資料１－２

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
中間取りまとめ（案）

平成２４年４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、2,000万台を超えると予測される。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、今年度末には端末総契約者数のうち20％以上がスマートフォン契約者となることが予測されるなど、幅広い層への普及が進んできていると言える。

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など多数の情報の取得・蓄積が可能である。様々なアプリ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」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。

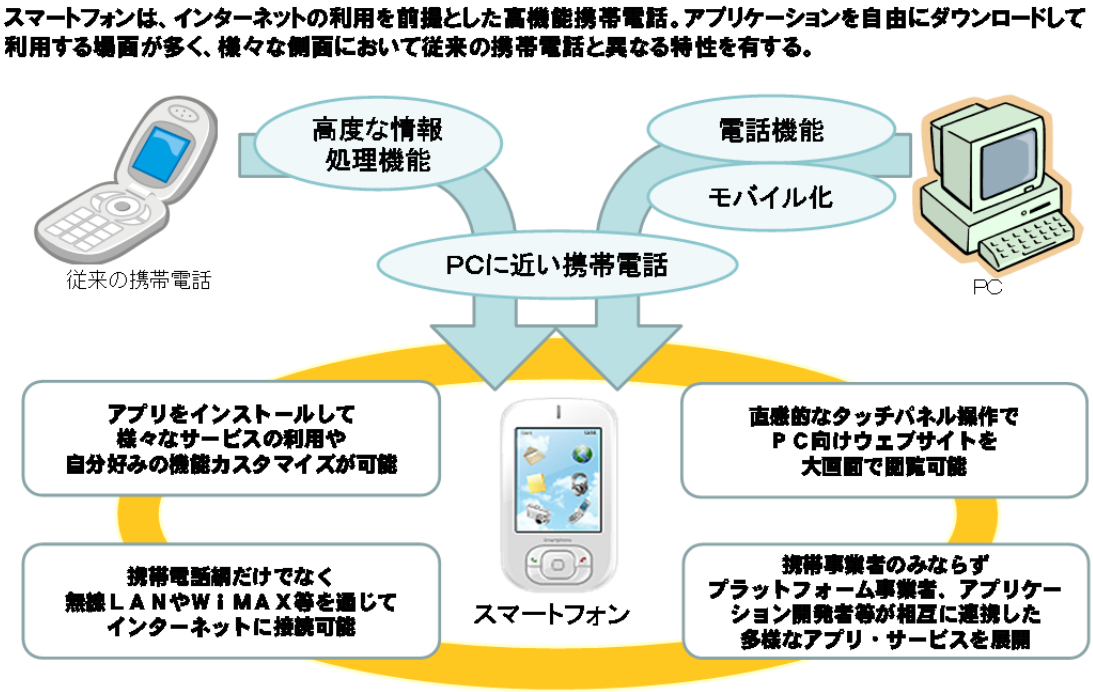
これらの要請を受けて、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」において「スマートフォンを経由した利用者情報の取扱いに関するWG」を設置することが決定された。2012年（平成24年）１月には第１回会合が開催され、より便利で多様なサービスが提供される環境を確保しつつ、利用者の情報が守られ、安全・安心にこれらサービスを利用者が享受し、選択することができるために、多様な関係者がどのような対応を行っていくことが望ましいか、精力的な検討が進められてきた。この中間取りまとめは、その議論の現段階までの成果を取りまとめたものである。

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見られ、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）上半期におけるスマートフォンの国内出荷台数は1,000万台を超えたとされており、全携帯電話端末出荷台数に占める比率も約半分となった。同年度通期の予測値では、スマートフォンの国内出荷台数は2,330万台、出荷台数に占める比率は56%となることが予測されており、今後更に一層の普及が見込まれる[1]。

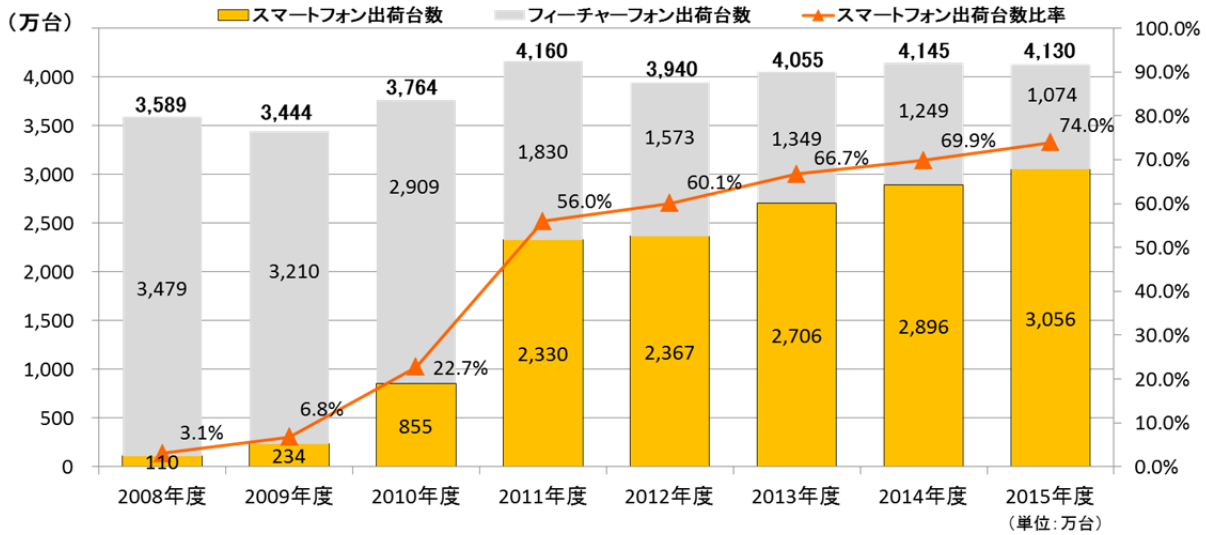
スマートフォンは、外出先を含むいつでもどこでもインターネット利用を容易とするものであり、スマートフォン利用者の携帯電話端末により様々インターネット利用が行われている。スマートフォンは通信環境によりその能力を発揮するが、我が国は3G回線普及率が世界

[1] 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（平成 23 年 7 月）」

的に比較しても非常に高く、WiMAX[2]等のBWA[3]やLTE[4]など更に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60%を越えるとの見通しもある。



	2008年度	2009年度	2010年度	2011年度	2012年度	2013年度	2014年度	2015年度
総出荷台数	3,589	3,444	3,764	4,160	3,940	4,055	4,145	4,130
うちスマートフォン出荷台数	110	234	855	2,330	2,367	2,706	2,896	3,056
スマートフォン比率	3.1%	6.8%	22.7%	56.0%	60.1%	66.7%	69.9%	74.0%

※ 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[5]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[6]が2009年（平成21年）7月にアンドロイド[7]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[8]。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。

---

2 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。

3 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。

4 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。

5 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。

6 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。

7 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。

8 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）

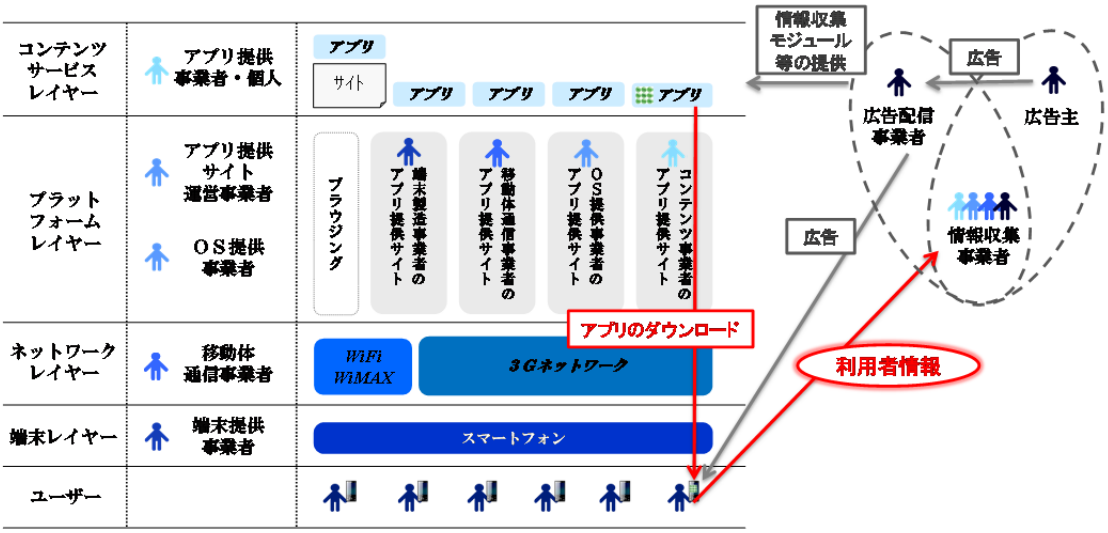
この中で、プラットフォームレイヤーにおいてスマートフォンに搭載されるオペレーティングシステム（OS）[9]を提供する者は、コンテンツやアプリケーション提供サイトの運営[10]も行っており、端末開発、通信ネットワーク利用、アプリケーション提供、課金や認証など各レイヤー[11]に影響力を有する存在であるといえる。

