者の取組の小節（2.2.6）で述べるが、2014 年の 8 月から Google が広告目的で使用する端末 ID として広告用 ID (AdID) を使用する必要があるとしており、今後は主要な海外事業者も Google の意向に従うものと考えられる。そのため、端末固有 ID の取得の有無において、海外と日本の差は無くなると予想される。

「情報取得の目的」において、一番の目的は広告主への広告費の請求・アプリ提供者への報酬の確定のために、利用者を識別し、広告の閲覧数・クリック数などの広告効果を正確に測定することである。一部の事業者では取得した情報を利用してターゲティング広告を行っているが、アプリ広告においてはターゲティング広告はまだ一般的ではないようである。ヒアリングの中では、アプリ広告においてターゲティング広告はそれほど普及しておらず、全体の 10~30% 程度ではないかという意見も出た。また、アプリ広告では利用者属性によるターゲティング広告が難しいため、自社のターゲティング技術が活かせず、アプリ広告から撤退したという事業者も存在している。

「ユーザー識別手法」では、①端末固有 ID、②OS 事業者が提供する広告用 ID、③広告配信事業者による独自 ID（独自 ID は端末のローカルストレージ・SD カードに保存）、④デバイスフィンガープリンティングの 4 つの手法が存在する。デバイスフィンガープリンティング技術の登場や Android、iOS における広告用 ID の導入により、端末固有 ID を利用しない手法の採用が増えつつある。ユーザー識別手法の特徴、仕組みは図表 2.2.20、2.2.21 のとおりである。

ターゲティング広告の種類としては、アプリをインストールしていないユーザーに対するリターゲティング広告やグループ会社の利用者の属性情報を用いたターゲティング広告などが存在する。アプリ広告の主要な広告主はアプリ提供者であり、自社アプリの利用を促す広告が多く出稿されている。そのため、アプリをインストールしていないユーザーにインストールを促したり、アプリをインストールしているが利用が滞っているユーザーに利用を促したりすることが可能なリターゲティング広告が人気のようである。位置情報を利用した広告はまだ普及していないが、インターネット広告を活用した実店舗への誘導など O2O のニーズが高まれば、将来的に普及する可能性は十分に存在している。

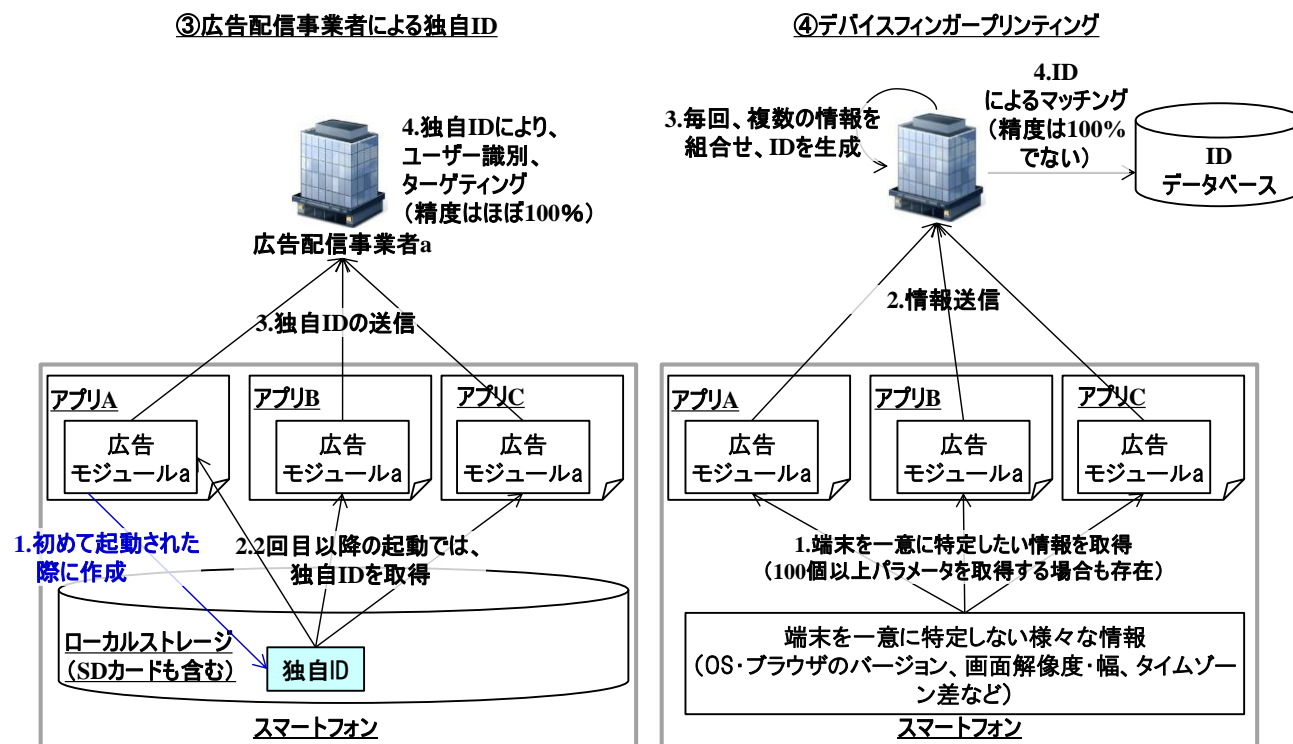
「プライバシーポリシーの作成状況」では、広告モジュールごとのプライバシーポリシーは提供されておらず、企業の個人情報保護方針をモジュールのプライバシーポリシーとして提示しているケースも存在している。このような広告モジュールの多くは、端末固有 ID を取得しない手法でユーザー識別を行っている。端末固有 ID を取得しない場合でも、何らかの利用者情報を取得し、利用者を識別しているならば、プライバシーポリシーを作成すべきと考えられるところ、こうした事業者に対する普及啓発も引き続き行っていくべきである。

【図表 2.2.20】ユーザー識別の手法の特徴整理²¹

手法	Androidにおける利用			iOSにおける利用			ユーザーによる変更の可否	事業者間での名寄せ	
	利用可否	国内事業者	海外事業者	利用可否	国内事業者	海外事業者			
①端末固有ID	【○】 利用可能 ※脚注24	【×】 現在は利用していない	【○】 利用	【×】 利用不可 ※脚注24			【×】 不可能	【○】 容易	
端末固有ID非利用	②OS事業者が提供する広告用D	【○】 利用可能	△ 一部の事業者が利用	×～△ 利用され始めている	【○】 利用可能	【○】 利用	【○】 利用	【○】 容易	
	③広告配信事業者による独自ID(端末に保存される)	【○】 利用可能	【○】 利用	【×】 ほぼ利用されていない	【○】 利用可能	【×】 ほぼ利用されていない	【×】 ほぼ利用されていない	【△】 事業者により異なる	【×】 難しい
	④デバイスフィンガープリンティング(様々な情報の組合せでサーバー側でユーザーを推測し、識別)	【○】 利用可能	【○】 利用	【○】 利用	【○】 利用可能	【○】 利用	【○】 利用	【△】 理論上は可能	【△～○】 比較的容易(精度は100%ではない)

(出所) 各種公開情報を基に日本総合研究所作成

【図表 2.2.21】ユーザー識別手法の概要(広告配信事業者による独自ID、デバイスフィンガープリンティング)



(出所) 各種公開情報を基に日本総合研究所作成

次に「アプリ提供者・利用者に対する取組」について図表 2.2.22 のように取りまとめた。

²¹ 「①端末固有ID」に関しては、iOSは2013年5月より、端末固有IDの利用を禁止している。Androidは2013年10月よりAdIDの提供を開始している(2014年8月以降、端末固有IDの利用は規制されるとしている)が、2014年3月時点では端末固有IDは利用可能である。

【図表 2.2.22】利用者情報の取扱いに関するアプリ提供者・利用者に対する取組

項目	概要
アプリ提供者 に対する取組	<p>マニュアルやアプリ開発に関する講習会において、利用者情報の取扱いに関する働きかけを行っているケースが存在</p> <p>❖一部の事業者がモジュールのマニュアルやアプリ開発に関する講習会において、利用者情報の取扱いに関する働きかけを行っているものの、大多数の事業者はアプリ提供者に対して、利用者情報の取扱いにおいて具体的な取組は行っていない。</p>
利用者に対す る取組	<p>アプリの広告枠から広告配信事業者のプライバシーポリシーにジャンプできるマーク(インフォメーションマーク)を既に提供している事業者が存在</p> <p>❖ただし、アプリ広告においてインフォメーションマークを提供している事業者は限られている。</p>
アプリ提供者 に対する取組 の課題	<p>広告配信事業者がアプリ提供者に対して、アプリプラポリの掲載を求めることは難しい</p> <p>❖広告配信事業者はアプリ提供者から選ばれる立場にあるため、広告配信事業者からアプリ提供者に対して、アプリプラポリの掲載を求めるのは難しい。</p> <p>❖ウェブ広告の世界と比較して、媒体主(アプリ提供者)には、個人事業主や中小企業が多いため、アプリプラポリを作成する余力が無い場合が多い。</p>

(出所) 広告配信事業者へのヒアリング内容(2014年2月～3月)を基に日本総合研究所作成

「アプリ提供者に対する取組」では、一部の事業者がアプリ提供者向けのモジュールのマニュアルにおいてSPIの紹介やアプリ開発に関する講習会で利用者情報の取扱いに関する説明などの働きかけを行っているが、多くの事業者はアプリ提供者に対する具体的な取組は行っていない。「アプリ提供者・利用者に対する取組の課題」でも詳述するが、アプリ提供者自体が利用者情報の取扱いに対して興味・関心が少ないため、広告配信事業者にとって、アプリ提供者のニーズが少ない事項(利用者情報の取扱い)に取り組むインセンティブが働かないと考えられる。

「利用者に対する取組」では、一部の事業者がインフォメーションマーク(クリックすると広告配信事業者のオプトアウトページにジャンプする広告上に表示されたマーク)を既に提供しているが、多くの事業者は未実装の段階にある。もともとインフォメーションマークは行動ターゲティング広告において利用者にオプトアウトへの導線を提供するためのものであり、前述したようにアプリ広告では行動ターゲティング広告がそれほど普及していないために実施事業者が少ないと推測される。そのため、アプリ広告における行動ターゲティング広告の割合が増加し、さらに改訂されたJIAA「行動ターゲティングガイドライン」が浸透すれば、インフォメーションマークを実装する企業は増加すると考えられる。

「アプリ提供者に対する取組の課題」として、アプリ提供者に対して広告配信事業者がアプリプラポリの掲載を強く求めることが難しいこと、そもそもアプリ提供者の利用者情報の取扱いに対する意識が低いことが存在する。アプリ提供者は広告配信事業者を選ぶ立場にあるため、アプリプラポリの掲載について強く求めると、他の広告配信事業者を利用してしまいう可能性が高いのではないかと多くの事業者が考えている。また、ウェブの世界と比較して、アプリの媒体主(アプリ提供者)には、個人事業主や中小企業が多いため、収入増加にのみ強く関心を示す事業者が多く、プライバシーポリシーを作成する余力やモチベーションが少ない場合が多い。

(2) 第三者検証への協力可能性・要望

「第三者検証への協力可能性・要望」について図表 2.2.23 のように取りまとめた。

【図表 2.2.23】第三者検証への協力可能性・要望

項目	概要
協力可能性	<p>広告モジュールのリスト化に対して前向きな事業者も存在</p> <ul style="list-style-type: none"> ❖ 第三者検証におけるアプリ解析の精度・速度向上のための広告モジュールのリスト化、アプリ提供者向けに広告モジュールのホワイトリストの作成に対して、協力的な事業者が複数存在 ❖ 第三者検証において不適切なアプリが検出された際に、当該アプリに広告を配信しないという措置が技術的に可能
要望	<p>広告配信事業者はアプリ提供者に対して負担が少なく、かつ、海外の状況と乖離しない形を希望している</p> <ul style="list-style-type: none"> ❖ アプリ提供者の負担の少ない体制が求められる。 ❖ 海外と日本において、広告モジュールの取得情報の仕様の差が大きいと、海外企業との提携や日本企業の海外展開において足かせになる可能性が存在する。 ❖ 広告モジュールに対して「情報収集モジュール」という名称をつけることは不適切ではないか。「広告モジュール」等に名称を変更してもらいたい。

(出所) 広告配信事業者へのヒアリング内容(2014年2月～3月)を基に日本総合研究所作成

「協力可能性」では、第三者検証におけるアプリ検証の精度・速度向上のための広告モジュールのリスト化の作成、アプリ提供者向けに利用者情報の取扱いが適切に行われている広告モジュールのホワイトリスト作成に対して、前向きな事業者が複数存在した。広告モジュール自体が広くアプリ提供者に公開しているものであるため、リスト化に対する抵抗は少ないようである。

「要望」では、アプリ提供者に対して負担の少ない仕組み、第三者検証の評価基準などが海外の状況と乖離していないことを求める事業者が多い。広告配信事業者は、海外の状況と乖離することが海外事業者との提携や海外市場への参入に対する足かせになることを懸念している。また、広告用のモジュールもトラッキング用のモジュールもひとまとめに「情報収集モジュール」とするのは、利用者に誤解を与えかねず、「広告モジュール」等に名称を変更してもらいたいという声も存在する。

(3) 今後の課題

1) SSPの普及による利用者情報の取扱いへの影響

SSP (Supply Side Platform) とは、複数の広告ネットワークや DSP (Demand Side Platform) と連携して、広告掲載率や収益の最大化をサポートするアプリ提供者向けのサービスである。SSP の機能は、大きく 2 つあり、1 つ目はアプリ提供者が自ら設定した基準・ルールに基づいて広告配信を行う機能であり、2 つ目は広告掲載 (インプレッション) のたびに、複数のアドネットワークや DSP の中から最も収益性の高い広告を選択する機能 (RTB、リアルタイムビidding) である。SSP の利用はウェブ広告では一般的なものであり、アプリ広告においても近年、多数のアドネットワークや DSP と連携し、RTB を備えた SSP が出てきており、アプリ広告においても一般的に利用されるようになって考えられる。

SSP を導入した場合のアプリの実装や利用者情報の流通経路は図表 2.2.24 のようになる。アプリ提供者は SSP 用のモジュールのみをアプリに実装する。広告掲載の際には、SSP 用のモジュールが情報を取得し、SSP 提供事業者のサーバーに送信する。次にサーバーが複数のアドネットワーク・DSP と通信を行い、配信する広告が決定され、アプリに広告が掲載される。

