

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調査・分析の請負

～スマートフォン プライバシー アウトルックV～

3月28日

株式会社日本総合研究所

1. 背景

- ・ 総務省の「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」の議論を経て、平成24年8月、アプリケーション(以下「アプリ」)ごとのプライバシーポリシー(以下「プラポリ」)の作成・掲載等を提言内容とする「スマートフォン プライバシー イニシアティブ」(以下「SPI」)が公表され、平成25年9月には、利用者情報の適正な取扱いの実効性を確保するために、運用面・技術面から第三者がアプリを検証する仕組みを民間主導で推進すること等を提言内容とする「スマートフォン プライバシー イニシアティブⅡ」(以下「SPIⅡ」)が公表された。
- ・ 総務省のタスクフォースにおける議論を踏まえ、平成25年度はアプリの利用者情報取扱い実態調査や関係団体の取組等の検討結果が「スマートフォン プライバシー アウトルック」(以下「SPO」)として取りまとめられた。平成26年度は引き続き実施したアプリの利用者情報取扱い実態調査の結果、平成26年度から実施された第三者検証に係る実証実験の結果等が「スマートフォン プライバシー アウトルックⅡ」(以下「SPOⅡ」)として取りまとめられた。平成27年度も引き続き実施したアプリの利用者情報取扱い実態調査の結果、第三者検証に係る実証実験の結果等が「スマートフォン プライバシー アウトルックⅢ」(以下「SPOⅢ」)として取りまとめられた。平成28年度も「スマートフォン プライバシー アウトルックⅣ」として引き続き実施したアプリの利用者情報取扱い実態調査の結果、第三者検証システムの運用設計・最適化の実証実験結果、民間、諸外国の取組状況調査の取組状況を取りまとめられた。また、平成28年度は個人情報保護法の改正や平成26年～28年までの第三者検証に係る実証実験等を踏まえて、関係事業者等の役割分担の明確化や取組の具体化等を目的として、「スマートフォン プライバシー イニシアティブⅢ」にこれまでの検討内容を取りまとめた。
- ・ 平成29年度も引き続き実施したアプリの利用者情報取扱い実態調査の結果、民間、諸外国の取組状況調査を、「スマートフォン プライバシー アウトルックⅤ」として取りまとめた。

平成29年度の調査内容

アプリケーションの
利用者情報取扱い実態調査

民間や諸外国における
取組状況調査

2.1.アプリプラポリ調査 調査概要①～調査対象～

Android、iOSのアプリを対象とし、国内の①人気アプリ(各OS：100アプリ)と②新着アプリ(各OS：50アプリ)、③海外の人気アプリ(各OS:50アプリ)についてアプリケーションのプライバシーポリシー(アプリプラポリ)調査を実施した。

また、今年度から、国内・海外の情報収集モジュール事業者(国内・海外10社ずつ)を対象として、プラポリの作成・掲載状況、プラポリの記載内容を新たに調査した。

【調査目的】

- ・SPIにおけるスマートフォン利用者情報取扱指針を踏まえ(※)、アプリプラポリの作成・掲載等の実態を調査する。
- (※)スマートフォンにおける利用者情報を取得するアプリ等については、取得情報の項目や利用目的、外部送信の有無等といった8項目について明示するプラポリを作成し、利用者が容易に参照できる場所に当該プラポリを掲示することが望ましい旨が記載されている。(SPIの59ページ参照)

【調査対象】

アプリケーションのプラポリに関する調査			今年度から新たに追加 情報収集モジュール提供者 のプラポリに関する調査
国内		海外(米国・英国)	④国内外の情報収集モジュール事業者
①国内人気アプリ	②国内新着アプリ	③海外人気アプリ	
対象 サンプル数	計200アプリ (Android:100、iOS:100)	計100アプリ (Android:50、iOS:50)	計20社 (国内:10、海外:10)
抽出基準	アプリマーケットの無料アプリの ランキングから上位100アプリを 抽出※1	新着アプリの中から50アプリを 抽出※2	過去のアプリプラポリ調査及び今 回の調査で取得したアプリプラポリ に記載されていた事業者を抽出
抽出日※3	2017年11月	2017年11月	2018年1月

※1 「App Annie」から2017年11月20日の「Google Play」、「App Store」の日本の無料ランキングにおける上位100アプリを抽出。調査実施時にアプリがマーケットから削除されていた場合には繰り上げを行い抽出した。

※2 Androidの新着アプリは「App Annie」から2017年11月20日の「Google play」の新着無料ランキングの200位～250位を抽出(①の無料ランキングの重複を避けるため)。iOSの新着アプリはiPhone・iPod touchアプリの様々な情報の配信サイト「CatchApp」の新着アプリ一覧からリリース日が2017年11月20日以前のアプリを抽出。調査実施時にアプリがマーケットから削除されていた場合には繰り上げを行い抽出した。

※3 「App Annie」から2017年11月20日の「Google Play」、「App Store」の米国と英国の無料ランキングにおける上位アプリを抽出し、OS別に両国のランキングで共通する50アプリを抽出。調査実施時にアプリがマーケットから削除されていた場合には繰り上げを行い抽出した。

2.1.アプリプラポリ調査 調査概要②～調査項目～

調査項目は【1】プラポリの作成・掲載状況、【2】SPIで示される8項目の記載状況、【3】利用者情報の取得に関する同意取得状況、【4】プラポリの概要版作成・公表状況 の4つである。

【1】については昨年度までの調査の考察を踏まえて、分類を詳細化した(詳細は次ページ)。【3】についてはOSの仕様変更に合わせて、昨年度から調査内容と調査対象の変更を行った。

【調査項目】

大項目	小項目
【1】プラポリの作成・掲載状況	【1-1】プラポリの掲載率(「アプリ紹介ページ内」、「アプリ内」の2か所の掲載率) 【1-2】プラポリの記載内容の分類⇒ 分類を一部細分化(次ページ参照) 【1-3】プラポリの掲載階層(アプリのトップ画面から何タッチで遷移できる場所にプラポリがあるか)
【2】 SPIで示される8項目※1の記載状況	【2-1】プラポリにおけるSPIで示された8項目の記載有無
【3】利用者情報の取得に関する同意取得状況 (Android・iOS両方を対象⇒ 範囲拡張) ※OSの仕様変更により各アプリの取得する情報が 端末の設定で確認できるようになったため	【3-1】電話番号、メールアドレス、位置情報、アドレス帳の取得する可能性の有無 【3-2】プラポリの中での情報取得の記載有無(プラポリの取得情報の中に、取得する可能性のある情報が記載されているか)
【4】プラポリの概要版作成・公表状況	【4-1】プラポリの概要版の掲載率(「アプリ紹介ページ内」、「アプリ内」の2か所の掲載率)

※1 【SPIで示される8項目】①情報を取得するアプリ提供者等の氏名または住所、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、⑤通知・公表又は同意取得の方法、利用者関与の方法 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の変更を行う場合の手続き

【調査対象別の調査項目】

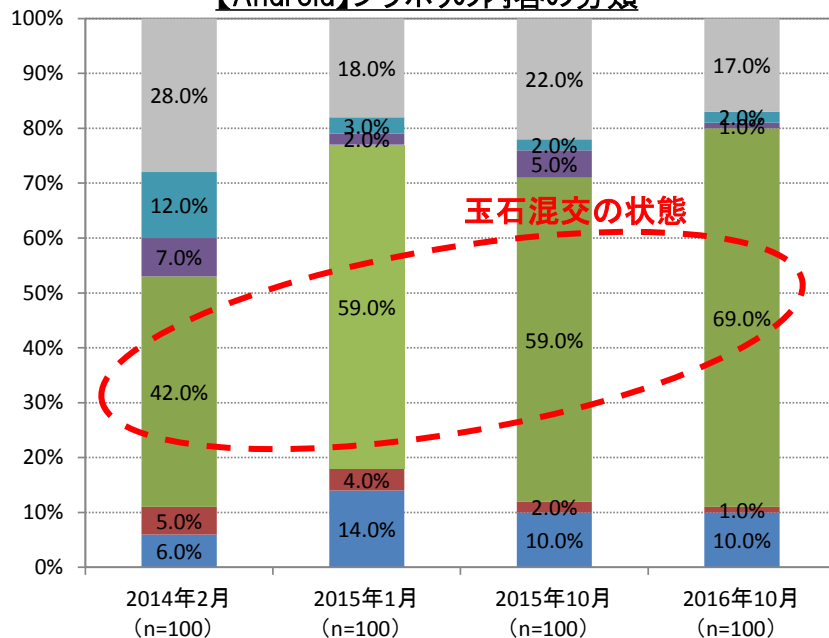
	国内		海外(米国・英国)	④国内外の情報収集モジュール事業者
	①国内人気アプリ	②国内新着アプリ	③海外人気アプリ	
【1】	○:実施	○:実施	○:実施	△:一部実施(ウェブページにおける掲載有無のみを評価、掲載階層の評価は行わない※2)
【2】	○:実施	○:実施	○:実施	○:実施
【3】	○:実施	○:実施	○:実施	×:実施しない(技術的に不可能)
【4】	○:実施	○:実施	○:実施	○:実施

※2 情報収集モジュール事業者のプラポリは、アプリプラポリにリンクが掲載され、閲覧される形を想定しているため、階層という概念がそぐわない。

(参考) プラポリの分類の細分化の背景(昨年度の【1-2】プラポリの内容の分類)

プラポリの記載内容の分類に関する過去の調査結果では、全体の5割以上が分類「C」に該当する結果になっており、また、分類「C」の中には「スマホアプリを意識した記載」のプラポリや「全くスマホアプリを意識していない記載」のプラポリが混在していた。そのため、分類「C」を「スマホアプリ」を意識した記載の有無で細分化した。

【Android】プラポリの内容の分類



- 【A】 個々のスマホアプリ専用のプラポリが用意されている
- 【B】 サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない
- 【D】 一般的なWebサイトのプラポリがあるだけ
- 【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】 プラポリが記載されていない

【「C」の分類基準】

- ◆ 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

「スマホアプリ」を意識した記載の有無で細分化

【「C-1」の分類基準】※スマホアプリを意識した記載有り

- ◆ アプリ提供者が提供する複数アプリ/全アプリを対象としたプライバシーポリシーが提供されている
又は
- ◆ サービス全体のプライバシーポリシーがあり、その中にスマホアプリを意識した記載になっている