また、コンテンツサービスレイヤーにおいては、100万以上[12]のアプリケーションが提供されていると言われており、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、携帯キャリア等が提供するマーケットも存在する。さらに、大手SNS提供事業者などインターネットにおけるプラットフォーム提供事業者[13]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、無料若しく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、更には広告配信事業者が提供する情報収集モジュール[14]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。

【図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。

---

9 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。

10 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。

11 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。

12 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）。

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

14 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。

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

（1）スマートフォンにおける利用者情報の種類

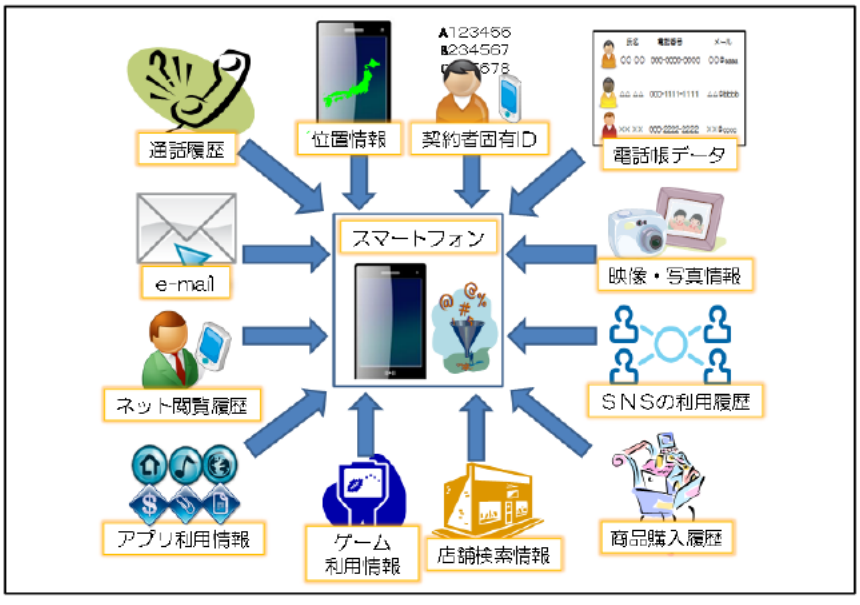
常に電源を入れて持ち歩くスマートフォンは、PCに比べて利用者との結びつきが強く、利用者の行動履歴や通信履歴など多数の情報の取得・蓄積が可能である。

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）、端末識別ID（IMEI）、加入者識別ID(IMSI)、MACアドレス等）が挙げられる[15]。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[16]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、GPS機器等が標準的に搭載されていることから、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、精度の高い位置情報も存在する。同様の情報には、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も含まれる。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[17]、システムの利用に関するログなどもこの区分に該当する。

【図4：スマートフォンにおける主な利用者情報】



15　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。

16　Web サイトの提供者が、Web 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。

17　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５：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）。
	契約者固有ＩＤ	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）、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[18]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[19]）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[20]。

① iOS

18 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

19 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。

20 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）。

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、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６－１】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[21]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[22]・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追加的記述がない限り表示されない[23]。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。

---

21 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。

22 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）。

23 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）

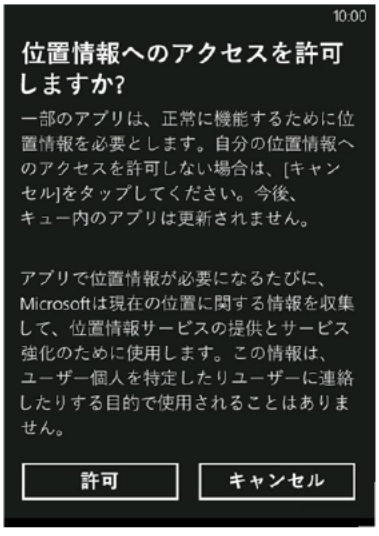
【図６－２：アンドロイドによる利用許諾画面[24]】

（※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、端末情報など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。

【図６－３　ウィンドウズフォンにおける利用許諾画面】



（資料提供：日本マイクロソフト（株））

24 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7－1： 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[25]	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 但しキャリア判断によるカスタマイズが可能。	Windows Phone Marketplaceのみ

【図7－2： 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[26]	@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（アンドロイド搭載端末）	au Androidスマートフォン（アンドロイド搭載端末）	ソフトバンクスマートフォン（アンドロイド搭載端末）
アプリケーション数	約1,000アプリ （2012年3月末現在）	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またはそのおそれのあるもの、マルウェアまた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。

25 2012 年（平成 24 年）3 月 7 日より名称変更。
26 2012 年（平成 24 年）3 月 1 日より名称変更。

（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[27]
- 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[28]
- 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[29]
- 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[30]
- 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[31]

（3）アプリケーションによる情報収集の実態

KDDI研究所[32]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

---

27 「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。

28 「アップティービー」（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。

29 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。

30 「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し、今後は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 を導入予定。「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。今後、同意した利用者の情報を収集を予定。「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。

31 「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

32 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）

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。

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[33]。

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など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ページ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、無料もしく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

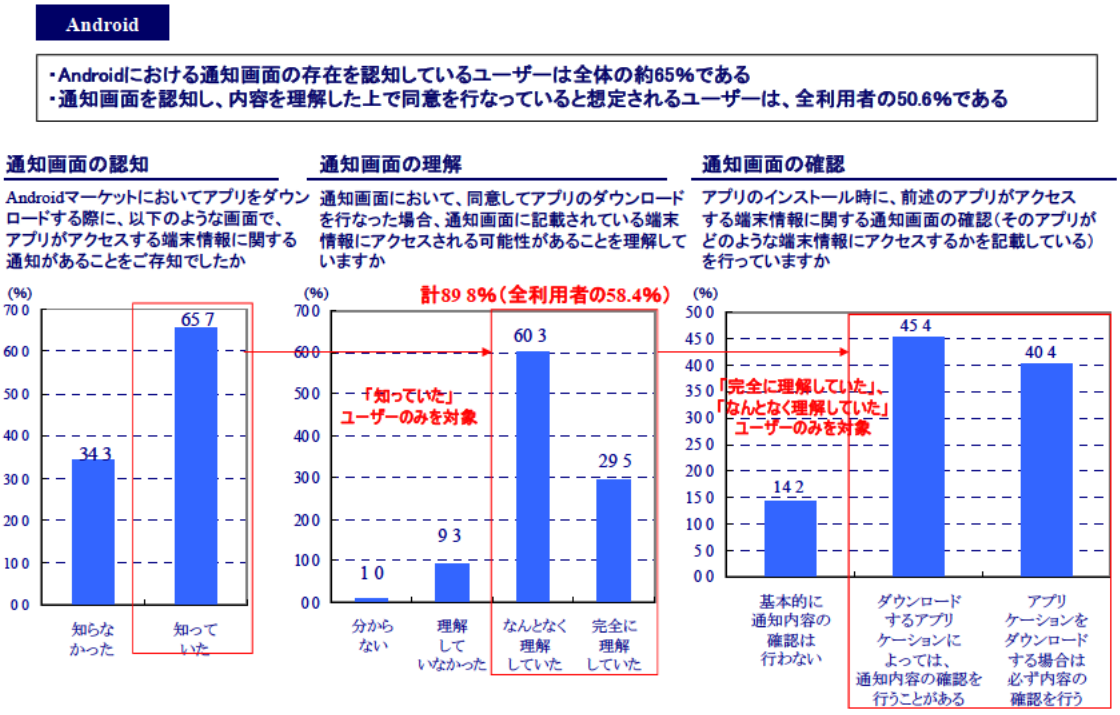
2012年（平成24年）2月に総務省が行ったウェブアンケート調査[34]によれば、通知・同意画面を理解し確認している利用者は5－6割程度いるが（図8－1、8－2参照）、8割のユ

