資料２－２

スマートフォンを経由した利用者情報の取扱いに関するWG　最終取りまとめ

スマートフォン プライバシー イニシアティブ

－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－

（案）

スマートフォンを経由した

利用者情報の取扱いに関するWG

平成24年６月

目次

はじめに

2011年度（平成23年度）の我が国におけるスマートフォンの新規出荷台数は、国内における携帯電話端末の新規出荷台数のうち50%以上を占め、2,000万台を超えたとされる。これに伴い、我が国においてスマートフォンが急速に普及してきており、平成23年度末にはスマートフォンの世帯普及率が約3割となり前年度の約3倍増となるなど、幅広い層への普及が進んできているといえる。

高度な情報処理機能が備わったスマートフォンは、様々なアプリケーションをインストールすることにより、自分好みにカスタマイズして多様な目的のために活用することができる。高い利便性は、オープンイノベーションの成果でもあり、各アプリケーションがスマートフォンの中の様々な機能や情報を活用することによっても達成されている。

一方、常に電源を入れて持ち歩くスマートフォンは、利用者の行動履歴や通信履歴等、多数の情報の取得・蓄積が可能である。様々なアプリケーションがスマートフォンの中の情報へアクセスを行い、利用者がそれぞれの情報がどのように共有され利用される可能性があるか十分に理解することが難しくなり、不安を覚える場合もある。

このような状況の下で、「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（以下「諸問題研究会」という。）」が2011年（平成23年）12月に公表した「電気通信サービス利用者の利益の確保・向上に関する提言」において、スマートフォンのセキュリティ確保等スマートフォンに係る安全・安心の在り方について専門家による検討を進める必要があるとされた。さらに、「スマートフォン・クラウドセキュリティ研究会」が同じく2011年（平成23年）12月に公表した「中間報告～スマートフォンを安心して利用するために当面実施されるべき方策～」において、スマートフォンのセキュリティに関して利用者が最低限とるべき対策が「スマートフォン情報セキュリティ３か条」として発表されるとともに、位置情報等の利用者情報を利用者が意図しない形で外部に送信するアプリケーションが問題となっていることから利用者情報に関する課題について別途検討の場を設けて詳細な検討を進めることが必要であるとされた。

これらの要請を受けて、2011年（平成23年）12月に諸問題研究会において「スマートフォンを経由した利用者情報の取扱いに関するWG」を設置することが決定された。2012年（平成24年）1月には第１回会合が開催され、4月にはスマートフォンの利用者情報に係る事実関係及び主な論点を取りまとめた「中間取りまとめ」及び利用者が少なくとも注意すべき事項について取りまとめた「スマートフォン　プライバシー　ガイド」が発表された。

その後、便利で多様なサービスが提供される環境を確保しつつ、利用者の情報が守られ、安全・安心にこれらサービスを利用者が享受し、選択することができるために、多

様な関係者がとるべき対応について精力的な検討が進められ、①スマートフォンの利用者情報の取扱いに関する「スマートフォン利用者情報取扱指針」、②利用者に対する情報提供・周知の在り方、③国際的連携の推進を含む最終取りまとめを行った。本最終取りまとめを踏まえた利用者情報の適切な取扱いにより、スマートフォンの安全・安心な利用環境が確保され、スマートフォン市場の中長期的な発展に資することが期待される。

なお、本最終取りまとめのタイトルである「スマートフォン・プライバシー・イニシアティブ」については、本報告書がスマートフォンにおける利用者情報の取扱いに係るプライバシー問題等についての我が国における先駆的な検討結果であることを示すとともに、関係事業者等や業界団体のイニシアティブによる自主的な取組の推進が期待されるものであることを示している。こうした課題への対応は、欧米先進国をはじめ世界に共通する課題でもあり、本報告書が世界における政策協調に向けて一定の役割を果たすとすれば望外の喜びである。

第Ⅰ部

スマートフォンと利用者情報に関する現状

第Ⅰ部では、スマートフォンと利用者情報の現状について、具体的事例や諸外国の動向、制度的な現状について取りまとめることとする。

第1章では、スマートフォンの現状について、スマートフォンの特性、普及動向とともに、スマートフォンをめぐるサービス構造を把握する。スマートフォンをめぐるサービス構造は、垂直統合モデルの従来の携帯電話と異なり水平分業モデルであり、広告配信事業者や情報収集事業者等が提供する情報収集モジュールをアプリケーション提供者が組込み、この情報収集モジュールを通じて、スマートフォン上の利用者情報が情報収集事業者等に取得される場合があるといった特徴がある。

第2章では、スマートフォンにおける利用者情報の現状について把握する。常に電源を入れてネットワークに接続した状態で持ち歩くスマートフォンには、電話帳や通信履歴、GPS位置情報、写真やビデオ、アプリケーションの利用履歴、ウェブページ上の行動履歴など様々な個人の生活に密着した情報が蓄積されている。スマートフォンに対しては100万以上のアプリケーションが提供され、利用者情報を活用しつつ、多種多様な利便性の高いサービスが提供されている。一方、様々なアプリケーションやこれに組み込まれた情報収集モジュールがスマートフォンの中の利用者情報へアクセスし、利用者がそのことを十分理解・把握しないまま、これら情報が自動的に取得され外部に送信されることなどに伴い、個人情報漏洩やプライバシー侵害のおそれも指摘される。

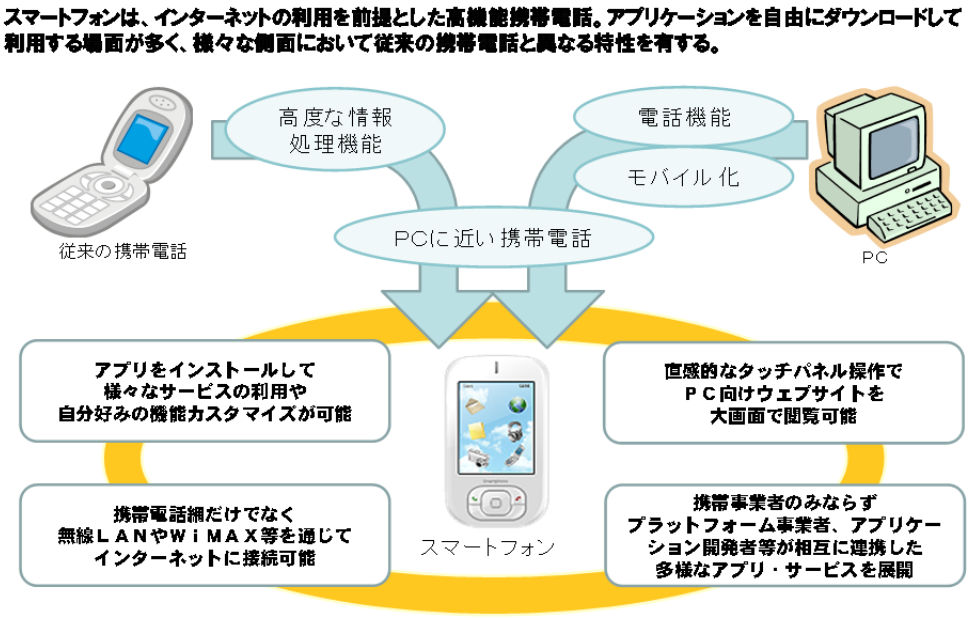
第3章では、利用者情報に係る制度とこれまでの取組について把握する。具体的には、個人情報の保護に関する法律、プライバシーに係る情報としての法的保護、利用者視点を踏まえたICTサービスに係る諸問題に関する研究会の「第二次提言」における「配慮原則」などとともに、米国、欧州等における消費者のプライバシーや個人データ保護に関する最近の動向について把握する。

第１章　スマートフォンに関する現状

１　スマートフォンの特性

スマートフォンは、従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末である。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的である。また、スマートフォンは、インターネットの利用を前提としており、携帯電話の無線ネットワーク（いわゆる3G回線等）を通じて音声通信網及びパケット通信網に接続して利用するほか、Wi-Fi等無線LANに接続して利用することも可能である。

【図表1-1：スマートフォンの特性】



２　スマートフォンの普及動向及び将来展望

近年、世界的にスマートフォンの普及がみられ、日本においても年々出荷台数が伸びている等、スマートフォンがより身近な存在になっている。2011年度（平成23年度）におけるスマートフォンの国内出荷台数は2,417万台とされており、全携帯電話端末出荷台数の56.6%を占めたとされる[1]。2012年度（平成24年度）以降も普及の拡大が見込まれており、2016年度（平成28年度）には8割を占めることが予想されている[2]。また、2011年度（平成23年度）末におけるスマートフォンの世帯普及率が29.3%となり、前年度末（9.7%）

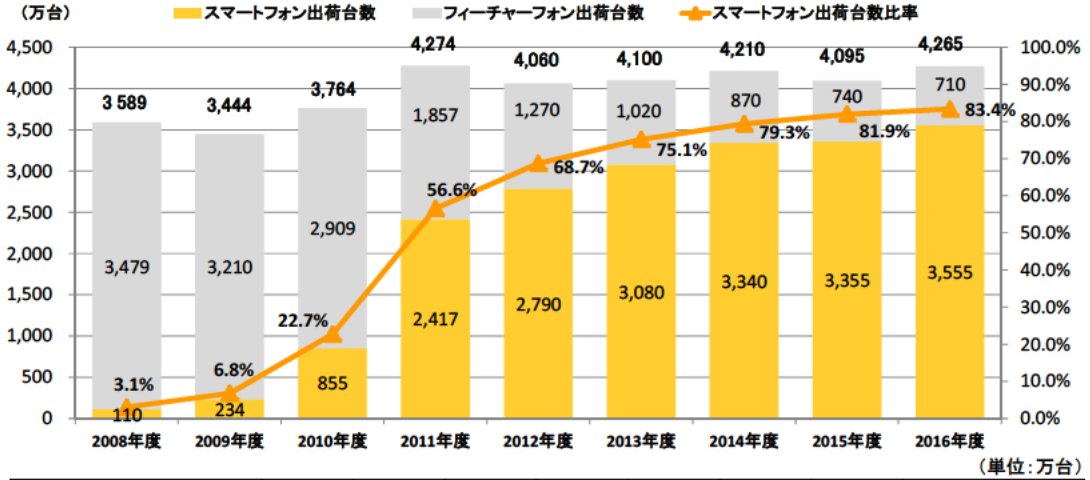
1 株式会社 MM 総研調べ「2011 年度通期国内携帯電話端末出荷概況（12 年 5 月）」。
http://www.m2ri.jp/newsreleases/main.php?id=010120120509500
2 株式会社 MM 総研調べ「スマートフォン市場規模の推移・予測（12 年 3 月）」。

の約3倍に達する[3]など、一般世帯の利用者の間にも普及が進んでいる。

スマートフォンは、外出先を含むいつでもどこでもインターネット利用を容易とするものであり、スマートフォン利用者の携帯電話端末により様々にインターネット利用が行われている。スマートフォンは通信環境によりその能力を発揮するが、我が国は3G回線普及率が世界的に比較しても非常に高く、WiMAX[4]等のBWA[5]やLTE[6]等のより高速の通信回線の提供も開始されており、スマートフォンがモバイル接続環境の高度化の恩恵を受ける環境がある。

【図表1-2：スマートフォン国内出荷台数の推移・予測】

携帯電話端末の国内における年間出荷台数のうち、スマートフォンの占める比率が急速に上昇を続けており、2012年度には70%近くまで達するとの見通しもある。



（単位：万台）

	2008年度	2009年度	2010年度	2011年度	2012年度	2013年度	2014年度	2015年度	2016年度
総出荷台数	3,589	3,444	3,764	4,274	4,060	4,100	4,210	4,095	4,265
うちスマートフォン出荷台数	110	234	855	2,417	2,790	3,080	3,340	3,355	3,555
スマートフォン比率	3.1%	6.8%	22.7%	56.6%	68.7%	75.1%	79.3%	81.9%	83.4%

※ 株式会社MM総研調べ（11年度以降は予測値）（「スマートフォン市場規模の推移・予測（11年7月）」（2011年7月7日）及び「2011年度上期国内携帯電話端末出荷概況」（2011年10月27日））：いずれも国内メーカー製品・海外メーカー製品を含む。PHS・データ通信カード・通信モジュールは含まない。

3　スマートフォンをめぐるサービス構造

従来の携帯電話端末においては、通信事業者が端末、プラットフォーム[7]及びコンテンツ・アプリケーションの各々に影響力を有するいわゆる垂直統合モデルのサービス提供構

---

3 総務省通信利用動向調査(2012 年 5 月 30 日発表)。
http://www.soumu.go.jp/johotsusintokei/statistics/data/120530_1.pdf

4 Worldwide Interoperability for Microwave Access の略。ワイヤレスブロードバンド通信規格の一つ。

5 Broadband Wireless Access の略。IEEE(米国電気電子学会)で承認された、固定無線通信の標準規格（IEEE802.16 規格）。この規格に変更を加えたものが、WiMAX となる。

6 Long Term Evolution の略。携帯電話の通信規格で、第 3 世代（3G）と第 4 世代（4G）の間に位置する規格。

7 アプリケーションソフトを動作させる際の基盤となるオペレーションシステム（OS）の種類や環境、設定などをいうが、広義には、コンテンツやアプリケーションなどの利用を可能とする「場」のことをいう。

造があり、利用者に対して通信事業者がワンストップにサービスを提供する傾向にあった。

一方、日本国内市場において2008年（平成20年）7月にiPhone[8]が2009年（平成21年）7月にアンドロイド[9]OS搭載端末が発売され、その後急速に普及しつつあるスマートフォンにおいては、水平分業モデルのサービス構造がある[10]。様々な事業者が特定のレイヤー又は複数のレイヤーに係る事業を展開しており、マルチステークホルダーの下で利用者にサービスが提供されている。

この中で、プラットフォームレイヤーにおいてスマートフォンに搭載されるオペレーティングシステム（OS）[11]を提供する者は、コンテンツやアプリケーション提供サイトの運営[12]も行っており、端末開発、通信ネットワーク利用、アプリケーション提供、課金や認証等の各レイヤー[13]に影響力を有する存在であるといえる。

また、コンテンツサービスレイヤーにおいては、100万以上[14]のアプリケーションが提供されているといわれており、アプリケーションを自由にインストールして利用することが一般的であるスマートフォンの特性を踏まえ、多種多様なアプリケーションが様々な開発者等によって提供されている。

アンドロイド搭載端末に対するアプリケーション提供サイトとしては、移動体通信事業者等が提供するアプリ提供サイトも存在する。さらに、大手SNS提供事業者等インターネットにおけるプラットフォーム提供事業者[15]がインターネットと親和性の高いスマートフォンにおいてもマーケットを運用しビジネス展開を推進していくことが予想される。

スマートフォンのアプリケーションの中には、無料又は低額の一回払いの料金で利用可能となるものも多くある。このようなサービス構造において、広告配信による収益化を図る場合もあり、さらには広告配信事業者が提供する情報収集モジュール[16]を組み込むことにより、アプリケーション開発者が一定の対価を得る事例もあると指摘される。

---

8 アップル社が販売するスマートフォン。搭載する OS はアップルが開発した iOS。

9 グーグル社が開発した OS。国内外の多くのメーカーがアンドロイド OS を用いたスマートフォンを発表している。

10 第 1 回会合資料 3「スマートフォンにおける利用者情報の取扱いに関する考察」（北構成員）。

11 コンピュータシステム全体を管理するソフトウェアで、多くのアプリケーションソフトから共通して利用される基本的な機能を提供する。一般的に「基本ソフトウェア」と呼ばれている。

12 アップル社は iOS を提供し App　Store を運用。グーグル社はアンドロイドを提供し、Google Play を運用。マイクロソフト社はウィンドウズフォン（Windows Phone）を提供し Windows Phone Marketplace を運用。

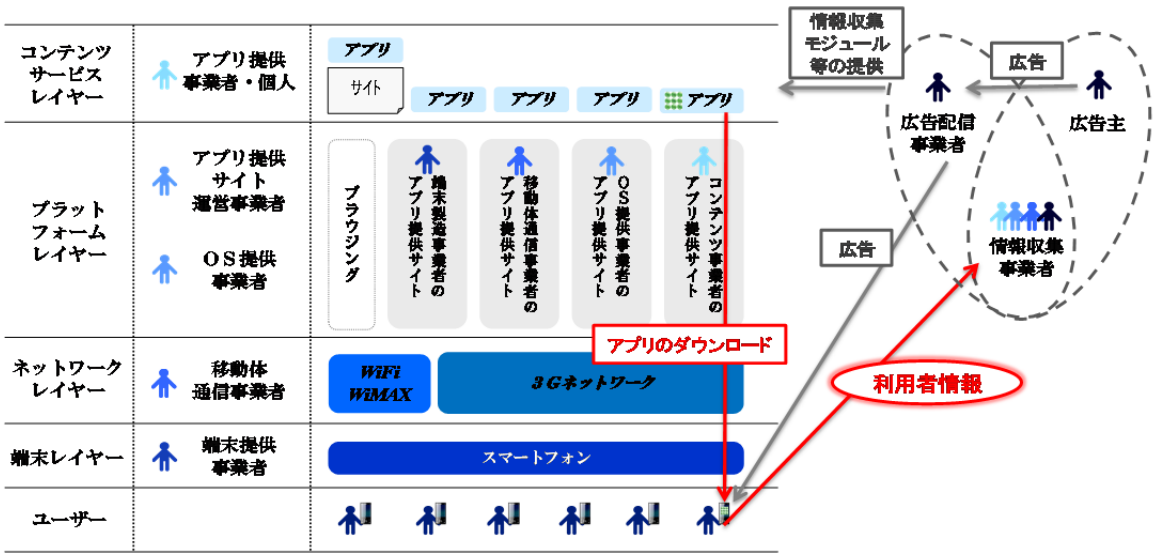
13 構造や設計などが階層状になっているとき、その一つ一つの「階層」（レイヤー）のことをいう。

14 App Store58 万 5 千（2012 年（平成 24 年）3 月 7 日発表）、Google Play45 万以上(2012 年（平成 24 年）3 月 7 日 Android Market から Google Play 移行時)、Windows　Phone　Marketplace 約 6 万 4 千以上（2012 年（平成 24 年）3 月）。

15 例えば、Facebook、Twitter、GREE、DeNA などが事例として挙げられる（第 1 回会合 北構成員資料）。

16 スマートフォン等に蓄積された様々な情報を収集する機能を持つ、一連のプログラムのこと。

【図表1-3：スマートフォンをめぐるサービス構造】



スマートフォンを経由した利用者情報の取扱いについては、このようなサービス構造について考慮した上で検討を進めていくことが必要である。

第２章　スマートフォンにおける利用者情報の現状

１　スマートフォンにおける利用者情報の種類と性質

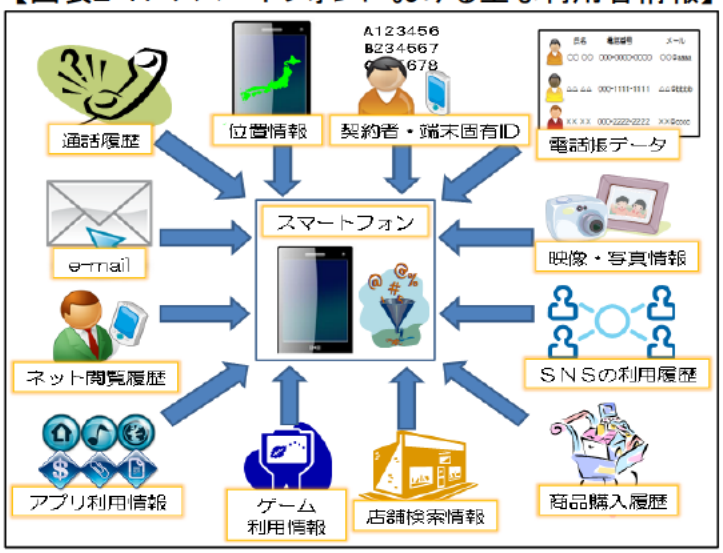
常に電源を入れてネットワークに接続した状態で持ち歩くスマートフォンは、PC に比べて利用者との結びつきが強く、利用者の行動履歴や通信履歴等の多数の情報の取得・蓄積が可能である。

利用者の識別に係る情報としては、契約者固有ID（OSが生成するID（Android　ID）、独自端末識別番号（UDID）、加入者識別ID（IMSI）、端末識別ID（IMEI）、MACアドレス等）が挙げられる[1]。これらのIDは利用者側で変更できない固有値である。また、従来のPCブラウザと同様にクッキー技術[2]を用いて生成された識別情報もこの区分に含まれる。

また、第三者の情報としては、スマートフォンが電話や通信端末として利用されることによる電話番号や電話帳データ（主に第三者の氏名、電話番号、メールアドレス）が挙げられる。

さらに、通信サービス上の行動履歴や利用者の状態に関する情報として、GPS機器等が標準的に搭載されていることから精度の高い位置情報が存在し、通話履歴（通話内容・履歴、メール内容・送受信内容等）、ウェブページ上の行動履歴等も存在する。加えて、解像度の高いカメラにより撮影される写真やビデオ、アプリケーションの利用により蓄積される情報やアプリケーションの利用ログ[3]、システムの利用に関するログ等もこの区分に該当する。

【図表2-1：スマートフォンにおける主な利用者情報】



1 これとともに、契約者情報（氏名、住所、生年月日、性別、年齢、電話番号、決済関係情報（クレジットカード番号等））について事業者側で有している場合がある。

2 ウェブサイトの提供者が、ウェブブラウザを通じて訪問者の PC 等に一時的にデータを書き込んで保存させる仕組みで、利用者に関する情報や最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができることから、認証など利用者の識別に使われる。

3 アプリケーションにおける個人の医療・健康・生活状況・金融関係の情報、スケジュール情報、SNS 等による交流状況、本・雑誌・音楽やニュースなどの閲覧履歴などの情報については個人情報及びプライバシーの両面から考慮する必要がある。

【図表2-2：スマートフォンにおける利用者情報の例】

区分	情報の種類	含まれる情報
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じ一時的にPCに書込み記載されたデータ（ウェブサイト訪問回数・サイト内履歴等）。
	契約者・端末固有ID	OSが生成するID（Android ID）、独自端末識別番号（UDID）、加入者識別ID（IMSI）、端末識別ID（IMEI）、MACアドレス等
第三者の情報	電話帳で管理されるデータ	氏名、電話番号、メールアドレス等
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォン等で撮影された[4]写真、動画

２　スマートフォンにおける利用者情報の取得

（１）OSによる利用者情報へのアクセス制限

スマートフォンにおける利用者情報へのアクセスについては、各OSにより異なる制限が行われている。また、アプリケーション提供サイト運営事業者により、掲載するアプリケーションについて、一定の審査やポリシーが存在している。一方、アプリケーションが利用者情報を収集するためのプログラムインターフェース（API[5]）があらかじめ決まっており、APIを用いた情報収集は比較的容易である。また、収集した情報を含めネ

[4] スマートフォンで撮影された写真の場合、設定により位置情報を含む場合もある。また、解像度の高い画像は、個人識別性を有する可能性があるとの指摘がある。

[5] Application Program Interface の略。プラットフォーム向けのソフトウェアを開発する際に使用できる命令や関数の集合。また、それらを利用するためのプログラム上の手続を定めた規約の集合。開発者は規約に従ってその機能を「呼び出す」ことで、自らプログラミングせずにその機能を利用したソフトウェア作成が可能となる。

ットワークに常時接続されるため、クラウドベースの外部サーバーと連携したサービス構築が容易である[6]。

① iOS

アップル社が提供するiOSの場合、アプリケーションが取得しようとする利用者情報についてOSによる一般利用者への情報提供や利用許諾（パーミッション）の取得（権限確認）は行われていない。ただし、アップル社によるアプリケーションの事前審査が行われるとともに、アプリケーション側で例えば位置情報を用いる場合にはポップアップにより個別に利用者の承認がとられている。

【図表2-3： iOSによる利用許諾画面】

（※App storeから入手したアプリをもとに総務省作成）

② アンドロイド

グーグル社が提供するアンドロイドの場合には、利用者がGoogle Play[7]等からアプリケーションをダウンロードする際に、アプリケーションが取得しようとする利用者情報等に関する利用許諾の確認画面が一覧的に表示され、利用者がこれに包括的に「同意」して初めてダウンロードすることが可能となっている。この利用許諾については、OSとして利用者情報へのアクセスにつき、利用者へ情報提供をする観点から、一定の透明性が確保されている。ただし、①取得する利用者情報の詳細項目、②利用目的・利用形態[8]・利用主体、③第三者提供の有無等については、アプリ開発者からの

6 スマートフォンのアプリケーションは、一般の PC ソフトよりも機能制限されているが、従来の携帯電話のアプリケーションと比べると任意のサイトとの通信や電話帳へのアクセスなどができることが多い（第３回会合資料２「情報取得手段ごとに相当な同意確認基準の提案」産業技術総合研究所 高木浩光氏）。

7 平成 24 年 3 月 7 日 Android Market、Google Music、Google eBookstore を統合してサービス開始。

8 情報の使用と情報の外部送信は別の同意であるが、技術的に OS の利用許諾は、端末内で情報を使用す

追加的記述がない限り表示されない[9]。アプリ開発者はグーグル社との契約に基づき、利用者情報についても適切な取扱いを行うこととされている。

【図表2-4：アンドロイドによる利用許諾画面[10]】

（※Google Playから入手したアプリをもとに総務省作成）

③ ウィンドウズフォン

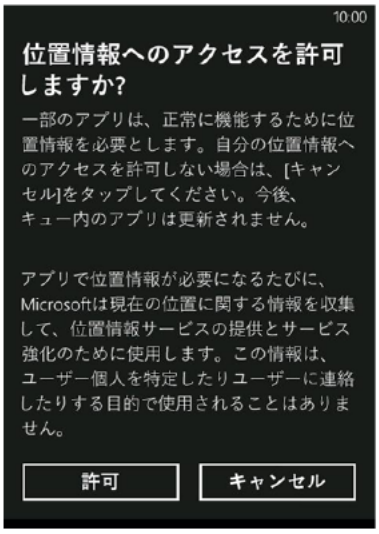
マイクロソフト社が提供するウィンドウズフォンの場合、アプリからは限定された利用者情報のみにアクセス可能とされており、位置情報、端末情報等にアクセスしようとする場合には、個別の利用者の許可を事前に得た場合のみ可能とされている。

ることと当該情報を外部に送信することについて区別して許可することができないという限界がある。（第３回会合　高木氏資料）。

9 Google Play において３段階の構造により利用者情報を守るように意図されている。①パーミッションにより特定の情報へのアクセスについて包括的に同意を得る OS の機構、②アプリケーション開発者とマーケット運営者の間で締結する規約（Developer Distribution Agreement）（利用者情報を利用する際に事前の許諾を取得するようアプリを作成し、利用者が意図しない情報使用を禁止）、③アプリケーション開発者に対して勧めている望ましい方法（例：自由記述欄に利用者情報の利用目的を記載）。

10 アンドロイドによる利用許諾画面において、電話／通話、電話帳へのアクセス、ネットワーク通信、現在地などアプリケーションが利用する権限の一覧が表示され、利用者は一括して同意しダウンロードするか否かを判断する。

【図表2-5：ウィンドウズフォンにおける利用許諾画面】



【図表2-6：アプリケーション提供サイトの主な事例（OSベンダー）】

	App Store	Google Play[11]	Windows Phone Marketplace
運営母体	Apple Inc.	Google Inc.	Microsoft Corporation
アプリケーション提供対象	iOS搭載端末	アンドロイド搭載端末	Windows Phone 7以降搭載端末
アプリケーション数	58万5千 (2012年3月7日)	45万以上 (2012年3月7日)	約64,000以上 （2012年2月27日）
アプリケーション掲載に係る審査、ポリシー	**アップル社による事前審査** ユーザーの事前の許可を得ずデータがどこでどのように使用されるかの情報を提供せずに、アプリケーションはユーザーに関する情報を送信してはならない。	**アプリケーション開発者と締結する契約（Developer Distribution Agreement）とアプリケーション掲載者の自己審査** アプリケーション開発者はユーザーのプライバシーと法的権利を守ることに同意する（法的に適切な通知と保護を行う必要）。	**マイクロソフト社による事前審査** アプリケーションが取得できる情報が限定されている上、使用目的、送信するデータの内容について事前にユーザーに許可を得る必要がある。
アプリケーションを導入できるマーケット	App Storeのみ	デフォルトはGoogle Play ただし移動体通信事業者の判断によるカスタマイズが可能。	Windows Phone Marketplaceのみ

11 2012 年（平成 24 年）3 月 7 日より名称変更。

【図表2-7：アプリケーション提供サイトの主な事例（国内）】

	dメニュー、dマーケット（spモード）	au Market[12]	@アプリ
運営母体	NTTドコモ	KDDI	ソフトバンクモバイル
アプリケーション提供対象	NTTドコモスマートフォン（アンドロイドOS搭載端末）	au Androidスマートフォン（アンドロイドOS搭載端末）	ソフトバンクスマートフォン（アンドロイドOS搭載端末）
アプリケーション数	約1,000アプリ（dマーケット掲載数、2012年3月末現在）	約8,800アプリ（2011年12月末現在）	約1,800アプリ（2012年2月末時点）
アプリケーション掲載に係る審査、ポリシー	**NTTドコモによる事前審査** ・dメニュー：日本国内法人提供のアプリケーションのみ掲載（個人は不可）。 ※掲載基準：http://newsp.nttdocomo.co.jp/ ・dマーケット（アプリ＆レビュー）：海外法人提供を含むアプリケーションを紹介。	**KDDIによる事前審査** KDDIの指定する事項を届出、同社の承諾を得る。変更しようとする場合も同様。（第三者の財産、プライバシー等個人の権利を侵害し又はそのおそれのあるもの、マルウェア又はそのおそれのあるもの等は掲載不可）	**ソフトバンクモバイルによる事前審査** ・Google Play内のアプリケーションを紹介するサービス ・キャリア課金が利用可能な有料アプリに関して独自ガイドラインに基づきパトロール（事後審査）を実施。

（２）アプリケーションによる情報収集事例

スマートフォンの普及が急速に進んだ昨年（2011年（平成23年））夏頃から、利用者情報の取扱いに関する事例が多く報道され、我が国においても利用者の関心が高まってきている。

昨年夏以降の報道事例としては、例えば下記のようなものがある。

- GPS等によるスマートフォンの位置情報等を、利用者（端末所有者以外の第三者を含む）がPCサイトにログインすることによりリアルタイムに把握できるサービスを提供するアプリ[13]
- スマートフォンにインストールされたアプリケーション並びに起動されたアプリケーションの情報及び契約者固有ID等を、利用者の同意を取得する前に外部へ送信していたコンテンツ視聴用アプリ[14]
- GPS等によるスマートフォンの位置情報等を、組み込まれた情報収集モジュールが海外の広告会社に送信していた無料ゲームアプリ[15]

12 2012年（平成24年）3月1日より名称変更。

13 「カレログ」（2011年9月7日付産経新聞1面、他）。現在は、利用者の同意取得の方法や収集する情報に改良を加え、「カレログ２」としてサービス提供中。

14 「アップティーピー」（2011年10月11日付読売新聞夕刊15面）。提供事業者であるミログ社は、「同意を得ていない段階で情報を収集・送信している重大な瑕疵が発見された」とし、2012年3月30日付でサービス終了。

15 2011年11月28日付読売新聞夕刊17面。指摘されたゲームアプリは、金魚すくいゲーム。

・ 閲覧履歴及び契約者固有ID等を、利用者に十分説明しないまま取得し、外部に送信していた雑誌や新聞等の閲覧アプリ[16]
・ 動画を再生するアプリケーションにみせかけ、端末のメールアドレス、電話番号等を取得し料金請求画面を出すワンクリック詐欺的アプリ[17]
・ 人気のアプリを動画で紹介するように見せかけ、端末内の電話帳に登録された名前、電話番号、メールアドレス等の情報を外部サーバーに送信していたアプリ[18]

（３）アプリケーションによる情報収集の実態

KDDI研究所[19]によれば、2011年（平成23年）8月に収集したアンドロイド上で動作する980個のアプリケーションの利用許諾について分析を行った結果、558（56.9%）のアプリケーションに合計1,065の情報収集モジュールが存在していたとされる。

また、利用許諾の内容については、端末ID等を取得可能とする電話／通話の利用許諾は57.9%、GPSを用いた位置情報の利用許諾は26.4%に存在していた。さらに、980個のうち400個のアプリケーションについて、2011年12月から2012年1月の間に5分間の挙動解析を行い、外部への送信情報を確認した結果、Android ID の送信が12.5%、端末ID（IMEI）の送信が14.3%、位置（緯度・経度）の外部送信が8.0%であったとされる。

---

16 「ビューン」、iPhone 用のアプリケーション「マガストア」及び「産経新聞」（2012 年 1 月 31 日付読売新聞夕刊 13 面）。「ビューン」は、同年 1 月 20 日、閲覧履歴情報および端末識別情報の取得について利用規約に明記するとともに、同年 4 月中に当該情報の収集について個別の同意を取る措置の実施、端末識別を目的とした独自 ID を導入した。「マガストア」は同年 1 月 13 日、利用規約に閲覧情報を収集することを明記するとともに、収集データと端末 ID との紐付けを防止する措置を実施し、同年 2 月 27 日には同意した利用者の情報のみ収集するよう措置した。「産経新聞」は、開発中に試験的に組み込んだ機能について、情報の利用・蓄積はしていないとしつつ、同年 1 月 31 日付で同機能を削除した。

17 「ANDROIDOS_FAKETIMER(フェイクタイマー)」（2012 年 2 月 2 日付日刊工業新聞 9 面）。スマホアプリケーションを装い「ワンクリック詐欺」を行うウイルスとされ、トレンドマイクロ株式会社がインターネット脅威マンスリーレポート(2012 年 1 月度)において発表。同社によれば「スマートフォンの電話番号を攻撃者に送信するように作成されているため、攻撃者から直接電話がかかってくることも否定できません」とされている。
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20120206035719.html
実際に事業者から料金請求のメールが届いた事例や、電話番号や現在位置情報が表示されたため利用者が不安に思った事例などが東京都消費生活センターへの相談事例として複数公表されている。
http://www.shouhiseikatu.metro.tokyo.jp/sodan/kinkyu/120323.html

18 人気ゲーム名等などのタイトル名に「the Movie」を付けた動画系の複数のアプリ。いずれも無料動画を楽しめると称している。アプリをインストールしようとすると、「ネットワーク通信」「個人情報」「電話／通話」の利用許諾を要求し、利用者が許諾してアプリをダウンロードしインストールすると、攻撃者が用意するサーバーに接続し電話帳の情報を送信していたとされる。(2012 年 4 月 13 日 NHK ニュース「スマホアプリ情報大量漏洩か」、2012 年 4 月 14 日付読売新聞 35 面他)。
シマンテックによれば、個人情報を盗む悪質な Android アプリは 29 種類、潜在的なインストール数は 30 万件で、数百万人分の個人情報が盗まれたおそれがあるとしている。
（http://www.symantec.com/connect/blogs/android-movie　2012 年 4 月 16 日）
警視庁は不正指令電磁的記録（ウイルス）供用容疑で捜査中（2012 年 5 月現在)。

19 第 1 回会合資料 4「スマートフォンからの利用者情報の送信～情報収集の実態調査～」（KDDI 研究所 研究主査 竹森敬祐氏)。

一方、何らかの形でIDあるいは位置情報を送付していた181のアプリケーションのうち、14件（7.7%）にはアンドロイドによる利用許諾とは別に、アプリケーションによる説明があり、10件（5.5%）は許諾を取得していたが、それ以外の167(92.3%)のアプリケーションについてはアンドロイドによる利用許諾以外の説明はアプリケーション内において表示されなかったとしている[20]。

３　スマートフォンにおける利用者情報の収集目的と活用状況

スマートフォンによる利用者情報の収集目的は、一般にサービスの提供・向上や利用者の趣向に応じた広告の表示等とされているが、介在するそれぞれの関係者において、実際にどのように活用されているかは、必ずしも明確ではない。

アプリケーションによる利用者情報の活用方法については、大きく分けて①～④のようなものが現時点で想定される。

① アプリケーションがそれ自体のサービス提供のために用いる場合（利用者が情報を入力等しなくとも既存の情報を活用してすぐに利便性の高いサービスを利用することが可能となる場合も多い）

② アプリケーション提供者が、アプリケーションの利用状況等を把握することにより、今後のサービス開発や市場調査のために用いる場合

③ スマートフォンの位置情報あるいは契約者固有ID等の利用者情報を情報収集事業者等が取得し、広告サービス等に活用する場合又はその他の市場調査等の情報分析等に活用する場合

④ 現段階では目的が明確ではないが、将来的な利用可能性等を見込んで、利用者情報を取得する場合

スマートフォンは個人との結びつきが強いためターゲティング型のサービスをより有効に提供しやすいとの指摘がある。5頁に示したサービス構造にあるように、スマートフォンのアプリケーションの中には、無料又は低額の一回払いの料金で利用可能となるものも多くあり、広告等を活用した収益モデルを志向する開発者も多く存在するとされる。

このようなビジネスモデルを背景として、情報収集モジュールを組み込むことにより、アプリケーション開発者が情報収集事業者等から一定の対価を得ている事例も多く見られると指摘されている。