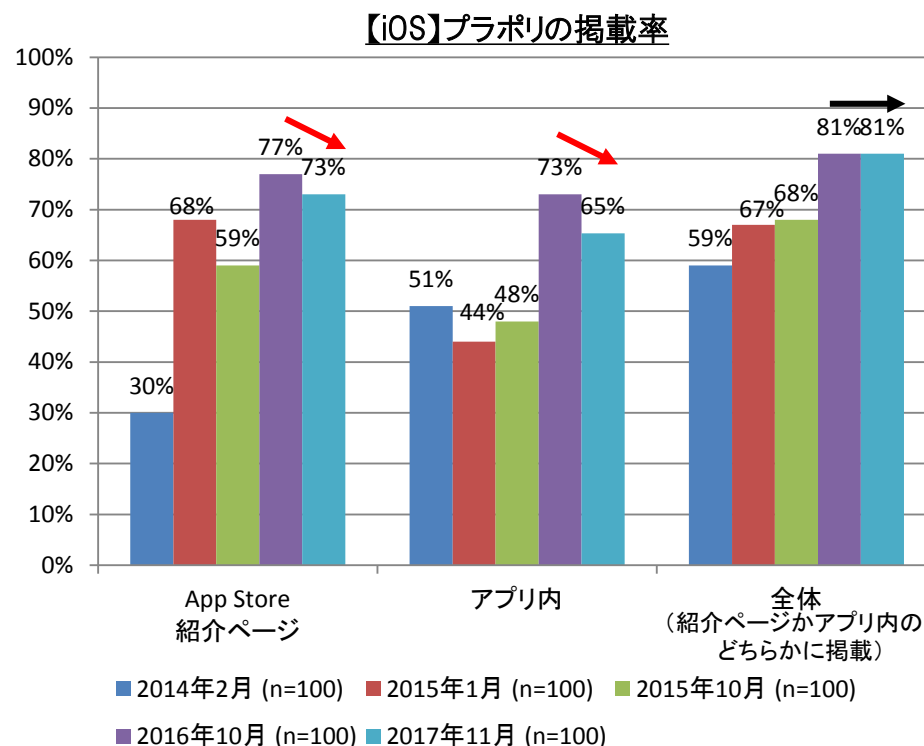
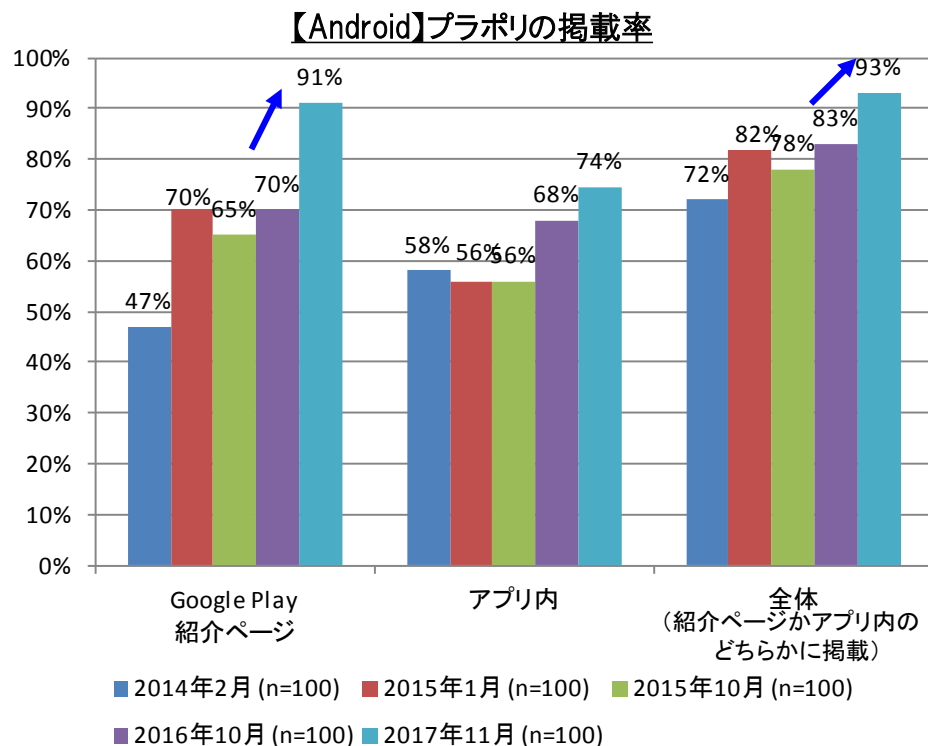
【「C-2」の分類基準】※スマホアプリを意識した記載無し

- ◆ サービス全体のプライバシーポリシーがあり、その中にスマホアプリを意識した記載が一切ない
(企業活動やサービス提供の中で取得した一般的な個人情報の取扱いに関する記載のみ)

2.2.アプリプラポリ調査 調査結果(①国内人気アプリ:【1-1】プラポリの掲載率)

Androidにおける「全体」の掲載率は93%であり、昨年度よりも10ポイントの増加(特に「紹介ページ」の掲載率が伸びている)。

iOSにおける「全体」の掲載率は81%であり、昨年度からは横ばいで推移。



※掲載率:以下の「A」から「F」までのうち、「F」判定以外であれば、「プラポリ有り」と判断。

(「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない)

A: 個々のスマホアプリ専用のプラポリが用意されている。B: サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない。D: 一般的なWebサイトのプラポリがあるだけ。

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: プラポリが記載されていない。

※紹介ページの掲載率:「紹介ページのリンク」が「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。

※アプリ内の掲載率:「初回起動時」又は「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。

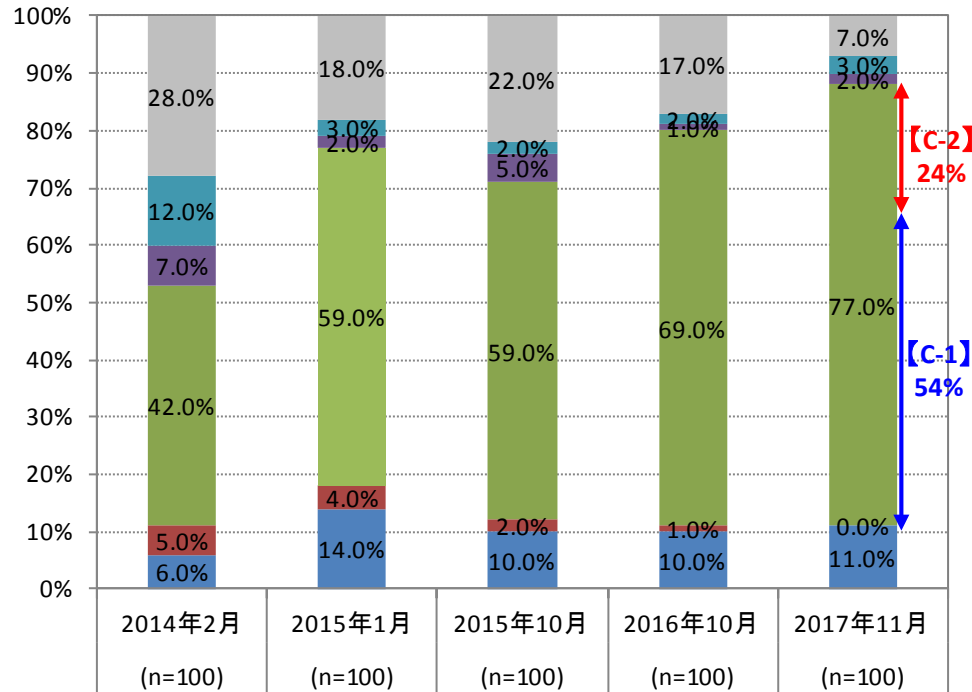
※全体の掲載率:「紹介ページ」又は「アプリ内」のどちらかが「F」以外の判定となったアプリの割合。

2.2.アプリプラポリ調査 調査結果(①国内人気アプリ:【1-2】プラポリの内容の分類)

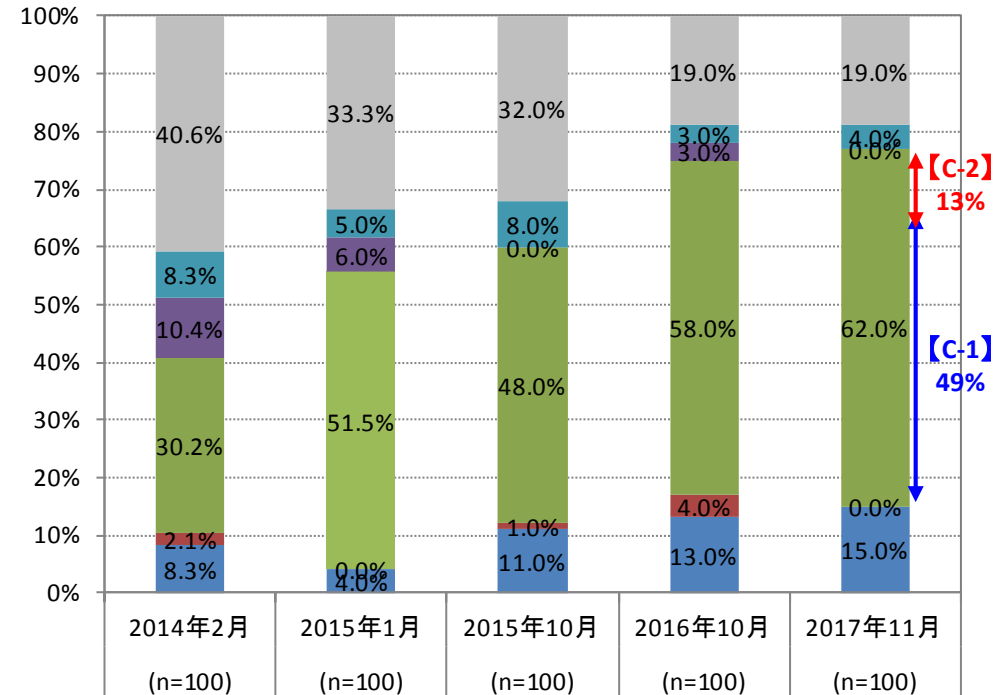
Android・iOSともに、プラポリの掲載率が伸びたものの(【F】の減少)、個々のスマホアプリ向けのプラポリ(【A】・【B】)の割合は伸びず、サービス全体のプラポリ(【C】)の割合が増加しており、全体の6割～7割が【C】に分類される。

分類【C】を細分化した結果、Android・iOSともに分類【C】における大半のプラポリがスマホアプリを意識した記載になっていた。

【Android】プラポリの内容の分類



【iOS】プラポリの内容の分類



■ 【A】 個々のスマホアプリ専用のプラポリが用意されている

■ 【B】 サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない

■ 【D】 一般的なWebサイトのプラポリがあるだけ

■ 【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】 プラポリが記載されていない

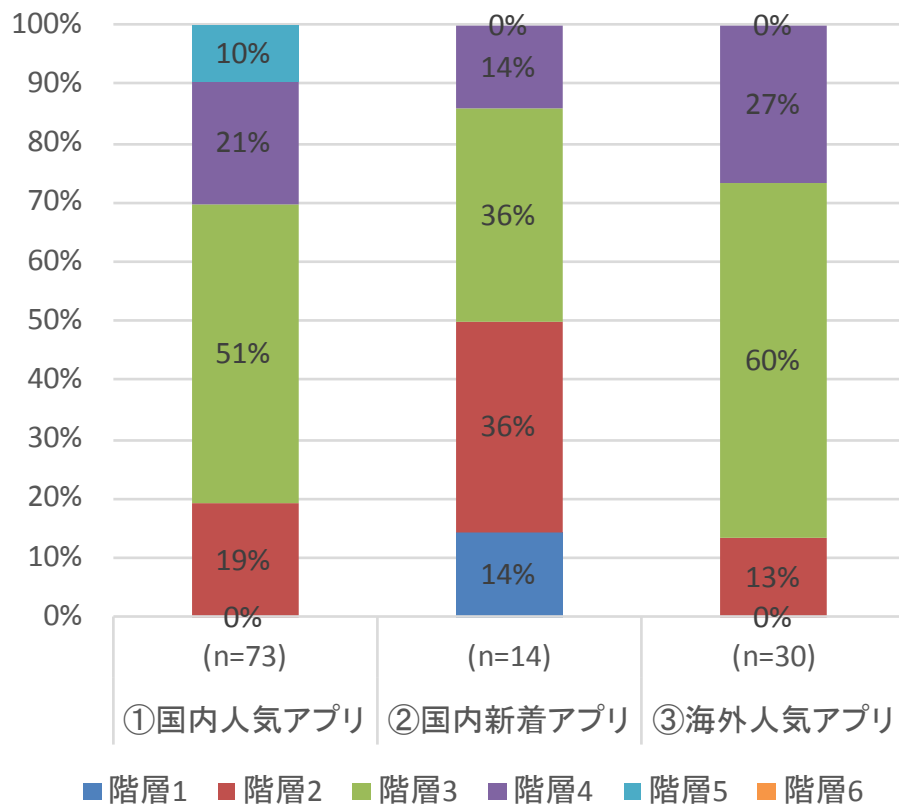
【C-1】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっている。(【C】の中で【A】・【B】に近い)

【C-2】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっていない。(【C】の中で【D】・【E】に近い)