[33] Web 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についてはカウントしていない。

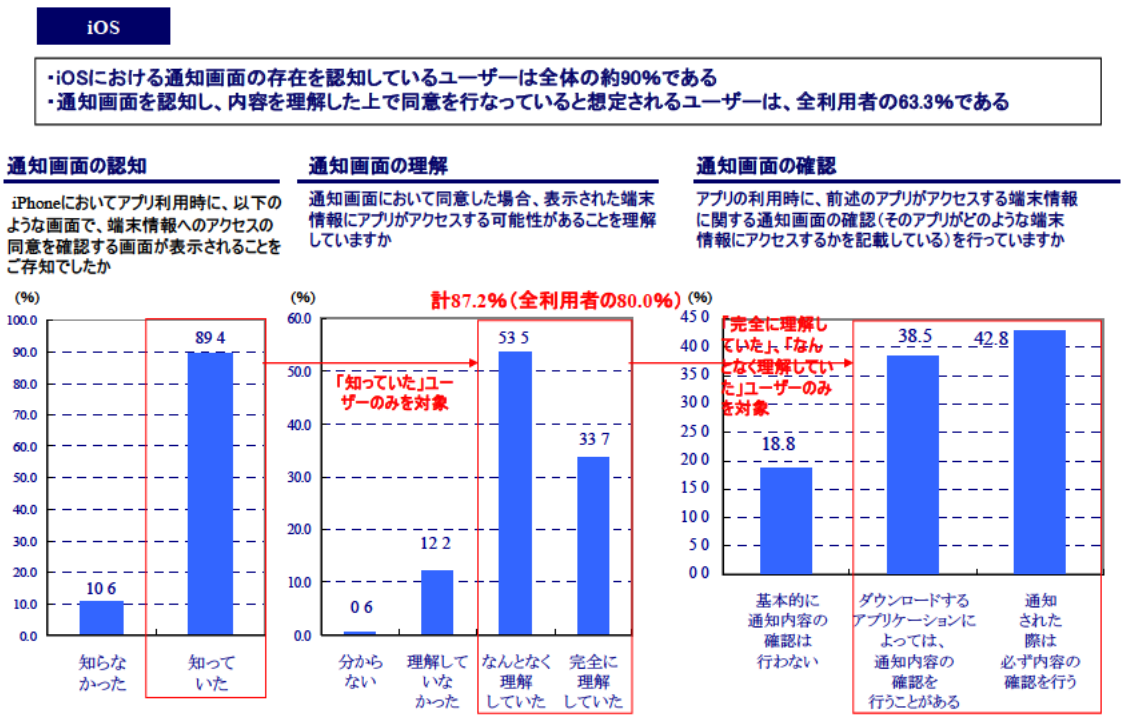
[34] 有効回答数 1,576 人、スマートフォン利用者を対象 OS、年代・性別に従って抽出（協力：株式会社日本総合研究所、NTT レゾナント株式会社）

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８－３、８－４参照。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８－４参照）。

【図８－１：通知画面の認知・理解・確認（アンドロイド搭載端末利用者）】



【図８－２：通知画面の認知・理解・確認（iPhone利用者）】

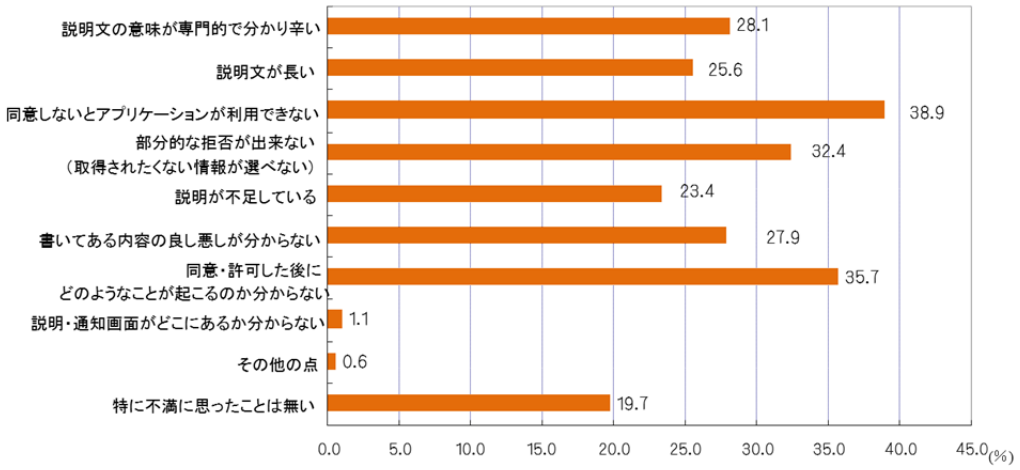


（※総務省ウェブアンケート調査結果）

【図８－３：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わからない」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）

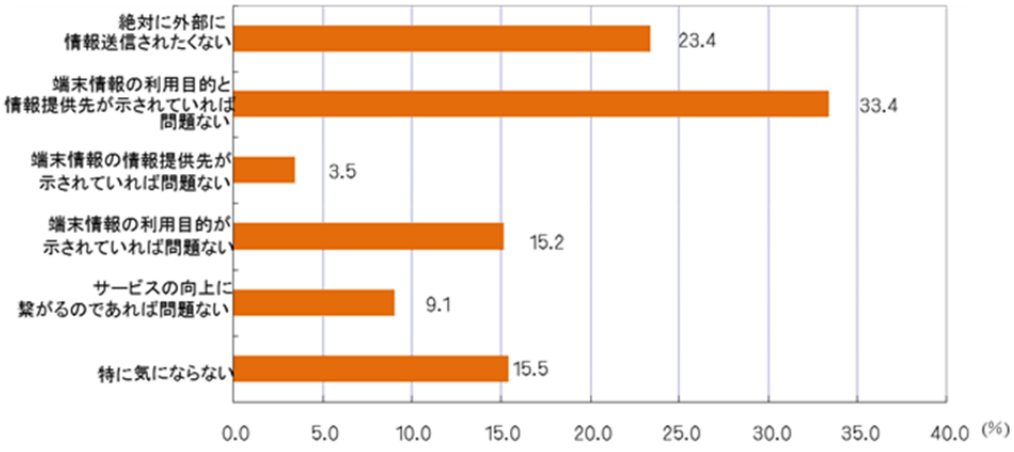


（注）平成24年2月総務省調査（有効回答数：1,576人、スマートフォン利用者を対象OS、年代・性別に従って抽出。
協力：株式会社日本総合研究所、NTTレゾナント株式会社）