４　アプリケーションの利用に関する利用者の意識

（１） アプリケーション利用に関する不安等

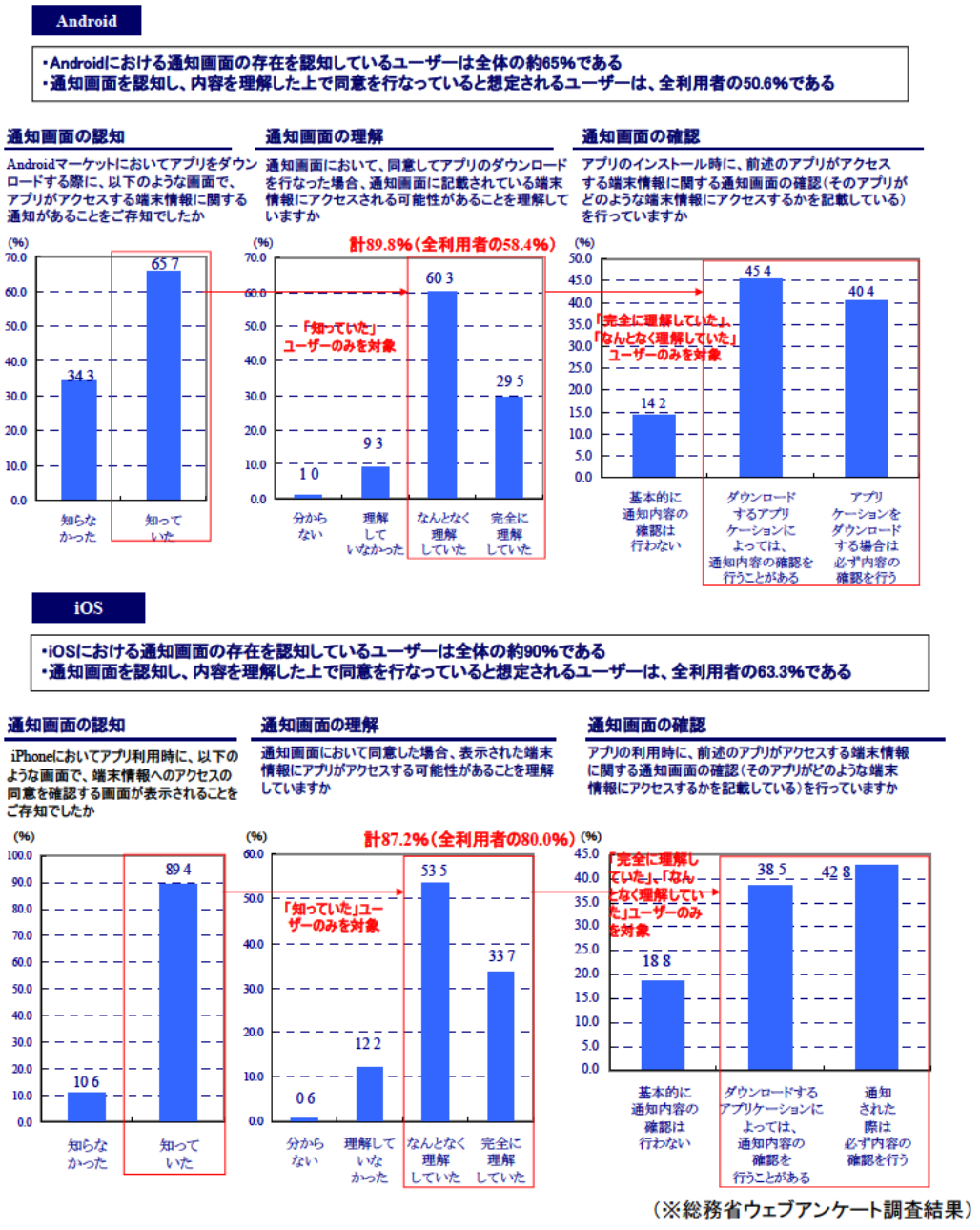
2012年（平成24年）2月に総務省が行ったウェブアンケート調査[21]によれば、通知・

[20] ウェブサイトのみにプライバシーポリシーを示していたアプリケーションはカウントしていない。

[21] 総務省ウェブアンケート調査（2012 年 2 月実施）：有効回答数 1,576 人、スマートフォン利用者を対象 OS、年代・性別に従って抽出（協力：株式会社日本総合研究所、NTT レゾナント株式会社）。

同意画面を一定程度理解し確認している利用者は5～6割程度いるが（図表2-8参照）、８割のユーザーは通知・同意画面に何らかの不満・不安を有している（図表2-9、2-10参照。同意しないとアプリケーションが利用できない（約40%）、同意・許可した後にどのようなことが起こるか分からない（約36%）等）。また、アプリケーションの機能に必要な場合以外にも利用者情報を外部送信することについては、23%の利用者は情報送信されたくないとし、半数以上の利用者は利用目的や情報提供先の開示を希望している（図表2-10参照）。

【図表2-8：通知画面の認知・理解・確認（アンドロイドOS端末、iPhone利用者）】

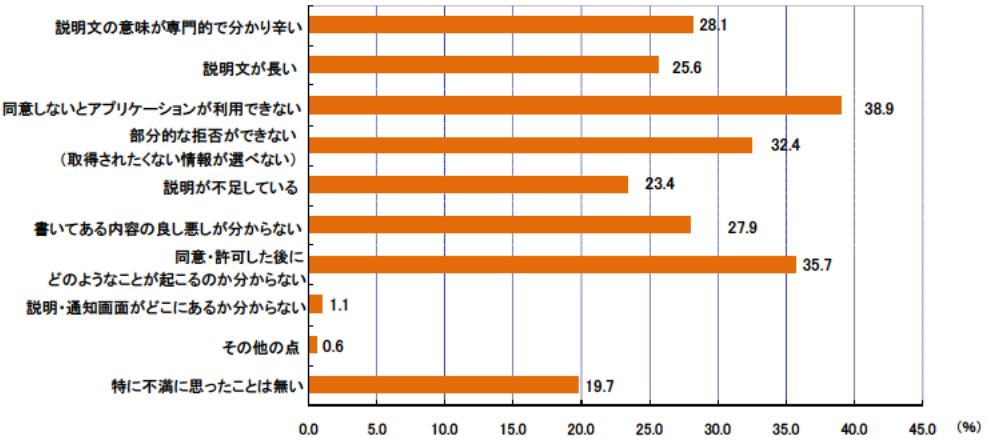


（※総務省ウェブアンケート調査結果）

【図表2-9：アプリケーションの通知・同意画面に対する不満】

・通知・同意画面に対する不満として「同意しないとアプリケーションが利用できない」と回答したユーザーは 全体の約40%と最も多い
・次いで、「同意・許可した後にどのようなことが起こるか分からない」と回答したユーザーは35.7％である

アプリケーションの通知・同意画面に対する不満
アプリケーションが端末情報へアクセスすることの通知・同意画面に関して不満・不安に思ったことはありますか（複数回答）

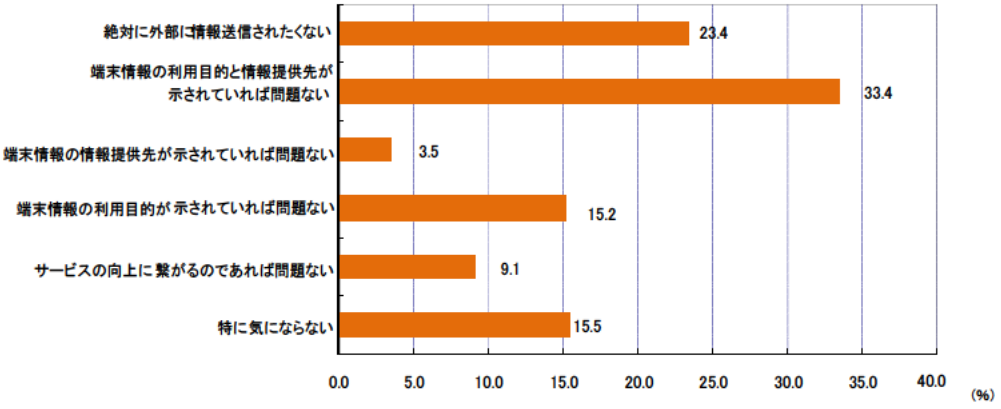


（注）平成24年2月総務省調査（有効回答数：1,576人、スマートフォン利用者を対象OS、年代・性別に従って抽出。
協力：株式会社日本総合研究所、NTTレゾナント株式会社）

【図表2-10：端末情報の外部送信に対するユーザーの認識】

・端末情報の利用目的と情報提供先が示されていれば、端末情報の外部送信について問題ないと考えるユーザーは、全体の約33%である

端末情報の外部送信に対するユーザーの認識
インストールしたアプリケーションがあなたのスマートフォンの端末情報を外部に送信することをどう思いますか
（ただし、アプリケーションの機能上必要な場合を除きます）

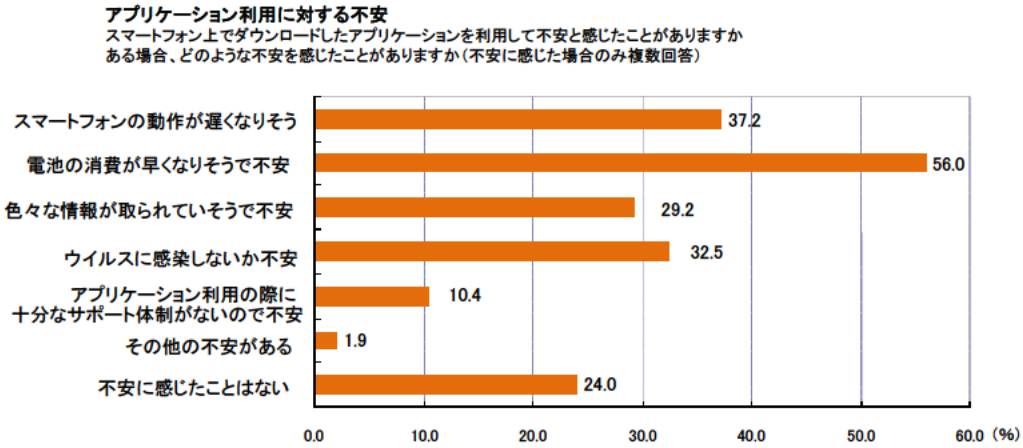


（※総務省ウェブアンケート調査結果）

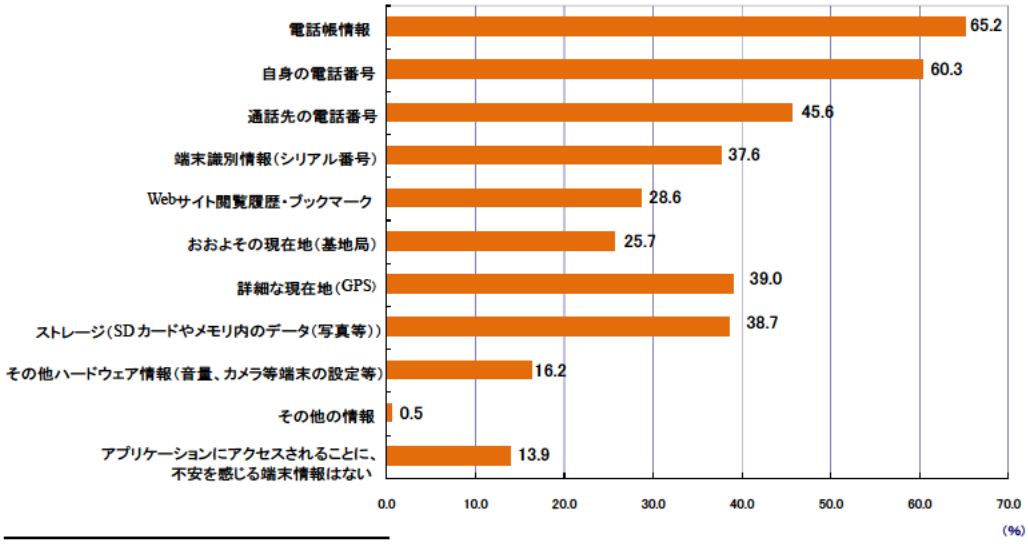
なお、アプリケーション利用に対する不安として、「色々な情報を取られていそうで不安」とする利用者は約３割程度おり（図表2-11参照）、電話帳情報について約６５％の利用者がアクセスされることに不安を感じるとしている（図表2-12参照）。アプリケーションによるトラブルについては約７割の利用者が経験していない[22]（図表2-13参照）が、アプリケーションによるトラブルに対して行ってほしい対応として総合的に問合せができる窓口の設置を約５割の利用者が望んでおり、自身の提供していた個人情報の削除を約４割の利用者が望んでいると回答している（図表2-14参照）。

【図表2-11：アプリケーション利用に関する不安】

・76 %のユーザーがアプリケーションの利用に関して何らかの不安を感じている
・不安を感じる主な理由は、「電池の消費速度への影響」、「端末動作速度への影響」といった端末の性能に係わるものが多い
・ユーザー情報を取得されることやウィルスへの感染に対して不安を感じるユーザーは、約3割である

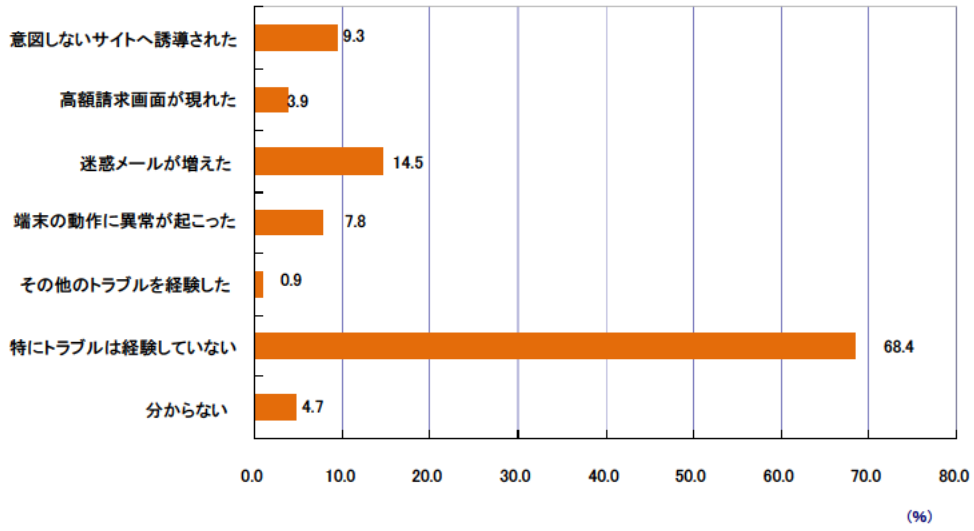


【図表2-12：ユーザーがアクセスされることにより不安を感じる利用者情報】

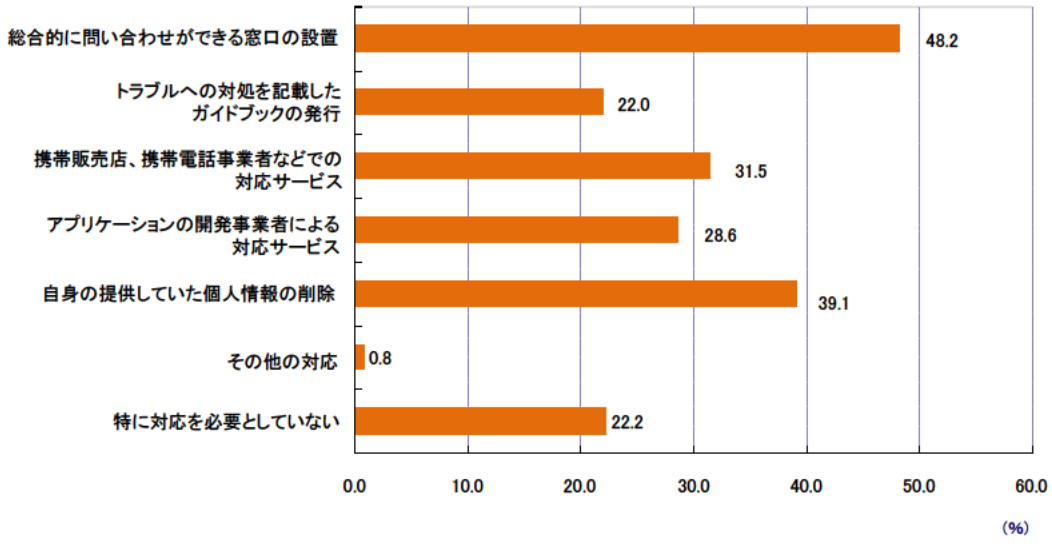


22 アンケートによれば、アプリケーションによるトラブルがあった利用者は約３割であり、迷惑メールの増加（約 15%）、意図しないサイトへの誘導（約 10%）、端末の異常動作（約 8%）、高額請求画面（約 4%）等の回答があった。

【図表2-13：アプリケーションによるトラブル経験】



【図表2-14：ユーザーの期待するトラブルへの対応】



（※総務省ウェブアンケート調査結果）

（２） アクセスされる利用者情報の意識

総務省のウェブアンケート結果によれば、アプリケーションがスマートフォンにおける利用者情報にアクセスする可能性があることを認知している利用者は全体の約8割弱であり、利用者が各分野のアプリケーションにアクセスされていると想定する利用者情報は、図表1-15のとおりであった。

例えば、通信系アプリケーションは電話帳情報にアクセスしている可能性があることを5割弱のユーザーが認識し、地図系、天気系又は交通系アプリケーションが位置情報にアクセスしている可能性があることを約4割の利用者が認識している。一方、ゲーム系やニュース系についてはどのような端末情報にもアクセスされているとは思わな

いと約4割の利用者が認識しており、利用者意識が実態と乖離している可能性もある。

【図表2-15：各アプリケーションがアクセスしている情報に関する利用者の意識】

	アクセスされていると想定する利用者情報（回答%）			
通信系アプリ	自分の電話番号（49.2%）	電話帳情報（47.3%）	端末ID（37.6%）	端末情報へのアクセスはない（20.9%）
SNS系	端末ID（32.2%）	おおよその現在地（基地局）（31.7%）	端末情報へのアクセスはない（27.1%）	詳細な所在地（GPS）/通話先の電話番号：（24.6%）
ゲーム系	端末情報へのアクセスはない（37.0%）	端末識別番号（31.0%）	おおよその現在地（基地局）（22.1%）	詳細な所在地（GPS）（15.1%）
ニュース系	端末情報へのアクセスはない（39.9%）	おおよその現在地（基地局）（27.4%）	端末識別番号（20.9%）	詳細な現在地（GPS）（18.7%）
天気系	おおよその現在地（基地局）（41.3%）	詳細な現在地（36.3%）	端末情報へのアクセスはない（29.2%）	端末識別番号（シリアル番号）（19.5%）
地図系	おおよその現在地（基地局）（49.4%）	詳細な現在地（44.2%）	端末情報へのアクセスはない（25.1%）	端末識別番号（シリアル番号）（20.4%）
交通系	おおよその現在地（基地局）（42.4%）	詳細な現在地（40.8%）	端末情報へのアクセスはない（27.7%）	端末識別番号（シリアル番号）（19.5%）

（※総務省ウェブアンケート調査結果）

５　諸外国の状況

（１）アプリケーションに関する事例

① ウォール・ストリート・ジャーナルによるアプリケーション調査

アプリケーションによる情報収集の問題が報道された事例として、2010年（平成22年）12月米国におけるウォール・ストリート・ジャーナル社がiPhone及びアンドロイド搭載端末向けの人気のあるアプリケーションをそれぞれ50本ずつ選び、同社提供のiPhone向けアプリケーションとともにアプリケーションが外部へ送信する情報等を解読・調査した結果を掲載した記事が発表されている[23]。

[23] 『Your Apps Are Watching You: A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone』(2010 年 12 月 20 日)。調査会社は Electric　Alchemy　Limited で、アプリケーションの選定は 2010 年 10 月中旬に実施され、スマートフォン端末は iPhone3G 及び Samsung Captiva を使用。

記事によれば、調査を行った101本のアプリケーションのうち、56本が端末固有のIDをユーザーの同意なく外部に送信し、47本のアプリケーションが端末の位置情報を、5本のアプリが年齢・性別等の情報を外部に送信していたとされる。さらに、45本のアプリケーションは調査時点において、アプリケーション内及びウェブサイト上のいずれにもプライバシーポリシーを示していなかった[24]。

② Pandora Media（インターネットラジオ視聴アプリ）

2011年（平成23年）4月には、インターネットラジオ視聴アプリ「Pandora Media」が複数の広告会社へユーザー情報を送信していたことについて連邦大陪審が召喚状を発していたことが、同社が証券取引委員会（SEC）へ提出した書類において明らかになった。

③ Path（SNSアプリ）

2012年（平成24年）2月には、SNSアプリである「Path」が利用者のスマートフォン内の電話帳情報等を利用者の同意を得ないままPathサーバーに送信していたことが指摘され、Path社はこれを認め謝罪するとともに今まで収集した連絡先データを全て削除し、今後はオプトイン[25]機能を付けるようにアップデートした[26]。

④ ケンブリッジ大学コンピュータ研究所等による研究

ケンブリッジ大学のコンピュータ研究所等が発表した研究成果[27]によれば、アンドロイドマーケット（当時）におけるアプリケーションを分析[28]したところ73%が無料であり、無料アプリはより多くダウンロードされる傾向にある（1万件以上ダウンロードされたアプリケーションは有料アプリの中の0.2%のみであったが、無料アプリの中の

---

24 なお、端末固有 ID、位置情報等の情報送信先は、グーグル社（Admob, AdSense, Analytics 等）、アップル社（iAD 等）が多かったとされるが、中には 6～7 か所にこれら情報を送信している無料ゲームアプリ等も存在した。

25 事前に同意を取得するということ。例えば、特定電子メールの送信の適正化等に関する法律（平成 14 年 4 月法律第 26 号）において、広告又は宣伝を行うためのメールについては、事前に同意した者に対してのみ送信することが可能と定められている。

26 米国下院エネルギー商業委員会議長 Henry　A. Waxman 議員及び商業製造貿易小委員会議長 G.K.Butterfield 議員は「アップル社の iOS アプリケーション開発者に対するポリシーは i Phone ユーザーとその連絡先情報に対する保護という点において不十分なのではないかという疑問が生じる」等と記した書簡をアップル社の CEO 宛てに送付し、アップル社はこれに対し、アプリケーションがユーザーの連絡先データを許可なく収集することは同社の規定に違反しているとし、今後連絡先データへアクセスするアプリケーションについて、GPS 位置情報へアクセスするアプリケーションと同様に、個別に明確なユーザーの承認を必要とする方向で見直しを検討する予定であると述べている 。

27 『Don't kill my ads! Balancing Privacy in an Ad-Supported Mobile Application Market』Ilias Leontiadis, Christos Efstratiou, Marco Picone, Cecilia Mascolo, Computer Laboratory, University of Cambridge, Cambridge, UK, Department of　Information Engineering, University of Parma, Italy. http://www.cl.cam.ac.uk/~il235/HotMobile12_Leontiadis.pdf

28 2011 年 7 月から 6 週間かけてアンドロイドマーケットの全てのアプリケーションを Java ベースのクローラーにより調査し、251,342 のアプリケーションのメタデータ（アプリケーションの名前、種類・カテゴリー、ダウンロード数、評価、パーミッション）を分析したとしている。

20%であった）。また、人気のある無料アプリの約80%がターゲット広告を行っていた。

同研究成果によれば、無料アプリは有料アプリに比べて、注意を要する利用許諾を要求する割合が高いとされる。また、同じカテゴリーに属するアプリケーションで比較すると、無料のものは有料のものよりも要求する利用許諾の数が多い傾向にある（例：例えば漫画、カードゲーム、パズル等のカテゴリーで無料版は有料版より要求する利用許諾が多い）。背景として、注意を要する利用許諾に分類される①インターネットアクセス、②利用者の位置情報、③電話／通話の3つの利用許諾をアドネットワーク[29]が求める場合が多いことを指摘している。

アンドロイドマーケット（当時）はダウンロード時に注意を要する利用許諾については特に注意喚起をしているが、この注意喚起はユーザーの行動に大きな影響を与えてはいないことが指摘されている。

無料の広告に支えられたアプリケーションというビジネスモデルに対応し、開発者が収入を得る必要性とユーザーのプライバシーを守る必要性のバランスをとるための新しいアプローチの必要性を提唱している。

（２）その他の事例

① OSによる位置情報収集について

2011年（平成23年）4月に利用者が位置情報サービスをオフに設定したときもiPhoneの位置情報について収集・記録[30]されていることを研究者等が指摘したことを契機に、米国下院エネルギー・商業委員会通信・テクノロジー小委員会メンバーのエドワード・マーキー（Edward Markey）議員がアップル社のスティーブ・ジョブスCEOに対してプライバシーの観点から説明を求める書簡[31]を送付した。

5月にアップル社のiOS搭載端末やグーグル社のアンドロイド搭載端末において定期的に位置情報を収集・送信していることについて、「モバイルプライバシーの保護：あなたのスマートフォン、タブレット端末及び携帯電話とあなたのプライバシー」として米国上院司法委員会が公聴会[32]を行い、アップル社及びグーグル社の代表者等が出席している。

---

29 インターネット広告において、広告媒体のウェブサイトを多数集めてネットワーク化した「広告配信ネットワーク」を形成し、広告受注を請け負い、広告を配信するサービスのこと。中小規模の多様な広告媒体もネットワーク化し利用者の傾向を分析する行動ターゲティングが導入される場合も多い。

30 端末内のファイルに記録し長期間にわたり保存されていた。アップル社は、ソフトウェアのバグであるとして、これを解消するアップデートを行った。

31 2011 年 4 月 21 日発出されている。

32 2011年5月10日に開催された公聴会。米国上院司法委員会のウェブサイトに掲載されている。
http://www.judiciary.senate.gov/hearings/hearing.cfm?id=e655f9e2809e5476862f735da16bd1e7

② CarrierIQ

2011年（平成23年）12月には、「Carrier IQ」というスマートフォン出荷時にあらかじめ端末にインストールされていたソフトウェアが利用者情報の一部を携帯端末と携帯電話事業者のサービスの品質管理等を目的として収集していることについて、米国上院司法委員会プライバシー・テクノロジー・法律小委員会委員長（アル・フランケン（Al Franken）議員）がCarrierIQ社、AT&T社、スプリント・ネクステル社、サムスン社及びHTC社に説明を求める書簡を送付した。また、エドワード・マーキー下院議員が連邦取引委員会（FTC）に対して「CarrierIQ」に関する問題について調査を行うように求める書簡を送付し、「モバイル端末プライバシー法」を発表した。CarrierIQ社は、同年12月12日テクノロジーに関する資料を発表した[33]。

③ グーグル社による新プライバシーポリシーの導入

2012年（平成24年）1月に、同年3月1日よりグーグル全体で60以上あるプライバシーポリシーを原則１つの新プライバシーポリシーに統一するとグーグル社が発表した。これに対して、米国下院議員、米国の36の州・特別区等の司法長官、 カナダのプライバシーコミッショナーが書簡を送付し、質問を行うとともに懸念を表明した[34]。 EU個人データ保護作業部会[35]議長、フランスの情報処理及び自由に関する国会委員会（CNIL）委員長がＥＵデータ保護指令へ違反する可能性を指摘し延期を求める書簡を送付した[36]。また、日本政府も個人情報保護法上の法令遵守及び利用者に対する分かりやすい説明等の対応をすることが重要である旨を文書で通知を行い注意喚起したほか、韓国政府が個人情報保護規定遵守の観点から勧告を行い[37]、消費者による訴訟[38]も提起されるなど、世界的に様々な動きが見られた。

---

33 Carrier IQ について、日本において動作している事例は確認されていない。

34 2 月 22 日に発出された米国 36 州・特別区等の司法長官の書簡において、「国内のスマートフォン市場の 50%以上を占めるアンドロイドスマートフォン利用者にとってプライバシー侵害から逃れるのは事実上不可能ではないか」と指摘されている。また、2 月 24 日に発出されたカナダプライバシーコミッショナーの書簡において「電話や SMS 等はログインしなくても使えると説明しているが、Gmail やアンドロイドマーケット、カレンダー等はログインを必要とするため、実質的に利用者に選択権はないのではないか」、「グーグルは端末 ID の収集を行い、グーグルアカウントと結びつけることもできるのではないか」との指摘がある。

35 EU データ保護指令第 29 条に基づくデータ保護作業部会。

36 CNIL(La Commission nationale de l'informatique et des libertés)は、3月16日にGoogle社に対して６９問の詳細な質問状を送付し、2012年4月20日にグーグル社がCNILに回答した。CNILは5月23日にGoogleに追加の質問状を送付し、6月8日までの回答を求めている。

37 韓国放送通信委員会は 2012 年 2 月 28 日付でグーグルに対し、プライバシーポリシーの統合に関し、①個人情報利用目的の包括的記載及び明示上同意手続きの不備、②情報通信網法上の必須明示事項の脱落、③プライバシーポリシーを受け入れない利用者にも選択権を保障すること、についてグーグルへ勧告を行った。これに対し、グーグルが勧告事項に対する改善方策を提出したことを、放送通信委員会は同年 4 月 5 日付で明らかにしている。

38 報道によればカルフォルニア州等で新プライバシーポリシーによるプライバシー権の侵害等に係る訴訟が提起されている。

米国下院議員の書簡に対する2012年１月30日付のグーグル社返信によれば、グーグル社はアカウントにログインしている際に当該アカウント内の情報のみを統合するとしている。また、ログインをせずに使用できるサービスも多くあり、（統合を避けたい場合）複数のアカウントを作ることも可能であるとしている。アンドロイド搭載端末については、PCと同様ログインをしなくても使用できるサービス[39]が多くあるが、アンドロイドマーケット及びGmail等はログインを必要とすると説明している。

【図表2-16：諸外国の状況】

	北　米	欧　州
2010年	12月： **ウォールスストリートジャーナル**が、独自調査により、スマートフォンのアプリケーションによる利用者情報の取扱いについて、問題点を指摘する記事を掲載。	
2011年	4月： **Pandora**（インターネットラジオ視聴アプリ）が複数の広告会社へユーザー情報を送信していたことについて、米国連邦検事局が召喚状を発していたことが証券取引委員会に提出され書類により明らかになった。	
	5月： **iOS及びAndroid OSによる位置情報取得**が問題となり米国上院司法委員会の公聴会へアップル社、グーグル社の代表者が出席（端末の位置情報の取得方法及び履歴の保存方法等）。	
	12月： 「**Carrier IQ**」というネットワーク診断用ソフトウェアが一部のiPhone及びAndroid端末において端末内の利用者情報を取得し、Carrier IQ社への送信が疑われた問題。 連邦取引委員会（FTC）や連邦通信委員会（FCC）がCarrier　IQ社に聞き取り調査。アップル、AT&T、スプリント･ネクステル、T-Mobile、HTC、サムスンが採用を認める。	**ドイツ** **Carrier IQ**についてバイエルン州のデータ保護規制当局がアップル等に対し、情報提供を求める。
	12月： **モバイルマーケティングアソシエーション（MMA）**は、アプリケーション開発者が消費者にプライバシーポリシーを分かりやすく伝えられるように配慮し「モバイル・アプリケーション・プライバシーポリシー」を発表。	
2012年	1月： **グーグルの新プライバシーポリシー**について、８人の米国下院議員がグーグル社CEOのラリー・ペイジ氏宛てに書簡を送付し、質問を行うとともに懸念を表明。	**EU** **「個人データ保護規則」案**を公表。

[39] 電話やSMS、ウェブ閲覧、検索サービス、YouTube、グーグルマップ、グーグルニュース等がログインなしに使用可能なサービス例として挙げられている。

<table>
<tr><td></td><td colspan="2">1月：
携帯通信事業者の業界団体 GSMA(GSM Association)は、携帯端末向けのプライバシー原則（Mobile Privacy Principles)を発表し個人情報にアクセスし収集するアプリケーションやサービスを利用する消費者のプライバシーが尊重される必要があるとした。また、携帯端末向けアプリケーション開発におけるプライバシーデザインのガイドライン（Privacy Design Guidelines for Mobile Application Development）について発表した。</td></tr>
<tr><td></td><td>2月：
・iPhone用のSNSアプリ「Path」が電話帳情報等を利用者の同意を得ないままPathサーバーに送信していたとされる問題。アップル社は米国下院議員からの書簡を受け、ユーザー承認の必要性について見直しを検討。
・グーグルの新プライバシーポリシーについて、米国の36の州・特別区等の司法長官がグーグル社CEOのラリー・ペイジ氏宛てに書簡を送付し、懸念を表明。
・グーグルの新プライバシーポリシーについて、カナダのプライバシーコミッショナーが米グーグル社に書簡を送付し、質問を行うとともに懸念を表明。
・米カリフォルニア州司法長官が、モバイルデバイス市場の大手6社（アップル、グーグル、アマゾン、マイクロソフト等）がプラットフォームを通じて提供する全てのアプリについてプライバシーポリシーを明示的に提示すること等をこれらの企業と合意したことを発表。
・FTCスタッフレポート「子供のためのモバイルアプリ」：アンドロイドOS 及び iOSのアプリ各100ずつ（合計200）の調査結果として、「プライバシーに係る情報公開水準は不十分である」旨を発表。
・ホワイトハウス「プライバシー権利章典」を発表（7箇条：①個人のコントロール、②透明性、③経緯の尊重、④安全性、⑤アクセスと正確性、⑥対象を絞った収集、⑦説明責任）。</td><td>EU
グーグルの新プライバシーポリシーについて、個人データ保護作業部会議長が、ラリー・ペイジ氏宛てに発効延期を求める書簡を送付。

フランス（CNIL）
グーグルの新プライバシーポリシーについて、CNIL委員長がラリー・ペイジ氏宛てにEUデータ保護指令へ違反する可能性を指摘し、再度延期を求める書簡を送付。

英国
ケンブリッジ大学コンピュータ研究所等によるAndroid向けアプリケーションの利用者情報の収集状況を分析。</td></tr>
<tr><td></td><td>3月：
・グーグルの新プライバシーポリシーが1日付で発効。
・FTC報告書「急速に変化する時代における消費者プライバシー保護」：FTCがトラッキング拒否の簡易化等今後取り組む「5つの主要なエリア」を公表。</td><td>フランス（CNIL）
がグーグルの新プライバシーポリシーについて、ラリー・ペイジ氏宛てに質問を送付。
これに対し、グーグルは4月20日付で全質問に対し回答。</td></tr>
<tr><td></td><td colspan="2">・商業活動上のプライバシー及び個人情報の保護に関し、EU・米国が共同声明を発表。プライバシー保護に係る双方の取組を尊重すること、プライバシー侵害に関する共同監視、セーフバーバー協定の有効性等について確認されている。</td></tr>
<tr><td></td><td>5月：
・オンライン、モバイルメディアにおける広告及びプライバシー開示に関するワークショップ：FTCは、オンラインやモバイル環境における広告やプライバシー開示に関するベストプラクティスの考察など新たなガイダンスの必要性を考えることを目的として、官民の関係者を集めた会合を5月30日に開催。</td><td></td></tr>
</table>

第３章　利用者情報に係る制度とこれまでの取組

１　我が国における現状

今まで見てきたように、スマートフォンにおける利用者情報をアプリケーション等を通じて収集・活用し、利用者に対して利便性の高いサービスが提供されている一方、利用者が十分認識しないまま、あるいはその同意なく、利用者情報が収集・利用され、さらには第三者に提供される場合もある状況に対し、利用者が不安感等を抱く事例もみられる。

この章においては、本中間取りまとめ以降、スマートフォンにおける利用者情報の取扱いについての検討を深めるに当たり、関連し得る国内法制度、ガイドライン及びこれまでの検討状況、これを踏まえた民間の取組について概観する。

（１）個人情報の保護に係る制度等

① 個人情報保護法

「個人情報の保護に関する法律」（平成15年法律第57号。以下「個人情報保護法」ないし単に「法」という。）は、「個人情報取扱事業者」に対して、「個人情報」、「個人データ」及び「保有個人データ」の取扱いに関して様々な義務を課している。アプリケーションやサービスの提供者等の利用者情報を活用する事業者が、同法にいう「個人情報取扱事業者」に当たる場合、法第15条以下の義務規定が適用される。

「個人情報」とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより個人を識別することができることとなるものを含む。）」。（法第2条第1項）をいい、生存性及び個人識別性の有無が「個人情報」該当性の要件となることとされている。スマートフォンにおける利用者情報の中には、個人情報又は個人情報となり得るものも含まれる。

