別紙３

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Ⅳ～

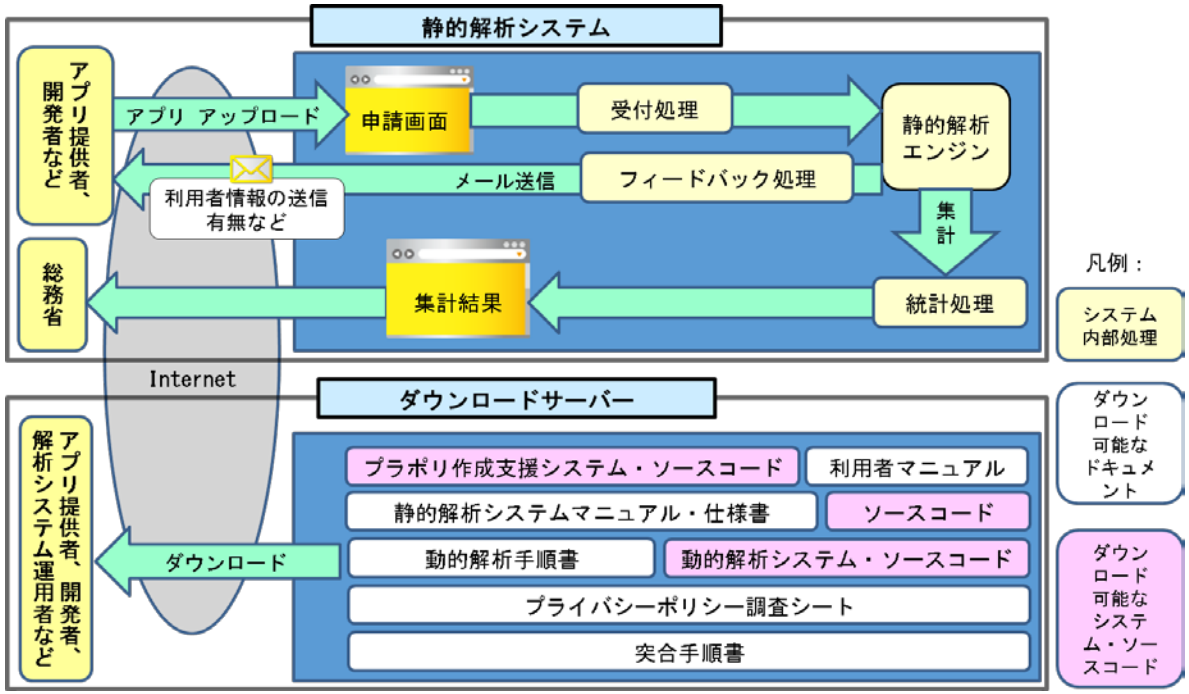
平成29年7月10日

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

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（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」（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年度は、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た。

実証実験



連携・反映

その他の施策

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. 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

SPIⅡ（平成25年9月）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25年度・平成26年度・平成27年度に各4回会合を開催）。平成28年度は3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
- 定期的なアプリプラポリ調査の実施
- 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
- 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

（3） 平成26年度・平成27年度の検討を踏まえたSPIの改訂

3. 構成員

（平成28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	曽我部 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 情報技術研究部門 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理事	竹森　敬祐	株式会社KDDI総合研究所 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　セキュリティエキスパート本部 コンシューマテクニカルサポート部　部長代行	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		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.アプリケーションのプライバシーポリシー調査　調査概要

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(50アプリ)について、アプリケーションのプラポリ(以下「アプリプラポリ」)の作成・掲載状況、SPIで示される8項目の記載内容、利用者情報の取得に関する同意取得状況(Androidアプリのみ)、概要版の掲載状況を調査した。

【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】

	①人気アプリ(上位100アプリ)	②新着アプリ
アプリ数	Android・iOS：100アプリ	Android・iOS：50アプリ
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(2017年1月)の中から50アプリを抽出※2
抽出日※3	2016年10月	2017年1月

【調査項目】

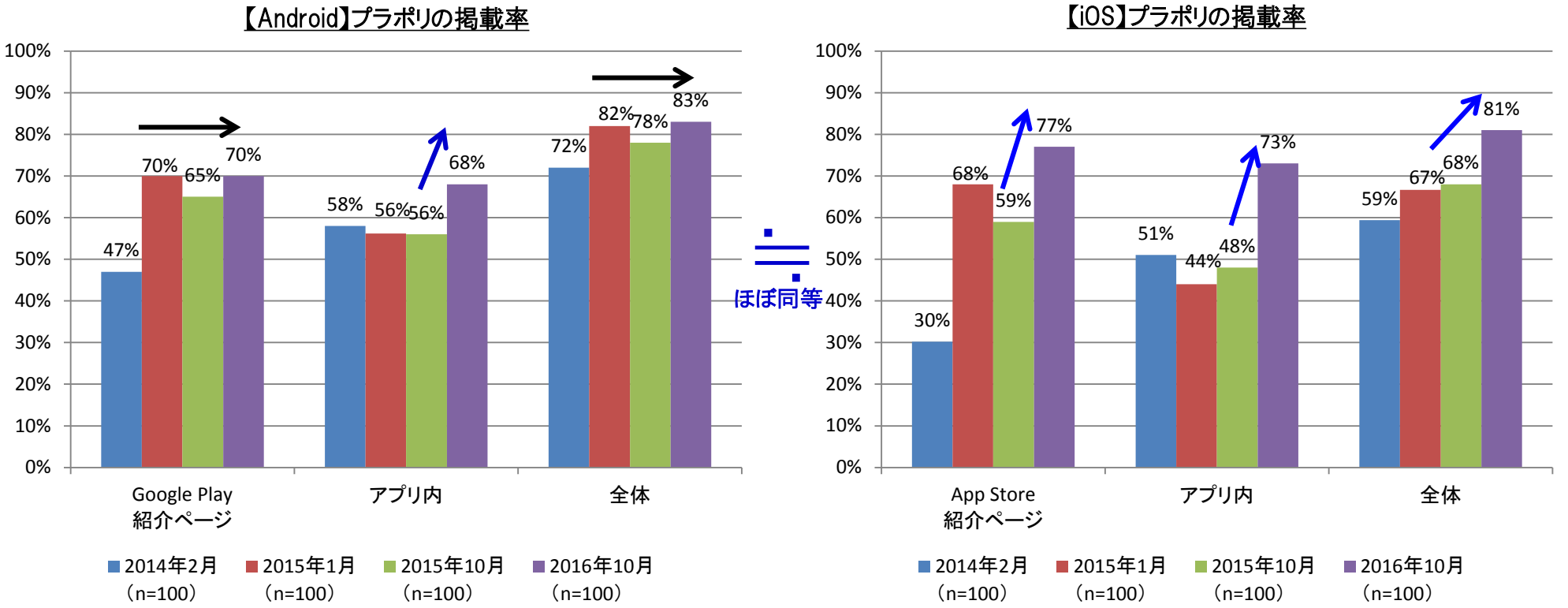
	調査内容
【項目1】アプリプラポリの作成・掲載状況	◆「Google Playのアプリ紹介ページ内」、「アプリケーション内」におけるプラポリシの掲載有無 ◆ プラポリの記載内容の分類
【項目2】「スマートフォン プライバシー イニシアティブ」で示される8項目の記載状況	◆ プラポリにおけるSPIで示された8項目の記載有無
【項目3】利用者情報の取得に関する同意取得状況 ※Androidアプリのみ実施	◆ 電話番号、メールアドレス、位置情報、アドレス帳の取得する可能性の有無 ◆ 取得する可能性のあるアプリにおけるプラポリへの情報取得の記載の有無 ◆ 取得する可能性のあるアプリにおけるアプリ内で個別同意の有無
【項目4】プラポリの概要版作成・公表状況	◆「アプリケーション内」、「Google Playのアプリ紹介ページ内」におけるプラポリの概要版の有無