【図８－４：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）

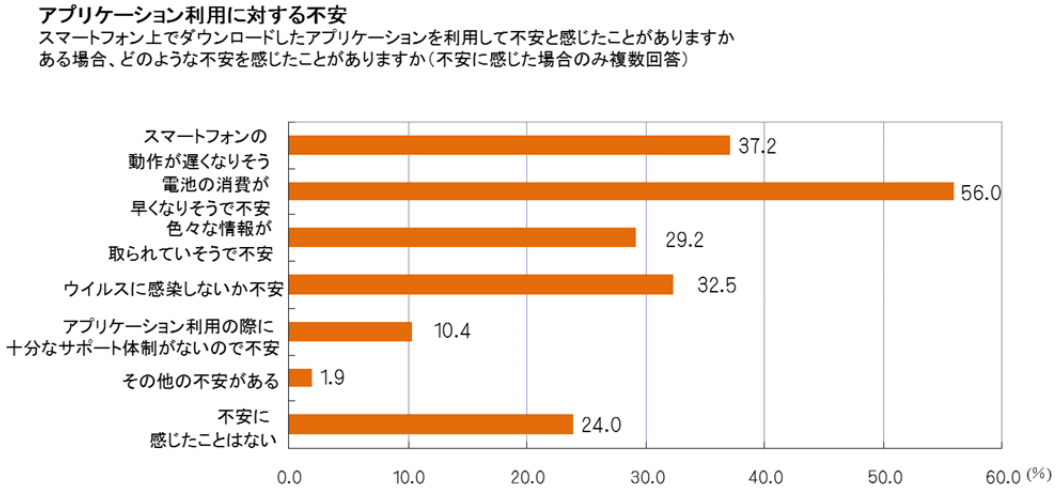


（※総務省ウェブアンケート調査結果）

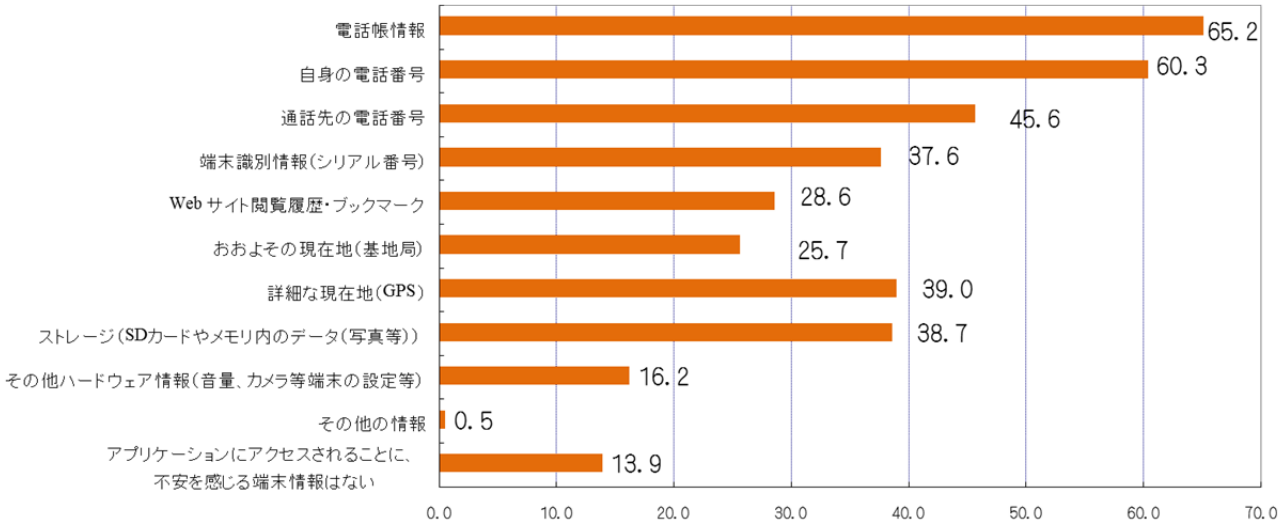
なお、アプリケーション利用に対する不安として、「色々な情報を取られていそうで不安」とする利用者は約3割程度おり（図８－５参照）、電話帳情報について約65％の利用者がアクセスされることに不安を感じるとしている（図８－６参照）。アプリケーションによるトラブルについては約7割の利用者が経験していない[35]（図８－７参照）が、アプリケーションによるトラブルに対して行ってほしい対応として総合的に問合せができる窓口の設置を約5割の利用者が望んでおり、自身の提供していた個人情報の削除を約4割の利用者が望んでいると回答している（図８－８参照）。

【図８－５：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



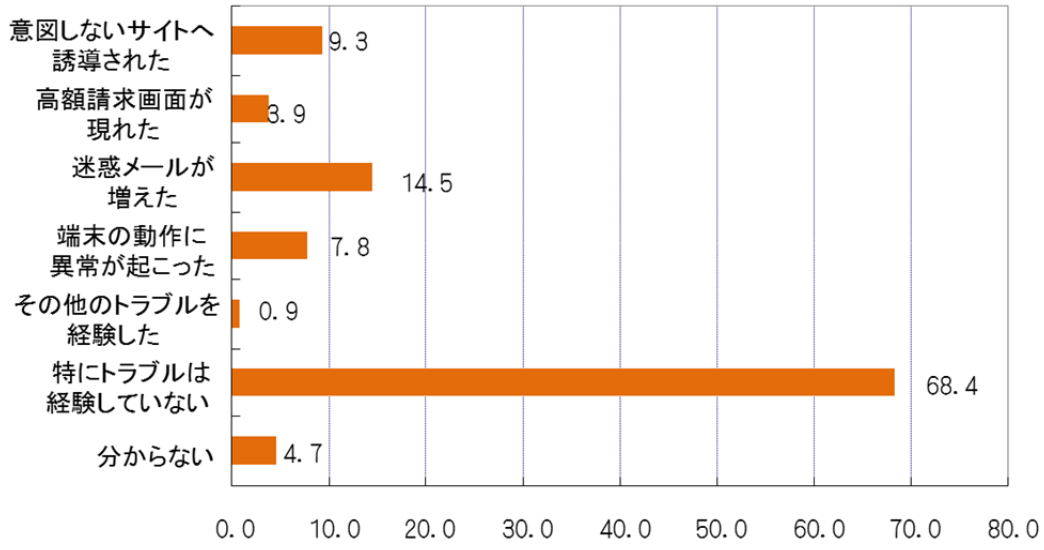
【図８－６：ユーザーがアクセスされることにより不安を感じる利用者情報】



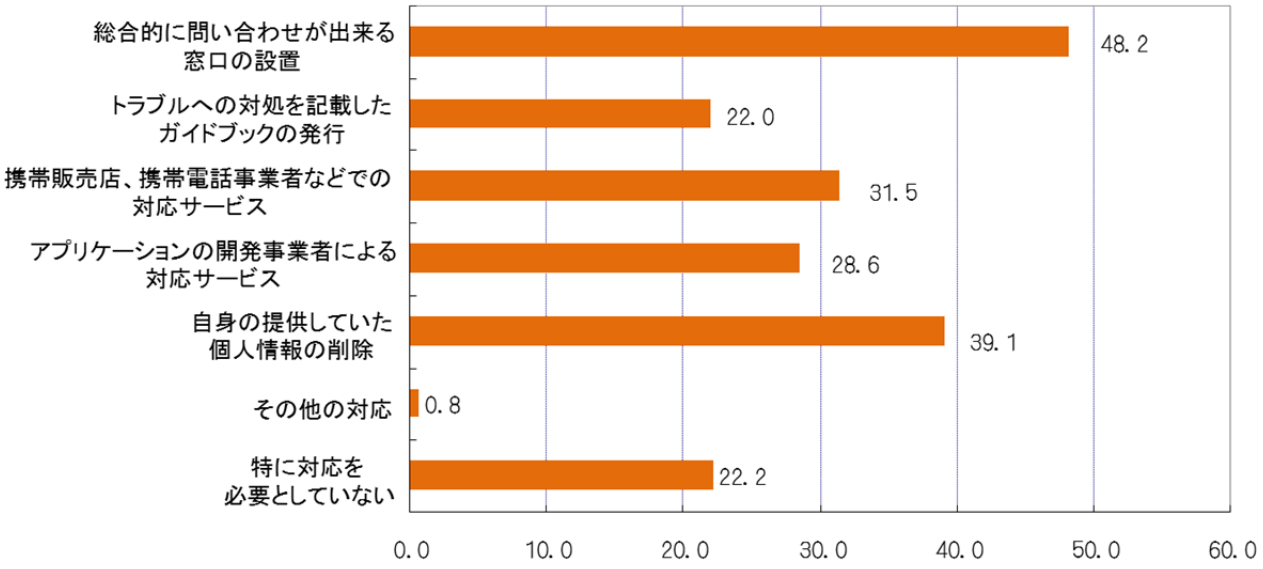
（※総務省ウェブアンケート調査結果）

35 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８－７：アプリケーションによるトラブル経験】



【図８－８：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９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

ュース系など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9：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・調査した結果を調査記事が発表されている[36]。

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Web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[37]。

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「Pandroa 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検事局が召喚状を発していたことを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[38]機能を付けるようにアップデートした[39]。

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[40]によれば、アン

---

36 『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。

37 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。

38 事前に同意を取得するということ。なお、我が国において、広告・宣伝メールについて事前に同意した者に対してのみ送信することが可能となっている。

39 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iPhone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 。

40 『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;

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[41]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[42]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時もiPhoneの位置情報について収集・記録[43]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[44]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[45]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。

---

http://www.cl.cam.ac.uk/~il235/HotMobile12_Leontiadis.pdf

41 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。

42 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。

43 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。

44 2011年４月21日発出されている。

45 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ＨＰ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（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[46]。

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[47]。 EU個人データ保護作業部会[48]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[49]）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。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、消費者による訴訟[50]も提起されるなど、世界的に様々な動きが見られた。

米国下院議員の書簡に対する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[51]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。

---

46 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。

47 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。

48 EU データ保護指令第 29 条に基づくデータ保護作業部会

49 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た。

50 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。

51 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。

【図10：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（WSJ）**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などに対し、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
	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。	

	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」**：Android 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）	**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。
	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スタッフレポート「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。	**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。

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、関連しうる国内法制度、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など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[52]」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[53]とされている。アプリケーションやサービス提供者や関係事業者が取扱う情報が「個人情報」に当たるか、「個人情報データベース等」に当たるか等については、今後の検討が必要であるが、仮にいずれかの者が「個人情報取扱事業者」に該当する場合には、個人情報保護法における以下の規定等が適用される。

- 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)。

52 個人情報保護法第２条第２項第１号
53 個人情報保護法第２条第３項

・ 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（または、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、最終改正平成23年11月２日）において、通信の秘密[54]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[55]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」の取り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、個人情報保護法をふ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。

---

54 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。

55 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）。

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など電気通信事業者が取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などがある。

（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などにより、ライフログ[56]を利活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。

