第Ⅰ部　スマートフォンにおける利用者情報に関する課題への対応

スマートフォン　プライバシー　イニシアティブⅡ

～アプリケーションの第三者検証の在り方～

① 第一に、利用者情報の適正な取扱いに関し、アプリケーションの利用者の安心感向上とともに、適正なアプリケーションへの信頼向上・利用拡大にもつながる「アプリケーションの第三者検証の在り方」等について議論し、その結果を「スマートフォン プライバシー イニシアティブⅡ」として取りまとめた。昨年の報告書において提言された、利用者情報の適正な取扱いに関する「指針」の実効性を確保するために、アプリケーションの第三者検証の在り方について提言している。我が国の先導的な取組を普及・推進していくことにより、安心安全なプライバシー環境の実現を通じてスマートフォン市場の拡大に寄与するとともに、国際的な連携を推進していくことが期待される。

（「はじめに」より抜粋）

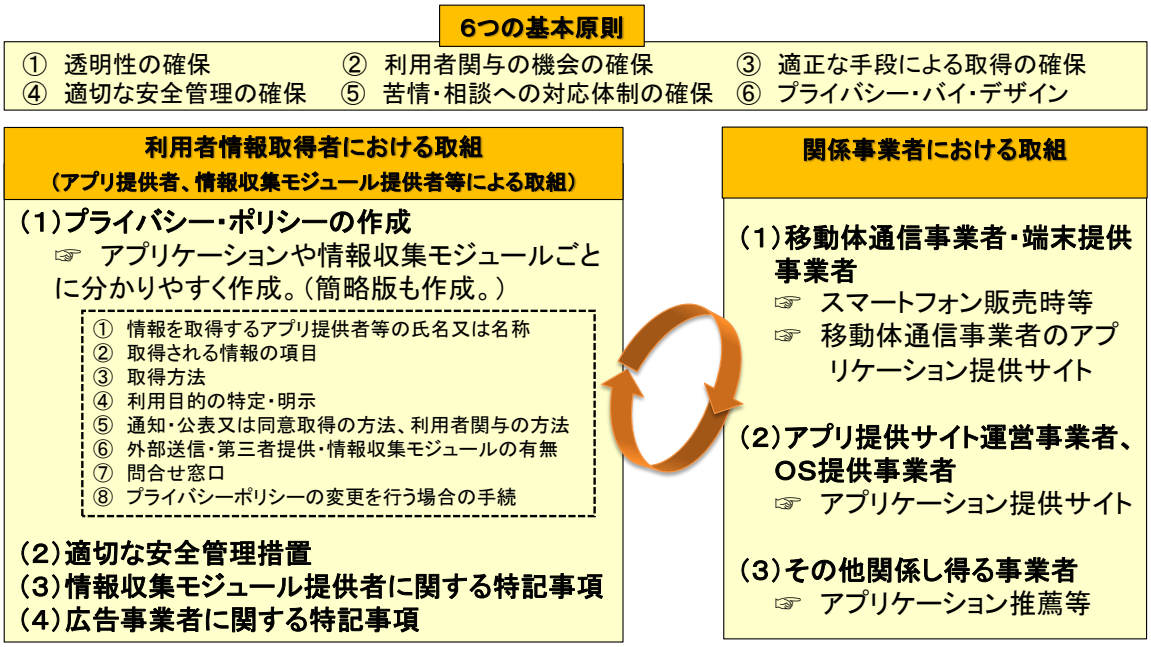
目次

第１章　「スマートフォン　プライバシー　イニシアティブ」を踏まえた対応
～「スマートフォン利用者情報取扱指針」の実効性を上げるための取組～

我が国において急速にスマートフォンが普及する中で、スマートフォンにおいて取得・蓄積された行動履歴や通信履歴等を含む様々な利用者情報[1]について、利用者へ十分説明がないままアプリケーション等により外部送信される場合も見られ、利用者が不安を覚える場合も出てきている。このような状況を踏まえ、2012年（平成24年）８月、「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」によって「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～（以下「スマートフォン　プライバシー　イニシアティブ」という。）」が取りまとめられ、公表された。

「スマートフォン　プライバシー　イニシアティブ」において、スマートフォンにおける利用者情報の適正な取扱いに関する「スマートフォン利用者情報取扱指針」（以下「指針」という。）が示され、安心・安全な利用環境の確保に向けて、アプリケーション提供者や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、移動体通信事業者等のスマートフォンの関係事業者による取組が提言されている。

