

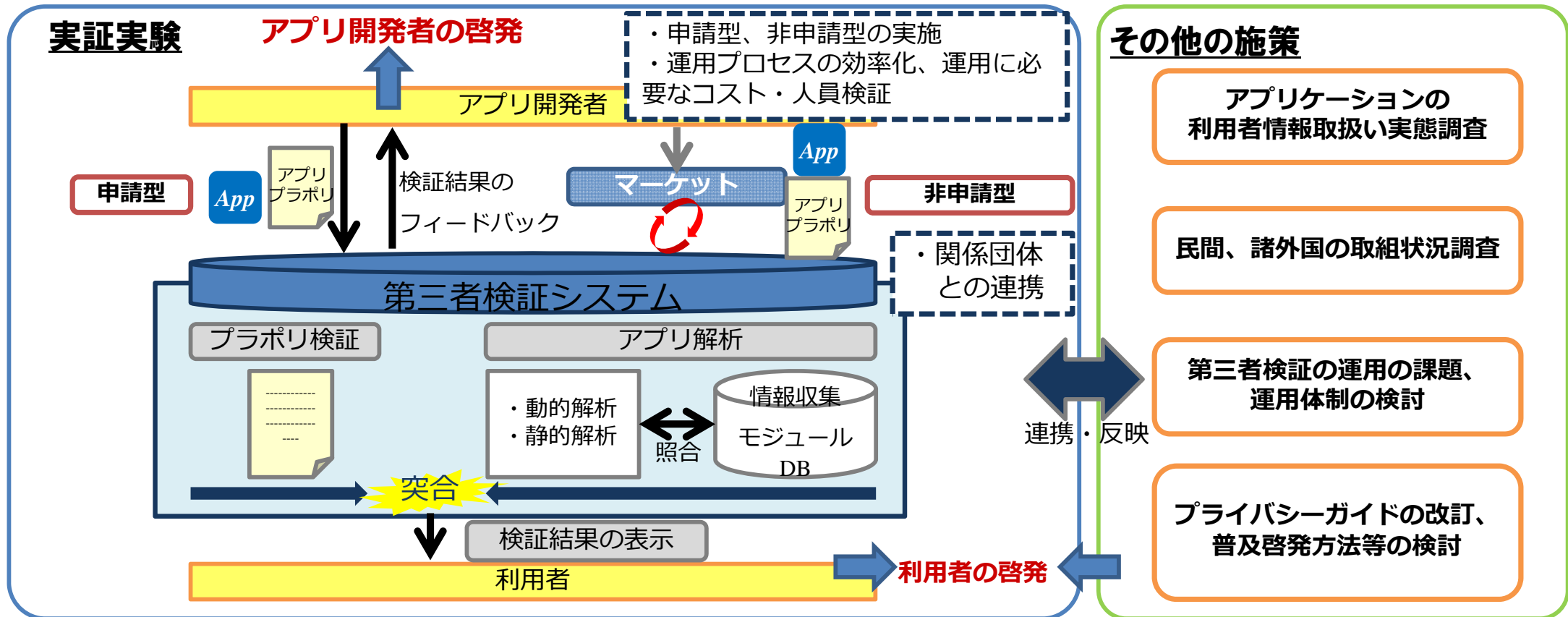
スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る技術的検証等の諸問題に係る実証調査研究

～スマートフォン プライバシー アウトルックⅢ～

平成28年4月28日

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

- 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（次ページ参照）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（SPO）」として取りまとめられ、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や、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取りまとめられた「スマートフォン プライバシー アウトルックⅡ（SPOⅡ）」が発表された。
- 平成27年度の本報告書においては、平成26年度から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取りまとめられた。



2. 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

1. 概要

SPI IIを踏まえ、スマートフォンのアプリプラポリの普及とアプリの第三者検証を推進するにあたっての諸課題について検討し、プラポリの普及並びに民間における検証サービスの提供と利用者による当該サービスの活用を促進することを目的として、平成25年12月に設置。(平成27年度においては、9月から年度末にかけて4回の会合を開催)

2. 主な検討項目

(1) アプリプラポリの作成・掲載等の推進

- ・ 定期的なアプリ調査の実施
- ・ 業界団体等関係者との連携による取組推進

(2) アプリの第三者検証の推進

- ・ アプリ検証サービスのための詳細な標準的検証基準の作成
- ・ 検証結果の適正な表示方法の検討
- ・ 検証結果の活用の在り方の検討

3. 構成員

(平成27年度:五十音順・敬称略)

主査	新保 史生	慶應義塾大学総合政策学部教授	曾我部 真裕	京都大学大学院法学研究科教授
主査代理	森 亮二	英知法律事務所弁護士	高木 浩光	国立研究開発法人 産業技術総合研究所セキュアシステム研究部門主任研究員
	石田 幸枝	公益社団法人全国消費生活相談員協会IT研究会代表	竹森 敬祐	株式会社KDDI研究所ネットワークセキュリティグループ研究マネージャー
	岸原 孝昌	一般社団法人モバイル・コンテンツ・フォーラム専務理事	三好 眞	株式会社アイ・エス・レーティング代表取締役社長
	櫻井 勉	トレンドマイクロ株式会社テクニカルサポートグループ コンシューマサポートセンター課長	谷田部 茂	一般社団法人日本スマートフォンセキュリティ協会技術部会長
	佐藤 進	アンドロイダー株式会社	矢橋 康雄	一般社団法人電気通信事業者協会業務部長

3.1.アプリプラポリ調査 調査概要

アプリプラポリ調査として、日本のAndroid、iOSのアプリを対象とし、①人気アプリ(上位100アプリ)、②新着アプリ、③20カテゴリのアプリについて、アプリプラポリの作成・掲載状況、SPI8項目(下記①から⑧までの項目。以下同じ。)の記載内容、同意取得の方法、概要版の掲載状況等を調査した。

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、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、⑥外部送信・第三者提供の有無、⑦問い合わせ窓口、⑧プライバシーポリシーの変更を行う場合の手続き

【調査目的】

・SPIにおけるアプリの利用者情報の取扱いに関する基本原則を踏まえ(※)、アプリプラポリの作成・掲載等の実態を調査する。

(※)SPIにおいては、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報告書の59ページ参照)

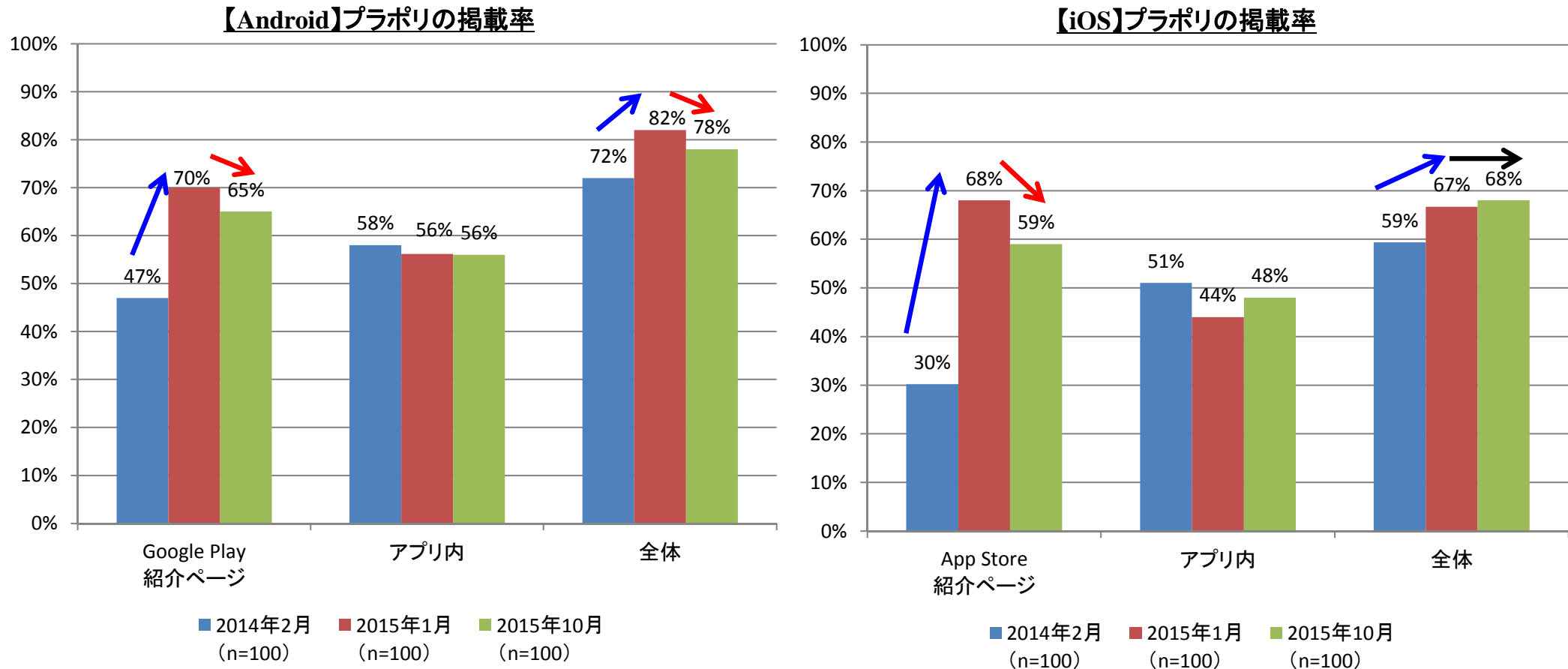
【調査対象・調査項目】

		①人気アプリ	②新着アプリ	③20カテゴリのアプリ※2
調査対象	アプリ数	Android:100アプリ iOS:100アプリ	Android:50アプリ iOS:50アプリ	Androidアプリ:850 (20カテゴリ× 40~45アプリ)
	抽出基準	無料アプリランキングの 上位100アプリを抽出	新着アプリの中から50アプ リを抽出※1 (①のアプリと重なりが無い ように抽出)	各カテゴリ別の人気アプリ を40~45抽出 (①、②のアプリと重なりが 無いように抽出)
調査項目	【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項目の記載状況	○	○	○
	【3】利用者情報の取得に関する同意取得方法 ※Androidアプリのみ実施	○	○	○
	【4】プラポリの概要版作成・公表状況	○	○	○

※1 Androidの新着アプリは「Google play」の新着無料トップから抽出、iOSの新着アプリは「iPad iPhone Wire」の新着アプリランキングから抽出。

※2 20カテゴリの詳細: Google Playのカテゴリから、抽象的なカテゴリ(ウィジェット、ツール、ライフスタイル等)を除き、カテゴリ内のアプリが想像しやすいカテゴリを抽出。具体的なカテゴリ名は、医療、SNS、エンタメ、音楽、教育、ゲーム、健康フィットネス、交通、コミック、書籍、写真、ショッピング、スポーツ、通信、ニュース、ビジネス、ファイナンス、ファミリー、メディア、旅行(50音順)。

全体においてAndroid、iOSともに2014年2月から2015年1月にかけてプラポリの掲載率は伸びたものの、2015年1月から2015年10月にかけては横ばい・微減で推移している。



※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。

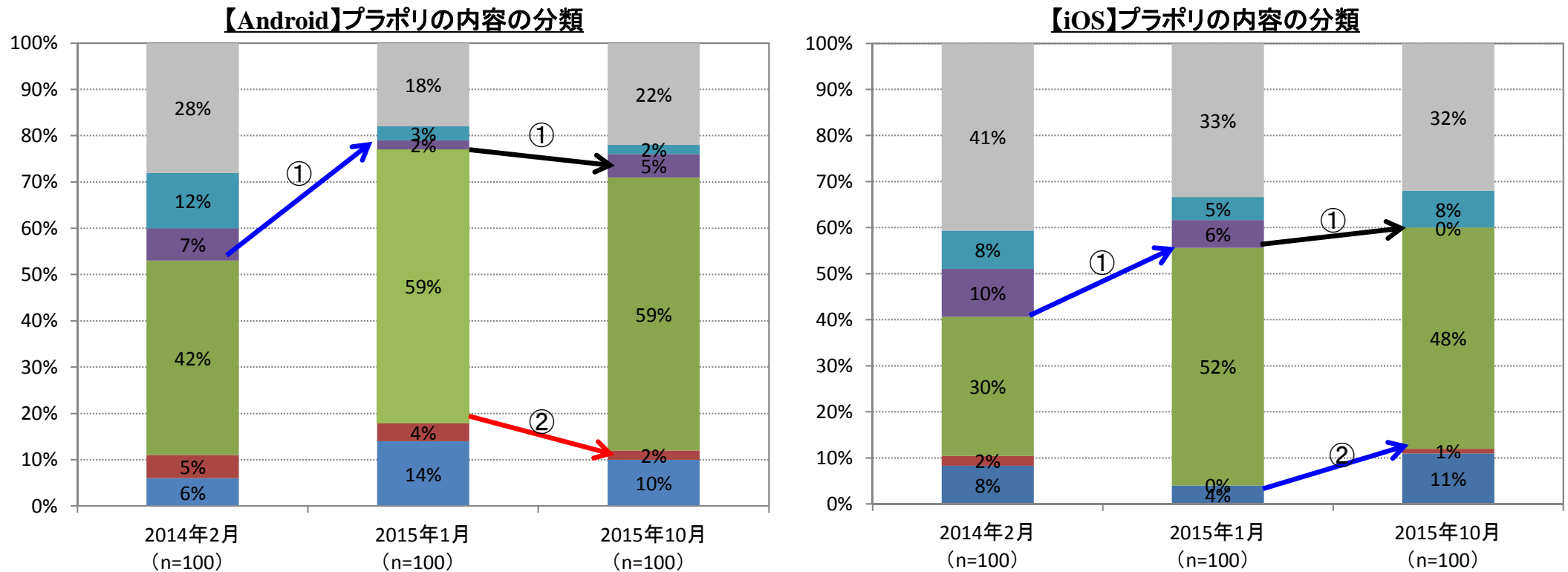
※紹介ページの掲載率：「紹介ページのリンク」が「紹介文内での記載」のどちらかが「F」以外の判定となったアプリの割合。

※アプリ内の掲載率：「初回起動時」、もしくは、「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」、もしくは、「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。

Android、iOSともに2014年2月から2015年1月にかけて【A】～【C】の割合の合計が上昇しているが、2015年1月から2015年10月にかけてはほぼ横ばいで推移。（グラフの①の矢印参照）

【A】・【B】の割合の合計については、2015年1月から2015年10月にかけてiOSについては上昇している一方、Androidは減少している。（グラフの②の矢印参照）



■ 【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

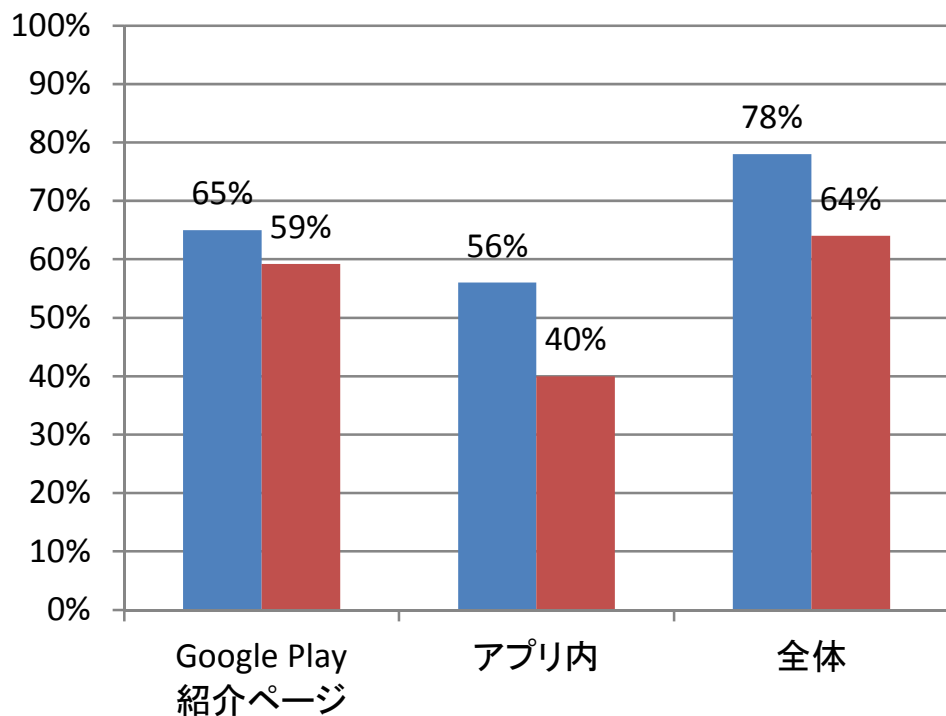
■ 【D】 一般的なWebサイトのプラポリがあるだけ

■ 【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

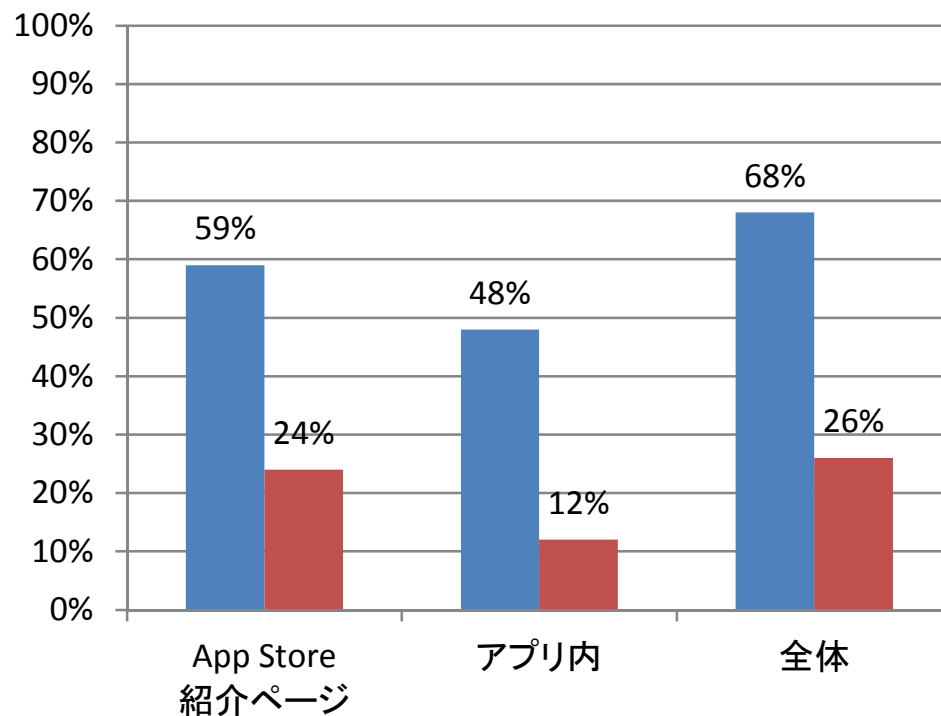
Android、iOSともに人気アプリの方が、新着アプリよりもプラポリ掲載率が高くなっている。