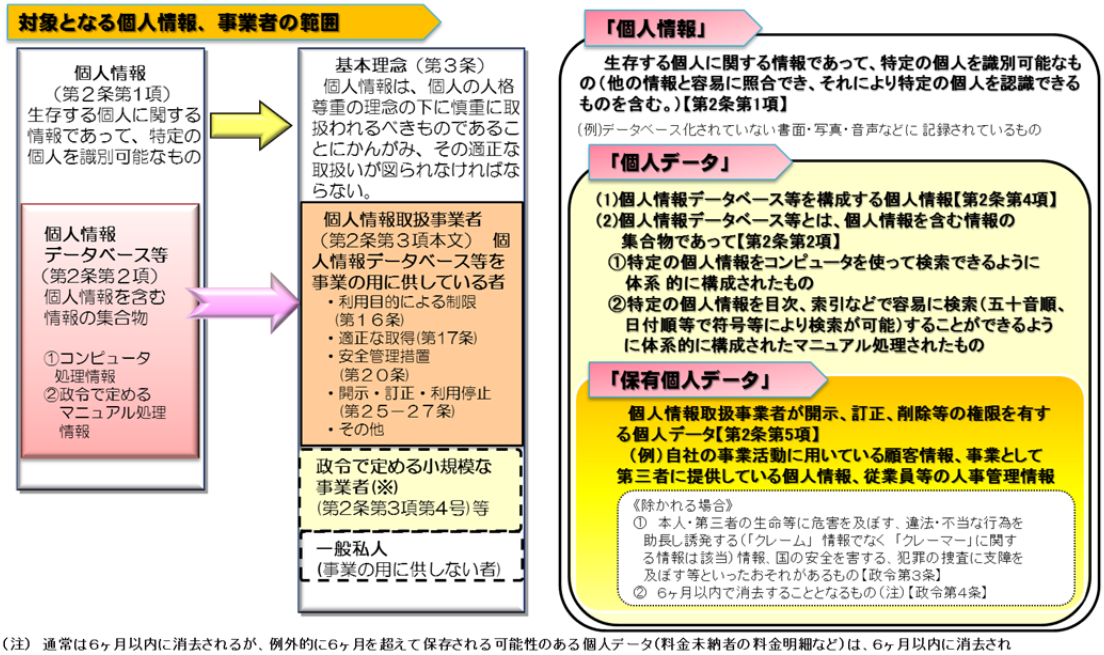
一般的に、個人情報を含む集合物であって「特定の個人情報を電子計算機を用いて検索できるように体系的に構成したもの[1]」等の「個人情報データベース等」を事業の用に供している者である場合、「個人情報取扱事業者」に該当する[2]とされており、個人情報取扱事業者には個人情報保護法における以下の規定等が適用される。

---

1 個人情報保護法第２条第２項第１号

2 個人情報保護法第２条第３項

【図表3-1：個人情報保護法の概要】



（注）通常は6ヶ月以内に消去されるが、例外的に6ヶ月を超えて保存される可能性のある個人データ（料金未納者の料金明細など）は、6ヶ月以内に消去されなかった段階で「保有個人データ」となる。また通常6ヶ月を超えて保存される個人データについても、6ヶ月を超えて保有された段階から「保有個人データ」となる。
※ 事業の用に供する個人データによって識別される人数が5,000以下の者（なお、市販のカーナビや電話帳をそのまま利用する場合、これらに含まれる個人データによって識別される人数は算定に含まれない。）

・ 利用目的の特定：
　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的をできるだけ限定。利用目的の変更は変更前と相当の連関性を合理的に認める範囲を超えてはならない（法第15条）。
・ 利用目的による制限：
　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、第15条により特定された利用目的達成に必要な範囲を超えて、個人情報を取り扱ってはならない（法第16条）。
・ 適正な取得：
　偽りその他不正の手段により個人情報を取得してはならない(法第17条）
・ 第三者提供の制限：
　あらかじめ本人の同意を得ないで個人データを第三者に提供してはならない（又は、必要な事項をあらかじめ本人に通知等し、本人の求めに応じて第三者への提供を停止する）（法第23条）。
・ 利用停止等：
　第16条、第17条、第23条に違反して取り扱われているという理由により、利用停止等を求められた場合の対応（法第27条）　。
・ 苦情の処理：
　個人情報取扱事業者による苦情の適切かつ迅速な処理、必要な体制の整備（法第31条）。

② 電気通信事業における個人情報保護に関するガイドライン

電気通信事業における個人情報保護に関するガイドライン（平成16年総務省告示第695号）において、通信の秘密[3]に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信サービスの利便性の向上を図るとともに、利用者の権利利益を保護することとされている。本ガイドラインにおける電気通信事業者[4]にアプリケーションやサービス提供者や関係事業者が該当する場合には、当該事業者における「個人情報」の取扱い等に本ガイドラインが適用されることとなる。

ガイドラインの第1章（総則）において、目的、定義のほか、通信の秘密に関する電気通信事業法の規定及び個人情報保護法の規定とガイドラインの関係等を明確化している。なお、本ガイドラインの対象は電気通信事業を行う者（登録、届出の有無を問わない）となっている。

ガイドラインの第2章（個人情報の取扱いに関する共通原則）については、個人情報保護法を踏まえ電気通信事業者が遵守すべき事項について定めている。

ガイドラインの第3章（各種情報の取扱い）については、通信履歴、発信者情報、位置情報、迷惑メール等送信に係る加入者情報等、電気通信事業者が取り扱う各種情報の取扱いに関する規定を整備している。

本ガイドラインの特色として、個人情報だけではなく通信の秘密の観点からも規定していること、保有する個人情報等の数にかかわらず、全ての電気通信事業を行う者が対象であること、個人データ・保有個人データの用語は用いずに全ての個人情報が対象であること等がある。

---

3 通信の秘密に関連する主な規定としては、日本国憲法第 21 条第 2 項、電気通信事業法（昭和 59 年法律第 86 号）第 4 条、有線電気通信法（昭和 28 年法律第 96 号）第 9 条、電波法（昭和 25 年法律 131 号）第 59 条が挙げられる。

4 同ガイドライン第 2 条第 1 項において「電気通信事業者は、電気通信事業（電気通信事業法（昭和 59 年法律第 86 号）第 2 条第 4 号に定める電気通信事業をいう。）を行う者をいう。」とされおり、電気通信事業を営むことについて登録、届出という行政上の手続きを経た者とともに、電気通信事業法の適用除外とされている同法第 164 条第 1 項各号に定める事業を営む者についても本ガイドラインの対象とすることとされている（同ガイドライン第 2 条解説）。

（２）プライバシーに係る取組

①　第二次提言における「配慮原則」（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）

「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」の第二次提言が2010年（平成22年）5月に発表された。同提言中において「ライフログ活用サービスに関する検討について」として、ネットワーク機器や携帯端末の高機能化等により、ライフログ[5]を利用したビジネスが注目される一方、利用者に不安感や不快感が存在するとの指摘があることから、我が国において懸念される法的問題点について、主に個人情報保護及びプライバシー保護の観点を踏まえ検討を行っている。

このうち、プライバシーについては、一般的に規定した法律はないが、判例法理上、プライバシーは法的に保護されるべき人格的利益として承認されてきている。同提言において、行動ターゲティング広告等において一般的に取得・利活用されるウェブページ上の行動履歴（閲覧履歴、購買履歴等）や位置情報についてプライバシーの観点から分析し、これら情報は他人にみだりに知られたくないと考えることは自然なことであり、その取扱いの態様によってはプライバシーに係る情報として法的保護の対象となる可能性があるとしている。また、これらは一般にそれ単独では個人識別性を有しないが、大量に蓄積され個人が容易に推定可能になるおそれや、転々流通するうちに個人識別性を獲得するおそれがあることを指摘している。プライバシー侵害が成立する可能性のリスクを低減する観点や、利用者の不安感等を軽減し円滑なサービス展開に資する観点より、事業者は行動履歴や位置情報の取扱いについて透明性を高めることや、利用停止や取得停止等の利用者関与の手段を提供するなど、相応の配慮が求められるとしている。

同提言において、揺籃期にあるサービスの現状を考慮し、規制色の強い行政等によるガイドライン化を避けて、事業者による自主的なガイドラインの策定を促すこととし、ライフログを取得・保存・利活用する事業者が利用者に対してなすべき配慮に係る緩やかな配慮原則が策定された。

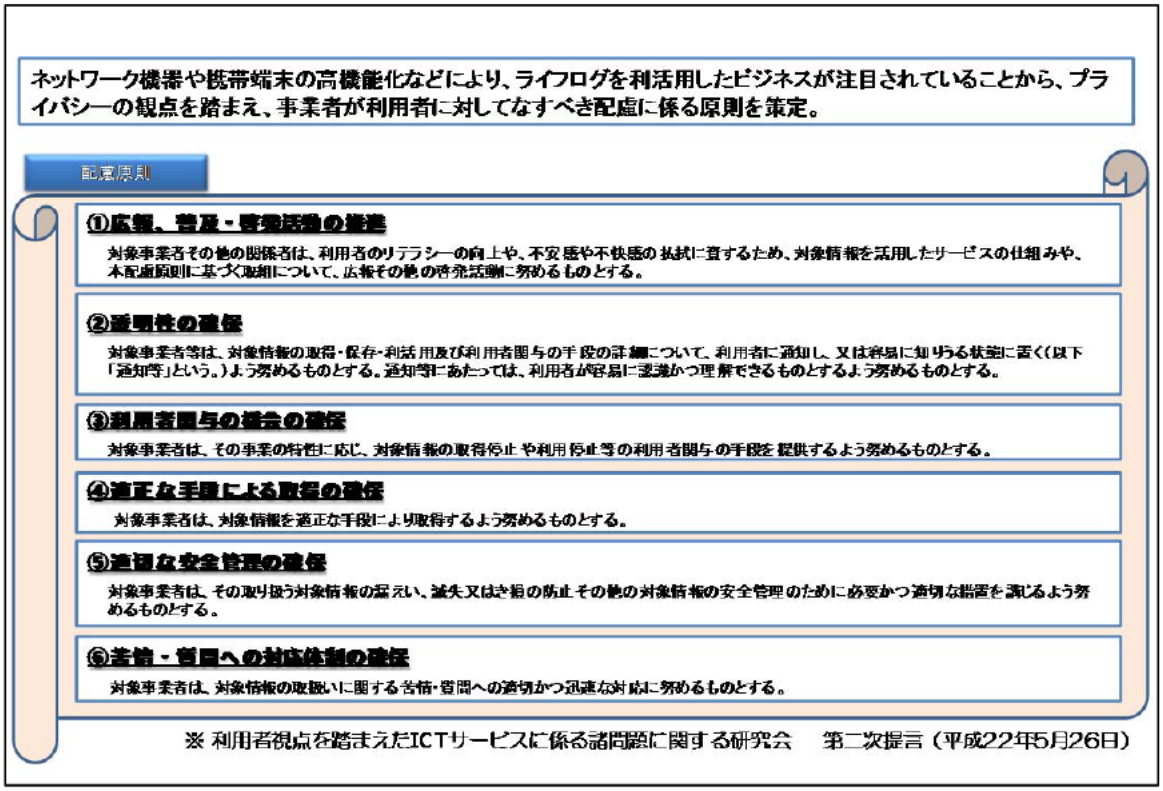
配慮原則は下記のとおり、①広報、普及、啓発活動の推進、②透明性の確保、③利用者関与の機会の確保、④適切な手段による取得の確保、⑤適切な安全管理の確保、⑥苦情・質問への対応体制の確保の6項目となっている[6]。

---

5 ライフログ：蓄積された個人の生活の履歴をいい、ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末の GPS（Global Positioning System 全地球測位システム）により把握された位置情報等々が含まれる。

6 諸問題研究会第二次提言（http://www.soumu.go.jp/main_content/000067551.pdf）参照。
なお、参考として、新保史生『ライフログの定義と法的責任　個人の行動履歴を営利目的で利用することの妥当性』（http://www.jstage.jst.go.jp/article/johokanri/53/6/53_295/_article/-char/ja）がある。

【図表3-2：配慮原則】



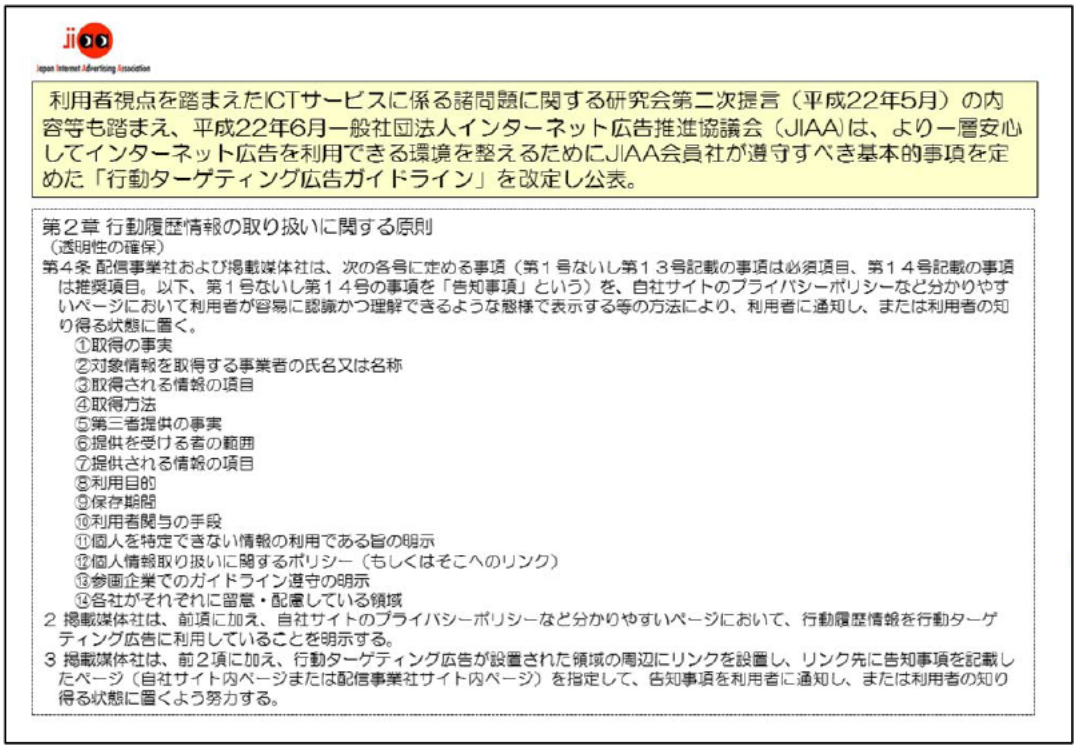
② 配慮原則を踏まえた民間による取組

第二次提言における「配慮原則」を踏まえ、一般社団法人インターネット広告推進協議会（JIAA）は、2010年（平成22年）6月に「行動ターゲティング広告ガイドライン」を改定し、行動履歴情報の取扱いに関する原則規定を追記した。

行動ターゲティング広告ガイドラインは、インターネットユーザーのウェブサイト上での行動履歴情報を収集し、そのデータを利用して広告を表示する行動ターゲティング広告に対して適用されることとされており、2010年6月の改定当時においてスマートフォンについて想定していたわけではないが、スマートフォン上において行動ターゲティング広告が行われる場合には適用され得ると考えられる。

JIAAは会員社におけるガイドラインの遵守状況の把握を行う等、適切な運用に努めるとともに、関係団体等との連携を図りながら、スマートフォンの普及など社会情勢や技術動向を踏まえつつ、ガイドラインに関する協議を継続することとしている。

【図表3-3：行動ターゲティングガイドライン】



利用者視点を踏まえたICTサービスに係る諸問題に関する研究会第二次提言（平成22年5月）の内容等も踏まえ、平成22年6月一般社団法人インターネット広告推進協議会（JIAA）は、より一層安心してインターネット広告を利用できる環境を整えるためにJIAA会員社が遵守すべき基本的事項を定めた「行動ターゲティング広告ガイドライン」を改定し公表。

第２章 行動履歴情報の取り扱いに関する原則
（透明性の確保）
第４条 配信事業社および掲載媒体社は、次の各号に定める事項（第１号ないし第１３号記載の事項は必須項目、第１４号記載の事項は推奨項目。以下、第１号ないし第１４号の事項を「告知事項」という）を、自社サイトのプライバシーポリシーなど分かりやすいページにおいて利用者が容易に認識かつ理解できるような態様で表示する等の方法により、利用者に通知し、または利用者の知り得る状態に置く。
①取得の事実
②対象情報を取得する事業者の氏名又は名称
③取得される情報の項目
④取得方法
⑤第三者提供の事実
⑥提供を受ける者の範囲
⑦提供される情報の項目
⑧利用目的
⑨保存期間
⑩利用者関与の手段
⑪個人を特定できない情報の利用である旨の明示
⑫個人情報取り扱いに関するポリシー（もしくはそこへのリンク）
⑬参画企業でのガイドライン遵守の明示
⑭各社がそれぞれに留意・配慮している領域
２ 掲載媒体社は、前項に加え、自社サイトのプライバシーポリシーなど分かりやすいページにおいて、行動履歴情報を行動ターゲティング広告に利用していることを明示する。
３ 掲載媒体社は、前２項に加え、行動ターゲティング広告が設置された領域の周辺にリンクを設置し、リンク先に告知事項を記載したページ（自社サイト内ページまたは配信事業社サイト内ページ）を指定して、告知事項を利用者に通知し、または利用者の知り得る状態に置くよう努力する。

２　諸外国における現状

世界的にスマートフォンの急速な普及が進展する中で、アプリケーションの提供については、グローバルなアプリケーション提供サイトにおいて行われることとなるため、アプリケーションを通じた利用者情報の取扱いについては米国、欧州等の主要市場においても共通した状況が見られる。

米国、欧州等でスマートフォンに特化した立法措置が行われている事例は現時点ではみられないが、一般的な消費者のプライバシーや個人データに係る制度がスマートフォンにおける利用者情報にも適用されると考えられる。また、行動ターゲティング型の広告の普及や利用者に関する情報収集が、スマートフォンのアプリケーション等を含めた様々な手法で幅広く行われている状況を踏まえ、消費者のプライバシーや権利を守るための新たな政策の枠組みや立法措置を検討する動きもみられる。

（１）米国

①　連邦取引委員会(FTC)

ア　FTC法

米国では、個人情報・プライバシー全般を所管する統一的な第三者機関は存在しない。FTC（Federal Trade Commission）は、消費者保護に関する職務・権限（FTC法第５条で規定）を担う独立の機関として消費者のプライバシー保護を図ることとされている。インターネット上の個人情報全般については、包括的な立法が行われ

ておらず、FTCが業界全体を監視しつつ、自主規制を促す形でルール形成している。

連邦取引委員会法第5条（a）において、不公正・欺瞞的行為又は慣行が禁止されており、その中には、消費者のプライバシー侵害も含まれる。違反行為に対する措置は、差止め請求、排除命令、民事制裁金等がある。

イ スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則

2009年（平成21年）2月、FTCは、事業者が自主的なガイドラインを作成するに当たっての根本的な原則となる「スタッフレポート：オンライン上の行動ターゲティング広告に関する自主行動原則」を公表した。同原則は、データ収集の詳細を明示すべきことや収集の可否については、利用者が決定すること等を内容としている。複数の業界団体が、FTCによるこの原則を受けて、自主的なガイドラインを策定している。

ウ スタッフレポート：子供向けのモバイルアプリ

2012年（平成24年）2月、FTCは、「児童向けのモバイルアプリ：現在のプライバシーに係る情報公開水準は不十分」をスタッフレポートとして発表した。レポートによれば、児童オンライン・プライバシー法（COPPA）に基づき13歳以下の子供の情報の収集に規制があるが、実際はプライバシーポリシーが示されない等、親に十分な情報提供がないまま情報収集を行うアプリケーションも多く、残念な結果であるとされた。

スタッフレポートの提言において、アプリケーション開発者は簡潔な説明やアイコンを通じて情報提供を行うべきであること、2つの主要なアプリマーケットの運用者は、アプリケーションのデータ収集に関する情報をアプリ開発者に表示させるように一貫性ある方法を提供すべきであり、門番としてもっと行動すべきとされている[7]。

エ FTC報告書：急速に変化する時代における消費者プライバシー保護

2012年（平成24年）3月、FTCは、2010年12月に発表された予備スタッフレポート[8]の最終版として「急速に変化する時代における消費者プライバシー保護」をFTC報告書として発表した。特定の消費者、コンピュータやその他の端末と合理的に関連付けることが可能な消費者のデータを収集又は利用する商業主体が対象としている。

---

7 第３回会合資料３「スマートフォンをめぐる国際的動向」（石井構成員）。

8 特定の消費者、PC やその他端末と合理的に関連付けることが可能な消費者データを収集、保持、共有又は利用する全ての商用主体が対象とされ、①Privacy by Design（※1）、②選択する権利の簡易化（Do Not Track 制度（※2）等を提案）、③さらなる透明性の確保等が原則として提案。
（※1）ビジネス設計段階からのプライバシー保護を行うこと
（※2）オンライン上の行動を追跡拒否する措置を講ずること。

消費者のプライバシー保護のため、企業が採用すべきプライバシーの枠組みとして、①プライバシー・バイ・デザイン、②企業は消費者にシンプルな選択肢を提供する、③透明性の増進を示している。

FTCが来年にかけて取り組んでいく「5つの主要なエリア」として、①トラッキング拒否の簡易化（Do Not Track）、②モバイル[9]、③データ販売業者[10]、④大規模プラットフォーム・プロバイダー[11]、⑤強制力のある自主規制基準の推進を挙げている。

2012年（平成24年）5月30日にFTCは公開ワークショップ「デジタル世界における広告とプライバシーの簡潔な情報開示」を開催[12]し、モバイル広告の情報開示及びモバイルプライバシー情報開示等について業界団体、消費者団体及び学者等が参加して意見交換を行われた。その中で、モバイル端末向けのアプリのダウンロード時に表示されるプライバシー情報取得についての情報開示は不十分で分かりにくいこと、スマートフォンを含むモバイル端末はPCと比較し画面が小さいことなどから同一画面に重要な情報から優先的に表示すべきであること、利用者の利便性を損なわずに必要かつ十分な情報開示をする検討が必要であること等について指摘があった[13]。

② プライバシー権利章典（ホワイトハウス）（2012年（平成24年）2月）

2012年（平成24年）2月23日オバマ米政権（ホワイトハウス）は、デジタルエコノミーにおいて消費者の信頼を維持するために消費者のデータプライバシーの保護は必要不可欠とし、政策大綱「ネットワーク化された世界における消費者データプライバシー」を発表。7か条からなる消費者のオンライン・プライバシーを守るための「消費者プライバシー権利章典（Consumer Privacy Bill of Right）[14]」が含まれており、インターネットへの信頼とイノベーションの推進のために、プライバシー権利章典は尊重され、多数の関係者の行動規範（Codes of Conduct）となるべきとした。

このプライバシー権利章典において、個人データの定義が、従来の「特定の個人を

9　モバイルについては、携帯電話会社に対して「簡潔で意味のある情報公開」を求めている。なお、本年5月30日に開催するワークショップにおいて「業界の自主規制が一層促進される」ことを期待するとしている。

10　消費者がデータ販売業者の保有する自らに関するデータにアクセスするための法整備を推進するとしている。また、業者に対し「集約化されたウェブサイトの作成を検討」し集めているデータについて明らかにするよう求めている。

11　大規模プラットフォーム・プロバイダーについては、インターネットサービスプロバイダー、オペレーティングシステム、ウェブブラウザ、ソーシャルメディアサービスが「消費者のオンライン行動の包括的追跡」を試み「プライバシーに関する懸念を増加させている」としている。2012年後半にFTCは本分野におけるワークショップを開催する予定としている。

12　“In Short Advertising & Privacy Disclosures in a Digital World”
http://www.ftc.gov/bcp/workshops/inshort/index.shtml#comment

13　わかりやすい情報開示のため業界で統一したアイコンやデザインの導入の検討、アプリケーション開発者の教育のための統一的で明解な指針の検討等を求める意見も出された。FTCはワークショップの結果やパブリックコメントの結果等を踏まえ、今後新たな指針を検討するとしている。

14　1970年代以降の米国において、プライバシー保護関係の法律制定時に取り入れられる。公正情報実施原則（FIPP）から発展（第3回会合　石井構成員資料）。

識別される（identifiable）から」拡大されており、集積されたデータを含むあらゆるデータであって、特定個人と結びつき得る（Linkable)ものとされた（例：利用履歴を蓄積するスマートフォンや家庭用コンピュータの識別子等）[15]。

消費者プライバシー権利章典の7箇条は下記のとおりである

1　個人のコントロール:
消費者は、事業者がどの個人データを収集し、どのように使用するかコントロールする権利を有する。

2　透明性:
消費者は、プライバシー及びセキュリティの実務について、容易に理解しアクセス可能な情報を得る権利を有する。

3　経緯の尊重:
消費者は、事業者が自分の個人データを、自らが情報を提供した経緯に沿う形で、収集、利用、開示することを期待する権利を有する。

4　安全性:
消費者は、個人データが安全かつ責任をもって扱われる権利を有する。

5　アクセスと正確性:
消費者は、データの機微性及び不正確な情報が消費者にとって望ましくない結果を生むリスクに応じた方法で、利用可能な書式により個人データにアクセスし訂正する権利を有する。

6　対象を絞った収集:
消費者は、事業者が収集・保有する個人データに合理的な制限を設ける権利を有する。

7　説明責任:
消費者は、事業者が個人データをプライバシー権利章典に従って適切な手段を施されて扱われることを保証される権利を有する

米国政府は、今後、新しい権利章典に準ずる行動規範を検討する予定としている。行動規範に準じるかどうかは企業の自主判断に任されるが、遵守を公表した企業が違反した場合、FTCは行動規範に基づいて既存の権限の下で執行を行うことができる[16、17]。

15 第３回会合 石井構成員資料。

16 FTC 及び州検事総長に消費者権利章典を施行するための特定の権限を与える法制化を議会に働きかけていくとしており、また、国際的な相互運用性を強化すべきとしている。

17 オンライン広告事業者団体デジタル・アドバタイジング・アライアンスは、ウェブブラウザの「Do Not Track（追跡拒否機能）」ボタンをサポートしていく方針を決めたことを発表した。これについて、ブラ

③ カリフォルニア州司法長官とプラットフォーム6社の合意（2012年（平成24年）2月）

2012（平成24年）年2月、カリフォルニア州のハリス司法長官は、スマートフォン等のアプリケーションに係るプライバシーの保護についてプラットフォーム６社（アップル社、グーグル社、アマゾン社、マイクロソフト社等）と合意に達した[18]。

報道によれば、合意においてカリフォルニア州法「オンライン・プライバシー保護法」で定める基準を各社アプリケーション掲載サイトにおいて遵守することに合意し、①全てのアプリケーションについて明示的なプライバシーポリシーを提示すること、②ダウンロード前に利用者がプライバシーポリシーを確認できるようにすること、③収集する個人情報の種類・用途・提供先を示すこと、④違反するアプリケーションを通報する仕組みを作ること、⑤プラットフォーム事業者による開発者への教育を行うこと等が含まれている[19]。

アプリケーション開発者のプライバシーポリシー違反は、州の不正競争行為又は虚偽広告法に抵触し、同州司法当局は消費者の情報をプライバシーポリシーに違反する形で利用した場合、アプリケーション・メーカーを訴追するとしている。

（２）欧州

欧州において、1995年（平成7年）「個人データ処理及びデータの自由な移動に関する個人の保護に関する指令(95/46/EC)（EUデータ保護指令）」、2002年（平成14年）「個人情報の処理と電子通信部門におけるプライバシーの保護に関する指令（2002/58/EC）（eプライバシー指令）」、2009年（平成21年）「Telecom Reform Package」（eプライバシー指令の一部改正）等に基づき個人データ保護が行われている。2002年 eプライバシー指令によれば、ロケーションデータ利用の際にオプトイン[20]による利用者同意を義務付けており、さらに、2009年の改正において、個人情報の利用目的の明示と目的外利用の禁止等が定められた。

また、2012年（平成24年）1月に、EUの個人データ保護に関する現行基本法である1995年ＥＵデータ保護指令を見直す「個人データ保護規則」案が公表され欧州議会に提出された。この案において、「個人データはデータ主体に関連する（relating to）あらゆる情報を意味する」（第4条（2）項）こととされた[21]。EU域内における規制の単一

ウザ大手のグーグル社, マイクロソフト社等は Do Not Track 技術に対応することを約束するとした。

18 現在最もダウンロードされているアプリケーション 30 のうち、7 割以上の 22 にプライバシーポリシーがない。同司法長官は「（モバイル・テクノロジーの）潜在的にある利用方法に関する知識を持たない住民がおり、かれらは潜在的に被害を受けやすい」と述べた。

19 合意文書: http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf?

20 サービス提供者が個々のサービスを提供するに当たり、事前に提供条件等を利用者側に提示し、利用者側から個別的な承諾（同意）を得ないと、当該利用者にはサービス提供を行わない仕組みのこと。利用者側がサービス利用を事前に選択（オプト）できる。

21 第３回会合、石井構成員資料。なお、第 4 条(2)項の定義には識別性の要件がないが、第 4 条(1)項のデータ主体の要件に特定性又は特定可能性が含まれているため、全ての規制において本人の特定識別が要求されないわけではないとの指摘がある。

化、簡素化が図られるとともに、より強固な個人データ保護ルールの整備（忘れられる権利、プライバシー・バイ・デザイン原則等）、データ保護に関するグローバルな対応（EU域内居住者に対する商品・役務の提供を行う場合、域外事業者にも法令の効力が及ぶ）、課徴金（企業の全世界での売上高の最大2%相当額）、欧州データ保護ボードの設置等が提案されている。

【図表3-4：個人データ保護規則(案)のポイント】

1　EU域内における規制の単一化・簡素化
- ・EU法令が全加盟国に同一に適用されるよう、国内法制化の不要な「規則」に変更。※EU規則は各国に直接適用
- ・事業者による事務負担（行政手続等）の簡素化
  （事業者がEU域内のうち一のデータ保護当局の承認を得れば、他国の当局からの承認を不要とする制度の導入）
- ・EU加盟国のデータ保護当局間の円滑な協力メカニズムの創設
  （EU加盟国のデータ保護当局は、他の加盟国の当局からの求めに応じて調査等の協力を行う制度の導入）

2　より強固な個人データ保護ルールの整備
- ・個人データ保護に関する個人の権利の強化
  （「**忘れられる権利**」（個人の求めに応じ、ネット上にアップロードされた個人データの削除の義務化）の導入　等
- ・事業者による個人データ処理に関する説明責任の強化：
  （「**プライバシー・バイ・デザイン**」原則の導入（サービス導入に際しプライバシー対策を考慮）、データ保護官の任命義務等）
- ・個人データのセキュリティの強化（個人データ漏えい時の通知義務）
- ・データ保護に関する個人の権利行使方法の改善
  （EU加盟国のデータ保護当局の独立性及び権限の強化、行政及び司法による救済策の強化）

3　データ保護に関するグローバルな課題への対応
- ・EU域内居住者に対する商品・役務の提供を行う場合、域外の事業者による個人データの取扱いにも法令の効力を及ぼすための規定を整備
- ・EU域内から域外の第三国への個人データの移転に関するルールの明確化・簡素化

4　その他
- ・新たな制裁の導入（企業の全世界での売上高の最大2%相当額の課徴金）　等

（３）民間団体における取組

①　モバイルマーケティングアソシエーション（MMA）

2011年（平成23年）12月、国際的な携帯端末向けのマーケティングに関する業界団体であるモバイルマーケティングアソシエーション（MMA）[22]はアプリケーション開発者が消費者にプライバシーポリシーを伝えるよう配慮した「モバイル・アプリケーション・プライバシーポリシー」を発表した[23]。

これは、アプリケーション開発者がプライバシーポリシーを作る際の参考となるように作成されたもので、①アプリケーションが取得する情報（ユーザーの登録情報及び自動取得情報）、②位置情報の取得、③第三者による情報の扱い、④自動情報取得及び広告、⑤オプトアウト[24]の権利、⑥データ保持及び管理、⑦子供の情報の取扱い、⑧セキュリティ、⑨本ポリシーの変更、⑩利用者の同意、⑪連絡先等について、それぞれ記載例・方法を示している。

22　700以上の企業が加入しており、北米、南米、アジア、欧州等に地域支部がある。

23　http://mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobie-apps 参照。

24　利用者側がサービス利用の停止を事後に求めることができる仕組みをいう。なお、個人情報保護法第23条第2項には本人の求めに応じて個人データの第三者提供の停止を行うこと（オプトアウト）が規定されている。

② GSM Association（GSMA）

2012年（平成24年）1月、世界的な携帯通信事業者の業界団体GSMAは、携帯端末向けのプライバシー原則（Mobile Privacy　Principles）[25]、プライバシーデザインのガイドライン（Privacy Design Guidelines for Mobile Application Development）[26]を発表している[27]。

アプリケーションとモバイル端末に関連するプライバシーデザインのために、アプリケーション開発者、機器製造事業者、プラットフォーマー、OS事業者、通信キャリア及び広告や情報分析事業者等、関連する全ての主体に適用されるものとして、プライバシー・バイ・デザインアプローチを採用し、モバイル・アプリケーションの開発時にユーザーのプライバシーや個人情報の保護を促進することを目的としている。

ガイドラインの内容として、透明性とユーザーによる選択とコントロール：①ユーザーに個人情報の収集項目、利用目的、利用方法等について事前に通知、目的変更について改めて説明（位置情報や電話帳については十分配慮）、②情報取得者の名称・連絡先を明記、③適切なプライバシーに関する説明の提供（アプリケーションに係る最初のページ等へ表示）、④最小限の情報収集と限定された利用、⑤必要な時ユーザーの積極的合意を得る（位置情報、第三者との情報シェア）、⑥プライバシー・バイ・デザイン、⑦秘密アップデートの禁止等が定められている。また、その他、データの保存とセキュリティ、教育、SNS、モバイル広告、位置情報、青少年、説明責任等について規定している[28]。

25　http://www.gsma.com/documents/mobile-privacy-principles/20005/　参照。

26　http://www.gsma.com/Mobile-Privacy-Design-Guidelines 参照。

27　背景として、携帯電話とウェブが融合し利用者は様々なサービスを享受しており、利用者情報の活用がこの革新的ビジネスモデルや個人への最適化を支えているが、一方利用者の個人情報への不正なアクセスを引き起こすおそれもあることを指摘。法的に問題がなくとも、利用者のプライバシーへの期待を裏切り、利用者の携帯事業そのものへの信頼を損ねてしまうおそれがあるという懸念を示している。
本ガイドラインにおいて、個人情報（Personal information）は、個人に関連づけられた情報であるとされ、名前、住所等、携帯電話番号、IMEI，UDID、行動履歴、電話帳、写真等が含まれるとされており、名前が分からなくても端末固有の ID（電話番号、IMEI、UDID）等に利用者の情報が結びつけられるだけでも個人を識別し得ることが指摘されている。

28　ガイドラインにおいて実装として、利用者に対して、どの個人情報がアクセス、収集されるか、どのように利用されるか、誰と共有されるか、利用目的は何か、どの期間保存されるのか等をあらかじめ利用者に示す必要があるとしている。また必要な最小限度の情報利用を促しており、情報利用について一定のタイミングで利用者が再確認・再設定できることも提言している。さらに、位置情報、電話帳などの情報の種類により、望ましい使用レベルや説明方法を提示している点も特徴的である。

第Ⅱ部

課題認識と具体的対応

1　課題認識

第Ⅰ部における検討を踏まえ、スマートフォンにおける利用者情報の取扱いに関する課題は、次のとおりに整理される。

（１）スマートフォンにおける利用者情報の適正な取扱いの在り方

① スマートフォンにおける利用者情報の性質・分類

スマートフォン上の利用者情報の適正な取扱いの在り方を論ずる前提として、スマートフォン上の利用者情報の取扱いと現行法制度等との関係性を整理する必要がある。【第４章関連】

② スマートフォンにおける利用者情報の適正な取扱いの在り方

次に、①の整理を踏まえ、関係事業者等が利用者情報を適正に取り扱う上で従うことが望ましい具体的な規範について整理する必要がある。【第５章関連】

（２）利用者に対する情報提供・周知等の在り方

スマートフォンの一層の普及が見込まれる中で、広く青少年から高齢者までの幅広い利用者が安全・安心に利用できる環境を整備するためには、利用者のリテラシー向上のための環境作りの方策について整理する必要がある。【第６章関連】

（３）国際的な連携の推進

スマートフォンにおけるプライバシー問題が諸外国においても政策課題となっており、こうした課題の解決には外国事業者を含む多くの関係事業者の連携が極めて重要になっていることから、国際的な連携の推進の在り方について整理する必要がある。【第７章関連】

2　第Ⅱ部における検討の方向性

上記課題認識から、第Ⅱ部では次のとおり検討を行う。

第４章においては、スマートフォン上の利用者情報の取扱いに関して、利用者情報・それを取り扱う者・取扱い方法等といった構成要素ごとに、利用目的や現行法制度等（個人情報保護法、プライバシーに関する諸整理等）から見た位置付けを整理する。

また、第５章においては、第４章における検討結果も踏まえ、アプリケーション提供者等の関係事業者等が利用者情報を適正に取り扱う上で従うことが望ましい具体的な規範として、「スマートフォン利用者情報取扱指針」を提示する。

さらに第６章においては、スマートフォンの一層の普及が見込まれる中で、広く青少年から高齢者までの幅広い利用者が安全・安心に利用できる環境を整備するためには、「誰が」「どのような情報を」「誰を対象に」「どのような方法で」提供し、また利用者側でこれをいかに利用すべきかを明らかにする。

最後に第７章においては、国際連携の具体的な推進方策として、先進国との間での連携、国際機関等を活用した連携、民間団体間の連携及び我が国の取組の発信強化について明らかにする。

第４章　スマートフォンにおける利用者情報の性質・分類

スマートフォンの利用者の個人情報やプライバシーが尊重され、安全・安心にスマートフォンにおける利用者情報が活用されていく環境を実現していくために、本章においては、スマートフォンにおける利用者情報の性質・分類と望ましい取扱方法について、利用目的との関係の観点、個人情報保護法の観点、プライバシーの観点等から検討を進めることとする。