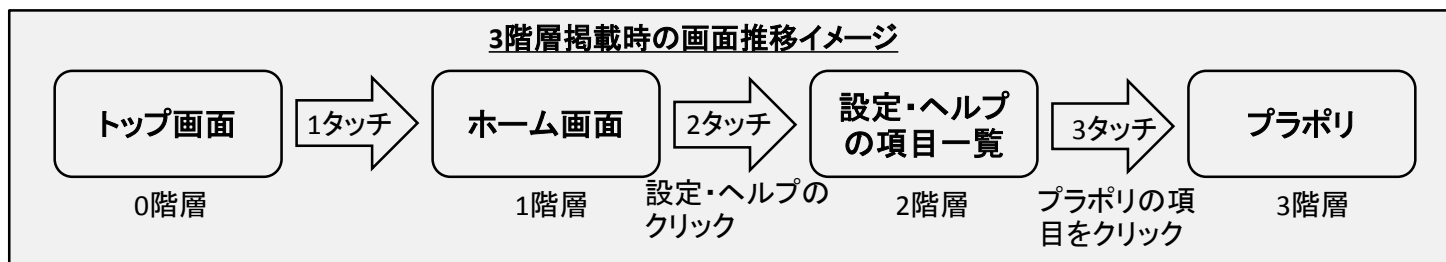
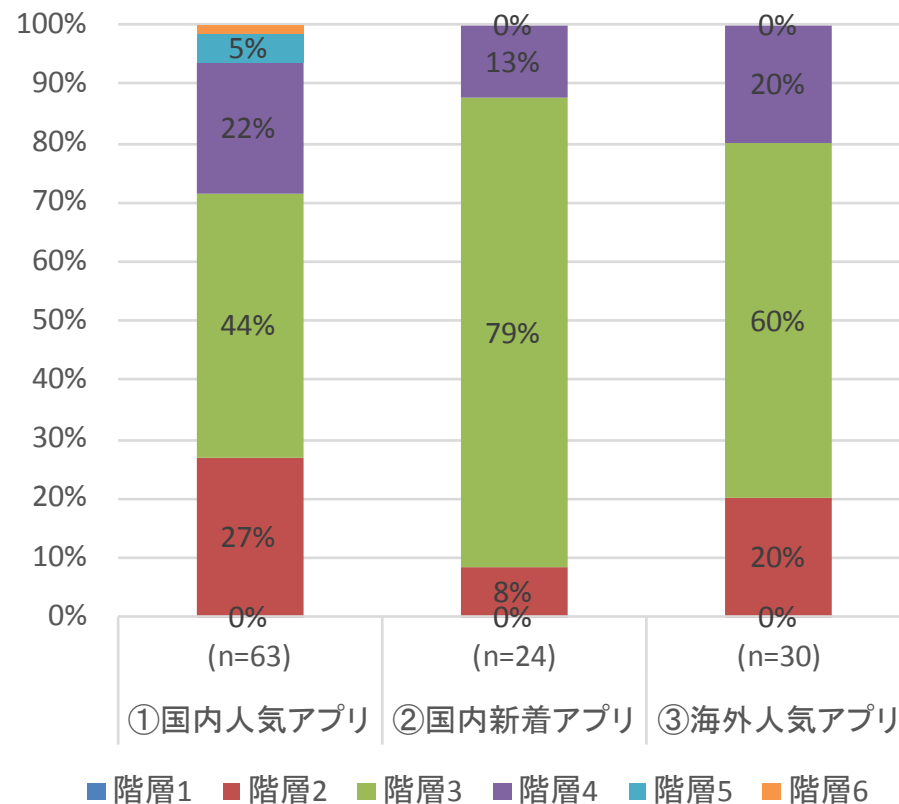
2.2.アプリプラポリ調査 調査結果(全アプリ:【1-3】プラポリの掲載階層)

OSや調査対象に関係なく、7割程度のアプリが3階層以内(アプリのトップ画面から3タッチ以内に遷移できる場所)にプラポリを掲載している。最も主流の掲載階層は3階層(トップ画面⇒ホーム画面⇒設定・ヘルプの項目一覧⇒プラポリ掲載画面)。

【Android】アプリ内のプラポリの掲載階層



【iOS】アプリ内のプラポリの掲載階層



2.2.アプリプラポリ調査 調査結果(①国内人気アプリ:【2】SPI8項目の記載率)

Android・iOSともにSPI8項目の中で重要性が高い4項目(水色の項目)の記載率に大きな変化はない(一部の項目のみ増減)。

SPI8項目の記載率※

番号	項目	Android		iOS	
		2016年10月 (n=83)	2017年11月 (n=93)	2016年10月 (n=81)	2017年11月 (n=81)
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	98%	98%	100%	100%
②	取得される情報の項目	89%	87%	80%	93%
③	取得方法	33%	55%	47%	60%
④	利用目的の特定・明示	87%	92%	95%	95%
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	22%	31%	17%	33%
	利用者情報の削除の記載	47%	58%	59%	60%
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	89%	90%	84%	93%
	利用者情報の送信先の記載	34%	27%	46%	32%
	情報収集モジュールに関する記載	23%	22%	22%	25%
⑦	問合せ窓口	86%	87%	79%	85%
⑧	プライバシーポリシーの変更を行う場合の手続き	55%	60%	61%	62%

SPI8項目において、特に重要性が高いと考えられる項目

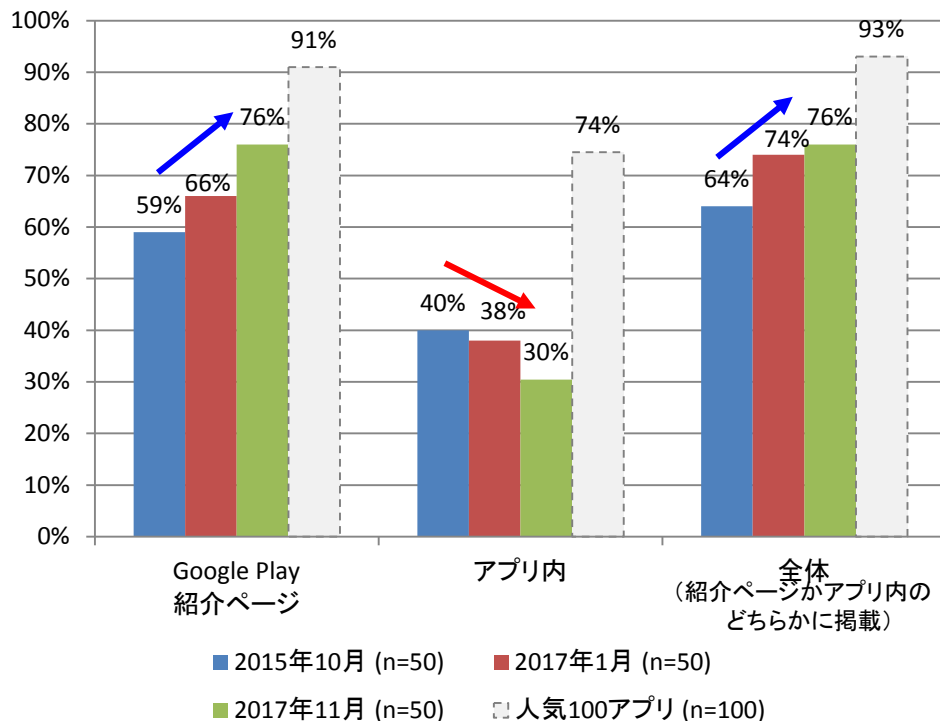
※プラポリが存在していたアプリ数を母数として割合を算出。

特に重要性が高い項目の中で、昨年度から記載率が5ポイント以上増加(青枠)、減少(赤枠)している箇所

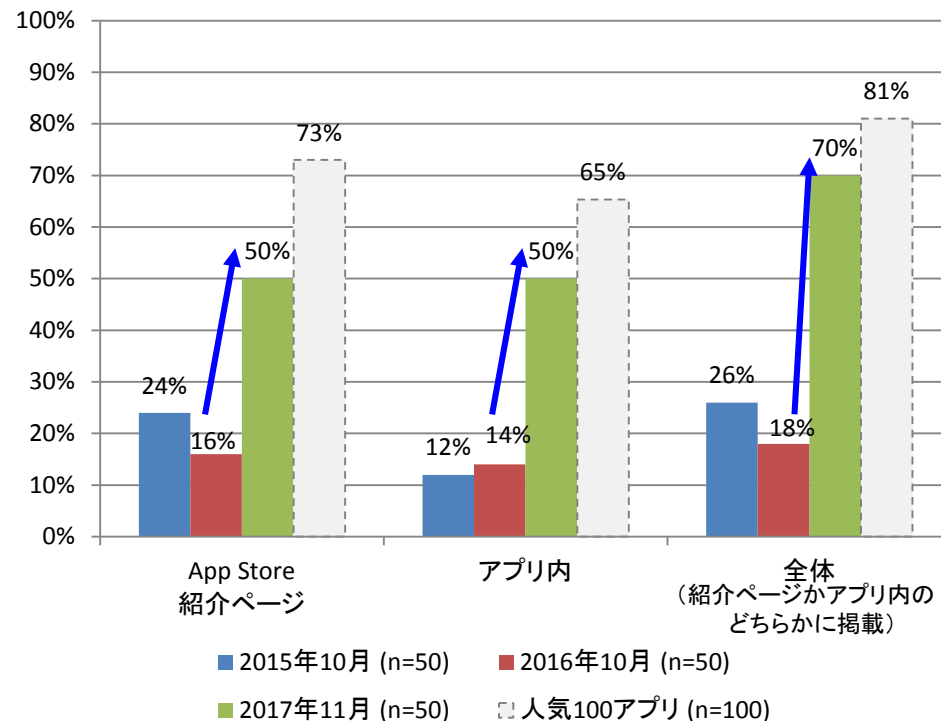
2.2.アプリプラポリ調査 調査結果(②国内新着アプリ:【1-1】プラポリの掲載率)

Android・iOSともに「全体」及び「紹介ページ」のプラポリ掲載率は増加している。特にiOSは掲載率が倍増している。また、新着アプリと人気アプリの掲載率の差も埋まりつつある。

【Android】プラポリの掲載率



【iOS】プラポリの掲載率



※掲載率:「F」判定以外であれば、「プラポリ有り」と判断。

(「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない)

A: 個々のスマホアプリ専用のプラポリが用意されている。B: サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない。D: 一般的なWebサイトのプラポリがあるだけ。

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: プラポリが記載されていない。

※紹介ページの掲載率:「紹介ページのリンク」か「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。

※アプリ内の掲載率:「初回起動時」又は「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。

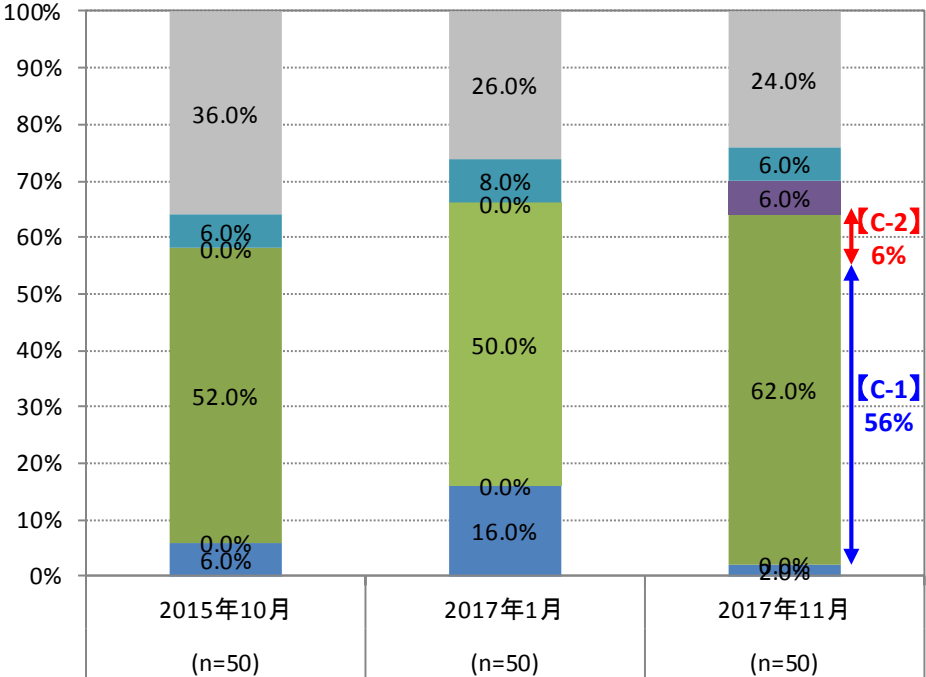
※全体の掲載率:「紹介ページ」又は「アプリ内」のどちらかが「F」以外の判定となったアプリの割合。