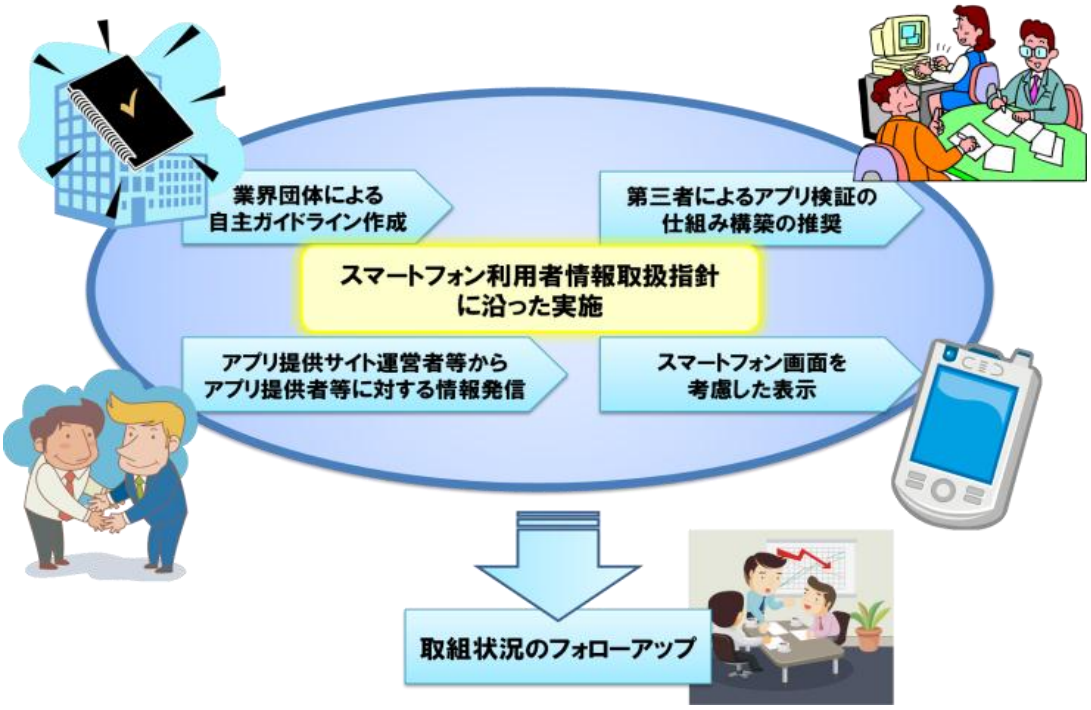
図表１－１－１：スマートフォン利用者情報取扱指針の概要



[1] スマートフォンにおける利用者情報の例として、①利用者の識別に係る情報（氏名・住所等の契約者情報、ログインに必要な識別情報、クッキー技術を用いて生成された識別情報、契約者・端末固有ID）、②第三者の情報（電話帳で管理されるデータ）、③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、ウェブページ上の行動履歴、アプリケーションの利用履歴等、位置情報、写真・動画等）などが挙げられている（「スマートフォン　プライバシー　イニシアティブ」第２章 11ページ 図表２－２：スマートフォンにおける利用者情報の例）。

また、この指針の実効性を上げるため、業界団体等における自主ガイドラインの策定、第三者によるアプリケーション検証の仕組みの検討、アプリケーション提供サイトからアプリケーション提供者等に対する情報発信、スマートフォン画面を考慮した表示を行うことなどが併せて提言されている。

図表１－１－２：指針の実効性を上げる取組



【プライバシー・バイ・デザインの実現に向けて】

「スマートフォン　プライバシー　イニシアティブ」の指針の「基本原則」において「⑥プライバシー・バイ・デザイン」が位置づけられている。スマートフォンに関連した新たなアプリケーションやサービス開発時、アプリケーション提供サイトやソフトウェア、端末の開発時から、関係事業者は、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されている。また、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・開発を行うことが求められている。

プライバシー・バイ・デザインの原則[2]も踏まえ各関係事業者にそれぞれにおける取組が期待される。例えば、アプリケーション提供者には正確な情報に基づくアプリケーションのプライバシーポリシーの作成と遵守が期待されている。また、アプリケーション提供サイトの運営者、OS 提供者等、端末提供者、その他関係事業者に

2 「プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流」堀部政男/一般財団法人日本情報経済社会推進協会（JIPDEC）（日経 BP 社、平成 24 年 10 月 29 日）
7 つの基本原則は後述（http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/参照）

ついても、それぞれの立場において、利用者のプライバシー保護の仕組みが予防的に導入され運用が可視化され透明性が確保されるようにすることにより、各事業者の協力のもとに安心安全な利用環境が確保されることが望ましい。

なお、第３章で検討される第三者検証を実施することは、プライバシー・バイ・デザインを補完的に実現することに資するものである。アプリケーションに関する第三者検証の実施は、アプリケーションのプライバシーポリシーを通じたアプリケーションの透明性向上に資するとともに、利用者情報の取扱いに関する公正性や公平性の確保の観点からも重要である。