１　利用目的による分類

スマートフォンにおける情報は適切に活用されることにより、利用者に対し、スマートフォンにおける様々なアプリケーションを通じて利便性の高いサービスを提供するために貢献することが可能となる[1]。現状としては、利用者の期待するサービスやアプリケーションの内容・目的を実現するために必要となる利用者情報と、そうでない利用者情報の双方がアプリケーションにより取得されている。本項においては、利用者情報の取得について利用目的との関係に着目し、アプリケーションやサービスの内容・目的を実現するために必要であるものとそうではないもの等に分類し、利用者の認知が容易であるかどうか、またそれによる情報取得や説明の在り方について考察する。

第 2 章においても指摘されるように、利用者に提供されるアプリケーションやサービスの内容・目的との関係により、アプリケーションによる利用者情報の利用目的には、大きく分けて①～④のような事例があると考えられる。

① アプリケーション等がそれ自体のサービス提供のために用いる場合[2]

② アプリケーション提供者が、アプリケーションの利用状況等を把握することにより、今後のサービス開発や市場調査のために用いる場合。

③ スマートフォンの位置情報あるいは契約者・端末固有 ID 等の利用者情報を情報収集事業者等が取得し、広告サービス等に活用する場合又はその他の市場調査等の情報分析等に活用する場合

④ 現段階では目的が明確ではないが将来的な利用可能性等を見込んで取得する場合

---

1 例えば GPS 位置情報の取得により地図アプリにおける現在地や現在地から目的地までの経路表示など。

2 アプリケーションのサービス提供のために取得した情報について、その他の利用目的のために転用しない場合。なお、利用者が期待するサービス実現のために技術的必然性のある処理により結果的に生じる情報取得については、（目的外利用しない前提で）黙示の同意があるのではないかという指摘がある（第 3 回会合、産業技術総合研究所 高木氏資料）。

【図表 4-1：　利用者情報の利用目的と取得者】

情報の利用目的	想定される情報取得者	利用者認知
① アプリケーションがそれ自体のサービス提供のために用いる	アプリケーション提供者	◎
② アプリケーション提供者によるサービス利用動向等把握	〃	△
③ 広告サービス等への活用	アプリケーション提供者、情報収集事業者･広告配信事業者等第三者	△～×
④ 目的が明確ではないもの	〃	×

アプリケーションがそれ自体のサービス提供のために用いる場合（①）について、利用者が情報を入力等しなくともスマートフォンにおける既存の利用者情報を活用してすぐに利便性の高いサービスを利用することが可能となるなど利用者が直接的な利益を受ける場合が多く、利用者にも直感的に認識・理解しやすいと考えられる。

一方、アプリケーションそれ自体のサービスには用いない②及び③の利用目的の場合については利用者が情報の利用目的、情報取得者ともに一般の利用において想定しておらず、そのような情報が取得されることを認知しにくいため、利用者のためにより丁寧な説明が求められる。

また、④に該当する場合については、例えば、単に動画を再生するアプリケーションや壁紙のアプリケーションであるのに電話帳の情報などの個人情報を取得する場合についてマルウェアに該当するとされた事例もあるため、目的が不明確なまま利用者情報を取得しようとするアプリケーションは、原則として情報を取得するべきではないと考えられる。

２　個人情報保護法の観点からの検討

次に、取得されるスマートフォン上の各利用者情報が個人情報保護法上の個人情報に該当するのか、アプリケーション提供者や情報収集モジュール提供者等が個人情報取扱事業者に該当し得るのか等について検討を行い、個人情報保護法との関係を明らかにすることとする。なお、個人情報保護法は主務大臣制を執っており、各主務大臣が所管する分野及びその指定された特定分野における事業者等の個人情報の取扱いについては、当該主務大臣が必要に応じ報告、助言等を行い得るものである。

（１）　個人情報保護法上の検討

①　個人情報への該当性

第３章で確認したように、個人情報保護法において「個人情報」とは、「生存する個

人に関する情報であって、氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（法第２条第１項）と定義されており、個人識別性の有無が「個人情報」該当性の要件となる。

【個人識別性がある場合】

スマートフォンからアプリケーション提供者又は第三者が取得する利用者情報に個人識別性がある場合、個人情報となる。例えば、電話帳においては、一般的には氏名、電話番号、メールアドレス等の連絡先が結びつけられ個人識別可能な形で登録される場合が多く、個人情報を含むと考えられる。契約者情報も、一般的に氏名、住所等を含み個人の識別が可能であるため個人情報となると考えられる。

【他の情報と容易に照合し個人識別性を獲得する場合】

また、スマートフォンからアプリケーション提供者又は第三者が取得する利用者情報単体でみた場合に個人識別性がない場合であっても、取得した者が有している情報等、他の情報と容易に照合し個人識別性を獲得する場合などには個人情報となる場合がある。例えば、電話番号、メールアドレス、契約者・端末固有 ID[3]、ログイン ID などが情報単体では個人識別性がない場合でも、契約者の氏名等個人情報と容易に結びつく場合には個人識別性を獲得する。

契約者・端末固有 ID については、契約者・端末固有 ID のみでは個人識別性はないと考えられる。アプリケーション提供者等が特定の個人を識別可能な情報を保有していない場合又は識別可能な情報を有していても照合することが困難である場合は、個人識別性を獲得しないと考えられる。

一方、スマートフォンの契約者・端末固有 ID は通常、契約や端末によって一義的に決まり、利用者側が変更することが困難である上、様々なアプリケーション提供者等により取得される可能性がある。このことから、多くの関係事業者等が特定のスマートフォンの契約者・端末固有 ID を用いて各々個人情報やプライバシー情報を蓄積する可能性が指摘されている。この場合、特定の個人に関する多くの情報が同一 ID に紐付けられると、個人識別性を獲得する可能性もある。

なお、クッキー技術を用いて生成された識別情報等については、利用者側で容易に変更可能であること、一定の期間のみの利用であることから、契約者・端末固有 ID に比べると、個人識別性を取得する蓋然性は低いと考えられている。

また、ログインのための識別情報は、氏名等個人識別性を有する場合もあるが、単

[3] OS が生成する ID(Android　ID)、独自端末識別番号（UDID）、加入者識別 ID(IMSI)、IC カード識別番号（ICCID）、端末識別 ID（IMEI）、MAC アドレス等。利用者側で変更困難であり、多くの事業者等が共通番号として用いる可能性があることから「グローバル ID」としてプライバシー等の懸念等を指摘する者もいる（第３回会合、産業技術総合研究所 高木氏資料）

なる数字や記号等、それ単体では個人識別性を有しない場合もある[4]。

【行動履歴や利用履歴に関する情報】

行動履歴や利用履歴に関する情報としては、GPS や基地局・Wi-Fi アクセスポイント情報に基づく位置情報、通話履歴（通話内容・履歴、メール内容・送受信内容等）、ウェブページ上の行動履歴などが蓄積されている。また、アプリケーションの利用により蓄積される情報やアプリケーションの利用ログ[5]、システムの利用に関するログなどが蓄積される。位置情報やウェブ閲覧履歴、アプリケーション利用状況などは、それ自体で一般には個人識別性を有しないが、長期間網羅的に収集・記録した場合等において、態様によって個人が推定可能となる場合もある。また、個人の人格と密接に関係する可能性が指摘される。

【図表 4-2： スマートフォンにおける利用者情報の性質と種類】

区分	情報の種類	含まれる情報	利用者による変更可能性	個人識別性等
第三者の情報	**電話帳で管理されるデータ**	**氏名、電話番号、メールアドレス等**	×～△	電話帳には一般に氏名、電話番号等が登録されることが多く、個人識別性を有している場合が多い。
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、**電話番号**等の情報や、クレジットカード番号等の個人信用情報等	×～△	契約者情報には一般に氏名、住所等が含まれており、個人識別性を有している場合が多い。
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	・ログインのための識別情報は変更可能な場合も有り。 ・ログインのための識別情報は、氏名等個人識別性を有する場合もあり、単なる数字や記号等で単体では個人識別性を有さない場合もある。
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じ一時的に PC に書込み記載されたデータ（ウェブサイト訪問回数・サイト内履歴等）。	○ 利用者が必要に応じて変更・修正を行うことが可能	・利用者がウェブブラウザ上で削除やオプトアウトを行うことが可能。 ・単体では個人識別性を有しないが、発行元等において他情報と照合し個人識別性を有する場合がある。

4 ログインに用いる ID 以外にも、個人情報や行動履歴を結びつけるために各アプリケーションやサイト独自の ID 付与を検討する動きもある。この場合、結びつけられる個人情報やプライバシーの範囲、ID の使用期間（利用者によるオプトアウトの可能性）や情報共有の範囲をコントロールされると指摘される。

5 アプリケーションにおける個人の医療・健康・生活状況・金融関係の情報、スケジュール情報 SNS 等による交流状況、本・雑誌・音楽やニュースなどの閲覧履歴などの情報については個人情報及びプライバシーの両面から考慮する必要がある。

	契約者・端末固有 ID	**OS が生成する ID（Android ID）、独自端末識別番号（UDID）、加入者識別 ID（IMSI）、IC カード識別番号（ICCID）、端末識別 ID（IMEI）、MAC アドレス等**	× 端末交換や契約変更をしない限り変更が困難	・スマートフォンの OS やシステムプログラム、SIM カード、端末そのもの等に割り振られ管理される。利用者は端末交換や契約変更をしない限り変更困難。 ・単体では個人識別性を有しない。他の情報と容易に照合できる場合、個人識別性を獲得する。 ・同一 ID に紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が指摘される。
通信サービス上の行動履歴や利用者の状態に関する情報	**通信履歴**	**通話内容・履歴、メール内容・送受信履歴**	×～△ 端末や電気通信事業者のサーバーにおいて管理	・通信相手等により個人識別性を有する場合がある。 ・電気通信事業者の取扱い中のものは通信の秘密の保護の対象。 ・通信履歴はプライバシー上の懸念が指摘される。
	ウェブページ上の行動履歴	**利用者のウェブページ上における閲覧履歴**、購買履歴、検索履歴等の行動履歴	×～△ 端末やウェブページ管理者、アプリケーション提供者等のサーバーにおいて管理	・利用者の行動履歴や状態に関する情報については、内容・利用目的等によりプライバシー上の懸念が指摘される。 ・相当程度長期間にわたり時系列に蓄積された場合等、態様によって個人が推定可能になる可能性がある。
	アプリケーションの利用履歴等	**アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等**		
	位置情報	**GPS 機器によって計測される位置情報、基地局に送信される位置登録情報**		
	写真・動画等	**スマートフォン等で撮影された写真、動画**		・内容、利用目的等によりプライバシー上の懸念がある。 ・顔認識技術等が進むと、個人識別性に結びつく可能性が高まるとの指摘がある。

※下線はスマートフォンのアプリケーションが利用許諾を取得すること等により、自動的に取得を行うことが可能となり得る情報。
※UDID 等の契約者・端末固有 ID の代わりに、UUID、OpenUDID 等の利用に関する検討等も行われている。

② 個人情報取扱事業者への該当性

個人情報保護法において、個人情報データベース等は、「個人情報を含む情報の集合物」であって、「特定の個人情報を電子計算機を用いて検索することができるように体系的に構築したもの」（法第２条第２項）を指している。「個人情報データベース等を事業の用に供している」場合[6]に、「個人情報取扱事業者」となる（法第２条第３項）。

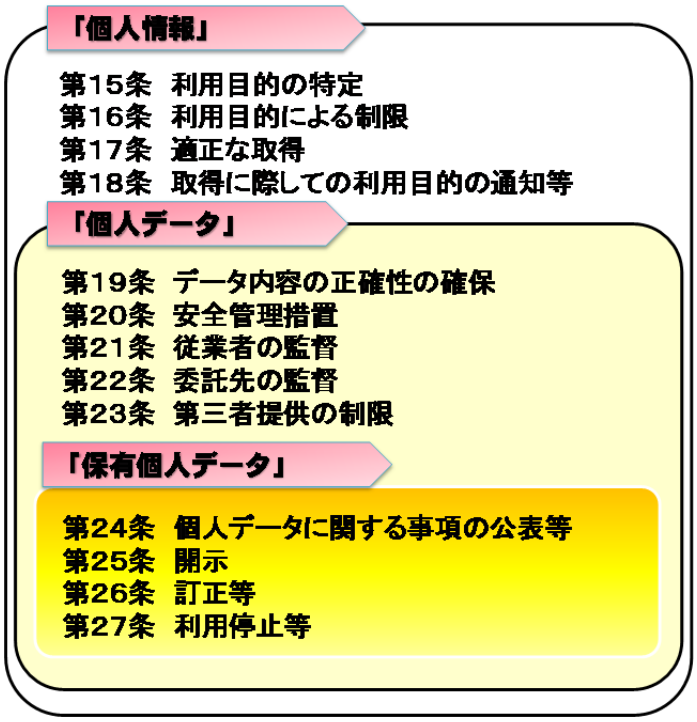
アプリケーション提供者等の中には、個人情報を含むスマートフォンの利用者情報

6 その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 ヶ月以内のいずれの日においても 5 千を超えない者は除く（法第 2 条第 3 項、個人情報の保護に関する法律施行令第 2 条）。

を取得し、データベース等を構築しアプリケーションを通じたサービス提供等の事業の用に供している場合も想定されるため、具体的適用関係は個別の判断が必要にはなるが、個人情報を含む利用者情報を蓄積活用するアプリケーション提供者及び第三者については個人情報取扱事業者となる場合も十分想定される[7]。

アプリケーション提供者等が個人情報取扱事業者に当たる場合には、法第15条以下の義務規定が適用されることとなる[8]。

【図表4-3： 個人情報取扱事業者の主な義務】



【個人情報に関する規定】

個人情報取扱事業者が個人情報を取り扱う際に適用される規定が、法第 15 条以下に設けられている。

① 法第 15 条（利用目的の特定）、法第 16 条（利用目的による制限）

法第 15 条では、利用目的をできる限り特定することを求めており、利用目的の変

7 スマートフォン外部への送信があれば、送信先であるアプリケーション提供者あるいは第三者による取得・利用等があったといえる。一方、アプリケーションによる利用者情報の利用がスマートフォン内部のみに留まり利用であれば、アプリケーション提供者や第三者のサーバー等へ外部送信しない場合、個人情報保護法上の個人情報の取得には該当しないとの指摘がある。

8 個人情報の取扱いについて利用目的の特定（第 15 条）、利用目的による制限（第 16 条）、適正な取得（第 17 条）及び取得に際しての利用目的の通知等（第 18 条）が、個人データの取り扱いについてデータ内容の正確性の確保（第 19 条）、安全管理措置（第 20 条）及び従業者の監督（第 21 条）、委託先の監督（第 22 条）及び第三者提供の制限（第 23 条）が、保有個人データの取り扱いについて保有個人データに関する事項の公表等（第 24 条）及び開示、訂正等、利用停止等（第 25 条～第 27 条）がそれぞれ適用される。

更は変更前と相当の関連性を有すると合理的に認められる範囲内である必要がある（同条第 2 項）。

また、法第 16 条において、本人の同意を得ないで、法第 15 条の規定により特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならないこととされている。

したがって、例えば「マイニング[9]すれば何か役に立つ情報を抽出できるかもしれない」等との意図の下、明確な利用目的を示さずに個人情報を取り扱うことは、法第 15 条の違反となる可能性が高い。また、当初想定された利用目的のみをプライバシーポリシーに記載している場合に、その利用目的とは関係の薄い別の目的のために、本人の同意を得ないまま個人情報を取り扱うことは、法第 16 条の違反となる可能性が高い。

なお、これらの規定については、一般利用者が利用目的を理解・想定しやすいようにする観点から、プライバシーポリシー等に利用目的を適切に記載するための在り方について検討をすべきとの指摘がある。

② 法第 17 条（適正な取得）

法第 17 条により、個人情報について、「偽りその他不正の手段」による取得が禁じられている。「偽り」は、真の利用目的を秘匿して個人情報を取得する場合などに該当する。「その他不正の手段」は、不適法又は適正性を欠く方法や手続を含み、「不正」の有無は社会通念に基づいて判断される。偽りその他不正の手段により取得された個人情報を二次的に取得する場合も本条に抵触し得る。

例えば、個人情報の持ち主が気付かないようにアプリケーションをインストールさせ、意図的に本人に対して情報の送信（取得）を隠ぺいしようとする方法などをとる場合、本条の違反となる可能性が高いとの指摘がある。

また、個人情報を外部に送信し取得する際、OS の利用許諾によって、アプリケーションがアクセスする情報は明らかにされているものの、個人情報を取得することが明らかにされていない場合には、OS の利用許諾とは別に、個人情報を取得することの通知又は公表若しくは同意取得等を行うことが適切であると考えられる[10]。このため、個人情報を取得することの通知又は公表や同意取得の在り方など、適正な取得の在り方について検討すべきとの指摘がある。

---

9 販売データや電話の通話履歴、クレジットカードの利用履歴など、企業に大量に蓄積されるデータを解析し、項目間の相関関係やパターンなどを探し出す技術をいう。

10 アプリケーションに関する OS による利用許諾のみしかなく、アプリケーションの機能等から考えて本人にとって全く予想できない情報を送信する場合等、事情によっては本条の違反となる可能性があると指摘される。

③ 法第 18 条（取得に際しての利用目的の通知等）

法第 18 条では、個人情報を取得した場合、「あらかじめその利用目的を公表」又は取得後速やかに利用目的を「本人に通知し、又は公表」することが求められる[11]。

【個人データに関する規定】

個人情報取扱事業者が個人情報データベース等を構成する個人情報（個人データ）を取扱う際に適用される規定が、法第 19 条～第 23 条に規定されている。

個人情報データベースとして構築されたものについては、データの正確性の確保（法第 19 条）、個人データの漏洩、滅失又は既存の防止その他の安全管理のための措置（法第 20 条）をとる必要がある。また、個人データの安全管理が図られるように従業者を監督（法第 21 条）するとともに、取扱いを委託する場合委託先を監督（法第 22 条）する必要がある。

- **法第 23 条（第三者提供の制限）**

法第 23 条では、アプリケーション提供者が自らのサーバー等に蓄積された個人データを第三者提供する場合、原則として事前に本人の同意（オプトイン）が必要となる。

なお、法第 23 条第 2 項においては例外的にオプトアウトの規定があるが、スマートフォンのアプリの場合、一度に大量の情報を取得し第三者に提供することが技術的に可能であり、一度情報が第三者提供された場合にその情報を取り戻すことが困難であるため、例えばプライバシーポリシー等にオプトアウトについて記載するだけで、個人の権利侵害を十分に防止することはできないのではないかとの指摘がある[12]。

【保有個人データに関する規定】

個人情報取扱事業者が開示、訂正、削除等の権限を有する個人データであり、政令で定める期間（6 ヶ月）以内に消去するもの以外のものを有する場合、透明性を確保するため、個人情報取扱事業者の氏名、名称、保有個人データの利用目的等を本人の知

11 アプリケーションに関する OS による利用許諾に利用目的が記載されていない場合、これ以外に何も表示や公表等をしないまま個人情報を取得する場合には、個人情報の利用目的の通知又は公表が行われていないこととなり、本条の違反となる可能性が高いと指摘される。アプリケーション提供者がプライバシーポリシーを公表するなどの方法により、利用目的を通知又は公表あるいは同意取得している場合は問題ない。

12 個人データを特定の者との間で共同して利用する場合について、共同利用される個人データの項目や共同して利用する者の範囲・利用目的、個人データの管理の責任者などについて通知又は公表する場合は第三者提供に該当しないこととされている（法第 23 条第 4 項第 3 号）。なお、スマートフォンの利用者情報をめぐるサービス構造には多様な事業者等が関係すること、大量かつ詳細な利用者情報が容易に共有されうるため、共同して利用する者の範囲や個人データの管理の責任者等をあらかじめ明確に定めその範囲内の利用を確保することは、難しいのではないかとの指摘もあった。

り得る状態におく必要がある（法第 24 条）。また、本人から開示（第 25 条）、訂正等（第 26 条）、利用停止等（第 27 条）等を求められた際に適切に対応する必要がある。

③ 情報収集モジュールを用いた情報収集の場合

アプリケーション提供者により組み込まれた情報収集モジュール等により、スマートフォンからアプリケーション提供者を経ずに、直接情報収集モジュール提供者（情報収集事業者、広告配信事業者等）へ個人情報等が送信される場合、情報収集モジュール提供者による個人情報の取得となる[13]。情報収集モジュール提供者が、5,000 件を超える個人情報を電子計算機を用いて検索できるように体系的に構築する場合、個人情報取扱事業者として義務を負うこととなる。このため、利用目的の特定（第 15 条）、利用目的の範囲内における利用（第 16 条）、適正な手段による取得（第 17 条）、「あらかじめその利用目的を公表」又は取得後速やかに利用目的を「本人に通知し、又は公表」（第 18 条）、安全管理措置（第 20 条）等について適切に対応する必要がある。

一方、情報収集モジュール提供者は、一般に利用者に対する接点を直接持っておらず、利用者側も何の情報収集モジュールが入っているか等の情報を提供されない限り知り得ず、情報収集モジュール提供者のウェブページを参照する等の措置もできない。

また、情報収集事業者や広告配信事業者等による情報収集モジュールの配布を通じた情報取得については、情報収集モジュールをアプリケーション提供者へ配布しこれをアプリケーション提供者がアプリケーションに組み込むことによって可能となるが、情報収集モジュールの中には、アプリケーション提供者により一部変更されて組み込まれているものもあり、変更内容についてアプリケーション提供者でないと正確に分からない場合もあると指摘される[14]。

このため、詳細は情報収集モジュール提供者が掲載するプライバシーポリシー[15]等を通知又は公表し説明する必要があるものの、アプリケーション提供者のプライバシーポリシーにおいて情報収集モジュール別に最低限必要な情報を利用者に通知又は公表するなど、アプリケーション提供者と情報収集モジュール提供者の間の役割分担により透明性を高めることが現実的かつ必要ではないかとの指摘がある[16]。

---

13 この場合、アプリケーション提供者には当該情報は取得されておらず、アプリケーション提供者による個人情報の取得にはならないため、第 23 条の適用対象とはならない。

14 アプリケーション提供者による改変ができない場合や変更可能でもそのまま組み込まれる場合もある。

15 個人情報の保護に関する基本方針(平成16年4月2日閣議決定、平成20年4月25日一部変更、平成21年9月1日一部変更)において「6　個人情報取扱事業者が高ずべき個人情報の保護のための措置に関する基本的な事項」「（１）個人情報取り扱い事業者に関する事項」「①事業者が行う措置の対外的明確化」において、「事業者が個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を策定・公表することにより、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知又は公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。」とされている。

16 アプリケーション提供者が本人に対して適切な説明をしていないことを知りつつまたはそのことを知るべくして必要な対策を講じることなく、情報収集モジュールを配布し、結果として、本人の認識なく

（２）電気通信事業における個人情報保護に関するガイドラインの観点からの検討

ガイドラインにおける電気通信事業者は、電気通信事業（電気通信事業法第 2 条第 4 号に定める電気通信事業をいう。）を行う者をいう。すなわち、電気通信事業を営むことについて登録、届出という行政上の手続を経た者とともに、電気通信事業法の適用除外とされている同法第 164 条第 1 項各号に定める事業を営む者、すなわち登録・届出を要しない電気通信事業を営む者も含まれることとなっている。また、保有する個人情報の数にかかわらず、全ての電気通信事業を行う者が対象である。

電気通信事業者が取り扱う個人情報とともに、通信の秘密の保護等の観点から、通信履歴、利用明細、発信者情報、位置情報等について規定している。

スマートフォンにおけるアプリケーションやサービスは様々な種類の形態のものが提供されており、適用関係については個別に判断する必要がある。「登録・届出を要しない電気通信事業」又は「登録又は届出を要する電気通信事業」に該当する場合には、ガイドラインに従い、個人情報及び通信の秘密等を取り扱う必要がある[17]。

【図表 4-4： 電気通信事業における個人情報保護に関するガイドライン】

【電気通信事業における個人情報保護に関するガイドライン（平成16年総務省告示第695号）】

➢目的：通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信サービスの利便性の向上を図るとともに、利用者の権利利益を保護すること

➢構成：
第1章　総則
（目的、定義のほか、通信の秘密に関する電気通信事業法の規定及び個人情報保護法の規定とガイドラインの関係等を明確化）
第2章　個人情報の取扱いに関する共通原則
第3章　各種情報の取扱い
（電気通信事業者が取り扱う各種情報の取扱いに関する規定を整備。例：通信履歴、発信者情報、位置情報、不払い者情報、迷惑メール等送信に係る加入者情報等）

➢特色：個人情報だけではなく通信の秘密の観点からも規定、保有する個人情報等の数にかかわらずすべての電気通信事業を行う者が対象、個人データ・保有個人データの用語は用いずにすべての個人情報が対象、等。

アプリケーションから情報を取得することは、第 17 条の違反となる可能性があると指摘される。

17 ▪登録・届出を要しない電気通信事業の事例：他人の通信を媒介せず、かつ、電気通信回線設備を設置しない場合であり、事例として例えば各種情報のオンライン提供、ウェブサイトのオンライン検索、ソフトウェアのオンライン提供、ネット対戦ゲーム等がある。
・登録又は届出を要する電気通信事業の事例：加入電話、携帯電話、PHS、ADSL、FTTH、フリーメール　等
・いわゆるポータルサイト、SNS など様々なサービスを包含した総合サービスについては、それぞれのサービス毎に判断することとなる。

３　プライバシーの観点からの検討

プライバシーについて一般的に規定した法律はないが、判例法上、プライバシーは法的に保護されるべき人格的権利として承認されてきている。

「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」第二次提言（平成 22 年５月）において、行動ターゲティング広告等で一般に取得・利活用されるウェブページ上の行動履歴（閲覧履歴、購買履歴等）や位置情報は、他人にみだりに知られたくないと考えることは自然なことであり、その取扱いの態様によってはプライバシーに係る情報として法的保護の対象となる可能性があるとされている。

【プライバシーの権利】

プライバシー権とは、一般人の感受性を基準にして公表されたくない個人に関する情報を、みだりに第三者に開示又は公表されない権利であるとされる[18]。これを踏まえれば、アプリケーション提供者が、スマートフォン内の利用者情報のうち、①一般人の感受性を基準にして公表されたくない情報[19]を、②本人の同意又は正当な目的なしに、③アプリケーション提供者自身または情報収集モジュール提供者等が取得・外部送信することあるいはその他第三者に提供することは、プライバシー権の侵害に当たる可能性がある。

① 一般人の感受性を基準にして公表されたくない情報

スマートフォンにおける通信履歴、ウェブ上の行動履歴、アプリケーション利用状況の履歴、位置情報、写真やビデオなどの情報については、「一般人の感受性を基準にしてみだりに第三者に開示又は公表されたくない情報」に当たる可能性がある。個人識別性がなくとも、プライバシー保護の対象となる可能性があるとの議論があるため、注意して取扱う必要がある。

なお、位置情報については、適切に利用されることにより子供や高齢者の見守りや災害時における救助活動等利用者の安全・安心のために活用される場合がある一方、不適切に取得・利用されることはプライバシー上の懸念があり、場合によっては生命・身体・財産の安全を脅かすおそれもあることから、特別の配慮をもって扱う必要がある。

② 本人の同意又は正当な目的

一般に、本人の同意があればプライバシー権侵害に当たらない場合がある[20]が、どの

18　『宴のあと』事件判決（東京地判昭和 39 年 9 月 28 日）

19　スマートフォン内の利用者情報のうち、個人情報は「一般人の感受性を基準にして公開されたくない情報」にあたる可能性がある。また、個人識別性がなくとも、個人の人格と密接に関係する情報については、「一般人感受性を基準にして公開されたくない情報」にあたる可能性がある。

20　「プライバシー情報の収集について，本人の同意がある場合や，収集方法等に照らして定型的に推定的同意があると認められる場合には，人格的自律ないし私生活上の平穏を害する態様で収集されたということはできない。」（東京地判平成 22 年 10 月 28 日 客室乗務員 DB 事件）

ような場合に有効な同意が認められるか事案に応じて検討が必要である[21]。

また、正当な目的に基づく外部送信は、プライバシー権侵害に当たらない場合がある[22]。アプリケーションを利用するうえで、利用者情報の外部送信が当然必要な場合は、正当な目的があるといえる。例えば、位置情報サービスを提供するために、現在地を示す位置情報を外部送信することがこれに当たる。

③ 外部送信その他第三者への提供

さらに、第三者に送信することは「開示又は公表」に該当すると考えられる。アプリケーション提供者自身に送信することは、アプリケーション提供者による利用者情報の取得であって、「開示又は公表」とはいえないが、その場合でもプライバシー権侵害は生じ得る[23]。

アプリケーション提供サイト運営事業者は、直接的には、情報の送信等に関与しておらず、プライバシー権侵害の主体ではない。ただし、アプリケーション提供サイトにおいて、仮にプライバシー侵害を行うアプリケーションが多数販売されているような場合、アプリケーション提供サイト運営事業者は、ユーザーに対して注意喚起その他の義務を負うと解される可能性がある[24]。

【青少年の保護】

この他、青少年がスマートフォンを利用する場合の利用者情報の取扱いについては、青少年の利用実態や利用者情報が流出した場合のリスクの認識状況等を踏まえ、事業者が適切に取り扱う必要があるほか、保護者の役割やリテラシーの向上にも配慮する必要がある。

【個人の行動の詳細な把握】

また、利用者が十分認識できないところで、スマートフォンを経由して高精度の位置情報、アプリケーションの利用履歴、ウェブの閲覧や検索履歴等の様々な利用者情

---

21 アンドロイドOSによる利用許諾しか出ない場合には、送信されるかどうかは分からないので不十分ではないか、アプリケーション提供者独自の説明・許諾を出す場合内容が利用者にとって容易に分かるようにする必要があるのではないかとの指摘がある。

22 「本件原告ら各情報のうち原告らがその収集について同意したと認められないものについても，被告組合が正当な目的に基づいて収集したと認められる場合には，プライバシー侵害について違法性が阻却される場合があると解するのが相当である。」（脚注21，東京地判平成22年10月28日）

23 「第三者に知られたくない個人に関する情報をみだりに開示又は公表されないという利益が法的保護の対象となることの一環として，当該個人に関する情報をみだりに収集されないという利益，収集された当該個人に関する情報をみだりに保管されないという利益，及び，当該個人に関する情報をみだりに開示又は公表されないだけでなくみだりにその他の使用もされないという利益も法的保護の対象となると解するのが相当である。」（脚注21，東京地判平成22年10月28日）

24 インターネットオークションにおいて詐欺の被害が増加している場合に、オークション運営者は、ユーザーに対して注意喚起を行うべき義務を負うと判断した裁判例がある（名古屋地判平成20年3月28日（第一審）、名古屋高判平成20年11月11日（控訴審））。これは直接の売主ではない「場の管理者」も、「場」のユーザーの安全性について、一定の義務を負うという考え方である。

報が何らかの方法で統合して集積されることにより、個人の行動や私生活の内容について詳細な把握が可能となることが、プライバシー侵害につながる可能性もあることも指摘されている[25]。

スマートフォンの契約者・端末固有 ID は、契約や端末によって一義的に決まり、利用者側が変更することが困難である一方、様々なアプリケーション提供者等により取得され得るため、多くの事業者等が契約者・端末固有 ID をこのような統合の方法として用いる可能性があるとの指摘がある。

４　その他

不正指令電磁的記録に関する罪（いわゆる「ウィルス作成罪」）は、正当な理由がないのに、人の電子計算機における実行の用に供する目的で、人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録等を作成又は提供した場合等に適用される[26]ものであり、平成 23 年７月 14 日から施行されている[27]。

本条は正当な理由がないのに、人の電子計算機における実行の用に供する目的で、利用者の意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録を作成又は提供するものを対象としており、これに該当しない通常のアプリケーションやサービスの作成又は提供は適用対象とはならないと考えられる。一方、スマートフォン上のアプリケーション等の形式をとっていたとしても、利用者に何の説明もないまま、スマートフォンのアプリケーションやサービスの機能とは全く無関係に情報を漏洩するプログラムなどは「不正指令電磁的記録」に当たるとされる可能性もある[28]。

25　民間企業による情報集積とプライバシーに関する判例はまだないが、国による情報集積に関する判例としては、N システムによる情報集積（東京地判平成 13 年 2 月 6 日）がある。判例によれば、「車両を用いた移動に関する情報が大量かつ緊密に集積されると、車両の運転者である個人の行動等を一定程度推認する手がかりとなり得ることは否定できない。また、仮に、N システムの端末が道路上の至る所に張りめぐらされ、そこから得られる大量の情報が集積、保存されるような事態が生じれば、運転者の行動や私生活の内容を相当程度詳細に推測し得る情報となり、原告らの主張するような国民の行動に対する監視の問題すら生じ得るという点で、N システムによって得られる情報が、目的や方法の如何を一切問わず収集の許される情報とはいえないことも明らかである 」とある。

26 刑法（明治 40 年法律第 45 号）第 168 条の 2（不正指令電磁的記録作成等）において、「正当な理由がないのに、人の電子計算機
における実行の用に供する目的」で、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」等を「作成し、又は提供した者は、3 年以下の懲役又は 50 万円以下の罰金に処する。」と規定されている。

27 今年に入り、コンピューターウイルスを使い、他人から脅迫されているように見せかけた事件においてこの不正指令電磁的記録作成の容疑による裁判が開始された事例がある（産経ニュース平成 24 年 1 月 26 日「コンピューターウイルス作成罪を初適用　知人に送りつけた男を大阪府警が逮捕」http://sankei.jp.msn.com/west/west_affairs/news/120126/waf12012614060018-n1.htm））。

28 スマートフォンにインストールし起動すると電話帳に登録された名前や電話番号・メールアドレス等の情報をインターネット経由で外部に送信する複数のアプリケーションがアプリケーション提供サイトに掲載されていた問題についても、不正指令電磁的記録供用容疑による捜査が行われた事例がある（産経新聞平成 24 年 5 月 28 日「スマホアプリ個人情報流出問題　警視庁　IT 関連会社など捜索」他）。

第５章　スマートフォンにおける利用者情報の取扱いの在り方

本章においては、利用者がスマートフォンやそれを通じて提供される利便性の高いサービスを安全・安心に利用できる環境を整備するために、個人情報やプライバシーを保護しつつ関係事業者等[1]がスマートフォンにおける利用者情報を取り扱うための具体的な方針について検討を行う。

高度な情報処理能力が備わったスマートフォンは、様々なアプリケーションをインストールして多様な目的のために活用することが可能であり、第 1 章で考察したようなサービス構造の中で、スマートフォンの新たなサービスやイノベーションが生み出されてきている。一方、様々なアプリケーションがスマートフォンの中の利用者情報へアクセスを行い、利用者が自らの情報がどのように取得・利用されているのか十分理解することができなくなり、マルウェアやワンクリックウェア等も出現する中で利用者の不安感も高まっている状況である。

これまでも見てきたように、情報通信インフラとしてスマートフォンが急速に普及しつつある中で、ICT リテラシーが様々なレベルの利用者が増加してきている。利用者に一定の自己責任が求められるとしても、マルウェアやワンクリックウェアなどにより安全・安心な利用環境が損なわれる事案も発生しうる状況の中で、スマートフォン上の利用者情報の適正な取扱いに関する利用者の不安の解消は、一義的には関係事業者等の役割と責任においてなされるべきものと考えられる。

このため、スマートフォンにおける利用者情報を活用する関係事業者等は、利用者が個人情報やプライバシーの観点から安全・安心にサービスを活用できるように、利用者情報を適切に取り扱うとともに、利用者に対して分かりやすく透明性が高い説明を行い、その理解と有効な選択を促すことが求められている。

その基本的アプローチは、アプリケーションごとにプライバシーポリシーを策定するとともに、一定の情報の取得については、個別の情報の取得について同意取得を求めるというものである。この点において、個人情報保護法と異なる取扱いを部分的に採用しているが、これは、個人の人格・思想・信条等にもつながり得るプライバシーに関する情報が、非常に詳細なレベルで大量に保存されており、これらがアプリケーションを通じて自動的に取得され外部に送信され得るという、スマートフォンならではの特性を踏まえたものである。

また、スマートフォンのサービス構造において、多様な関係事業者等がサービス提供

[1] 関係事業者等：本提言における関係事業者等は、スマートフォンをめぐるサービス提供に関係している事業者等のことを指す。具体的には第 1 章図表 1-3 にあるように、①アプリ提供事業者・個人、②情報収集モジュール提供者、③アプリケーション提供サイト運営事業者・OS 提供事業者、④移動体通信事業者、⑤端末提供事業者、⑥広告配信事業者・情報収集事業者、⑦その他関係事業者（アプリ評価サイト運営者等）である。

や利用者情報の取扱いに係わっており、利用者が自らの情報の取扱いについてコントロールできる環境を整えていく上で、個別の事業者等のみでは対応できる範囲が限られる場合があるため、関係事業者等が連携し対応していくことが重要である。

このように、スマートフォンを安全・安心に活用できる環境を関係事業者等や業界団体自ら確保することが、スマートフォンにおけるイノベーションの継続的な創出や市場の中長期的な成長にもつながるものと考えられる。そのような認識の下、以下のスマートフォン利用者情報取扱指針を提示するものである。なお、関係事業者等及び業界団体は、個人情報保護法等の適用をはじめとしたスマートフォンにおける利用者情報の適切な取扱いについて、関係省庁の情報提供を必要に応じ受けることとする