アプリ広告における SSP の普及が利用者情報の取扱いに与える影響は、大きく 2 つ考えられる。

1 つ目は SSP 導入によりアプリが取得した利用者情報の送信先が多岐 (数社から数十社) に渡ることである。SSP の利用プロセスとして、アプリ提供者は SSP 用モジュールのみをアプリに導入し、SSP 事業者と契約するだけでよく、少ない手間で複数の広告配信事業者の広告掲載が可能になる。(SSP を利用せずに、

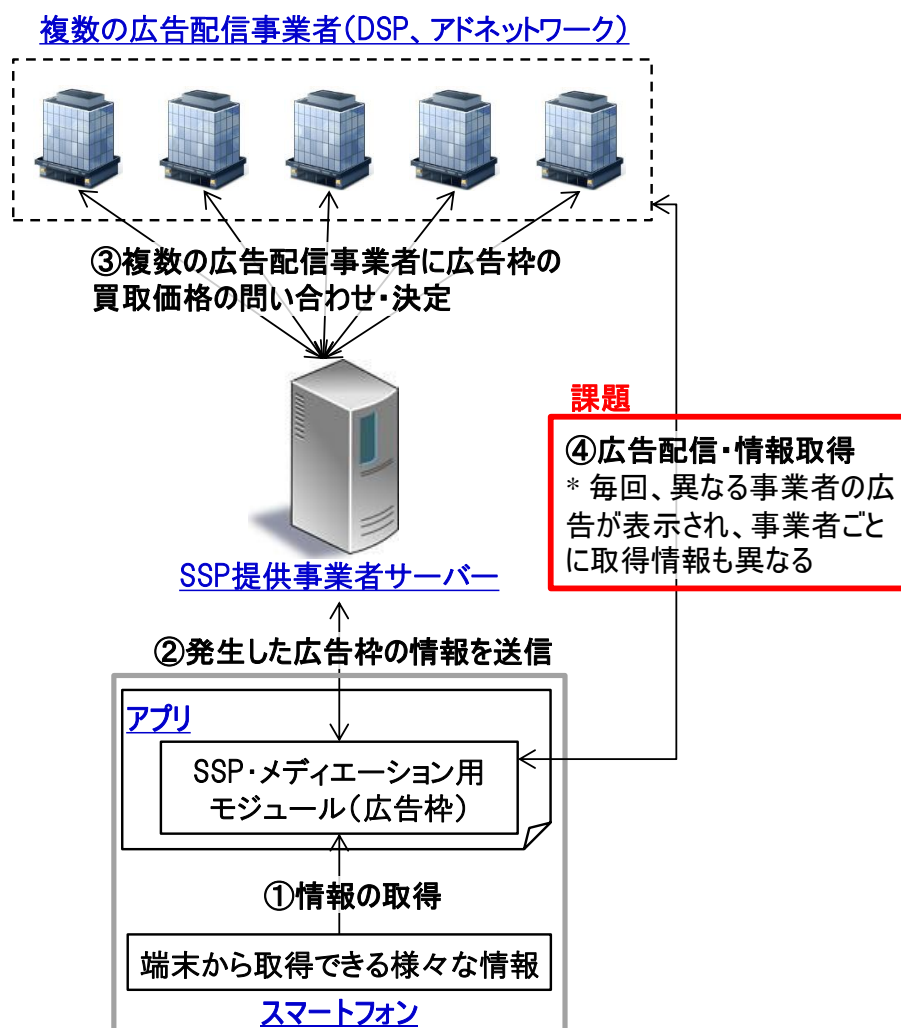
複数の広告配信事業者の広告を掲載するには、それぞれのモジュールをアプリに組み込み、かつ、各広告配信事業者と契約する必要がある。

2つ目は、アプリへの広告配信の際に、送信される情報の種類や送信先の把握が非常に難しくなることである。RTB では広告掲載のタイミングで、広告配信事業者が決まり、事業者ごとに取得情報や送信先が異なるため、実際に広告掲載がなされないと、どの情報がどこに送信されるかが把握できない。

上記のような状況においては、SPI で推奨されたプライバシーポリシーの 8 項目のうち、②取得される情報の項目、⑥外部送信・第三者提供・情報収集モジュールの有無を正確に記載する難易度が上がり、アプリ提供者の負担が大きくなることが懸念される。

また、SSP の普及は利用者情報取扱いについての技術的なアプリ検証にも影響を与える可能性がある。SSP モジュールが導入されたアプリに対して、静的解析を行っても、情報の送信先として SSP 事業者のサーバーしか検出されず、最終的な情報送信先を検出できない。また、動的解析においても、端末が持つ情報によって広告配信事業者が異なり、情報の送信先や取得情報が変わるため、短時間のアプリ起動や仮想端末による動的解析では不適切な情報送信・取得を見逃す確率が高まると考えられる。

【図表 2.2.24】 SSP 導入におけるアプリの実装や利用者情報の流通経路



(注)* 「アプリへのモジュールの実装方法」: SSP を通した広告と広告配信事業者から直接配信される広告を併用する場合などにおいては、SSP 用のモジュールと広告モジュールの両方をアプリに実装するケースも存在する。アプリ提供者の広告掲載の運営方針によって、アプリに導入するモジュール数は大きく異なる。

(出所) 広告配信事業者へのヒアリング内容(2014年2月～3月)および各種公開情報を基に日本総合研究所作成

2.2.6 アプリマーケット運営事業者

(1) Apple

AppleはiOSの開発、iOSを搭載したタブレット・スマートフォン（iOS端末）の製造・販売、iOS端末向けのアプリマーケット「App Store」の運営、iOS端末向けアプリの開発環境の提供を行っている。現状、Appleはスマートフォンにおいて垂直統合的なエコシステムを構築しており、iOS端末で利用するためのアプリを入手するルートは「App Store」のみである。アプリ提供者が「App Store」にアプリを公開するためには、まず開発者登録が必要であり、Appleは登録時にiPhone Developer Program License Agreementに基づき、アプリ提供者のアプリ開発に対する制約を課している。また、Appleは、アプリ提供者が「App Store」にアプリを公開・アップデート際に、アプリの利用者情報の取得や取扱状況等を審査し、不適切とみなされたアプリについてはアプリの公開・アップデートを拒否(リジェクト)している。

Appleの利用者情報の取扱いに関する動向を、OSにおける取組、アプリマーケットにおける取組、アプリ提供者に対する取組という項目で取りまとめた（図表2.2.25）。

OSにおける取組では、①IDFAの導入、②MACアドレス・UDID取得の制限、③アプリ単位での取得情報の許可設定、④情報取得タイミングでの特定の利用者情報取得に関する個別同意について説明する。

①Appleは2012年9月にリリースしたiOS6.0から広告用の識別子IDFA(Identification For Advertisers)を導入している。IDFAはAppleがiOSアプリに対する広告配信のために用意した識別子であり、端末ごとにユニークなIDとなっており、広告配信事業者はIDFAを取得すれば各端末を識別できる。IDFAと端末固有IDの違いは次の2つである。1つ目はiOS端末の利用者がIDFAを利用した追跡型広告（行動ターゲティング広告）の制限を端末側で設定できること、2つ目は利用者が自由に利用端末のIDFAをリセットできることである。これらの2つの機能により、利用者が端末・利用者識別、ターゲティング広告の配信を拒否できるようになった。留意が必要な点として、端末側での追跡型広告の制限の設定は、アプリがIDFAを取得できなくするのではなく、端末の追跡型広告に対するステータスを「制限」と変更することである。そのため、アプリ側に広告配信の前に端末の追跡型広告に対するステータスを取得し、そのステータスに合わせて対応する仕組みが実装されていないと、端末側で追跡型広告の制限を設定しても効果を発揮しない仕組みになっている。また、Appleは「iOS Developer Library」に、利用者が追跡型広告の制限を端末側で設定している場合であっても、広告の頻度上限、コンバージョン計測、ユニークユーザーの計測、セキュリティや詐欺行為の発見、デバックの用途には、IDFAを取得し、使用していいと記載している。

②Appleは2013年9月にリリースされたiOS7において、アプリがMACアドレス・UDIDを取得するAPIを実行しても、無効な値²²を返すように仕様を変更した。

③iOSでは、図表2.2.26のように利用者は位置情報、連絡先、カレンダー、写真などの情報について、アプリ単位で情報取得の許可設定をできるようになっている。

④iOSでは、アプリ起動後に、アプリが最初に位置情報等の特定の利用者情報を取得するタイミングでポップアップを表示し、利用者情報の取得目的を伝えた上で同意を取得する仕組みになっている。

アプリマーケットにおける取組では、Appleは2013年3月にアプリにおける端末固有IDの利用の禁止

²² MACアドレス取得時には固定値(20:00:00:00:00:00)、UDID取得時には「FFFFFFFF+identifierForVendor」という値が返される。UDIDに代わるIDとして、iOS6.0から使えるようになったIDで、ベンダー（開発者）が異なるアプリでは、異なるIDが返される。

を発表し、2013 年 5 月から UDID を利用するアプリが、App Store にアプリを公開・アップデートする際にリジェクトされるようになった。さらに、2014 年 2 月からは広告が表示されないにもかかわらず IDFA を取得するアプリが審査でリジェクトされるようになった。また、2013 年 9 月に Apple は App Store に「子ども向け」アプリカテゴリを設置し、13 歳未満の子供向けアプリは、「App Store Review Guidelines」によりプラポリの掲載等が義務付けられている。

アプリ提供者に対する取組では、アプリ提供者向けのウェブサイト「iOS App Programming Guide」内の「App Design Basics」²³において、「Best Practices for Maintaining User Privacy」として、「SPI」・「SPI II」（英語版）が紹介されている。

【図表 2.2.25】 Apple の利用者情報の取扱いに関する最近の取組

大項目	小項目	概要
OS における取組	IDFA の導入	<ul style="list-style-type: none"> ● iOS6.0 から広告用の識別子 IDFA の導入。 ● iOS6.1 から IDFA をユーザーがリセットできる機能の追加。
	MAC アドレス・UDID 取得制限	● iOS7 からアプリが MAC アドレス・UDID を取得できないようになった。
	アプリ単位での取得情報の許可設定	● 利用者が位置情報、連絡先、カレンダー、写真などの情報について、アプリ単位で情報取得の許可設定をできる。
アプリマーケットにおける取組	UDID を利用するアプリのリジェクト	● 2013 年 5 月から端末固有 ID の UDID を取得するアプリが、App Store にアプリを公開・アップデートする際の審査で、リジェクトされるようになった。
	広告以外の目的での IDFA の利用禁止	● 2014 年 2 月から広告が表示されないにもかかわらず IDFA を取得するアプリが審査でリジェクトされるようになった。
	子ども向けアプリのプライバシー対応	● 2013 年 9 月 App Store に「子ども向け」アプリカテゴリを設置。加えて 13 歳未満の子供向けアプリは、「App Store Review Guidelines」によりプラポリの掲載等が義務付けられている。
アプリ提供者に対する取組	「SPI」・「SPI II」の紹介	● アプリ提供者向けのウェブサイトで、「SPI」・「SPI II」（英語版）が紹介されている。

(出所) 各種公開情報を基に日本総合研究所作成

【図表 2.2.26】 アプリ単位での取得情報の許可設定画面



(出所)日本総合研究所作成

(2) Google

Google は Android の開発、Android 端末向けのアプリマーケット「Google Play」の運営、Android 端末向けアプリの開発環境の提供を行っている。Android では、iOS と異なり、Android 端末向けのアプリを「Google Play」以外の場所（他の事業者のアプリマーケットやアプリ提供者のウェブページなど）からも入手可能である。アプリ提供者が「Google Play」にアプリを公開するためには、開発者登録が必要である。また、アプリ提供者が Google Play にアプリを公開・アップデートする際には、Google が実施する審査を受ける必要がある。

Google の利用者情報の取扱いに関する動向を取りまとめた（図表 2.2.27）。

OS における取組では、Google も Apple と同様に、Android に広告用の識別子 Android 広告 ID（AdID）の導入を発表しており、Android アプリの最新の開発環境（Google Play 開発者サービス バージョン 4.0）では、AdID および関連する API が既に導入され、AdID を利用したアプリが開発可能になっている。AdID の正式な導入開始時期は 2014 年 8 月とされており、「Google Play デベロッパー プログラム ポリシー」には「2014 年 8 月 1 日から、Play ストアにアップロードされたすべての更新や新着アプリには、広告目的で使用する端末 ID として広告 ID（端末で利用可能な場合）を使用する必要があります。」と記載されている。また、「Google Play デベロッパー プログラム ポリシー」には「(AdID を) リセットする際にユーザーの明示的な同意なしに、新しい広告 ID を以前の広告 ID や以前の広告 ID からのデータにリンクしてはいけません。さらに、ユーザーの [インタレストベース広告をオプトアウト] 設定を遵守する必要があります。」と記載があるため、IDFA と同様に、AdID においても、端末側でのインタレストベース広告（行動ターゲティング広告）の制限、AdID のリセットが可能になると考えられる。利用者がインタレストベース広告の制限を行った場合の仕組みについては IDFA と同様であり、利用者がインタレストベース広告の制限を端末側で設定していても、コンテンツターゲット広告、フリークエンシーキャップ、コンバージョントラッキング、レポート、セキュリティや不正行為の検出などに AdID を使用できる。

Android 広告 ID の導入以外の OS における取組として、各アプリが取得する利用者情報の確認機能「Verify Apps」の導入が挙げられる。Verify Apps はアプリをインストールする前に有害な挙動がないかどうかをチェックして、マルウェアなどが見つかった場合はインストールを阻止する機能であり、Google は Android 4.2 から同機能を搭載している。さらに、2014 年 4 月から同機能をインストール前だけでなく、定期的に端末にインストールされたアプリの安全性もチェックするようにアップデートすると発表されている。また、各アプリが取得する利用者情報の確認機能では、図表 2.2.28 のように、「設定」のアプリケーション管理画面から、各アプリが取得する利用者情報の確認とアンインストールが可能になっている。