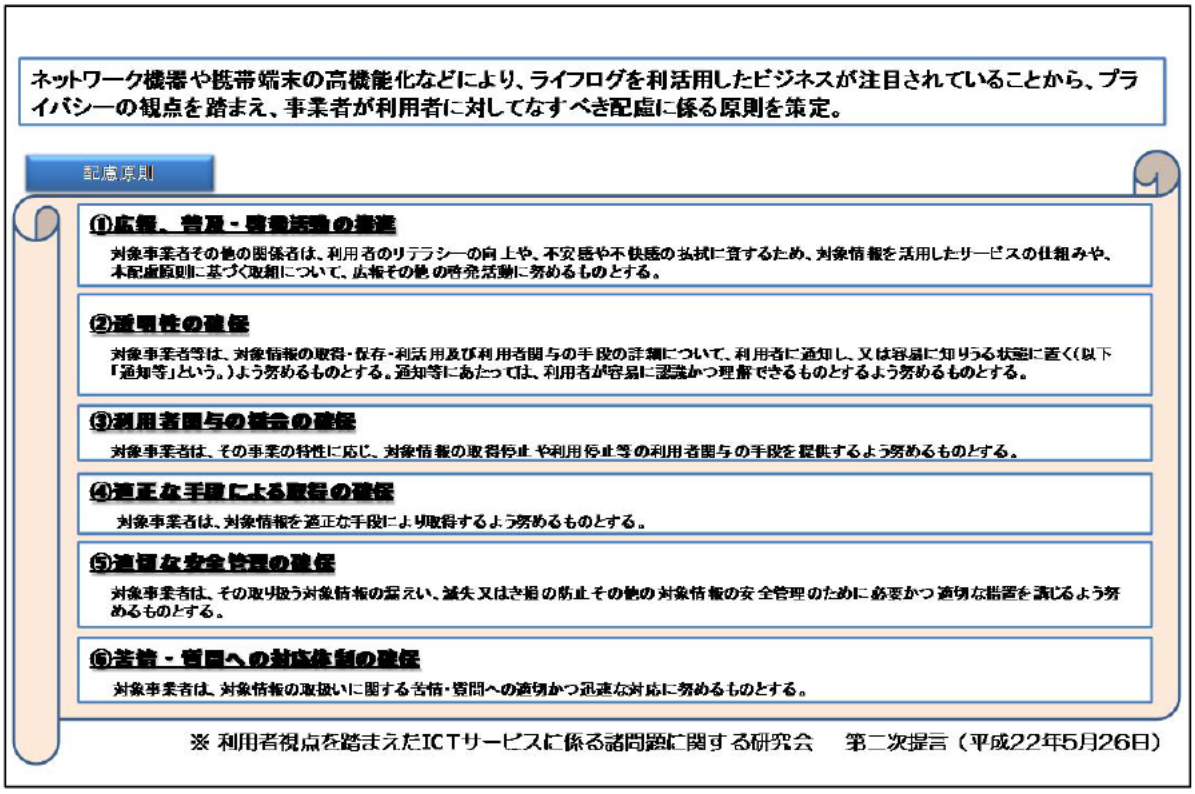
同提言において、揺籃期にあるサービスの現状を考慮し、規制色の強い行政等によるガイドライン化を避けて、事業者による自主的なガイドラインの策定を促すこととし、ライフログを取得・保存・利活用する事業者が利用者に対してなすべき配慮に係る緩やかな配慮原則が策定された。

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、

56 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苦情・質問への対応体制の確保の6項目となっている[57]。

【図11：配慮原則】



② 配慮原則を踏まえた民間による取組

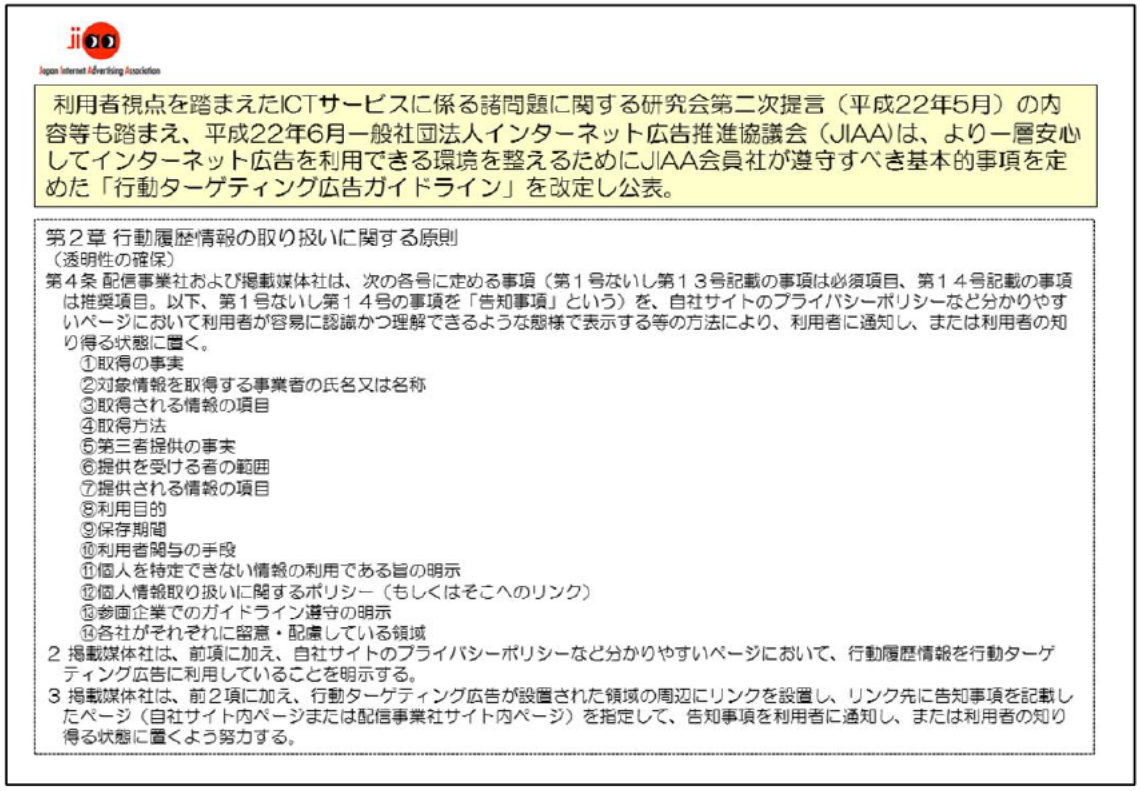
第二次提言における「配慮原則」を踏まえ、一般社団法人インターネット広告推進協議会（JIAA）は、2010年（平成22年）6月に「行動ターゲティング広告ガイドライン」を改定し、行動履歴情報の取扱いに関する原則規定を追記した。

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うると考えられる。

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など、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。

57 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

【図12：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。

（※JIAAホームページをもとに総務省作成）

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、欧州など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、民事制裁金などがある。

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など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。

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[58]。

エ スタッフレポート: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[59]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」をスタッフレポートとして発表した。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[60]、③データ販売業者[61]、④大規模プラットフォーム・プロバイダー[62]、⑤強制力のある自主規制基準の推進が挙

---

58 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

59 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、共有または利用するすべ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。

60 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。

61 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。

62 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、ウェブブラウザー、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。

げられている。

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箇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）[63]」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、個人データの定義は、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。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とされ、個人データ概念が従来の「特定の個人を識別される（identifiable）から」拡大されている（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）[64]。

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

63 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）。

64 第３回会合 石井構成員資料

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[65、66]。

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[67]。

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つくること、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るとされている。

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個人データ保護指令）」、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[68]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

---

65 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。

66 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。

67 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。

68 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）出来る。

情報を意味する」（第４条（２）項）こととされた[69]。EU域内における規制の単一化、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効力）、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１３：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、携帯端末向け広告の業界団体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[70]。

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[71]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。

---

69 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また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。

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

71 利用者側がサービス利用の停止を事後に求めることが出来る仕組みをいう。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）[72]、プライバシーデザインのガイドライン（Privacy Design Guidelines for Mobile Application Development）[73]を発表している[74]。

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など関連する全ての主体に適用されるものとして、“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などが定められている。 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[75]。

---

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

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

74 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恐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恐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うることが指摘されている。

75 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4章　利用者情報の性質・取扱いの在り方に関する主な論点

本章においては、スマートフォンにおける利用者情報が多様なサービス提供に活用されている現状を踏まえ、大きく2つの検討課題に分けて論点を検討する。

第一の検討課題は、利用者情報の取扱いの在り方である。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心・安全に利用できるよう、①利用者情報の性質・分類、②利用者情報の取得・管理・利用の在り方に関する主な論点につき検討する。なお、これら論点を今後検討する際には、第3章までに見てきたようなグローバルな状況や制度・取組との整合性についても留意することが必要である。