【Android】プラポリの掲載率



■ 人気アプリ (n=100) ■ 新着アプリ (n=50)

【iOS】プラポリの掲載率



■ 人気アプリ (n=100) ■ 新着アプリ (n=50)

※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。

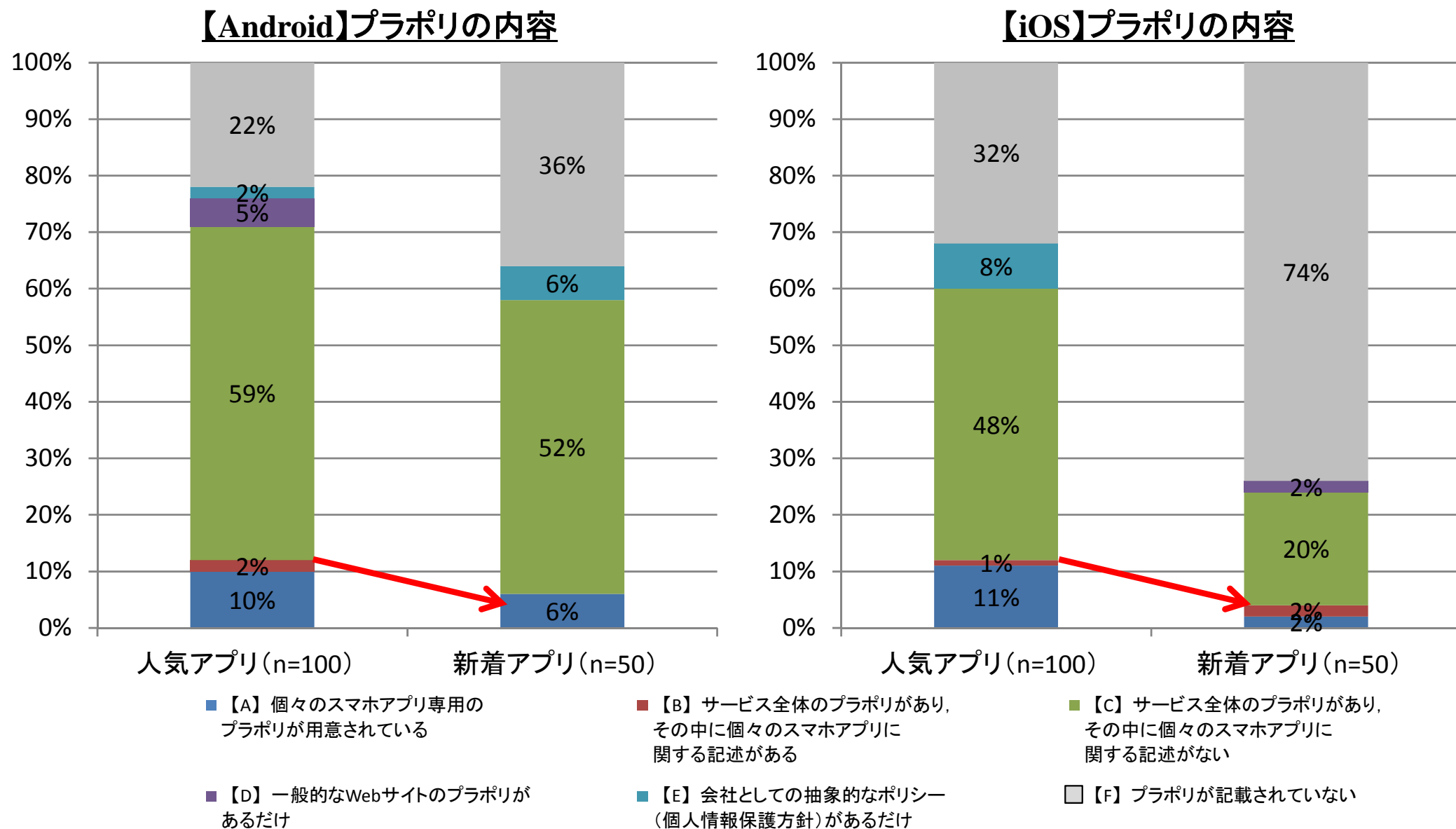
E: 会社としての抽象的なポリシー（個人情報保護方針）があるだけ。F: プラポリが記載されていない。

※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」のどちらかが「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」、もしくは、「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」、もしくは、「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。

Android、iOSともに新着アプリについては、個々のアプリに言及したプラポリの掲載の割合（【A】・【B】の割合の合計）が10%以下であり、人気アプリと比較して、半分以下の割合である。



AndroidではSPI8項目の中で特に重要性が高い4項目のうち、②において、人気アプリと新着アプリの記載率の差は10%以上であった。

iOSでは特に重要性が高い4項目のうち、②、④及び⑥において、人気アプリと新着アプリの記載率の差は10%以上であった。

SPI8項目の記載率※

番号	項目	Android		iOS		
		人気アプリ (n=78)	新着アプリ (n=32)	人気アプリ (n=68)	新着アプリ (n=13)	
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	98.7%	93.8%	98.5%	100.0%	
②	取得される情報の項目	70.5%	56.3%	58.8%	46.2%	
③	取得方法	35.9%	25.0%	26.5%	23.1%	
④	利用目的の特定・明示	80.8%	75.0%	79.4%	53.8%	
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	26.9%	21.9%	22.1%	23.1%
		利用者情報の削除の記載状況	38.5%	37.5%	44.1%	46.2%
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	79.5%	71.9%	85.3%	38.5%
		利用者情報の送信先の記載状況	38.5%	28.1%	22.1%	7.7%
		情報収集モジュールに関する記載状況	12.8%	12.5%	14.7%	0.0%
⑦	問合せ窓口	65.4%	59.4%	61.8%	76.9%	
⑧	プライバシーポリシーの変更を行う場合の手続き	69.2%	43.8%	57.4%	53.8%	

SPI8項目において、特に重要性が高いと考えられる項目

特に重要性が高い項目の中で、人気アプリと新着アプリの記載率の差が10%以上ある項目

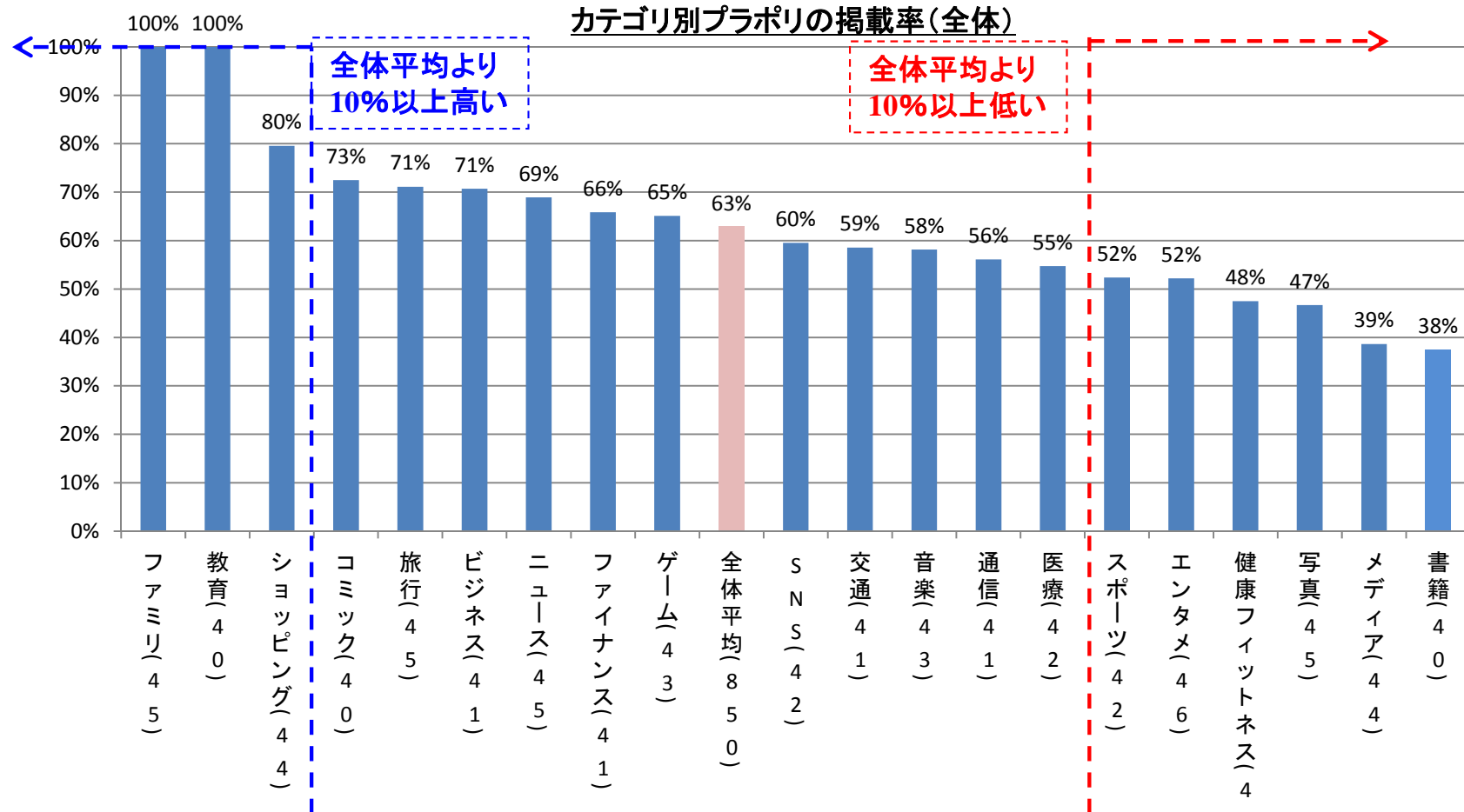
※プラポリが存在していたアプリ数を母数として割合を算出。

3.2.アプリプラポリ調査 調査結果（20カテゴリ：作成・掲載状況）

プラポリの掲載率が「全体平均」より10%以上高いカテゴリは、「ファミリー」、「教育」、「ショッピング」である。

「ファミリー」については、同カテゴリに分類されるためにはGoogle Playのガイドラインで「プラポリの掲載が必須」となっており、掲載率が100%となっている（「教育」については、「教育」アプリの9割程度が「ファミリー」にも分類される（「ファミリー」認定を取得している）ため、結果的に100%となっている※1）。

「ショッピング」については、同カテゴリのアプリの大半がECのアプリであり、WebのECサイトで利用しているプラポリを流用しているため、プラポリの掲載率が高くなっていると考えられる。



※1 調査対象となっているカテゴリ間で重複は存在したいため、「教育」アプリと「ファミリー」アプリ間でも重複は存在しない。

※2 掲載率(全体)：「紹介ページ」、もしくは、「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。

※3 括弧内の数値は調査したアプリ数。

「ファミリー」カテゴリに分類されるための要件(抜粋)

Designed for Families プログラムに申請するアプリは、Designed for Families デベロッパー販売 / 配布契約の補足条項 の要件に加え、下記の資格基準すべてに準拠している必要があります。Google Play は、Designed for Families プログラムに適さない要素がアプリにあると判断した場合、そのアプリを拒否または削除する権利を留保します。

注 13 歳未満の子供に特定の利益や関連性がない一般向けアプリは、このプログラムを利用できません。

利用資格要件

1. アプリは ESRB の Everyone、Everyone 10+、または同等のレーティング設定が必要です。
2. Designed for Families のアプリで広告を表示する場合、次のことを確認します。
 - 2.1 広告関連の該当する法的義務に準拠している。
 - 2.2 子供向けに表示される広告にインタレストベース広告やリマーケティングが含まれていない。
 - 2.3 子供向けに表示される広告が子供に適した内容である。
 - 2.4 子供向けに表示される広告が Designed for Families の広告のフォーマット要件を満たしている。
3. コンテンツのレーティングに関するアンケートで、次のようなアプリのインタラクティブ要素は正確に開示する必要があります。
 - 3.1 ユーザー間で交流や情報の交換ができる。
 - 3.2 ユーザーから提供された個人情報を第三者と共有する。
 - 3.3 ユーザーの物理的な場所を他のユーザーと共有する。
4. 子供向けアプリでは、Google ログインや Google Play ゲームサービスをアプリのログイン操作として使用することまで

Designed for Families 補足条項

2015年4月14日

Designed for Families プログラムを使用するよう設定することで、既存の Google Play デベロッパー販売 / 配布契約および Google Play デベロッパープログラムポリシー(「契約」)に加え、以下の条件に同意するものとします。この条件と契約の間に矛盾がある場合は、この条件が優先されます。かぎ括弧「」で囲んだ用語が以下で定義されていない場合は、「契約」で用いられている意味とします。

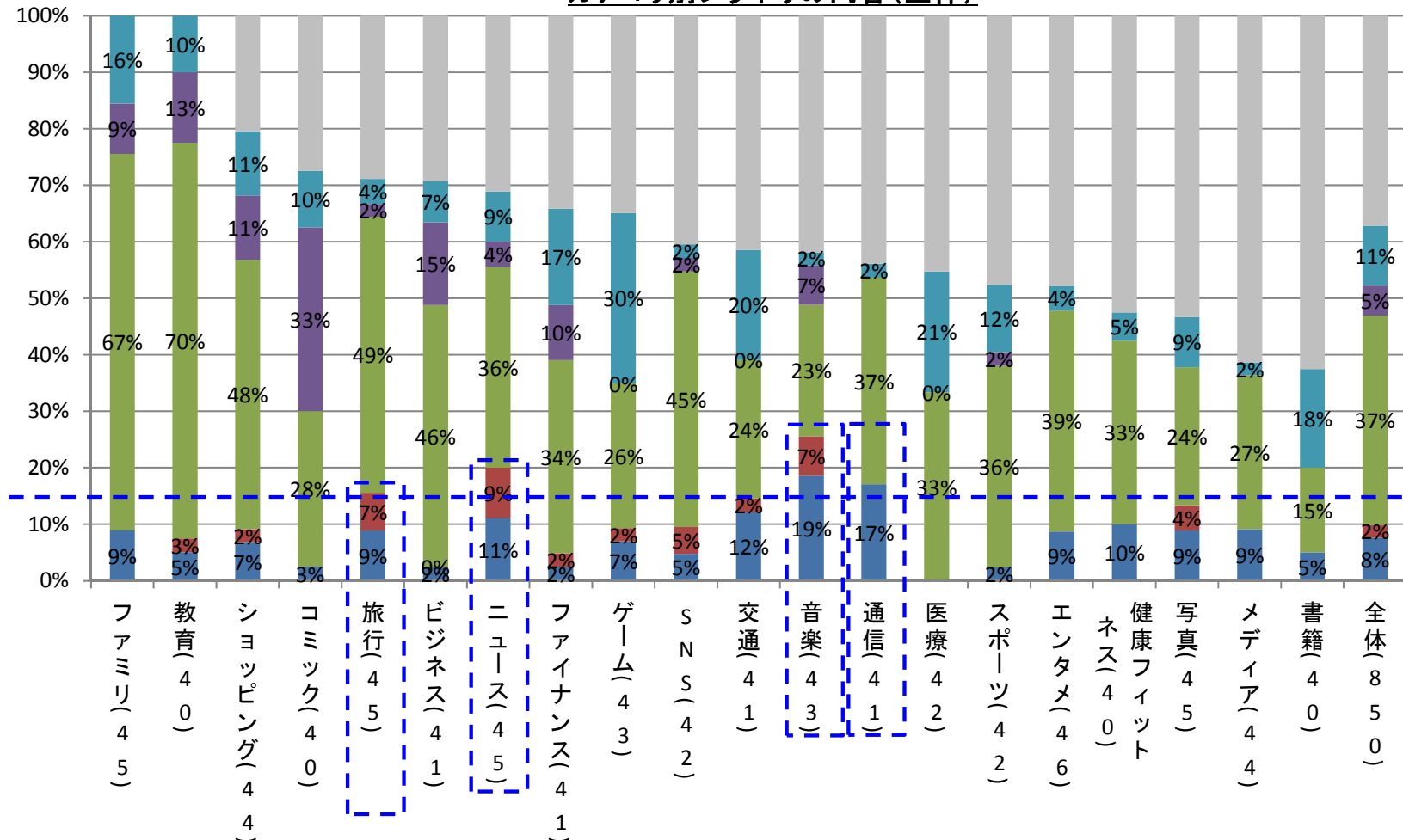
1. **参加**。Designed for Families プログラムに参加すると、子供やファミリー向けとしてアプリを宣伝できるようになります。このプログラムに参加している間は、Designed for Families プログラムの要件を遵守している必要があります。
2. **コンテンツのレーティング**。デベロッパーは、Google Play におけるアプリのコンテンツのレーティングを規定するために、正確かつ最新の情報を提供する責任を単独で負うものとします。
3. **Play ファミリー バッジ**。Designed for Families を使用するように設定すると、必ずアプリのターゲット ユーザーを選択することになります。デベロッパーは、選択したターゲット ユーザーにとって、アプリ(広告を含む)が適切なものであることに責任を負うものとします。
4. **法令遵守**。デベロッパーは、Designed for Families に提出したアプリ(およびそのアプリでサービスの提供に使用する API)が、COPPA(児童オンラインプライバシー保護法)およびその他の関連法規に準拠していることを表明します。デベロッパーは、ユーザーを対象としたプライバシー ポリシーを保持する必要があり、また、アプリによってユーザーから収集するデータの種類と用途を明確に開示する必要があります。
5. **承認と一般公開**。Designed for Families プログラムにアプリを提出すると、アプリは特別な審査の対象となります。各アプリを登録するかどうかの判断は Google の単独の裁量によるものとします。
6. **一時停止または解除**。Designed for Families プログラムの要件に準拠していないと、Designed for Families プログラムにおいてアプリが直ちに一時停止または除外されることがあり、場合によっては Google Play ストアから削除されることもあります。