１　スマートフォン利用者情報取扱指針

【総論】

（１）基本原則

スマートフォンは、一般に常時電源をオンにし、インターネットにも常時接続された状態で、利用者が常時携帯して利用する高機能端末という特性を有している。今まで見てきたように、電話帳などの第三者を含む個人情報、電話番号やメールアドレス等を含む利用者の個人情報、通信ログ、検索やウェブアクセス履歴といったインターネットの利用履歴、アプリケーションのダウンロード履歴、位置情報等の個人のプライバシーに係る情報など広範な利用者情報が存在している。

このようなスマートフォン特有の事情を踏まえ、スマートフォンやそれを通じて提供される利便性の高いサービスを利用者が安全・安心に利用できる環境を整備するためには、関係事業者等が利用者情報を適切に取り扱い、利用者のサービスへの信頼を確保することが必要である。個人情報保護法違反やプライバシー侵害等が成立するリスクを低減する観点からも、関係事業者等は利用者に対して透明性の高い分かりやすい説明を行い、利用者情報を適正な手段により取得する必要がある。

また、利用者の不安感等を軽減する観点から、適切な安全管理措置や苦情・相談への対応を講ずべきと考えられる。

さらに、今後大量の利用者情報の取扱いが可能となりこれを前提とする新たな技術やサービスの開発・提供が見込まれるが、そうした場合にはあらかじめプライバシーについて考慮した上でそのような開発・提供を行うべきである。

このような観点から、スマートフォンにおける利用者情報の取扱いについて、関係事業者等は下記のとおりの基本原則に従うことが望ましいと考えられる。

基本原則

① 透明性の確保

対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③ 適正な手段による取得の確保

関係事業者等は、対象情報を適正な手段により取得するものとする。

④ 適切な安全管理の確保

関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤ 苦情・相談への対応体制の確保

関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥ プライバシー・バイ・デザイン

関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。

利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

（２）本指針の適用対象

本指針は、アプリケーション等を通じてスマートフォン上の様々な利用者情報が外部に送信され活用されている現状に鑑み、アプリケーション提供者を中心として、スマートフォン上の利用者情報の取扱いに係るあらゆる関係事業者等に対し、それぞれの役割に応じた形で適用されることを想定している。

具体的な適用対象は、アプリケーション提供事業者・個人（以下「アプリケーション提供者」という。）、情報収集モジュール提供者、アプリケーション提供サイト運営事業者・OS 提供事業者、移動体通信事業者、端末提供事業者、広告配信事業者・情報分析事業者、その他関係事業者（アプリケーション評価サイト運営者等）等が想定される。なお、関係事業者等及び業界団体は、個人情報保護法等の適用をはじめとしたスマートフォンにおける利用者情報の適切な取扱いについて、関係省庁の情報提供を必要に応じ受けることとする。

とりわけ、アプリケーション提供者は、大企業からベンチャー企業、個人に至るまで多様であり、業界団体に加入していない者も多い。本指針は、このような者も含め、関係事業者等が直接参照して適切な対応を行うことができるためのものとして提示されている。もとより、各業界団体が業界の実情を踏まえ、追加的な事項を盛り込む等してガイドライン等を作ることも期待される。

なお、これら事業者であっても、スマートフォン上の利用者情報を、外部送信や蓄積を伴わない形で、スマートフォン内において一時的に取得・利用するのみの場合には、本指針の適用対象として想定していない[2]。

（３）用語の定義

① 関係事業者等：

スマートフォンをめぐるサービス提供に関係している事業者等。具体的には、①アプリケーション提供事業者・個人、②情報収集モジュール提供者、③アプリケーション提供サイト運営事業者・OS提供事業者、④移動体通信事業者、⑤端末提供事業者、⑥広告配信事業者・情報収集事業者、⑦その他関係事業者（アプリ評価サイト運営者等）のこと。

② アプリケーション提供者等：

アプリケーション提供者及び情報収集モジュール提供者等。

---

[2] なお、利用者の端末内部で一時的にアクセスするのみであっても、OS による利用許諾について取得・表示される場合がある。このため、利用者の理解を助け透明性を高めるためには、例えば「端末内部で○○の目的のための一時的に使用し、蓄積や外部送信をしない」等を利用者に通知又は公表することも有用である。

③ スマートフォンにおける利用者情報：

利用者の識別に係る情報[3]、電話帳等の第三者に関する情報、利用者の通信サービス上の行動履歴、利用者の状態に関する情報など、スマートフォンにおいてスマートフォンの利用者と結びついた形で生成、利用、蓄積されている情報の総称。

④ 情報収集モジュール：

スマートフォン等に蓄積された様々な情報を収集する機能を持つ、アプリケーションに組み込んで利用される一連のプログラムのこと。

⑤ プライバシーポリシー：

アプリケーション提供者等が個人情報等を取り扱う上での考え方や方針を明らかにする文書。

本指針においては、スマートフォンにおいて提供されるアプリケーションや情報収集モジュール等について、具体的な取得情報の項目、利用目的等を記載したものを想定している。

⑥ 通知又は公表：

「通知」は、一般に書面（郵送等）、電子メール、ファクシミリ、口頭（電話等）等のいずれかの方法で伝えること。「公表」は、一般には官報・公報・新聞紙等への掲載、インターネット上での公表、パンフレットの配布、窓口等への書面の掲示・備付等のいずれかの方法により公にしておくこと（スマートフォンの場合、通知は書面、電子メールやアプリによるポップアップ等、公表はアプリケーション上あるいはウェブサイト等へのリンクを示すこと等により行うことが想定される。）。

⑦ アプリケーションに関する同意取得：

アプリケーション等に係るプライバシーポリシー等に基づき、アプリケーションの利用者情報の取得や取扱いについて一括して同意を取得すること。

⑧ 個別の情報に関する同意取得：

アプリケーション等により取得される個別の情報（電話帳、位置情報等）について、取得や取扱いについて独立した形で同意を取得すること。

---

[3] 第４章 図表 4-2（44～45 頁）における「利用者の識別情報に係る情報」をいう。

【各論①：スマートフォンにおける利用者情報を取得する者における取組（アプリケーション提供者、情報収集モジュール提供者、広告事業者等）】

（１）プライバシーポリシーの作成

スマートフォンにおける利用者情報を取得しようとするアプリケーション提供者、情報収集モジュール提供者（これらを提供する広告事業者等を含む）は、個別のアプリケーションや情報収集モジュール等について、以下の①から⑧までの事項について明示するプライバシーポリシー等をあらかじめ作成し、利用者が容易に参照できる場所に掲示またはハイパーリンクを掲載する。

① 情報を取得するアプリケーション提供者等の氏名又は名称

- アプリケーション提供者等の名称、連絡先等を記載する。

② 取得される情報の項目

- 取得される利用者情報の項目・内容を列挙する。

③ 取得方法

- 利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等を示す。

④ 利用目的の特定・明示

- 利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。
- 広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤ 通知・公表又は同意取得の方法、利用者関与の方法

- 通知・公表の方法、同意取得の方法：プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。
- 利用者関与の方法：利用者情報の利用を中止する方法等を記載する。

⑥ 外部送信・第三者提供・情報収集モジュールの有無

- 外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦ 問合せ窓口

- 問合せ窓口の連絡先等（電話番号、メールアドレス等）を記載する。

⑧ プライバシーポリシーの変更を行う場合の手続

- プライバシーポリシーの変更を行った場合の通知方法等を記載する。
  （当初取得した同意の範囲が変更される場合、改めて同意取得を行う。）

（２）プライバシーポリシーの項目に関する説明

④利用目的の特定・明示

- 利用者情報を、アプリケーション自体の利用者に対するサービス提供（提供するサービス概要を簡単に記載）のために用いるのか、それ以外の目的のために用いるのかをまず明確に記載する。
- アプリケーション自体が利用者に提供するサービス以外の目的のために利用する場合については、利用者が利用目的や利用方法を容易に想定できないことから、利用目的と取得される情報の項目の関係について丁寧な説明を行うこととする。例えば、「利用者のエクスペリエンスの向上」等の記載のみでは、アプリケーション自体の機能向上、広告表示、マーケティング等のいずれを目的とするのか把握困難であるため利用目的を十分特定するとはいえない。
- 広告配信・表示やマーケティング目的のために利用者情報の取得を行う場合には、その旨の目的を明示する。利用者に対してターゲティング広告等の配信を行う場合にはその旨記載する。第三者である他の情報収集者等へ情報を提供する場合にはその旨を明示する。
- 現段階では利用目的が明確ではなく、将来的な活用を見込んで利用目的の範囲を定めず様々な利用者情報を取得することは、利用目的が特定されているとはいえないため、適切ではない。想定される利用目的の範囲できるだけ特定し利用者に通知又は同意取得をした上で、その範囲で情報を取得し取り扱う。

⑤通知・公表又は同意取得の方法、利用者関与の方法

◎ 通知・公表又は同意取得の方法

[一般的な取扱い]

- プライバシーポリシーを定め公表するとともに、アプリケーションをダウンロードしようとする者が容易に参照できる場所に掲示又はリンクを張る。
- アプリケーションをダウンロードしようとする者がスマートフォンの画面上で容易に理解できるように、プライバシーポリシーの分かりやすい概要を作成して利用者が容易に参照できる場所に掲示又はリンクを張ることが望ましい（概要から詳細なプライバシーポリシーへリンクを張る方法なども有用である）。
- プライバシーポリシーによる通知・公表又は同意取得は、原則として利用者がアプリケーションをダウンロードあるいはインストールしようとする際に行うこととする。それらの時点で行うことが難しい場合には、初回起動時に処理が実行される前に行うものとする。

- 特に同意取得を要する利用者情報については、アプリケーションをダウンロードあるいはインストールする際、初回起動時に処理が実行される前など、当該情報を取得するための処理が実行されうる前に同意取得が行われるように設計する。

- アプリケーションに関するOSによる利用許諾は一般にアプリケーションがどのような情報にアクセスするかを示しているが、利用目的や外部送信・第三者提供の有無等の項目の記載がない場合には、OSによる利用許諾単体のみでは本項に示す通知又は同意取得として十分ではない[4]。
  OSによる利用許諾が表示される際に別途[5]アプリケーション提供者が作成したプライバシーポリシーのリンク先を示すなどの方法により通知・公表を行うか、必要に応じて個別の情報についての同意取得等を行うことが適切である。

[同意取得等を要する利用者情報の取扱い]

スマートフォンに蓄積され、アプリケーションを通じて外部に自動的に送信され得る利用者情報であって、プライバシー性が高いと考えられる情報のうち、現状の利用実態を踏まえ代表的なものの取扱いについて、以下のとおり個別に記述する。

- 個人情報を含む電話帳などについては、目的に応じ必要とされる範囲（フィールド）を限定するとともに、プライバシー侵害を回避する観点から個別の情報を取得することについて同意を取得する[6]。

- アプリケーションが提供するサービス[7]への利用以外の目的で、個人と結びつきうる形でGPSの位置情報などを取得する場合については、プライバシー侵害につながらないよう原則として個別の情報を取得することについて同意を取得する。

- 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得については、通信相手等の個人識別性を有する場合があること、通信の内容を含むプライバシー上の懸念が想定されることから、個別の情報を取得することについて同意を取得する。

---

4 OS の利用許諾等において、実際に取得される情報の項目及び利用目的等が具体的に記載されるような形式がとられた場合等には、当該利用許諾により通知・同意を行う可能性もある。

5 現在も、利用許諾を表示する際に合わせて表示される自由記入欄にプライバシーポリシーを表示することも一案と考えられる。

6 その場合であってもこれら情報は一方当事者の同意のみしか得られていないため、利用者の一定の責任を免れない場合もあると考えられる。

7 原則として位置連動型の広告はアプリケーションが提供するサービスとは別と認識される。
一方、例外的に、位置連動によるクーポン等を取得することそのものを目的としているアプリケーションであって、利用者が位置情報を取得することによりクーポンを付与されることを理解しそのサービスを利用している場合には、アプリケーションが提供するサービスと考えられる可能性がある。

- スマートフォンのアプリケーションの利用履歴[8]やスマートフォンに保存された写真・動画については、アプリケーションによるサービス提供のために必要な範囲で用いられる場合を除き、プライバシー上の懸念が想定されるため、その取得に当たっては個別の情報に関する同意を取得する。
- 契約者・端末固有ID[9]など、契約や端末に対して一義的に指定・作成され、利用者側で変更が困難であるが、幅広い主体により利用される可能性[10]があるものが取得者において個人識別性を有する情報と結びつきうる形で利用される場合、同一IDの上に様々な情報が時系列的に蓄積し得ること、取得者又は第三者において個人識別性を有する可能性があることから、個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱うことが適切と考えられる[11]。具体的には、取得される項目及び利用目的を明確に記載し、その目的の範囲内で適正に扱うこととする。

（参考）

アプリケーションや情報収集モジュールの目的に応じ、プライバシーを保護する観点から、利用者が事後的に変更しうるIDやアプリケーション独自のID等の代替手段の利用について検討を行うことが有用であると考えられる[12]。

◎　利用者関与の方法

- 利用者情報の利用を中止してほしい場合に、アプリケーションそのものをアンインストールする以外に方法がない場合はその旨記載する。アプリケーションを使用しながら、情報の取得が中止される方法がある場合、あるいは情報の取得は継続されるがその利用が中止される方法がある場合には、そのいずれであるかが分かるようにして記載するものとする。
- 一度利用者が同意を行った場合に、後から同意撤回などの変更が可能となる機会についてもできるだけ提供するよう努める。

---

8 アプリケーションの品質向上等のために当該アプリケーションの利用履歴等を活用することは、アプリケーションにより提供されるサービス提供の一環と考えられるため、プライバシーポリシー等に明示しアプリケーションに関する同意の取得又は通知を行うことで可能である。一方、他アプリケーションの利用履歴等については、個別の情報に関する同意を取得することが望ましい。

9 OS が生成する ID（Android ID）、独自端末識別番号（UDID）、端末識別 ID（IMEI）、加入者識別 ID（IMSI）、SIM シリアル ID（ICCID）、MAC アドレス等のことを指す。

10 アンドロイド OS において、Android ID のアプリケーションによる取得は利用許諾不要である。READ_PHONE_STATE という利用許諾を取得することにより、加入者識別 ID（IMSI）、SIM シリアル ID（IC Card ID : ICCID）、端末識別 ID（IMEI）等が取得可能。ACCESS_WIFI_STATE という利用許諾を取得することにより、Wi-Fi 等の無線通信確立のためにネットワーク機器に割り当てられている MAC（Media Access Control）アドレスが取得可能。

11 端末内において一時的に利用し蓄積しない場合は除く。

12 UDID 等の契約者・端末固有 ID の代わりとして、利用者が望む時に端末の交換や契約内容の変更等を行うことなく異なる ID を付与しうるものとして、UUID や OpenUDID 等の検討が開始されている。

- 利用者に関する情報が、プライバシーポリシーに反して取得され、取り扱われていることが明確である場合などについては、利用者からの申出を受け利用の停止又は消去を行うものとする。

⑥外部送信・第三者提供・情報収集モジュールの有無

［第三者提供する場合の取扱い］

- アプリケーション提供者や情報収集モジュール提供者等が取得した利用者情報を第三者提供する場合[13]、あらかじめ本人の同意を取得する。
- この場合、①第三者への提供を利用目的とすること、②第三者に提供される利用者情報の項目、③第三者への提供の手段又は方法についてそれぞれ明確にプライバシーポリシーに記載することとする。
- アプリケーションに関するOSによる利用許諾により「アプリケーションが当該情報にアクセスする権限」に対する同意（許諾）を得たとしても、「利用目的」、「利用者情報の外部送信」及び「第三者提供」について説明がない場合には、単体では第三者提供に係る同意取得の条件を満たしているとはいえない。

（参考：委託する場合）

利用者情報の取得者が、利用目的の達成に必要な範囲内において、利用者情報の取扱いの全部又は一部を外部委託することは第三者提供には該当しない。ただし、この際、委託先における利用者情報の取扱いの安全管理についても監督責任を負う。

［情報収集モジュールを組み込む場合の取扱い］

- アプリケーション提供者が情報収集モジュールを組み込む場合、アプリケーションを通じた情報収集の実態について明らかにする上で、アプリケーション提供者は、自らが組み込んでいる情報収集モジュールの数、名称、提供者等の基本的な情報について、利用者に対して説明する[14]。
- 具体的には、アプリケーション提供者は、アプリケーションに情報収集モジュールを組み込んでいる場合、アプリケーションのプライバシーポリシーにおいても、①組み込んでいる情報収集モジュールの名称、②情報収集モジュール提供者の名称、③取得される情報の項目、④利用目的、⑤第三者提供の有無等[15]について情

13 個人識別性を獲得し得ない匿名化された情報を統計処理した結果などを第三者に提供する場合を除く。

14 これらの情報についてアプリケーション提供者を通じて提供されない限り、利用者は自らが利用するアプリケーションに組み込まれているか知ることは困難であり、それゆえ当該情報収集モジュールのプライバシーポリシーを参照することも困難であると指摘される。

15 情報収集モジュールにより③取得される情報の項目、④利用目的、⑤第三者提供の有無等について、情報収集モジュールのプライバシーポリシーやウェブサイト等に明示されている場合、そのリンク先等を

報収集モジュールごとに記載するとともに、各情報収集モジュール提供者のプライバシーポリシーにリンクを張るなどして容易に見られるようにする。

⑦問合せ窓口

- 利用者情報を取得する者は、利用者情報の取扱いに関する苦情や相談の適切かつ迅速な処理に努める。具体的には、苦情相談窓口・連絡先を設置するなど必要な体制の整備に努める。

（３）適切な安全管理措置

- 取り扱う利用者情報が漏えい、滅失又はき損の危険にさらされることがないように、利用者情報の安全管理のために必要かつ適切な措置を講じるものとする。
- 利用目的に必要な期間に限り保存し、目的達成等により不要となった際には、適切に消去等の措置を行うものとする。
- 利用者がアプリケーションをアンインストール等したことが判明した後のデータの保存期間、その後の処理等についてあらかじめ定めておくものとする。

（４）情報収集モジュール提供者に関する特記事項

- スマートフォンから利用者情報を収集する情報収集モジュール提供者は、（１）～（３）を踏まえ、それぞれプライバシーポリシーを定め公表するものとする。
- 情報収集モジュール提供者は、当該情報収集モジュールを組み込もうとするアプリケーション提供者へ①取得する情報の項目、②利用目的、③第三者提供の有無等について通知する。
  これら内容について変更があった場合はプライバシーポリシーを更新するとともに、重要な変更があった場合にもアプリケーション提供者へ通知するものとする。

（５）広告配信事業者に関する特記事項

- 広告配信事業者は、スマートフォンからアプリケーションや情報収集モジュールにより利用者情報を取得する場合、アプリケーション提供者や情報収集モジュール提供者として（１）～（３）をふまえそれぞれプライバシーポリシーを定め公表するものとする。
- 行動ターゲティング広告を行う場合には、「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」の第二次提言における「配慮原則」を踏まえて作成された自主的なガイドラインを本指針を踏まえて見直したもの等に基づき行う。

示すことにより代えることも可能。

【各論②：関係事業者における取組】

適切な取扱いや利用者における安全・安心の向上のために、各論①におけるアプリケーション提供者及び情報収集モジュール提供者以外の関係事業者についても、基本原則や指針（総論）等を考慮しつつ、以下のような取組をそれぞれの立場で、また相互に協力しつつ進めることが望ましい。

（１）移動体通信事業者・端末提供事業者

- スマートフォン販売時等に、既存チャンネルを通じて利用者に必要事項を周知する。（例えば、従来の携帯電話との違い[16]、情報セキュリティやプライバシー上留意すべき点等の周知等）
- 移動体通信事業者のアプリケーション提供サイトにおいて、アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促す。プライバシーポリシー等の表示場所[17]を提供するなど、アプリケーション提供者等に対し、適切な対応を行うように支援する。必要に応じ関係事業者や団体等とも協力しつつ、アプリケーション提供者や情報収集モジュール提供得者等に対し啓発活動を進める。
- 説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応を検討するとともに、連絡通報窓口を設置する。
- 今後「利用者」として増加する可能性があるのは、現在スマートフォンを使いこなしている層に加えて、ICTリテラシーに乏しい消費者、高齢者等と考えられることから、リテラシーに応じたスマートフォンの機器やサービス設計、周知啓発活動を移動体通信事業者は端末提供事業者との協力も考慮しつつ検討する。

（２）アプリケーション提供サイト運営事業者、OS提供事業者

- アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促す。
- プライバシーポリシー等の表示場所を提供するなど、アプリケーション提供者等に対し、適切な対応を行うように支援する。
- 必要に応じ関係事業者や業界団体等とも協力しつつ、アプリケーション提供者や情報収集モジュール提供者等に対し啓発活動を進める。

---

16 水平分業モデルでPCと類似した自由度があるが、マルチステークホルダーで自己責任リスクがあるスマートフォンの違いを十分周知する必要がある。

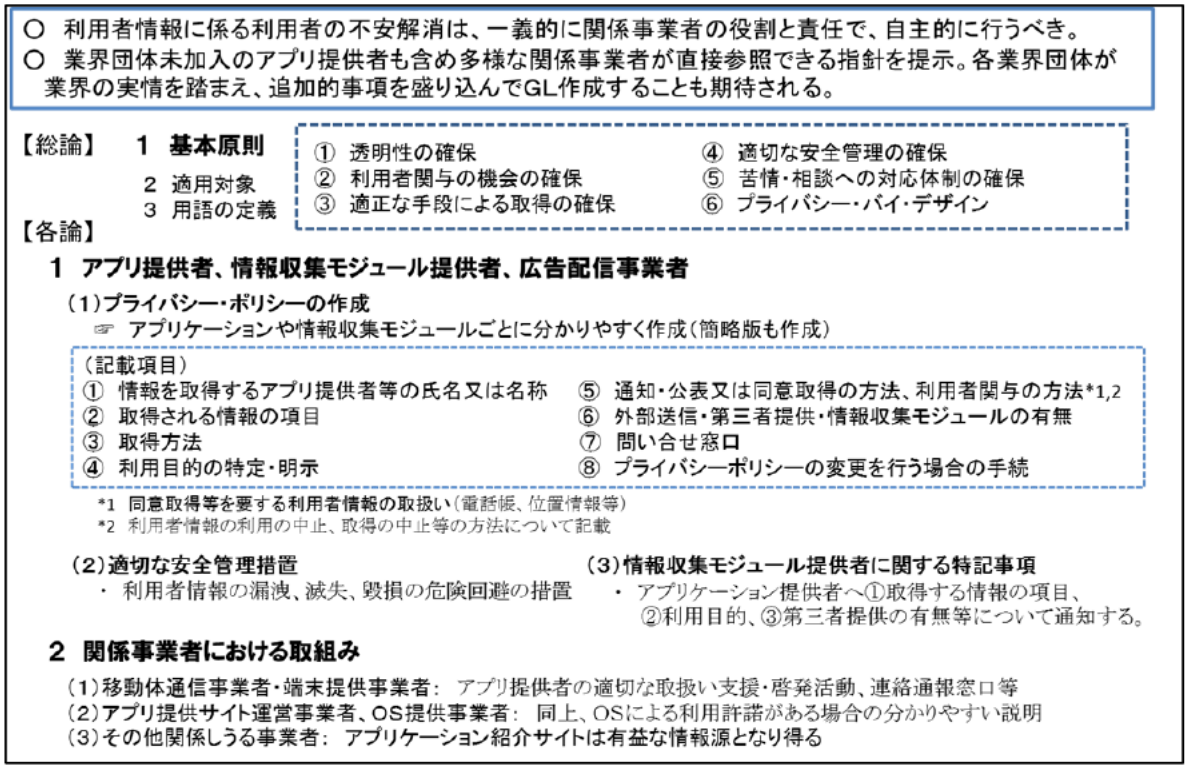
17 プライバシーポリシーが掲載されているウェブサイトのURLを掲載しハイパーリンク可能とする場所を用意する方法や、プライバシーポリシーの全文を記載できる場所を用意する方法が例えば考えられる。

- 説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応を検討するとともに、連絡通報窓口を設置する。
- OSによる利用許諾がある場合、利用者に分かりやすい説明を行う努力を継続する。目的に応じ注意すべき利用許諾等がある場合、利用者が安全に利用できるための方策を検討する。

（３）その他関係しうる事業者

- 独自の基準に基づきアプリケーションの推薦等をしているアプリケーション紹介サイトは利用者がアプリケーションを選択する上での有益な情報源となる場合がある。
- アプリケーション紹介サイト等関係する事業者は、可能な限りプライバシーポリシー概要の掲載等を検討したり、説明や情報取得の方法が適切でないアプリケーションが判明した場合の対応を検討するなど、基本原則や指針等を考慮しつつ、望ましい取組を協力して進めることが期待される。

【図表5-1：　スマートフォン利用者情報取扱指針の全体構造】



２　指針の実効性を上げるための様々な取組み

（１）業界団体によるガイドライン作成

各業界団体は、本指針がスマートフォンにおける利用者情報の取扱いに関する共通的事項を記載したものであることを踏まえ、必要に応じ、関係省庁の情報提供も受けつつ、各業界の実情を踏まえて必要な事項を追加的に盛り込む等した業界ガイドライン及び必要な場合はプライバシーポリシーのモデル例を作成し、これに沿った活動を進めることが期待される。

（２）アプリケーション提供者等への情報発信

アプリケーション提供サイト運営事業者や業界団体等がアプリケーション提供者、情報収集モジュール提供者に向けて、指針や業界ガイドラインを考慮し、個人情報やプライバシーに配慮した適切な利用者情報の取扱いを進めるように情報発信を行っていくことが望ましい。

例えば、アプリケーション提供サイト運営事業者や業界団体等が、利用者のプライバシーへの配慮に関する事項を盛り込んだ形でアプリケーションの設計やコーディング等に関するガイド等を作成・公表し、アプリケーション提供者や情報収集モジュール提供者となりうる者へ周知しこれを参照可能とすることも有用である。また、アプリケーションの作成を取り扱っている専門学校等の生徒への講義も有用である。

（３）スマートフォン画面を考慮した表示

業界団体及びアプリケーション提供者等は、スマートフォンの画面上において、利用者の利便性を損なわないように必要かつ十分な情報を提供するために、重要な情報を簡易に取りまとめた上で利用者に示すための方策を検討する。

（４）第三者によるアプリケーション検証の仕組みの検討

本指針や業界団体のガイドラインに沿って、アプリケーション及び情報収集モジュールごとの適切なプライバシーポリシーの作成・運用等利用者情報の適切な取扱いがなされることが期待されるが、実際に個々のアプリケーション等について、適切な取扱いが行われているかどうか等を、運用面・技術面から第三者が検証する仕組み[18]が民間主導により整えられることが望ましいと考えられる。

このような仕組みが整えられた場合、アプリケーション提供者においては、例えばあらかじめその提供するアプリケーションについて、本指針等に沿った適切な取扱い

18 具体的には、①アプリケーション等のプライバシーポリシーの有無、②当該プライバシーポリシーの妥当性、③アプリケーション等の実際の動作が当該プライバシーポリシーの表示内容に合致しているかどうか等を専門的に検証・確認することが求められ、そのためには、審査基準をはじめとした運用方針の策定や技術的な検証を行い、その結果を公表したり、マーク等により表示することが考えられる。

を行っていることの確認を申し出、確認が得られれば、その旨を表示することにより、当該アプリケーションに対する利用者の信頼向上につながるものと考えられる。

また、利用者にとっては、上記確認がなされたアプリケーションについては、何らかのマーク等によって分かりやすく表示されれば、利用者情報を適切に取り扱っているアプリケーションを容易に判別できることとなると考えられる。

さらに、あるアプリケーション又は情報収集モジュールについて、利用者情報を適切に扱っていないのではないかとの疑いがある場合、このような検証の仕組みに対して通報できることとなれば、利用者が安心して利用できる環境の整備に資すると考えられる[19]。

このような、アプリケーションの検証スキームの検討にあたっては、アプリケーション検証の位置づけ、検証対象となるアプリケーションの範囲等を含めた様々な課題・論点について検証しつつ、利用者情報の取扱いとマルウェア対策について関係者が連携し実効性のある仕組みを検討することが望ましい。

（５）関係者の取組状況に関するフォローアップ

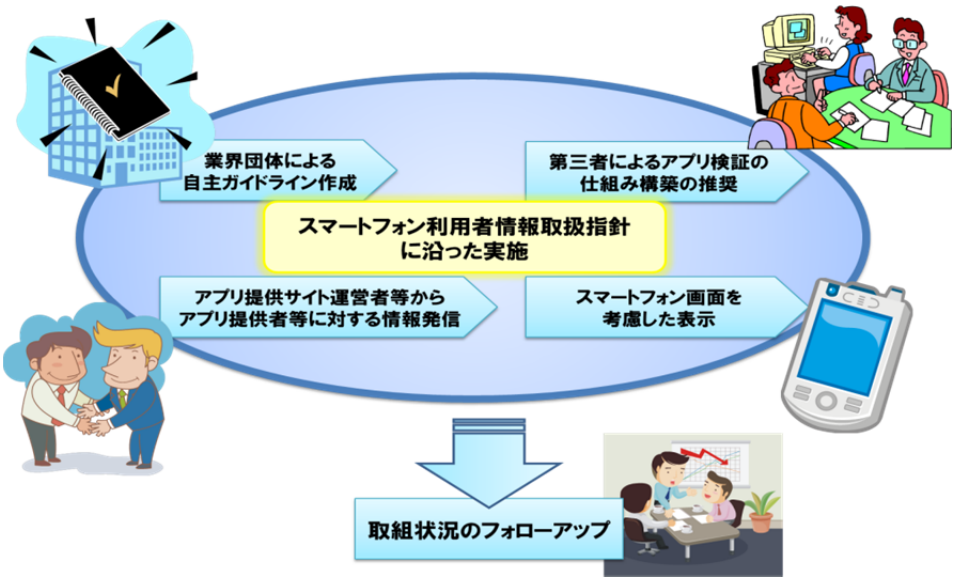
急速に普及するスマートフォンのサービスと市場の健全な発達を推進するため、関係事業者等、業界団体、関係省庁等が連携・協力しつつ、早急に安全・安心な利用環境の確保に向けて取り組むことが重要である。そのためにも、関係事業者等やガイドラインを作成した業界団体において、指針を踏まえプライバシーポリシーの策定等の自主的な取組を推進するとともに、取組状況等について自らフォローアップを行い、必要に応じその結果を公表することが期待される。

また、指針等を踏まえた関係事業者等や業界団体における取組状況等について、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等の適切な場[20]において、一定期間の後にフォローアップを行い、利用者情報及びその取扱いについて状況を把握するとともに、客観的なデータについても把握に努め、将来に向けた対応の在り方について必要に応じ検討を行うこととする。

19　スマートフォンのアプリケーションにおけるマルウェアや、マルウェアには直ちに該当しなくとも、利用者情報を適切に取り扱っていないおそれのあるアプリケーション等について、危険・注意情報を収集し、関係者内で共有するとともに、利用者に対しても必要な情報を分かりやすく発信することも併せて期待される。

20 その他関係省庁の各種会合等も含まれる。

【図表5-2：　指針の実効性を上げる取組】



３　今後の技術・サービスの進展に対する柔軟な対応

本章 1(1)（基本原則）及び２（スマートフォン利用者情報取扱指針）においては、アプリケーションをダウンロードしてその提供するサービス等を利用する場合の利用者情報の取扱いについて論じてきた。

他方、既にスマートフォンやタブレッド端末などのウェブ・ブラウザ（ウェブ閲覧ソフト）はほぼ全て HTML5 と呼ばれるプログラム言語に対応するブラウザとなっており、今後のスマートフォンの利用においてアプリケーションの代わりに HTML5 のウェブブラウザを通じて、コンテンツにアクセスしたりサービスを利用したりすることが普及するとの指摘もある[21]。

アプリケーションの場合、それをあらかじめダウンロードすることを前提とし、サービスを利用する際にはアプリケーションのアイコンをタップするだけで直ちに利用できる一方、利用者側での適時のアップデートを要する。これに比較して、HTML5 に対応したブラウザの場合は、ブラウザを使ってコンテンツにアクセスするため利用者側でのアップデートの手間が軽減されいつでも最新の情報を利用できる[22]。

利用者情報の取扱いについては、アプリケーションの場合、第２章において見たようにスマートフォンにおける大半の利用者情報にアプリがアクセス可能であることから、プライバシー上の問題等が生じうる。一方、HTML5 に対応したブラウザを通じた情報閲覧やサービス利用の場合、スマートフォン上の利用者情報へのアクセス権限が少ないた

21　スマートフォンを経由した利用者情報の取り扱いに関する WG 発表資料（第 6 回会合　株式会社エル・カミノ・リアル代表取締役　木寺祥友氏資料）

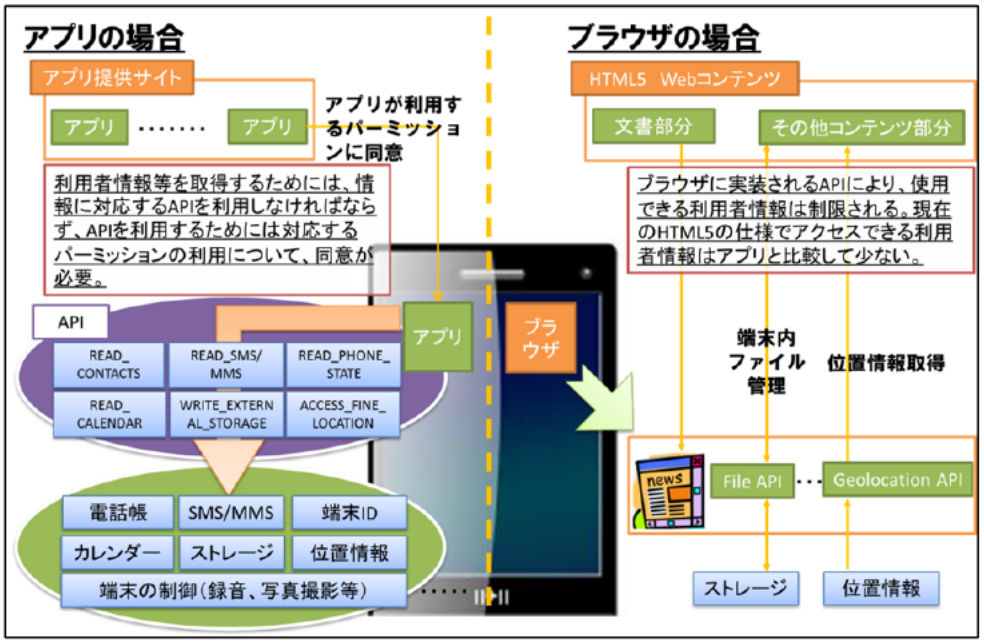
22　一定程度端末のローカル部分にデータを保存しオフラインで活用することも可能である。

めプライバシー上の問題等は生じにくいとされる[23]。このため、HTML5 に対応したブラウザを通じたサービス利用が普及した場合[24]、これまで検討してきた利用者情報の取扱いの中の課題の一部については技術的に解決できる可能性も指摘される[25]。

今後、スマートフォンをめぐり新しい技術やサービスが導入され普及が進む際にも、本章で検討を行った「基本原則」を踏まえ、スマートフォンにおける利用者情報の取扱い等について透明性が確保され、利用者関与の機会を付与しつつ、適切に取り扱われることにより、利用者が安全・安心にこれら技術やサービスを活用できる環境が確保されることが重要である。また、関係事業者等は技術やサービスの設計段階から、「プライバシー・バイ・デザイン」の視点を取り入れていくことも期待される。

また、業界団体や関係事業者等により、新しい技術やサービスの導入や普及の動向に応じて、「基本原則」の考え方などを踏まえつつ、利用者情報の取扱い等を検証し柔軟に必要な対応を行っていくことが望ましいと考えられる[26]。

【図表 5-3： アプリケーション及びブラウザがアクセス可能な情報等の違い】



23 スマートフォンにおける利用者情報は、HTML5 を用いたブラウザからはアクセスできない領域にあると指摘される（第 6 回会合　木寺氏資料）。

24 HTML5 によるブラウザーベースのサービス提供の普及については、それが主流になっていくとする見方があるとともに、利用するサービス・閲覧する情報の内容によってアプリケーション利用と棲み分けとなるとする見方等もある。なお、米国 IDC 社の調査によれば、モバイル分野の開発者の間で HTML5 への注目が増しており、79%の開発者が今年のモバイルアプリ開発に HTML5 を採用すると回答したとされる（2012 年 3 月 20 日、http://www.idc.com/getdoc.jsp?containerId=prUS23388912）

25 「今後 PC 版のブラウザでも HTML5 が主流になりつつあり、PC のブラウザに対するセキュリティ対応がそのままスマートフォンでも生かされる」（第 6 回会合　木寺氏資料）

26 具体的にアプリケーションの場合を念頭においた「指針」は新しい技術において当てはまらない部分も出てくる可能性はある。今後、フォローアップにおいて、新たな技術の導入及びその普及の進展及び必要度合いと、利用者情報の取扱い上の課題の有無などを把握に努めるものとする。

第６章　利用者に対する情報提供・周知啓発の在り方

１　基本的考え方

従来、携帯電話は、日常生活に不可欠なものとして、国民の間に深く浸透してきた。今後、スマートフォンの普及が進展し、従来の携帯電話に置き換わっていくことも想定される現状に鑑みれば、スマートフォンは高度なリテラシーを有する一部の者のみが利用できるものではなく、青少年及び高齢者を含めた国民が広く利用できるものであるべきと考えられる。