※1「App Annie」から2016年10月31日の「Google Play」、「App Store」の無料ランキングにおける上位100アプリを抽出。
※2 Androidの新着アプリは「App Annie」から2017年1月10日の「Google play」の新着無料ランキングから抽出。iOSの新着アプリは2017年1月10日に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1月10日以前のアプリを抽出。
※3 調査日が異なっている原因は上位100アプリを先行的に調査し、その後新着アプリの調査を実施したため。

3.2.アプリプラポリ調査　調査結果（上位100アプリ:【調査項目1】プラポリの掲載率）

Androidにおける「全体」の掲載率は70%～80%前後（直近3年間の調査では80%前後）を保っている。一方、iOSにおける「全体」の掲載率が昨年度から13ポイント向上し、80%以上となった。

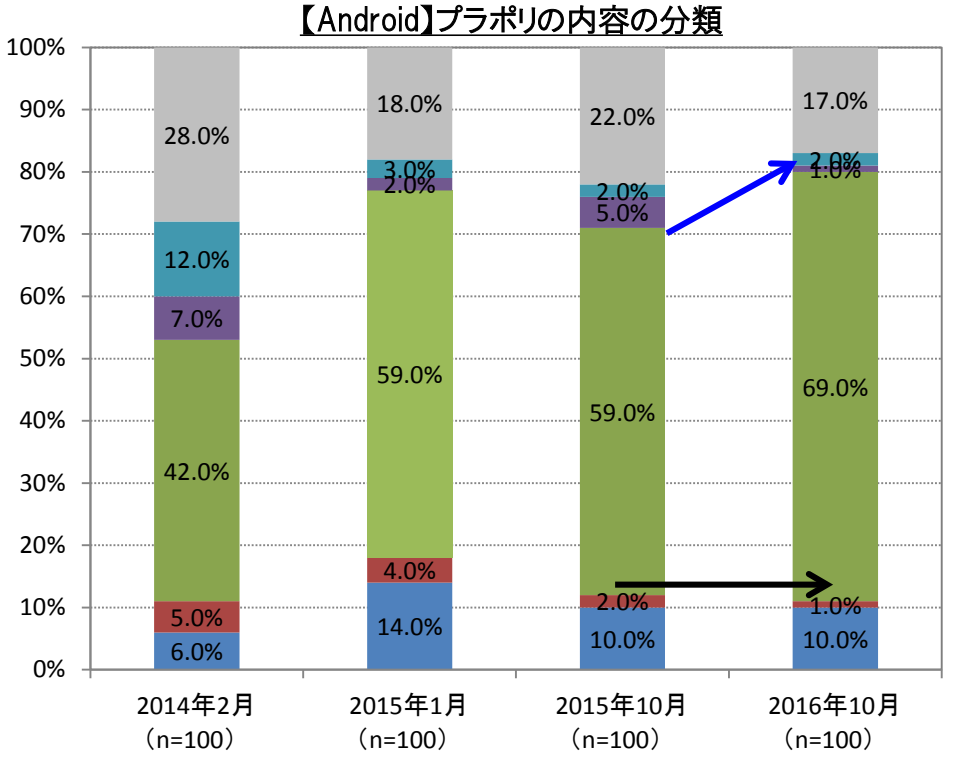
AndroidとiOSのプラポリの掲載率は、「場所別（紹介ページ/アプリ内）」でも「全体」でもほぼ同じ水準になっている。

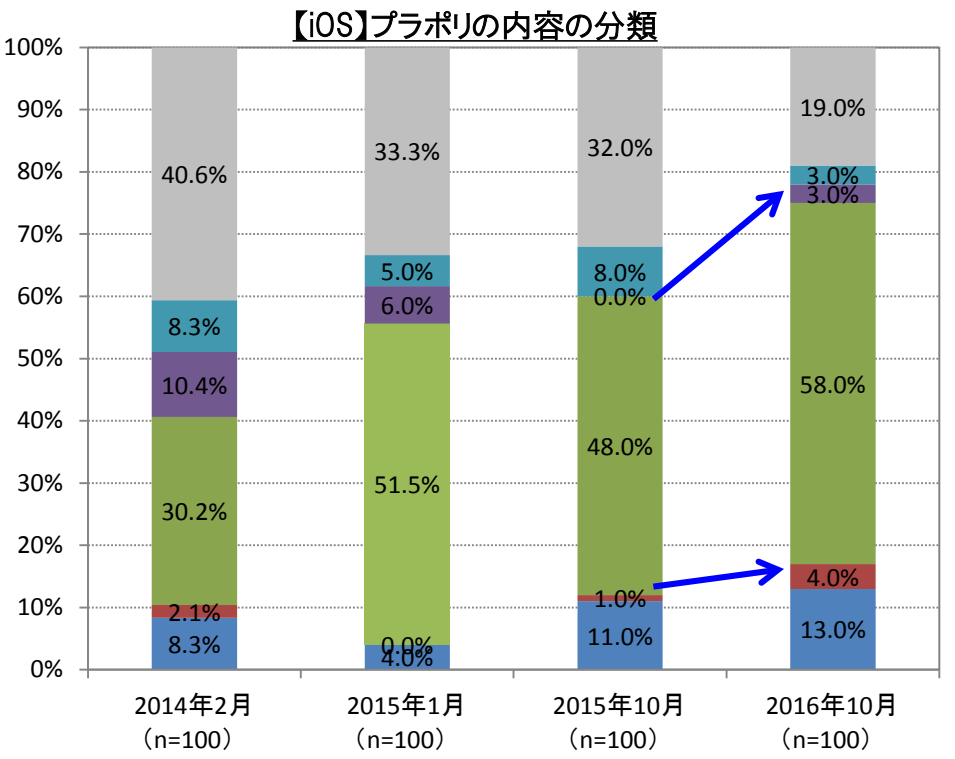


※掲載率：以下の「A」から「F」までのうち、「F」判定以外であれば、「プラポリ有り」と判断。
（「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない）
A：個々のスマホアプリ専用のプラポリが用意されている。B：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある。
C：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がない。D：一般的なWebサイトのプラポリがあるだけ。
E：会社としての抽象的なポリシー（個人情報保護方針）があるだけ。F：プラポリが記載されていない。
※紹介ページの掲載率：「紹介ページのリンク」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」、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。