第二の検討課題は、利用者に対する周知の在り方である。今後我が国においてスマートフォンの一層の普及が見込まれる中で、青少年から高齢者まで、スマートフォンを安心・安全に利用できる環境を整備するため、どのような情報を、誰が、どのように周知すべきか利用者の視点から検討するに当たっても主な論点について検討する。

なお、各論点に対する詳細な検討については、WGの最終提言における取りまとめに向けて、今後本WGの中において議論を進めることとする。具体的には、スマートフォンのサービス構造において関与する多様な事業者や各関係者において、個人情報に関する法令遵守やプライバシーの保護、利用者の不安感に対する配慮などの観点から利用者情報の取扱いをどのように行う必要があり、また望ましい取組はどのようなものであるか検討を深める。

その際、スマートフォンが急速に普及し、様々なリテラシーレベルの方々が新たに利用者となる見込みであることから、利用者が必要な事項を分かりやすく理解し確認できるよう十分配慮することが重要である。また、スマートフォンにおけるサービスやアプリケーション提供はグローバルに行われていることから、グローバルな議論の動向にも十分配慮するものとする。最終提言においては、これら検討課題に対する検討結果を踏まえ、関係者[76]が今後それぞれ取り組むべき事項について提言を行うこととする。

なお、上述のように、利用者情報の適正な取扱いは関係事業者において行われるべきものであるが、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ことから、利用者が自らのプライバシーを守るために少なくとも知っておくべきこと、とるべき行動について、「スマートフォン　プライバシー　ガイド」（別紙）を取りまとめ、公表することとする[77]。

---

76 通信事業者、OS・アプリケーション提供サイト運営者、アプリケーション開発者、機器製造事業者、業界団体等

77 なお、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として「スマートフォン情報セキュリティ３か条」がある（スマートフォン・クラウドセキュリティ研究会 中間報告、平成 24 年 12 月）。

1　利用者情報の取扱いの在り方【検討課題1】

（1）　スマートフォンにおける利用者情報の性質・ 分類

利用者情報を情報の利用目的と種類のマトリックスにより分類し、望ましい情報の取得方法や利用上の問題点などを検討し普及啓発すべきではないか。客観的情勢や情報の使われ方の妥当性も見て、サービスごとにどういう目的で何故必要とするのか整理を行うことも必要ではないか。

- 利用者の期待するサービスやアプリケーションの内容・目的のために当然必要となる情報と、そうでない情報があると考えられる。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、望ましい情報の取扱いや取得方法を検討することが考えられる。
- 第2章において述べたように、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。特に、利用者も直感的に認識・理解しやすい①の利用目的以外の②～④の場合について、利用者が理解できるような丁寧な説明を行う必要があるのではないか。
  - 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[78]（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など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取得する場合

アプリケーション及びサービス提供者や関係事業者が取り扱う情報が「個人情報」に当たるか。「個人情報」に該当する場合、「個人情報データベース等」に当たるか。プライバシーとの関係はどうか。

- スマートフォンにおける利用者情報の性質を分類し、アプリケーションやサービス提供者や関係事業者が取り扱う情報が「個人情報」に当たるかどうか検討する必要があるのではないか。
- 個人情報が含まれる場合、「個人情報データベース等」に当たるかについて検討する必要があるのではないか。
- 上記検討を踏まえ、「個人情報取扱事業者」に該当しうる場合につい検討する必要があるのではないか。
- 上記とあわせて、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適用可能性についても検討する必要があるのではないか

78 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、（目的外使用しない前提で）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、高木氏資料）。

・ プライバシー侵害の有無の程度の観点から、スマートフォンにおける利用者情報の取扱いについてどのように考えるべきか。

氏名、生年月日、住所、年齢、性別、クレジットカード番号等の個人信用情報についてどのように取り扱うことが適当であるか。

・ これらの情報については、アプリケーション等を利用する際に、あくまでも利用者が自ら記載する（自ら提供する）データと理解してよいか。スマートフォンから自動取得する例はないと考えてよいか。
・ 利用者からこれら情報をスマートフォン経由で記入し提供された場合、どのように取り扱うことが適切であるか。
・ 第三者等へ情報提供する場合に留意すべき事項は何か。

電話帳データや所有者の電話番号について、どのように取り扱うことが適当であるか。

・ 電話帳データや所有者の電話番号等は、利用者がアクセスされることに不安を感じる情報[79]でもあるため、利用者に対して提供するアプリケーションやサービスの機能上で必要なのかどうかという点で分類し検討してはどうか。
・ これらの情報について外部に転送する場合には、どのような手続を行うことが適当か。
・ これらの情報について第三者に提供する場合、どのような手続を行うことが適当か。

直ちに氏名に到達できなくても、特定の契約者や端末等に付与された契約者固有のIDについてどのように取り扱うことが適当であるか。

・ 二次提言において整理したPCの場合と比べ、スマートフォンの場合における契約者固有のID（例：IMEI、IMSI、アンドロイドID、UDID等[80]）や電話番号等は利用者側では削除できない固定値である点が異なるのではないか。
・ これらの契約者固有のIDが保有される態様や利用形態によって、情報収集事業者において又は第三者へ共有され集積される中で特定の個人を識別可能な情報と容易に結びつきうる可能性があるのではないか。
・ 電子的な情報が同一IDに紐付き時系列的に蓄積される可能性があるのではないか。
・ 個人情報の取扱いに関し、諸外国の取組を考慮して検討すべきではないか。
・ IDの中に取扱いや性質に違いを設けるべきものがあるか。その場合、どのような視点で取扱いについて検討することが適当と考えられるか。

---

79 2012年（平成24年）2月総務省ウェブアンケートによれば、65.2%の利用者がアプリケーションにより電話帳情報に、60.3%の利用者が自身の電話番号にアクセスされることに対して不安を感じると回答している。

80 IMEI、UDID、MACアドレス、Android_ID等及びそれから変換された値（ハッシュ値）についてアプリケーション間で共通して仕様されるID（グローバルID）であり、提供先や流出先で個人が特定され得るため「匿名の」IDというべきではないという指摘がある。また技術的にアプリケーションにローカルなＩＤを使用する方法を検討し、できる限りグローバルIDを使用すべきではないという指摘もある（第３回会合、高木氏資料）。

通信履歴（通話内容・履歴、メール内容・送受信内容等）について、どのように取り扱うことが適当であるか。

- どのような場合に、電気通信事業者が取扱中の通信ととらえられるか。端末において蓄積された通信履歴について、どのように取り扱われることが適当であるか。
- 利用者に対して提供するアプリケーションやサービスの機能上で必要なのかどうか（利用者から見たメリット）の点で分類し検討してはどうか。

ウェブ閲覧履歴、電子書籍の閲覧履歴、アプリケーション利用状況の履歴等について、どのように取り扱うことが適当であるか。

- これらの情報について収集する場合、どのような点に留意し、利用者に対してどのような配慮を行い知らせることが望ましいか。
- これらの情報の第三者提供を行う場合、留意すべき点は何か。
- 長期間網羅的に収集・記録した場合等において、個人の人格と密接に関係すると考えられる場合があるのではないか。

位置情報などのように、上手く活用されれば高い利便性が得られるが、アクセスされることを不安に思うユーザーもいる情報について、どのように取り扱うことが適当であるか。

- 位置情報の性質は、利用者に対して提供するアプリケーションやサービスの機能上で必要なのかどうか（利用者から見たメリット）の点で分類し検討してはどうか。
- 位置情報を、アドネットワーク等が活用する場合、利用目的に対応しどのような位置情報の取得と利用が必要であるのか利用者に説明を行うことが望ましいのではないか。
- 目的に応じ、取得する情報の精度と頻度の必要性について検討してはどうか[81]。
- 位置情報を取得する場合、一目で分かるマークや位置情報の転送先・利用目的等を分かりやすく示し同意をとってはどうか。
- 包括的選択オプトインだけではなく、内容によっては個別的選択オプトインが望ましいのではないか。

写真やビデオについて、どのように取り扱うことが適当であるか。

- カメラにより撮影される写真やビデオについて、どのように取り扱われることが適当であるか。高精細の画像の場合、個人が特定される場合があると考えられるか。
- スマートフォンで写真を撮る場合、設定によってはGPS位置情報が記録されていることを利用者に周知すべきではないか。

81 広告モジュールにおいて位置情報の使用が見られるが、国別の広告配信を行う目的である場合には詳細な位置は不要であるため他の手段を用いるべきではないかとの指摘もある（第３回会合、高木氏資料）

青少年の情報について、どのような扱いを行うべきか。

- 米国においては、一定年齢以下の青少年の情報について特別の扱いを求めているが、我が国において、青少年の情報についてどのような配慮を行うことが必要であるか。
- 同意ベースで利用者情報の取得が認められるとしても、同意の帰結が真に理解できない者からの情報収集については抑制すべきではないか。