アプリマーケットにおける取組では、AdID 導入に関連したアプリマーケットでの対応について、Google は明言していない。

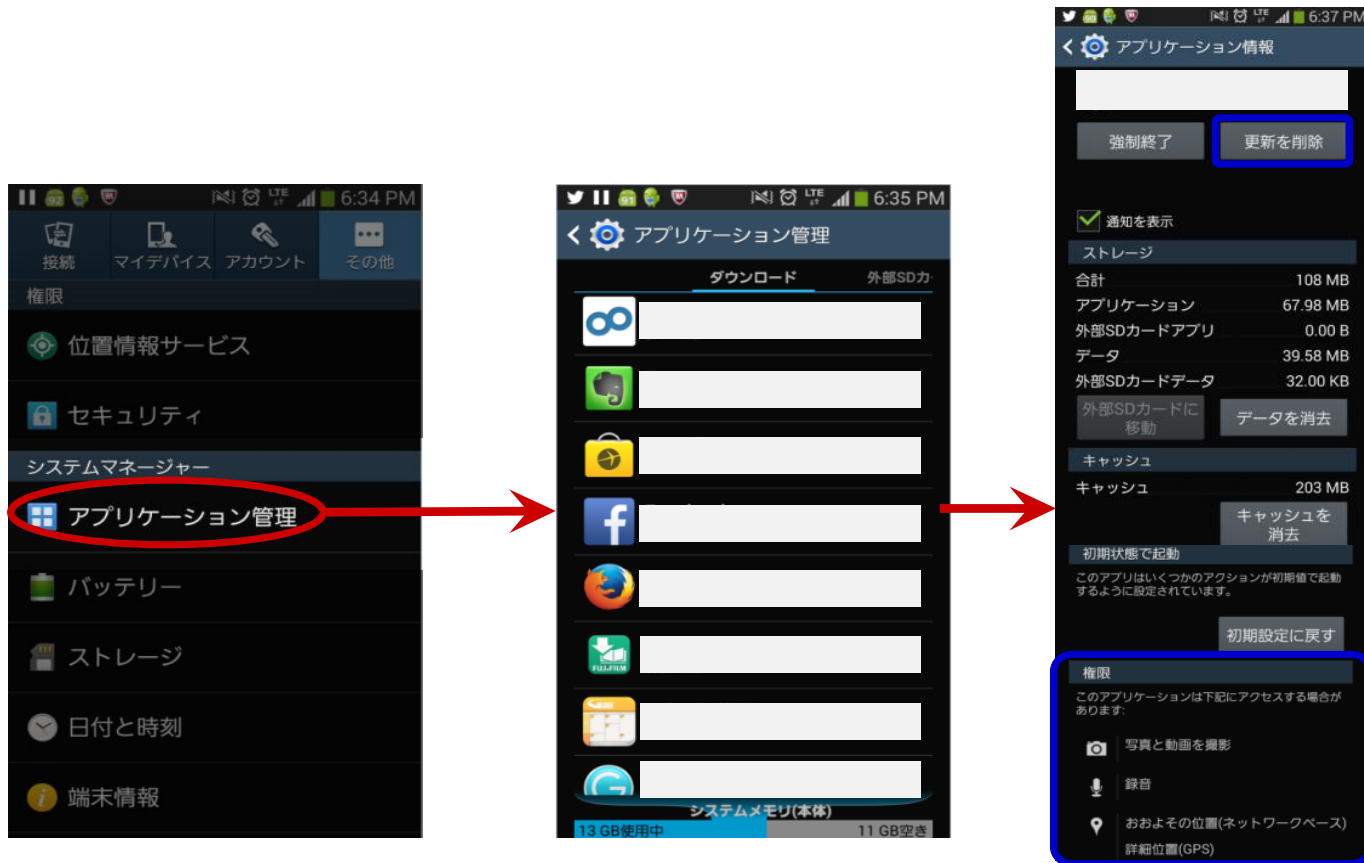
アプリ提供者に対する取組では、2014 年 2 月 1 日からアプリ提供者向けに Google Play の各種ポリシー・規約をわかりやすく説明したウェブサイト「Google Play アプリポリシーセンター」を開設した。同サイトの中では、ユーザーに対してアプリ内の広告についてわかりやすく伝えること、起動時のオプトインなどを推奨している（図表 2.2.29）。

【図表 2.2.27】 Google の利用者情報の取扱いに関する取組

大項目	小項目	概要
OS における取組	Android 広告 ID の導入	<ul style="list-style-type: none"> ● Android において利用者が変更可能な広告用の ID (AdID) が導入された (AdID は広告と利用者の分析以外では使用してはいけない)。 ● 利用者は、端末側でインタレスト広告をオプトアウトというステータスを設定できる。 ● 2014 年 8 月 1 日から Google Play にアップロードされたすべての更新・新着アプリでは、広告目的で使用する端末 ID として AdID を使用する必要がある。 ● ※ただし、広告目的で AdID 以外を利用しているアプリに対する措置は明言されていない。
	不正アプリチェック機能の「Verify Apps」の搭載	<ul style="list-style-type: none"> ● Android 4.2 からアプリをインストールする前に有害な挙動がないかどうかをチェックして、マルウェアなどが見つかった場合はインストールを阻止する機能が追加された。 ● 2014 年 4 月にセキュリティ強化のため当該機能をアップデートし、インストール後のアプリも定期的に検査を行う機能が追加された。
アプリマーケットにおける取組		
アプリ提供者に対する取組	Google Play アプリポリシーセンターの開設	<ul style="list-style-type: none"> ● 2014 年 2 月 1 日からアプリ提供者向けに Google Play の各種ポリシー・規約をわかりやすく説明したウェブサイトを開設した。 ● 同サイトの中では、利用者に対してアプリ内の広告についてわかりやすく伝えること、起動時のオプトインなどを推奨している。

(出所) 各種公開情報を基に日本総合研究所作成

【図表 2.2.28】各アプリが取得する利用者情報の確認機能



(出所)日本総合研究所作成

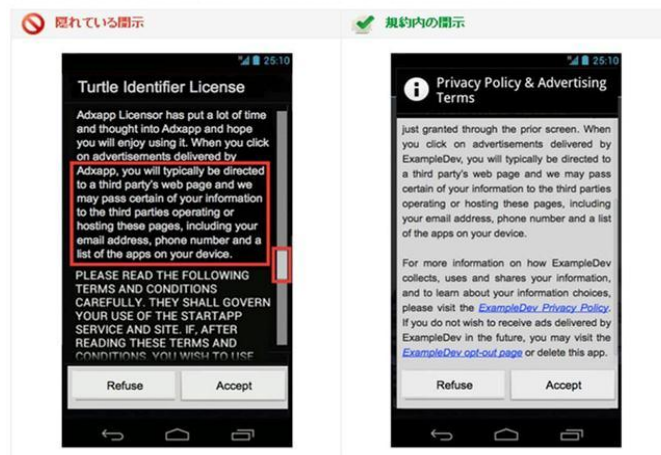
【図表 2.2.29】 Google Play アプリポリシーセンターにおける解説例

アプリで広告をどのように使用するかについてユーザーに十分に開示することは重要です。アプリ内に表示する広告の種類や場所について、関連する動作があればそれについて、ユーザーにわかりやすく示す必要があります。さらに、ユーザーの同意を求めると、広告やオプトアウトを管理するオプションを提供することが必要です。

ガイドライン

- ユーザーに広告について伝える - ユーザーの情報をどのように使用し、広告のオプションをユーザーがどのように管理できるかを伝える、簡単明確で十分な開示を行います。
- ユーザーにわかりやすく表示する - 広告の開示は、ユーザーが見る可能性の低い場所に隠すのではなく、目につきやすい場所に掲載します。
- 起動時に同意(オプトイン)を求める - 可能であれば、広告の開示をアプリの説明のほか、広告規約、エンドユーザー使用許諾契約(EULA)などのドキュメントにも含めます。初回の起動時に規約を表示し、アプリの使用前に、ユーザーの同意を求めます。

おすすめの方法は、広告の開示をエンドユーザー使用許諾契約(EULA)に含めることです。開示は簡潔で明確な記述で、モーダルダイアログに表示し、アプリの使用前にユーザーがその条項に同意することを求める必要があります。



左上の図は、長い EULA に広告の開示が隠れている例です。開示情報そのものもテキストに明示されず、ユーザーが EULA を十分下までスクロールしない限り表示されません。

(出所) Google Play アプリポリシー センターから抜粋

(3) NTTドコモ

NTTドコモはスマートフォンアプリに関連するサービスとして、Google Play や App Store のアプリを紹介し、各アプリのマーケットページへのリンクを記載した「d アプリ&レビュー」、定額制のコンテンツ提供サービス「スゴ得コンテンツ」を提供している。「スゴ得コンテンツ」では、現在、120 のコンテンツを提供しており、そのうち 70 程度が Android アプリである。

「d アプリ&レビュー」は、アプリを掲載する前にコンテンツの内容、動作確認、取得しているパーミッション (Android アプリの場合)、アプリプラポリをチェックし掲載している。動作確認ではアプリのコンテンツ内容をチェックしているだけであり、通信内容、ログ解析などの動的解析は行っていない。

「スゴ得コンテンツ」では、Android アプリに対して、アプリの公開・アップデート時に審査を行っている。アプリの審査では動作確認やリスクファインダ等における技術的動作確認、プラポリの有無の目視確認、アプリの内容のチェックを行っている。原則として、アプリが取得した情報の第三者送信は認められていないが、アプリ提供者がアプリ改善、ユーザー分析のためにトラッキング用情報収集モジュールを利用し、情報収集モジュール提供事業者へ情報を送信することは例外として認めている (ただし、事前に申請が必要)。

アプリ提供者に対する取組として、アプリ提供者向けのポータルページにプライバシーポリシーに関するガイドラインを掲載しており、SPI を踏まえてアプリプラポの掲載などを推奨している。また、年に 2 回 (東京、大阪) アプリ提供者向けのセキュリティ勉強会を提供しており、その中でも SPI やプライバシーポリシーの掲載について説明している。また、アプリ提供者に限らず、「d メニュー」のコンテンツプロバイダーに対して、プラポリの掲載を要請している。

(4) KDDI

KDDI は Android 端末向けのアプリマーケット「au Market」、 「au スマートパス」を提供している。au スマートパスは Google Play で有料となっているアプリなどを無料で制限無くダウンロードできるサービスである。

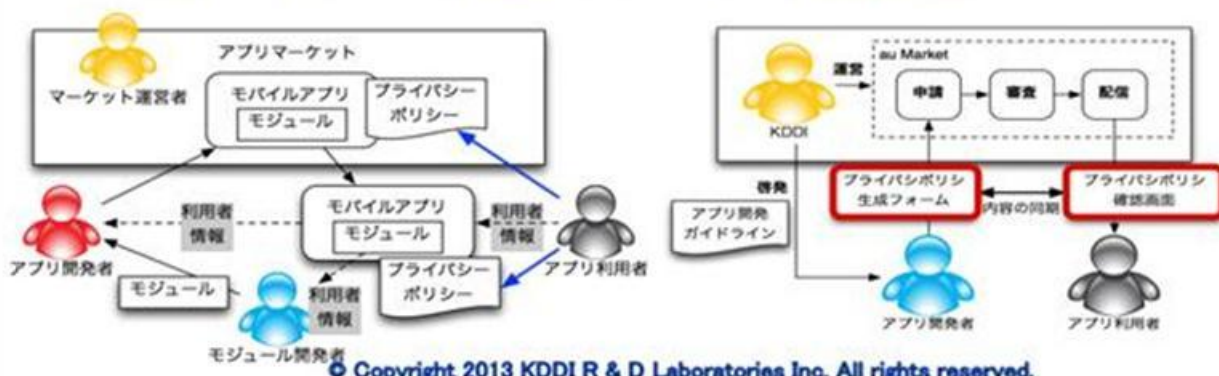
KDDI は「au Market」、 「au スマートパス」で配布するアプリに関して、サービス内のアプリ全てに対して、公開・アップデート時に審査を行っている。アプリの審査では、マルウェア、利用者情報の送信先、その他不適切・迷惑な動作を検証している。マルウェア・その他不適切・迷惑な動作の検証では、情報取得 API の検知、情報収集モジュールの検知などの静的解析、アプリの画面・各種ログ・外部との通信状況の動的解析を行い、取得しているパーミッション、通信の頻度、通信の宛先などを評価している。また、第三者検証事業者の取組の小節 (2.2.4) で述べたようにアプリプラポリの手動・自動での審査も実施しており、アプリプラポリの記載内容と実際の動作が一致しているかを評価している。

また、同社はプライバシーポリシー管理フレームワーク (図表 2.2.30) を構築しており、アプリプラポリの記載をマーケットの全てのアプリに義務づけている。

【図表 2.2.30】 KDDI のプライバシーポリシー管理フレームワークの概要

プライバシーポリシー管理フレームワーク KDDI KDDI R&D LABS

- ・ 目的
 - ・ アプリによる利用者情報の取り扱いの透明性を確保する
- ・ 概要
 - ・ 透明性を確保する手段として、適切な「プライバシーポリシー」を用いて、アプリの利用者の承諾を得る利用形態を定着させる
- ・ プライバシーポリシーの作成指針
 - ・ プライバシーポリシーの作成に関する指針として、スマートフォン プライバシー イニシアティブ(総務省) の以下の8項目を配慮