3.2.アプリプラポリ調査　調査結果（上位100アプリ:【調査項目1】プラポリの内容の分類）

Android、iOSともに昨年度から、【A】・【B】・【C】の割合（アプリもしくはサービスに関する記載があるプラポリの割合）が増加している。
【A】・【B】の割合（アプリに関する記載があるプラポリの割合）については、Androidはほぼ横ばいで推移しており、iOSは増加している。





■【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（上位100アプリ:【調査項目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項目の「②取得される情報の項目」、「④利用目的の特定・明示」、「⑥情報収集モジュールに関する記載」の記載率が5ポイント以上増加している。

さらに、iOSについては「利用者情報の送信先の記載」の記載率が前年比で約2倍になっている。

SPI8項目の記載率※

番号	項目		Android		iOS	
			2015年10月（n=78）	2016年10月（n=83）	2015年10月（n=68）	2016年10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		98.7%	97.6%	98.5%	100.0%
②	取得される情報の項目		70.5%	89.2%	58.8%	80.2%
③	取得方法		35.9%	32.5%	26.5%	46.9%
④	利用目的の特定・明示		80.8%	86.7%	79.4%	95.1%
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	26.9%	21.7%	22.1%	17.3%
		利用者情報の削除の記載	38.5%	47.0%	44.1%	59.3%
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	79.5%	89.2%	85.3%	84.0%
		利用者情報の送信先の記載	38.5%	33.7%	22.1%	45.7%
		情報収集モジュールに関する記載	12.8%	22.9%	14.7%	22.2%
⑦	問合せ窓口		65.4%	85.5%	61.8%	79.0%
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%	55.4%	57.4%	60.5%

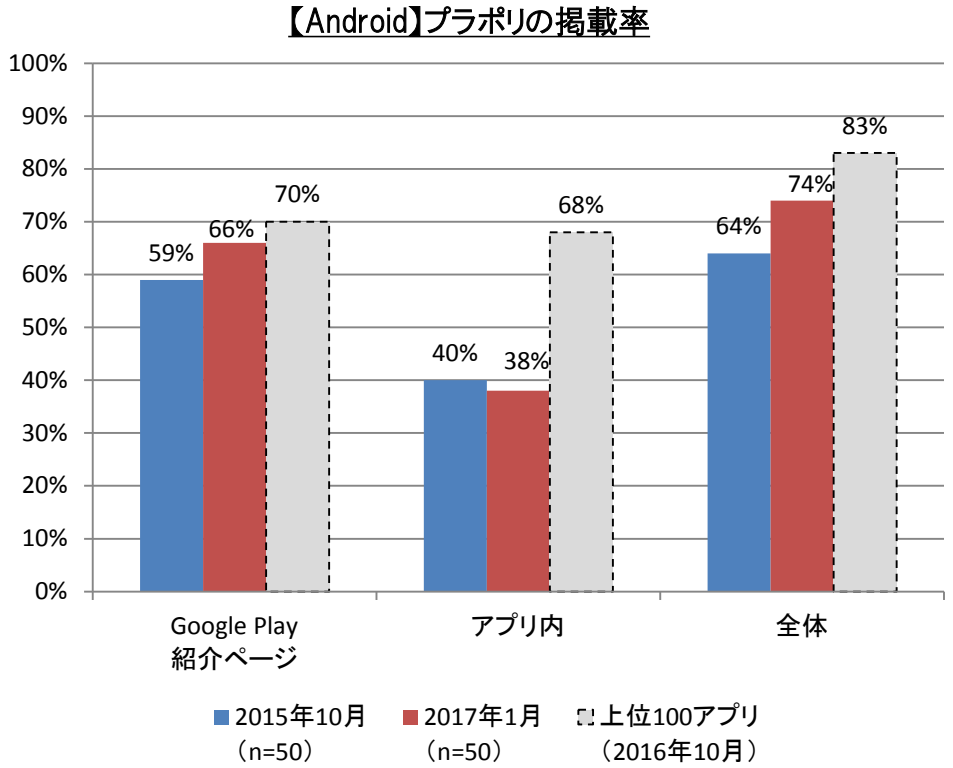
SPI8項目において、特に重要性が高いと考えられる項目

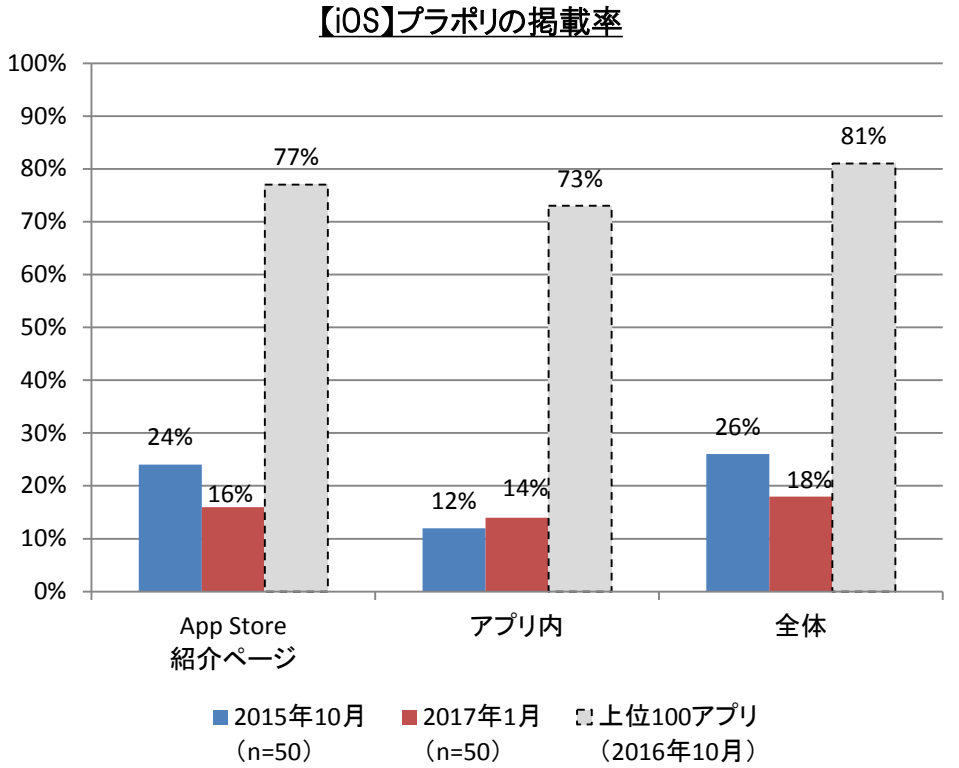
特に重要性が高い項目の中で、昨年度から記載率が5ポイント以上増加している箇所

※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(新着アプリ:【調査項目1】プラポリの掲載率)