2.2.アプリプラポリ調査 調査結果(②国内新着アプリ:【1-2】プラポリの内容の分類)

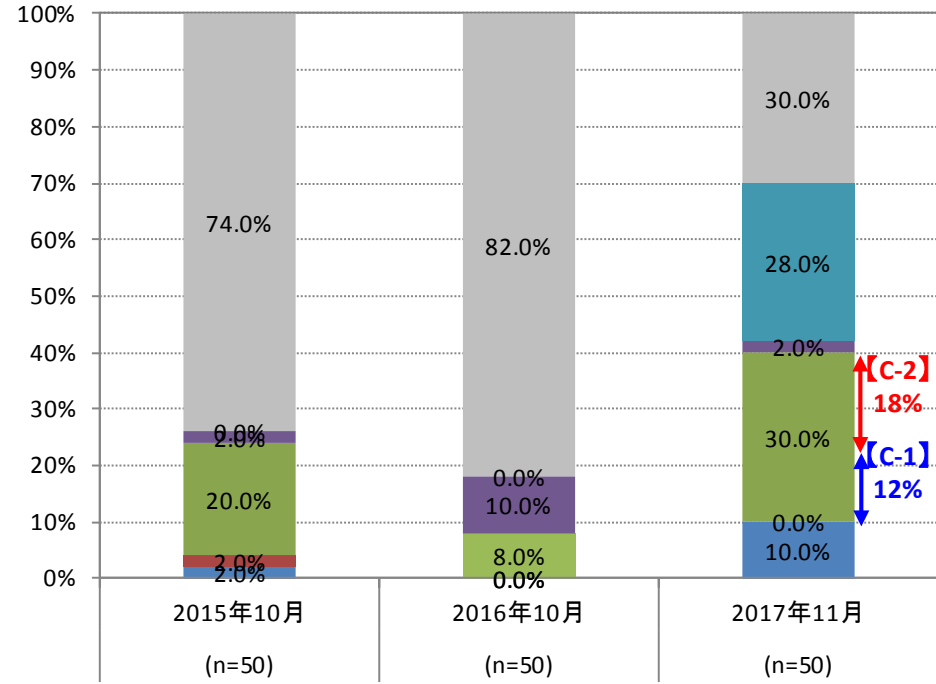
Androidでは、個々のアプリについて記載されたプラポリ(【A】・【B】)の割合が大幅に減少し、代わりに【C】の割合が増えている。ただし、【C】に該当するプラポリの9割がスマホアプリを意識した記載(【C-1】)に該当した。

iOSでは、掲載率は伸びたものの、スマホアプリを意識した記載になっていないプラポリ(【C-2】・【D】・【E】)の割合が高い。

【Android】プラポリの内容の分類



【iOS】プラポリの内容の分類



- 【A】 個々のスマホアプリ専用のプラポリが用意されている
- 【B】 サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない
- 【D】 一般的なWebサイトのプラポリがあるだけ
- 【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】 プラポリが記載されていない

【C-1】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっている。(【C】の中で【A】・【B】に近い)

【C-2】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっていない。(【C】の中で【D】・【E】に近い)

2.2.アプリプラポリ調査 調査結果(②国内新着アプリ:【2】SPI8項目の記載率)

Androidでは「④利用目的」や⑥の「情報の送信先」が伸びているものの、⑥の「第三者への送信有無」・「モジュール有無」の記載率が減少している。人気アプリとの比較ではほぼ遜色ない記載率。iOSでは「④利用目的」の記載率が減少し、⑥の「モジュール有無」の記載率が増加している。人気アプリとの各項目の記載率の差は大きい。

SPI8項目の記載率※

番号	項目	Android			iOS		
		新着アプリ		人気アプリ (2017年11月、 n=93)	新着アプリ		上位100アプリ (2016年10月、 n=81)
		2017年1月 (n=74)	2017年11月 (n=76)		2015年10月 (n=18)	2016年10月 (n=70)	
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	97%	97%	98%	100%	100%	100%
②	取得される情報の項目	78%	76%	87%	44%	40%	93%
③	取得方法	46%	55%	55%	22%	26%	60%
④	利用目的の特定・明示	68%	92%	92%	67%	57%	95%
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		31%	11%	6%	33%
		利用者情報の削除の記載		58%	32%	46%	60%
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		90%	89%	57%	93%
		利用者情報の送信先の記載		27%	14%	11%	32%
		情報収集モジュールに関する記載		22%	32%	9%	25%
⑦	問合せ窓口	78%	89%	87%	44%	60%	85%
⑧	プライバシーポリシーの変更を行う場合の手続き	49%	58%	60%	0%	31%	62%

SPI8項目において、特に重要性が高いと考えられる項目

※プラポリが存在していたアプリ数を母数として割合を算出。

特に重要性が高い項目の中で、昨年度から記載率が5ポイント以上増加(青枠)、減少(赤枠)している箇所

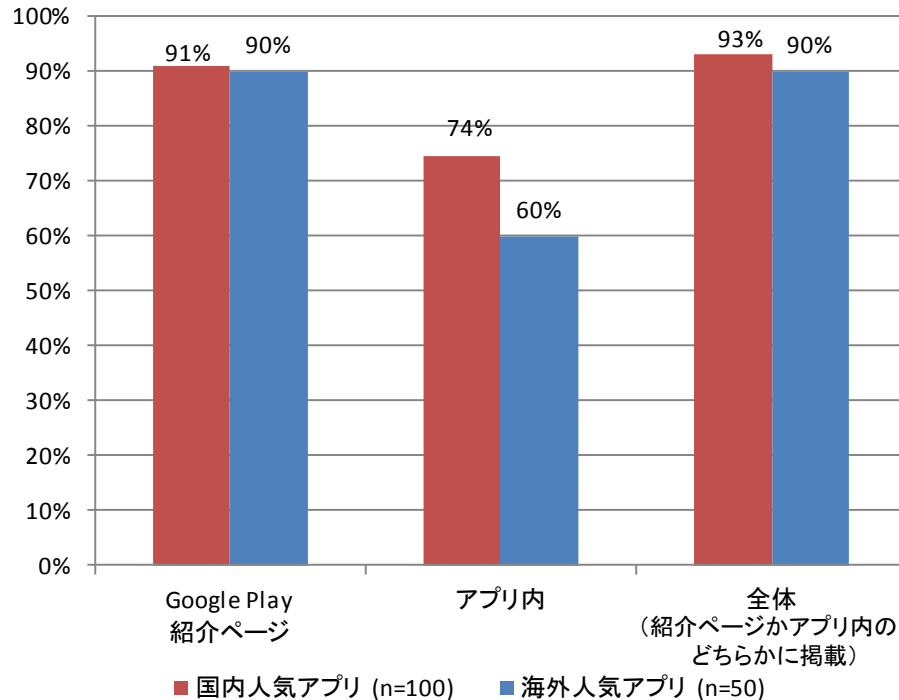
特に重要性が高い項目の中で、人気アプリの方が5ポイント以上高い項目

2.2.アプリプラポリ調査 調査結果(①国内人気アプリ・③海外人気アプリ:【1-1】プラポリの掲載率)

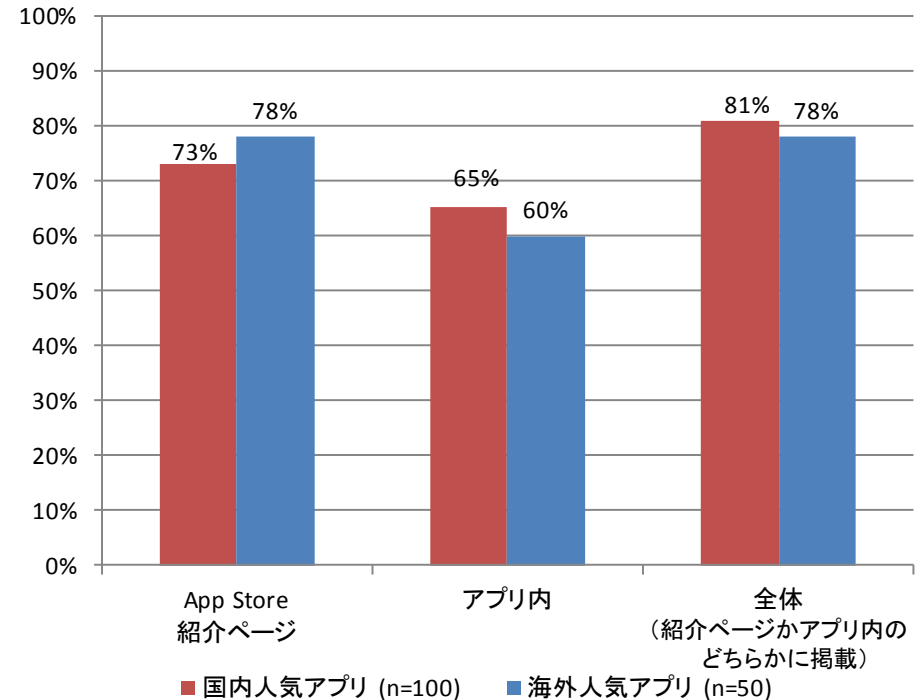
Android・iOSともに、「全体」でのプラポリ掲載率に差は殆ど無い。

「アプリ内」の掲載率については、Android・iOSともに①国内人気アプリの方が高い傾向にある。

【Android】プラポリの掲載率の比較



【iOS】プラポリの掲載率の比較



※掲載率:「F」判定以外であれば、「プラポリ有り」と判断。

(「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない)

A: 個々のスマホアプリ専用のプラポリが用意されている。B: サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない。D: 一般的なWebサイトのプラポリがあるだけ。

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: プラポリが記載されていない。

※紹介ページの掲載率:「紹介ページのリンク」か「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。

※アプリ内の掲載率:「初回起動時」又は「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。

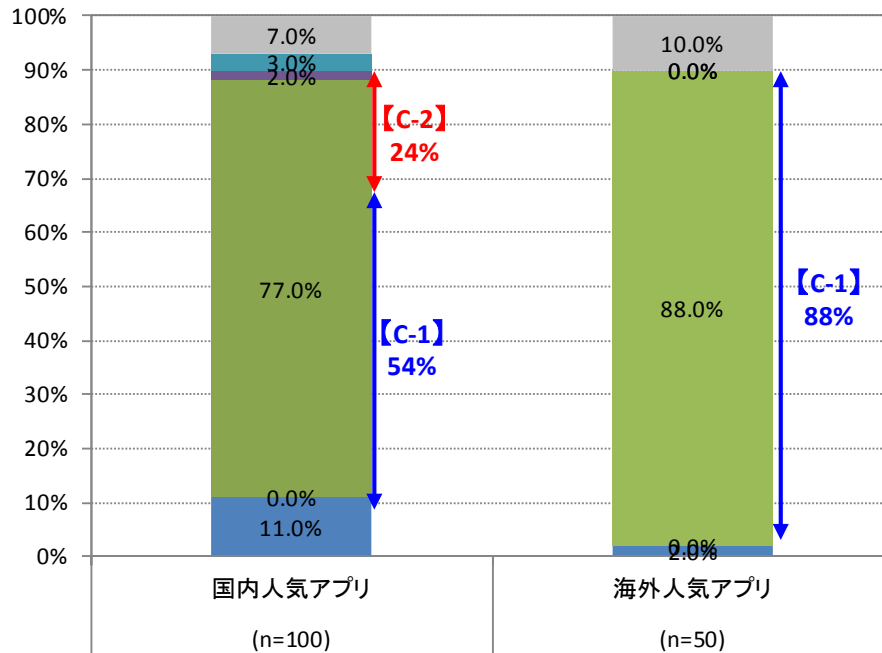
※全体の掲載率:「紹介ページ」又は「アプリ内」のどちらかが「F」以外の判定となったアプリの割合。