23

プライバシーポリシーの利用者への告知 KDDI KDDI R&D LABS

許諾文を読む文化のない日本のユーザ向けに、読みやすさを考慮した1ページの画面で重要な3項目を説明！！

利用者情報の取り扱いに関する申請画面

取り扱う情報

取り扱う目的

情報の送信先

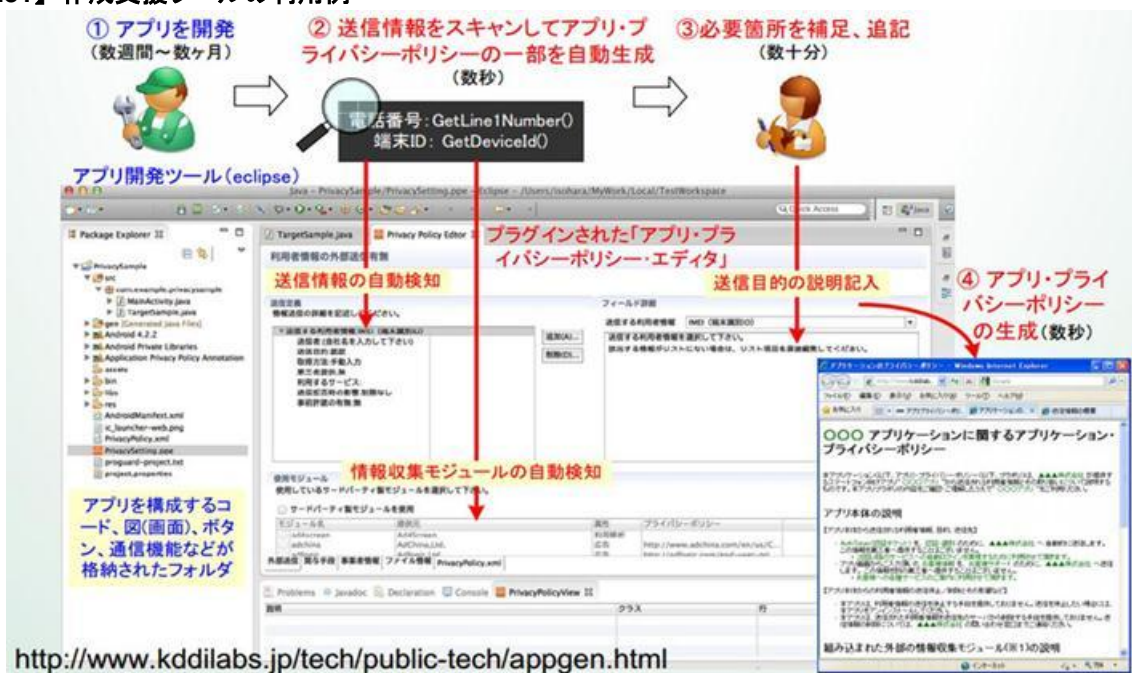
利用者情報の取り扱いに関する告知画面

(出所) KDDI 研究所「スマートフォンにおけるプライバシー問題と対象の方向性」(2013 年 2 月)から抜粋

また、au Market、au スマートパスの審査を担当している KDDI 研究所は、アプリが取得する利用者情報を高精度で検出し、SPI に対応したアプリのプライバシーポリシー作成を支援するツール（アプリプラポリ作成支援ツール）を開発し、アプリ提供者向けに広く無償公開を行っている。KDDI 研究所によると同ツールの特徴は以下のとおりである（図表 2.2.31）。

- ◇アプリ開発環境である Eclipse へのプラグイン型のため開発工程に無理なく組み込める点
- ◇ソースコードから外部送信される可能性のある利用者情報を網羅的に検出し、「取得される情報の項目」を正確に記載できる点
- ◇アプリ本体や広告などの外部モジュールを見分けて、「外部送信・第三者提供の有無、情報収集モジュールの有無」を自動的に記載できる点

【図表 2.2.31】作成支援ツールの利用例



(出所) JSSEC「スマホアプリのプライバシーポリシー作成・開示についての考察」から抜粋

2.3 諸外国における取組状況

2.3.1 政府における取組

(1) 米国

米国におけるプライバシーに関する検討として、米国商務省の下の、米国電気通信情報庁（NTIA）が開催しているマルチステークホルダー会合がある。本会合は、モバイルアプリケーションの透明性に関する議論を行う会合であり、本会合を通じて、関係者間でのモバイルアプリケーションの透明性に関する行動規範（Code of Conduct）に対する合意形成を目的としている。

2012年の7月より2013年の7月まで、定期的に会合が開かれ、その中で行動規範の草案が作成された。主な内容は図表 2.3.1 にあり、収集状況をユーザーに通知しなければならない利用者情報の具体的な項目や、利用者情報の第三者提供先の記載、アプリ提供者の明記などのルールを定めており、会合の参加者内で同意を得ている。具体的に、本行動規範で定められている利用者への通知が求められる情報の種類は、図表 2.3.2 となる。

【図表 2.3.1】 NTIA 行動規範構成(2013/7/25 時点)

- | |
|--|
| <ol style="list-style-type: none"> 1. 序文 2. 簡易版の通知 <ol style="list-style-type: none"> A. データの収集について B. データの共有について C. データの収集・共有に関する例外規則に関して 3. 簡易版通知のデザインの要素 4. 利用者情報の用途、利用条件、詳細版のプライバシーポリシーへのリンクについて |
|--|

(出所) NTIA ホームページより抜粋

【図表 2.3.2】 収集状況をユーザーに通知しなければならない利用者情報

- | |
|--|
| <ol style="list-style-type: none"> 1. 身体情報（指紋、顔認識、筆跡、声紋等） 2. 検索履歴（訪れたサイトのリスト） 3. 通信履歴（電話、メールの履歴） 4. 連絡先・電話帳（連絡先リスト、SNSでのつながり、電話番号、郵便番号、メールアドレス、住所等） 5. 財政情報（クレジット、銀行、変更用データの様な消費者固有の財政情報） 6. 医療情報（健康状態をはかるために使われる情報） 7. 位置情報（過去、現在の位置情報） 8. ユーザーファイル（カレンダー、写真、文章、ビデオの様なデバイスにためられたユーザーのコンテンツ） |
|--|

(出所) NTIA ホームページより抜粋

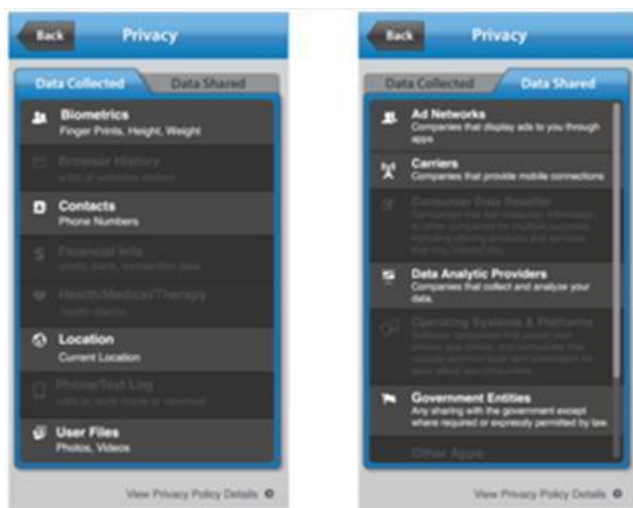
また行動規範に加え、実際にユーザーに対して利用者情報の取扱状況について説明するダッシュボード作成についても検討している。2013 年 7 月に、Association for Competitive Technology²⁴ (ACT) より、ダッシュボードのβ版が発表された(図表 2.3.3)。それ以外に、同会合の加盟企業である米国シンクタンクの Future of Privacy Forum からも、簡易版の通知のデザインに関して複数の例が提示されている(図表 2.3.4)。

【図表 2.3.3】 モバイルアプリケーション プライバシーダッシュボード案(ACT)



(出所)NTIA ウェブページから抜粋

【図表 2.3.4】 モバイルアプリケーション プライバシーダッシュボード案(FPF)



(出所)NTIA ウェブページから抜粋

2013 年 7 月以降、同会合の参加者は、上記のダッシュボードのユーザーテストを行っている。テストは ACT が中心的に行っている。キーワードは「short form privacy policy」であり、プライバシーポリシーを消費者に分かりやすい形で提示することが求められている。2013 年 11 月には、ACT より、ユーザーテスト

²⁴ ACT は主にモバイルアプリを開発する中小規模のソフトウェア会社で構成される業界団体。

イングが次の段階に入ったという発言があり、Apple、Facebook、BlackBerry、TRUSTe らの大手企業と連携する予定である。

(2) 欧州

欧州における取組状況として、第一に2013年4月2日、欧州6か国のプライバシー関連当局が、共同で米Googleに対する規制強化に取り組むことを発表した。背景として、Googleは2012年1月にプライバシーポリシーを変更して、複数のGoogleサービスを使用しているユーザーの情報を単一のGoogleアカウントのもとで統一する方針を発表した。この方針に対して欧州の一部の国が疑問を呈し、データ保護指令第29条作業部会、Jacob KohnstammがGoogleのCEOに宛てて新たなプライバシーポリシー導入の延期を求める書簡を送った。最終的にこの要請は無視され、3月には改訂版のプライバシーポリシーが導入されていた。英国のInformation Commissioner's Office (ICO) は今回、グーグル (Google) の新しいプライバシーポリシーが英国の法律に従っていない可能性が高いとの見解を示している。

また、2014年2月には、EU域内におけるプライバシー保護に関する規制の単一化を図るEU個人データ保護規則案が、現地時間12日に欧州議会で採択された。新ルールのなかには、ユーザーの個人情報の扱いが適切でない企業に対し、最高1億ユーロもしくは世界全体の売上高の最大5%のどちらか高いほうを罰金として科すことができるとする条項などが含まれている。EU域内の居住者のデータが、欧州で活動を行っている米国企業などによって欧州以外の地域で処理される場合等も、規制の対象となる見込みである。

(3) 英国

英国の取組状況として、情報コミッショナー事務局 (Information Commissioner's Office) より、2013年12月に、モバイルアプリのプライバシーに関する、開発者向けのガイダンス²⁵が作成された。本ガイダンスは、アプリ開発者が1998年のデータ保護法を準拠することと、利用者のプライバシーを保護することを目的として作成された。本ガイドラインの構成は図表2.3.5となる。

【図表 2.3.5】モバイルアプリのプライバシーに関する、開発者向けのガイダンス 構成²⁶

- | |
|--|
| <ul style="list-style-type: none"> □ 序文 □ パーソナルデータに関して □ パーソナルデータの取扱いについて □ アプリが収集するデータについて □ ユーザーに対する通知と同意取得について □ ユーザーに対するフィードバックと取得情報のコントロールについて □ データの安全な補完について □ 開発したアプリのテストと管理に関して □ その他の法的に配慮すべき事項 |
|--|

(出所) Information Commissioner's Office Privacy in mobile apps を基に日本総合研究所作成

²⁵ Privacy in mobile apps : Guidance for app developers
http://ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/privacy-in-mobile-apps-dp-guidance.pdf

²⁶ 構成の各タイトルに関しては、意識を掲載している。

本ガイドラインは、上記の内容について、具体例を含め、基本的な内容から説明を行っている。プライバシーポリシーに関しては、一つの文章上で全体を説明する必要はなく、プライバシーポリシーに関連する情報を、モバイルの小さい画面と、タッチスクリーンのインターフェースに適した方法で掲載すべきであると記載している。またモバイルアプリにおける通知や情報提供時の重要なポイントとして、図表 2.3.6 の内容を挙げている。

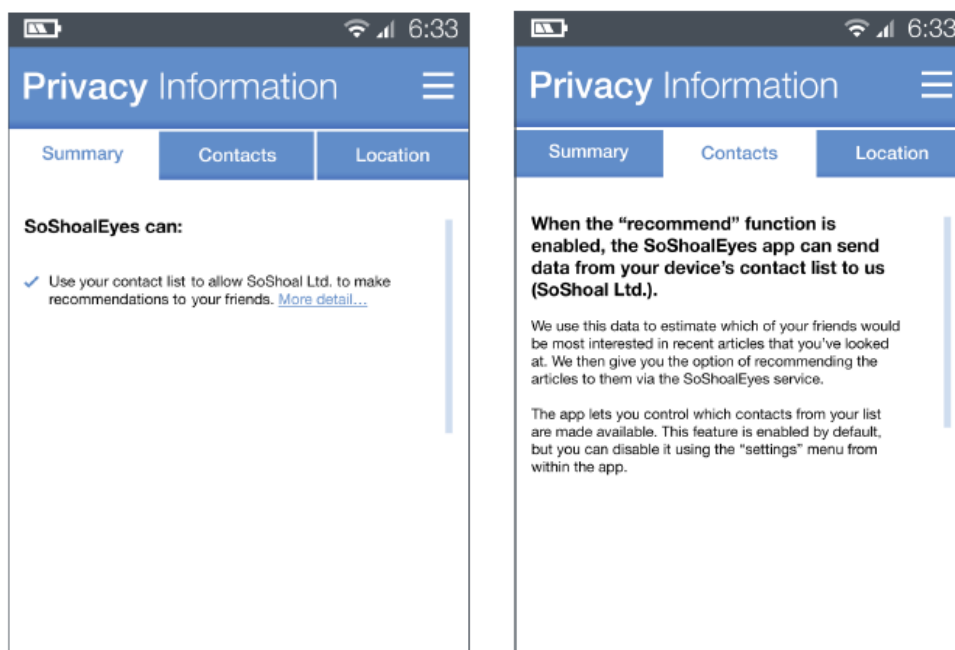
【図表 2.3.6】モバイルアプリの通知・情報提供における重要なポイント

- 平易な英語を使うこと
- 想定される利用者に適した言語を使うこと
- 情報の取得目的に関する透明性を高めることが重要であり、取得情報だけでなく理由を説明すること(OS上の利用許諾では十分とはいえない)
- アプリのプライバシーに関する情報を早期に提供すること(理想的にはアプリダウンロードの前にアクセス可能にすべき)
- 適切な場合には、重要な部分を要約した概要版と詳細版による階層化された表示を用いること

(出所) Information Commissioner's Office Privacy in mobile apps を基に日本総合研究所作成

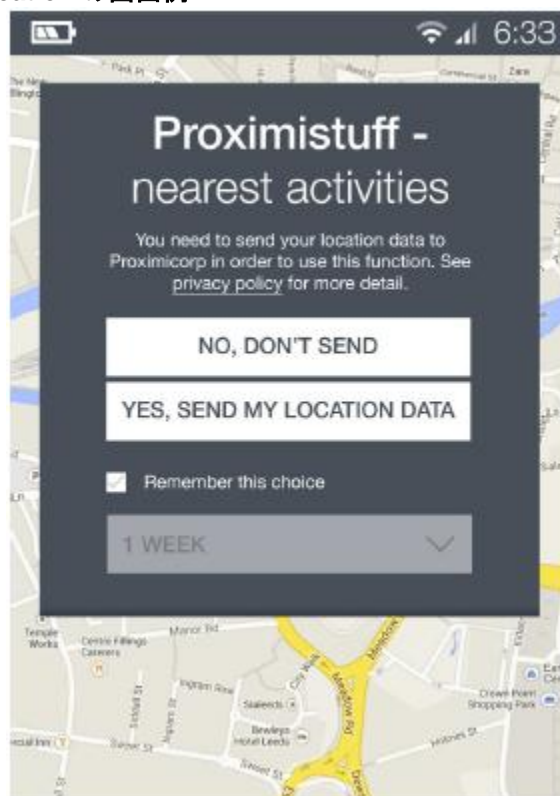
また具体的に、階層化したプライバシー情報の表示や、just-in-time-notification について、画面例を提供している(図表 2.3.7、図表 2.3.8)。