Androidの新着アプリにおける「全体」のプラポリ掲載率は昨年度よりも10ポイント増加。また、「紹介ページ」や「全体」の掲載率は上位100アプリの掲載率と比較しても、遜色ない水準となっている。
iOSの新着アプリにおける「全体」のプラポリ掲載率は昨年度よりも10ポイント近く減少しており、上位100アプリの掲載率と比較すると、4倍以上の差が存在。





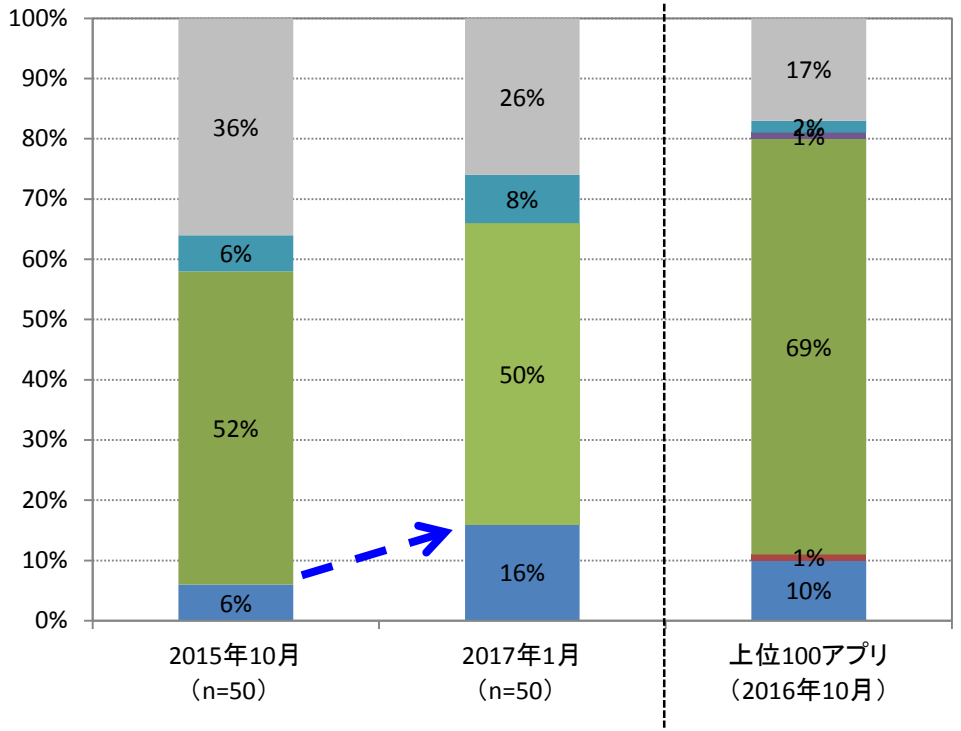
※掲載率:「F」判定以外であれば、「プラポリ有り」と判断。
（「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない）
A:個々のスマホアプリ専用のプラポリが用意されている。B:サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある。
C:サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がない。D:一般的なWebサイトのプラポリがあるだけ。
E:会社としての抽象的なポリシー(個人情報保護方針)があるだけ。F:プラポリが記載されていない。
※紹介ページの掲載率:「紹介ページのリンク」か「紹介文内での記載」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」、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。

3.2.アプリプラポリ調査　調査結果(新着アプリ:【調査項目1】プラポリの内容の分類)

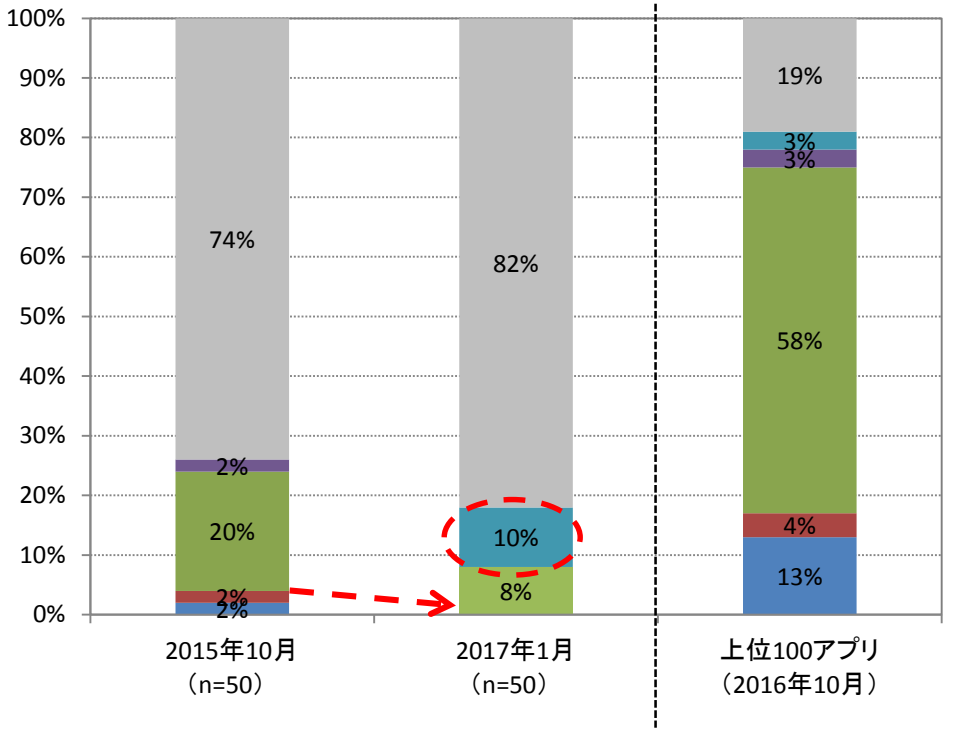
Androidにおいては、個々のアプリについて記載された【A】・【B】の割合(アプリもしくはサービスに関する記載があるプラポリの割合)が前年比2倍以上に増加している。

iOSにおいては、【A】・【B】(アプリに関する記載があるプラポリ)に該当するものは無く、抽象的なポリシーである【E】の割合が0%から10%に増加している。

【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

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

Android、iOSともに、重要性が高いと考えられる項目の記載率について、一部の項目の記載率は伸びているものの、逆に一部の項目の記載率が減少している。また、上位100アプリと比較すると、重要性が高い項目の大半で、記載率に大きな差が存在している。

SPI8項目の記載率※

番号	項目		Android			iOS		
			新着アプリ		上位100アプリ	新着アプリ		上位100アプリ
			2015年10月 (n=32)	2017年1月 (n=37)	(2016年10月、n=83)	2015年10月 (n=13)	2016年10月 (n=9)	(2016年10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		93.8%	97.3%	97.6%	100.0%	100.0%	100.0%
②	取得される情報の項目		56.3%	78.4%	< 89.2%	46.2%	44.4%	< 80.2%
③	取得方法		25.0%	45.9%	32.5%	23.1%	22.2%	46.9%
④	利用目的の特定・明示		75.0%	67.6%	< 86.7%	53.8%	66.7%	< 95.1%
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	21.9%	10.8%	21.7%	23.1%	11.1%	17.3%
		利用者情報の削除の記載	37.5%	32.4%	47.0%	46.2%	33.3%	59.3%
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	71.9%	89.2%	89.2%	38.5%	55.6%	< 84.0%
		利用者情報の送信先の記載	28.1%	13.5%	< 33.7%	7.7%	11.1%	< 45.7%
		情報収集モジュールに関する記載	12.5%	32.4%	> 22.9%	0.0%	0.0%	< 22.2%
⑦	問合せ窓口		59.4%	78.4%	85.5%	76.9%	44.4%	79.0%
⑧	プライバシーポリシーの変更を行う場合の手続き		43.8%	48.6%	55.4%	53.8%	0.0%	60.5%