このことを踏まえると、スマートフォンをめぐるサービスを提供する関係事業者等は、まず、前章で論じた「スマートフォン利用者情報取扱指針」を参照し、適切な対応を行うことが望ましい。加えて、関係事業者等は、自らが関わるサービスについての知見を有することから、自らの責任として、利用者への情報提供・周知啓発[1]により、利用者のリテラシーの向上を図っていくことが重要である。その際、利用者がスマートフォンを利用するに当たって抱いている不安等の解消や、同意のない個人情報の外部送信及びプライバシーの侵害、それらから生ずる二次被害といったリスクの軽減に向けてできるだけ努力をすることが肝要である。

なお、スマートフォンは自由にアプリケーションをダウンロードして利用するサービスであり、利用者に自己責任が求められる側面があることを考慮すると、利用者リテラシーの向上のためには、利用者自身による能動的な情報収集も重要である。

（１）関係事業者等による利用者への情報提供・周知啓発

①　情報提供・周知啓発を行う主体

スマートフォンをめぐっては、マルチステークホルダーによるサービスが提供されていることから、アプリケーション提供者、情報収集モジュール提供者、アプリケーション提供サイト運営事業者、OS提供事業者、移動体通信事業者、端末提供事業者、広告配信事業者等関係する事業者・団体等のそれぞれにおいて、利用者に対する情報提供・周知啓発に取り組むことが求められる。また、国における取組も必要であるほか、②で挙げる青少年及び高齢者への情報提供・周知啓発に当たっては、上記主体のみならず、学校等の教育機関、PTA、消費者団体、PCに係る高齢者向けボランティア団体、地方自治体、更にはこれらに加えて関係事業者等が参加する安心ネットづくり促進協議会（会長：堀部政男一橋大学名誉教授）[2]等と連携し、地域社会における情報提供・周知

---

1 本章における「情報提供」の「情報」とは、前章までの検討に係る「利用者情報」ではなく、利用者のリテラシーを向上させるためのスマートフォンに関する一般的な情報をいう。

2 青少年が安全安心にインターネットを利用できる環境を整備するため、2009 年（平成 21 年）2 月に設立された、利用者・産業界・教育関係者等の相互連携を図る民間の協議体。「1 億人のネット宣言　もっとグッドネット」のキャッチフレーズの下、普及啓発イベントや、青少年保護に係る諸問題についての

啓発体制の強化を意識した活動を行う事が望ましい。

② 情報提供・周知啓発を行う対象

今後一層のスマートフォンの普及・進展が見込まれる現状においては、あらゆる世代への情報提供・周知啓発が求められるところであるが、とりわけリテラシーが未成熟である青少年[3]及びスマートフォンの利用率が低い高齢者に対し、その利用実態や特有の事情を踏まえた形での情報提供・周知啓発が重要である。

このうち、青少年については、本年2月、経済協力開発機構（OECD）において「オンライン上の青少年保護に関する理事会勧告」[4]が採択されている。インターネットの利用を前提とするスマートフォンについては、本勧告を踏まえた青少年保護のための施策が重要であり、意識の向上及び教育の促進のための取組等が必要と考えられる。取組に当たっては、青少年は、スマートフォンの機能等は理解し、使いこなす傾向にあるものの、同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクや、同意することの意味についての理解が不足していると考えられる。保護者の責任と役割を十分踏まえ、その保護を図る視点が重要である。

他方、高齢者については、年齢別のインターネット利用率、特にスマートフォンによるインターネット利用率が高齢者になるほど減少する傾向がみられる現状に鑑みれば、スマートフォンの普及によって従来のICT利用環境がより大きく変化し得るため、そのことも踏まえた情報提供・周知啓発が必要と考えられる[5]。その際、高齢者は、上記のリスク等については意識していると考えられるが、スマートフォンの機能等の理解不足や画面に表示される文字が小さいこと等によって利便性の享受が妨げられていると考えられるなど、利用者情報の取扱いの観点のみならず、利用を支援する観点からの情報提供・周知啓発が重要である。

③ 情報提供・周知啓発を行う方法

総務省調査（図表2-9、第2章参照）によれば、アプリケーションの通知・同意画面

政策提言等を実施している。

3　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では、第二次提言（平成 22 年 5 月）において、青少年が CGM（Consumer Generated Media）を利用することに伴う被害の防止等に係る方向性を打ち出している。その際も、青少年が判断能力の未成熟さゆえに様々なインターネット上のリスクに対して無防備な状態となっていることや、青少年が自らリスクへの対応能力を高めていく必要性を踏まえて検討が行われたところである。

4　“Recommendation of the Council on the Protection of Children Online” (February 16, 2012, OECD)。自由で情報交換に有用なインターネットの利点を確保しつつ、未発達な青少年に対する害悪をどう防ぐべきかについて政策原則を策定するもの。2008 年 11 月の日本提案を端緒として、日本主導で報告書を作成。
(http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False)

5　総務省「通信利用動向調査」（http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html）及び第 7 回会合　近藤構成員資料。

に対する利用者の不満として、「同意・許可した後にどのようなことが起こるのかわからない（35.7%）」「説明文の意味が専門的で分かり辛い（28.1%）」「書いてある内容の良し悪しがわからない（27.9%）」等が挙げられている。他方、同調査においては（図表2-10、第2章参照）、端末情報の外部送信に対するユーザーの認識として、端末情報の利用目的又は情報提供先が示されていれば問題ないとする回答の合計が過半数を占めており、一定の情報を基に利用者情報の取得を許容する利用者の判断が窺える。情報提供・周知啓発に当たっては、個人情報を取得することに対する承諾等に関して、利用者が過度な負担を受けずに実質的な判断を行い得るよう、利用者の視点に立ち、分かりやすく平易かつ明確な表現を使用するように努めることが重要である。

また、利用者が青少年や高齢者である場合には、上記②に記載した視点・観点を踏まえた情報提供等を行うことが重要である。

④ 情報提供・周知啓発を行う内容（詳細については、２を参照）

情報提供・周知啓発を行う内容としては、同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクの軽減や利用者がスマートフォンを利用するに当たって抱いている不安の解消に資するものであることが必要である。具体的には、スマートフォンに係る利用者情報の取扱いや情報セキュリティ対策に係る内容が考えられるが、これらは互いに密接な関連を有する事項であることから、両者を組み合わせた上で一貫した情報提供・周知啓発を行うことが適当である。

また、利用者が青少年や高齢者である場合には、その特有の事情により必要な情報提供等を併せて行うことが適当である。

（２）利用者自身による能動的な情報収集

上記のような関係事業者等による利用者への情報提供・周知啓発を受け、利用者は、同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクの軽減や利用者がスマートフォンを利用するに当たって抱いている不安の解消に資する内容を、分かりやすく平易かつ明確な表現の情報として、受領することが可能となる。

スマートフォンにおける利便性の高いサービスを安心・安全に利用する観点から、「スマートフォン プライバシー ガイド」においてもすでに取りまとめているように、利用者においても受け身ではなく、このような情報を能動的に収集するよう努めることが望ましい。具体的には、契約時の説明をよく聞き、内容の理解に努めるほか、今後、関係事業者等の取組によって提供されるプライバシーポリシー等の理解や、周知啓発セミナーへの参加の機会を利用して、スマートフォンについての認識を深め、利便性の高いサービスを享受していくことが期待される。

２　情報提供・周知啓発を行う内容の詳細

第５章までの検討結果に加え、昨今のスマートフォン利用における情報セキュリティ対策、青少年や高齢者の事情を踏まえた情報提供等へのニーズ等に鑑み、以下の情報について出来るだけ全体として、あるいは、相手方や時宜に応じて最も適切な形で提供・周知啓発が行われることが望ましい。

（１）スマートフォンの特性及びスマートフォンをめぐるサービス構造

① スマートフォンの特性

スマートフォンの利用者、特にこれまでスマートフォンを利用していなかった消費者は、第１章１で述べたようなスマートフォンの特性を理解し、従来の携帯電話端末との相違点等を把握することが、スマートフォンにおける利便性の高いサービスを安心・安全に利用するための第一歩となる。

② スマートフォンをめぐるサービス構造

スマートフォンをめぐるサービス構造も、前項で述べたスマートフォンと従来の携帯電話端末との相違点のうち主なもののひとつである。第１章３等でも述べたように、無料のアプリ等の中には、広告主からの広告収入等によって収益を得ることによりアプリの提供を実現しているものもあることや、アプリに組み込まれた「情報収集モジュール」と呼ばれるプログラムなどを通じ、利用者情報が情報収集事業者や広告配信事業者等へ送信される場合もあるという特徴を利用者において知ることが重要である。

（２）利用者情報の取扱い

① 利用者情報の取扱いに係る現状

具体的には、第２章３等において述べているが、スマートフォンにおいては、様々な利用者情報が蓄積・送信され、利用者の趣味・趣向に応じた広告の表示等に利用される場合もあることや、収集される利用者情報に関する利用許諾を求める画面が表示される場合があり、また、アプリケーションの利用規約やプライバシーポリシーが定められ、公表されている場合もあること等が情報提供・周知啓発に係る内容として重要である。

② 利用者自身で注意すべき事項

利用者においては、上記の現状に加え、利用者自身で注意すべき事項を併せて知ることで、一層リスクの軽減や不安の解消が図られると考えられる。例えば、「スマートフォン プライバシー ガイド」としてすでに公表している、アプリケーションの機能や評判、提供者など、アプリケーションの信頼性に関する情報を自ら入手し、理解に努めること、利用許諾画面や利用規約等において、収集される利用者情報の範囲など

をよく確認し、内容を理解した上で、同意・利用するよう努めること等が重要である。また、不安が解消されないアプリケーションの利用は避けるほか、利用を開始した後であっても端末から削除することで、以降の利用を行わないことも重要である。

（３）情報セキュリティ対策

関係事業者等の情報提供・周知啓発及び利用者の能動的な情報収集に当たり、安全・安心なスマートフォンの利用環境の構築という観点からは、利用者情報の取扱いに係る事項と同様に、情報セキュリティ対策に係る次の事項を周知していくことも重要と考えられる。

①「スマートフォン情報セキュリティ３か条」[6]

利用者が最低限守るべき情報セキュリティ対策として、次の事項が示されている。

１）OS（基本ソフト）を更新

２）ウイルス対策ソフトの利用を確認

３）アプリケーションの入手に注意

②「安心して無線LANを利用するために」[7]

スマートフォンは、Wi-Fi等無線LANに接続して利用することも可能であり、PCと同様に情報セキュリティ上の一般の脅威に晒されることになるため、無線LANの情報セキュリティについて理解を深め、適切な対応をとることが肝要である。「安心して無線LANを利用するために」においては、無線LANを安全に利用するための情報セキュリティ対策として、実施が推奨される項目が示されている。

③ ワンクリックウェア、マルウェア等の具体的事例等

同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクは、ワンクリックウェアやマルウェア等の脅威により顕在化する。このため、ワンクリックウェア、マルウェア等の具体的事例や注意すべき事項が関係事業者等から情報提供・周知啓発されることで、利用者が当該脅威に対する対応を行うこと、ひいてはそれらのリスクを軽減することが可能になると考えられる。

（４）青少年に必要な情報（フィルタリング等）

スマートフォンにおける利用者情報の取扱いや情報セキュリティに関する情報のほかに、特に青少年が利用する場合については、法律[8]により義務付けられているフィルタリ

6　2011 年（平成 23 年）12 月、総務省のスマートフォン・クラウドセキュリティ研究会が中間報告を行った際、その別添として公表。同研究会の最終報告は平成 24 年 6 月に公表。

7　総務省において、無線 LAN の安全な利用を促進するために、無線 LAN の情報セキュリティ関するガイドラインとしれ、平成 16 年 4 月に公表。また、改訂版を平成 19 年 12 月に公表。今般のスマートフォン等の急速な普及による無線 LAN の利用形態変化等を踏まえ、当該ガイドラインを改訂予定。

8　青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（2009 年（平成 21

ングが、無線LANを経由してインターネットアクセスしたときやアプリケーションを利用するときは、従来の携帯電話と同様にはフィルタリングを利用できないことがあること、利用可能なスマートフォンのフィルタリングの利用方法や機能について、契約時等に保護者や利用者に対して適切に情報提供がなされる必要がある。なお、関係事業者等が利用者の意見を踏まえつつ進められている検討によってフィルタリングの改善がなされた場合には、それに関する情報も迅速に提供される必要がある[9]。

（５）高齢者に必要な情報

高齢者に対しては、やはりスマートフォンにおける利用者情報の取扱いや情報セキュリティに関する情報にとどまらず、利用を支援する観点からの情報が提供されるべきと考えられる。具体的には、スマートフォンを購入する際の契約に係る手続や、購入後に利用する際の設定等について、丁寧な情報提供・周知啓発が必要である。

３　関係者における取組

（１）関係事業者等における取組

① アプリケーション提供者、情報収集モジュール提供者

アプリケーション提供者は、主に利用者がアプリケーション提供サイト等からアプリケーションをダウンロードする際や、アプリケーションを起動している際に、利用者に対して情報提供・周知啓発を行う機会を有する。これらの機会を利用して、取得する情報の種類、利用目的、同意取得等の具体的方法、第三者提供の範囲等について、アプリの「利用規約」「プライバシーポリシー」「利用許諾画面（パーミッション）」等、情報の種類ごとに最も適した場面において情報提供・周知啓発を行うことが重要である。情報提供・周知啓発に当たっては、「スマートフォン利用者情報取扱指針」を踏まえ、利用者の視点に立って、わかりやすい表現・方法で行うことが重要である。

他方、情報収集モジュール提供者においては、情報提供・周知啓発を利用者に対して直接行う機会がアプリケーション提供者に比べて相対的に少ないと考えられるが、利用者とのコミュニケーションを行う意識を持ち、利用者がアプリケーションを利用する際や自らのウェブページを通じて、取得する情報の種類、利用目的、同意取得等の具体的方法、第三者提供の範囲等について情報提供・周知啓発を行うことが重要で

年）4月施行）。

9　安心ネットづくり促進協議会・スマートフォンにおける無線 LAN 及びアプリ経由のインターネット利用に関する作業部会報告書（2012 年（平成 24 年）6 月）において、フィルタリング改善に関する検討においては、一定の基準によるカテゴライズに基づいたアプリに関するフィルタリングの提供の在り方についても検討されていること、端末側での制限機能の高度化という形でのフィルタリングは、無線 LAN 接続等ネットワークの接続形態によらずにフィルタリングがかかることになる点において、保護者の負担軽減となること等が指摘されている。

ある。

② アプリケーション提供サイト運営事業者、ＯＳ提供事業者（プラットフォーム事業者）

アプリケーション提供サイト運営事業者は、運営するアプリケーション提供サイトにおいて、アプリケーション提供者及び利用者双方との接点を有する。その立場を生かし、アプリケーション提供者に利用者への情報提供・周知啓発を促す取組を実施することが期待される。具体的には、第5章の「スマートフォン利用者情報取扱指針」を踏まえて、アプリケーション提供サイト上に、アプリケーション提供者が明示する「利用規約」「プライバシーポリシー」等利用者情報の取扱いに関する規程を利用者が直接確認できる欄を設け、又は当該規程へのリンクを記載できる欄を設けることが望ましい。

さらに、アプリケーション提供サイト運営事業者が、アプリケーション提供者に対し、アプリケーションの提供に係る契約等を通じて、利用者に情報提供・周知啓発を行うことの意識付けを啓発する等、間接的に利用者が受ける情報提供・周知啓発を改善することも期待される。

他方、OS提供事業者は、利用者の端末において、利用者情報の取扱いに係る表示を行い得る立場にある。このため、上記「スマートフォン利用者情報取扱指針」を踏まえ、特定の情報についてはポップアップ等の手段により利用許諾を利用者から求める等、どのような利用者情報がアプリ等によって利用されているのか、利用者が認識し、利用の可否を選択できるようにすることが望ましい。

これらの事業者が利用許諾等の文言を表示するに当たっては、利用者が理解しやすいよう、可能な限り平易な表現を用いることが重要である。

③ 移動体通信事業者、端末提供事業者

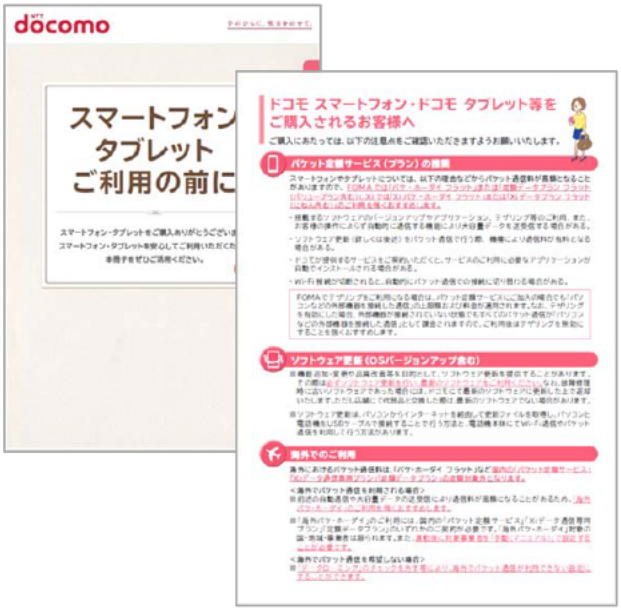
移動体通信事業者は、スマートフォンに係る契約時に、利用者に対して、電気通信役務に関する提供条件の概要の説明を行うこととなる[10]。現時点においても、その機会を利用し、スマートフォンと従来の携帯電話との相違点等を、リーフレット又はチェックリスト等を使用して説明している。具体的な説明事項としては、例えば次のようなものが挙げられるが、これらの事項に比べて、利用者情報の取扱いに関する事項は取り上げられてこなかったところである。

・アプリケーションのアップデート等自動的に通信する機能により、常時パケット通信が行われ、通信料が高額になるおそれがあること
・インストールするアプリケーションによっては、ウイルスへの感染や動作不良が発生するおそれがあること

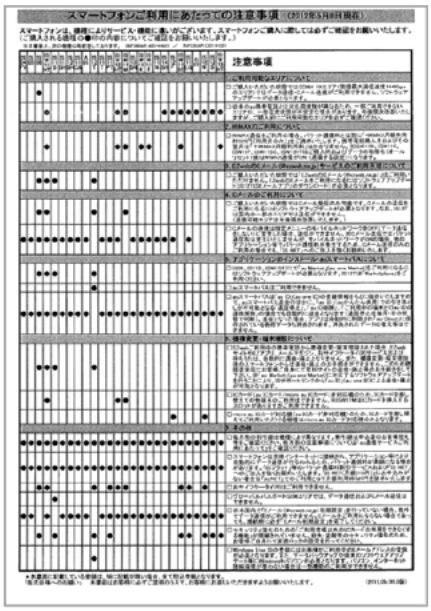
10　電気通信事業法第 26 条。

【図表 6-1：移動体通信事業者において使用されている説明資料の例】

【リーフレットの例】



【チェックリスト等の例】



※出典：（株）NTTドコモ及びKDDI（株）説明資料

また、移動体通信事業者は、電気通信消費者支援連絡会[11]（以下「消費者支援連絡会」という。）等への参加や、スマートフォンに係る利用者向けセミナーを自主的に開催する等の方法により[12]、様々なリテラシーの利用者を対象として、携帯電話・スマートフォンに係る基礎知識やトラブルへの対処法、利用する際のマナー等の情報提供・周知啓発に努めてきたところである。

移動体通信事業者においては、このような取組を引き続き実施することが求められる。実施に際しては、スマートフォンは青少年及び高齢者を含めた国民が広く利用できるものであるべきとの観点を踏まえ、同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクの軽減や利用者がスマートフォンを利用するに当たって抱いている不安の解消に資する情報提供・周知啓発を行うことが重要である。

11　総務省では、本省及び地方総合通局等において、消費生活センター及び消費者団体、電気通信事業者、総務省の３者間での電気通信サービスの現状に関する意見交換会を毎年２回程度開催し、関係者間の連携強化を図っている。

12　例えば、（株）NTT ドコモ及び KDDI（株）においては、青少年や保護者・教職員等を対象に、携帯電話を使う際のマナーやトラブルへの対処方法等の周知啓発を行うための講座を実施している（（株）NTT ドコモ：ケータイ安全教室、KDDI（株）：KDDI ケータイ教室。（株）NTT ドコモにおいては、当該講座に係る映像教材の配布も実施）。また、販売代理店においてもスマートフォンに係る講座等を開催している（（株）NTT ドコモ：電話教室、KDDI（株）：シニア向けスマートフォン教室）。さらに、（株）ソフトバンクモバイルにおいては、「情報モラル学習プログラム」等として、保護者・教職員等を対象に、携帯電話に関する授業等を開催するための教材配布・研修会の開催を行っている。

今後、情報提供・周知啓発を行う内容としては、2で述べた事項をできるだけ全体として、あるいは、相手方や時宜に応じて最も適切な事項を提供していくことが肝要である。特に今後初めてスマートフォンを契約する利用者、青少年、高齢者等に対しては、利用者のリテラシーに合わせた適切な説明がなされることが望ましい。資料の内容について、移動体通信事業者は端末提供事業者と協力して検討することも考えられる。例えば、青少年に対しては、保護の観点から同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクや、同意することの意味についての情報提供・周知啓発を行うことが考えられる。また、高齢者に対しては、利用支援の観点から、契約の手続、端末の機能及び設定等についての情報提供・周知啓発を行うことが考えられる。このとき、説明事項の拡充による利用者の負担を軽減するため、一層わかりやすい資料を作成する等の配慮を行うことが適当である。

他方、消費者支援連絡会やスマートフォンに係る利用者向けセミナー等においては、アプリケーション提供者、アプリケーション提供サイト運営事業者等、利用者に対して直接の説明等を行う機会がこれまで相対的に少なかった者との連携を図っていくことも期待される。

④ セキュリティベンダー、研究機関等

セキュリティベンダーは、これまでもマルウェア等と判断したアプリケーションを公表し、注意喚起を図ってきたところである。今後も、同意のない個人情報の外部送信やプライバシーの侵害、それらから生ずる二次被害といったリスクを軽減するため、引き続きマルウェア等と判断したアプリケーションや、それに関する注意事項等の情報提供・周知啓発に努めることが期待される。

⑤ 業界団体

移動体通信事業者に係る業界団体においては、これまで、「電気通信サービス利用者の利益の確保・向上に関する提言」[13]の内容も踏まえ、利用者に対する一層わかりやすい資料の提供等の取組がなされてきたところである。今後も、移動体通信事業者が行うスマートフォンの契約時の説明において用いるわかりやすい資料に係る検討を行うほか、関係の資料を業界団体のホームページに掲載し、情報提供・周知啓発を行っていくことが求められる。

また、消費生活センターや消費者支援連絡会、e-ネットキャラバン等への講師派遣を通じて、スマートフォンに係る注意事項の説明を実施し、基本的な知識の普及や利用者の意識啓発を行ってきたところである。これらの取組について一層の充実を図り、利用者への情報提供を強化することが重要である。

13　総務省「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」（2011年（平成23年）12月21日公表）

（２）利用者側における取組

① 消費者団体等

消費者団体等においては、これまで、高齢者を対象としたいわゆる悪質商法に関する講座や青少年及び保護者を対象とした携帯電話及びネットに関する講座[14]を開催するなどして、関連するトラブルへの対処法等の周知啓発に取り組んできているところである。今後、このような機会を生かして、スマートフォンに係る利用者情報の取扱いに関する情報提供・周知啓発を実施するとともに、特にトラブルの生じやすい無料のアプリケーションに関する仕組みや利用者自身が能動的に情報収集を行うことの重要性についても注意喚起を行うことが期待される。

② 教育関係者、保護者

関係事業者等における取組や国における取組によって提供された情報については、利用者の間で広く共有されることが望ましい。このような観点から、教育関係者及び保護者において、研究大会、講演会及び研修会等の機会を利用し、本章2（１）～（４）で述べている事項の共有を図っていくことが期待される。

（３）国における取組

総務省は、関係省庁と連携しつつ、スマートフォンに係る情報セキュリティやプライバシー等について、利用者に必要な情報を総合的に提供するため、「スマートフォン安全安心プログラム」（仮称）を早急に取りまとめ、自治体や教育関係者・保護者、関係事業者・団体等の協力を幅広く得て、情報提供・周知啓発を行うことが必要である。

また、とりわけ以下（４）③で論ずる地域での草の根レベルでの具体的な活動においては、各地の総合通信局が地域のコーディネーターとして、また講師等自らプレーヤーとして果たす役割が重要である。

加えて、従来取り組んできている消費者支援連絡会、e-ネットキャラバン等、利用者又は利用者からの相談を受ける者に直接説明できる機会を捉え、「スマートフォン プライバシー ガイド」「スマートフォン情報セキュリティ3か条」の説明等利用者への情報提供・周知啓発を行っていくことが求められる。さらに、電気通信サービスQ&Aや消費者保護ホームページ、広報誌への記載[15]を通じて、スマートフォンを取り巻く状況に係る利用者への意識付けを一層強化していくことが求められる。

14　（公社）全国消費生活相談員協会は、平成 13～23 年度の 11 年間に、全国約 17,500 箇所で「消費者問題出前講座」を開催。

15　また、独立行政法人情報処理推進機構で作成している「スマートフォンのセキュリティ対策のしおり」やスマートフォンをテーマとした情報セキュリティ啓発用の DVD などを活用することも有用である。

【図表6-2：平成24年度電気通信サービスQ&A（抄）】

【図表6-3：総務省広報誌平成24年4月号（抄）】

（４）関係者の連携による取組

① 青少年に関するこれまでの取組

本章２（１）④で触れた、経済協力開発機構（OECD）における「オンライン上の青少年保護に係る理事会勧告」では、保護者の役割や官民一体での取組が重要であること等が指摘されるなど、国際的な取組の強化も図られているところである[16]。

我が国では、安心ネットづくり促進協議会が、青少年の安全・安心なインターネッ

[16] 本勧告においては、定量的定性的な国際比較分析のための国際指標づくりの必要性も指摘されている。

ト利用環境整備の観点から、利用者・産業界・教育関係者等が連携しつつ、これまでも時宜に応じた ICT サービスの青少年による利用に係る課題の検討や各種の周知啓発活動を行ってきた。最近では、同協議会スマートフォンにおける無線 LAN 及びアプリ経由のインターネット利用に関する作業部会報告書「青少年保護・バイ・デザイン及び利用者のインターネット・リテラシー向上に向けて」（本年６月）において、これまでの関係者の幅広い具体的な取組を踏まえ、各事業者や利用者における課題と今後に向けた取組の方向性等が指摘されている[17]。

② 高齢者に関するこれまでの取組

高齢者による携帯電話の利用については、従来、メール等の機能を利用していない高齢者も多く存在していると考えられる状況において、高齢者を対象とした端末の普及がみられたところである。このような高齢者に対する情報提供・周知啓発の取組としては、移動体通信事業者による高齢者向け無料電話教室、非営利団体による講座、民間の PC 教室やカルチャーセンター等による有料講習会等が小規模に開催されてきた。このうち、移動体通信事業者による高齢者向け無料電話教室においては、端末の操作方法だけではなく、「携帯電話を使った振り込め詐欺の手口」や「災害用伝言板の使い方」等の説明も行われてきている。

③ スマートフォンに関する今後の連携による取組

スマートフォンについては、本 WG で検討してきた利用者情報に係る対応等、従来以上に利用者が知るべきことも多いが、青少年、高齢者を含め、広く利用者一般に当てはまる。

このため、多様な情報を地域間格差なく浸透させるためには、関係事業者や国が本章において論じてきたそれぞれの役割を果たすとともに、上記安心ネットづくり促進協議会スマートフォン利用作業部会報告書で指摘されている多くの具体的な視点も踏まえて、草の根レベルでの連携を通じて、青少年はもとより、保護者や高齢者[18]等も適宜対象に含めながら、このような周知啓発等の活動を全国的に展開することが重要である。

---

17 安心ネットづくり促進協議会・スマートフォン利用作業部会報告書においては、「関係事業者による、特に青少年のスマートフォン利用において求められる無線 LAN、アプリのフィルタリングに関する留意事項、利用者情報の扱い等について、関係事業者の連携により、利用する青少年・保護者の立場に立った分かりやすい説明と現場（店頭）レベルでの統一的な対応、さらにはアフターフォローとしての継続的な情報提供が望まれる。」「青少年の利用においては一義的には保護者の責任が重要であり、保護者に対するリテラシー向上への取組が重要である。事業者間の連携による分かりやすい情報提供が重要であるとともに、効果的な周知のためにも安心ネットづくり促進協議会を通じた事業者と利用者との連携強化が図られるべきとの指摘があるところ、事業者と利用者の連携においては、PTA 団体、消費者団体の役割が重要であり、積極的な取組が期待される。」等と指摘されている。

18 高齢者については、NPO サイトからのシニア向けインターネット利用支援講座の発信や NPO による高齢者のための生活支援サービス等が実施されている（第 7 回会合 近藤構成員資料）。シニアを対象としたこのような諸活動との連携を図ることも重要と考えられる。

また、特に青少年については、総務省が作成作業を進めている「青少年のインターネットリテラシー指標（ILAS: Internet Literacy Assessment indicator for Students）」により、プライバシーやセキュリティを含めた様々なリスクに対する対応能力の現状（青少年の得意分野・不得意分野、地域間格差等）が把握される[19]。その結果を踏まえ、関係事業者や教育関係者等において、従来の安全・安心のための周知啓発等の取組を見直し、各地での周知啓発活動にも生かすことも期待される。

さらに、高齢者に関して、今後は、従来の携帯電話と比較して大きな画面を有し、高齢者にも使いやすいことを強調したスマートフォンの普及が見込まれており、過去に業務の一環として ICT に親しんだ高齢者が増加することにも鑑みれば、スマートフォンを利用する高齢者が増加していくことが想定される。このため、老人大学の生涯学習講座等として、スマートフォンに関する講座の開催が期待される。また、当該講座の開催に向け、高齢者に配慮した教材の制作や開催情報の提供について、移動体通信事業者と自治体との間で、連携が強化されることが望ましいと考えられる。

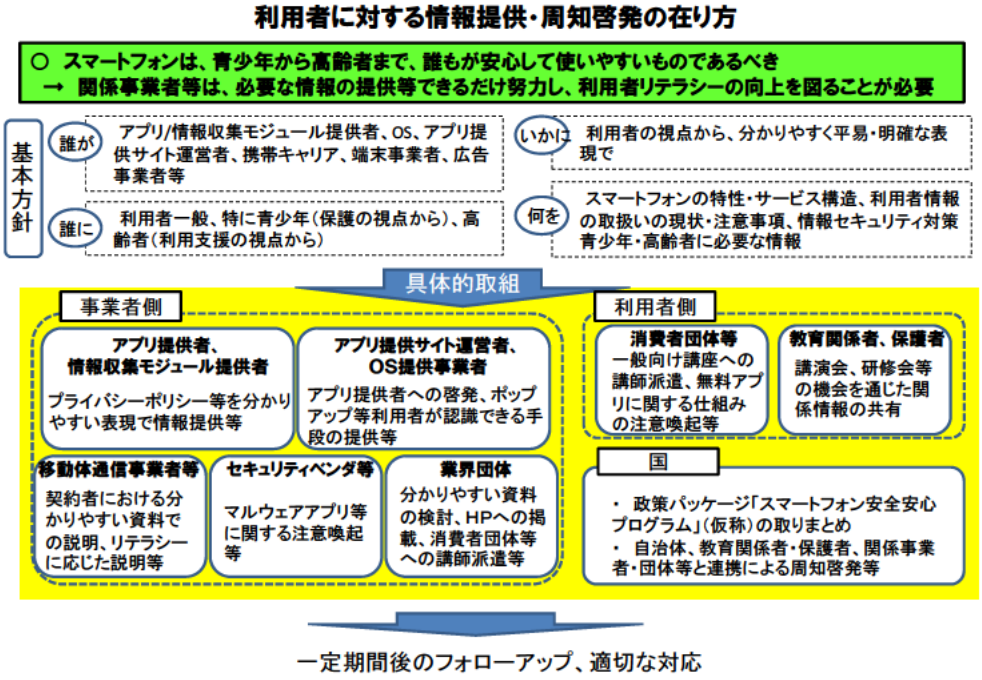
（５）関係者の取組状況に関するフォローアップ

今後、スマートフォンの一層の普及が見込まれることに鑑みれば、関係事業者等、業界団体、関係省庁等が連携・協力しつつ、早急にこれらの取組を行い、継続的かつ効果的に推進することが重要である。このため、一定期間の後に、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等の適切な場[20]において、一定期間の後にフォローアップを行い、取組の状況を把握することが肝要である。また、フォローアップの結果及びスマートフォンをめぐる環境の変化を踏まえつつ、必要に応じて取組の見直しの検討を行うことが求められる。

[19] インターネット利用におけるリスク分類に基づき、必要な知識や行動を問うテスト問題を作成して実施（本年２月に全国約 600 名弱の高校１年生を対象にプレテスト、6 月から 7 月にかけて 2000 名規模でのテストを実施等）して、青少年のリテラシーの現状を可視化することとしている。

[20] その他関係省庁の各種会合等も含まれる。

【図表 6-4：　利用者に対する情報提供・周知啓発の在り方】



第７章　国際的な連携の推進

１　国際連携の必要性

第2章及び第3章において論じたように、アプリケーションを通じてスマートフォン上の利用者情報が利用されることについては、内外において様々な事例が報告され、欧米におけるプライバシーに関する議論の進展とも相俟って、スマートフォンにおける利用者情報の適正な取扱いの在り方や、スマートフォンに係るプライバシー問題は諸外国においても政策課題となっている。

他方、無線ネットワークからアプリケーション、コンテンツまで携帯電話事業者が提供していた従来の携帯電話サービスと異なり、スマートフォンの場合、レイヤーにより様々な事業者がそれぞれの役割を果たしており、プライバシー問題をはじめとする諸課題の解決には、事業者間の連携が極めて重要になっている。

とりわけプラットフォーム（OSやアプリケーションのマーケット）やアプリケーションの提供は、外国事業者や国境を越えてグローバルな活動を行う事業者によりなされる場合も多いことから、スマートフォンの利用者情報の適正な取扱いを効果的に確保していくためには、二国間・多国間の場を活用した課題解決に向けた情報共有や連携が重要であり、官民を挙げて国際的な連携を推進する必要がある。

２　今後とるべき対応の方向性

（１）先進国間での二国間・多国間連携の推進

米国との間では、現在インターネットエコノミーに関する日米政策協力対話（政府間会合、民間会合）に代表される、二国間の政策的協力を推進するための枠組みが構築されている。また、欧州各国との間でも二国間の定期協議等の枠組みが存在している。

多国間連携の場としては、経済協力開発機構（OECD）の情報・コンピュータ・通信政策委員会（ICCP）情報セキュリティ・プライバシー作業部会（WPISP）において、プライバシー問題等がこれまでも議論されてきている。

こうした場面において、スマートフォン上の利用者情報の取扱いやプライバシー問題について国及び民間において積極的に議論し、基本的な認識や各国の取組みに関する情報を共有するとともに、関係事業者に係る行動規範の国際的調和を目指すことが重要である。

（２）国際機関等を活用した普及啓発・情報共有

190を超える加盟国と、約700に及ぶセクターメンバー（民間事業者、NGO等）が参加する国際電気通信連合（ITU）や、その地域連合であるアジア太平洋電気通信連合（APT）、あるいはアジア太平洋国際協力（APEC）においては、全権委員会議（ITUの

場合）や国際的な展示会をはじめとした大きなイベントの際、あるいは各国の独自のイニシアティブにより、数多くのワークショップ、シンポジウム等が開催されてきている。また、具体的なサービス展開等に関し、ポリシーや技術仕様等に関する政策協調や国際標準が必要な場合には、個々のテーマに特化した専門的な議論も行われてきている。

スマートフォンの普及拡大が今後見込まれる途上国・新興諸国の関係者が多数集まるこのような場を国及び民間において積極的に活用し、プライバシー上の問題の所在や対応策等について普及啓発と情報共有を図るとともに、必要な場合には政策協調、国際標準に関する議論を行い、安全・安心な利用環境を確保しつつ円滑なスマートフォンの普及に寄与することが重要である。

（３）民間団体間の国際連携の推進

本年3月のインターネットエコノミーに関する日米政策協力対話においては、特にオンライン上の青少年保護について、官民のイニシアティブ、自発的な産業界主導の努力等の重要性等について認識が共有された[1]。こうした認識の共有を受け、本年4月には日米両国の民間団体間の直接対話として、安心ネットづくり促進協議会[2]（会長：堀部政男一橋大学名誉教授。以下「安心協」という。）と、オンライン上等の青少年保護等の活動を行う米国NGOがテレビ会議を行い、ベストプラクティスの共有等に向け、今後の交流を継続することで一致した。

スマートフォンにおけるプライバシー問題等についても、このような民間団体間の交流を通じて、課題認識や具体的な取組みの共有を図ることが重要である。

（４）スマートフォンに関する我が国の取組みの発信

スマートフォンにおける利用者情報の取扱いについては、本WGにおいて検討してきたが、青少年保護の文脈で、スマートフォンにおけるフィルタリングの在り方やリテラシー向上方策等について、安心協スマートフォン利用作業部会[3]が昨年10月より本年5月まで検討を行い、報告書を取りまとめている。