（2）利用者情報の取得・管理・利用の在り方

利用者情報の適切な取得方法はどうあるべきか。

- 利用者情報をどのように取得することが望ましく、適正な取得であるか[82]。どのような方法で利用者に利用者情報の取得について通知し又は利用者の同意を得ることが適当であるか。
- 普通の人が理解できるような説明を、どのようにすれば行うことが可能となるか。
- 説明し切れないほど大量の情報を取得・送信することにも問題があるのではないか。
- 選択の余地を利用者に与えるためには透明性の確保が重要なのではないか。
- どのような態様であれば、利用者情報の利用目的・取得を公表・通知したと言えるのか。アプリケーションのダウンロード時、インストール時、アプリケーションを最初に立ち上げた際、情報を取得する際、送信する際、アプリ開発事業者のホームページ上に掲載されているプライバシーポリシーに記載するなど、どのような方法が想定されうるか。

利用者情報の取得・利用の目的はどのような範囲で許容され、どの程度特定すべきか

- 利用目的と取得項目をどの程度特定することが望ましいのか。プライバシーポリシー等においてどの程度具体的に記載することが望ましいと考えられるか[83]。例えば、「ユーザエクスペリエンスの向上」等の記載は利用目的を十分特定しているのか。
- 上記②～③のようにアプリケーションの内容から取得目的が推測できない場合にどう対処すべきか。
- ④のように将来的に活用するという発想で、その段階では利用目的もなく情報をとっている場合について、どのように考えられるか。
- 詳細に記載しすぎることにより、利用者がかえって理解できなくなることはないか。望ましい利用規約の在り方はどのようなものか。
- ビジネスモデルや競合優位性に係わる重要情報の開示につながるおそれはない

82 個人情報保護法第17条には「適正な取得」を行うことが必要とされている。第二次提言の配慮原則「②透明性の確保」において、利用者に通知すべき事項が定められており（ア．取得の事実、対象情報を取得する事業者の氏名又は名称、ウ．取得される情報の項目、エ．取得方法、オ．第三者提供の事実、カ．提供を受ける者の範囲、キ．提供される情報の項目、ク．利用目的、ケ．保存期間、コ．利用者関与の手段）、「④適正な手段による取得の確保」が求められている。

83 個人情報保護法第 15 条には「その利用の目的をできる限り特定」することとされている。第二次提言の配慮原則「②透明性の確保」において、利用目的を明らかにすることとされている。

か。

利用者情報の第三者提供は、どのような範囲・方法でなされるべきか。

- 個人情報保護法上、第三者提供は本人の同意又はオプトアウトの機会を伴う事前の通知が必要であり、また本人の同意又は通知は実質を伴う必要があるが、どのような場合に実質的にこれを行ったと考えられるか。
- 個人情報に容易に結びつく可能性があるものを第三者提供する場合、どのように扱うべきか。

一つのアプリケーションの中で複数の者が情報収集をする場合に、どのように扱うべきか。

- アドネットワークの場合、情報の第三者提供ととらえるべきか、複数の者（アプリケーション開発者・提供者）とアドネットワークが別々に情報収集を行っているととらえるべきか。
- 個別に利用者に対して説明し情報を収集することは可能であるか。

取得・利用される利用者情報の項目や利用目的、第三者提供の範囲などについて、利用者に対してどのように通知し、また同意を取得すべきか。

- 事業者の氏名又は名称、利用目的の特定、適正な取得、通知又は公表をどのように行うべきか。
- 望ましい利用者への通知又は同意取得のタイミング及び方法はどのようなものか。
- アプリケーションやサービス提供事業者としてもどのような方法で利用者の同意取得や通知をした上で利用者情報へアクセスすればよいか。明確な指針がない状況となっているのではないか。
- OSレベルの利用許諾において利用目的が十分明らかにされていると考えられるか。また利用形態として、端末内における利用、外部サーバー等への情報送信、アプリケーション提供者以外の第三者等への提供等の有無が示されていない場合についてどのように考えるべきか。
- 利用者情報へのアクセスが行われている場合であっても、アプリケーションのインストール時には特段情報が示されない場合もあるが、その場合どのような方法で利用者へ通知あるいは同意取得を行うことが望ましいと考えられるか。
- 情報の種類に応じ、どのような同意確認のレベルが求められるか[84]。

取得後の利用者情報の利用・蓄積において考慮すべき事項は何か。

- 望ましい情報取得後の情報管理体制の在り方はどのようなものか。

84 同意確認の類型・レベルとして、オプトイン方式の中に、①機能使用時に個別的選択が出来る場合、②アプリを起動時に包括的選択ができる場合、③同意しなければ一切の利用ができない強制的オプトインがある。他に、オプトアウト方式、黙示の同意があるという指摘もある（第３回会合、高木氏資料）

・ 同一IDの上に様々な情報が時系列的に蓄積しうることについて利用者が認識すべきではないか。
・ 同意なく様々な情報を収集・利用することはプライバシー侵害になりうるか。

事後的オプトアウトの機会をどのように提供すべきか。

・ 広告カスタマイズのオプトアウトだけではなく、利用者情報の収集の停止も出来るオプトアウトを用意すべきなのではないか。
・ 取得された情報について、削除や訂正を求めうる場合はどのようなものか。

ライフログ活用サービスに関する検討を行った第二次提言における緩やかな配慮原則を策定し事業者による自主的なガイドラインの策定を促すなどの手法の在り方についても検討を深めてはどうか。

・ 個人情報保護法が適用されうるもの、プライバシーの保護を受けうるもの、直ちには明確ではないが該当しうるものが混在する場合、どのような手法が一番効果的であると考えられるか。
・ 配慮原則などに基づく事業者による自主的なガイドラインの策定とその効果について把握し、スマートフォンにおける利用者情報の性質を踏まえ、我が国における新たな取組みの状況についても把握し、今後の在り方について検討してはどうか。
・ 自主規制について取り入れる場合、どのような形態や手法を導入することにより、より効果的かつ実質的に機能することが可能となるか。

グローバルな議論の動向について配慮し、海外との連携も進めることが望ましいのではないか。

・ 米国、欧州、アジア諸国などと必要に応じ意見交換を行うとともに、OECDやITU、APECなどの国際的な場においても議論を行い、スマートフォンにおける消費者プライバシーに関連した課題を共有するとともに、国際的に連携した対応を推進することが重要ではないか。
・ グローバルな民間団体における取組についても把握し、必要に応じて民間団体間の連携なども視野に入れることが望ましいのではないか。
・ グローバルな民間事業者による取組について把握し、利用者情報の保護や利用者の不安感解消に向けて連携を深めることが望ましいのではないか。

苦情相談窓口について検討してはどうか。

・ アプリケーションによる個人情報等の送付について、苦情相談窓口を設置してはどうか。
・ 個人情報保護法違反のおそれがある場合の対応を進めてはどうか。

プライバシー・バイ・デザインについてどのように考えるか。

- プライバシー・バイ・デザイン（様々な技術に関する設計仕様のなかに、プライバシー保護を組込む）の考え方を関係者の間に普及すべきではないか。

2 利用者に対する周知の在り方【検討課題2】

どのようなスマートフォンの特性及びスマートフォンを通じたサービスの状況について周知すべきか。

- 通信事業者による垂直統合モデルで、自由度は少ないがワンストップサービスにより安全安心が確保されたフィーチャーフォンに慣れた日本のユーザーに、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のではないか。
- スマートフォンのOSについては、スマートデバイス、スマートテレビにも実装されることを視野にいれるべきではないか。
- サービス内容と情報の取り方の望ましい組合せや問題について取りまとめ普及・啓発を行うとよいのではないか。
- 「利用者」として想定すべきなのは、現在スマートフォンを使いこなしている層ではなく、今後、意識せずにスマートフォンを利用することになるITリテラシーに乏しい消費者、高齢者等ではないか。

どのようなスマートフォンを利用する上でのリスクを周知すべきか。

- ユーザーがアンチウイルスソフト等でできることは何か、どんな情報が取得され送信されているか分かる手段は何かを周知すべきではないか。
- 端末のメールアドレス、電話番号、端末ID、位置情報などを取得した上で、料金請求画面を出し続けるワンクリック詐欺的アプリも登場しており、正確な情報を把握した上で注意喚起すべきではないか。
- セキュリティ対策ソフトは悪用もでき、誰が提供しているか分からないものもあるなど、危険度はインターフェースの使い方にもよるということを周知すべきではないか。