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、昨年度から記載率が5ポイント以上増加している箇所

※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（上位100アプリ・新着アプリ:【調査項目3】同意取得状況）

上位100アプリについては、昨年度の調査結果と大きな変化は無い。

新着アプリについては、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2倍弱に増加しているものの、アプリプラポリに記載有りの割合（≪項目2 ≫が7ポイントに増加した結果（前年比6割増）、どちらも無いアプリの割合（ ≪項目4 ≫ ）は減少している。

【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（電話番号、電話帳、位置情報、メールアドレス）を取得し得るアプリを抽出した。
- 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		上位100アプリ		新着アプリ	
		2015年10月	2016年10月	2015年10月	2017年1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		59% (59/100)	54% (54/100)	16% (8/50)	28% (14/50)
≪項目≫1に置いて4つの情報を取得し得とされたアプリが対象	≪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	36% (21/59)	37% (20/54)	13% (1/8)	21% (3/14)
	≪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	12% (7/59)	11% (6/54)	13% (1/8)	7% (1/14)
	≪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	59% (35/59)	56% (30/54)	87% (7/8)	71% (10/14)

プライバシー性の高い情報の取得し得る割合

調査項目	上位100アプリ		新着	
	2015年10月	2016年10月	2015年10月	2017年1月
「電話番号」を取得し得るアプリの割合	19%(19/100)	16%(16/100)	2%(1/50)	12%(6/50)
「電話帳」を取得し得るアプリの割合	26%(26/100)	16%(26/100)	4%(2/50)	4%(2/50)
「位置情報」を取得し得るアプリの割合	47%(47/100)	43%(43/100)	12%(6/50)	14%(7/50)
「メールアドレス」を取得し得るアプリの割合	21%(21/100)	24%(24/100)	6%(3/50)	8%(4/50)

3.2.アプリプラポリ調査　調査結果（上位100アプリ・新着アプリ:【調査項目4】概要版の作成・掲載状況）

上位100アプリの概要版の掲載率はAndroidが2%、iOSが6%であり、昨年度からほぼ横ばいで推移。

一方、新着アプリの概要版の掲載率は、Android、iOSともに0%であった。

アプリプラポリ概要版の掲載率　調査結果

対象OS	上位100アプリ		新着アプリ	
	2015年10月	2016年10月	2015年10月	2017年1月
Android	1%	2%	2%	0%
iOS	6%	6%	0%	0%

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 コチラ でご覧いただけます。

3.2.アプリプラポリ調査　調査結果（上位100アプリ・新着アプリ：4つの達成基準による整理）

上位100アプリにおいてはAndroid、iOSともに「プラポリの掲載（基準①）」、「SPI8項目の重要の高い4項目の記載（基準②）」を満たしているアプリの割合が昨年度よりも増加し、6割以上のアプリが基準②までを満たしている。iOSについては、更に「SPI8項目の記載（基準③）」を満たしているアプリの割合も昨年度よりも増加している。

新着アプリにおいては、Androidについて基準①・②を満たしているアプリ割合が増加しているものの、iOSでは減少している。

			基準① 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）	基準② 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」	基準③ 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④ 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）
上位100	Android	15年	78%	51%	10%	1%
		16年	83% ↑	63% ↑	7% ↓	0%
	iOS	15年	68%	32%	9%	2%
		16年	81% ↑	63% ↑	15% ↑	1%
新着アプリ	Android	15年	64%	26%	10%	0%
		16年	74% ↑	40% ↑	10%	0%
	iOS	15年	26%	10%	4%	0%
		16年	18% ↓	6% ↓	0% ↓	0%

3.3.アプリプラポリ調査　調査結果総括

現状分析と傾向	○上位100アプリのプラポリ掲載率はAndroid、iOSともに80%以上に達し、Androidの新着アプリ（新着アプリのランキングでの人気アプリ）の掲載率も70%以上に達しており、**「プラポリの作成・掲載」については、大手のアプリ提供者には浸透してきた**と考えられる。ただし、iOSの新着アプリ掲載率は20%と低く、中小・個人事業者には浸透しているとは言い難い。（P4、P7） ※iOSの新着アプリはリリース日順で取得したため、他の調査対象よりも中小・個人事業者の割合が高いと考えられる。 ○しかし、大半のプラポリは会社全体やサービス全体の個人情報の取扱いに関してのみ記載されており、**アプリの取得情報を意識して記載されているプラポリは少ない**。（P5、P8） ○また、概要版の掲載率は、上位100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。（P11）
環境変化	○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計画が明らかになり、App Storeでもガイドライン変更によって**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。この結果、Android、iOSともに「プラポリの作成・掲載」は更に浸透していく可能性が存在している。（P15、P17） ○最新のAndroid・iOSでは、連絡帳や位置情報などの取得については、**アプリ内で個別の同意取得が必須**となった。この結果として、今年度のプラポリの「取得される情報の項目」、「利用目的の特定・明示」の記載率が増加しており、この傾向は続くと考えられる。（P6、P16）
今後の課題・取組	○プラポリの掲載率は向上しているものの、**アプリに関連する記載やアプリを意識した記載が無いプラポリの割合が高く**、今後は**プラポリの質を向上していく**ことが重要となる。また、概要版の掲載率は相変わらず低く、**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**も重要と考えられる。 ○今後はAndroid・iOSともに**プライバシー性の高い情報の取得については、アプリ内での個別の同意取得が一般的となる**ため、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備されていないと、利用者の不安をいたずらに増大させてしまう可能性が存在している。

4.1.利用者情報の取扱いに関する調査の実施概要

「民間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」について、下記のような観点で調査を実施した。

民間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・業界団体の取組みを調査し、過去の調査内容をベースに、最新の情報を更新する。

【調査対象の事業者】
◆アプリ提供者
◆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）
◆セキュリティベンダー
◆業界団体　等

諸外国における取組状況に関する調査・分析

【調査概要】
◆諸外国の取組み状況を次の①～③の観点で調査する。
①政府における取組状況
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状況
※その他事業者として、各国の通信事業者等を想定

【調査対象国】
◆米国
◆欧州（EU、ドイツ、フランス、イギリスなど）
◆韓国

※上記以外の国でも、大きな取り組みがあれば、適宜調査を実施予定

4.2.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〕:App　Store審査ガイドラインの大幅な改定）

2016年6月にApp Store審査ガイドラインが大幅に改定され、30の大項目が「安全性」、「パフォーマンス」、「ビジネス」、「デザイン」、「法的事項」に集約。プライバシーに関する記載も「法的事項」の中の小項目「プライバシー」に集約された。