2.2.アプリプラポリ調査 調査結果(①国内人気アプリ・③海外人気アプリ:【1-2】プラポリの内容の分類)

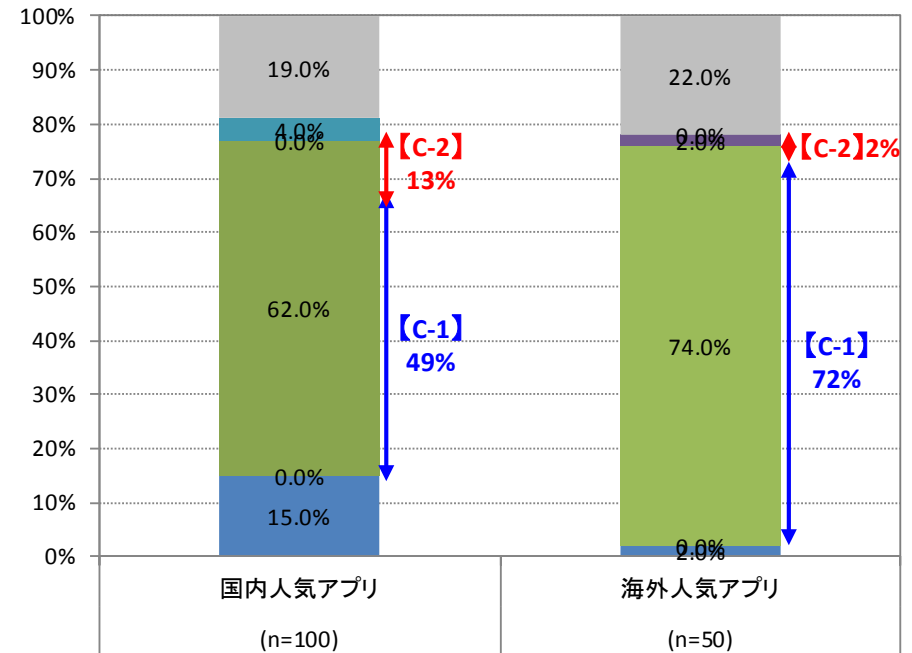
Android・iOSともに国内人気アプリの方が個々のアプリについて記載されたプラポリ(【A】・【B】)の割合が高い。
海外人気アプリのプラポリの大半はサービス全体について記載したプラポリ(【C】)に該当するものの、同プラポリのほぼ全てがスマホアプリを意識した記載になっているプラポリ(【C-1】)である。

アプリを意識した記載があるプラポリ(【A】・【B】・【C-1】)の割合では海外の方が国内より高い。

【Android】プラポリの内容分類の比較



【iOS】プラポリの内容分類の比較



■ 【A】 個々のスマホアプリ専用のプラポリが用意されている

■ 【B】 サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない

■ 【D】 一般的なWebサイトのプラポリがあるだけ

■ 【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】 プラポリが記載されていない

【C-1】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっている。(【C】の中での【A】・【B】に近い)

【C-2】:分類【C】に該当し、かつ、スマホアプリを意識した記載になっていない。(【C】の中での【D】・【E】に近い)

2.2.アプリプラポリ調査 調査結果(③海外人気アプリ:【2】SPI8項目の記載率)

Android、iOSともに、海外人気アプリの方が「②取得される情報の項目」の記載率が国内人気アプリよりも高い。
一方で、国内人気アプリは⑥において「利用者情報の送信先」や「情報収集モジュール」の記載率が海外よりも高い。

SPI8項目の記載率※

番号	項目	Android		iOS	
		国内人気アプリ (n=93)	海外人気アプリ (n=90)	国内人気アプリ (n=81)	海外人気アプリ (n=90)
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	98%	98%	100%	97%
②	取得される情報の項目	87% <	100%	93% <	100%
③	取得方法	55%	82%	60%	82%
④	利用目的の特定・明示	92%	93%	95%	95%
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	31%	60%	33%	51%
	利用者情報の削除の記載	58%	62%	60%	69%
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	90% <	98%	93%	97%
	利用者情報の送信先の記載	27% >	4%	32% >	0%
	情報収集モジュールに関する記載	22% >	4%	25% >	3%
⑦	問合せ窓口	87%	76%	85%	59%
⑧	プライバシーポリシーの変更を行う場合の手続き	60%	73%	62%	87%

SPI8項目において、特に重要性が高いと考えられる項目
※プラポリが存在していたアプリ数を母数として割合を算出。

< > 特に重要性が高い項目の中で、国内と海外で記載率が5ポイント以上差が開いている項目

2.2.アプリプラポリ調査 調査結果(【3】プラポリでの同意による情報の取得状況)

Androidの①国内人気アプリ・②国内新着アプリについては、情報を取得し得る割合が増加している。

Androidの①国内人気アプリと③海外人気アプリの比較では大きな差は無い。iOSでは③海外人気アプリの方が情報を取得する割合が高いものの、プラポリへの記載率も高い。

iOS・Androidともに、②国内新着アプリのプラポリへの記載率(項目2)が低い。

【調査概要】

- ・ <項目1> 各端末の設定画面からアプリの取得情報を確認し、プライバシー性が高い4つの情報(電話番号、電話帳、位置情報、メールアドレス)を取得するかを確認
 ※iOSの場合は、OSの仕様として「電話帳」と「位置情報」の取得有無しか確認できず、また、実際にアプリを動かして、アプリ内で「電話帳」と「位置情報」の取得確認のポップアップを呼び出した後に、設定画面で確認できる仕様になっている(動的解析的なリストアップと推測)
 ※Androidの場合は、アプリのインストール直後から設定画面から各アプリの情報取得の権限を確認できる(静的解析的なリストアップと推測)。そのため、Androidの場合には、アプリのコードを基にアプリの利用者情報の取得有無を判断したものであり、必ずしもアプリが利用者情報を取得するわけではないことに留意が必要。
- ・ <項目2> 項目1で抽出したアプリのプラポリにおいて、取得し得る情報について、取得する旨が記載されているかを調査。

【Android】プラポリでの同意による情報の取得状況 調査結果

調査項目	①国内人気アプリ		②国内新着アプリ		③海外人気アプリ
	2016年10月	2017年11月	2017年1月	2017年11月	2017年11月
<項目1> プライバシー性が高い4つの情報のいずれかを 取得し得る アプリ(静的解析ベース)	54% (54/100)	72% (72/100)	28% (14/50)	72% (36/50)	64% (32/50)
<項目2> 取得し得る 情報に関して、 プラポリ内で取得する旨の記載がある アプリ	37% (20/54)	29% (21/72)	21% (3/14)	8% (3/36)	31% (13/32)

【iOS】プラポリでの同意による情報の取得状況 調査結果

調査項目	①国内人気アプリ		②国内新着アプリ		③海外人気アプリ
	2016年10月	2017年11月	2017年1月	2017年11月	2017年11月
<項目1> プライバシー性が高い4つの情報のいずれかを 取得する アプリ(動的解析ベース)		18% (18/100)		16% (8/50)	36% (18/50)
<項目2> 取得する 情報に関して プラポリ内で取得する旨の記載がある アプリ		56% (10/18)		13% (1/18)	78% (14/18)

※iOSは今年度から調査開始。

2.2.アプリラボリ調査 調査結果(【調査項目4】概要版の作成・掲載状況)

- ①国内人気アプリの概要版の掲載率はAndroidが2%、iOSが5%であり、昨年度から横ばいで推移。
- ①国内人気アプリと③海外人気アプリの概要版の掲載率はほぼ同等であった。
- ②新着アプリの概要版の掲載率はAndroid、iOSともに0%であった。

アプリラボリ概要版の掲載率 調査結果

		①国内人気アプリ		②国内新着アプリ		③海外人気アプリ
		2016年 10月	2017年 11月	2017年 1月	2017年 11月	2017年 11月
対象 OS	An droid	2%	2%	0%	0%	2%
	iOS	6%	5%	0%	0%	4%

↑ ↑
ほぼ同等

2.2.アプリプラポリ調査 調査結果(①国内人気アプリ・③海外人気アプリ:4つの達成基準での評価)

Androidでは基準①～③を達成しているアプリの割合が昨年度よりも増加。iOSでは基準②～④に達しているアプリの割合が増加。海外人気アプリとの比較では、大きな差は無い。

		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(プラポリの掲載)	SPI8項目の内、重要度の高い4項目を記載している(重要4項目※1の記載)	SPI8項目の全項目について記載している(全8項目の記載)	基準③に加えて概要版のプライバシーポリシーを作成・掲載している(概要版の掲載)※2	
人気アプリの経年比較	Android	15年	78%	51%	10%	1%
		16年	83%	63%	7%	0%
		17年	93% ↑	71% ↑	24% ↑	2% →
	iOS	15年	68%	32%	9%	2%
		16年	81%	63%	15%	1%
		17年	81% →	70% ↑	24% ↑	4% ↑
国内・海外比較	Android	国内	93%	71%	24%	2%
		海外	90%	80%	24%	2%
	iOS	国内	81%	70%	18%	4%
		海外	78%	70%	18%	2%

※1 重要4項目:「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」

※2 具体的なアプリ・事業者は以下の通り

- Android国内人気アプリ: ディズニー ツムツムランド(コプロラ)、ニュースパス(KDDI)
- iOS国内人気アプリ: ディズニー ツムツムランド(コプロラ)、au WALLEET (KDDI)、My au (KDDI)、データお預かり(KDDI)
- Android海外人気アプリ: eBay (eBay)
- iOS海外人気アプリ: eBay (eBay)

2.2.アプリプラポリ調査 調査結果(②国内新着アプリ:4つの達成基準での評価)

Androidでは、基準②・基準③に達しているアプリの割合が増加している。
 iOSでは、基準①～③に達しているアプリの割合が増加している。

		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(プラポリの掲載)	SPI8項目の内、重要度の高い4項目を記載している(重要4項目※の記載)	SPI8項目の全項目について記載している(全8項目の記載)	基準③に加えて、概要版のプライバシーポリシーを作成・掲載している(概要版の掲載)	
新着アプリ	Android	15年	64%	26%	10%	0%
		16年	74%	40%	10%	0%
		17年	76% →	50% ↑	30% ↑	0%
	iOS	15年	26%	10%	4%	0%
		16年	18%	6%	0%	0%
		17年	70% ↑	28% ↑	14% ↑	0% →