【図表 2.3.7】階層化したプライバシー情報の表示 画面例



(出所) Information Commissioner's Office Privacy in mobile apps より抜粋

【図表 2.3.8】just-in-time-notification の画面例



(出所) Information Commissioner's Office Privacy in mobile apps より抜粋

(4) 豪州

豪州では、2013年9月に、連邦情報コミッショナー事務所（OAIC²⁷）より、モバイルプライバシーに関するガイドライン²⁸が作成された。このガイドラインの目的は、アプリ提供者に、自身のアプリにおいて、プライバシーに関するルールを導入させることである。具体的な内容は、図表 2.3.9 のように、開発者のアプリ開発における留意点について記述している。また同様の内容を、開発者に対する分かりやすい説明手法として、具体的なチェックリストにして提供している。

また、豪州連邦情報コミッショナー事務所では、2014年3月に「オーストラリアプライバシー原則ガイドライン（Australia Privacy Principles guidelines）」の改正を行った。本ガイドラインでは、データ収集における、匿名性や通知の必要性等の原則について述べており、携帯電話における個人情報、利用者情報の取扱においても、適用される原則である。

加えて、豪州政府は、2013年に消費者のプライバシーに対する認識・態度をアンケートにより調査を行っている。本調査により、豪州の消費者の約36%が、アプリの取り扱う個人情報を懸念して、アプリを利用しなかった経験があるという結果が得られた（図表 2.3.10）。

²⁷ Office of the Australian Information Commissioner

²⁸ Mobile privacy : A better practice guide for mobile app developers

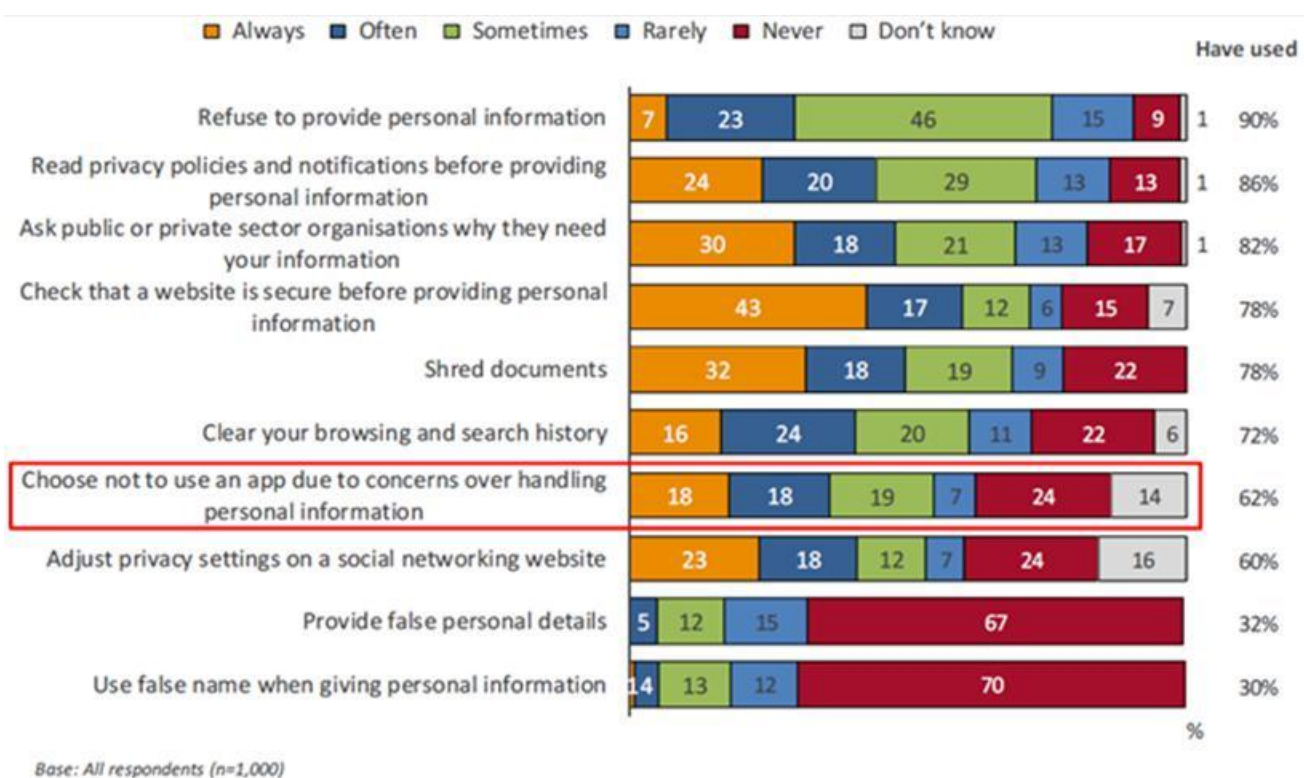
<http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/better-practice-guide-for-mobile-developers.pdf>

【図表 2.3.9】アプリ開発における留意点

- プライバシーに対する責任
- プライバシー慣行についての透明性の確保
 - ✓ 利用者情報の用途が簡潔に伝わるプライバシーポリシーを作成する。
 - ✓ プライバシーポリシーを見つけやすい場所に掲載する。
 - ✓ 個人情報プライバシーポリシーの記載通りに扱われていることを保証するための監視プロセスを導入する。
 - ✓ アップデート時に、個人情報の取扱いの変化を通知し、明示的な同意を取得する。
- 小さい画面における同意の取得
- 利用者への的確なタイミングでの通知と同意取得
- アプリが機能上必要な個人情報のみ収集
- 取得したデータの保管

(出所) OAIC「Mobile privacy: a better practice guide for mobile app developers」

【図表 2.3.10】アプリ開発における留意点



(出所) OAIC「Community Attitudes to Privacy survey」

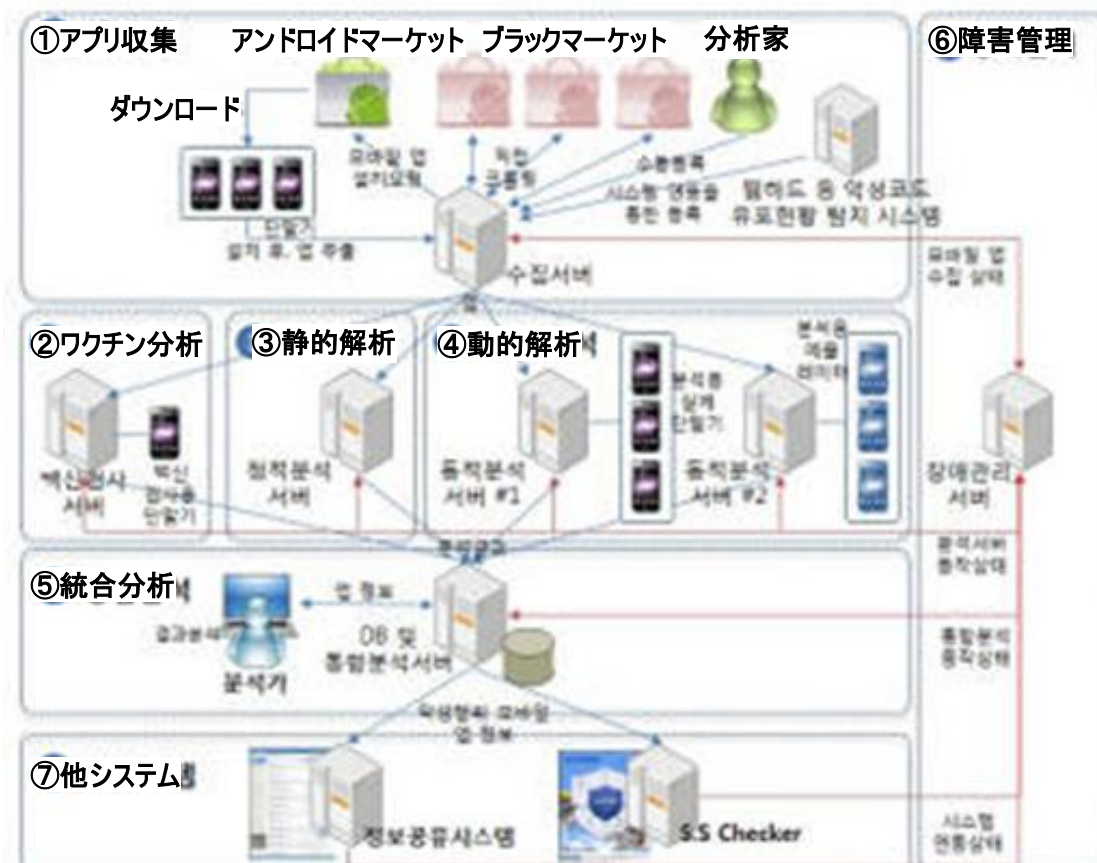
(5) 韓国

韓国インターネット振興院 (KISA) は、2012 年 5 月にスマートフォンから個人情報・位置情報などを不法に収集・利用する不正なアプリケーションを把握することができる悪意のあるアプリのモニタリングシステム (Android アプリが対象) を構築し、同年 10 月から 3 人の監視員がアプリの分析に乗り出すことを発表した (図表 2.3.11)。2014 年 3 月には、2013 年末までに同モニタリングシステムによって、約 12,000 個のアプリが検証され、うち、関連法規に従っていないアプリが約 2,000 個発見され、開発者に対してメールや固定電話などを通じて改善案内していることが KISA から発表された。

また、2013 年 7 月には、個人情報保護委員会は、放送通信委員会に対して、「スマートフォン関連個人情報保護ガイドライン」(仮称) を用意すべきという意見を伝えたことを発表した。同ガイドラインの作

成目的は、スマートフォンから様々な情報を収集・処理する会社（端末メーカー、OS 提供者、マーケット運営者、アプリ提供者、通信事業者など）が必要以上の個人情報を収集・処理しないようにして個人情報の流出などの事故を予防するための措置を講じなければならないようにすることである。

【図表 2.3.11】 KISA のモバイルアプリのモニタリングシステム



(出所) KISA ウェブページより抜粋

2.3.2 業界団体における取組

業界団体の取組の一つとして、アプリ提供者・事業者の業界団体である The Application Developers Alliance は、会員企業である Intuit 社を中心に、プライバシーに関する通知のオープンソースコードを開示している。また 2013 年 10 月には、「Mobile Privacy Summit」を開催するなど、啓蒙活動も行っている。

広告関連の業界団体としては、米国にオンライン広告・モバイル広告に関する自主規制の団体として、Network Advertising Initiative (NAI) が存在する。同団体は、スマートフォンアプリにより収集した情報に基づく広告配信における行動規範²⁹を 2013 年に作成した（図表 2.3.12）。行動規範では NAI のメンバーに対する要求として、データ収集時の明確かつ意味のある通知の提供や、オプトアウトの権利の提供等、取得したデータの取扱いなどを義務づけている。

²⁹ http://www.networkadvertising.org/2013_Principles.pdf

【図表 2.3.12】 アプリ広告に対する行動規範

- 教育
- 透明性と通知
- 利用者の情報コントロール
- アプリが機能上必要な個人情報へのみの収集
- 収集したデータの保管
- データ外部送信に対する規制。
- データに対するアクセス、品質、安全性、セキュリティ
- etc

(出所) Future of Privacy Forum ウェブページから抜粋

また業界団体に近い組織として、各国のパーソナルデータの保護機関が、プライバシーに関して様々な議論を行うため、1979 年から毎年開催されている「データ保護プライバシー・コミッショナー国際会議³⁰」がある。2013 年 9 月に開催された第 35 回においては、社会の「アプリケーション化」について議論が行われ、最終的な決議として、ワルシャワ宣言（Warsaw Declaration）が発表された。本宣言では、アプリケーションがさまざまな形で普及した現在社会における、アプリ利用者、アプリ開発者、OS 事業者、プライバシー・データ保護コミッショナーの役割に関して言及している。

本宣言では、アプリ利用者が、自身のデータを管理できることは必須であり、どのデータを誰と、何の目的で共有できるかについて決定できなければならないとしている。そのためには、アプリが実際に情報の取得を始める前に、データの取得について明確で分かりやすい情報を提供しなければならず、位置情報や電話帳情報等の特定の情報については、個々の場合に依って情報へのアクセスの可否を選択できるようにしなければならない。一方、アプリ開発者は、既存のプライバシー・データ保護のルールを順守することが求められ、そのため開発者は、広告モジュールを含めアプリに本当に必要な情報のみを収集するようにしなければならない。また、本宣言の中では、OS 事業者がプライバシーに関する責任をアプリ開発者と共有していると考えている。OS 事業者はアプリのプラットフォームを提供し、アプリが利用されるフレームワークを決めることが出来るため、データ保護において最も重要なポジションにいると考えられており、同事業者のプライバシーに関する認証や検証に関する取組が推奨されている。最後にプライバシー・データ保護コミッショナーの役割は、モバイルアプリの業界において、事業者・利用者双方のプライバシーに対する意識を高めることである。もしプライバシーに配慮した取組を奨励するだけでは効果が得られない場合には、ユーザーコントロールの確保のため、法による規制を行うことも考えられる。

2.3.3 その他関係する事業者における取組

米シンクタンク Future of Privacy Forum (FPF) は、消費者が一括で店内追跡サービスをオプトアウト（拒否）させるためのウェブサイト（www.smartstoreprivacy.org）の提供を、2013 年 11 月 18 日に開始した。ここでの店内追跡サービスとは、事業者が通行の流れの改善や商品の配置に関する判断を行うため、携帯電話が発する Wi-Fi や Bluetooth の通信信号を検知し、利用者の位置情報を判断するサービスである。FPF の新しいサービスでは、サイト（図表 2.3.13）を訪問し全てのスマートフォンに割り当てられている MAC アドレスを入力すると、携帯電話の持ち主が追跡を拒否していると参加企業に通知される仕組みになっている。2014 年 2 月時点で、位置分析を手掛ける 11 社がこのプロジェクトへの参加に同意している。

³⁰ International Conference of Data Protection and Privacy Commissioners

【図表 2.3.13】 FPF Opt out of Smart Store Tracking

(出所) Future of Privacy Forum ウェブページから抜粋

また、個社での取組として、Yahoo!の元従業員の Jim Brock 氏により設立された Web サイト、「PrivacyChoice」が存在する。本サイトでは、申請した Web サイトのトラッキング状況や、スマートフォンアプリの外部送信先のスキャンサービスが提供されている（図表 2.3.14）。また、プライバシーポリシーの作成支援ツールも提供しており、個人のサイトでも、このようにプライバシーに関する取組を行っている場合がある。