改定後のガイドラインではプラポリを明示すべきアプリとして、新たに「デバイスからのユーザーデータ（位置情報、連絡先、カレンダーなど）へのアクセスを実行するアプリケーション」が追加された。

改定前のガイドラインにおけるプラポリ掲載に関わる記載

17. プライバシー
17.5　ユーザーの既存アカウント登録やアクセスの際にプライバシーポリシーを含まないアプリは審査を通せない。

25. 拡張機能プライバシー
25.7キーボードの拡張機能を提供しているアプリは、カテゴリをUtilitiesで、プライバシーポリシーが設定されていない場合、審査を通せない。

26. Homikit
26.2 Homekit frameworkを利用する際にマーケティング文書とプライバシポリシーが必要です。それがなければ審査を通せない。

27. Healthkit
27.7　被検体の研究の際にHealth Kitを利用する場合にプライバシーポリシーを提供しないアプリは審査を通せない。

29. Apple Pay
29.4　Apple Payを利用しているアプリはプライバシーポリシーを提供する必要があります。なければ審査を通せない。

集約

改定後のガイドラインにおけるプラポリ掲載に関わる記載

5. 法的事項
5.1 プライバシー
5.1.1 データの収集及び保存
(i)ユーザーまたは使用状況に関するデータを収集するアプリケーションでは、データ収集に関するプライバシーポリシーを明示し、ユーザーからの同意を得る必要があります。これにはHealthKitまたはその他の健康および医療テクノロジー、HomeKit、Keyboard extension、Apple Pay、ステッカーとiMessage extensionを実装するアプリケーション、ログイン、デバイスからのユーザーデータ（位置情報、連絡先、カレンダーなど）へのアクセスを実行するアプリケーションが含まれますが、これらがすべてではありません。

4.2.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〕:ユーザーデータへのアクセス許可取得の規制強化）

iOSでは数年前からプライバシー性の高い情報にアクセスする際にはアプリ内で個別に同意を取得する仕様であったが、iOS10では同意を取得する際に説明文（情報の取得理由・利用目的）の記載が必須となった。

iOS10での変更点

アクセス許可の取得画面

【補足】

◆ 左記の部分に記載が無いと、アプリ公開の申請を実施した際に、機械的にリジェクトされる模様

◆ 開発者向けリファレンスにも下記のような記載が存在

” To protect user privacy, an iOS app linked on or after iOS 10.0, and which accesses the user‘s photo library, must statically declare the intent to do so.
<中略> If your app attempts to access the user’s photo library without a corresponding purpose string, your app exits. ”

※上記は“photo library”に関する記載だが、他の情報についても同様の記載が存在

規制強化の対象となっているアクセス権

	対象となる操作	対応するキー
1	メディアライブラリへのアクセス	NSAppleMusicUsageDescription
2	Bluetooth インターフェースへのアクセス	NSBluetoothPeripheralUsageDescription
3	カレンダーへのアクセス	NSCalendarsUsageDescription
4	カメラへのアクセス	NSCameraUsageDescription
5	連絡先へのアクセス	NSContactsUsageDescription
6	ヘルスデータへのアクセス	NSHealthShareUsageDescription
7	ヘルスデータの変更	NSHealthUpdateUsageDescription
8	HomeKit の設定データへのアクセス	NSHomeKitUsageDescription
9	位置情報へのアクセス (常に許可)	NSLocationAlwaysUsageDescription
10	位置情報へのアクセス (使用中のみ許可)	NSLocationWhenInUseUsageDescription
11	マイクへのアクセス	NSMicrophoneUsageDescription
12	加速度計へのアクセス	NSMotionUsageDescription
13	フォトライブラリへのアクセス	NSPhotoLibraryUsageDescription

4.2.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）

Googleが世界中の開発者に警告通知を送信し、有効なプラポリが記載されていないGoogle Playのアプリ(Google Playのユーザーデータポリシーに違反するアプリ)にペナルティを科す計画を明らかにしている。

- 2016年12月頃、「ユーザーデータポリシーに違反する」と同社が判断した開発者に対し、警告通知が送信された。
- ユーザーの個人情報や機密情報を扱うアプリに対してプラポリをユーザーが読める場所にはっきりと表示すること(最低でもGoogle Playの紹介ページにプラポリのURLの掲載、アプリ本体への掲載は必須)を求めている。
- 通知を受け取った開発者は2017年3月15日までに上記について対応する必要があり、対応しないアプリについては、「表示を制限」、あるいは削除する可能性があるとしている。

Googleの取組の概要

【2016年12月に警告通知の送信】
◆「ユーザーデータポリシーに違反する」と判断された開発者らに対し、警告通知が送信

【Googleの要求内容】
◆ プライバシーポリシーをユーザーが読める場所にはっきりと表示すること
◆ Google Playの紹介ページへのリンクの掲載、アプリ本体への掲載は必須

【違反者への措置】
◆ 2017年3月15日までにユーザーデータポリシーに対応しないアプリについては、「表示を制限」、あるいは削除する

Google Playのユーザーデータポリシー

ユーザーデータ

ユーザーデータ(ユーザーから提供される情報、ユーザーについて収集する情報、ユーザーによるアプリや端末の利用に関して収集する情報など)の扱い方については、データの収集、使用、共有を開示するなどして、その旨を明らかにする必要があり、データの使用は開示での説明に限定する必要があります。アプリが個人情報や機密情報を扱う場合は、下記のように追加の要件があります。このポリシーは Google Playの最小プライバシー要件を規定するものであり、該当法で求められる場合は、デベロッパーやアプリがその他の制限や手続きに従うことが必要になります。

個人情報や機密情報

プライバシー ポリシーと安全な転送

ユーザーの個人情報や機密情報(個人識別情報、財務情報、支払い情報、認証情報、電話帳や連絡先のデータ、マイクやカメラのセンサーデータ、端末の機密情報など)を扱うアプリは、以下の要件を満たす必要があります。

- プライバシー ポリシーを Play Developer Console の所定の欄から送信し、また Play で配信するアプリ本体にも掲載すること。
- 最新の暗号手法を使用して(HTTPS 経由などで)転送するなど、ユーザーデータを安全に扱うこと。

4.3.諸外国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（米国　政府〔FTC〕：ヘルスケアアプリの開発者向けガイダンスツールの公開）

FTCは2016年4月にヘルスケアアプリの開発者向けのガイダンスツール（ウェブサイト）を発表した。ツールではアプリの機能や取得情報等について質問が表示され、回答に応じて、適用される可能性のある法律や規制の情報が表示される。

ヘルスケアアプリの開発者向けのガイダンスツール概要

◆FTCは同ツールを米国保健福祉省国家医療IT調整室（ONC）、教育省公民権局（OCR）、米国食品医薬品局（FDA）と共同で開発した。

◆同ツールでは、アプリが収集する情報や情報共有機能の有無・範囲、疾患や健康診断や治療に関する機能の有無などについての質問が表示され、適用される可能性のある法律や規制に関する詳細な情報が表示される。対象となっている法律・規制は次の通り。

- 医療保険の携行性と責任に関する法律（HIPAA ：Health Insurance Portability and Accountability Act）
- 連邦食品医薬品化粧品法（FD&C Act：Federal Food, Drug, and Cosmetic Act ）
- 連邦取引委員会法（FTC Act：Federal Trade Commission Act ）
- FTC’s Health Breach Notification Rule　※HIPAAで保護されない医療情報が漏えいした時の通知に関する順守ルール

＊「ONC」：The Office of the National Coordinator for Health Information Technology. ＊「OCR」：Office for Civil Rights.＊「FDA」：Food and Drug Administration.