3.2.アプリプラポリ調査 調査結果 (20カテゴリ：プラポリの内容の分類)

個々のアプリに言及したプラポリの割合(【A】・【B】の割合の合計)が全体平均より5%以上高いカテゴリは「旅行」、「ニュース」、「音楽」、「通信」の4カテゴリ。

プラポリの掲載率トップ3「ファミリー」・「教育」・「ショッピング」(前ページ参照)では、サービス全体やWebサイトに関するプラポリや個人情報保護方針の割合(【C】・【D】・【E】の割合の合計)が高くなっており、アプリを意識して作成されているプラポリは少ない。

カテゴリ別プラポリの内容(全体)



【A】・【B】の割合の合計が全体平均よりも5%以上高い(15%以上のライン)

- 【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

3.2.アプリプラポリ調査 調査結果（20カテゴリ：SPI8項目の記載）

「交通」、「音楽」、「通信」では11の調査項目のうち、8以上の項目が全体平均よりも5%以上高い数値になっている。

SPI8項目の記載率※

		ファミリ (n=45)	教育 (n=40)	ショッピ ング (n=35)	コミック (n=29)	旅行 (n=32)	ビジネス (n=29)	ニュース (n=31)	ファイナ ンス (n=27)	ゲーム (n=28)	SNS (n=25)	全体 (n=534)
①	情報を取得するアプリケーション提供者等	86.7%	100.0%	100.0%	100.0%	90.6%	100.0%	100.0%	92.6%	82.1%	92.0%	93.4%
②	取得される情報の項目	22.2%	32.5%	14.3%	17.2%	28.1%	24.1%	32.3%	3.7%	17.9%	16.0%	24.0%
③	取得方法	6.7%	7.5%	11.4%	10.3%	15.6%	13.8%	25.8%	3.7%	17.9%	20.0%	19.5%
④	利用目的の特定・明示	31.1%	37.5%	48.6%	20.7%	65.6%	10.3%	67.7%	29.6%	50.0%	64.0%	44.8%
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	15.6%	17.5%	34.3%	13.8%	25.0%	20.7%	19.4%	7.4%	14.3%	32.0%	24.9%
	利用者情報の削除の記載状況	35.6%	22.5%	57.1%	20.7%	34.4%	58.6%	38.7%	40.7%	35.7%	48.0%	41.0%
⑥	外部送信・第三者提供の有無											
	第三者への送信の有無の記載状況	48.9%	60.0%	91.4%	79.3%	65.6%	89.7%	83.9%	59.3%	60.7%	84.0%	74.2%
	利用者情報の送信先の記載状況	15.6%	17.5%	28.6%	34.5%	25.0%	31.0%	35.5%	22.2%	21.4%	20.0%	27.9%
	情報収集モジュールに関する記載状況	0.0%	0.0%	14.3%	13.8%	0.0%	17.2%	9.7%	3.7%	10.7%	12.0%	11.2%
⑦	問合せ窓口	68.9%	77.5%	82.9%	69.0%	90.6%	89.7%	67.7%	66.7%	75.0%	76.0%	75.3%
⑧	プライバシーポリシーの変更を行う場合の手続き	42.2%	70.0%	60.0%	55.2%	68.8%	72.4%	67.7%	51.9%	42.9%	68.0%	58.6%
		交通 (n=24)	音楽 (n=25)	通信 (n=23)	医療 (n=23)	スポー ツ (n=22)	エンタメ (n=24)	健康 フィット ネス (n=19)	写真 (n=21)	メディア (n=17)	書籍 (n=15)	全体 (n=534)
①	情報を取得するアプリケーション提供者等	95.8%	84.0%	100.0%	95.7%	90.9%	87.5%	89.5%	100.0%	76.5%	100.0%	93.4%
②	取得される情報の項目	29.2%	64.0%	39.1%	17.4%	9.1%	20.8%	26.3%	14.3%	29.4%	20.0%	24.0%
③	取得方法	41.7%	52.0%	34.8%	0.0%	18.2%	12.5%	31.6%	33.3%	41.2%	33.3%	19.5%
④	利用目的の特定・明示	54.2%	72.0%	60.9%	60.9%	40.9%	33.3%	36.8%	38.1%	70.6%	6.7%	44.8%
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	75.0%	60.0%	30.4%	17.4%	18.2%	12.5%	31.6%	23.8%	17.6%	26.7%	24.9%
	利用者情報の削除の記載状況	79.2%	60.0%	56.5%	30.4%	36.4%	37.5%	31.6%	33.3%	41.2%	26.7%	41.0%
⑥	外部送信・第三者提供の有無											
	第三者への送信の有無の記載状況	95.8%	80.0%	73.9%	82.6%	68.2%	62.5%	78.9%	76.2%	94.1%	80.0%	74.2%
	利用者情報の送信先の記載状況	33.3%	44.0%	26.1%	8.7%	27.3%	25.0%	57.9%	42.9%	29.4%	40.0%	27.9%
	情報収集モジュールに関する記載状況	33.3%	20.0%	17.4%	8.7%	4.5%	0.0%	26.3%	28.6%	11.8%	20.0%	11.2%
⑦	問合せ窓口	70.8%	84.0%	60.9%	65.2%	86.4%	79.2%	63.2%	71.4%	94.1%	60.0%	75.3%
⑧	プライバシーポリシーの変更を行う場合の手続き	50.0%	72.0%	69.6%	21.7%	59.1%	54.2%	52.6%	71.4%	82.4%	40.0%	58.6%

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。

※青字：全体平均よりも5%以上高い

※赤字：全体平均よりも5%以上低い

人気アプリはプライバシー性の高い情報を取得し得るアプリの割合が新着アプリや20カテゴリのアプリよりも高いが、取得し得る情報に関してアプリプラポリに記載があるアプリの割合が新着アプリや20カテゴリのアプリよりも高くなっている。

情報を取得し得るアプリのうちアプリ内で個別同意がある割合は、人気・新着アプリで10%強、20カテゴリのアプリで4%である。

【調査概要】

- 静的解析(注)によりプライバシー性が高い4つの情報を取得し得るアプリを抽出した。
 - ✓ プライバシー性が高い4つの情報：電話番号、アドレス帳、位置情報、メールアドレス
 - 抽出したアプリ(プライバシー性が高い情報を取得し得るとされたアプリ)に対して、取得し得る情報に関してプラポリ内での記載状況やアプリ内でのポップアップ等による個別同意状況を調査した。
- (注)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。また、実証実験側で実施している静的解析とは、解析手法が異なることにも留意が必要。

個別同意の取得状況 調査結果

調査項目	人気アプリ	新着アプリ	20カテゴリのアプリ
【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	59% (59/100)	16% (8/50)	38% (322/850)
【項目2】取得し得る情報に関して アプリプラポリに記載がある アプリ ※【項目1】でプライバシー性が高い情報を取得し得るとされたアプリのみ対象	36% (21/59)	13% (1/8)	22% (72/322)
【項目3】取得し得る情報に関してアプリ内でポップアップ等による 個別同意がある アプリ ※【項目1】でプライバシー性が高い情報を取得し得るとされたアプリのみ対象	12% (7/59)	13% (1/8)	4% (11/322)
【項目4】アプリプラポリへの記載、ポップアップ等による個別同意が どちらも無い アプリ ※【項目1】でプライバシー性が高い情報を取得し得るとされたアプリのみ対象	59% (35/59)	87% (7/8)	74% (239/322)

カテゴリ別の調査結果

調査項目	教育	コミック	医療	ファミリー	ファイナンス	書籍	メディア	健康フィットネス	エンタメ	音楽	ニュース	SNS	ゲーム	写真	スポーツ	ビジネス	ショッピング	交通	通信	旅行
項目1	5% (2/40)	13% (5/40)	14% (6/42)	18% (8/45)	20% (8/41)	20% (8/40)	20% (9/44)	30% (12/40)	30% (14/46)	37% (16/43)	38% (17/45)	40% (17/42)	42% (18/43)	42% (19/45)	43% (18/42)	44% (18/41)	48% (21/44)	80% (33/41)	83% (34/41)	87% (39/45)
項目2	50% (1/2)	20% (1/5)	50% (3/6)	13% (1/8)	25% (2/8)	13% (1/8)	11% (1/9)	33% (4/12)	14% (2/14)	38% (6/16)	41% (7/17)	18% (3/17)	17% (3/18)	11% (2/19)	17% (3/18)	22% (4/18)	10% (2/21)	24% (8/33)	21% (7/34)	28% (11/39)
項目3	0% (0/2)	0% (0/5)	0% (0/6)	0% (0/8)	14% (1/8)	0% (0/8)	13% (1/9)	0% (0/12)	8% (1/14)	0% (0/16)	0% (0/17)	0% (0/17)	0% (0/18)	0% (0/19)	0% (0/18)	0% (0/18)	5% (1/21)	10% (3/33)	6% (2/34)	5% (2/39)
項目4	50% (1/2)	80% (4/5)	50% (3/6)	88% (7/8)	63% (5/8)	88% (7/8)	78% (7/9)	67% (8/12)	79% (11/14)	63% (10/16)	59% (10/17)	82% (14/17)	83% (15/18)	89% (17/19)	83% (15/18)	78% (14/18)	90% (18/21)	67% (22/33)	79% (25/34)	70% (26/39)

情報の項目別にプライバシー性の高い情報の取得し得る割合を集計した結果、「位置情報」を取得し得るアプリの割合がどの調査対象においても最も高い。

プライバシー性の高い情報の取得し得る割合の調査結果

調査項目	人気アプリ	新着アプリ	20カテゴリのアプリ
「電話番号」を取得し得るアプリの割合	19% (19/100)	2% (1/50)	5% (40/850)
「電話帳」を取得し得るアプリの割合	26% (26/100)	4% (2/50)	10% (86/850)
「位置情報」を取得し得るアプリの割合	47% (47/100)	12% (6/50)	31% (262/850)
「メールアドレス」を取得し得るアプリの割合	21% (21/100)	6% (3/50)	4% (36/850)



カテゴリ別の調査結果

調査項目	教育	コミック	医療	ファミリー	ファイナンス	書籍	メディア	健康フィットネス	エンタメ	音楽	ニュース	SNS	ゲーム	写真	スポーツ	ビジネス	ショッピング	交通	通信	旅行
電話番号	0% (0/40)	5% (2/40)	0% (0/42)	0% (0/45)	7% (3/41)	3% (1/40)	2% (1/44)	3% (1/40)	7% (3/46)	2% (1/43)	0% (0/45)	2% (1/42)	2% (1/43)	4% (2/45)	2% (1/42)	5% (2/41)	2% (1/44)	7% (3/41)	34% (14/41)	7% (3/45)
電話帳	0% (0/40)	0% (0/40)	5% (2/42)	0% (0/45)	2% (1/41)	3% (1/40)	7% (3/44)	13% (5/40)	7% (3/46)	9% (4/43)	2% (1/45)	19% (8/42)	5% (2/43)	11% (5/45)	14% (6/42)	17% (7/41)	11% (5/44)	7% (3/41)	56% (23/41)	16% (7/45)
位置情報	5% (2/40)	5% (2/40)	14% (6/42)	13% (6/45)	7% (3/41)	18% (7/40)	16% (7/44)	30% (12/40)	22% (10/46)	23% (10/43)	31% (14/45)	36% (15/42)	35% (15/43)	38% (17/45)	38% (16/42)	29% (12/41)	32% (14/44)	80% (33/41)	56% (23/41)	84% (38/45)
メールアドレス	0% (0/40)	3% (1/40)	0% (0/42)	4% (2/45)	7% (3/41)	3% (1/40)	0% (0/44)	8% (3/40)	11% (5/46)	2% (1/43)	7% (3/45)	2% (1/42)	2% (1/43)	0% (0/45)	0% (0/42)	7% (3/41)	7% (3/44)	0% (0/41)	10% (4/41)	11% (5/45)

概要版の掲載率は人気アプリのiOSの6%。カテゴリ別の調査結果では「交通」や「ファミリー」の7%が最大であり、概要版を作成・掲載しているアプリは極めて少ない状況である。

アプリプラポリ概要版の掲載率 調査結果

対象OS	人気アプリ	新着アプリ	20カテゴリのアプリ
Android	1% (1/100)	2% (1/50)	2% (16/850)
iOS	6% (6/100)	0% (0/50)	***



カテゴリ別の調査結果(Android)

交通	ファミリ-	ニュース	エンタメ	健康フィットネス	通信	音楽	メディア	旅行	書籍
7% (3/41)	7% (3/45)	7% (3/45)	4% (2/46)	3% (1/40)	2% (1/41)	2% (1/43)	2% (1/44)	2% (1/45)	0% (0/40)

ビジネス	写真	SNS	コミック	ファイナンス	医療	スポーツ	ショッピング	ゲーム	教育
0% (0/41)	0% (0/45)	0% (0/42)	0% (0/40)	0% (0/41)	0% (0/42)	0% (0/42)	0% (0/44)	0% (0/43)	0% (0/40)

概要版の事例(出典:KDDI「au お客さまサポート」)

送信情報の概要

auお客さまサポート は、以下のお客様情報を外部送信します。

■送信するお客様情報

- ・ AuthToken (認証チケット)
- ・ cookie(ランダムに生成した識別ID)
※AuthTokenはCookieで送信しています。
- ・ ログイン情報から取得する電話番号
- ・ お客様による入力情報
アプリ内でお客さまが登録した情報 (au ID,パスワード,サポートID,パスワード,暗証番号)
内部ブラウザの遷移で画面(au お客さまサポートWEBサイト)より取得した情報
- ・ 端末から取得する広告ID(端末の設定で送信停止設定ができます)
- ・ 画面の閲覧数、クリック数などの数値情報

■送信する目的

- 認証・識別
- auお客様サポートでの利用のため
- アプリ・サービスの利用状況解析のため

■送信先

- KDDI株式会社
- KDDI株式会社(業務委託先：株式会社ビットセラー)
- Google Inc.

より詳細なアプリケーションプライバシーポリシーを [こちら](#) でご覧いただけます。

3.2.アプリプラポリ調査 調査結果（全アプリ：総括）

プラポリの記載状況について4点の基準を定め、それぞれの基準を満たすアプリの比率を記載した。

「基準①プラポリの掲載」、「基準②重要4項目の記載」の基準を満たしている人気アプリの割合は新着アプリや20カテゴリのアプリよりも高くなっている。

「基準③全8項目の記載」、「基準④概要版の掲載」については、全ての調査対象で基準を満たしている割合が10%以下。

		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) 「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 (全8項目の記載) 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・掲載している※ (概要版の掲載)
Android	人気	78%	51%	10%	1%
	新着	64%	26%	10%	0%
	20カ	63%	33%	10%	1%
iOS	人気	68%	32%	9%	2%
	新着	46%	10%	4%	0%

10%以下

※「20カ」:「20カテゴリ」の略。

※概要版が存在するアプリプラポリの中には基準③も満たしていないアプリも存在するため、基準④は概要版の掲載率と一致しない。

現状分析と傾向	<p>○人気アプリのプラポリの掲載率はAndroid、iOSともに70%前後に達している。Androidの新着アプリ、20カテゴリのアプリの掲載率も60%以上に達しており、「<u>プラポリの作成・掲載</u>」については浸透してきたと考えられる。(P6、P9)</p> <p>○しかし、大半のプラポリの内容は会社全体やサービス全体の個人情報の取り扱いに関してのみ述べたものであり、「<u>アプリが取得する利用者情報を意識して記載されているプラポリ</u>」は少ない。(P7、P11)</p> <p>○プライバシー性が高い情報取得に対する同意取得状況については、人気アプリが他のアプリよりも取得率が高いものの、プラポリでの取得情報に関する記載率が高い。(P13)</p> <p>○概要版は、<u>昨年同様、ほとんど作成されていない</u>。(P15)</p>
環境変化	<p>○GoogleやAppleが<u>特定カテゴリのアプリや特定フレームワークを利用するアプリに対して、プラポリ掲載を義務付けており、「プラポリの作成・掲載」は更に浸透していく可能性は存在</u>。</p> <p>○Android 6.0では、連絡帳や位置情報などのパーミッションはアプリ内で個別に取得するようになり、また、利用者が<u>端末の画面でアプリごとにアクセス可能な情報を設定できるようになるため、利用目的等を記載したプラポリの記載内容の重要性が増す可能性が存在</u>。</p>
今後の課題・取組	<p>○「<u>アプリ毎のプラポリ</u>」作成が原則ではあるものの、「<u>複数のアプリに関するプラポリ</u>」・「<u>サービス全体のプラポリ</u>」の掲載率が大半を占めるため、「<u>複数のアプリに関するプラポリ</u>」・「<u>サービス全体のプラポリ</u>」に対する評価やルールについて検討が必要ではないか。</p> <p>➤ 現状では「<u>複数のアプリに関するプラポリ</u>」も、「<u>アプリを意識していない「サービス全体のプラポリ</u>」(会社全体の個人情報の取扱い等)も、プラポリの内容分類では【C】とされてしまうため、実態を把握するためには、【C】の評価を細分化する必要があるのではないか。</p>

4.1.利用者情報の取扱いに関する調査の実施概要

「関係団体等における取組状況に関する調査・分析」、「諸外国における取組状況に関する調査・分析」、「ウェアラブルデバイス等新技術に関する調査・分析」について、下記のような観点で調査を実施した。

関係団体等における取組状況に関する調査・分析

【調査概要】

- ◆ 民間事業者・業界団体等の取組を調査し、過去の調査内容をベースに、最新の情報を更新した。

【調査対象の事業者等】

- ◆ 業界団体
- ◆ 情報収集モジュール提供者
- ◆ アプリマーケット運営事業者（OS提供事業者、モバイルキャリア）
- ◆ アプリ提供者 等

諸外国における取組状況に関する調査・分析

【調査概要】

- ◆ 諸外国の取組状況を①～③の観点で調査した。
 - ①政府における取組
 - ②業界団体における取組
 - ③その他関係し得る事業者における取組

【調査対象国】

- ◆ 米国
- ◆ 欧州（EU、フランス、イギリスなど）
- ◆ 韓国
- ◆ 香港

ウェアラブルデバイス等新技術に関する調査・分析

【調査概要】

- ◆ スマートフォンと連動するウェアラブルデバイスについて、①～④の観点で調査した。
 - ①サービス動向調査
 - ②利用者情報の取扱いに関する実態調査
 - ③諸外国の先端的な取組についての調査
 - ④その他、セキュリティ等関係しうる諸課題の整理