図表１－１－３：プライバシー・バイ・デザイン　７つの基本原則

プライバシー・バイ・デザイン　７つの基本原則

１　事後的ではなく事前的、救済策的ではなく予防的
２　プライバシー保護が初期決定で有効化されていること
３　プライバシー保護の仕組みがシステムの構造に組み込まれること
４　全機能的であること－ゼロサムではなく、ポジティブサム
５　データがライフサイクル全般にわたって保護されること
６　プライバシー保護の仕組み運用の可視化、透明性の確保
７　利用者のプライバシーを最大限に尊重すること

【先行的ルールとしての「スマートフォン　プライバシー　イニシアティブ」】

情報通信技術の進展に伴いパーソナルデータの取扱いに関する様々な議論が政府部内で開始されており、「スマートフォン　プライバシー　イニシアティブ」を踏まえたスマートフォンの利用者情報の取扱いに関する取組も位置づけられている[3]。

「世界最先端 IT 国家創造宣言」[4]において、いわゆるビッグデータ利活用による新事業・新サービス創出の促進として、「ビッグデータ」のうち特に利用価値が高いと期待されている個人の行動・状態等に関するデータである「パーソナルデータ」の取扱いについても、その利活用を進めるため個人情報やプライバシー保護との両立を可能とする事業環境整備を進めることとされ、プライバシーや情報セキュリティ等に関するルールの標準化や国際的な仕組み作りの必要性が指摘されている。「スマートフォン　プライバシー　イニシアティブ」における「スマートフォンの利用者情報の取

3　例えば、総務省「パーソナルデータの利用・流通に関する研究会報告書」において、パーソナルデータの分野のうちスマートフォンにおける利用者情報の取扱いに関する先行的指針として「スマートフォン プライバシーイニシアティブ」が位置づけられている。
http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html

4　「世界最先端IT国家創造宣言について」（平成25年6月14日 閣議決定）
http://www.kantei.go.jp/jp/singi/it2/pdf/it_kokkasouzousengen.pdf

扱い」については、同宣言において「先行的にルール策定が行われた分野」と位置づけられており、「取組の普及を推進する」こととされている。

また、「消費者基本計画（改定原案）」[5]においても、「②急速に普及が進むスマートフォンにおける利用者情報の取扱いについて、「スマートフォン プライバシー イニシアティブ」（平成24年８月）を踏まえ、利用者に分かりやすい形で説明するなどの方法により、プライバシー保護等に配慮した安心安全な利用環境の確保に向けた取組を推進します」とされている。

さらに、「サイバーセキュリティ戦略」[6]において、「スマートデバイスについては、特に常時、電源が入り、インターネットと接続状態のままで携帯されているスマートフォンにおいて、位置情報等の様々な利用者情報が扱われる一方で、その構造上、情報セキュリティ対策ソフトによる対応の限界等があるため、個々人におけるリテラシーの強化が一層必要となる」「スマートフォンのアプリケーションについて一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する」とされている。

第１章においては、このように、「スマートフォン　プライバシー　イニシアティブ」に基づく取組が政府全体の取組の中でも位置づけられていることも踏まえつつ、指針の実効性を上げるための様々な取組の状況について、その進捗状況を整理するとともに、「スマートフォン　プライバシー　イニシアティブ」公表後のスマートフォンの普及状況と利用者情報をめぐる問題を概観することとする。

---

5 消費者基本計画（改定原案）平成25年6月
http://www.cao.go.jp/consumer/iinkai/2013/123/doc/123_130611_shiryou2-2.pdf

6 「サイバーセキュリティ戦略」情報セキュリティ政策会議決定、内閣官房情報セキュリティセンター(NISC)平成 25 年 6 月 10 日発表、http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf

１　業界団体等におけるガイドラインの検討

2012年（平成24年）８月に「スマートフォン　プライバシー　イニシアティブ」がまとめられたことを受け、関係する業界団体等においてガイドラインの検討が進展している。最も早い動きとしては、2012年（平成24年）８月に「スマートフォン　プライバシー　イニシアティブ」に準拠したスマートフォンのアプリケーション用のプライバシーポリシーの雛形を試案として公表[7]した例などが挙げられ、また、2012年（平成24年）10月に一般社団法人日本スマートフォンセキュリティ協会会員でもあるタオソフトウェア株式会社が「アンドロイドスマートフォンプライバシーガイドライン」を策定・公表[8]している。

業界団体としては、2012年（平成24年）11月に一般社団法人モバイル・コンテンツ・フォーラム（MCF）が「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」を策定・公表[9]しており、この中には、アプリケーション・プライバシーポリシーのモデル案や概要版等も含まれている。