【図表 2.3.14】 PrivacyChoice の概要

(出所) PrivacyChoice から抜粋

第3章. 利用者情報の適切な取扱いに向けた課題と提言

3.1 提言に向けた検討実施体制について

第2章において、スマートフォン上のアプリを取り巻く事業者・団体を対象に、利用者情報の取扱いやプライバシーポリシーに関する取組について調査を行った。当該調査結果を基に、アプリプラポリの普及および第三者検証の在り方に関する課題についての検討および提言のとりまとめを「スマートフォン アプリケーション プライバシーポリシー普及・検証推進タスクフォース」（以下、「TF」とする）の下に設置した「広告検討WG」、「技術検討WG」で実施し、最終的な取りまとめをTFにて行った。

検討実施体制およびWGの実施概要については図表3.1.1に示す。

【図表 3.1.1】 広告検討WG・技術検討WGの実施概要

第三者検証の広告検討WG
<p>【目的】</p> <ul style="list-style-type: none"> ・ 広告配信事業者の視点から、第三者検証に対する意見を収集し、検証における連携体制の在り方について検討する。 ・ アプリプラポリの普及のための広告配信事業者との協力可能性を検討する。 <p>【参加メンバー】</p> <ul style="list-style-type: none"> ・ 広告配信事業者（約6社程度） <p>【実施回数】</p> <ul style="list-style-type: none"> ・ 2014年3月中に2回実施 <p>【検討内容】</p> <ul style="list-style-type: none"> ・ 広告配信事業者ヒアリング結果の共有 ・ 第三者検証での協力の在り方等についての意見交換 ・ 広告モジュールのプラポリの記載および普及啓発についての検討 等
第三者検証の技術検討WG
<p>【目的】</p> <ul style="list-style-type: none"> ・ 第三者検証における解析・表示等の技術面での課題等について構成メンバーで第三者検証の進め方について検討を実施し、具体的な技術検証の実施内容を定める。 <p>【参加メンバー】</p> <ul style="list-style-type: none"> ・ アプリ、アプリプラポリの解析・検証に携わる有識者（約5社程度） <p>【実施回数】</p> <ul style="list-style-type: none"> ・ 2014年3月中に実施 <p>【検討内容】</p> <ul style="list-style-type: none"> ・ 検証におけるアプリの取得の方法、技術検証の手法とリスクおよび第三者検証体制の構築における技術・運用面の課題の洗い出し 等

(出所) 日本総合研究所作成

本調査における、第三者検証の在り方に関する体制として、関連する事業者から意見を収集するために、「広告検討WG」および「技術検討WG」を開催した。広告検討WGは、広告配信事業者を対象として、今後第三者検証実施時の協力体制等について議論を行った。また、技術検討WGに関しては、既にアプリの検証を行っている事業者や、検証について研究を行っている事業者を集め、技術的な観点から第三者検証の進め方等について議論を行った。

3.2 アプリケーションのプライバシーポリシー普及および第三者検証の在り方に関する課題について

ここでは、上記の両 WG の検討結果を基に、アプリプラポリ普及および第三者検証の在り方に関する課題について取りまとめる。

3.2.1 広告検討 WG の検討内容について

広告検討 WG では、広告配信事業者の視点から、第三者検証に対する意見を聴取し、検証においての連携体制の在り方およびアプリプラポリ普及のための広告配信事業者との協力可能性について検討した（実施概要は図表 3.1.1 に記載）。

具体的には、アプリプラポリ普及の観点から、「普及・啓発における協力の可能性」、「広告モジュールのプライバシーポリシーの記載」の検討、第三者検証の在り方の観点から、「第三者検証における協力可能性について」の意見交換を実施した。

本 WG の検討結果について、図表 3.2.1 に取りまとめる。

【図表 3.2.1】 広告検討 WG の検討結果

大項目	小項目	概要
普及・啓発における協力の可能性	「SPI」およびアプリプラポリ作成支援ツールの紹介	<p>「SPI」やアプリプラポリ作成ツールの紹介には前向きな事業者が多いが、利用者からの問合せ対応やツールの利用により発生した問題への対応などの懸念がある。</p> <ul style="list-style-type: none"> ❖ 作成ツール等の紹介では、紹介した責任が発生するため、ルール変更等があった場合に作成ツールのバージョンアップ等の情報管理を実施する必要性が有り、運用方法や責任分解を明確にする必要がある。
広告モジュールのプラポリの記載	広告モジュールのプラポリの必要性	<p>プラポリの作成には総論賛成だが、広告配信事業者のプラポリ作成基準について、アプリ事業者の記載基準と同様にするかの議論は残っている。</p> <ul style="list-style-type: none"> ❖ 利用者の立場に立てば、情報取得・送信がない場合でも、その旨を明記すると分かりやすい。また、アプリプラポリ、広告モジュールのプラポリが一か所にまとまっていると分かりやすいのではないかと懸念している。 ❖ 広告配信事業者のプラポリ項目である「情報の第三者提供」については、利用者から見たときの主語はあくまでアプリ提供事業者であるので、そのあたりは整理が必要であると思料する。
	広告モジュールのプラポリの表示の在り方	<p>アプリ提供者にアプリプラポリの作成やアプリプラポリへの広告モジュールのプラポリのリンク掲載を求めることは難しい。</p> <ul style="list-style-type: none"> ❖ アプリ提供者の中には、アプリプラポリを作成・掲載すると、アプリに対する利用者の不安を煽り、アプリの利用を妨げるのではないかと懸念している事業者も存在している。 ❖ ターゲティング広告の場合にはオプトアウトへの導線確保のために広告枠にマークを表示することが考えられる。しかし、プラポリへの導線用にすべての広告にマークを表示することは考えにくい。
第三者検証における協力可能性	情報収集モジュールのリスト化	<p>広告モジュールを更新した際に、第三者検証主体に更新内容やモジュールのプラポリ、公開可能な範囲でのモジュールの仕様を提供することは可能</p> <ul style="list-style-type: none"> ❖ 広告配信事業者が、適切な情報管理を行っていることを示し、第三者検証を容易にするために、当該事業者がモジュールの更新状況などを提示することは有効である。 ❖ また、上記適切に対応している事業者をリスト化することにより、海外の不適切な

大項目	小項目	概要
		広告配信事業者は利用されなくなりマーケットの自浄作用が働くことも考えられる。
	不適切なアプリへの対応方法	第三者検証主体から不適切なアプリが見つかった際に、広告配信事業者にその旨の連絡があれば、各社が個別で対応することは可能 ❖ 複数事業者が連携して対策を取ることは、現時点では対応が難しい状況にある。

(出所) 日本総合研究所作成

アプリプラポリ普及の観点では、広告配信事業者からアプリ提供者に対して、アプリプラポリの作成を強く要請することが難しい側面があるが、大きな枠組みの中で役割分担を実施することは可能であるとの意見を得た。

また、第三者検証時の協力体制として、情報収集モジュールをリスト化した際、モジュールのアップデートに関して情報を共有することは可能であり、これによって第三者検証主体は、検証にかかるコストの削減が見込まれるという意見を得た。

加えて、第三者検証主体が不適切なアプリを見つけた場合、検証主体がモジュール事業者に連絡をとり、個別に当該アプリに対する対応を依頼することは可能であり、それによってアプリマーケットをより安全に維持することが可能という意見も得た。

3.2.2 技術検討 WG の検討内容について

技術検討 WG では、第三検証を技術的に実施する視点から、第三者検証における解析・表示等の技術面での課題等について検討を実施し、第三者検証を進めるにあたり具体的な技術検証の実施内容を定めることとした（実施概要は図表 3.1.1 に記載）。

本 WG では、第三者検証の実施手法として、「クローリング型」、「申請型」の 2 パターンに分けて検討を実施した。クローリング型は、第三者検証主体がマーケット等からアプリを自動的に抽出し、解析を行う検証手法である。申請型は、アプリ提供者が第三者検証主体にアプリを提供し、第三者検証主体は、受領したアプリのみ検証を行う検証手法である。

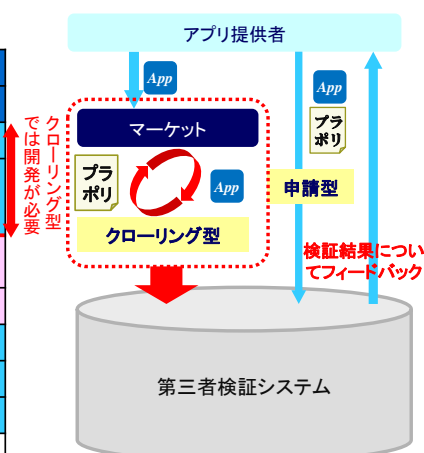
本 WG では、OS 別に、現在どこまで技術検証が可能であるかどうかについて民間で実施されている検証状況の調査を実施し取りまとめた（図表 3.2.2）。その結果、現在、民間で実施されている第三者検証は主に Android の申請型、クローリング型であった。

申請型、クローリング型それぞれにおいて、検証システム構築の範囲や表示の在り方等が異なると共に、現状行われている第三者検証は、Android を主な対象としているため、iOS の第三者検証については多くの技術研究テーマや課題が残るといった意見が、本 WG により挙げられた。

【図表 3.2.2】技術検討 WG の検討結果

機能	第三者検証事業者での実施・研究状況	
	iOS	Android
クローリング (アプリ取得)	【×:実施されていない】	【○:複数の事業者が実施】
簡易解析	【×:実施されていない】 Androidの数倍のコストと時間を要する	【○:複数の事業者が実施】
アプリ プラボリ評価	記載場所探索	【×:実施されていない】
	記載内容評価	【×:実施されていない】
アプリ解析	動的解析	【×:実施されていない】
	静的解析	【○:複数の事業者が実施】
モジュールデータベース	【×:実施されていない】	【○:複数の事業者が実施】
アプリ解析とアプリプラボリ評価の突合	【×:実施されていない】	【△:一部の事業者が実施】
検証結果の表示	【×:実施されていない】 バージョンアップ対応、信頼性設計、偽造マーク対策等が必要	【△:一部の事業者が実施】 バージョンアップ対応、信頼性設計、偽造マーク対策等が必要

(出所) 日本総合研究所作成



3.2.3 課題

スマートフォンアプリケーションを取り巻く事業者・団体を対象とした利用者情報の取扱いやプライバシーポリシーに関する取組についての調査結果ならびに広告検討WGおよび技術検討WGの検討結果を踏まえた今後の課題について整理を行う。

●アプリプラボリ普及に向けた課題について

これまでの検討結果より得られた、アプリプラボリ普及に向けた課題を図表 3.2.3 に取りまとめる。

【図表 3.2.3】アプリプラボリ普及に向けた課題

事業者・団体	アプリプラボリ普及に向けた課題
アプリ提供者	<ul style="list-style-type: none"> ◆アプリプラボリ作成において人的リソースが不足している、または高コスト構造が生じている。 ◆アプリプラボリを詳細に記載することに伴い、利用者の不安を煽るリスクが存在するため、利用者にとって分かりやすい見せ方(表示方法)についても検討が必要。
業界団体	<ul style="list-style-type: none"> ◆団体で作成したガイドラインなどのルールを加盟企業に遵守させることがまだまだ難しい。 ◆加盟企業のプライバシーポリシーに係る取組状況について把握しきれていない。
広告配信事業者	<ul style="list-style-type: none"> ◆広告配信事業者のプライバシーポリシーの作成基準についての検討が必要。 ◆アプリ開発事業者に対して、アプリプラボリ作成を立場上強く要請することは困難である。
第三者検証事業者	<ul style="list-style-type: none"> ◆プライバシーポリシーの第三者検証について明確な基準が定まっていないこともあり、コストなどの問題から少数の事業者しか検証を行っていない。
アプリマーケット 運営事業者	<ul style="list-style-type: none"> ◆マーケットで公開されているアプリにプライバシーポリシーの掲載が不十分なケースがまだ存在する。
その他(プライバシー ポリシー調査等より)	<ul style="list-style-type: none"> ◆SPIの8項目を満たすアプリが少ない。 ◆他国と比べて、アプリプラボリの記載率が低い。

(出所) 日本総合研究所作成

広告検討 WG では、今後の課題として、プラポリ作成基準がまだ不明確であるという意見が得られた。具体的には、広告配信事業者のプラポリ項目である「情報の第三者提供」については、利用者から見たときの主語はあくまでアプリ提供事業者であるので、広告配信事業者としてどのように記載すべきかが不明確であるという意見であった。

今後、広告配信事業者にもプライバシーポリシーの掲載を促す場合、どのような内容を記載し、どのように表示するのかについても検討が必要になると考えられる。

以上を取りまとめると、以下のような課題が残されており、対応について検討が必要である。

- ① アプリ提供者に対してアプリプラポリの作成方法が十分には普及していない。
- ② アプリ提供者側のアプリプラポリの作成にあたる人的リソースが不足しており、コストも高い。
- ③ アプリプラポリの記載内容の検証が未だに困難である。
- ④ 利用者にとって、分かりやすいアプリプラポリの見せ方についての検討が出来ていない。
- ⑤ 利用者に向けた業界一丸となった効果的・効率的なアプリプラポリの普及・啓発が出来ていない。