---

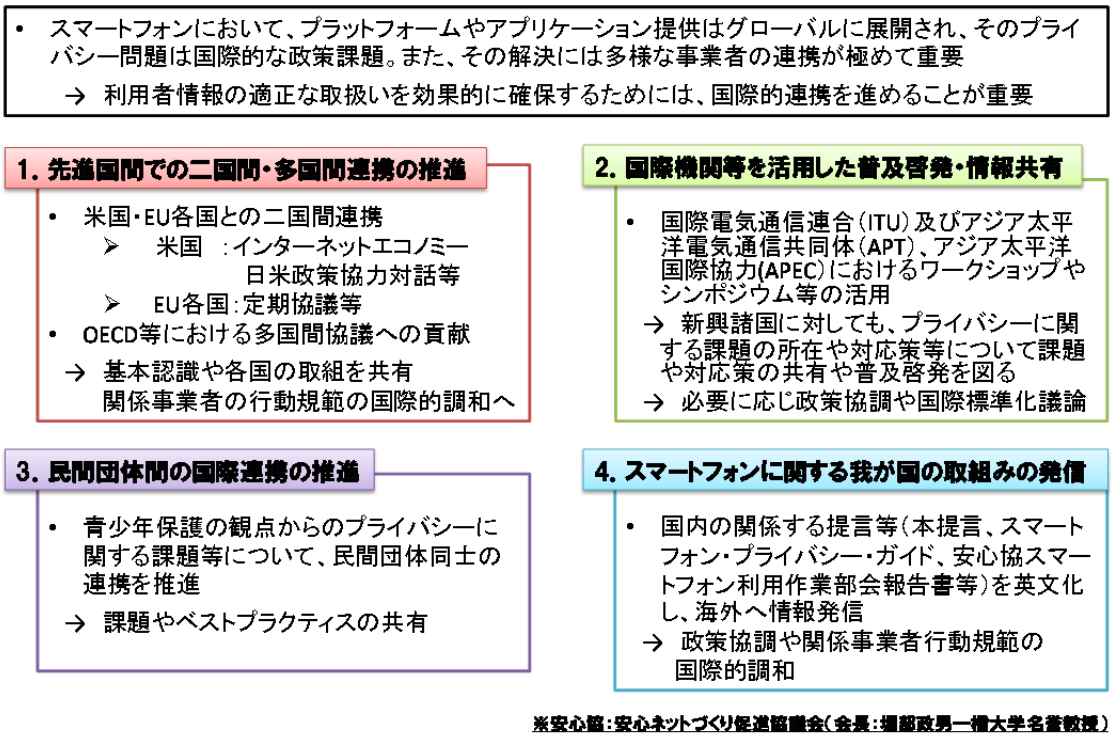
1 （7）オンライン上の青少年保護
双方は、オンライン上の青少年保護の重要性について認識した。特に、双方は、官民のイニシアティブ、自発的産業界主導の努力、消費者及び産業界の教育が、法令と、重要な補完関係にあることで一致した。共に作業することで、これらの要素は、青少年にとって、安全なインターネット環境を提供する最良のアプローチであることを示すものである。参加者は、また、更なる協力が利益をもたらすことで一致した。（インターネットエコノミーに関する日米政策協力対話第３回局長級会合に係る共同記者発表（2012 年 3 月 23 日）

2 青少年が安全安心にインターネットを利用できる環境を整備するため、2009 年（平成 21 年）2 月に設立された利用者・産業界・教育関係者等の相互連携を図る民間の協議体。「１億人のネット宣言　もっとグッドネット」のキャッチフレーズの下、普及啓発イベントや、青少年保護に係る諸課題についての政策提言等を実施している。

3 「スマートフォンにおける無線 LAN 及びアプリ経由のインターネット利用に関する作業部会（主査：藤川大祐千葉大学教育学部教授）」。総務省の研究会（利用者視点を踏まえた ICT に係る諸問題に関する研究会）の提唱する「青少年保護・バイ・デザイン」の概念を推進する観点から、フィルタリング等スマートフォンに関する諸課題について検討を行った。

これらスマートフォンに係る様々な検討結果は、相互に関連性を有する部分もあり、また諸外国との政策協調や関係事業者における行動規範の調和等を図る観点から、報告書等を英文化し、海外関係機関への配布やウェブサイトを通じた情報提供等を積極的に推進することが重要である。

【図表 7-1：国際連携の推進】



おわりに

常時電源オン・常時接続・高い携帯性というデバイス特性、無線LANからの高速アクセスが一般に可能というネットワーク特性、アプリケーション利用を前提とした高機能性等を備えたスマートフォンの急速な普及により、モバイルビジネスや利用シーンが新たな局面を迎えている。

しかし、十分なリテラシーを必ずしも有していない利用者層にまでスマートフォンの普及が急速に進む中で、本WGが検討した利用者情報の取扱いをはじめ、スマートフォンに関する諸課題に対する関係事業者等の対応が追いついていない、あるいは利用者に対する適切な表示や説明がなされていない部分があるのは事実である。

スマートフォンが新たな社会インフラとなるまでに浸透するならば、高度なリテラシーを有する利用者しか使えないものであってはならず、青少年から高齢者まで、誰もが使いやすいものであるべきである。サービスを提供する側は、自らの責任として、利用者の懸念を取り除くため最大限の努力をするとともに、利用者が知っておくべきことを、分かりやすい言葉で、効果的に説明することが必要である。

一方、利用者の側でも、スマートフォンの利用には一定の自己責任を求められる面があることを認識し、受け身ではなく、能動的に必要な情報を入手する態度が重要である。

グローバルな水平分業モデルのサービス構造であるスマートフォンにおいて、アプリケーションの提供や利用に係る業界団体等は、こうした責任を果たす一環として、業界ガイドライン策定等の努力を行ってきているが、その促進剤として、多くの関係者が共有し連携することができるための共通的な指針が求められている。さらに、アプリケーション提供者は、大企業からベンチャー企業、個人に至るまで多様であるが、業界団体に加入しない者も同様の対応をとることが望まれている。

こうした状況の下とりまとめられた本報告書は、関係者が直接参照できる指針を提示するとともに、業界ガイドライン作成等の取組に対しては、指針を通じてそれを後押ししている。

その基本的アプローチは、アプリケーションごとにプライバシーポリシーを策定するとともに、一定の情報の取得については、個別の同意取得を求めるというものである。この点において、個人情報保護法と異なる取扱いを部分的に採用しているが、これは、個人の人格・思想・信条等にもつながり得るプライバシー情報が、非常に詳細なレベルで大量に保存されており、これらがアプリケーションを通じて自動的に取得されるという、スマートフォンならではの特性を踏まえたものである。

また、この指針に沿った実運用の確保を支援するため、プライバシーポリシーの内容の適否

や、アプリケーション等の実際の動作がそれに合致しているかどうか等を運用面、技術面等の専門的観点から確認できる第三者機関的な仕組みの導入を提言している。

今後も、スマートフォンをめぐり新しい技術やサービスの導入や展開が進むことが想定されるが、その際も関係事業者等が「スマートフォン利用者情報取扱指針」における「基本原則」等を参照し、「プライバシー・バイ・デザイン」の視点を取り入れつつ、柔軟に必要な対応を行っていくことが期待される。

なお、スマートフォンに用いられているOSはスマートフォンに限らず、タブレットや電子ブック等に活用され、今後スマートテレビ等にも搭載されることも想定される。また、クラウドを介して、一つのアプリケーションやコンテンツがデバイスを超えて利用可能となるサービスの普及も想定される。このように多種多様なデバイスがインターネットにつながることにより、将来スマートフォンが多様なデバイスと連携[1]して用いられる可能性も視野に入れつつ、利用者がスマートフォンを用いた様々なサービスを安全・安心な環境で活用できる環境整備に向けて関係者が協力をしていくことが期待される。

関係者が本提言に沿った取組を自主的に進め、新たな技術やサービスのイノベーションを推進しつつ、安全・安心な利用環境の下でスマートフォンの利用が一層拡大する日本モデルを成功事例として世界へ向けて発信することで、課題を共有する各国の関係者との間で、本分野における世界的な政策協調や事業者の対応の調和が一層進められることが期待される。

1 第一回 WG　北構成員資料

用語解説

索引	用語	用語解説	初出
3	3G 回線	第 3 世代移動通信システム（「IMT-2000」規格に準拠したデジタル方式の移動通信システム）を提供する通信回線のこと。NTT ドコモの「FOMA」、au の「CDMA2000 1x」「CDMA 1x WIN」、ソフトバンクモバイルの「Softbank3G」サービスが該当。	P.5
A	Android ID	Android OS を搭載する機器を識別する番号。機器の初回起動時に OS により自動で生成される。	P.9
	API	Application Program Interface の略。プラットフォーム向けのソフトウェアを開発する際に使用できる命令や関数の集合。また、それらを利用するためのプログラム上の手続きを定めた規約の集合。開発者は規約に従ってその機能を「呼び出す」ことで、自らプログラミングせずにその機能を利用したソフトウェア作成が可能となる。	P.10
B	BWA	Broadband Wireless Access の略。IEEE(米国電気電子学会)で承認された、固定無線通信の標準規格（IEEE802.16 規格）。この規格に変更を加えたものが、WiMAX となる。	P.6
G	GPS	Global Positioning System の略。全地球測位システム。人工衛星を利用して、利用者の地球上における現在位置を正確に把握するシステム。	P.9
H	HTML5	Web ページの記述などに用いるマークアップ言語である「HTML」の第 5 版のこと。HTML5 を使用することでブラウザベースのウェブコンテンツの開発も可能となり、アプリとの違いとして、常に最新のデータを利用でき、バージョンアップやアップデートの手間がない、端末内の個人情報にアクセスできないため安全などの利点もある。	P.69
I	IMEI	International Mobile Equipment Identity の略。「国際移動体装置識別番号」といい、スマートフォンや携帯電話端末等 1 台 1 台に付与される国際的な識別番号。 端末製造事業者が番号を付与している。	P.9

索引	用語	用語解説	初出
I	IMSI	International Mobile Subscriber Identity の略。「国際移動体加入者識別番号」といい、携帯電話サービス加入者に付与される識別番号。SIM カードに書き込まれており、電話番号と 1 対 1 で対応する。	P.9
L	LTE	Long Term Evolution の略。携帯電話の通信規格で、第 3 世代（3G）と第 4 世代（4G）の間に位置する規格。	P.6
M	MAC アドレス	Media Access Control Address の略。LAN（Local Area Network）カード等のネットワーク機器に原則として一意に割り当てられる番号。	P.9
O	OS （オペレーティング システム）	コンピュータシステム全体を管理するソフトウェアで、多くのアプリケーションソフトから共通して利用される基本的な機能を提供する。一般的に「基本ソフトウェア」と呼ばれている。スマートフォンの OS には、グーグル社の「Android OS」、アップル社の「iOS」、マイクロソフト社の「Windows Phone」などがある。	P.6
S	SNS	Social Networking Service の略。インターネット上で友人を紹介し合い、個人間の交流を支援するサービス。主なサービスには、Facebook、mixi、GREE など。	P.7
U	UDID	Unique Device Identifier の略。Apple 社が提供する機器（iPhone/iPad 等）において当該機器を識別する番号。	P.9
W	Wi-Fi	Wireless Fidelity の略。業界団体の Wi-Fi Alliance が無線LANの標準規格である IEEE 802.11 シリーズに準拠していることを示すブランド名で、他社製品との相互接続性などに関する試験をパスした装置にロゴの表示などが許可される。	P.5
	WiMAX	Worldwide Interoperability for Microwave Access の略。ワイヤレスブロードバンド通信規格の一つ。	P.6
あ	アカウント	コンピュータや各種のネットワーク上のサービス等を利用できる権利、または利用（ログイン）する際に必要な ID のこと。	P.24
	アップデート	ソフトウェア（アプリ）や OS の小規模な更新、改善、修正、機能追加などのこと。	P.22
	アドネットワーク	複数のメディアサイトをネットワークして（「広告配信ネットワーク」を形成）広告受注を請け負い、広告を配信するサービスのこと。	P.23

索引	用語	用語解説	初出
あ	アプリケーション （アプリ）	アプリケーションソフトウェアの略。通話やEメールなどのコミュニケーションツール、写真やゲームなどの様々な機能を実行するためのソフトウェアをいう。スマートフォンではアプリをインストールすることで、機能を拡張・カスタマイズすることが可能。	P.1
	アプリケーション 提供サイト	アプリを提供するウェブサイトのことで、利用者はこのサイトからアプリをダウンロードする。OS 提供者が運営するサイト（グーグル社の「Google Play」、アップル社の「App Store」、マイクロソフト社の「Windows Phone Marketplace」）や携帯電話事業者が運営するサイトなどがある。	P.7
い	インターフェース	機器や装置等が他の機器や装置等と交信し、制御を行う接続部分のこと。	P.10
お	オプトアウト	利用者側がサービス利用の停止を事後に求めることができる仕組みをいう。なお、個人情報保護法第 23 条第 2 項には本人の求めに応じて個人データの第三者提供の停止を行うこと（オプトアウト）が規定されている。	P.37
	オプトイン	サービス提供者が個々のサービスを提供するに当たり、事前に提供条件等を利用者側に提示し、利用者側から個別的な承諾（同意）を得ないと、当該利用者にはサービス提供を行わない仕組みのこと。利用者側がサービス利用を事前に選択（オプト）できる。	P.22
き	キャリア	自前の回線網などの設備を保有して固定通信サービスや移動体通信サービスを提供する電気通信事業者のこと。携帯電話キャリアとしては、NTT ドコモ、KDDI、ソフトバンクモバイル、ウィルコム、イー・アクセスをいう。	P.14
く	クッキー	ウェブサイトの提供者が、ウェブブラウザを通じて訪問者の PC 等に一時的にデータを書き込んで保存させる仕組みで、利用者に関する情報や最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができることから、認証など利用者の識別に使われる。	P.9

索引	用語	用語解説	初出
く	クラウド	クラウドコンピューティング（Cloud Computing）の略。データサービスやインターネット技術等が、ネットワーク上にあるサーバー群（クラウド：雲）にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」利用することができる新しいコンピュータ・ネットワークの利用形態。	P.1
け	契約者・端末固有 ID	契約者が所持する端末（スマートフォンや携帯電話等）等を識別する番号の総称。	P.9
こ	コーディング	プログラミング言語を使ってソフトウェアの設計図であるソースコードを作成すること。	P.67
	行動ターゲティング広告	蓄積されたインターネット上の行動履歴（ウェブサイトの閲覧履歴や電子商取引サイト上での購買履歴等）から利用者の興味・嗜好を分析して利用者を小集団（クラスター）に分類し、クラスターごとに広告を出し分けるサービス。	P.30
	個人情報	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものをいう。なお、他の情報と容易に照合することができ、それにより個人を識別することができることとなるものも含まれる（個人情報保護法第2条第1項）。	P.4
	個人データ	個人情報データベース等を構成する個人情報をいう（個人情報保護法第 2 条第 4 項）。	P.27
	個人情報データベース	個人情報を含む集合物であって、特定の個人情報を電子計算機を用いて検索できるように体系的に構成したもの。	P.27
	個人情報取扱事業者	5,000 人を超える個人データを含む「個人情報データベース等」を事業の用に供している者をいう（個人情報保護法第 2 条第 3 項）。	P.27
	コンテンツ	文字・画像・動画・ゲーム等の情報全般、またはその情報内容のこと。電子媒体やネットワークを通じてやりとりされる情報を指して使われる場合が多い。	P.6
し	情報収集モジュール	スマートフォン等に蓄積された様々な情報を収集する機能を持つ、一連のプログラムのこと。	P.4

索引	用語	用語解説	初出
す	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。	P.1
た	ターゲティング型	マーケティング手法の一つで、自社商品等が訴求しやすく、競争力を持つ特定の顧客層・購買層を標的（ターゲット）にして、商品等を市場に投入することをいう。	P.16
て	デバイス	スマートフォン、タブレット型端末、電子ブック、スマートテレビ等などの各種の機器のこと。	P.87
	電気通信事者	電気通信事業（電気通信事業法第 2 条第 4 号に定める電気通信事業をいう。）を行う者であり、電気通信事業を営むことについて登録、届出という行政上の手続を経た者とともに、電気通信事業法の適用除外とされている同法第 164 条第 1 項各号に定める事業を営む者も含む。	P.29
と	トラッキング	追跡、追尾。ICT の分野では、人の行動やシステムの挙動、データの推移などの情報を継続的に収集、監視すること。	P.26
は	パケット通信	データを小さなまとまりに分割して一つ一つ送受信する通信方式で、分割されたデータは「パケット」と呼ばれる。	P.5
ふ	フィルタリング	インターネットのウェブページ等を一定の基準で評価判別し、違法・有害なウェブページ等の選択的な排除等を行う機能・ソフトウェア。主に、青少年が安全安心にインターネットを利用できることを目的としている。 18歳未満の青少年が携帯電話、PHS でインターネットを利用する場合、原則としてフィルリング機能を利用することが義務付けられている。	P.75
ふ	プライバシー、 プライバシー権	個人に関する情報をみだりに公開されない法的な保障と権利のことで、学説上は、放っておかれる権利（古典的なプライバシー論）から自己情報コントロール権のように積極的に捉える（積極的プライバシー）ものへと移り変わっている。我が国においては、一般的に規定した法律はないが、判例法上、法的に保護されるべき人格的利益として承認されてきている。	P.2

索引	用語	用語解説	初出
ふ	プライバシー・バイ・デザイン	Privacy by Design。 サービスの導入の際に、プライバシー侵害のリスクを低減するために、システムの開発等において事前にプライバシー対策を考慮し、企画から保守段階まで一貫した取り組みを行うこと。1992 年にカナダ オンタリオ州のプライバシーコミッショナーが提唱した概念。	P.33
	プライバシーポリシー	インターネット上のサービスにおいて、サービス提供が明らかにするサービスを受ける者の個人情報取扱方針のこと。メールアドレスや通信記録の管理方法等を明らかにする。	P.16
	プラットフォーム	アプリケーションソフトを動作させる際の基盤となるオペレーションシステム（OS）の種類や環境、設定などをいうが、広義には、コンテンツやアプリケーションなどの利用を可能とする「場」のことをいう。	P.6
	プロバイダー	通信回線を通じて企業や家庭にインターネット接続サービスを提供する「インターネットサービスプロバイダ」（ISP：Internet Service Provider）のこと。	P.34
	ブラウザ	データや情報を閲覧するためのソフトウェア。ここでは、ウェブサイトを閲覧するためのアプリケーションソフトをいう（ウェブブラウザ）。	P.9
ほ	ポップアップ	利用者による何らかの作用なしに、自動的に表示される画面のこと。	P.11
	保有個人データ	個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう（個人情報保護法第2条第5項）。	P.27
ま	マイニング	販売データや電話の通話履歴、クレジットカードの利用履歴など、企業に大量に蓄積されるデータを解析し、項目間の相関関係やパターンなどを探し出す技術。	P.47

索引	用語	用語解説	初出
ま	マルウェア	malicious software（悪意のあるソフトウェア） の短縮された語。ウイルス、またはスパイウェアなどの被害を起こすように設計されたソフトウェア全般を示す。	P.14
む	無線 LAN	無線を使って構築される LAN（Local Area Network: 企業内、宅内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク）。 通信方式は、2.4GHz 帯を用いる IEEE802.11b(最高伝送速度 11Mbps)や、5.2GHz 帯を用いる IEEE802.11a（最高伝送速度 54Mbps）等がある。	P.5
ら	ライフログ	蓄積された個人の生活の履歴をいい、ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末の GPS（Global Positioning System 全地球測位システム）により把握された位置情報等々が含まれる。	P.30
り	リテラシー	本来、「識字率」を意味するが、その分野における知識、教養、能力を意味することにも使われる。	P.40
	利用許諾 （OS による利用許諾）	アンドロイド OS が搭載されたスマートフォンでは、アプリケーションをダウンロードする際、各アプリケーションが、アクセスする機能（電話、カメラ、GPS など）やファイル（電話帳など）についての許諾（パーミッション）を求め、利用者が同意する仕組みとなっている。	P.11
れ	レイヤー	システムの構造や設計、サービス提供の構造などが階層状になっている場合に、それを構成する一つ一つの階層（レイヤー）をいう。	P.7
ろ	ログ	ソフトウェア等の利用状況やデータ通信の記録。日時、操作の内容や送受信されたデータの中身などが記録される。	P.9
わ	忘れられる権利	The right to be forgotten。個人からネットにアップロードされた個人データの削除等を求める権利をいう。 2012 年 1 月に提出された EU データ保護規則改正案で盛り込まれた。	P.37
	ワンクリックウェア	ワンクリック詐欺を目的として、サイトの料金請求を行うための画面を表示させるソフトウェア。	P.54

参考資料集

参考１　スマートフォンを経由した利用者情報の取扱いに関するWG　構成員名簿
参考２　スマートフォンを経由した利用者情報の取扱いに関するWG　審議経過
参考３　参考資料

参考１

スマートフォンを経由した利用者情報の取扱いに関するWG　構成員名簿

（平成２４年6月１２日現在）

※敬称略　五十音順

【構成員】

	石井　夏生利	筑波大学 図書館情報メディア系 准教授
	石田　幸枝	公益社団法人全国消費生活相談員協会 消費者団体訴訟室長、 ＩＴ研究会代表
	上沼　紫野	虎ノ門南法律事務所 弁護士
	北　　俊一	株式会社野村総合研究所 上席コンサルタント
	近藤　則子	老テク研究会 事務局長
	宍戸　常寿	東京大学大学院 法学政治学研究科 准教授
主　　査	新保　史生	慶應義塾大学 総合政策学部 准教授
	中尾　康二	独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 主管研究員
主査代理	森　　亮二	弁護士法人英知法律事務所 弁護士

【オブザーバ】

板倉　陽一郎	消費者庁 消費者制度課個人情報保護推進室 政策企画専門官
尾崎　高士	ＫＤＤＩ株式会社 商品統括本部プロダクト企画本部 パーソナルプロダクト企画部長
岸原　孝昌	一般社団法人モバイル・コンテンツ・フォーラム（ＭＣＦ） 常務理事
熊谷　宜和	株式会社エヌ・ティ・ティ・ドコモ スマートコミュニケーションサービス部 コンテンツ推進室長
武市　博明	一般社団法人情報通信ネットワーク産業協会（ＣＩＡＪ） 常務理事
竹田　御眞木	経済産業省 商務情報政策局情報経済課 課長補佐
千葉　芳紀	ソフトバンクモバイル株式会社 プロダクト・サービス本部PS推進統括部商品戦略部商品戦略課 課長
西本　逸郎	一般社団法人日本スマートフォンセキュリティ協会（ＪＳＳＥＣ） 事務局長
宮澤　由毅	一般社団法人インターネット広告推進協議会（ＪＩＡＡ） 新領域ワーキンググループリーダー

【事務局】

総務省　総合通信基盤局　電気通信事業部　消費者行政課

参考２

スマートフォンを経由した利用者情報の取扱いに関するWG　審議経過

会合	開催日	主な議題
第１回	平成24年１月20日	【プレゼンテーション】 ・北構成員 「スマートフォンにおける利用者情報の取扱いに関する考察」 ・（株）KDDI研究所研究主査　竹森敬祐氏 「スマートフォンからの利用者情報の送信～情報収集の実態調査～」 【その他】 ・スマートフォンをめぐる現状と課題
第２回	平成24年２月８日	【プレゼンテーション】 ・（株）ディー･エヌ･エー 「弊社のスマートフォーンにおける端末情報取得について」 ・（株）ナビタイムジャパン 「「NAVITIME」スマートフォンコンテンツサービスにおける個人情報の取り扱いについて」 ・NHN Japan（株） 「スマートフォンアプリの利用者情報に関する当社の取組について」 ・（株）NTTデータ 「スマートデバイスのプライバシに関する考察」 ・（一社）モバイル・コンテンツ・フォーラム 「スマートデバイスのプライバシに関する考察」 ・森主査代理 「グーグル社の新プライバシーポリシー」 【その他】 ・諸外国の現状と今後の論点
第３回	平成24年３月８日	【プレゼンテーション】 ・日本マイクロソフト（株） 「Windows Phone概要と利用者取り組みについて」 ・（独）産業技術総合研究所情報セキュリティ研究センター 主任研究員　高木浩光氏 「情報取得手段ごとに相当な同意確認基準の提案」 ・石井構成員 「スマートフォンをめぐる国際的動向」 【その他】 ・スマートフォンアプリケーションに係る利用者の動向 ・中間取りまとめに向けて
第４回	平成24年３月21日	【その他】 ・スマートフォン利用者及び関係事業者の動向 ・中間取りまとめ（案）について

会合	開催日	主な議題
第５回	平成24年４月12日	【プレゼンテーション】 ・森主査代理 「個人情報保護法、プライバシーに関する現状の評価－骨子」 【その他】 ・スマートフォンのOS及びアプリケーション提供サイトの動向 ・中間取りまとめを踏まえた今後の議論について
第６回	平成24年５月15日	【プレゼンテーション】 ・（株）エル・カミノ・リアル　代表取締役　木寺祥友氏 「スマートフォンを経由した利用者情報の取扱いに関するWG発表資料」 ・一般社団法人インターネット広告推進協議会 宮澤オブザーバ、安達 紳之介氏、宮一 良彦氏 「スマートフォン向け広告を含むインターネット広告におけるユーザー情報の収集と利用に関するプライバシー保護の取り組み」 【その他】 ・最終取りまとめ骨子（案）について
第７回	平成24年５月29日	【プレゼンテーション】 ・石田構成員 「利用者情報を取り扱う事業者に求められる取組み」 ・近藤構成員 「日韓シニアネットユーザーの声から考察したスマートフォンを経由した利用者情報の利用許諾等高齢者や初心者への広報・利用支援のありかた」 ・一般社団法人日本スマートフォンセキュリティ協会 西本オブザーバ、谷田部 茂氏 「JSSECにおける提供物について」 【その他】 ・スマートフォンに係る利用者周知の状況 ・最終取りまとめ骨子（案）について
第８回	平成24年６月12日	【その他】 ・最終取りまとめ（案）について

WGにおける関係者からのプレゼンテーションの概要

会合	主な概要
第１回	北構成員 ・ビジネスモデルと利用者環境の変移について ・スマートフォンアプリによる利用者情報取得時の利用目的と同意取得の在り方
	KDDI研究所　竹森敬祐氏 ・スマートフォンにおける利用者情報とパーミッションの仕組み ・アプリケーションによる利用者情報収集の実態調査 ・利用者情報収集の課題と考察
第２回	(株)ディー・エヌ・エー ・SNSサイトMobage（モバゲー）のビジネスモデル ・取得する利用者情報と利用目的及び許諾方法
	(株)ナビタイムジャパン ・「NAVITIME」サービスの概要 ・取得する利用者情報と利用目的及び許諾方法、個人情報の取扱いに係る提案
	NHN Japan(株) ・コミュニケーションアプリ「LINE」の概要 ・取得する利用者情報と利用目的
	(株)NTTデータ ・スマートデバイスにおけるプライバシーに関する懸念 ・BYOD(Bring Your Own Device)により高まる個人情報漏えいリスク ・利用者における心構え
	（一社）モバイル・コンテンツ・フォーラム ・ユーザー情報活用の有益性 ・スマートフォンにおけるユーザー情報取得の課題 ・安心・安全な利用環境への私案
	森主査代理 ・グーグル社の新プライバシーポリシーの概要（収集情報と利用目的） ・新プライバシーポリシーへの移行に関する法的問題点
第３回	日本マイクロソフト(株) ・Windows Phoneの概要と設計方針 ・アプリケーション提供方針とセキュリティ対策
	産業技術総合研究所情報セキュリティ研究センター　高木浩光氏 ・利用者の意図の確認：同意確認の方法とレベル、Permission確認方式の限界 ・情報の種類と望ましい同意確認の方法、基準適用例の検討 ・IDの匿名性レベル、端末ID使用の問題点、議論を要する事項
	石井構成員 ・米国におけるスマートフォン及びオンライン上のプライバシーに係る政策動向 （カリフォルニア州司法長官との合意、消費者プライバシー権利章典、子供のためのモバイルアプリ等） ・EUデータ保護指令改正提案の主な論点
第４回	―

第５回	森主査代理 ・個人情報保護法について（要件に関する問題、遵守すべき事項） ・プライバシー権侵害について（各主体によるプライバシー権侵害） ・不正指令電磁的記録について
第６回	（株）エル・カミノ・リアル　代表取締役　木寺祥友氏 ・スマートフォンにおけるHTML5の適用（HTML5とアプリの関係、アプリ・HTML5の利点・欠点） ・HTML5の適用による利用者情報の扱い
	一般社団法人インターネット広告推進協議会 宮澤オブザーバ、安達 紳之介氏、宮一 良彦氏 ・インターネット広告業界におけるガイドラインの取り組み ・スマートフォンアプリでの広告配信におけるユーザー情報利用の現状と課題 ・今後のプライバシー保護の取り組み
第７回	石田構成員 ・相談事例（昨年度の相談事例、スマートフォンを狙った架空請求急増、今後の相談件数） ・消費者が安心して利用するために（同意の取得方法と記載方法等、消費者啓発が必要、プライバシー・バイ・デザイン）
	近藤構成員 ・情報格差、国内外の高齢者層への情報教育支援事情 ・日韓シニアネットユーザーへのアンケート結果 ・関係事業者等への提案
	一般社団法人日本スマートフォンセキュリティ協会 西本オブザーバ、谷田部 茂氏 ・JSSEC（日本スマートフォンセキュリティ協会）の活動成果と提供物 ・アプリケーション攻撃性の検査 ・アプリケーションの設計と作成
第８回	―

参考３

参考資料

- 総務省によるスマートフォン利用者調査（ウェブアンケート調査）結果
- 諸外国における取組状況
- アンドロイド OS による利用許諾
- スマートフォンに関連する主な ID
- セキュリティソフトウェア（Android スマートフォン（個人利用）向け）機能一覧

総務省によるスマートフォン利用者調査（ウェブアンケート調査）について

アンケート調査の概要

スマートフォンのアプリケーションの利用実態等について、総務省においてウェブアンケート調査を実施。

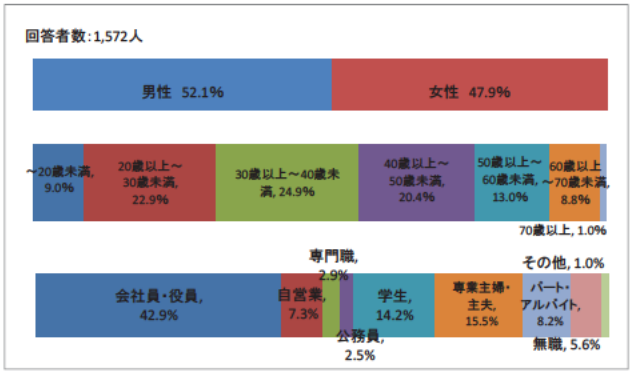
◆ **調査実施方法**
民間調査会社が保有する消費者モニターの約10万人に対しプレ調査を行い、回答のあった19,212名のうち、1,576名を利用しているOS及び性別年齢の割合に応じて無作為に抽出。

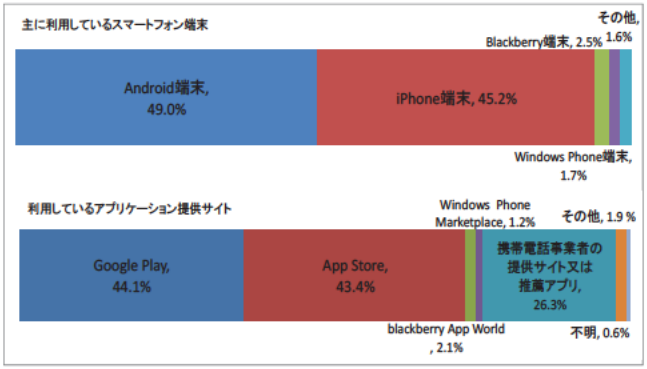
◆ **回答者（1,576名）の割付方法**
① スマートフォン（OS）の種類に応じた割付
Android OSスマートフォンユーザー742名、iPhoneユーザー732名、BlackBerryユーザー50名、WindowsPhoneユーザー52名
② 性別・年代別の割付
総務省「平成22年度通信利用動向調査」より、携帯電話からのインターネット利用人口：性年代別

◆ **アンケート実施時期**
プレ調査：2012年2月14日～2月21日　本調査：2012年2月24日～2月28日

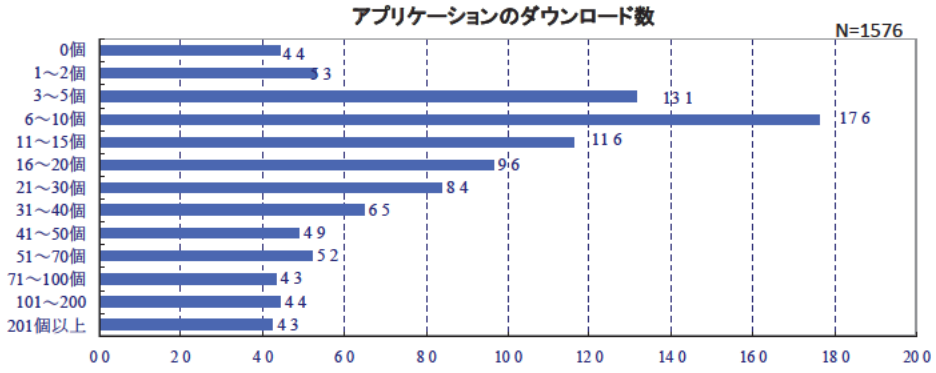
◆ **有効回答数**
1,576人

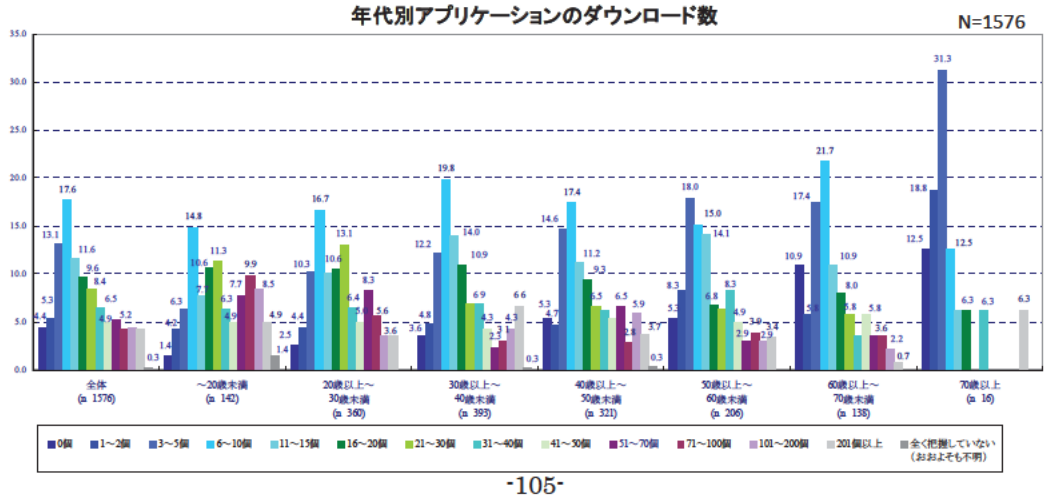
◆ **調査協力**
(株)日本総合研究所、NTTレゾナント(株)