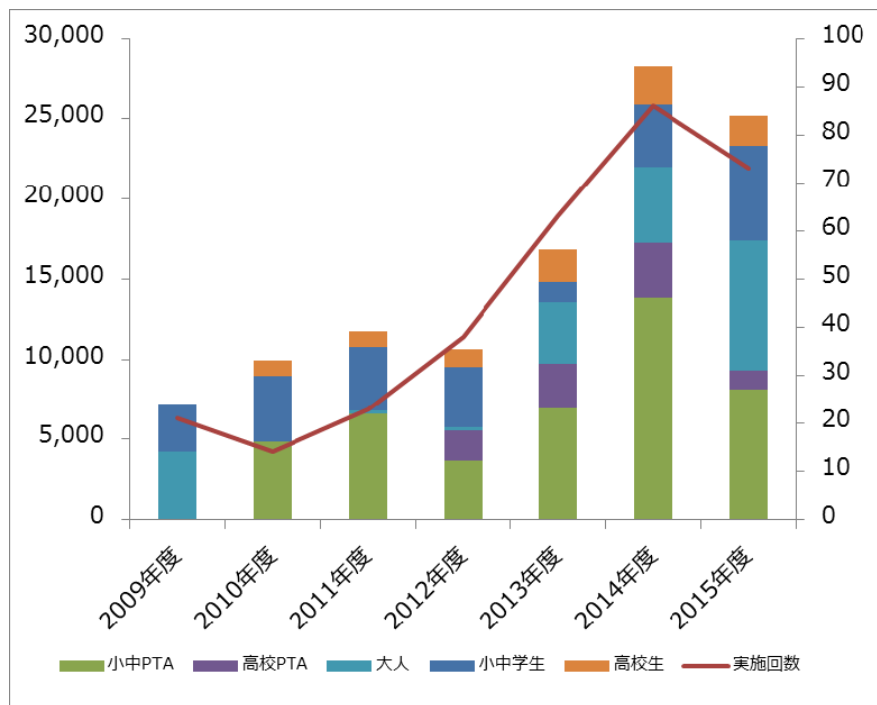
【調査対象】

- ◆ スマートフォンと連動するウェアラブルデバイス
- ◆ ウェアラブルデバイスと連携するスマートフォン上のアプリ

【安心ネットづくり促進協議会】

- 2009年2月、これまで普及啓発活動等に各々取り組んできた利用者・産業界・教育関係者等が相互に連携してよりわかりやすく国民一人ひとりへの浸透を図る目的で設立。
- 活動キャッチフレーズ「1億人のネット宣言 もっとグッドネット」を掲げ、全国各地での普及啓発イベントの開催のほか、スマートフォン等に関する課題を検討し提言を行うなど、民間主導により様々な活動を実施。

啓発事業開催状況（2009年度～2015年度）



2015年度は2016年2月29日時点

<参考> ホームページ、啓発リーフレット等



【ホームページ】

「知りたいことを教えてくれる安心協」をキャッチフレーズに、「提供する情報」と「知りたい情報」をつなぐ協働の場を目指す。



【保護者のためのスマホ安心安全ガイド】

保護者向けに、青少年のスマートフォン利用のリスクと対策を具体例を用いてわかりやすく解説したリーフレットを研修会等で配布する。

【低年齢層へのアプローチ】

インターネット利用の低年齢化の傾向を捉えて、低年齢層とその保護者のネット利用実態、保護者の意識についてのアンケート調査を実施し、現状と課題について認識を行うことで、普及啓発活動の手法・テーマ等への提言を行う。

PTA等の保護者向け研修会の実施



青少年向けのイベントの実施



その他、街頭等でのイベントの実施



【一般社団法人 日本オンラインゲーム協会(JOGA)】

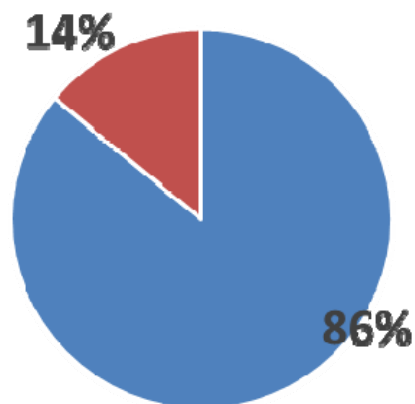
「SPI」のプライバシーポリシー遵守状況 アンケート調査結果

- 2015年の12月にJOGAは会員企業に対して、「SPI」のプライバシーポリシー遵守状況に関するアンケートを行った。
- アンケートの結果、回答した全企業が全てのタイトルもしくは一部のタイトルでプラポリの提示を行っている。86%の企業が全てのタイトルでSPI8項目全てを提示しており、残りの14%は全てのタイトルもしくは一部のタイトルで一部の項目のみを記載している状況である。

《設問》

個人情報保護に関する法令及びガイドラインを遵守し、総務省が策定した「スマートフォンプライバシーイニシアティブ」のプライバシーポリシーに準拠する形で、下記の事項についてプライバシーポリシーを作成し、利用者が容易に参照できる場所に掲示またはリンクを貼ることで明示する。

- ① 情報を取得するゲームアプリ事業者等の氏名または名称
- 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・公表または同意取得の方法、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



- 全てのタイトルでプライバシーポリシーとして上記①～⑧の全てを掲示している。
- 全てまたは一部のタイトルでプライバシーポリシーとして上記①～⑧の一部を掲示している。
- 全てまたは一部のタイトルでプライバシーポリシーは掲示していない。

【一般社団法人 電気通信事業者協会(TCA)】

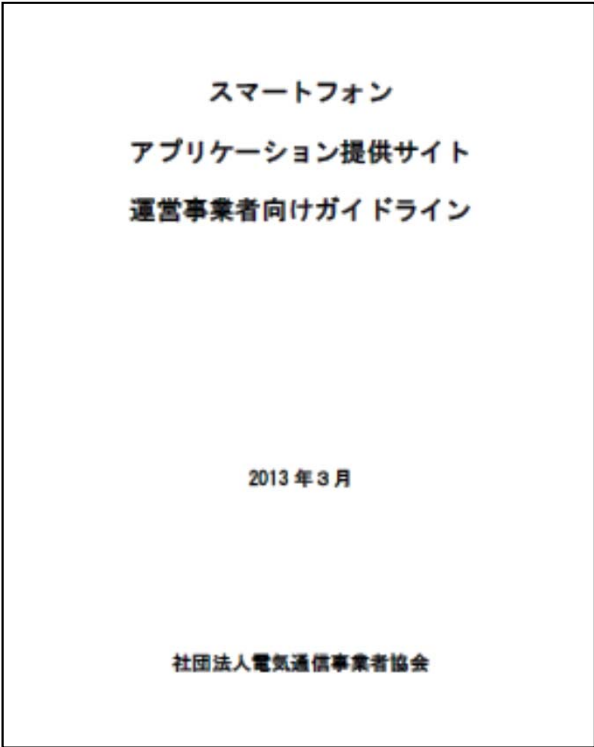
TCAの取組

TCAのホームページ上に

- スマートフォンアプリケーション提供サイト
運営事業者向けガイドライン

を掲載し、運営事業者や開発者への啓発を図っている

運営事業者向け
ガイドライン



携帯電話事業者の取組

契約の際に、重要事項説明ツールを配布し、スマートフォンとフィーチャーフォンとの違いなどについて利用者への注意喚起を図っている。



ケータイ電話教室にて啓発活動を展開し、利用者への注意喚起を図っている。携帯電話事業者の1社の教室では、2014年度に約7,000回の教室を開き、約103万人の消費者が受講している。



スマホ端末の設定画面でも「プライバシー」や「セキュリティ」の設定ができます。

ケータイ電話教室での配布資料では、フィルタリングソフト・サービス、ウィルス対策やセキュリティ対策、家庭でのルール作りなどについて普及・啓発を行っている。

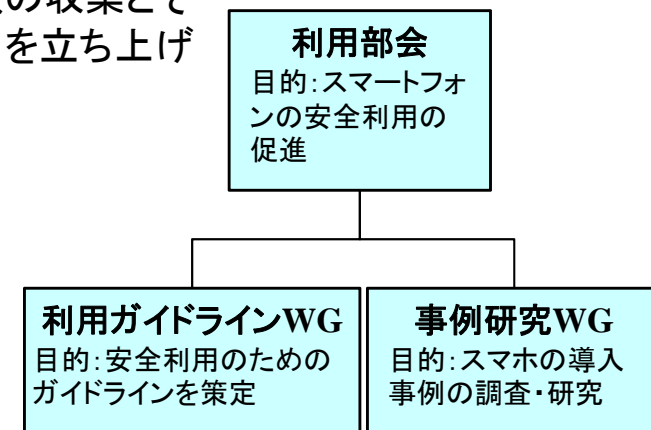


【一般社団法人 日本スマートフォンセキュリティ協会(JSSEC)】

利用部会

- JSSECの利用部会は「スマートフォンの安全利用促進のための『事実』に基づいた情報の収集とその共有のための情報発信」を目的とし、2つの「利用ガイドラインWG」、「事例研究WG」を立ち上げて、活動を行っている。
- 「利用ガイドラインWG」の目的・活動内容
 - 目的:スマートフォンの利用状況に沿った安全利用のためのガイドラインを策定
 - 活動内容:スマートフォンを業務利用する際のセキュリティガイドラインの策定
 - 事例体系化を基にした利用者の利用シーンに合わせたガイドラインを目指す
 - 事例体系化の分析を踏まえて広い用途で実践的に利用できるものを目指す
- 「事例研究WG」の目的・活動内容
 - 目的:導入事例についての調査・研究を実施
 - 活動内容:利用ガイドラインWGの成果を現実と比較確認のための事例の収集

利用部会の体制



スマートフォン&タブレットの業務利用に関するセキュリティガイドライン

- JSSECは2014年4月にスマートフォンの利用シーンという観点から、企業や組織が考慮しなければならないセキュリティ上の脅威と対策を明確化した「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン」の第2版を発行した。(第1版は2011年12月に発行)。
- 同ガイドラインの構成は下記の通り。
 - スマートフォンの利活用によるメリット
 - スマートフォンのしくみと概要
 - スマートフォンの特性と留意点
 - 利用シーンから見る脅威と対策
 - ライフサイクルにおける留意点
 - 付録A(対策チェックシート)
 - 付録B(BYODの現状と特性)

A-1 特性格別 対策チェックシート

章番号	分類	脅威	対策 または 要件	推奨レベル
4.2	特性から見る脅威	デバイスの盗難、紛失	・ デバイスをロック設定する。 ・ ロック解除失敗時に強制的にデータを消去する。 ・ 本体および外部記憶媒体のデータ領域を暗号化する。 ・ ユーザIDやパスワードを非保存設定にする。 ・ 定期的にデータのバックアップをとる。 ・ 不要になったデータをデバイスから削除する。	■ □ □ □ □ □
		SIMカードの盗難	・ 通信事業者へ連絡し回線利用を停止する。	■
		水没や落下による故障	・ 定期的にデータのバックアップをとる。 ・ 落下防止用ストラップ等を装着する。 ・ 防水や衝撃耐性の高いデバイスを選択する。	□ □ □
		覗き見	・ 覗き見防止シート等を装着する。	□
		誤認識	・ 慎重に操作するよう注意を喚起する。 (静電容量方式を採用したパネルが多いため、静電気の影響を受けやすい)	□
		脆弱性	・ デバイスやOSの種類を絞り込む、または統一する。	□
		信頼できないマーケット	・ 信頼できるマーケットからアプリケーションを入手する。 ・ アプリケーションのインストール時に不用意にアクセス許可をしない。 ・ アプリケーションに関する最新情報(不正な動き、意図しない動き、信頼できる情報等)を入手する。 (5.9節「アプリケーションを利用する」参照)	■ □ □
		利用者による改造	・ 改造を禁止する。	■



【一般社団法人 モバイル・コンテンツ・フォーラム(MCF)】

スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン

- MCFはアプリ提供者が、利用者に対して分かりやすく透明性が高い説明を行い、理解と有効な選択を促すことを目的とした、「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」を策定し、2012年11月に内容を公表した。
- ガイドラインでは、「アプリケーション・プライバシーポリシー」の実装にあたって考慮すべき具体的な要件や、実装にあたってのモデル案が記載されており、実践的な内容となっている。

ガイドラインの構成

- アプリケーションプライバシーポリシーの実装にあたっての推奨要件の整理
 - SPIを踏まえて実装するにあたっての具体的な要件を整理(名称、提示タイミング、掲載場所、変更プロセス、個別同意が望ましい情報の種類など)
- アプリケーションプライバシーポリシーのモデル案
 - アプリプラポリに記載すべき項目についての詳細な解説、具体的な文面案

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

- 総務省のSPIの公表等の動きを受けて、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」を公表した。
また、同時に、プライバシーマーク付与を受けようとするスマートフォン等におけるアプリケーション配信事業を行う事業者(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。
- 同ガイドラインの中では、スマートフォン等におけるアプリケーション配信事業を行う事業者に対して、下記の取組を行うことを推奨。
 - 特定の個人が識別できる個人情報に該当する利用者情報(電話帳、入力フォームから取得する氏名、写真・動画など)に対する、個別の個人情報の特定・リスク分析(リスクの認識、分析及び対策)の実施
 - 特定の個人が識別できる可能性がある利用者情報(契約者・端末固有ID、位置情報、通信履歴、アプリケーション利用履歴など)について、事業の用に供する個人情報と同等に位置付けて、リスクの認識、分析及び対策の実施
 - アプリケーション・プライバシーポリシーの通知又は公表

【老テク研究会】

「スマートスクール」・「スマホサロン」・「スマートカフェ」の実施

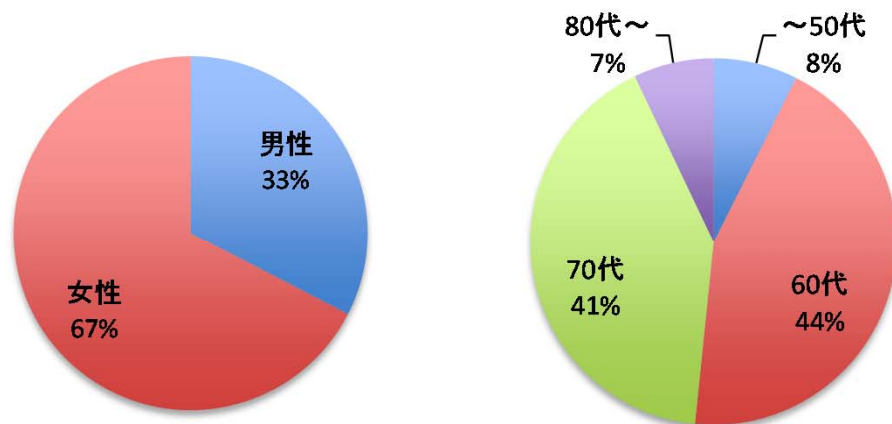
《スマートスクール》

- 高齢者を対象に4週間スマートフォンを貸与し、週1回3時間、計12時間の無料スマホ講習会。（2013年11月-2015年3月）
- 全国（青森、仙台、東京、千葉、横浜、愛知、滋賀、京都、大阪、香川、広島、福岡、佐賀）で2,000名の高齢者が受講。
- スマートフォンの基本操作、情報バリアフリー機能、地図、カメラ、LINE、災害時での活用、情報セキュリティ対策等を紹介した。
- 老テク研究会がサムスン電子ジャパン(SEJ)に推薦した団体、有識者で構成されるスマートスクール推進協議会が同スクールの企画・運営を担当。運営費、端末(SIM有)、通信料や教材をSEJが支援した。大阪NHKホールでのフォーラムには800名が参加。

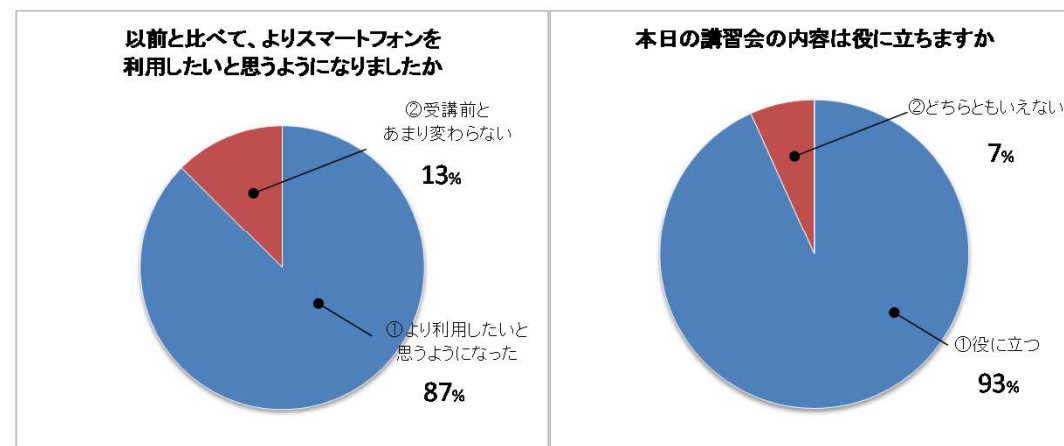
《スマホサロン》 《スマートカフェ》

- 高齢者、女性、障がい者を対象の無料スマホ講習会。SEJが端末や運営費を支援し、SIMカードを携帯キャリアが貸与した地域もある。スマホ料金や契約についての説明には一般社団法人全国携帯電話販売代理店協会が協力。2015年は約2,500名が受講した。

スマートスクールの参加者属性



スマートスクールの受講者へのアンケート結果



4.2.関係団体等における取組状況に関する調査・分析 調査結果 (情報収集モジュール提供者)

【株式会社ファンコミュニケーションズ、株式会社VOYAGE GROUP】

情報収集モジュールの利用規約におけるアプリ提供者へのプラポリ掲載の要請

- ファンコミュニケーションズ、VOYAGE GROUPでは、モジュールの利用規約の中で、アプリ提供者に対して、モジュールが取得する情報やモジュール・事業者に関するプラポリを、アプリの利用者に通知することを求めている。