※「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」

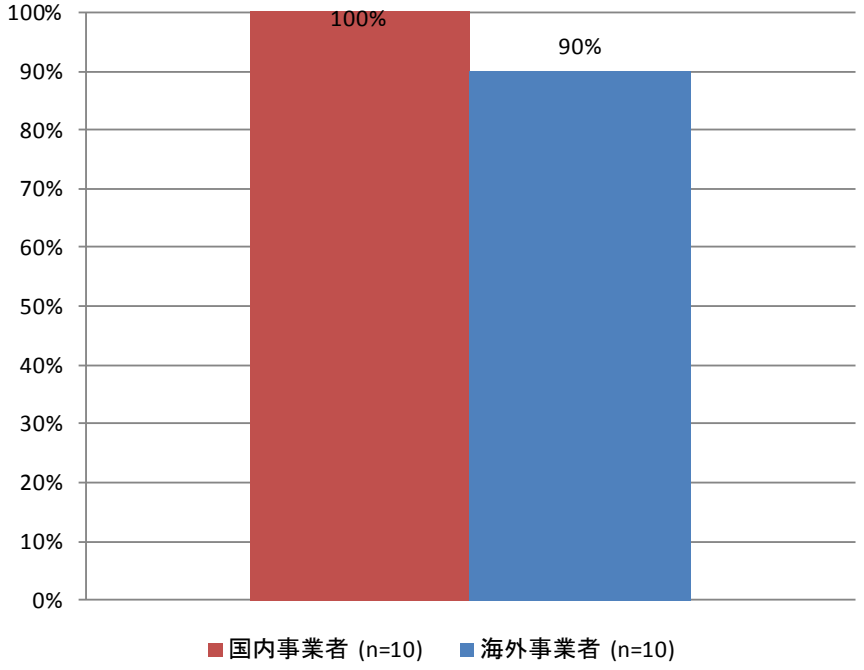
2.3.アプリプラポリ調査 調査結果総括

<p>現状分析と 傾向</p>	<p>○国内人気アプリのプラポリ掲載率はAndroid、iOSともに80%以上に達し、国内新着アプリの掲載率もAndroid、iOSともに70%以上に達しており、「<u>プラポリの作成・掲載</u>」については、<u>大手のアプリ提供者には浸透してきた</u>と考えられる。また、海外人気アプリとの比較では、国内人気アプリの掲載率は海外人気アプリとほぼ同等の水準である。(P5、P9、P12)</p> <p>○プラポリの記載内容について、国内人気アプリでは、大半のプラポリが会社全体やサービス全体について記載しているもの(分類Cに該当)であったが、<u>これらのプラポリのうち約7割はスマホアプリを意識して記載されたプラポリであった</u>。また、海外人気アプリとの比較では、国内人気アプリの方が個別アプリに記載したプラポリの割合が高かったものの、<u>スマホアプリを意識して記載されたプラポリ(【A】・【B】・【C-1】)</u>の割合では<u>海外の方が国内よりも高い</u>。国内新着アプリについては、Androidでは、ほぼ国内人気アプリと同様の傾向であったものの、iOSでは、スマホアプリを意識して記載されていないプラポリ(【C-2】・【D】・【E】)の割合が高く、プラポリの質の向上が必要と言える。(P6、P10、P13)</p> <p>○また、概要版の掲載率は、国内人気アプリにおいても横ばいか減少しており、利用者情報の取扱いについて容易に理解できる環境が整っているとは言えない。(P16)</p>
<p>環境変化</p>	<p>○昨年度からGoogle Play・App Storeともにプラポリの掲載に関して取組みを実施しており、Google Playではユーザーデータを扱うアプリがプラポリを掲載しない場合にペナルティを科すとしており、App Storeではガイドライン変更によって<u>プラポリを明示すべきアプリとして「ユーザーデータへのアクセスを実行する」アプリが追加された</u>。その結果、今年度の調査では、人気アプリだけでなく、新着アプリの掲載率が著しく向上したと考えられる。</p>
<p>今後の 課題・取組</p>	<p>○人気アプリではプラポリの掲載率は8割を超え、<u>アプリを意識して記載されているプラポリの割合も高く、プラポリの質も一定程度に達した</u>と考えられる。一方で、概要版の掲載率は相変わらず低く、<u>利用者情報の取扱いについて容易に理解できる環境整備も重要</u>と考えられる。</p> <p>○新着アプリに関しては、アプリを意識して記載されているプラポリの割合は高くなく、アプリマーケット運営者のガイドラインに対応するために、一般的な個人情報の取扱い等の掲載している事業者が多く、<u>今後はプラポリの質を向上していくことが重要</u>となる。</p>

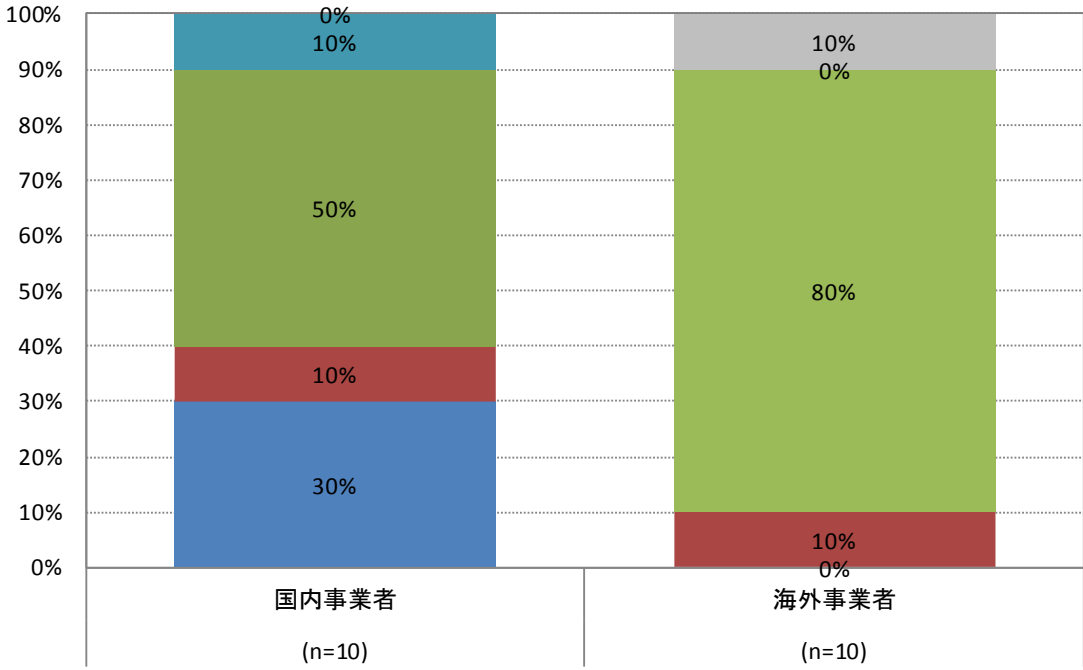
2.4.情報収集モジュール事業者のプラポリ調査 調査結果(【調査項目1】)

大半の事業者がウェブページ上にプラポリは掲載しているものの、個々の広告・分析サービスやモジュールに対応したプラポリ(【A】・【B】)の割合は国内で10社中4社、海外で10社中1社。

プラポリの掲載率※



プラポリの内容分類※



※掲載率: プライバシーポリシーや個人情報保護方針やこれらに準ずるものが記載されたページが事業者のウェブページ上で見つければ、「プラポリ有り」と判断。(「個々の情報収集モジュール、もしくは、広告ネットワーク等のサービスに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない)

- 【A】 個々のスマホアプリ専用のプラポリが用意されている
- 【B】 サービス全体のプラポリがあり、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ポリがあり、その中に個々のスマホアプリに関する記述がない
- 【D】 一般的なWebサイトのプラポリがあるだけ
- 【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】 プラポリが記載されていない

※「個々のスマホアプリ」を「個々の広告・分析サービスやモジュール」と読み替えて分類を実施

2.4.情報収集モジュール事業者のプラポリ調査 調査結果(【調査項目2】)

重要性が高いと考えられる4項目については、国内・海外ともに大半の事業者がプラポリに記載している(「送信先」は除く)。

SPI8項目の記載率

番号	項目	国内事業者 (n=10)	海外事業者 (n=9)	備考 (アプリプラポリとの評価と異なる点)
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	100%	100%	*** (アプリプラポリと同様)
②	取得される情報の項目	90%	100%	*** (アプリプラポリと同様)
③	取得方法	-	-	自動取得以外の方法は考えられな いため、評価せず
④	利用目的の特定・明示	90%	100%	*** (アプリプラポリと同様)
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	70%	67%	自社サービスのオプトアウトの仕組みの記載があれば「記載有」とした
⑥	外部送信・第三者提供・情報収集モジュールの有無			
	利用者情報の削除の記載	10%	33%	*** (アプリプラポリと同様)
	利用者情報の第三者への送信の有無の記載	80%	100%	*** (アプリプラポリと同様)
⑦	問合せ窓口	90%	100%	*** (アプリプラポリと同様)
	プライバシーポリシーの変更を行う場合の手続き	30%	100%	*** (アプリプラポリと同様)
⑧	外部送信・第三者提供・情報収集モジュールの有無			
	利用者情報の送信先の記載	30%	22%	*** (アプリプラポリと同様)
	情報収集モジュールに関する記載	-	-%	情報収集モジュール事業者のプラポリには不要な項目のため評価せず

SPI8項目において、特に重要性が高いと考えられる項目

※プラポリが存在していたアプリ数を母数として割合を算出。

3.1.民間及び海外における取組み状況の調査 調査概要

日本やEUにおける大幅な法改正、米国の政権交代により、スマートフォンの利用者情報を巡る環境が変化した。本調査研究では、当該環境変化のスマートフォンの利用者情報の取扱いに対する影響について調査・分析した。

調査対象		個人情報保護法等に関する動向	調査・分析の実施方針
民間における取組調査		<ul style="list-style-type: none"> 個人情報保護法の全面施行 	<ul style="list-style-type: none"> 民間事業者(アプリ提供者サイト運営者、セキュリティベンダー、モジュール事業者等)の利用者情報保護に関する取組調査 業界団体におけるガイドライン改正の有無、利用者情報に係わる箇所の分析 (※) IoTに関する取組を含む
諸外国における取組調査	EU(仏等を含む)	<ul style="list-style-type: none"> GDPRの制定 2018年5月全面施行予定 	<ul style="list-style-type: none"> スマホに関するガイダンス等の策定有無の調査 IoT等に関する取組の調査
	英		<ul style="list-style-type: none"> スマホに関するガイダンス等の策定有無の調査 IoT等に関する取組の調査
	米	<ul style="list-style-type: none"> 2017年1月、トランプ政権誕生 ISPの履歴情報の販売にあたって同意の取得を義務付けたプライバシー保護規則を撤回 	<ul style="list-style-type: none"> 政府および政府関連機関におけるガイダンスの発行、法執行の状況の調査(IoTを含む) 業界団体、消費者団体等における自主規制等の調査(IoTを含む)
	その他(韓国、香港等)	<ul style="list-style-type: none"> その他韓国や香港等において特徴的な取組を調査・分析 	

3.2.民間における取組状況に関する調査・分析 アプリに関する調査結果 (アプリマーケット運営事業者[Google]:ユーザーデータを扱うアプリへの規制強化)

2017年7月より有害アプリの検出を行う「Google Playプロテクト」を導入。

2017年12月、個人情報ユーザーの同意なく収集するAndroidアプリに対しGoogle Playプロテクト等で警告を表示すると発表。

2018年1月、「2017年にアプリストアから削除したポリシー違反アプリは70万本以上」であったと発表。

取組/報道名	発表年月	概要
Google Play プロテクトの導 入	2017年7月	<ul style="list-style-type: none"> ◆ ユーザーがアプリをダウンロードする際にアプリが有害な可能性があるかをチェックし、端末を定期的にスキャンする。有害な可能性があるアプリを検出すると、アプリを停止し、以下の処理を行う <ul style="list-style-type: none"> ➢ ユーザーへ警告: 端末に有害な可能性があるアプリが検出された場合は通知が表示される ➢ アプリを自動的に削除: 場合によっては、有害なアプリが検出された場合に、アプリが削除されたという通知を受け取る場合がある
個人情報ユーザーの同意なく収集するAndroidアプリに対する警告	2017年12月	<ul style="list-style-type: none"> ◆ Googleが個人情報をユーザーの同意なく収集するAndroidアプリに対しGoogle Playプロテクト又はアプリを配布するWebページで警告を表示すると発表した <ul style="list-style-type: none"> ➢ ユーザーの電話番号、メールアドレス等の個人情報や機器情報を収集するアプリに対して、アプリ内にプライバシーポリシーを掲載することを義務付け ➢ アプリの機能と無関係な個人情報を収集又は提供する場合、あらかじめユーザーの同意を取得することを義務付け ◆ 12月1日から60日以内に執行するとしている
2017年の有害アプリ対策と結果に関する報道	2018年1月	<ul style="list-style-type: none"> ◆ Google Playストアで有害アプリとして削除したアプリの本数は70万本以上、2016年比で70%増であることを発表した <ul style="list-style-type: none"> ➢ 削除された有害アプリの一例として、有名アプリの偽装アプリ、ポルノや暴力等の不適切なコンテンツを含むアプリ、ユーザー情報をフィッシングする潜在的な有害アプリが挙げられるとしている。 ➢ 潜在的な有害アプリは一見して有害か否かがユーザーに判別しづらいが、Google Playプロテクトによってインストール率を2016年比で半減させることができたとしている