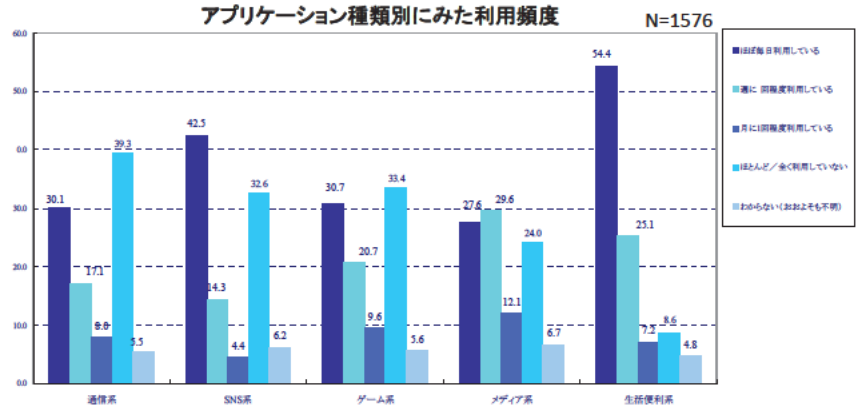


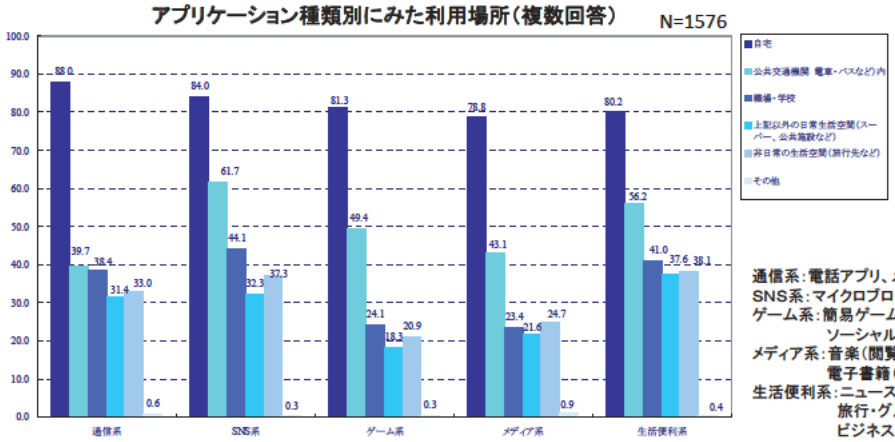
利用者アンケート調査結果①　アプリケーションダウンロード数





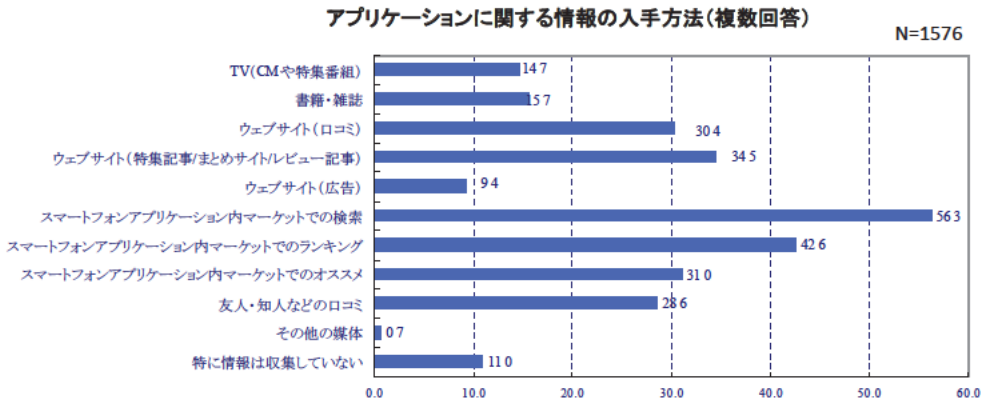
利用者アンケート調査結果②　アプリケーションの利用状況

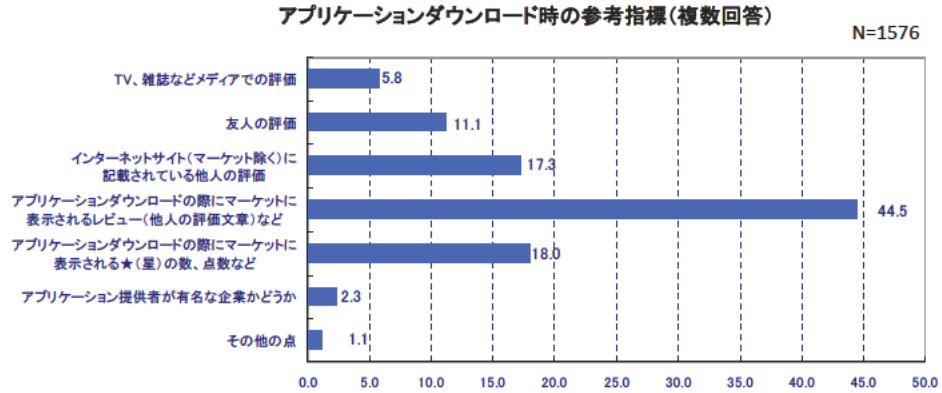




通信系：電話アプリ、メッセージアプリ等
SNS系：マイクロブログ含む
ゲーム系：簡易ゲーム、RPG、アクションゲーム、ソーシャルゲーム等
メディア系：音楽（閲覧、共有）、動画（閲覧、共有）、電子書籍（コミック、雑誌・新聞）等
生活便利系：ニュース・天気、地図、交通、旅行・グルメ（クーポン）、医療・健康、ビジネス（効率化、スケジュール）等

利用者アンケート調査結果③　アプリケーション入手に関する実態





利用者情報に係る諸外国の取組

■ 米国においては、本年（2012年）2月、
- ホワイトハウスが、消費者のオンライン・プライバシーを保護するため、消費者が自らの個人データに関して有する権利を明らかにしたプライバシー権利章典を発表
- カリフォルニア州司法長官が、プラットフォーム6社（アップル社、グーグル社、マイクロソフト社等）と、各事業者が運営するアプリケーション提供サイト等においてスマートフォン等のアプリケーションに係るプライバシーの保護に取り組むことで合意

■ 欧州においては、本年1月、EUの個人データ保護に関する1995年EUデータ保護指令を見直し、個人情報の一層の保護の図るための「個人データ保護規則」案を公表

米国		欧州	
プライバシー権利章典	カリフォルニア州司法長官とプラットフォーム事業者との合意	EUデータ保護指令の見直し（「個人データ保護規則」案）	
●「プライバシー権利章典」として、次の7箇条を規定 1. 個人によるコントロール 2. 透明性 3. 経緯の尊重 4. 安全性 5. アクセスと正確性 6. 対象を絞った収集 7. 説明責任 ● 今後、新しい権利章典に準ずる行動規範を検討する予定。	● カリフォルニア州法「オンラインプライバシー保護法」で定める基準を各事業者のアプリケーション提供サイトにおいて遵守することに合意 ・アプリケーションについて明示的なプライバシーポリシーの提示 ・ダウンロード前に利用者がプライバシーポリシーを確認できるようにすること ・収集する個人情報の種類・用途・提供先を示す 等	●より強固な個人データ保護ルールの整備 ・個人データ保護に関する個人の権利の強化（忘れられる権利） ・プライバシー・バイ・デザイン原則の導入、データ保護官の任命義務 ・個人データ漏えい時の通知義務 等 ● データ保護に関するグローバルな課題への対応 ・EU域内から域外の第三国への個人データの移動に関するルールの明確化・簡素化 等	

諸外国における現状：米国

・連邦取引委員会（FTC）が消費者保護に関する職務・権限（FTC法第5条で規定）を担う独立の機関として消費者のプライバシー保護を図っている。
・本年2月ホワイトハウスは、消費者のオンライン・プライバシーを守るための**プライバシー権利章典**を発表

消費者プライバシー権利章典
1 **個人のコントロール**：消費者は、事業者がどの個人データを収集し、どのように使用するかコントロールする権利を有する。
2 **透明性**：消費者は、プライバシー及びセキュリティの実務について、容易に理解しアクセス可能な情報を得る権利を有する。
3 **経緯の尊重**：消費者は、事業者が自分の個人データを、自らが情報を提供した経緯に沿う形で、収集、利用、開示することを期待する権利を有する。
4 **安全性**：消費者は、個人データが安全かつ責任をもって扱われる権利を有する。
5 **アクセスと正確性**：消費者は、データの機微性および不正確な情報が消費者にとって望ましくない結果を生むリスクに応じた方法で、利用可能な書式により個人データにアクセスし訂正する権利を有する。
6 **対象を絞った収集**：消費者は、事業者が収集・保有する個人データに合理的な制限を設ける権利を有する。
7 **説明責任**：消費者は、事業者が個人データをプライバシー権利章典に従って適切な手段を施されて扱われることを保証される権利を有する。
個人データの定義：集積されたデータを含むあらゆるデータであって、特定個人と結びつく（Linkable）もの。特定のコンピュータ又は他の装置と結びつくデータを含む（例：利用履歴を蓄積するスマートフォンや家庭用コンピュータの識別子等）

・本年2月**カリフォルニア州司法長官**は、スマートフォン等のアプリケーションに係るプライバシーの保護についてプラットフォーム6社（アマゾン社、アップル社、グーグル社、マイクロソフト社等）と合意。

●カリフォルニア州法「オンラインプライバシー保護法」で定める基準を各社アプリストアにおいて遵守することに合意。
（①アプリケーションについて明示的なプライバシーポリシーの提示、②ダウンロード前に利用者がプライバシーポリシーを確認できるようにすること、③収集する個人情報の種類・用途・提供先を示す、④違反するアプリを通報する仕組み、⑤プラットフォーム事業者による開発者への教育等）
●アプリ開発者のプライバシーポリシー違反は、州の不正競争行為又は虚偽広告法に抵触

カリフォルニア州司法長官とアプリマーケット事業者6社の共同声明

7

概要

- 2012年2月、米国カリフォルニア州のハリス司法長官が、アプリマーケットにおけるプライバシー保護強化について、アプリマーケット事業者6社（Apple社、Google社、Amazon社、Microsoft社、Hewlett-Packard（HP）社、Research In Motion（RIM）社）と合意したと発表した。
- ハリス長官は6か月以内にマーケットのプライバシー評価のため、事業者を招集する。

共同声明の位置づけ

- 司法長官とアプリマーケット事業者はアプリ開発者の消費者プライバシーを尊重すべきことの責務についての認識を向上し、プライバシーに関する行動の透明性向上を促すための原則を開発し、実施するため共同作業を実施。
- イノベーションを生むモバイルプラットフォームやアプリケーション開発者に不当に重い負担を強いることなく、消費者に一層の透明性とその個人データに対する一層のコントロールを与えるための創造的で前向きな解決策に合意。
- 共同声明は、法的拘束力ある責務を課したり、法令に基づく既存の責務に影響を与えることは意図しない。

合意の概要

1. 利用者から個人データを収集するアプリはプライバシーポリシー等をはっきり掲示しなければならない。

2. アプリ提供サイト運営事業者は、アプリ開発者のプライバシー問題に関する認識を高めるための努力として、
   ①アプリのプライバシーポリシー等にハイパーリンクするための追加的なデータ領域
   ②アプリのプライバシーポリシーを記載するための追加的なデータ領域

3. 利用者がサービス条件や法令に従わないアプリを通報する方法をアプリ提供サイト運営事業者は設ける。

4. アプリ提供サイト運営事業者は、サービス条件や法令違反の事案の事案について通報を踏まえ対応する

5. アプリ提供サイト運営事業者は、①モバイルプライバシー一般に関するベストプラクティスや、②モデルモデルプライバシーポリシーを開発することについて司法長官と引き続き協力して取り組む。
   6ヶ月以内に、モバイルプライバシーに関する教育プログラムの有用性を含め、プライバシーを評価するために招集。

米国FTC　Protecting Consumer Privacy in an Era of Rapid Change 報告書（2012年3月）
～急速に変化する時代における消費者プライバシー保護～

8

対象

- 連邦取引委員会（FTC）は、3月26日、消費者のプライバシー保護のため、企業が採用すべき行動枠組みを提示する報告書を公表。これは、2011年12月に公表された、FTCスタッフレポートをベースとしてまとめたもの。
- 特定の消費者、コンピュータやその他の端末と合理的に関連付けることが可能な消費者のデータを収集または利用する、すべての商業主体が対象（但し、年間5,000人未満の顧客の、センシティブではないデータのみを扱い、第三者とデータを共有しない企業は除く。）

プライバシー枠組み

①Privacy by Design：企業は、商品・サービス開発のすべての段階において、消費者のプライバシー保護を促進すべき
②Simplified Consumer Choice：企業は、消費者の選択権をシンプルにするべき
③Greater Transparency：企業は、プライバシーの取扱いの告知やアクセス権の透明性を増進させ、消費者教育により理解を増進させるべき

FTCが支援する5分野

①追跡禁止（Do not track）
→ 業界団体により、ブラウザベースで追跡拒否が可能なツールが開発されるなど、著しい進展を見せている。FTCとしては、これらの団体と協力し、使いやすく、永続的かつ効果的な追跡拒否システムの実施に向けて作業していく。

②モバイル（Mobile）
→ FTCは、モバイルサービスを提供する会社に対して、開示制度も含むプライバシー保護に向けて取り組むことを求めており、本年5月30日に主催するワークショップで、特にモバイルのプライバシー開示の課題に取り組む。

③データブローカー（Data Broker）
→ FTCは、消費者が、データブローカーが保持する自分のデータにアクセスを可能にするための法案を支援する。また、透明性向上のため、ブローカーに対し、誰が、どのようにデータを集めているのか特定し、消費者に対してアクセス権を説明するよう求めている。

④大規模プラットフォーム事業者（Large Platform Providers）
→ 大規模プラットフォーム（ISP、オペレーティングシステム、ブラウザ、ソーシャルメディア）が、消費者のオンライン上の全行動の追跡をする限り、プライバシーに対する懸念を増加させている。FTCは、2012年下期にワークショップを開催する予定。
※ Google、Facebookなどは、急速に業務を拡大しているが、現時点では消費者のインターネット上の全行動を追跡できるまでには至っていないため、上記のレベル程度のプライバシーの懸念はないとしている。

⑤強制力のある自主規制規範の推進（Promoting Enforceable Self-Regulatory Codes）
→ 商務省は、現在、分野毎の行動規範作成に取り組んでいる。FTCもこれに参画し、FTCの法執行の際、当該規範に準拠をしていることを有利に扱うこととする。

諸外国における現状：欧州

・2012年1月に、EUの個人データ保護に関する現行基本法である1995年EUデータ保護指令を見直す「個人データ保護規則」案を公表。

個人データの定義：データ主体に関連する（relating to）あらゆる情報を意味する（第4条(2)項）

1 EU域内における規制の単一化・簡素化
- ・EU法令が全加盟国に同一に適用されるよう、国内法制化の不要な「規則」に変更。※EU規則は各国に直接適用
- ・事業者による事務負担（行政手続等）の簡素化
  （事業者がEU域内のうち一のデータ保護当局の承認を得れば、他国の当局からの承認を不要とする制度の導入）
- ・EU加盟国のデータ保護当局間の円滑な協力メカニズムの創設
  （EU加盟国のデータ保護当局は、他の加盟国の当局からの求めに応じて調査等の協力を行う制度の導入）

2 より強固な個人データ保護ルールの整備
- ・個人データ保護に関する個人の権利の強化
  （「忘れられる権利」（個人の求めに応じ、ネット上にアップロードされた個人データの削除の義務化）の導入 等）
- ・事業者による個人データ処理に関する説明責任の強化
  （「プライバシー・バイ・デザイン」原則の導入（サービス導入に際しプライバシー対策を考慮）、データ保護官の任命義務等）
- ・個人データのセキュリティの強化（個人データ漏えい時の通知義務）
- ・データ保護に関する個人の権利行使方法の改善
  （EU加盟国のデータ保護当局の独立性及び権限の強化、行政及び司法による救済策の強化）

3 データ保護に関するグローバルな課題への対応
- ・EU域内居住者に対する商品・役務の提供を行う場合、域外の事業者による個人データの取扱いにも法令の効力を及ぼすための規定を整備
- ・EU域内から域外の第三国への個人データの移動に関するルールの明確化・簡素化

4 その他
- ・新たな制裁の導入（企業の全世界での売上高の最大2%相当額の課徴金） 等

諸外国における現状：民間団体における取組

■ モバイルマーケティングアソシエーション（MMA）（2011年12月）
・アプリケーション開発者が消費者にプライバシーポリシーを伝えられるように「モバイル・アプリケーション・プライバシーポリシー」を発表（※なお、実際の作成時には専門家への確認を強く推奨）

●アプリケーション開発者がプライバシーポリシーを作る際の参考となるように作成。それぞれ記載事例を示している。
1 アプリケーションが取得する情報とその使用方法（①ユーザーにより提供される情報、②自動的に取得される情報）
2 正確なリアルタイム位置情報取得について（※郵便番号や市町村による大まかな位置情報取得を除く）
3 取得された情報の第三者提供について
4 自動取得情報及び広告について（※広告配信を行う場合に記載）
5 利用者のオプトアウトの権利について（※アプリケーション削除、ターゲティング広告配信拒否、位置情報取得拒否等）
6 データ保持及び利用者情報の管理について
7 子供の情報の取扱い（※COPPA対応等）
8 セキュリティについて
9 プライバシーポリシーの変更
10 利用者の同意事項
11 連絡先情報

■ 携帯通信事業者の業界団体GSMA（2012年1月）
・携帯端末向けのプライバシー原則（Mobile Privacy Principles）、**プライバシーデザインのガイドライン**（Privacy Design Guidelines for Mobile Application Development）**について発表。**

●背景：携帯電話とウェブが融合し利用者は様々なサービスを享受。利用者情報の活用がこの革新的ビジネスモデルや個人への最適化を支えているが、一方利用者の個人情報への不正なアクセスを引き起こすおそれもある。法的に問題がなくとも、利用者のプライバシーへの期待を裏切り、利用者の携帯事業そのものへの信頼を損ねてしまう恐れがある。
●対象：アプリケーションとモバイル端末に関連するプライバシーデザイン（アプリ開発者、機器製造事業者、プラットフォーマー、OS事業者、通信キャリア、広告や情報分析事業者など関連する全ての主体に適用）
●目的：“Privacy by Design”アプローチを採用し、モバイル・アプリケーションの開発時にユーザーのプライバシーや個人情報の尊重や保護に関する確認の手助けとなること。
●個人情報（Personal information）：個人に関連づけられた情報であり、個人を識別するために利用されるもの。ユニークな識別子を利用しても個人を識別することができる。

補足資料：GSMAプライバシーデザインのガイドラインの概要

■ 携帯通信事業者の業界団体GSMAプライバシーデザインのガイドラインの概要（2012年1月）

1 透明性とユーザーによる選択とコントロール(TCC)
①ユーザーに個人情報の収集項目、利用目的、利用方法等について事前に通知（位置情報や電話帳については十分配慮、目的変更について改めて説明）
②誰が情報を取得するのか利用者に通知する（名称・連絡先を明記）
③利用者に十分プライバシーに関する説明を行う（プライバシー・ポリシーをアプリに係る最初のページ等へ表示）
④最小限の情報収集と限定された利用
⑤必要な時にはユーザーの積極的合意を得る（位置情報、アプリに直接必要のない情報収集、第三者提供、情報蓄積）
⑥ユーザーに一定の頻度で再度確認する
⑦秘密のアップデートの禁止

2 データの保存とセキュリティ(DRS)
①識別子の管理（識別子を正確かつ最新に保ち、正当なユーザー以外に割当てない）
②データーの安全性確保（UDIDや携帯番号、電話帳、金融情報等の慎重に扱うべき個人情報の取得送信方法等）
③安全性確保のための認証
④データの保管及び削除期間（個人情報は事業目的等に応じ不要となった際には破棄または匿名化される）

3 教育(E)
①利用者教育（プライバシー管理の設定や手法について、利用者にオンライン等で分かりやすく伝える）

4 ソーシャルネットワークとソーシャルメディア(SNS)
①登録情報の扱い（登録時に任意提供である情報は明示する、自動収集情報は利用者が確認するまで公表しない）
②初期設定がプライバシー保護的であること、利用者に各自情報を簡単にコントロール可能とすること
③青少年保護のための措置
④アプリやアカウントの無効化又はデータ削除する手段の提供

補足資料：GSMAプライバシーデザインのガイドラインの概要（つづき）

■ 携帯通信事業者の業界団体GSMAプライバシーデザインのガイドラインの概要（2012年1月）

5 モバイル広告(MA)
①広告配信機能について利用者に通知する（広告を配信する予定であることを、広告アイコンや短い通知で知らせる）
②ターゲティング広告について利用者の同意を取得（ターゲティングの手法や範囲、第三者提供、オプトアウト方法等）
③ターゲティング広告は合法的に取得された情報を利用（位置情報、他アプリやサイト利用による情報利用は限定的に）
④バイラルマーケティングにおいてプライバシーを配慮（電話帳利用は利用者の明示的同意が必要）
⑤広告内容が適切であること（想定されうる年齢層に適切な内容であること）

6 位置情報(L)
①利用者に位置情報の利用を通知し選択権を与える（位置情報の種類、保存期間、第三者提供等）
②位置情報の利用について適切な同意を得る（履歴を保持する場合、位置情報の種類、利用目的、保存期間、広告利用等同意を得ない限りバックグラウンドにおける位置情報収集やシェアは行わない、後からユーザーが設定変更可能）

7 青少年(CA)
①適切な年齢層に合わせたアプリケーションの作成（青少年の個人情報を収集・利用するリスクを考慮し対応）
②プライバシー保護を初期設定とすること（詳細な位置情報の共有制限、電話帳情報の収集制限等）
③子供を保護する法令の順守
④適切な場合には年齢確認を行う（年齢詐称の防止）

8 説明責任等(AE)
①ビジネスプロセス全体を通じた利用者のプライバシー確保のための責任
②アプリの問題を報告するための手法の提供

アンドロイドOSによる利用許諾画面

（※Google Playから入手したアプリをもとに総務省作成）

アンドロイドOSによる利用許諾の説明例

①種類	②項目	③説明	（参考）取得可能な情報
電話／通話	端末のステータスとIDの読み取り	端末の電話機能へのアクセスをアプリに許可します。許可すると、アプリではこの携帯端末の電話番号やシリアル番号、通話中かどうか、通話相手の電話番号などを特定できるようになります。	端末識別ID（IMEI）、加入者識別ID（IMSI）、電話番号、通話相手の電話番号等
アカウント	既知のアカウントの取得	携帯端末で認識済のアカウントリストを取得することをアプリに許可します	Googleアカウント（Gmailアドレス）
個人情報	連絡先データの読み取り	携帯端末に保存されているすべての連絡先（アドレス）データの読み取りをアプリに許可します。	電話帳（氏名、電話番号、メールアドレス、住所等の電話帳に記録された情報）
	カレンダーの予定と機密情報の読み取り	携帯端末に保存されているすべてのカレンダーの予定（友達や同僚の予定も含む）を読み取ることをアプリに許可します。	予定表に記載されたデータ
	機密ログ　データの読み取り	システムの各種ログファイルの読み取りをアプリに許可します。許可すると、アプリでは携帯端末の使用に関する全般的な情報を読み取れるようになります。	実行されたアプリ名、アプリから出力される情報、Webアクセス履歴、通話相手の電話番号等
現在地	おおよその位置情報（ネットワーク基地局）	携帯端末のおおよその現在地を特定できる情報源（セルラーネットワーク　データベースなど）がある場合は、その情報源にアクセスします。	携帯電話基地局、WiFi基地局を使った位置情報
	精細な位置情報（GPS）	携帯端末上で正確な現在地を特定できる情報源（GPSなど）を利用できる場合は、その情報源にアクセスします。	GPSを使った位置情報
システムツール	実行中のアプリの取得	現在実行中のタスクまたは最近実行したタスクに関する情報の取得をアプリに許可します。	実行されたアプリ名
ハードウェアの制御	画像と写真の撮影	カメラでの画像と動画の撮影をアプリに許可します。	カメラ撮影される画像の収集
ネットワーク通信	完全なインターネットアクセス	ネットワークソケットの作成をアプリに許可します	－

スマートフォンに関連する主なID①

15

		概要	データの詳細
OS	Android ID	Android OSにおいて端末を識別する番号。 アプリにおいて端末識別のために多く用いられる。アプリはこれを利用するためにパーミッションは不要。	端末内に記録される16桁の16進数。端末初期化により、再生成される。
	UDID：Unique Device Identifier （独自端末識別番号）	iOSにおいて端末（iPhone/iPad/iPod）を識別する番号。	端末内に記録される40桁の16進数。ユーザによる変更不可。
	ECID：Exclusive Chip Identification	iOSにおいて、端末のファームウェアアップデートの際に端末識別に用いられる番号。	端末内に記録される16桁の16進数。ユーザによる変更不可。
契約者	IMSI：International Mobile Subscriber Identitiy （国際移動体加入者識別番号（加入者識別ID））	GSMおよびW-CDMAの携帯電話加入者に割り当てる識別番号。電話番号と1対1で対応して携帯電話での通信に用いられる。 Android OSにおいて、アプリがこれを利用するためにはRead_Phone_Stateのパーミッションeが必要。ユーザによる変更不可。	SIMに記録される最大15桁の10進数。 国・事業者の別、個々の加入者に割り振られた番号等から為る。ユーザによる変更不可。
	ICCID：Integrated Circuit Card Identifier（ICカード識別番号）	ICカード（SIMカード）の識別番号。SIMカードを含むICカードそのものの識別に用いられる。Android OSにおいて、アプリがこれを利用するためにはRead_Phone_Stateのパーミッションが必要。	SIMに記録される最大19桁の10進数。 産業・事業者の別、個々のカードに割り振られた番号等から為る。ユーザによる変更不可。
	MIN：Mobile Identification Number （移動体識別番号）	AMPS/TDMS/CDMA方式の携帯電話加入者に割り当てられる番号。GSM方式のIMSIにあたる。	SIMに記録される10桁の10進数。
端末	IMEI：International Mobile Equipment Identity（国際移動体装置識別番号（端末識別ID））	端末識別番号とも言い、GSM/W-CDMA/iDENの全ての携帯電話や一部の衛星電話に付与される識別番号。GSMネットワークにおいて端末の正当性を確認するために用いる。盗難機器に対してネットワークへの接続を拒否することも可能。 Android OSにおいて、アプリがこれを利用するためにはRead_Phone_Stateのパーミッションが必要。	端末に記録される15桁の10進数。端末製造メーカー、機種、個々の端末に割り振られた番号等から為る。ユーザによる変更不可。
	MEID：Mobile Equipment Identifier	TDMA/CDMA方式の携帯電話に付与される識別番号。GSM方式のIMEIにあたる。	端末に記録される14桁の16進数。ユーザによる変更不可。
	MACアドレス：Media Access Control Address	LANカードなどのネットワーク機器に原則として一意に割り当てられる識別番号。機器間の通信に用いられる。Android OSにおいて、アプリがWi-Fiで用いるMACアドレスを取得するにはACCESS_WIFI_STATEのパーミッションが必要。	機器に記録される12桁の16進数。機器ベンダー番号と個々の機器に割り振られた番号等から為る。原則変更不可。

スマートフォンに関連する主なID②

16

	概要	データの詳細
UUID：Universally Unique Identifier （汎用一意識別子）	汎用一意識別子と言い、世界で一意な識別子として使用される乱数。ただし、絶対に一意であることを保証するものではなく、生成される識別子の数が(約$3.40282366 \times 10^{38}$) と非常に大きいため、同じ識別子が生成される確率がきわめて小さいというもの。	32桁の16進数。 UUIDの実装例としてMicrosoftのGUID(Globally Unique Identifier)がある。
Open ID	ID管理手法の一実現形態。認証サイトである、OpenID provider(OP)は、利用者を認証し、その結果をサービス提供者に提供することで、認証の一元化（シングルサインオン）を実現する。	IDはURLの形式をとる。 例）http://userid.openid.ne jp OpenID.ne.jp（http://www.openid.ne.jp/）上でOpen ID アカウントを登録することでID、パスワードを作成する。
ODIN：Open Device Identification Number	米国モバイル広告事業者8社が賛同する、モバイル広告におけるUDID代替手段。とりあえずの代替手段として、MAC Adderss(iOS)、Android ID(Android）又はDeviceUniqueID（Windows Phone)のハッシュ値を用いるODIN1規格を策定。	IDはUDIDとのデータ互換性を考慮し40桁の16進数。 Open Device Identification Number (http://code google.com/p/odinmobile/) OpenUDIDとの連携が模索されており、ODIN2で統合される可能性がある。
OpenUDID	米国モバイル広告事業者17社が賛同する、モバイル広告におけるUDID代替手段。米国Adfonic社が開発し、オープンソースとして公開されている。契約者・端末固有IDと異なり、オプトアウト機構を備えるなど、UDIDの問題点を解消するものとなっている。	IDはUDIDとのデータ互換性を考慮し40桁の16進数。 OpenUDID (https://github com/ylechelle/OpenUDID) 事業者ごとに異なるIDを発番する、secureudid (http://www secureudid.org/)というプロジェクトも存在する。

	概要	データの詳細
Cookie	Webサイトの提供者が、Webブラウザを通じて訪問者のコンピュータに一時的にデータを書き込んで保存させる仕組み。Cookieにはそれぞれ有効期限を設定することができ、有効期限を過ぎたCookieは消滅する。	Cookie名、Cookie送信先ドメイン、有効期限等が記載されたテキストファイル。

セキュリティソフトウェア（Androidスマートフォン（個人利用）向け）機能一覧

		カスペルスキー モバイルセキュリティ9 （カスペルスキー）	ノートン モバイルセキュリティ （シマンテック）	ウイルスバスター モバイル for Android （トレンドマイクロ）	マカフィー モバイルセキュリティ （マカフィー）
ウィルス対策	スキャン機能	手動/自動（ファイルアクセス時）	手動/スケジュール/自動（アプリインストール時）	手動/自動（アプリインストール時）	手動/スケジュール/自動（アプリインストール時、SMS/MMS送信時、SDカード挿入時、起動時）
	ウイルス定義	手動/自動更新	自動更新	自動更新	自動/手動更新
	その他	–	–	–	Permission一覧表示やアクセスするサイト一覧表示等
盗難・紛失対策	GPSによる盗難・紛失端末位置検索	Web経由：○/SMS利用：○	Web経由：○/SMS利用：○	Web経由：○/SMS利用：×	Web経由：○/SMS利用：○
	端末内データの遠隔消去	Web経由：×/SMS利用：○	Web経由：×/SMS利用：○	Web経由：○/SMS利用：×	Web経由：○/SMS利用：○
	SIMカード差し替え時の挙動	・端末自動ロック ・新しい電話番号を登録された宛先に対しSMSを送信	端末自動ロック	端末自動ロック	・端末自動ロック ・新しい電話番号を登録された宛先に対しSMSを送信
	遠隔ロック	Web経由：×/SMS利用：○	Web経由：○/SMS利用：○	Web経由：○/SMS利用：×	Web経由：○/SMS利用：○
	その他	–	・紛失時、Web経由で遠隔写真撮影 ・SMS送信によるアラーム鳴動	Web経由でのアラーム鳴動	・ロック画面のメッセージの変更 ・Web経由でのアラーム鳴動
電話・SMSフィルタ		ブラックリスト/ホワイトリスト	ブラックリスト	・ブラックリスト/ホワイトリスト ・キーワード（SMSフィルタ）	・ブラックリスト/ホワイトリスト ・キーワード（SMSフィルタ）
利用者情報保護		通話/SMS履歴、電話帳のパスワード保護	–	セキュリティソフトウェア自身の削除をパスワードにより保護	セキュリティソフトウェア自身の削除をパスワードにより保護
ブラウザ保護		–	危険なサイトへのアクセス遮断	・危険なサイトへのアクセス遮断 ・ペアレンタルコントロール機能	危険なサイトへのアクセス遮断
その他		–	–	–	クラウド上へのデータバックアップ及びリストア

※Web経由：PC等で専用のWebサイトに接続し、紛失端末の位置検索等の操作を行う。
SMS利用：セキュリティソフトウェアを搭載した紛失端末に対し、SMSを送信することによって、当該端末の操作を行う。

（別紙）

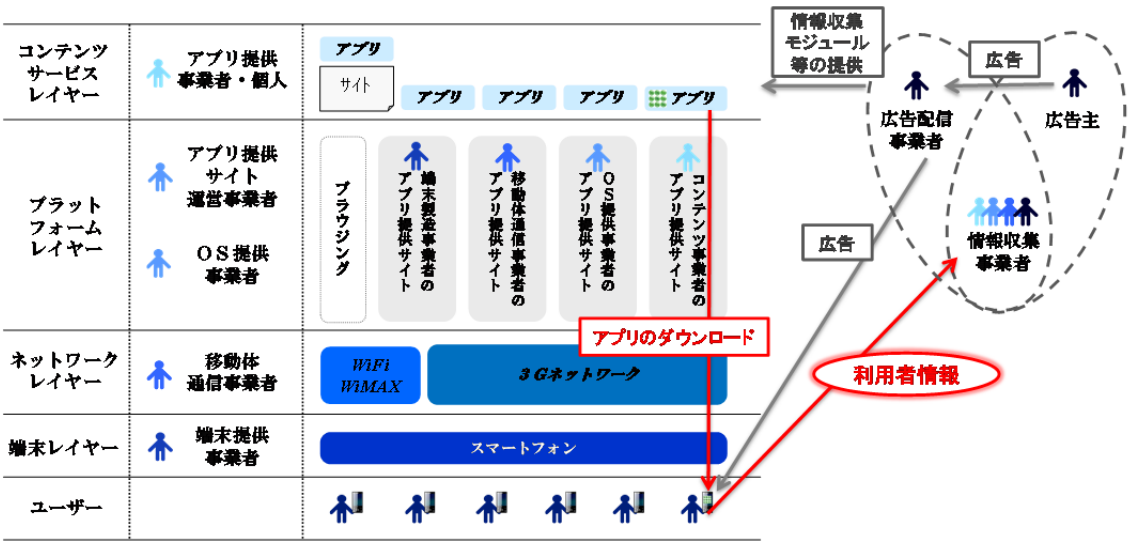
スマートフォン プライバシー ガイド

スマートフォンが急速に普及する中、スマートフォン上の利用者情報が様々なサービス提供等に利用されています。利用者情報の取扱いは、関係する事業者において適正に行われるべきものですが、スマートフォンの利用には自己責任が求められる側面もあるため、スマートフォンの利用者自身が少なくとも注意すべき事項について、「スマートフォン プライバシー ガイド」として取りまとめました。

1　スマートフォンのサービス構造を知りましょう

- スマートフォンは携帯電話事業者のみによるサービスではありません。アプリケーション（アプリ）提供者やアプリ提供サイトの運用者など多くの事業者が、それぞれ役割を持ちサービスを提供しています。
- スマートフォンでは、インターネットを経由して多様なアプリを自ら選択してダウンロードの上利用することができます。その一方、利用者の自己責任が求められる側面もあります。
- 無料のアプリ等の中には、広告主からの広告収入等によって収益を得ることによりアプリの提供を実現しているものもあります。このような場合、アプリに組み込まれた「情報収集モジュール」と呼ばれるプログラムなどを通じ、利用者情報が情報収集事業者や広告配信事業者等へ送信される場合もあります。

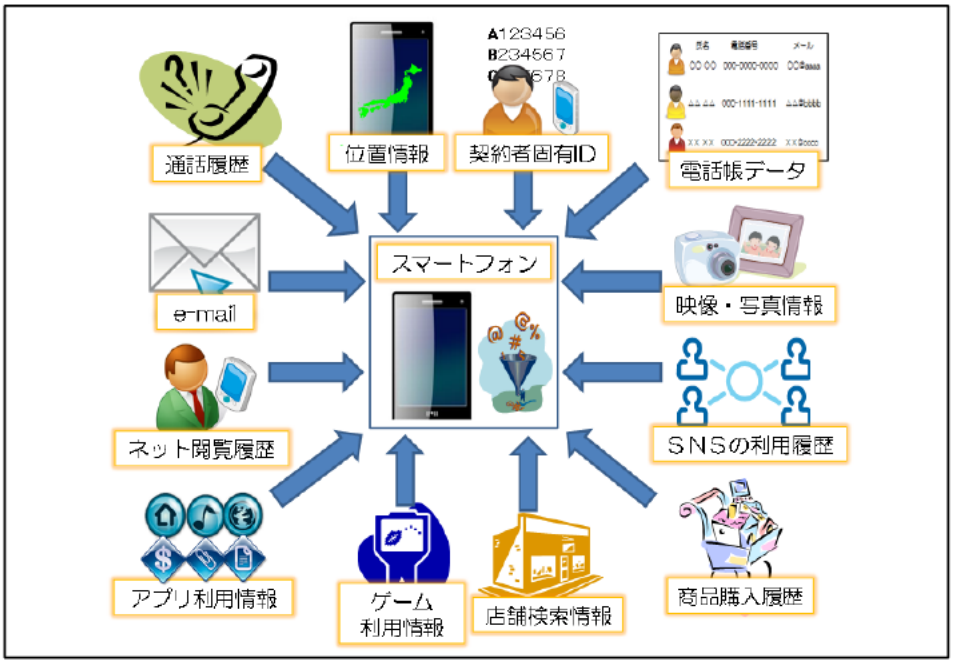
【スマートフォンのサービス構造】



2　アプリの信頼性に関する情報を自ら入手し理解するように努めましょう

- スマートフォンには、電話番号、メールアドレスなど連絡先の情報、通信履歴、ウェブページの閲覧履歴、アプリの利用履歴、位置情報、写真や動画など様々な利用者情報が蓄積されます。アプリをインストールすると、これらの情報は、アプリを通じたサービス提供に活用されるほか、広告配信事業者等へ送信され、利用者の趣味・趣向に応じた広告の表示等に利用される場合もあります。
- このように利用者情報が収集・送信されて利用されることについてプライバシー上の不安がある場合、利用者も受け身ではなく、アプリの機能や評判、提供者など、アプリの信頼性に関する情報を自ら入手し、理解に努めるようにしましょう。
- その場合、評価サイトの評価や利用者のコメント等を参考にすることもできますが、それでも不安な場合には利用を避けることも大切です。
- 携帯電話事業者及び端末ベンダーなどが安全性を確認しているアプリ提供サイトなども必要に応じて活用しましょう。

【スマートフォンにおける主な利用者情報】



3　利用者情報の許諾画面等を確認しましょう

- アプリの信頼性を確認するためには、利用者情報がどのような目的で収集されているか、必要以上の利用者情報が収集されていないかなどもヒントになります。
- アプリをダウンロードする時や利用（起動）する時などに、収集される利用者情報に関する利用許諾を求める画面が表示される場合があります。また、アプリの利用規約やプライバシーポリシーが定められ公表されている場合もあります。

・利用許諾画面や利用規約等において、収集される利用者情報の範囲などをよく確認し、内容を理解した上で、同意・利用するよう努めましょう。
・なお、利用許諾画面等が表示されない場合には、上記２の様々な方法によりアプリの信頼性の確認に努めましょう。

【利用者情報の利用許諾画面の例】

（※App storeから入手したアプリをもとに総務省作成）

（※Google Playから入手したアプリをもとに総務省作成）