VOYAGE GROUPの利用規約における該当する文面の抜粋

第6条（情報の取得及び告知）

- 本サービス利用者は、前項に定める当社の情報の取得及び利用について、自らの責任において利用規約等に明記し、ユーザーの承諾を得ると同時にプライバシーポリシー等に定めなければなりません。
- 当社が指定する広告モジュールを組み込む場合、本サービス利用者は、必ず以下の項目を利用規約に明記しなければなりません。
 - (1) 当社名及び当社の広告モジュールを組み込むこと
 - (2) 広告モジュールで収集する情報及びその目的
 - (3) 当社のプライバシーポリシーのURL (<http://zucks.co.jp/privacy/>)

情報収集モジュール専用のプライバシーポリシーの作成・掲載

- ファンコミュニケーションズでは、アプリ提供者及びアプリの利用者向けに、モジュール専用のプラポリを作成し、モジュールが取得する情報や利用目的、第三者提供の有無、ユーザ関与の方法等を公表している。

ファンコミュニケーションズのモジュールのプライバシーポリシー（抜粋）

第1条（定義）

この広告配信用モジュール・プライバシーポリシー（以下、本プライバシーポリシーといいます）は、株式会社ファンコミュニケーションズ（以下「当社」という）が提供するスマートフォンアプリケーション広告配信用モジュール「nend SDK」（以下、本モジュールといいます）およびアプリケーションに本モジュールの組み込みを必要とするサービスである nendメディアパートナーサービス（以下、本サービスといいます）に関するユーザー情報の取扱いを定めたものです。なお、本プライバシーポリシーにおいて定めのない用語の定義は、nendメディアパートナーサービス利用規約に定める定義に従います。

第2条（取得される情報の項目、利用目的）

本モジュールおよび本サービスは、以下のユーザー情報を以下の利用目的のためにアプリケーション経由で自動的に取得しサーバに送信します。

利用目的	取得する情報の項目
(1) 本サービスにおいてメディアパートナーごとに発行するキーで広告配信のため	apikey/spotID
(2) 本サービスにおける広告配信のため	<ul style="list-style-type: none"> ・OS/OSバージョン ・言語設定 ・機種名/デバイス名 ・nendSDKバージョン ・接続IPアドレス

4.2.関係団体等における取組状況に関する調査・分析 調査結果 (アプリマーケット運営事業者)

【Google】

アプリに対する「ファミリー向け」の認定の追加

- Googleは2015年4月に「Designed For Families」という開発者プログラムを発表した。このプログラムでは、開発者はアプリを追加の審査に出して「ファミリー向け」の承認を受けることができる。
- 2015年6月にGoogle Playのカテゴリに新カテゴリ「ファミリー」が追加され、「ファミリー向け」の承認を受けたアプリがまとめられている。
- 「ファミリー向け」の承認を受けるためには、ESRB(※)による「Everyone」または「Everyone 10+」の評価の取得(もしくは同等のレーティングの取得)、プラポリのリンクの掲載、表示広告がGoogleが定める要件を充足するなどの条件を満たす必要がある。

※ESRB: Entertainment Software Rating Boardの略。米国及びカナダにおけるコンピュータゲームのレーティングなどの審査を行う団体。

Android 6.0でのパーミッションモデルの変更

- Android 6.0ではパーミッションモデルが変更され、インストール時には危険ではないパーミッションのみ付与し、危険なパーミッションはアプリ内で個別にユーザから許可を取得するモデルとなった。
 - 危険なパーミッションとして、カレンダー、カメラ、電話帳、位置情報、マイク、電話、センサー、SMS、ストレージに関するパーミッションがAndroidのデベロッパページに記載されている。
- アプリインストール後も、ユーザが端末の設定から、各アプリのパーミッション(情報取得の権限)のオン/オフを切り替えられる。

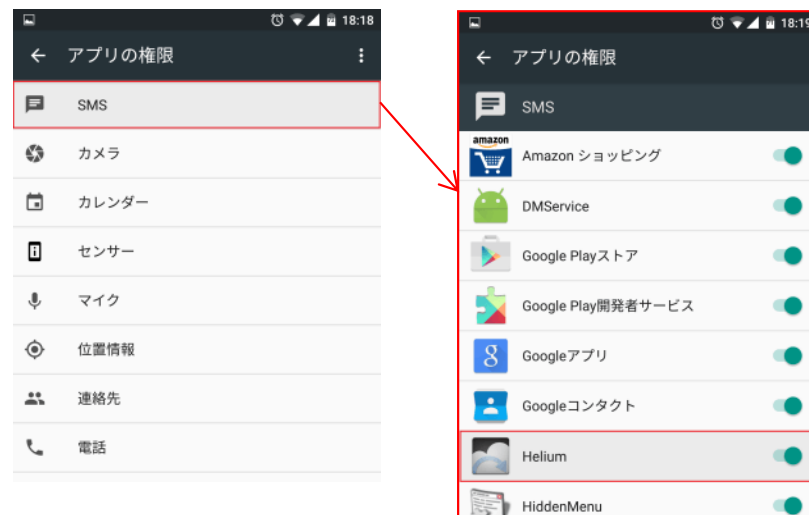
アプリ内でのパーミッションの取得画面



アプリ別のパーミッションの管理



パーミッション別での管理



4.2.関係団体等における取組状況に関する調査・分析 調査結果 (アプリマーケット運営事業者)

【Appleの取組】

アプリのダウンロード状況取得の禁止

- 2015年6月に新iOS9では、アプリが利用者のアプリのダウンロード情報の取得を禁止する方向であると一部のメディアで伝えられた。
 - 一部の広告配信モジュールがアプリのダウンロード情報を取得し、利用者が好むようなアプリや利用者がインストールしていないアプリの広告を表示していた。

アプリの通信の暗号化を強化

- 2015年9月に公開されたiOS9では「App Transport Security」(以下、「ATS」)という機能が追加された。
- 端末のATSを有効にしている場合(デフォルトではATSは有効)、Appleが推奨する条件を満たさない接続(HTTPでの通信等)は、接続失敗扱いとなる。

特定のアプリに対するプラポリ掲載の義務化

- AppleはiOSのアカウント登録またはユーザの既存アカウントへアクセスするアプリについて、アプリの紹介ページへのプラポリ掲載を義務付けている。
- 例えば、「HealthKit」に関する開発者向けのリファレンスでは、“You must also provide a privacy policy for any app that uses the HealthKit framework.”という記載が存在している。

4.3.諸外国における取組状況に関する調査・分析 米国

【2015年2月】大統領が「消費者プライバシー権利章典法案」を議会に提出

- 《背景》2012年2月に公表された「消費者プライバシー権利章典」を、2014年に米国内でサイバーセキュリティやデータ保護の問題が多発したことを受け、2015年1月オバマ大統領が制度改革を行なうことを発表し、法案として提出した。
- 《内容》個人データの定義が行われており、特定の個人だけでなく、端末に結びつくデータも個人データに含まれるとされている。

項目	概要
個人データの定義	個人データとは、(1)合法的な手段により一般に利用可能な場合を除き、適用対象事業者が管理し、かつ(2-1)適用対象事業者によって 特定の個人 に結びついた、若しくは実際に結びつけられうる、又は(2-2) 個人 に関係付けられた、若しくは個人が日常的に使用する 端末 に結びつく、すべてのデータをいう。(§ 4(a)(1)) ※個人データに該当するものとして、端末ID、生体認証情報などが例示列挙されている。
エンフォースメント	【FTC】これまで通り、FTC法第5条に基づいて執行可能 【罰則】最大で2,500万ドル(日本円で約30億円)の罰金(§ 203(a)(3))

【2015年9月】FTCが「子供向けアプリのフォローアップ調査」を公表

- 《背景》GPEN(※)における2015年の調査の一貫として、FTCが子供向けアプリの調査を実施した。
- 《内容》プラポリの掲載率だけでなく、米国でもパケットキャプチャによる動的解析が行われている。調査結果は2012年と比較して、プラポリの掲載率が上昇していた。動的解析の結果は非公開となっている。

項目	概要
調査対象・方法	<ul style="list-style-type: none"> ● Apple Store 及びGoogle Playにおける子供向けアプリ364個 ● 各マーケットで“kids”というワードで検索し、該当したアプリを対象としている。 ● 送信情報をパケットキャプチャによって解析(解析結果は非公表)
調査結果	<ul style="list-style-type: none"> ● アプリ紹介ページにプラポリへのリンクがあったアプリ: 約45% (2012年12月の調査では、20%弱) ● アプリ内又はデベロッパーページなどにプラポリが掲載されていたアプリ: 約10% ● アプリ紹介文に第三者提供などについて記載していたアプリ: 約13%

※Global Privacy Enforcement Network(GPEN)は、プライバシーに関する越境執行協力のための各国プライバシーコミッショナーの集まりである。2014年9月時点では、51のプライバシーコミッショナーが参加している。

- 《プラポリ掲載率向上の背景》2013年に改正児童オンライン・プライバシー法(COPPA)が施行され、Google及びAppleが、アプリ紹介ページにプラポリ掲載場所を設置した。Appleは、子供向けのカテゴリを設置し、情報を収集するすべてのアプリに対して、利用者がアプリをダウンロードする前にプラポリを提示することをデベロッパーに要求している。

4.3.諸外国における取組状況に関する調査・分析 米国・EU

【2015年9月】米国広告事業者業界団体DAA(※)がモバイルアプリプライバシーのガイドラインを施行

- 《背景》2013年7月にガイドライン「モバイル環境に対する自主規制原則の適用」が策定されたが、消費者のオプトアウトを支援するツールが開発されるまで、施行されないこととされていた。2015年9月、支援ツールが開発されたことに伴い、ガイドラインが施行されることとなった。
- 《自主原則の内容》

原則	概要
透明性・コントロール	● 情報の取扱いに係る通知や同意の取得について、情報の種類ごとに規定している。
目的制限	● 雇用、社会保険等のために、収集、使用及び提供してはならない。
センシティブデータ	● サードパーティーは、個人の同意なく、口座情報、社会保障番号、医療情報が含まれるアプリケーションのデータを収集してはならない。
セキュリティ	● 適切な物理的、電子的及び管理的安全措置を実施しなければならない。

- 《開発された支援ツール》オプトアウト支援アプリ「AppChoices」では、モジュールのオプトアウトを一括で実施できる。
- ※ Digital Advertising Alliance (DAA)は、米国におけるオンライン広告事業者の業界団体である。広告事業者だけでなく、自動車業界など幅広い分野の事業者が会員となっている。

【2016年4月】欧州議会の本会議でデータ保護規則(案)が可決(採択)

- 《目的》加盟国の個人情報保護法にばらつきがあり、域内での自由な経済活動を阻害していたため、制度の統一化を図るため。
- 《内容》技術進歩を踏まえて、位置情報などが個人データに該当することや新たな権利が明記された。

項目	概要
個人データの定義	<ul style="list-style-type: none"> ● 「個人データ」とは、識別された、又は識別可能な自然人(データ主体)に関するすべての情報をいう。 ● 「識別可能な自然人」とは、特に、当該自然人の、氏名、個人識別番号、位置情報、オンライン識別子又は、肉体的、生理的、遺伝的、精神的、経済的、文化的並びに社会的アイデンティティに特有な一つの並びにそれ以上の要素を参照することで、直接的又は間接的に識別され得る者をいう。(データ保護規則第4条(1))
主な内容	<ul style="list-style-type: none"> ● 新たな権利の明確化(忘れられる権利等) ● 中小企業に対する手続の簡素化 ● 現状を踏まえた明確なルールの整備 ● 法執行機関における個人データの取扱い ● 罰則の強化

《今後の予定》同規則の発効日から2年後を目途に加盟国に直接適用される。

4.3.諸外国における取組状況に関する調査・分析 仏国

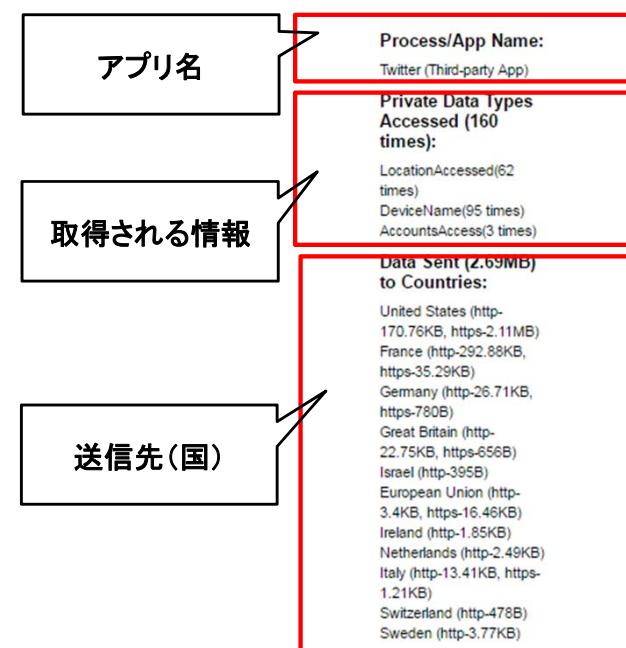
【2015年1月】 仏INRIAとCNILがアプリの情報収集・送信に関する実態調査の結果を公表

- 《背景》フランス国立情報学自動制御研究所(INRIA) (※1)とフランスの情報処理および自由に関する国会委員会(CNIL) (※2)は、スマートフォン上のアプリによる個人データの取扱いの実態を把握するため、“Mobilitics”と呼ばれるプロジェクトを実施している。
- 《内容》iOS・Androidそれぞれについて、アプリによる情報の収集・送信を解析するためのツールを開発した。同プロジェクトでは、3ヶ月間実際にアプリを利用者に使用してもらい、アプリによって取得された情報や送信先、調査期間における取得や送信の頻度を解析している。調査結果(アプリ名、送信された情報及び送信先)は、Mobiliticsプロジェクトのホームページ上で公開されている。

調査の概要

項目	概要
調査対象・方法	<ul style="list-style-type: none"> ● 被験者にMobiliticsがインストールされた端末を3ヶ月間使用してもらい、データへのアクセス頻度や送信先を調査した。 ● Mobiliticsは、送信先を特定するために、パケットキャプチャによって、データ収集し、解析する。
調査結果	<ul style="list-style-type: none"> ● Android、iOSともに、50～60%のアプリがある端末識別子にアクセスしている。 ● ある端末では、3ヶ月の間にSNSアプリが 15万回以上端末の位置情報にアクセスしていた。 ● プリインストールされたアプリでは、3ヶ月の間に100万回以上位置情報にアクセスしていた。

Mobiliticsによる解析結果の例



※1 フランス国立情報学自動制御研究所(INRIA)は、経済・財務省及び国民教育・高等教育・研究省傘下のコンピューターサイエンスに関する国立の研究機関である。情報セキュリティ、ネットワーク、画像処理等幅広くコンピューターサイエンスに係る研究開発を行っている。

※2 フランスの情報処理および自由に関する国会委員会(CNIL)は、フランスのプライバシーコミッショナーであり、独立した権限を有する独立行政機関である。

4.3.諸外国における取組状況に関する調査・分析 韓国

【2015年8月】韓国政府は「スマートフォンアプリプライバシーガイドライン」を公表

- <<目的>> アプリ開発者・アプリ提供者、アプリ開発環境(OS・アプリマーケットなど)を改善し、利用者がアプリの権限(アプリが取得できる情報等)やアプリ利用時の同意内容を簡単に理解できるように、情報を分かり易く公開することによる、利用者の自己情報統制権(プライバシー権)を確保すること
- <<内容>> 「アプリ開発」、「アプリマーケット登録」、「(利用者による)アプリ利用・削除」の各段階で、OS提供者、アプリ提供者が守るべきルールを策定している(下表はアプリ開発者が守るべきルールを抜粋したもの)。

項目	概要
アプリ開発	<ul style="list-style-type: none"> ● サービス提供に必要な範囲内でのアプリの権限の設定 ● 同意を得た範囲内で、端末情報の取得・送信する旨をプライバシーポリシーに明記 ● 同意の取得後でも、利用者がアプリのアクセス権限を事後的に変更できる機能の提供
アプリマーケット登録	<ul style="list-style-type: none"> ● アプリのアクセス権限の設定、端末情報アクセス時の利用者への告知手順の確認 ● 情報通信網法における個人情報の収集・保管・利用・提供・破棄規定の遵守の確認
(利用者による)アプリ利用・削除	<ul style="list-style-type: none"> ● 必須事項(利用規約、個人情報の取得・利用など)をワンクリックで同意できる画面の提供 ● 個人情報の第三者提供、マーケティング利用などの必須ではない項目の個別同意 ● 脱退申込メニューを分かり易い位置に配置、申込先のプライバシーポリシーへの記載

必須事項をワンクリックで同意できる画面の提供

※ 아이디
※ 비밀번호
※ 비밀번호 재확인
※ 이름
※ 이메일

[필수] 서비스 이용약관 주요내용보기 전문보기

[필수] 개인정보 수집 및 이용 동의 전문보기

약관 및 개인정보 동의내용을 확인하였으며 위 내용에 동의합니다.
(만14세 미만 아동은 회원가입이 제한됩니다)

- ①利用規約の主な内容を提示
 - ②利用規約の全文の提示
 - ③個人情報の収集・利用の同意に関する文面の提示
- ※**プライバシーポリシーの全文を表示しての同意は、法的に正当な同意とはみなされない**
- ④必須項目である利用規約・個人情報の収集・利用に関してワンクリック同意

必須ではない項目(第三者提供、マーケティング利用等)の個別同意

[선택] 개인정보 마케팅 활용 동의 ①

목적	항목	보유기간	동의여부
신규서비스 안내 등 마케팅 활용	이메일 휴대전화번호	회원탈퇴 후 5일까지	동의함 <input type="checkbox"/> 동의안함 <input type="checkbox"/>
상품추천 등 맞춤형 광고	쿠키 정보	회원탈퇴 후 5일까지	동의함 <input type="checkbox"/> 동의안함 <input type="checkbox"/>

※ 동의하지 않는 경우에도 서비스는 이용하실 수 있습니다.

[선택] 개인정보 제3자 제공 동의 ②

제공 받는자	목적	항목	보유기간	동의여부
㈜○○○	㈜○○○ 마케팅	이름 휴대전화번호	동의일 부터 1년	동의함 <input type="checkbox"/> 동의안함 <input type="checkbox"/>
㈜○○○	고객 맞춤형 상품 추천	아이디 쿠키 검색이력	동의일 부터 1년	동의함 <input type="checkbox"/> 동의안함 <input type="checkbox"/>

※ 동의하지 않는 경우에도 서비스는 이용하실 수 있습니다.