3.2.民間における取組状況に関する調査・分析 アプリに関する調査結果 (アプリマーケット運営事業者〔Apple〕:ユーザーに向けた機能追加と新たな情報公開)

2017年9月、アプリによる情報取得に関する許可をより細かに指定できるようにOSを仕様変更し、同月、プライバシー保護の取組についての解説ページを開設した。

取組/報道名	発表年月	概要
iOSアップデートに伴う新機能	2017年9月	<p>◆ iOSがiOS11にアップデートされ、端末内における情報の取得に関する新機能が追加された。</p> <ul style="list-style-type: none"> ➢ アプリが位置情報を取得する場合は、「常に許可」と「許可しない」のみならず、「使用時のみ許可」のオプションを提供することを義務付け ➢ アプリが写真に関する情報を取得する場合は、写真ライブラリ全体ではなく、1枚の写真のみに権限を与えることも可能となった
プライバシー保護の取組に関する情報公開	2017年9月	<p>◆ Apple製品に関するプライバシー保護の取組をユーザーに向けて分かりやすく説明したページを公開した。</p> <ul style="list-style-type: none"> ➢ ターゲティング広告のオプトアウト機能のみならず、HealthKitやHomeKitなど最新の機能・サービスに関するプライバシー保護の取組についても、ユーザー向けに分かりやすく説明 ➢ パスワードの設定や情報の共有先の設定などユーザーがプライバシーを保護するための機能やサービスについても説明



位置情報を管理する。

カレンダーでミーティングを設定している時や、道順をチェックしている時など、デバイスにあなたの位置情報を知らせると便利な場合があります。位置情報サービスは、GPS、Bluetooth、クラウドソーシングのWi-Fiホットスポット、携帯電話の中継塔を組み合わせることで、あなたの位置を判断します。Appleは、位置情報の収集と使用を、あなたのすべてのデバイスであなたがコントロールできるようにしています。位置情報サービスはデフォルト設定ではオンになっていないので、あなたが自分で有効にする必要があります。オンにしたあとも、気が変わったいつでもオフにできます。

3.3.民間における取組み状況の調査: AIスピーカーに関するプライバシーについて

Google HomeやSiriについては、AIアシスタント固有のプライバシーに関する記載が確認できた。

その他については、AIスピーカー・アシスタント利用規約に関連する記述があるケース、当該サービスの記載が一切見られないケースがあった。

AIスピーカーに関するプライバシーに関する記載

事業社名	AIスピーカー	AIアシスタント	プライバシーに関するサービス固有の記載	概要
Google	Google Home	Google アシスタント	有	◆ プライバシーポリシーには、Googleアシスタント/Google Homeに関する記載はないが、Google Homeヘルプページにおいて「Google Homeのデータ セキュリティとプライバシー」として、取得・送信される情報の一例、データの使用目的等をQ&A形式で掲載している。
Amazon	Amazon Echo	Alexa	無	◆ プライバシーポリシーには、Amazon Echo/Alexaに関する記載はない。
Apple	HomePod	Siri	有	◆ プライバシーポリシーには、Siriに関する記載はないが、iPhone等のデバイスから「プライバシーについて」「“Siriからの提案”とプライバシーについて」として、取得・送信される情報が掲載されている。 ※webサイトでの掲載はAppleのプライバシーポリシーのみ
LINE	Clova WAVE	Clova	無 ※利用規約に一部記載	◆ プライバシーポリシーには、Clova WAVE/Clovaに関する記載はない ◆ LINE Clova利用規約にて、「本サービスにおける情報の活用」として、取得・送信される情報の一例、データの使用目的等を掲載している。
KDDI	au HOME	(Google アシスタント)	無 ※利用規約に一部記載	◆ プライバシーポリシーには、au HOMEに関する記載はない。 ◆ au HOME利用規約にて、「個人情報の保護」として、取得・送信される情報の一例、データの使用目的等を掲載している。

3.3.民間における取組み状況の調査：“Google Home”のプライバシー記載

Google Homeヘルプページにおいて、取得・送信される情報の一例、データの使用目的等をQ&A形式で掲載している。「音声」の取扱いや、アカウント登録者以外のユーザーが使うという特徴からAIスピーカー固有の記載が見られた。

Google Homeヘルプページにおけるプライバシーに関する記載

大項目	小項目	AIスピーカー固有の記載
データの収集	取得の方法	
	データの項目	
	他のアプリからの情報取得	
	検索履歴・位置情報の取得	
	情報の加工	
データの使用	取得目的	
データストレージ	保存場所	
	保存期間	
	取得情報の参照方法	
	取得情報の編集	
セキュリティ	セキュリティの度合い	
データの削除	デバイス・アカウント破棄後の紛失・破棄後の情報の確認・削除	
	データ削除後の事業者における保管状況	
	削除の方法	

大項目	小項目	AIスピーカー固有の記載
プライバシー	会話の保存範囲	○
	情報を聞きだせるユーザー	○
	個人情報の第三者との共有	
	サービス利用停止の方法	
アカウントと設定	Googleアカウントとの連携	
	Googleアカウントの削除方法	
サービス	個人情報の第三者提供	
	会話履歴の保存有無	○
	サービスによるアカウント情報の取得	
	Googleによる外部サービスとの会話履歴の保存	○
	サードパーティープロバイダへの音声の送信	○

3.3.民間における取組み状況の調査: AIスピーカーに関するプライバシーについて

Google Homeヘルプページにおいて、SPI項目についても一部言及があった。

Google Home ヘルプページにおけるSPI項目の記載有無

番号	項目	記載有無	記載内容(一部抜粋)	
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	有	Google は、ユーザーにとってより迅速で、スマート、適切、便利なサービスの提供を実現するためのデータを収集する	
②	取得される情報の項目	有		
③	取得方法	有	Google Home の設定から又はGoogle アシスタントとのやり取りから、登録された設定や、その他の情報を共有することができる	
④	利用目的の特定・明示	有	よりの確な検索結果の表示や迅速なトラフィック更新を行うことなどにより、より迅速、スマート、便利なサービスの提供を実現すること。また、不正なソフトウェアやフィッシングなどの疑わしいアクティビティからユーザーを保護するためにもデータが役立つ	
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	無	
		利用者情報の削除の記載	有	セットアップ アプリや myactivity.google.com でアクティビティを削除できる
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	有	Google のプライバシー ポリシーに記載されている第三者と情報を共有する可能性はある
		利用者情報の送信先の記載	無	
		情報収集モジュールに関する記載	無	
⑦	問合せ窓口	無		
⑧	プライバシーポリシーの変更を行う場合の手続き	無		

SPI8項目において、特に重要性が高いと考えられる項目

3.4.民間における取組状況に関する調査・分析 アプリに関する調査結果 (業界団体のスマートフォンに関する取組み)

改正個人情報保護法の施行に伴い、業界団体からも個人情報保護指針制定・ガイドラインの改定の動きが見られた。

事業者名	会員企業	会員数	取組/報道名	発表日	概要
一般社団法人 モバイルコンテ ンツフォーラム	モバイルコンテ ンツ関連企業	120社 (2017年5 月時点)	個人情報保護指針 の公表	2017年5月	<p>◆ 認定個人情報保護団体として個人情報保護指針を制定。</p> <p>➢ 個人情報保護指針において、スマートフォン等の利用者情報の取扱いに関してはスマートフォンプライバシーイニシアティブを参照することが推奨されている。</p>
一般社団法人 日本インタラクティ ブ広告協会	インタラクティブ 広告ビジネスにか かわる企業(媒体 社、メディアレップ、 広告会社、調査 会社、システム・ サービス会社、制 作会社など)	260社 (2017年 12月11日 時点)	プライバシーポリ シーガイドラインの 改定	2017年5月	<p>◆ 改正個人情報保護法の全面施行に向けてインターネット広告におけるプライバシーポリシーの内容、同意取得の在り方等について定めた「プライバシーポリシーガイドライン」を改定した(同ガイドラインは2004年制定)。</p> <p>➢ 改正法・個人情報の保護に関する法律についてのガイドライン(通則編)を踏まえ、本人同意の在り方等に関して、インターネット広告ビジネスでの実務に即した具体例を用いて解説されている。</p>

3.5.諸外国における取組み状況の調査:米国 FTCスタッフレポート「クロスデバイストラッキング」

2017年1月、「クロスデバイストラッキング」に関する指針を示したスタッフレポートがFTC(連邦取引委員会:Federal Trade Commission)から公開された。

- 【背景】
- ◆ 複数の端末で同一のユーザーの行動履歴等の情報を収集する方法である「クロスデバイストラッキング」ワークショップが2015年11月に開催。
 - ◆ 当該ワークショップでは、同意取得が困難であるなどプライバシーのリスクが懸念されており、技術動向やプライバシーリスクの把握、自主規制等のあり方について議論がなされた。
 - ◆ ワorkshopでの議論を踏まえて、クロスデバイストラッキングに関するスタッフレポートが策定・公表された。

- 【指針】
- ◆ スタッフレポートでは、「透明性の担保」、「選択肢の提供」、「機微な情報への対応」および「セキュリティ」の4項目について指針が示されている。

項目	概要
透明性の担保	<ul style="list-style-type: none"> • 事業者は、トラッキングに関する情報を 消費者に対して、積極的に公開しなければならない。 • 広告事業者などのサードパーティは、アプリ提供者などにファーストパーティーに対して、トラッキングに関する情報を公開することが推奨される。
選択肢の提供	<ul style="list-style-type: none"> • 事業者は、消費者に対して、トラッキングに関する選択肢を提供しなければならない。 • 消費者に接する事業者が中心となり消費者に対する選択肢の提供など、消費者に接する事業者は関係する事業者を調整する役割を担う必要がある。

項目	概要
機微な情報への対応	<ul style="list-style-type: none"> • 消費者の事前の明示的な同意なくして、健康情報や子供の情報などの機微情報を収集してはならない。 • 同様に、「正確な位置情報」を取得する場合にも、事前の明示的な同意を取得しなければならない。
セキュリティ	<ul style="list-style-type: none"> • 不正なデータの使用やアクセスを防ぐため、事業者は、合理的なセキュリティの確保に向けた取組を実施する必要がある。 <ul style="list-style-type: none"> ➢ 事業者は、目的に照らして必要なデータのみ保有し、収集等の方法がセキュアであるようにしなければならない。

3.5.諸外国における取組み状況の調査：米国

FTC・NHTSA「コネクテッドカーに関するプライバシー・セキュリティワークショップ」

2017年6月、FTC及びNHTSA(米国運輸省道路交通安全局：National Highway Traffic Safety Administration)は、コネクテッドカーに関するプライバシーやセキュリティをテーマとしたワークショップを開催した。

【ワークショップ概要】

- ◆ワークショップには、消費者団体、自動車メーカー等の民間事業者、有識者等が参加し、マルチステークホルダーによる議論がなされた。
- ◆コネクテッドカーにおいて収集されるデータの多様性に応じた取扱いの在り方、自主規制とエンフォースメントを組み合わせた規制の在り方について検討がなされた。