ツールで表示される質問

1	識別可能な健康情報を作成、受信、維持、送信するか？ (Do you create, receive, maintain, or transmit identifiable health information?)	6	「最小限のリスク」をユーザーに提供しているか？ (Does your app pose “minimal risk” to a user?)
2	開発者は医療提供者や保健計画であるか？ (Are you a health care provider or health plan?)	7	アプリは「医療アプリ」かどうか？ (Is your app a “mobile medical app”?)
3	消費者はアプリを利用するための処方箋が必要か？ (Do consumers need a prescription to access your app?)	8	開発者は非営利団体化かどうか？ (Are you a nonprofit organization?)
4	アプリはHIPAA対象事業者（病院、診療所、保険会社等）を代表して開発されたものか？(Are you developing this app on behalf of a HIPAA covered entity?)	9	直接顧客に健康記録を提供しているか？（もしくは、それ以外の誰かと情報をやり取りしたり、サービス提供をしていないか？） (Do you offer health records directly to consumers (or do you interact with or offer services to someone who does)?)
5	アプリは疾患の診断、病気の治癒、緩和、治療、予防のためのものか？ (Is your app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease?)		

＊「医療アプリ(mobile medical app)」：医療機器の付属品としてのアプリ（例：輸液ポンプの設定変更を行うアプリ）、他の医療機器からのデータに対して高度な分析や解釈を行うアプリ（例：消費者固有のパラメーターを利用し、放射線治療のための投薬計画を作成するアプリ）などが該当する。

4.3.諸外国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（韓国：政府系アプリにおける個人情報の流出リスクに関する指摘）

2016年8月に韓国の消費者団体が、韓国政府が提供する政府系サービスのポータルアプリで紹介されている91のAndroidアプリを調査した結果、1アプリの平均パーミッション取得数が10以上であり、個人情報の流出リスクが高いことを発表した。

政府系サービスのポータルアプリの概要

◆ 既存の200の政府サービスの案内アプリであり、**分野別やライフサイクル別にサービスを案内したり、個人の事情に合わせたサービスを推奨したり**してくれる

◆ 同アプリの発表時に政府は「同アプリは、**個人情報の流出の懸念を払拭するために、不要なパーミッションを取得せず、個人情報の問題が発生しないように徹底的に管理**していく」と報道資料で明言している。

ポータルアプリの画面キャプチャ

消費者団体による政府系アプリに対する調査概要・結果

【調査内容】

◆ ポータルアプリで紹介されているサービスのうち、Android アプリの形式で提供されている91個のアプリに対して、**アプリが取得するパーミッション数とパーミッションの内容、取得パーミッションとアプリの内容との整合性等**について、調査・分析を実施

【調査結果】

◆ **91アプリの平均パーミッション取得数は10以上**（最もパーミッション取得数が多いアプリは、警察庁の情報提供アプリで27個）

◆ パーミッションの取得が**5つ以下のアプリは全体の14%**

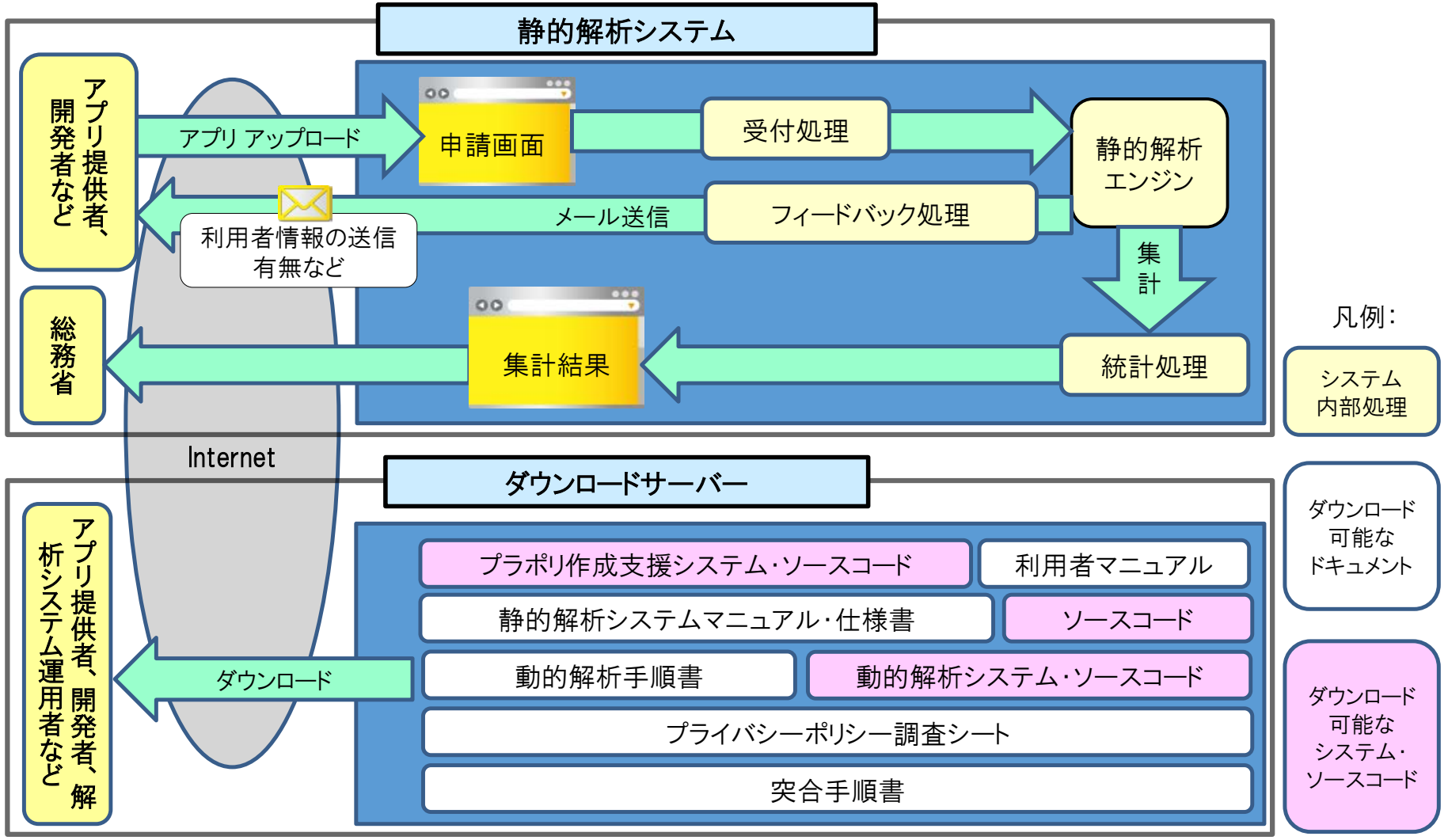
◆ 空港ガイドや登山情報、交通情報アプリ等の情報提供アプリが、端末IDや携帯電話の状態、連絡先等のパーミッションを取得