- ①個人情報をマーケティングで利用する場合の別途同意
 - ✓ 電子メール、携帯番号、クッキーなどをマーケティングに活用する場合には**別途、同意手続きを用意する必要有り**
 - ✓ **利用者がマーケティング利用に同意しない場合でも、サービス提供は必須**
 - ✓ **違反時は3千万ウォン(約300万円)以下の罰金**
- ②個人情報を第三者提供する場合の別途同意
 - ✓ 内容は①と同様。ただし、違反時の罰金が**1千万ウォン(約100万円)以下**

4.3.諸外国における取組状況に関する調査・分析 香港






【2014年12月】 香港のプライバシーコミッショナーが「The Best Practice Guide for Mobile App Development」を発表

- 《背景》 GPENの調査で香港におけるアプリのプラポリの掲載率が15%であったことを受けて、改善策として開発者向けガイダンス「The Best Practice Guide for Mobile App Development」を発表した。ガイダンス発表時に、今後、状況を改善しなかった場合、強制力の伴う施策を行なう準備があるとプライバシーコミッショナーが示唆した。
- 《内容》 同ガイダンスは中小企業を主な対象としており、以下の5つの項目について具体的かつ実践的な解説がなされている。

項目		概要
1.個人データ保護条例		● アプリが個人データを取得する場合には、アプリ開発者は個人情報保護条例を遵守すべきことを説明
2.データ保護の6原則		● 個人データ(プライバシー)条例における6原則を解説
3.プライバシー・バイ・デザイン		● アプリ開発のプロセス全般にわたって、プライバシーを考慮することを推奨
4.アプリ開発チェックリスト		● プライバシー・バイ・デザインの考え方をアプリ開発に適用するためのチェックリストを提供している
5. ベストプラクティスの紹介と推奨	個人データを収集するアプリ	<ul style="list-style-type: none"> ● 不必要なデータの収集や利用等しないための、ベストプラクティスを提示 ● ベストプラクティスのひとつとして、<u>プラポリのリンクをアプリの紹介ページに掲載することが挙げられている。</u>
	個人データを収集しないアプリ	<ul style="list-style-type: none"> ● データを収集しないアプリ向けにも、ベストプラクティスを提示 ● <u>データを収集しない場合でもプラポリのリンクをアプリの紹介ページに掲載することが強く推奨されている。</u>

4.4.ウェアラブルデバイス等新技術に関する調査・分析 サービス動向

ヘルスケア・医療用途のウェアラブルデバイスはスマートフォンでは取得が難しく、プライバシー性が高い情報を取得できる。大部分のデバイスがスマートフォンアプリと連携し、デバイスが収集した情報のサーバへの送信や分析結果の表示を実施。SDK(※)を外部の開発者に公開することで、新たなエコシステムを目指すウェアラブルデバイスもある。

製品名／企業名	用途	製品・サービス概要	測定データ	SDKの公開
Fitbit／Fitbit 	ヘルスケア	<ul style="list-style-type: none"> ● 移動距離、消費カロリー、睡眠時間など利用者の活動量や睡眠の状況をモニタリングするリストバンド型の端末。 	歩数、距離、消費カロリー 睡眠 目標達成度	公開
JINS MEME(ジンズ・ミーム)／JINS 	ヘルスケア	<ul style="list-style-type: none"> ● JINS MEME(ジンズ・ミーム)は独自技術の眼電位センサーと六軸センサーを用いて、眠気や集中度、体のバランスなどユニークな生体データを取得。 	眼電位 視線 まばたき・まばたきのスピード 加速度 眼鏡の角度や角速度	公開
Silmee Bar type／東芝 	ヘルスケア	<ul style="list-style-type: none"> ● 胸部に貼り付け、心電位や脈波、体道、皮膚温度を測定でき、自律神経の状態や体動、睡眠の質などを分析できる生体センサーを提供している。 	体表の動き 心電位 脈波 体動 皮膚温	公開
Embrace／Empatica 	医療	<ul style="list-style-type: none"> ● 活動量やストレスレベルの測定・モニタリングが可能な他、アプリ「Empatica Alert」を導入することで、てんかん発作を監視し、発作が起きた場合は自動的に介護者に通知することが可能なスマートウォッチ。 	活動データ 皮膚活動電位 体温 縦横回転 3軸加速度	非公開
BioStamp／MC10 	医療	<ul style="list-style-type: none"> ● 非常に薄く、直接肌に貼るタイプのウェアラブルデバイス。 ● 心電図・脳波・筋電図・体温を各種センサーにより測定し、不整脈など心臓慢性疾患やストレス状況を把握することが可能。 	電位 心電図 脳波 筋電図 温度 体温	非公開

※ Software Development Kit(SDK)とは、あるソフトウェアを開発するために必要なプログラムや文書をひとまとめにしたパッケージのこと。

ウェアラブルデバイスとスマートフォン上のアプリが連携することで、プライバシーリスクが高まる可能性として指摘されている。

スマートフォン上のアプリとウェアラブルデバイスの連携によるリスク

- 米国セキュリティソフトウェア会社のSymantec社は、ウェアラブルデバイスとスマートフォン上のアプリが連携した自己定量化サービスのセキュリティやプライバシーのリスク分析を行った。

項目	調査結果
ウェアラブルデバイスの位置の追跡	<ul style="list-style-type: none"> ● 市販の材料を使用し、ポータブル Bluetooth スキャンデバイスを作成。 ● 混雑した公共の場所等を何カ所か歩き回り、取得可能なデータを調査。 ● テストで検出されたデバイスは全て、そこから送信される一意のハードウェアアドレスを使って簡単に追跡可能であった。
個人データ等の平文での送信	<ul style="list-style-type: none"> ● 調査したアプリの内20%が平文でパスワードを送信していた。

(出所)Symantec(2014)“How safe is your quantified self?”

クロスデバイストラッキングのプライバシーリスク

- 2015年11月にFTCは、複数の端末の行動履歴等を収集する「クロスデバイストラッキング」についてワークショップを開催し、プライバシーリスクについて議論を行った。

項目		概要
定義		● 複数の端末で同一の利用者の行動履歴等の情報を収集する方法
類型	確定的トラッキング	● アプリ提供者などが異なる端末で同一のアカウントIDでログインしてもらうことで、同一の利用者の行動履歴を蓄積・解析する方法。
	推測的トラッキング	<ul style="list-style-type: none"> ● Web上から収集可能なOSバージョン、地域、画面サイズなどの情報をもとに推定的に名寄せする技術である「フィンガープリント」などを用いて、オンラインの行動履歴を収集・解析する方法。 ● 利用者には、同技術が使用されていることがわかりにくく、コントロールが難しいため、プライバシーのリスクが高いことが懸念されている。
論点		● 技術動向、クロスデバイストラッキングがもたらす利便性、プライバシー・セキュリティリスク、透明性・コントロールの確保等

SDKの利用規約では、開発したアプリについてプライバシーの掲載をアプリ提供者に対して求めている。また、アプリが利用者情報・個人情報を収集又は送信する際には、利用者から同意を取得することも求めている。

項目		JINS MEME	Fitbit
用途		ヘルスケア	ヘルスケア
アプリ提供者の義務に関する記載	透明性の確保	<ul style="list-style-type: none"> 開発者は、開発アプリによって取得される個人情報、JINS MEMEによって検知された生体データその他の情報を、関係法令およびガイドライン等を遵守して(開発アプリに適用されるプライバシーポリシーの施行および開示を含みます。)秘密に保持するとともに適正に管理するものとします。 	<ul style="list-style-type: none"> アプリに関するプライバシーポリシーをユーザーに提示しなければならない。 プライバシーポリシーには、ユーザーのデータの使用目的及び収集する可能性のあるすべての情報を明記しなければならない。 ユーザーがいつでもプライバシーポリシーを確認できるようにインストール時及びアプリ内で提示しなければならない。
	利用者関与の機会	<ul style="list-style-type: none"> 開発者は、個人情報(JINS MEMEによって検知された生体データを含む。)の取得に明示的に同意していない者から個人情報を取得するアプリを製作、販売ないし配布してはなりません。 	<ul style="list-style-type: none"> ユーザーの明示的な同意なしに、外部の媒体にユーザーのデータを表示又は分配してはならない。 ユーザーの明示的な意思又は確認なく、ユーザーのデータを上書き又は削除してはならない。
	適正な取得	記載なし	記載なし
	安全管理措置	※透明性の確保と同じ	記載なし
	苦情・相談等の処理	<ul style="list-style-type: none"> 開発アプリに関連して、または本利用規約に開発者が違反したことにより第三者からクレームが生じた場合には、開発者は、開発者の責任と費用においてこれを解決します。 	記載なし
その他		<ul style="list-style-type: none"> 開発者は、開発アプリが、開発者が独自に開発したものであり、開発アプリの利用が第三者の権利・利益を侵害せず、第三者との契約違反を構成しないものであることを保証します。 	<ul style="list-style-type: none"> Fitbitのシステムからデータを引き出す又は送信する際に、ユーザーに不正確な情報を伝えてはならない。

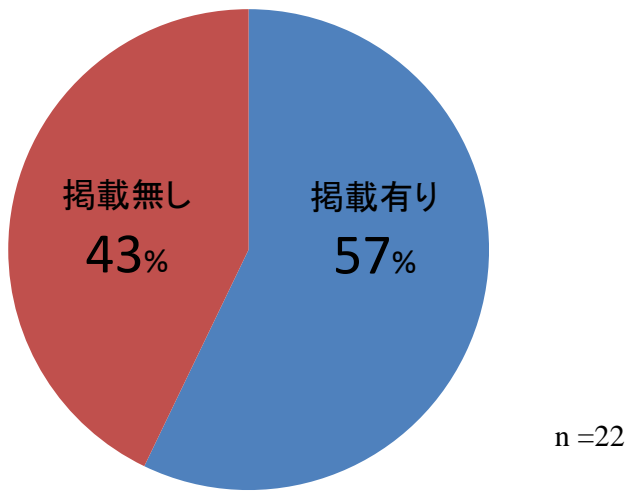
4.4.ウェアラブルデバイス等新技术に関する調査・分析 プラポリの掲載状況

Fitbitと連携するスマートフォン上のアプリの内、プラポリへのリンクをGoogle Playに掲載していたアプリは約60%であった。
アプリ専用のプラポリが掲載されていたのは、約10%であった。

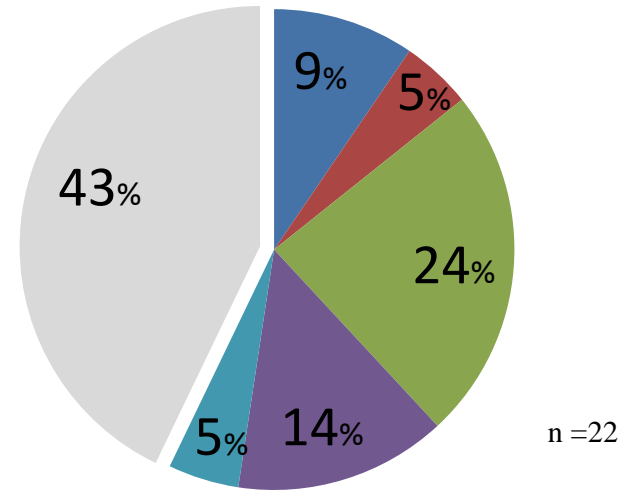
【調査方法】

- 外部デベロッパー向けにSDKを公開しているウェアラブルデバイスの内、外部デベロッパーがアプリを公表しているFitBitを対象とした。
- FitBit と連携するアプリの内、Google Play でアプリを公開しているものを対象としている。
- アプリ紹介ページにおけるプライバシーポリシーへのリンクの有無を調査。

プラポリの掲載率



プラポリの内容の分類



※ 対象となったアプリの内「健康 & フィットネス」が19個であった。

- 【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

5.1. WGの検討内容について

普及・啓発WG、制度・運用WG及び技術WGを開催し、将来的な普及啓発方法、第三者検証の運用体制、プロトタイプシステムの仕様などについて検討した。

普及・啓発WG

【検討事項】

- ◆ 関係事業者へのプライバシーポリシーに係る普及・啓発方法・内容

【構成員】※敬称略、50音順

- ◆ 川口洋司(一般社団法人日本オンラインゲーム協会(JOGA))
- ◆ 岸原孝昌(一般社団法人モバイル・コンテンツ・フォーラム)
- ◆ 後藤悦夫(一般社団法人日本スマートフォンセキュリティ協会)
- ◆ 近藤則子(老テク研究会)
- ◆ 佐藤進(アンドロイダー株式会社)
- ◆ 二宮幸司(株式会社ファンコミュニケーションズ)
- ◆ 平岩高弘(エクレ)
- ◆ 矢橋康雄(一般社団法人電気通信事業者協会)
- ◆ 吉村浩一郎(安心ネットづくり促進協議会)
- ◆ 渡部俊英(株式会社VOYAGE GROUP)

制度・運用WG

【検討事項】

- ◆ 将来的な第三者検証の運用体制の整理
- ◆ 第三者検証を実施する上での課題抽出・整理
 - ✓ 非申請型の検証の制度上の取扱い
 - ✓ 検証結果の表示方法

【構成員】※敬称略、50音順

- ◆ 上沼紫野(虎ノ門南法律事務所)
- ◆ 岸原孝昌(一般社団法人モバイル・コンテンツ・フォーラム)
- ◆ 佐藤進(アンドロイダー株式会社)
- ◆ 高木浩光(国立研究開発法人産業技術総合研究所)
- ◆ 森亮二(英知法律事務所)
- ◆ 谷田部茂(一般社団法人日本スマートフォンセキュリティ協会)
- ◆ 山田卓(ユアサハラ法律特許事務所)

技術WG

【検討事項】

- ◆ 第三者検証のプロトタイプシステムの仕様
- ◆ 技術的限界、将来的な運用体制を踏まえた上での現実的な検証の水準等

【構成員】※敬称略、50音順

- ◆ 岸原孝昌(一般社団法人モバイル・コンテンツ・フォーラム)
- ◆ 佐藤進(アンドロイダー株式会社)
- ◆ 杉浦隆幸(ネットエージェント株式会社)
- ◆ 竹森敬祐(株式会社KDDI研究所)
- ◆ 名雲孝昭(NTTコミュニケーションズ株式会社)
- ◆ 松並勝(ソニーデジタルネットワークアプリケーションズ株式会社)
- ◆ 谷田部茂(一般社団法人日本スマートフォンセキュリティ協会)

5.2.消費者に対する普及啓発内容・方法

具体的な普及啓発方法として、高齢者やPTAに対する既存の講習会を通じた普及啓発、各省庁との連携（サイバーセキュリティ月間での連携）、国民生活センターや消費生活推進員を通じた普及啓発などが挙げられた。

「プラポリの確認を促すために普及啓発すべき内容」としては、「プラポリの確認」が「プライバシーを守る事」につながるということ強く意識できる内容が望ましい、アプリをインストールする際に確認すべき具体的なステップを示すと良いという意見が出た。

項目	内容
具体的な普及啓発方法	<ul style="list-style-type: none"> ● 各業界団体やNPOなどが民間事業者や自治体と連携し、高齢者や学校・PTAに対する既存の講習会（「スマホサロン」など）を通して、S/P/Aやアプリの利用時の留意点などを普及啓発する方法は有効ではないか。 ● 国民生活センターや消費生活推進員、各省庁との連携による普及啓発も有効な手段の1つ。 <ul style="list-style-type: none"> ➢ スマートフォンの使い方に関する書籍や雑誌や記事を出している出版社や著者に対して働きかけを行い、スマートフォンアプリの利用者情報の取扱いについて取り上げてもらう方法も存在。
プラポリの確認を促すために普及啓発すべき内容	<ul style="list-style-type: none"> ● 「プラポリの確認」が「自身のプライバシーを守ること」につながるということが消費者に浸透していないため、まずはその点を普及啓発すると良いのではないか。 <ul style="list-style-type: none"> ➢ 「プラポリの確認」をすれば、自身のプライバシーを守れるわけではないため、「プラポリの確認」はプライバシーを守るための第1歩という点に留意する必要がある。 ● 消費者にとって、「プラポリの確認」だけを推奨されても納得感が少ないため、アプリを新規でインストールする際のステップに沿ってアドバイスをしながら、その中で「プラポリの確認」を推奨してはどうか。
「スマートフォンプライバシーガイド」改定に対するご意見	<ul style="list-style-type: none"> ● 消費者が「自分事」として捉えられるような事例を掲載するといいいのではないか。 <ul style="list-style-type: none"> ➢ セキュリティの普及啓発でも、不正アクセスの際の具体的な損失額を示した方がよいという話になる。 ● 事例により危険性を認識させることが重要。例えば、「電話帳情報が取られると詐欺に悪用され、周りに迷惑がかかる」という事例は周囲にも迷惑がかかり、金的な被害も出るということが伝わり、受け止め方が自分事になる。

5.2.アプリ提供者（主に中小企業・個人）に対する普及啓発内容・方法

中小企業・個人向けに、「SPIの要点をまとめた資料(スマートフォンプライバシーガイドのアプリ提供者版)やアプリ開発・提供の際のチェックシートなどが有れば、リテラシーの向上につながる」という意見や「プライバシーとセキュリティを合わせて普及啓発していく方法が有効」という意見が出た。

大項目	内容
具体的な普及啓発方法	<ul style="list-style-type: none"> ◆中小企業や個人のアプリ提供者の中には、SPIやプラポリ掲載の必要性、書くべき事項を理解していないアプリ提供者が存在しているため、アプリ提供者向けにSPIやプラポリの作成方法を分かりやすくまとめたガイドやチェックシートが有ると良い。 <ul style="list-style-type: none"> ▶ モジュール提供者に対して、アプリ提供者からプラポリに関して質問が来る場合もあり、その際に活用できる。 ◆プライバシーとセキュリティを合わせて普及啓発していく方法が有効ではないか。
事務局資料(ガイドやチェックシート)への意見	<ul style="list-style-type: none"> ◆情報収集モジュールには様々な用途のモジュールが存在しているため、ガイドやチェックシートの記述を広告モジュールに限定しない方が良い。 ◆モジュール提供者を選ぶ基準をもう少し明確化した方が良い。例えば、位置情報を取得しているモジュールは要注意など。

SPI等に関するガイドのイメージ

ポイント①スマートフォンの特徴や情報収集モジュールの特徴を理解しよう!!

ポイント②様々な情報を取得することによるリスクを考えよう!!