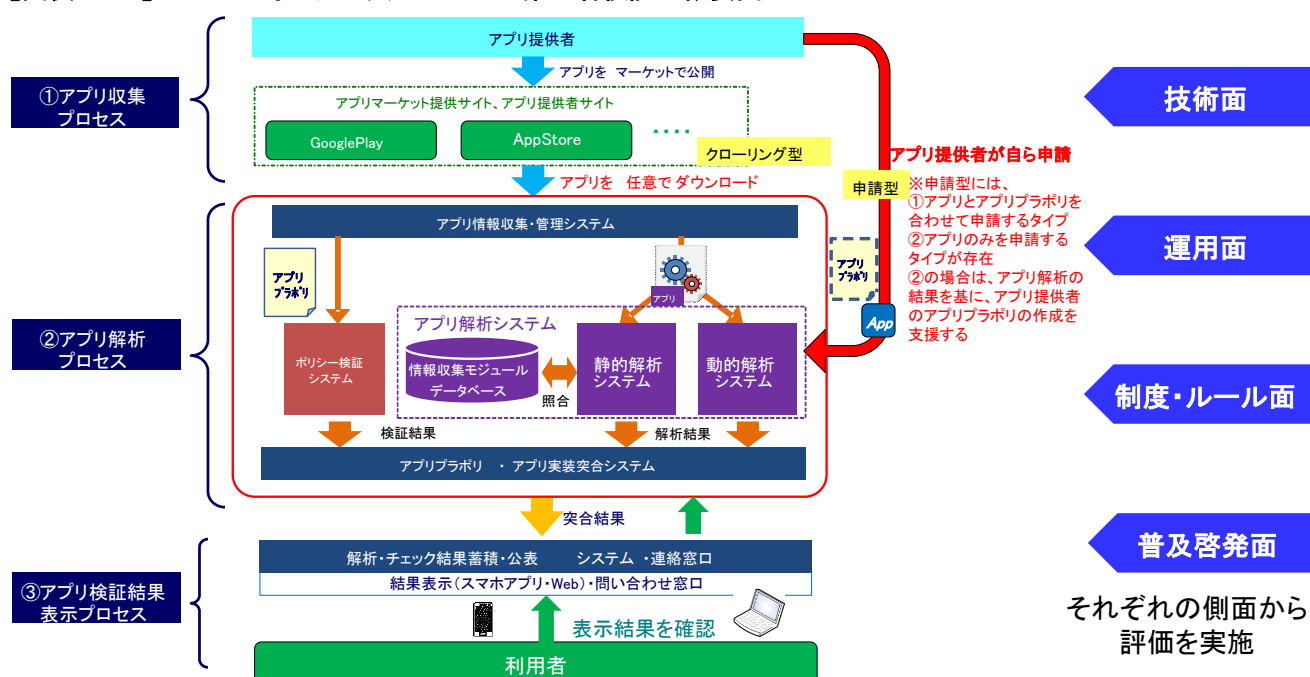
●第三者検証の在り方に関する課題について

ここでは主に技術検討 WG で挙げられた今後の課題について取りまとめる。図表 3.2.4 にスマートフォン上のアプリの第三者検証の概要について記す。アプリの第三者検証のプロセスを大きく分けると「アプリ収集プロセス」、「アプリ解析プロセス」、「アプリ検証結果表示プロセス」の3点に分けられる。アプリ収集プロセスは、先述した「クローリング型」および「申請型」に大別され、アプリ解析プロセスにおいて、アプリプラポリの記載内容とアプリの動作内容の突合解析が行われ、アプリ検証結果表示プロセスにおいて、上記解析結果が利用者に表示される。

アプリ検証結果表示プロセスにおいて、表示方法は、図表 3.2.5 に記載したとおり、「ホワイトリスト・ブラックリスト型」、「レーティング型」に大別され、それぞれにおいてメリット・デメリットが存在し、加えて検証結果の表示場所についてもアプリ内、マーケット上、その他ウェブサイト上など、どこに表示するのが最も適切かという検討課題も存在する。

技術検討 WG では、各プロセスにおいて実際の運用も含めた検討を主に技術的な側面から実施した。その結果、「技術面」、「運用面」、「制度・ルール面」、「普及啓発面」の複数の観点から課題が抽出され、今後第三者検証を進めていくにあたりさらなる検討が必要であることが明らかとなった。それぞれの側面から整理した第三者検証の在り方に関する課題について、図表 3.2.6 にとりまとめる。

【図表 3.2.4】スマートフォンアプリケーションの第三者検証の概要図



(出所) 日本総合研究所作成

【図表 3.2.5】第三者検証結果の表示方法についての整理

表示内容	メリット	デメリット
ホワイトリスト型・ブラックリスト型	・利用者にとって、安全性が分かり易い	・利用者情報の取扱いに対して、ホワイト(ブラック)と判断するための基準設定が困難である ・第三者検証の場合、表示結果が誤っていた場合のリスクがある
レーティング型	・個別のアプリに応じた評価を行い易い ・利用者が自身で利用の可否を判断できる	・利用者にとって安全性を判断しづらい

(出所) 日本総合研究所作成

課題の中で、最も重要な課題として、「運用面」、「制度・ルール面」での課題が挙げられる。

運用面では、今後、官民連携した第三者検証の実証実験を実施していくことが想定されるが、実証実験実施後の出口についても明確にする必要がある。具体的には、「民間で継続的に運用する場合の第三者検証実施主体にどこになるのか」という体制に関する検討や第三者検証の手法およびそれぞれの評価基準の妥当性、審査結果の表示についてのルール化、OS やアプリ更新のタイミングなどによる評価基準の変更などについてのルール化も必要である。

制度・ルール面では、実証実験後の実運用を考えた場合の制度面での課題や業界内での運用ルールについての検討が必要であり、クローリング型の実証実験を行う上でアプリの簡易解析を行う際の制度的課題について知的財産権や著作権の側面から検討する必要がある。また、第三者検証を実施した際の誤謬対策のための信頼性設計についての検討も必要である。

【図表 3.2.6】第三者検証の在り方に関する課題**■技術面での課題**

・Android、iOSにおけるアプリ解析の正確性には技術的限界が残るため、実運用を考えた上で、現実的な検証の水準について一定の評価基準を定めることが重要 等

■運用面での課題

- ・クローリング型と申請型について、第三者検証の手法、評価基準や、検証結果の表示についてルール化が必要
- ・OSやアプリ更新のタイミングにおける第三者検証の対応方法、評価結果の変更等について、運用のルール化も必要
- ・民間で継続的に運用するための第三者検証実施主体についての体制検討が必要 等

■制度・ルール面での課題

- ・実証実験後の実運用を考えた場合の制度面での課題や業界内での運用ルールについての検討が必要 等
- クローリング型の実証実験を行う上でアプリの簡易解析を行う際の制度的課題の検証
- 申請・マーク等付与型における不正対策
- 第三者検証を実施した際の信頼性設計について 等

■普及啓発面での課題

- ・業界一丸となった普及啓発の連携を強化し、一層の推進が必要
- 現在は、個別業界・企業(一部連携して)普及活動を開始しており、取組は進んでいると考えられる。今後も、継続してアプリ提供者および利用者に対しても普及啓発を行っていく必要性が有る。

(出所) 日本総合研究所作成

3.3 アプリケーションのプライバシーポリシー普及および第三者検証の在り方に関する提言について

3.3.1 アプリケーションのプライバシーポリシー普及および第三者検証実証実験に向けて

先述した課題を踏まえ、現状想定される第三者検証の在り方について提言を行う。

アプリプラポリ普及に向けた課題については、前節で①～⑤の課題を挙げたが、整理すると主に①～③までは「アプリ提供者」に向けた普及啓発に係る課題であり、④、⑤については「利用者」に対する普及啓発に係る課題である。

アプリ提供者に向けた普及啓発については、これまで同様、業界団体を含むスマートフォンに係る多様な関係者による普及啓発活動が重要である。

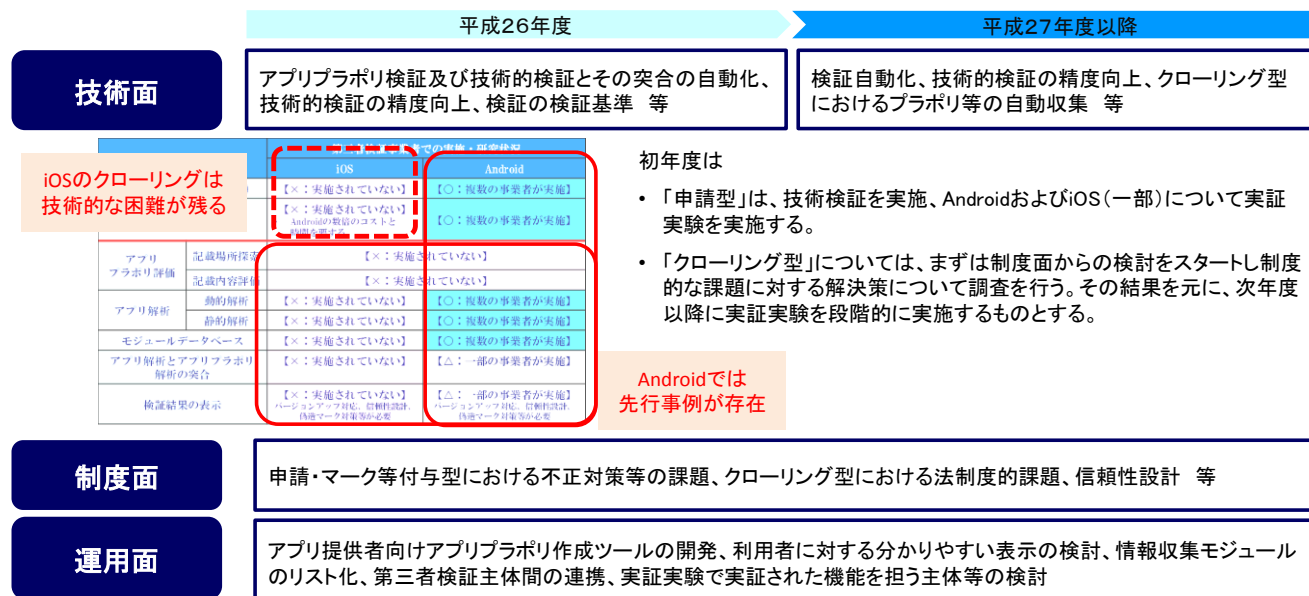
それ以外の周知方法としては、アプリプラポリの自動作成ツールやモデルとなるアプリプラポリの記載事例集などをアプリ提供者に対して提示することによって、上記の①～③に関する課題の解決策になると考えられる。特に、アプリプラポリの自動作成ツールの開発については、アプリの第三者検証において、アプリプラポリの記載内容とアプリの動作の突合検証を実施する上でも、効率よく検証が可能となるメリットもある。

今後より実効性のあるアプリプラポリの普及を行うために、次年度にアプリプラポリ普及および第三者検証実証実験を実施し、本調査で抽出された課題についての具体的な解決方法を開発する必要がある。

図表 3.3.1 に、技術面、制度面、運用面から整理した次年度以降のアプリの第三者検証に係る実証実験の進め方について示す。

技術検討 WG の結果も踏まえると、まず次年度においては、「申請型」を中心に、実証実験を実施するのが妥当であると思料する。「クローリング型」には、前述のとおりアプリ収集時および解析時において、知的財産権や著作権などの制度的な課題や iOS における解析の技術的困難性が想定されるため、まずはアプリ提供者の協力を基に申請型で第三者検証実証実験を実施することが望ましい。

【図表 3.3.1】次年度以降のアプリの第三者検証に係る実証実験の進め方



(出所) 日本総合研究所作成

したがって、次年度は実施のより容易な申請型から開始し、並行してクローリング型の机上で制度面からの検討および iOS に関する机上の技術調査等を実施し、翌年度以降にクローリング型の検証を開始し、

段階的に検討課題を解決し、第三者検証の実運用に向けた準備を行うことが妥当であるとする。

また、実証実験を実施するにあたり、TF と緊密に連携すると共に、制度面や運用面についても検討する WG の設置を行うことも重要と見られる。

3.3.2 第三者検証における検証基準、検証結果の表示方法について

検証結果の表示方法として、「検証基準の設定」と「検証結果の表示方法」の2点について検討する必要がある。第三者検証における検証基準および検証結果の表示方法についての全体概要図を図表 3.3.2 に示す。

検証基準に関して、まず第三者検証で見べきポイントは、

✓ アプリが利用者情報を取得するか否か

である。そもそも利用者情報を取得しないアプリに関しては、最も安全性が高いと考えられる。この場合のアプリプラポリの詳細版の作成についての必要性等に関しては、今後検討する必要がある。

次に、第三者検証で見べきポイントは、

✓ 対象となるアプリが利用者情報を取得する場合、アプリがその情報を外部送信（第三者提供）するか否か

である。利用者情報を第三者提供しない場合は、事業者単独で利用者情報を利用することになるため、アプリプラポリとそのアプリの挙動が一致しているかを評価することが重要である。

一方で、アプリが利用者情報の第三者提供を行う場合、第三者検証主体は、アプリプラポリのみならず、利用者情報の外部送信先に関する調査および評価を行う必要性が出てくる。

例えば情報収集モジュールが組み込まれている場合は、当該モジュールが利用者情報を適切に扱っているか等の調査が必要であり、今後モジュールリストを作成し、当該リストとの照合による調査も必要となると考えられる。

以上のような観点で、アプリプラポリの記載内容とアプリの動作が本当に一致しているかどうかの検証が必要となる。

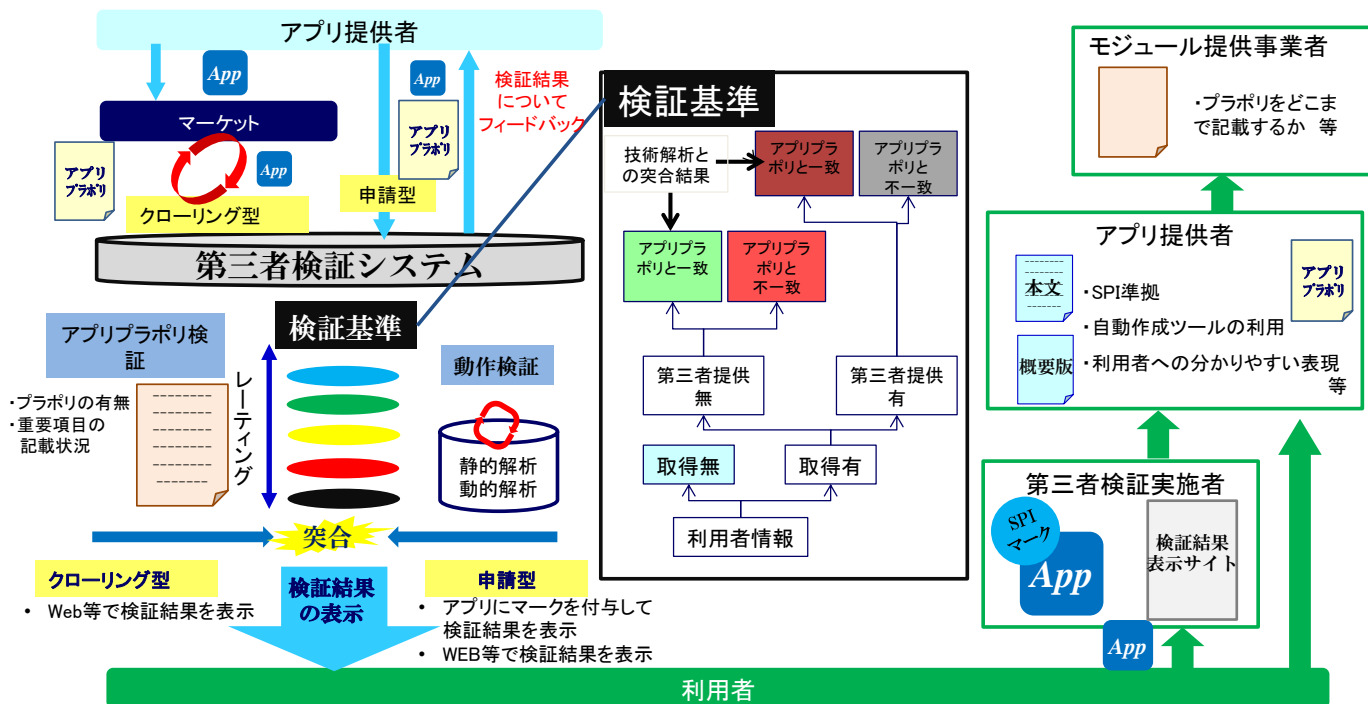
次に、検証結果の表示方法についてであるが、図表 3.3.2 に示すように利用者が検証結果をどこに参照しに行くのか、また、利用者にとって分かりやすい表示方法であるかが重要となる。この点においては、実証実験を実施した上で、利用者も参画した形での評価検証が必要となる。