【抗議内容】

◆ 調査結果の様な状況で、ポータルアプリが不要なパーミッションを取得していないというだけで、**「個人情報の問題が発生しないようにしている」というような趣旨の発言をすることは、消費者をだますこと（目隠し行為）につながる**

5.1. 実証実験の実施概要

●アプリ収集、アプリ解析、プラポリ作成支援など実証実験で構築した仕組みを一般に公開するため、下記のシステム改善を行った。
・アプリを申請し静的解析の結果を得るためのWebベースのユーザーインタフェースを開発（静的解析システム）
・プラポリ作成支援システム、動的解析システムについて、ダウンロードして実行できるよう使用性を改善
●選定した運用検証主体にて、上記システムを一般公開し、運用検証を行なった。



5.2. システムの運用検証実施事項

●運用検証を行なう主体の選定

運用検証主体として、以下の要件を満たす日本スマートフォンセキュリティ協会（以下「JSSEC」）を選定した。

要件	評価
「SPI」「SPIⅡ」「SPO」「SPOⅡ」「SPOⅢ」を十分に理解する者が所属していること	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及び技術WG、制度・運用WGの構成員として参画し、「SPI」「SPO」に精通したメンバが所属している。
システムの運用を行う能力及び体制を十分に備えていること	JSSECのホームページを運用し、セキュリティに関する啓発活動を行っている。 JSSECの活動を担う会員企業として幹事会員31社、正会員87社が登録しており、システム運用をサポートできる体制・能力が十分ある。

●実証実験結果

実証実験として下記の検証を行なった。

診断種別	実施内容	検証結果
アプリ検証 （2016.12）	マーケットでの無料アプリランキングの上位100アプリについて、静的解析を実施した。	利用者情報の送信を検出したアプリ数が42件あった。このうちプラポリに利用者情報を取得する旨の記載がないものが11件あり、記載不足と疑われるものが22件あった。 （公開検証直前におけるマーケットの動向を把握）
公開前ユーザビリティ検証 （2017.1）	スマートフォンのアプリ提供者、開発者などを対象に、公開内容について利用者の視点から意見を求めた。	合計10件の指摘に対して改善を行い、システムの使用性を向上した。
セキュリティ診断 （2017.1, 2017.3）	（事前）ネットワーク検査、サーバー検査、Webアプリケーション検査を実施した。 （事後）サーバーログなどを検査し、セキュリティ侵害の発生有無について診断した。	（事前）Webアプリケーション検査（Web動的コンテンツ検査、ソースコード解析）にて、2件の脆弱性を検出し適正に対策処置した。 （事後）セキュリティ侵害が発生していないことを確認した。
公開検証 （2017.2）	システムを一般公開し、JSSECがシステム運用を行った。	大きなトラブルはなく、安定的に運用できた。 検証後、アンケート項目を追加し統計情報を充実させた。

5.3. 課題に対する実施結果

第三者検証に必要となる実運用を想定した課題に対して、実施結果を以下に記載する。

No.	課題	主な実施結果
1	スケーラビリティの検討	●静的解析エンジンの要求条件を満足するとともに、実証実験での実績を考慮して、最適なサーバー構成およびスペックを選定した。 ●静的解析システムの公開検証期間中、サーバースペックなどに起因するトラブルは無かった。解析依頼の受付が輻輳したり、解析中にサーバーがダウンすることもなく安定的に運用できた。
2	運用設計、最適化の検討	●本実証実験の運用検証主体であるJSSECにヒアリングして、システム要件およびシステム構成を決定した。 ●アプリケーション第三者検証システムプロトタイプの実運用に向け、人手を掛けないで効率的なシステム運用ができることを目的として、アプリケーション提供者・開発者が自主的かつ自立的に活用できるシステムを設計・開発した上で、一般公開による運用検証を実施した。 ●運用検証ではトラブルやセキュリティ侵害などの大きな問題もなく、効率的なシステム運用が実現できた。 ●通常のWebサイト運用と同程度の対応稼働で運用可能であることが確認でき、民間における実運用に耐えられるアプリケーション検証システムの一つのモデルが確立できた。
3	セキュリティ対策	●一般公開に伴う脆弱性及びサイバー攻撃のセキュリティ対策として、運用検証前にシステムのセキュリティ診断を実施し、その指摘事項に対して適切な対策を実施した。 ●運用検証後にも、サーバーログなどを検査し、セキュリティ侵害が発生していないことを確認した。
4	申請型モデルの受付自動化	●静的解析システムについては、アプリ提供者がWebから解析依頼を申請し、システムが静的解析を自動実行することで解析結果をメールで該当利用者に返信するユーザーインタフェースを追加開発した。 ●運用者が人手で受け付けて対応処理するのではなく、申請受付から結果回答までの自動化が実現できた。
5	ユーザビリティの高度化	●静的解析システムについては、フロントエンド機能を開発し、使い勝手の向上を図った。 ●動的解析システム、プライバシーポリシー作成支援ツールについては、ダウンロードして利用できるよう機能を改善した。 ●プライバシーポリシー解析、静的・動的解析、突合、プライバシーポリシー作成支援の手順についてドキュメントを整備し公開することで、アプリ提供者が自立的に活用できる仕組みを提供した。 ●公開前ユーザビリティ検証を行なったことで、各システム毎に使用性の改善が図れた。

5.4. 今後の運用について

●JSSEC でのシステム運用

- 今回の実証実験により作成･公開された以下の成果物を基に JSSEC 内でシステムを再構築し運用を行う。
  - Androidアプリケーション静的解析システムのソースコード
  - Androidアプリケーション静的解析システム運用マニュアル

（注） Androidアプリケーションの解析エンジンについては、NTTソフトより利用許諾を受けた上で利用する。

- 公開アドレスは引き続き https://jsas.jssec.org/ とする。
  - 運用による統計資料も公開対象とする。
  - 資料についても引き続き https://www.jssec.org/jsas にて公開する。

- 公開するシステムの構成については、実験時に行ったシステム構成を踏襲する。
- システム運用を行うJSSEC内のタスクフォースでは主に以下の作業を行うことを想定している。
  - システムログなどの確認作業
  - システムのバージョンアップ、再起動などの作業
  - 運用についての判断
    - システムの運用期間については特に定めていない。

●体制

- 技術部会内にシステム運用を行うタスクフォース(もしくはワークグループ)を設置する。
  - 運用については、タスクフォースに参加する JSSEC内のメンバーによって実施される。