ポイント③必要最小限の利用者情報のみ取得し、プライバシーポリシーを作成しよう

アプリ開発・公開の際のチェックシートのイメージ

【アプリが利用者情報を外部に送信しない場合】

アプリが利用者情報を送信しない旨を紹介ページの説明文や紹介ページからリンクしているプラポリに記載しているか？

⇒詳細はSPIのページxxxを参照

【アプリが利用者情報を外部に送信する場合】

≪項目①アプリの利用者情報の取得状況≫

アプリが必要最低限の利用者情報のみを取得しているか？

⇒詳細はSPIのページxxxを参照

アプリに利用者情報を取得する外部モジュールが組み込まれているか？

※利用している場合は項目②を確認

⇒詳細はSPIのページxxxを参照

5.2. モジュール提供者に対する普及啓発内容

「透明性確保における広告モジュール提供者とアプリ提供者の役割分担」を制度・運用WGで制度的・法的関連からの整理を行い、普及・啓発WGで両者の関係性・実情を確認し、両者の役割を下記の通り明確化した。

【検討の背景】

- ◆ モジュール提供者への普及啓発内容は、アプリ提供者とモジュール提供者の役割分担によって変わる可能性が高いため、平成27年度は両者間の役割分担について議論を行った。※ただし、モジュールの種類により両者の関係性が異なるため、広告モジュールに限定して議論を実施。

【検討内容】

広告モジュール提供者とアプリ提供者の関与度合い

項目	アプリ提供者	モジュール提供者
モジュールの取得情報に対する関与	モジュールが送信した情報を把握、関与することはできない パーミッション等の設定に取得情報はコントロール可能	モジュールの挙動、取得した情報の利用に一義的に関与している
モジュールのプラポリの提示に対する関与	モジュールプラポリが存在すれば、利用者に提示可能	アプリ提供者に提示を義務付けることは難しい 「iマーク」のように広告枠内にリンクを用意することは可能

透明性の確保における広告モジュール提供者とアプリ提供者の役割分担

	モジュールプラポリの作成	モジュールプラポリの提示	利用者からのモジュールに関する問合せ
広告配信モジュール提供者	<ul style="list-style-type: none"> ● モジュールプラポリを作成する必要がある。 	<ul style="list-style-type: none"> ● モジュールプラポリのリンクを通知する必要がある。 ● アプリ提供者にモジュールプラポリのリンクの提示を促す必要がある。 	<ul style="list-style-type: none"> ● 取得した情報に関する問合せや送信の停止、取得した情報の削除等の要請にこたえる必要がある。
アプリ提供者	なし	<ul style="list-style-type: none"> ● モジュールプラポリの掲載を行う必要がある。 	<ul style="list-style-type: none"> ● モジュールプラポリに記載されている問合せ先に誘導する必要がある。

《参考》アプリ提供者とモジュール提供者の役割分担に関する議論内容詳細

項目	小項目	内容
制度・運用WG	アプリ提供者とモジュール提供者の関係	<p>モジュールによる情報の取得の主体は、モジュール提供者であると考えるのが妥当ではないか。</p> <p>(意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ アプリ提供者は、モジュールをアプリに組み込んでいるだけで、モジュールが取得した情報の取り扱い方に関与することはできない。実質的な情報の取得者は、モジュール提供者である。 ◆ モジュールによって取得される情報が個人情報に該当する場合は、モジュール提供者がアプリ提供者に対して個人情報の取得を委託しているとみなせ、モジュール提供者が個人情報保護法22条における委託監督義務を負うと整理できるのではないか。 <ul style="list-style-type: none"> ▶ このような関係は、保険や携帯の代理店の事例にも見られる。
	利用者視点からの関係性の整理	<p>利用者から見て分かりやすい関係性の整理となっているか検討する必要がある。</p> <p>(意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ 利用者はアプリを活用・楽しむことが主目的であり、モジュール提供者が情報の取得の主体という形で整理すると、利用者には責任の所在や関係性がわかりづらくなる。
普及・啓発WG	アプリ提供者とモジュール提供者の関係	<p>モジュール提供者は交渉力が弱いため、アプリ提供者を監督できる立場にない。</p> <p>(意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ モジュール提供者はアプリ提供者にモジュールの組み込みをお願いする立場にある。(モジュール提供者を委託元として関係を整理することについて)力関係としては、逆という印象を持っている。 ◆ モジュール提供者からアプリ提供者にプラポリのリンクの掲載を求めることは、非現実的なケースが少なくない。
	役割分担(責任)に関する意見	<p>モジュール提供者は、モジュールプラポリを正確に作成する義務がある一方で、アプリ提供者は、モジュールプラポリを掲載する義務がある。</p> <p>(意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ モジュールの全責任をアプリ事業者が負うのは無理。委託元と委託先で完全に責任を分けるのは現実的ではない。 ◆ アプリ提供者はモジュールプラポリを掲載する義務があり、モジュール提供者はモジュールプラポリの内容を正確に記載する必要がある。ただし、アプリ提供者はモジュール提供者が嘘をついていることを知りながら掲載した場合は、責任を問われる。以上のことを基本原則として、ケースバイケースで対応していくことが望ましいのではないか。

5.2.次年度（平成28年度）以降の普及啓発の進め方（案）

項目		検討内容
全般		<ul style="list-style-type: none"> ◆スマートフォンの利用者情報等に関する連絡協議会（SPSC）等をベースとして、政府や業界団体や事業者の各種資料（ガイド、普及啓発ツール、調査結果等）を共有し、展開する場の構築を目指す。 ◆SPIに関連する幅広い情報を集約したポータルサイトの設置を検討する。 <ul style="list-style-type: none"> ➢ 同サイトを通じたスマートフォンに関する書籍や雑誌や記事を出している出版社や著者に対して働きかけを行うことも検討する。
一般消費者	全般	<ul style="list-style-type: none"> ◆「プラポリの確認」が「プライバシーを守る事」につながるということの浸透を目指す。 <ul style="list-style-type: none"> ➢ 上記浸透のために、アプリ利用によるプライバシーリスクの具体例、「プラポリの確認」も含めた「プライバシーを守るため」のソリューションや具体的な行動などを普及啓発していく。
	高齢者	<ul style="list-style-type: none"> ◆各地のNPOや業界団体、携帯端末メーカーが連携し、実施している「スマホサロン」の場を借りて、基礎的な内容を対面で普及啓発することを検討する。 <ul style="list-style-type: none"> ➢ 平成27年度も「スマホサロン」の場を借りて、2016年3月にシニアに対して対面ヒアリングを実施。
	青少年	<ul style="list-style-type: none"> ◆安心ネットづくり促進協議会と連携し、各PTA等や青少年向けの講習会や各種イベントで、アプリ利用時の留意点（プラポリの読み方等）を普及啓発することを検討する。
アプリ提供者	大企業	<ul style="list-style-type: none"> ◆利用者情報の取扱いトラブルによる企業のブランド毀損の可能性、トラブルを避けるために最低限実施すべき事項を各企業の法務部門やシステム部門に対して普及啓発を行うことを検討する。
	中小企業・個人	<ul style="list-style-type: none"> ◆セキュリティとプライバシーを合わせて普及啓発するための体制を検討する。 ◆SPIなどの要点をまとめた、アプリ提供者向けのスマートフォンプライバシーガイドの作成を目指す。アプリの開発・提供時に留意すべき事項をまとめた、チェックシートの作成を目指す。
モジュール提供者		<ul style="list-style-type: none"> ◆モジュール個別のプラポリの作成・公表の必要性を浸透させていくことを目指す。
総務省		<ul style="list-style-type: none"> ◆「スマートフォンプライバシーガイド（改定版）」を用いた普及啓発、他の省庁や業界団体・関係事業者との普及啓発面での連携、SPIの改定等を実施することを目指す。

5.3.将来的な運用方法：具体的な運用方法の検討

普及啓発のためには非申請型の検証の実施が重要との意見があるものの、採算性に課題が存在している。採算が成立するための方策として、申請型の実施、既存のアプリ検証実施団体・事業者との連携、IoTへの取組みの拡張などが挙げられた。

運用方法	モデルの概要	検討結果
申請型のアプリの検証結果の公開サービス	◆ 検証結果は消費者向けに公表し、アプリの知名度・信頼性向上やDL数増加につなげる	現状では申請型のアプリ検証を有料で提供することは難しい可能性が高い。 ◆ 申請型の検証を受けることがアプリDL数にプラスの影響がないと、有料では申請してくれない可能性がある。
非申請型でのアプリ検証結果の公開サービス	◆ 大量のアプリを検証し、セキュリティアプリのように消費者がインストールしたアプリをチェックし、警告を発するサービスを想定	コスト対効果の面で実施の必要性が低く、技術面・制度面でも課題が多い。 ◆ アプリの検証コストに対する効果を踏まえると、全数調査の必要性は無い。
非申請型での定期調査	◆ マーケットの一部のアプリ(人気アプリや新着アプリ、カテゴリ別の人気アプリ等)を定期的に非申請型で検証し、検証結果を消費者向けに公表する	アプリ提供者への普及・啓発、業界の底上げという意味では重要性が高いが、実施主体や採算性に課題有り。 ◆ アプリ開発者への普及・啓発、アプリ業界に対するプレッシャー、業界の底上げという点では影響は大きく、重要性は高い。 ◆ 他の運用方法と合わせて実施することで実施コストを賄えないか。
アプリ開発者向けのアプリチェックサービス	◆ アプリ提供者から申請されたアプリを検証し、アプリが外部送信している情報やプラポリとの食い違いをアプリ提供者に提供し、改善方法等をフィードバックする	現状では申請型のアプリ検証を有料で提供することは難しい可能性が高い。 ◆ アプリ開発者に対して、アプリの外注を行っているナショナルクライアントが、アプリの第三者検証を受けることを求めれば、多くのアプリ開発者がアプリの第三者検証を申し込む可能性が存在する。

【運用方法に対するその他の意見】

項目	検討結果
その他の運営モデルの可能性	非申請型で、検証結果の公開先が開発者向けのモデルも他業界や海外では存在する。 ◆ 広告業界のような業界団体が事業者の広告をチェックし、事業者に警告するというモデルも存在する。 ◆ 米国では広告モジュールをチェックし、モジュールの挙動に関して疑わしいと判定した場合に、警告文を出す事例も存在。
守備範囲の拡張可能性	本実証実験の取組をIoTまで拡張することで、市場を拡大し、収益モデルを確立できるのではないか。 ◆ IoTまで対象範囲を広げるなどアップデート調査の中にも上手いモデルを作るためのやり方があるのではないか。 ◆ IoTであればスマートTV、自動車などを絡めることができ、メーカーや民放、自動車会社を巻き込める。
既にアプリの検証を実施している団体・事業者との連携	アプリの仕様・動作確認、アプリの有害情報の確認を行っている事業者や団体と連携すれば、解析に要するコスト等を抑えられるのではないか。 ◆ アプリの仕様・動作確認、アプリの有害情報の確認と作業内容が類似しており、共通化が可能ではないか。

5.3.将来的な運用体制・運用方法：申請型のアプリ検証のニーズ

IT企業以外の大手企業では、検証のニーズが存在する可能性がある。アプリの利用者情報の取扱いの検証に関する公的な基準やニーズが求められている。

【大手企業に対するヒアリング結果】

項目	検証結果
スマートフォン上のアプリの開発体制・開発時の留意事項	<p>IT企業以外では、外部にアプリの開発を依頼することが多く、個人情報や極力取得しないよう注意している。</p> <ul style="list-style-type: none"> ◆ (IT企業以外では) 基本的に、外部にアプリの開発を依頼している。納品時には、セキュリティや個人情報の取扱いに関するチェックは行っている。開発時には、極力個人情報を取得しないよう、開発者に依頼している。
アプリの利用者情報の取扱いの検証に関するニーズ	<p>アプリの利用者情報の取扱いに関する検証のニーズは、存在する可能性がある。</p> <ul style="list-style-type: none"> ◆ (開発を依頼される企業からの意見として) 電鉄系などIT系以外の企業の場合、個人情報や利用者情報の取扱いに関して余計に心配される事があり、説明を求められることがある。 ◆ 第三者検証を受けた上で、納品してもらう形にできるとよい。 ◆ 常駐のエンジニアがプログラムを作成する場合もあるが、彼らがどの程度のレベルなのか客観的に分からない。
政府や実証実験に対する要望	<p>アプリの利用者情報の取扱いの検証に関する公的な基準を策定してほしい。</p> <ul style="list-style-type: none"> ◆ 政府お墨付きの検証基準やマークなどがあるとよい。 ◆ 政府で利用者情報の取扱い状況に関するチェックリストを出してもらえるとよい。

【検証会社に対するヒアリング結果】

項目	検証結果
アプリの利用者情報の取扱いの検証に関するニーズ	<p>アプリの利用者情報の取扱いに関する検証(取得情報、プラポリの内容の検証)のニーズはほぼ無い。</p> <ul style="list-style-type: none"> ◆ 検証会社はアプリ提供者から指定された、アプリUI、利用規約の文面、アプリの動作の検証など幅広い項目を検証しているが、これまでSPIやアプリの利用者情報の取扱いに関する検証を依頼されたことは無い。
利用者情報の取扱いに関する検証の実施可能性	<p>動的解析も含め、アプリの利用者情報の取扱いに関する検証を行うことはそれほど難しく無い。</p> <ul style="list-style-type: none"> ◆ 現在のアプリ検証の中で、アプリを実際に動かしたり、その際のパケットを解析したり、利用規約やアプリの説明に不備が無いかわかりしきっているため、動的解析やプラポリ解析を行うことは、それほど追加コスト無く実施できる。
政府や実証実験に対する要望	<p>アプリ提供者のニーズ喚起のための施策、利用者情報の取扱いの検証に関する基準やツールの公開が望ましい。</p> <ul style="list-style-type: none"> ◆ 大半のアプリ提供者は問題が起こったり、規制ができたりしないと動かないスタンスであり、規制などによるニーズ喚起が必要。また、政府お墨付きの検証基準や検証方法・水準、ツールなどが決まっていると、検証を行いやすい。

5.3.アプリ検証で解決すべき課題：プラポリ掲載・作成ルールの明確化

利用者情報を蓄積・外部に送信しないアプリについては、利用者情報を蓄積・外部に送信しない場合でも利用者情報の取扱い状況について利用者に明記することが望ましいという意見があった。

プラポリの掲載場所については、原則として「アプリのインストールや利用前に、利用者がプラポリを容易に閲覧できる場所に掲載する必要がある」という意見があった。

論点	検討結果
<p>利用者情報を蓄積・外部に送信しないアプリのプラポリ掲載の必要性</p>	<p>アプリが利用者情報を蓄積・外部送信しない場合でも、利用者の分かり易い場所に蓄積・送信しない旨を通知する形が望ましい。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆利用者視点では、利用者情報を蓄積・外部送信しない場合でも、プラポリを作成し、情報を蓄積・送信しない旨を通知する形が望ましい ◆一方で、アプリ提供者の立場に立つと、1行程度の通知のためにプラポリを作成し、掲載場所を確保することに対する納得感は低い
<p>プラポリの掲載場所 (アプリ紹介ページにプラポリが掲載されていない場合の評価)</p>	<p>アプリのインストールや利用前に、利用者がプラポリを容易に閲覧できる場所に掲載する必要があるのではないか。 (アプリ内、開発者ページはこの条件に該当しない) (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆プラポリはアプリのインストール・利用前に利用者に提示するという原則に立てば、アプリ内やアプリ提供者ウェブページ内のみでのプラポリ提示は、「プラポリ掲載」とみなされない ◆アプリ起動時での提示は「プラポリ掲載」と認めるものの、アプリ起動と同時に情報を取得・送信するようなアプリも過去にはあったため、可能であれば、インストール前の提示が望ましい
<p>アプリ更新時のプラポリの提示方法</p>	<p>重要な変更があった場合には、アプリ更新後に利用者に変更した旨やプラポリを通知することが望ましい。</p>

5.3.アプリ検証を行う上で解決すべき課題：検証結果の公開方法

非申請型の定点調査でアプリ名を公表する場合には、全アプリの結果を公表するのではなく、アプリの動作とプラポリに乖離が大きい一部のアプリを公表する形が現実的という意見があった。

また、公表プロセスとして、公表前に調査を行ったアプリを提供する事業者を検証結果を伝えて、改善する機会を提供することが望ましいという意見があった。

公表方法		検討結果
アプリ名を 公開しない 方法	統計化 データ	統計データや匿名化データを掲載することに問題はないのではないか。 (意見・コメントなど) ◆ アプリ名が特定されないのであれば、プラポリ調査と同様に問題ないのではないか。 ✓ 制度的な問題は無いが、事業者や社会への影響は少ないのではないか。
	匿名化 データ	
アプリ名を 公開する 方法	検証結果の 表示方法	取得・送信する利用者情報とプラポリの記載内容に著しい乖離が存在するなど社会的に許容されない基準などを考えて、検証結果に応じて実名での公表を行うかを判断する方法が現実的ではないか。 (意見・コメントなど) ◆ 単純な事務的なミスによる乖離なども全て実名で公表することは現実的ではない。社会的に許容されないレベルとする基準などを考えて、検証結果ごとに公表するかどうかを判断をしていかざるを得ないのではないかと思う。 ◆ 「外部に送信していないという検証結果が出たが、実際は外部に送信している場合」が発生するならば、アプリが安全だとは言わない形がよいのではないか。
	検証結果の 表示プロセス	アプリ名を公表する場合には、公表前に当該事業者を検証結果を事前に伝えて、改善する機会を与えることが望ましい。 (意見・コメントなど) ◆ 事前に伝えるならば、ケアレスミスでの乖離している場合を救済できる。 ◆ そのような形であれば、検証結果の精度も上がり、アプリ提供者から名誉棄損等で訴えられる可能性は減少する

5.3.次年度（平成28年度）以降のSPI改定の際の論点

次年度（平成28年度）以降のSPI改定を行うことになった場合の論点として、運用WGの検討結果を踏まえると、次の5つが考えられる。

- ①アプリプラポリ作成・掲載ルールの詳細化
- ②アプリ提供者と情報収集モジュール提供者の役割分担
- ③モジュール提供者のプラポリ作成・掲載のルール
- ④アプリマーケット運営者が実施すべき取組
- ⑤一般消費者・アプリ提供者への普及啓発方法