また、第三者検証結果を表示するシステム概要について図表 3.3.3 に示す。利用者にとって分かりやすい第三者検証結果のマークを表示するにあたり、マークの信頼性の担保が重要となる。例えば、具体的には、第三者検証を受け、評価・認定されたアプリがバージョンアップ後に、審査を受けずマークを表示し続ける、認定されていないアプリがマークを偽造して提示する、等の課題に対応する必要がある。

そこで、第三者検証結果を「ホワイトリストデータベース」に登録しておき、当該データベースに検証結果表示モジュールが随時照合をかけるようなシステムも必要となると考えられる。

以上のような論点を基に、アプリケーションのプライバシーポリシーの作成・掲載および第三者検証を推進し、引き続き利用者にとって安心・安全なスマートフォンの利用環境の整備を図ることが重要である。

【図表 3.3.2】 第三者検証における検証基準および検証結果の表示方法についての全体概要図



(出所) 日本総合研究所作成

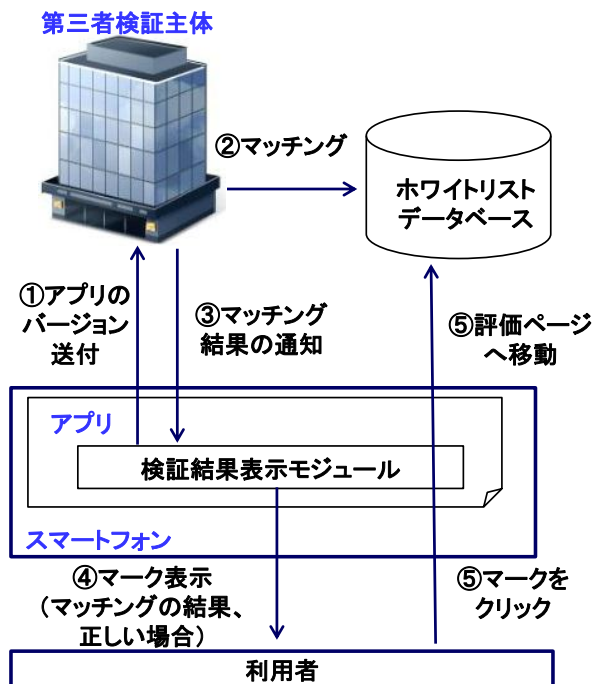
【図表 3.3.3】 第三者検証結果を表示するシステム概要

《ホワイトリスト方式における認定アプリへのマーク提供の課題》

- マークの信頼性の課題
 - ケース①: 認定されたアプリがバージョンアップ後に、審査を受けずマークを表示しつづける。
 - ケース②: 認定されていないアプリがマークを偽造して提示する。

《検証結果表示モジュールについて》

- 検証対象アプリに対して当モジュールをアプリに組み込むと、アプリ起動時やアプリ画面の隅に、認定マークが表示される。
- 検証結果表示モジュールは、起動の度にアプリのバージョンを取得し、第三者検証主体のデータベースと通信し、認定時のバージョンと現在のアプリのバージョンをチェックし、異なる場合にはマーク表示を行わない。
 - バージョンアップしたアプリにモジュールを組みこんでも表示されない。
- アプリに表示されたマークをクリックすると、第三者検証主体の同アプリの評価ページにジャンプできる。
 - 偽マークであれば評価ページに移動できないため、簡単に本物かどうか判断できる。
- 課題として、マークの表示に通信帯域を抑制する手法の検討も必要である。



(出所) 日本総合研究所作成

Appendix1: 自治体提供のスマートフォンアプリのアプリプラポリ作成状況

本節では、自治体が主体となって提供しているアプリの事例と、アプリプラポリの作成・記載状況について記述する。結論として、自治体の提供するアプリの場合、アプリプラポリを作成していないケースが大半である。アプリの内容としてナビゲーション用のアプリ等、位置情報を取得する場合は複数存在するため、アプリプラポリの作成が望ましいと考えられる。






自治体	アプリ名	ディベロッパー名	対応OS	アプリ概要	アプリプラポリの有無
大分県豊後高田市	豊後高田ナビ	吉蔵エックスワイゼットソリューションズ	Android/iOS	豊後高田公式の観光案内アプリ	なし
大阪市西区	きらきら、ぽかぽか。西区ふれあいnavi		Android/iOS	大阪市西区役所公式のナビゲーションアプリ。史跡、散歩ルート等案内。	なし
神奈川県横須賀市	海軍カレー		Android/iOS	須賀集客促進実行委員会(横須賀市横須賀商工会議所 京急電鉄)が開発した、横須賀観光情報の発信、ナビゲーション機能、ロコミ機能による周遊促進、クーポンなどによる店舗利用促進のためのアプリ	なし
京都府南丹市	なないろ 南丹		Android/iOS	南丹市公式観光情報提供アプリ。	なし(初回起動時に位置情報を使用するかどうかを聞かれる)
岐阜県	ミナモクイズ	岐阜県(Gifu Prefectural Government)	iOS	ぎふ清流国体・ぎふ清流大会に関するクイズアプリ	なし
	絵合せミナモ		Android/iOS	神経衰弱のようなゲームアプリ	なし
岡山県岡山市	桃太郎の吉備の国めぐり	岡山市	Android	岡山市が実施したスマホアプリコンテストで最優秀賞を受賞し、市名義で公開したフォトラリーアプリ。	なし
愛媛県新居浜市	新居浜いんふお	Heart Network	Android/iOS	行政情報、災害情報、イベント・環境情報などを提供する新居浜市公式アプリ。	なし
東京都西東京市	西東京市ゴミ分別アプリ	日本グリーンボックス	Android/iOS	西東京市が市民向けに提供するゴミ収集カレンダーアプリ。	なし(アプリ紹介ページにプラポリのリンクがあるが、公式ホームページに飛ぶ)

(出所) 日本総合研究所作成

(2) カスペルスキー

スマートフォン アプリケーションの第三者検証主体リスト

事業者名: カスペルスキー

商品・サービス名	プライバシーアドバイザー(開発中)		
事業者URL	http://www.kaspersky.co.jp/		
対象OS	<input checked="" type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> その他 ()		
対象言語	<input checked="" type="checkbox"/> 日本語 <input checked="" type="checkbox"/> 英語 <input checked="" type="checkbox"/> 中国語 <input checked="" type="checkbox"/> 韓国語 <input type="checkbox"/> その他 (露、仏、独、伊、蘭、北欧系4言語)		
検証したアプリケーションの数	400万件 (マルウェアを含むパッケージ数。2013年)	利用者数	利用顧客数 非公開
検証を行うアプリケーションの取得方法・頻度	<ul style="list-style-type: none"> ■取得方法:自動クローリング、インターネット セキュリティ for Android利用ユーザーからの申請、パートナーからの提出、ユーザー・パートナー以外からの申請 ■取得頻度:都度 ■取得対象:Google Play、サードパーティサイト、スパムメール、パートナーからの提出など 		
検証結果の表示方法	<ul style="list-style-type: none"> ■表示場所:未定 ■結果の表示方法:レーティング型 - リスクを3段階で評価(High、Middle、Low)およびユーザ定義によるホワイトリスト 		
検証基準			
① アプリケーションのプライバシーポリシー(APP)等の作成・公表の有無や掲載場所について検証している。			
<ul style="list-style-type: none"> ● APPを作成しているか ● APPを利用者が容易に参照可能な場所に掲載しているか、アプリケーション内で容易に参照可能であるか 		等	
② アプリケーションのプライバシーポリシーの記載事項・内容について検証している。			
<ul style="list-style-type: none"> ● スマートフォンプライバシーイニシアティブ推奨の8つの事項(※)について必要な内容を記載しているか (※)①アプリ提供者の氏名・名称、②取得情報、③取得方法、④利用目的、⑤通知・公表、同意取得、利用者関与、⑥外部送信・第三者提供・情報収集モジュールの有無、⑦問合せ窓口、⑧プライバシーポリシー変更手続 ● 情報収集モジュールの名称、提供者等 		等	
③ 同意取得に関する事項について検証している。			
<ul style="list-style-type: none"> ● プライバシー性の高い情報を取得するアプリケーションの場合、個別に同意を取得しているか ● 第三者提供を行う場合、あらかじめ本人の同意取得をしているか 		等	
④ 外部送信される利用者情報の有無等について技術的(動的解析・静的解析)に検証している。			
<ul style="list-style-type: none"> ● アプリケーションにより外部送信される利用者情報は何か ● 外部送信される利用者情報の送信先はどこか 		等	<input checked="" type="checkbox"/> 動的解析 <input checked="" type="checkbox"/> 静的解析
⑤ 技術検証結果とアプリケーションのプライバシーポリシーの記載内容との整合性について検証している。			
<ul style="list-style-type: none"> ● APPに記載される利用者情報の項目と、実際に外部送信される利用者情報の項目が合致しているか ● 外部送信される利用者情報の利用目的が明示されているか ● 情報収集モジュールの名前、提供者、送信情報等が合致しているか 		等	

(4) ネットエージェント

スマートフォン アプリケーションの第三者検証主体リスト

事業者名: ネットエージェント

商品・サービス名	secroid		
事業者URL	http://secroid.jp/		
対象OS	<input checked="" type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> その他 ()		
対象言語	<input checked="" type="checkbox"/> 日本語 <input checked="" type="checkbox"/> 英語 <input type="checkbox"/> 中国語 <input type="checkbox"/> 韓国語 <input type="checkbox"/> その他 ()		
検証したアプリケーションの数	1,555,314 件 ()	種類	利用者数 1ヶ月の平均 UU/day 4,226
検証を行うアプリケーションの取得方法・頻度	<ul style="list-style-type: none"> ■ 取得方法: 自動クロール ■ 取得頻度: 毎日 (バージョンアップの場合は自動検知で都度、実施) ■ 取得対象: Google Play (日本、米国)、非公式マーケット <ul style="list-style-type: none"> - Google Playでは、新着アプリ、人気のアプリ、売上TOP、Googleのおすすめを毎日検証 		
検証結果の表示方法	<ul style="list-style-type: none"> ■ 表示場所: アプリの検索エンジンに登録およびWebサイトに掲示 <ul style="list-style-type: none"> - 同サイトで、利用者がアプリ名を入力すれば、該当するアプリのリスクが表示される ■ 結果の表示方法: レーティング型 <ul style="list-style-type: none"> - リスクを5段階で評価 (DANGER、HIGH、MID、LOW、SAFE) 		
検証基準			
① アプリケーションのプライバシーポリシー (APP) 等の作成・公表の有無や掲載場所について検証している。			
<ul style="list-style-type: none"> ● APPを作成しているか ● APPを利用者が容易に参照可能な場所に掲載しているか、アプリケーション内で容易に参照可能であるか 			等 <input type="checkbox"/>
② アプリケーションのプライバシーポリシーの記載事項・内容について検証している。			
<ul style="list-style-type: none"> ● スマートフォンプライバシーイニシアティブ推奨の8つの事項(※)について必要な内容を記載しているか (※)①アプリ提供者の氏名・名称、②取得情報、③取得方法、④利用目的、⑤通知・公表、同意取得、利用者関与、⑥外部送信・第三者提供・情報収集モジュールの有無、⑦問合せ窓口、⑧プライバシーポリシー変更手続 ● 情報収集モジュールの名称、提供者等 			等 <input type="checkbox"/>
③ 同意取得に関する事項について検証している。			
<ul style="list-style-type: none"> ● プライバシー性の高い情報を取得するアプリケーションの場合、個別に同意を取得しているか ● 第三者提供を行う場合、あらかじめ本人の同意取得をしているか 			等 <input type="checkbox"/>
④ 外部送信される利用者情報の有無等について技術的(動的解析・静的解析)に検証している。			
<ul style="list-style-type: none"> ● アプリケーションにより外部送信される利用者情報は何か ● 外部送信される利用者情報の送信先はどこか 			等 <input checked="" type="checkbox"/> 動的解析 <input checked="" type="checkbox"/> 静的解析
⑤ 技術検証結果とアプリケーションのプライバシーポリシーの記載内容との整合性について検証している。			
<ul style="list-style-type: none"> ● APPに記載される利用者情報の項目と、実際に外部送信される利用者情報の項目が合致しているか ● 外部送信される利用者情報の利用目的が明示されているか ● 情報収集モジュールの名前、提供者、送信情報等が合致しているか 			等 <input type="checkbox"/>
備考: セキュロイドの解析システムを利用した、開発者向けのアプリ検証サービスを有償(1回3,000円)で提供している。			

調査研究担当者

株式会社 日本総合研究所
総合研究部門 リサーチ・コンサルティング事業部
戦略コンサルティング部

融合戦略クラスター
クラスター長 東 博暢
研究員 前田 裕文

通信メディア・ハイテク戦略クラスター
研究員 小竹 庸平