【ワークショップにおける検討結果】

- ◆ワークショップでは、「プライバシー」及び「セキュリティ」それぞれについて、議論がなされた。

項目	ワークショップにおける検討結果 概要
プライバシーへの懸念	<ul style="list-style-type: none"> • コネクテッドカーによって生まれる新たなサービスが普及するためには、消費者の不安を取り除くことが必要であることは、参加者の共通の認識であった。 <ul style="list-style-type: none"> ➢ アメリカ自動車製造連盟や世界自動車メーカー協会によるガイドライン(注)の公表など自主規制が進んでおり、重要な取組であるとの認識が業界から示された。 ➢ 一方で、消費者団体からは、収集・利用・共有されるデータの種別を把握することは、困難であるとの指摘があり、自動車メーカーごとに取得・利用する情報が比較できるようなポータルサイトを構築してはどうかとの提案がなされた。 • 参加者からは、スピードなど「安全性に直結するデータ」と「それ以外」のデータに分類した上で、取扱いの在り方を検討してはどうかとの指摘があった。 <ul style="list-style-type: none"> ➢ 自動車の故障診断や制御に係わる「安全性に直結するデータ」については、オプトアウトにより消費者が情報の共有をコントロールできるようにすべきではない、との指摘があった。
セキュリティへの懸念	<ul style="list-style-type: none"> • コネクテッドカーへのセキュリティの脅威は、深刻な問題である。脆弱性情報の共有の促進、業界標準などの策定を実施することが望ましいとの指摘があった。

(注)アメリカ自動車製造連盟・世界自動車メーカー協会“PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES”(2014年11月公表)

【今後の取組】

- ◆FTCとしては、引き続きコネクテッドカーの市場を注視しつつ、消費者保護とイノベーションの促進のバランスを取るための施策を検討していくことが示されている。

3.5. 諸外国における取組み状況の調査: 米国

FTC ボイスレコードに関するCOPPA法ガイダンス

2017年8月、ボイスレコードを活用したサービスの普及を受けて児童オンラインプライバシー保護法(COPPA)における当該サービスの位置づけに関するガイダンスがFTCより公表された。

【背景】

- ◆ 児童に関する個人データの保護について定めた児童オンラインプライバシー保護法(COPPA)が2013年に改正され、子供の画像や音声を含むビデオやオーディオファイルが、個人情報に該当することが明記された。
- ◆ 法改正後、多くの民間の事業者から、音声検索システムなどにおける音声の収集に関して、即座に情報をテキストに変換して、音声ファイルを削除する場合、COPPA法における「取得又は収集」にあたるのか、といった意見が寄せられた。
(「取得又は収集」に該当する場合には、あらかじめ、親権者の同意が必要となるが、上記のような対応を行う場合は、プライバシーへのリスクは少ないため、取得等の例外にして欲しいとの意見があった。)

【ガイダンス】

- ◆ ガイダンスでは、「取得又は収集」の解釈の明確化、およびFTCの法執行の在り方について言及がなされている。

項目	ガイダンスの内容
「取得又は収集」	<ul style="list-style-type: none"> • 音声検索システムなどにおける音声の収集に関して、即座に情報をテキストに変換して、音声ファイルを削除する場合であっても、「取得又は収集」に該当するため、規定上は、取得等に際して、あらかじめ親権者の同意が必要となる。
FTCによる執行	<ul style="list-style-type: none"> • 文字を書けない子供もおり、音声により検索等を行えることは、子供にとって非常に有用であるため、FTCは、親権者の同意をあらかじめ取得しない事業者に対して、法を執行しないこととする。 • ただし、事業者は、収集又は使用する音声データの内容、削除の方法などをプライバシーポリシー等により通知しなければならない。 • その他、音声ファイルをターゲティング広告などに利用する場合は、法執行の適用は除外されることが示されている。

3.5.諸外国における取組み状況の調査:米国民間団体 EPIC Google Homeに対するリコール要求

2017年6月、米国における消費者保護団体であるEPIC(電子プライバシー情報センター:Electronic Privacy Information Center)は、Google Homeのスマートスピーカーが消費者の同意なく個人データを取得しているとして、米国消費者製品安全委員会に対して、リコールを求めた。

【背景】

- ◆ 2017年10月、Google は、Google Home Miniの発売を公表した。
- ◆ 販売前に配布されたレビュー端末の利用者が、消費者の同意なく音声を取得し、Googleのサーバーに送信されるバグを発見した。
 - Google Home Mini上部にあるタッチパネルの誤動作により、Googleアシスタントが常時起動。音声コマンドの入力待ちになっており、音声
が常時取得され、サーバーへ送信されていた。(タッチパネルを長押することで起動)
- ◆ EPICは、消費者へのプライバシーリスクがあるとして、米国消費者製品安全委員会に対してリコールを要求した。
- ◆ また、FTCに対して、IoT製品に関する消費者保護を徹底するよう、IoTデバイスメーカーに求めることを要求している。

【政府への要求概要】

米国消費者製品安全委員会へのリコール要求

- Googleはバグの修正ファイルを配布しているが、[タッチパネルの設計に起因する問題](#)であり、リコールが必要である。
- [消費者へのリスクは製品に起因](#)することや、米国消費者製品安全委員会が法執行に関して広範な裁量を有していることから、米国消費者製品安全委員会がIoTデバイスの消費者へのリスクに対して責任を持つべきである。
- また、米国消費者製品安全委員会への報告義務を執行して、IoTデバイスメーカーに報告を求めるべきである。

FTC次年度以降の計画に対するパブリックコメント

- FTCは、IoT製品を提供する企業に対して、2015年に公表したスタッフレポート「Internet of things Privacy & Security in a Connected World」(注)を遵守を求めるとともに、特に以下を求めるべきである。
 - ① IT製品が準拠すべき情報セキュリティの要件を定めた連邦情報処理標準(FIPs)に準拠すべきこと
 - ② プライバシー・バイ・デザイン及びセキュリティ・バイ・デザインに取り組むこと
 - ③ インターネットに接続される玩具に関してCOPPA法を遵守した製造等を行うこと
 - ④ 透明性および消費者が自身のデータに関与できること

(注)同レポートでは、IoTデバイスメーカーに対して、「セキュリティバイデザイン」の採用、データ収集・保存の最小化、透明性の確保などを原則として、具体的な取引指針を明記している。

3.5.諸外国における取組み状況の調査:米国民間団体 医療業界団体 ヘルスケアアプリプライバシーガイドライン

2017年12月、米国医師会等が立ち上げた組織Xcertiaがヘルスケアアプリのプライバシーに関するガイドラインを公表した。

【ガイドラインの内容】

◆ ガイドラインでは、ヘルスケアアプリの提供者に対して、指針および具体的な取組内容が示されている。

指針	アプリの性能要求(一部抜粋)
<ul style="list-style-type: none"> 取得する情報、使用目的、情報の利用者、その他の事項がプライバシーポリシーに明記され、ユーザーに知らされなければならない。 	<ul style="list-style-type: none"> データにアクセスする主体が全て明記されていること等
<ul style="list-style-type: none"> データが収集された場合、データが保有される期間をユーザーに対して知らせなければならない。 	<ul style="list-style-type: none"> プライバシーポリシーに保有期間を明示すること等
<ul style="list-style-type: none"> アプリが端末に保存された情報やSNSの情報、Wi-Fiなどの機能に対してアクセスする場合は、アクセスの方法、理由を、適切な手段により、ユーザーに知らせなければならない。 また、端末情報等にアクセスする前に、同意を取得しなければならない。 	<ul style="list-style-type: none"> カメラにアクセスする場合は、使用目的がユーザーに知らされなければならないこと等
<ul style="list-style-type: none"> アプリが直接サードパーティーに情報を送信する場合(注)についても、関連する法令を遵守しなければならない。 	<ul style="list-style-type: none"> ユーザーが、積極的に、オプトイン又はオプトアウトをできるようにすること等
<ul style="list-style-type: none"> 法令を遵守して児童のプライバシーを保護するための施策を講じなければならない。 	<ul style="list-style-type: none"> 初期設定では、アプリ内購入を出来ないようにすること等
<ul style="list-style-type: none"> プライバシーポリシーを変更し、遡及的又は将来的に効力を及ぼす場合は、あらかじめ、ユーザーから同意を取得しなければならない。 	<ul style="list-style-type: none"> ユーザーに変更を通知する機能を実装すること 変更に対する同意を行う機能を実装すること

(注)アプリを提供している事業者のサーバーを介さず、直接サードパーティーに情報が送信される場合を意味していると考えられる。

3.6. 諸外国における取組み状況の調査: EU

欧州委員会・AIOT「IoTプライバシーおよびセキュリティワークショップ」

欧州委員会およびAIOT(IoTイノベーション・アライアンス:The Alliance for the Internet of Things Innovation)が2017年1月に共同で開催した「IoTプライバシー及びセキュリティワークショップ」を踏まえて作成されたレポートが2017年4月に公表された。

【目的】

- ◆ 最低限のセキュリティ・プライバシーの基準に向けて議論することを目的にワークショップを開催

【検討領域】

- ◆ ワークショップでは、ウェアラブル・スマートデバイス、コネクテッドカー、自動運転車、インダストリアル IoT、スマートシティについて検討を実施した。

【検討結果】

- ◆ ワークショップの検討結果として、各領域における最低限のシステムや運用の要求事項が策定された。

領域	最低限の要求
ウェアラブル・スマートデバイス	<ul style="list-style-type: none"> • データコントロール・バイ・ユーザー • 暗号化・バイ・デフォルト • 全ライフサイクルにおけるデータ保護の実施 • 更新性(信頼の出来るかつ透明性の高いアップデートの実施) • アイデンティティ・バイ・デザイン
コネクテッドカー、自動運転車	<ul style="list-style-type: none"> • データのセグメンテーション(コンテキストに応じて消費者の権利等の明らかにする) • データコントロール、データの使用者等の明確化 • 透明性の確保 • ユーザーコントロール(オプトアウトの実装等) • プライバシーバイデザイン、プライバシーバイデフォルト

項目	最低限の要求
インダストリアル IoT	<ul style="list-style-type: none"> • 持続可能性 • 透明性及びアカウントビリティ • セキュリティ・バイ・デザイン • セキュリティ・バイ・デフォルト • 保証(システムのセキュリティが管理され、メンテナンスされることと) • 安全とセキュリティの区別
スマートシティ	<ul style="list-style-type: none"> • ヒューマンセントリック • データ分離 • 明確な役割分担(データ主体、データプロセッサ等が誰か明確化する) • 問い合わせ窓口の一元化 • 差別的な取扱いの禁止 • プライバシー及びセキュリティに関する独立した監督機関の設置

3.7. 諸外国における取組み状況の調査: 韓国 情報通信網法改正

2017年3月、情報通信網法および同法施行令が公布・施行され、アプリ提供者に対して、端末情報へのアクセス権限に関する同意取得等が義務付けされた。

同日、改正法に関するガイダンスである「スマートフォンアプリケーションのアクセス権限に関するプライバシーガイド」が策定公表され、アプリ提供者の具体的な取組指針に加えて、関係する事業者等へのアクセス権限に関する取組指針が示された。

アプリ提供者に対する義務

項目	内容
アクセス権限に関する取得の義務付け	<ul style="list-style-type: none"> アプリ提供者は、以下の情報へのアクセス権限を取得する際に、利用者の同意を得なければならない。 <ol style="list-style-type: none"> ① 連絡先など利用者が保存した情報 ② 位置情報、通信記録など ③ 端末固有情報(IMEIなど) ④ 撮影、音声認識、バイオ情報など
同意取得の方法	<ul style="list-style-type: none"> アプリのインストール時または起動中に、アクセス権限の詳細及び取得する理由を利用者に明示する。 OSごとに定められた方法により、利用者の同意を得る。
罰則	<ul style="list-style-type: none"> 違反した場合は罰金が科される。

ガイドに規定されたその他ステークホルダーへの取組指針

主体		概要
事業者	OS提供者	<ul style="list-style-type: none"> 同意及び撤回に関する機能を提供すること OSのアクセス権限に関する運用基準をアプリ開発者が理解しやすいように作成し、公開すること
	端末製造者	<ul style="list-style-type: none"> アクセス権限に対する同意及び撤回することができるOSを端末に実装すること
	アプリ開発者	<ul style="list-style-type: none"> 端末及びOSの環境に合うようにアクセス権限に対する同意及び撤回するための設定を実装すること
	アプリマーケット運営者	<ul style="list-style-type: none"> アクセス権限に関する通知(ポップアップ)を表示するスペースを提供すること
利用者		<ul style="list-style-type: none"> アクセス権限に関する通知を確認した後、同意するか又は撤回すること