項目	論点
アプリプラポリ作成・掲載ルールの詳細化	<ul style="list-style-type: none"> ◆ 利用者情報を蓄積・外部送信しないアプリのプラポリ作成・掲載について ◆ アプリプラポリの掲載場所の具体化 ◆ アプリ更新時のプラポリの提示方法 ◆ モジュールを利用する際の留意事項
アプリ提供者とモジュール提供者の役割分担	<ul style="list-style-type: none"> ◆ モジュールの透明性の確保に関する役割分担（プラポリ・規約の作成・掲載など） ◆ 透明性確保のためにモジュール提供者、アプリ開発者がそれぞれ取り組むべき事項
モジュール提供者のプラポリ作成・掲載のルール	<ul style="list-style-type: none"> ◆ モジュールのプラポリに記載すべき事項 ◆ モジュールのプラポリの掲載に関する原則
アプリマーケット運営者が実施すべき取組	<ul style="list-style-type: none"> ◆ アプリマーケット事業者が透明性の確保のために実施すべき事項
一般消費者・アプリ提供者への普及啓発	<ul style="list-style-type: none"> ◆ 一般消費者への普及・啓発（アプリに利用者情報を取得されることのデメリットの明確化、高齢者・青少年に対する業界団体等の既存の取組み、既存メディアとの連携方法など） ◆ アプリ提供者への普及・啓発（プラポリの作成・掲載ルールに関するパンフレット・チェックシートの作成など）

5.4.第三者検証のシステム要件・実施対象・実施範囲についての要件・課題(1)

第1回～第2回の中で実証実験にて構築するシステムプロトタイプの様について検討した。

また、第3回では最終的な仕様の確認と将来的課題について議論した。

その中で、将来的に第三者検証する際に求められるシステム機能や検証機関が実施する対象や範囲について挙げられた要件や課題について以下に示す。

項目	内容
アプリ収集	<p>全てのアプリを対象とはできないが、抽出には様々な観点が必要ではないか。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ 開発者の業種という切り口で比較すれば、様々な業界に対する底上げにつながる。 ◆ IoTに繋げるため、Android OS搭載TV用アプリなどを対象としてはよいのではないか。 <p>アプリ更新に追従して解析するのは、運用面も含め検討が必要ではないか。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ 何か利用者から問い合わせがあった時に、必ずこのアプリが安全かどうかすぐに答えられるようにしようとした場合には、常に最新のものを追い続けなければならない。 ◆ アップロードもデータも過去のものから今のものまで保持し続けなければならない。解析したアプリの更新履歴の情報など大量のデータを蓄積する必要がある。
プラポリ収集	<p>プラポリの掲載箇所はアプリによって違い、システムで収集する範囲を整理する必要があるのではないか。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ アプリマーケットに記載しているもの、アプリ内にプラポリが記載しているものなどがあり掲載箇所は一定していない。 ◆ モジュールを使用している場合、リンクで示している場合がある。どこまでプラポリを収集するのかを整理する必要がある。
プラポリ解析	<p>完全自動化できない非定型プラポリについても、手動解析を支援する必要なのではないか。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ プラポリは自由テキストなので完全自動化は難しい ◆ 人による差がでないように、ツールである程度解析を行った後に手動で見直す方法がよい。 ◆ 該当箇所をキーワードマッチングするのが有効。市中技術を利用することを検討するのもよい。

5.4.第三者検証のシステム要件・実施範囲・実施対象についての要件・課題(2)

項目	内容
アプリ解析	<p>解析精度は重要であるが、精度をどう計測するかは課題である。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ 全送信中いくつかの送信を見つけられるかで解析精度を評価する必要があるが、全送信数を計測できない。 ◆ Androidアプリの動的解析到達率はアクティビティ数で評価ができるが、実態を反映していないことがある。 ◆ 動的解析の精度向上には、端末操作時間を増やすなどの対策が考えられるが、コストとのバランスを精査する必要がある。 <p>OSにより解析手段が制限される。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ iOSアプリの静的解析はリバースエンジニアリングなど法的な問題が残る。ソースコードに対してはできるが、実際問題として解析のためにソースを提供してくれるアプリベンダーはいないのではないか。 ◆ Androidのテイント解析はツールの更新がAndroid4.3で止まっている。それより後のバージョンのみしか対応していないアプリは解析できない。
解析結果の突合・結果表示	<p>突合基準は事前整理が必要ではないか。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ プラポリの記載が、動的解析結果とは一致するが、静的解析結果では不足があるなどの場合、どう判断するかは運営側のリスクに関わってくる。 ◆ 実証実験での一般ユーザ向け画面では、動的解析結果を優先し、静的解析結果については重要情報(電話帳、アドレス帳、位置情報、メールアドレス)の送信が検出された場合のみ採用し、表示している。 <p>一般利用者には解析結果が全てではないことを伝え、誤解を避けなければいけない。 (意見・コメントなど)</p> <ul style="list-style-type: none"> ◆ 解析精度を解析結果とともに伝える方法もあるが、正確に提示するには現在の技術では限界がある。 ◆ 技術的な限界、実運用上の限界を、利用者にどうわかりやすく表現するかを考えていかなければならない。

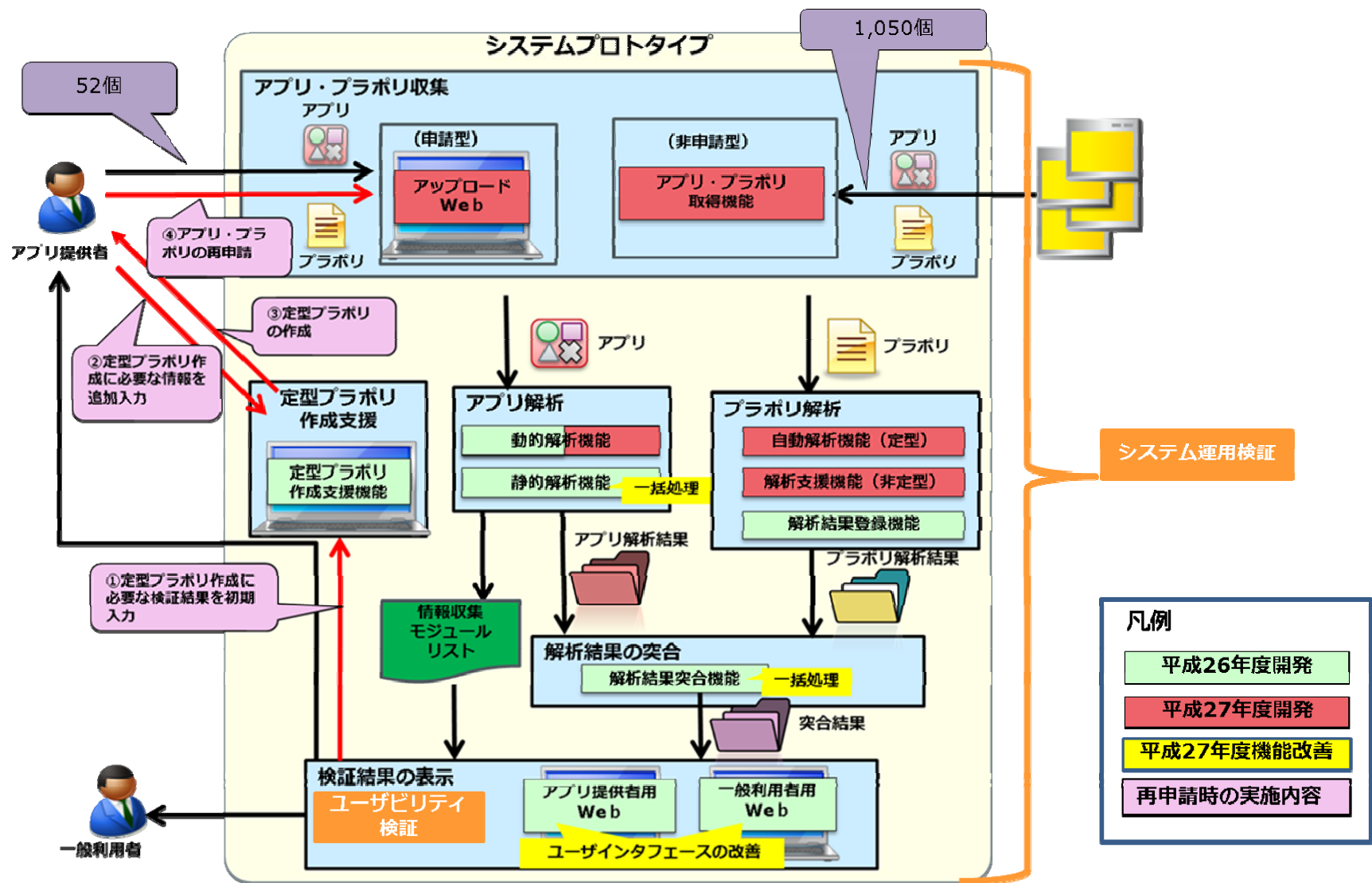
5.4. 第三者検証システムに求められる技術要素の全体像

H26年度・H27年度実証実験での実装機能とこれまでの技術WGで議論・整理した主な課題を以下にまとめる。(は実施済)

機能分類	分類	OS種別	H26 要素技術の確立 64アプリ	H27 高度化・最適化・非申請型モデルの検証 1102アプリ	課題	
アプリプラポリ取得	-	-	申請者からの送付	アプリリストの自動取得 プラポリ自動取得	<ul style="list-style-type: none"> ・アプリダウンロードの自動化はマーケット事業者の許可、協力が必要。 ・アプリのアップデートへのリアルタイムな対応（制度・運用WGで費用対効果を加味して議論） 	
プラポリ解析	-	-	手動による解析の実施	解析結果のプレを減らすために判定基準を明確化。	-	
	-	-		【定型プラポリ解析】 プラポリ作成ツールによって作成されたプラポリを自動で解析	-	
	-	-		【非定型プラポリ解析】 自動解析を行い、人による修正を実施	<ul style="list-style-type: none"> ・人による補正が必要なため、完全自動化が困難 	
アプリ解析	静的解析	Android	【バイトコード解析】 アプリケーションのJavaバイトコードからアプリケーションの利用するAPIや処理内容・フローを解析 【モジュールDB構築】 静的解析の結果を元に外部モジュールのデータベースを作成	【運用に向けた改良】 ・操作の自動化 ・apkビルド日付の追加 ・タイマー機能の追加など	<ul style="list-style-type: none"> ・Javaバイトコード以外で作られたアプリは解析不可 	
		iOS	【ソースコード解析】 利用者情報に関するAPIの調査を実施			<ul style="list-style-type: none"> ・逆アセンブルは制度的に課題がある。（著作物の複製禁止、利用規約などに抵触）
		Android	【ティント解析】 OSに利用者情報をタグ付けする機能を追加し、そのタグの送信状況から利用者情報の送信が行われているかを収集・解析 【パケットキャプチャ解析】 通信パケットを収集する。自営のプロキシサーバを経由させる事で、SSL/TLS(暗号化)通信も平文で収集・解析			【端末操作自動化・効率化】 画面情報を解析し、自動遷移を行う。 【ログ解析の自動化】 動的解析結果（通信・ティントログ）の解析自動化を行う
	iOS					
	突合	-	-	静的解析結果と動的解析結果の突合機能を作成	自動化・効率化、データ連携を改良	-
	結果表示	-	-	アプリ提供者向け、アプリ利用者向けのWeb画面を作成	画面デザインを改良	-
プラポリ作成ツール	-	-	検証結果からプライバシーポリシーを作成可能なWeb画面を作成	文言などの改良	-	

データ連携の自動化・効率化

- H27年度は、平成26年度に引き続き、スマートフォンアプリにおける利用者情報の適切な取扱いが行われているかどうか等を技術面から第三者が検証する仕組みについて構築・実証し、システムプロトタイプの高度化・最適化、検証範囲の拡大等に取り組んだ。
- システムプロトタイプの高度化・最適化については、アプリプラボリ取得機能の非申請型対応、プラボリ解析の効率化・省力化、動的解析自動化・効率化(端末操作、ログ解析等)、運用オペレーション・データ連携の自動化・効率化、結果表示ユーザインタフェースの改良等を実施した。
- 検証範囲の拡大については、申請型に加え非申請型のアプリプラボリ検証(1,000以上)、第三者による運用トライアル、アプリ提供者からの再申請プロセス検証、学生およびシニアを対象としたユーザビリティ検証等を実施した。



6.2. 実証実験まとめ①

<検証対象>

アプリ数：申請型52（Android：28、iOS：24）、非申請型1,050（Android：950、iOS：100）、合計1,102（Android：978、iOS：124）

(1) 技術検証について

①アプリプラポリ収集

●非申請型において、アプリマーケットより効率的にアプリプラポリを収集する仕組みを構築したことで、アプリDL・インストール、プラポリDL作業全てを手動収集する場合（10分／アプリ）と比較し、作業時間が改善（5分／アプリ）された。

（課題）申請型の受付をWeb化することで、オペレーション簡素化（受付確認メール送信、必須記載項目・添付資料確認等）を図ることができたが、質問対応や本人確認等において、更なる効率化の検討が望ましい。

②プラポリ解析

●解析対象としたアプリのうち、プラポリの記載があるものは708アプリ、記載がないものは394アプリとなった。

（課題）定型プラポリの自動解析機能を開発したことにより、今後のオペレーション効率化が期待されるが、本実証においては自動解析可能なアプリが1件（申請型：1、非申請型：0）であった。今後の効率化に向けては、定型プラポリ作成支援ツールの本格的な普及に向けた取り組みが重要である。

③アプリ解析

●動的解析（1,102アプリ）において、情報送信を検出したアプリは169（15.3%）、また、第三者送信を行っていたアプリは165（15%）であった。

端末操作自動化を導入したことで、手動操作（15.4分／アプリ）と比較し、自動操作（2.6分／アプリ）では1アプリあたり約13分の作業時間圧縮となった。

（課題）動的解析自動化は、大規模解析を継続的に実施する場合には、一定の効果（例：1,000アプリの解析で、約16人・日の運用コスト圧縮）を期待できるが、実行率（平均55.4%）や到達率（平均36.4%）等の精度向上に向けた改善が必要。

6.2. 実証実験まとめ②

④ プラポリ解析とアプリ解析の突合

- (A) 利用者情報の送信を利用者自身が認識できない若しくは認識と異なるアプリは165アプリあり、検証対象となった全体のアプリ数に占める割合は15.0%となり、平成26年度の突合結果(14.1%)と同等程度となった。また、情報送信を行うアプリ数に占める割合は97.6%という結果となった。
- (B) プラポリがないアプリは394アプリあり、検証対象となった全体のアプリ数に占める割合は35.8%という結果となった。

(プラポリ解析とアプリ動的解析の突合結果)

		動的解析結果		計	
		(A)送信あり	(B)送信なし		
プラポリ解析結果	①プラポリ「あり」	126(11.4%)	582(52.8%)	708(64.2%)	
	情報送信に関する記載「あり」	送信情報がプラポリの内容と「全て一致」	4(0.4%)	197(17.9%)	254(23.0%)
		送信情報がプラポリの内容と「不一致」	53(4.8%)		
	情報送信に関する記載「なし」	69(6.3%)	385(34.9%)	454(41.2%)	
②プラポリ「なし」	43(3.9%)	351(31.9%)	394(35.8%)		
計		169(15.3%)	933(84.7%)	1102(100.0%)	

(A) 利用者情報の送信を利用者自身が認識できない若しくは認識と異なるアプリ165アプリ
(全体の15.0%、情報送信を行うアプリの97.6%)

(B) プライバシーポリシーがないアプリ 394アプリ
(全体の35.8%)

(2) ユーザビリティ検証・システム運用検証について

- 学生およびシニア向けに、解析結果表示画面を提示し、アンケート・インタビューを実施した。

アプリ提供者には、解析結果の提示、再申請フローの実施に加え、アンケートを実施した。

第三者によるシステム運用検証を実施し、コメントなどのフィードバックを受けた。

① 一般利用者向けユーザビリティ検証

全体的な見やすさ・表現方法に関しては、おおむね高い評価を得られた。一方で、文章表現やページ切り替え「ボタン」の配置が分かり難い等の意見があった。

② アプリ提供者向けユーザビリティ検証

再申請に関して、自身の作ったプラポリがあるべき姿に修正されているか確認できる点が評価された。アプリ申請プロセスの更なる省力化や、より詳細な解析結果レポートへのニーズが確認された。

③ システム運用検証

システムの全体像や一連の解析フロー等への説明に対しておおむね理解を得られたが、「更なる自動化」、「信頼性担保」、「結果の公表方法」等への対応を求める意見があった。

(3) 今後の取組について

- ・ 第三者認証に必要となる実運用を想定し、スケーラビリティ(システム構成、スペック)や、稼働条件・保守運用条件等を含めた運用設計・最適化の検討が必要である。
- ・ 解析結果の信頼性担保を図るため、システム脆弱性等へのセキュリティ対策も併せて検討する必要がある。

7. 次年度（平成28年度）以降の工程（案）

- タスクフォース及び各WGの意見を受け、平成27年度は第三者検証の実運用に向け、まずは「申請モデルの検証」を実施し、「要素技術の確立」を行うとともに、第三者検証システムをもとに、制度・運用面からの諸課題の整理及び今後に残された課題の論点整理を行った。
- 今後、上記検討結果を踏まえ、以下の工程で第三者検証の実用化に向けた取組が必要である。具体的には、システム運用設計・適正化、検証の自動化・効率化、システムの脆弱性やセキュリティ対策、運用主体の選定・連携を実施するものとする。また、アプリ提供事業者、一般消費者等にスマートフォンアプリに係る安心・安全な利用環境整備に係る普及啓発活動を継続する。
- 加えて、平成26年度や平成27年度の検討、第三者検証の実運用を踏まえて、SPIの改定、他の省庁との連携を検討する。

第三者検証の実運用に向けた課題整理・解決

- システムの運用設計・最適化
- システムの脆弱性やセキュリティ対策
- 運用主体の選定・連携

第三者検証の実運用に向けた普及啓発の実施

- 業界団体等が実施するスマホ関連の普及啓発との連携、情報共有・発信のためのポータルサイトの構築、スマホ関連のメディアを通じた普及啓発の検討
- アプリ提供者向けのSPIやプラポリの作成方法の要点をまとめた普及啓発ツールの作成

SPIの改定及び政策的・制度的対応の検討

- 平成26年度・平成27年度の検討を踏まえたSPIの改定
- 他の省庁・行政法人、業界団体・事業者と連携した政策的・制度的対応の検討