利用者がスマートフォンに係る情報を入手する方法としてどのようなものがあり、どの方法を活用することが効果的であると考えられるか。

- スマートフォンを購入するときに、セキュリティやリスクへの注意喚起が不十分ではないか。携帯電話ショップや量販店などの店頭や携帯電話関連のウェブサイトなどにおいて必要な内容を説明することも重要ではないか。
- スマートフォンの仕組みやリスクについて、ユーザーの啓蒙・啓発が必要。店頭のコンサルテーション、業界等によるユーザー啓発、信頼できる第三者によるチェック等様々な対応が必要なのではないか。
- 高齢者がiPhoneを購入するときにはチェックシートの回答を求めた例があり（例　こ

の電話はPCの知識が必要であること等）、他OSのスマートフォンも含め同様の取組を行うことが望ましいのではないか。

スマートフォンに係る契約に関して、利用者が意識すべき事項は何か。利用者を支援するために必要な取組は何か。スマートフォンを利用するに当たり、利用者がリスク等に対応し得る方法としてどのようなものがあるか。

- プライバシー保護を念頭にしたサービス設計を行っている事業者（通信事業者、OS・アプリケーション提供サイト運営者等が利用者からきちんと評価されるための仕組みが必要ではないか。
- 利用者において適切な判断が可能となるよう、マーケットやレーティングの審査基準等も含め透明性を高め、利用者に必要な情報提供が事前に行われる仕組みづくりが必要なのではないか。

関係事業者・団体はそれぞれ又は相互に連携し、どのような方法によって利用者に向けた周知をすべきか。国、消費者団体等はそれぞれ又は相互に連携しどのような方法によって利用者に向けた周知をすべきか。

- 関係事業者（通信事業者、OS・アプリケーション提供サイト運営者、アプリケーション開発・提供者、機器製造事業者、広告・情報分析会社）、業界団体における今後のそれぞれの望ましい取組は何か。
- アプリケーション開発者に向けた周知・啓発をどのような形で行うことが適切か。
- 利用者が自らのプライバシーを守るために知っておくべきこと、とるべき行動について、どのように一般利用者に向けて周知を行うか。
- 一般利用者に向けた判りやすい用語を検討してはどうか。
- 今般取りまとめられた「スマートフォン　プライバシー　ガイド」などを関係者と協力しつつどのように周知していくことが効果的であるか。

おわりに

「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」は、2012年（平成24年）1月20日に第１回会合を開催し、その後幅広い関係者の方々からのプレゼンテーションや精力的な議論をいただいた上で、同年3月21日に第４回会合を開催し中間取りまとめについて議論を行った。

スマートフォンの安全安心な利用を促進するために、利用者情報の扱いについて通信事業者、OS・アプリケーション提供サイト運営者、アプリケーション開発・提供者、機器製造事業者、広告配信業者など関係する多様な主体が協力しながら、各領域における課題を共有するとともに、連携した取組を検討・推進することが求められており、その成果を利用者に分かりやすく説明し、利用者自らが判断できる環境を整えていくことが重要である。

スマートフォンの普及が進むとともに、その利用者層も比較的高いICTリテラシーを有する人とともにより幅広い利用者層に拡大していくことも想定される。しかしながら、ユーザーもスマートフォンの有する自由度と責任について理解し、安全安心に使いこなすリテラシーを身につける必要があり、これを関係者が協力し利用者へ分かりやすく伝えるとともに、利用者のリテラシーに応じた安全な使いこなし方法を用意していく必要性が高まっている。

中間取りまとめを踏まえ、今後最終的な提言に向けて検討を行っていく予定である。この課題については、幅広い関係者のご協力と英知を集めることにより、具体的な対応が進むと考える。関係者の幅広い議論と関心を高め、議論を進めることが重要である。

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などに活用され、今後スマートテレビなど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[85]して用いられる可能性も指摘に入れつつ、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。

85 第１回会合　北構成員資料

参考資料　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」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】 ・（株）野村総合研究所　北俊一構成員 「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

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
	一般社団法人モバイル・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
	森構成員 ・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

参考資料　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　構成員名簿

（平成２４年3月21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	社団法人全国消費生活相談員協会常任理事・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	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	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ＮＴＴ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
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
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
西本　逸郎	日本スマートフォンセキュリティフォーラム（ＪＳＳＥＣ）事務局長
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
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

（別紙）

スマートフォン プライバシー ガイド

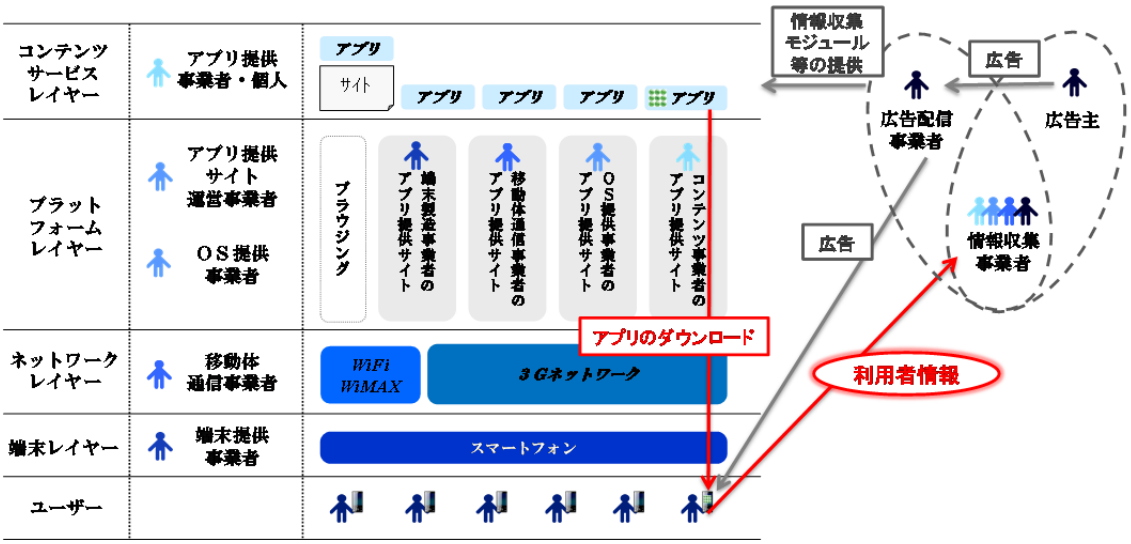
スマートフォンが急速に普及する中、スマートフォン上の利用者情報が様々なサービス提供等に利用されています。利用者情報の取扱いは、関係する事業者において適正に行われるべきものですが、スマートフォンの利用には自己責任が求められる側面もあります。

「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・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」においては、事業者における利用者情報の適正な取扱い方策について検討してまいりますが、現時点でもスマートフォンを利用者が一定程度安心して利用できるよう、利用者自身で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、中間取りまとめに際して整理しました。

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。

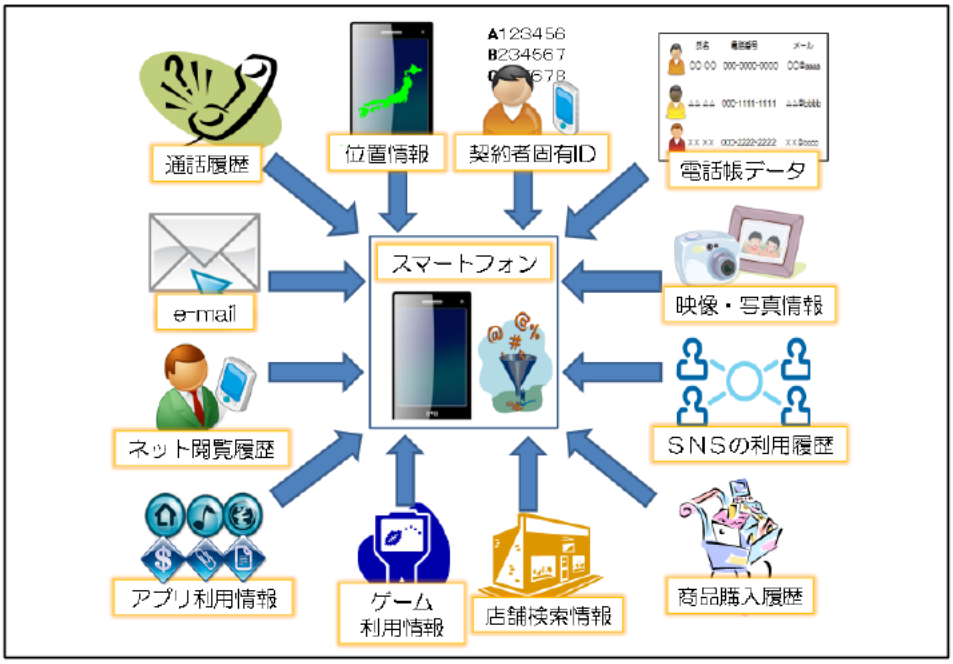
【スマートフォンのサービス構造】



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）