図表１－１－４：「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」の構成（MCF）

第1部：充足すべき必要要件
総務省「スマートフォン プライバシー イニシアティブ」スマートフォンにおける利用者情報の取扱いの在り方（**第5章**）を提示。

第2部：実装に当たっての推奨要件
「アプリケーション・プライバシーポリシー」の実装にあたって**推奨される要件**を提示。
指針では触れられていない**具体的な方法や実態に合わせた追加事項**等。

１　アプリケーション・プライバシーポリシーの名称について
２　通知又は公表及び同意取得等のタイミングについて
３　アプリケーション・プライバシーポリシーを提示する場所について
４　アプリケーション・プライバシーポリシーの変更について
５　同意が得られなかった場合に制限される事項について
６　取得した利用者情報の取扱いについて
７　必要要件以外の同意取得について
８　日本語以外での説明に対する対応について
９　既存のアプリケーションの本ガイドラインへの対応について

---

[7] 例えばAZX Professionals Groupがウェブサイトにおいて「スマートフォン　プライバシー　イニシアティブ」に準拠した「スマホアプリ用プライバシーポリシー（簡易版/試案）」を公表。今後、随時アップデートしていくとしている。（2012年（平成24年）８月27日）。http://www.azx.co.jp/modules/docs/index.php?cat_id=40

[8] 2013年（平成25年）１月には改訂版が公表されている。

[9] 2012年（平成24年）10月に意見募集を行い、その結果を踏まえ策定された。
http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf

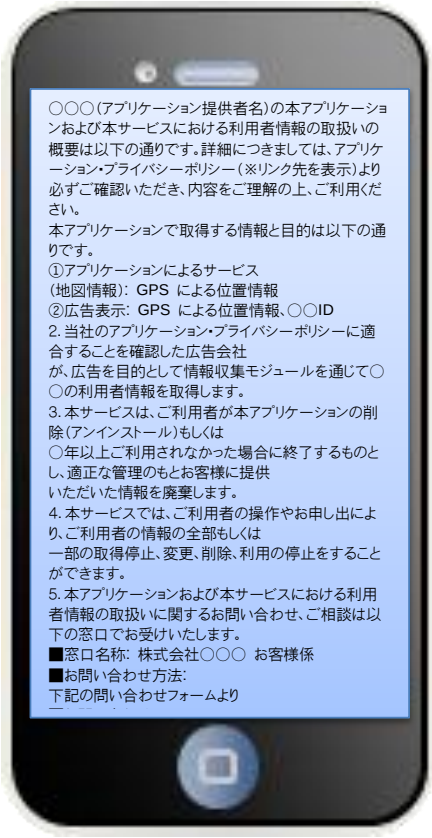
第3部：アプリケーション・プライバシーポリシーのモデル案

「アプリケーション・プライバシーポリシー」のモデル案と作成ガイドを提示。**詳細な本編**だけでなく**概要**の作成方法についても提示。

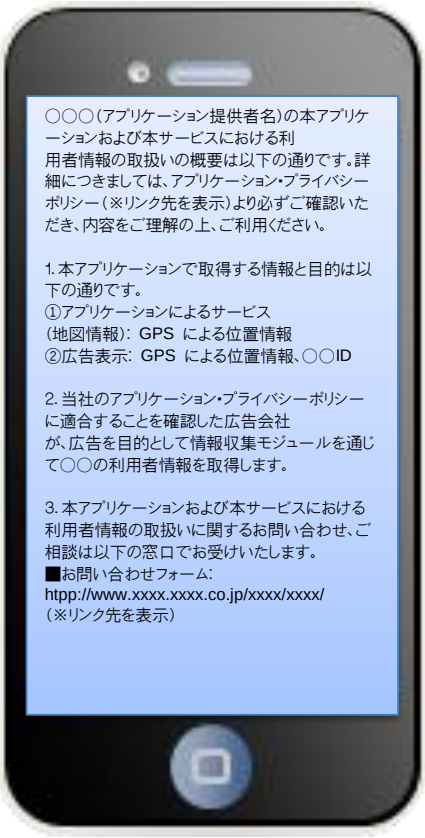
アプリケーション・プライバシーポリシーのモデル案

第１条（定義）
第２－１条（取得される情報の項目、利用目的、取得方法）
第２－２条（お客様ご自身によりご登録いただく情報）
第３条（同意）
第４－１条（外部送信）
第４－２条（第三者提供）※第三者提供がある場合
第４－３条（情報収集モジュール）※情報収集モジュールが組み込まれている場合
第５条（利用者関与の方法）
第６条（サービスの終了と情報の取扱い）
第７条（個人情報保護方針（プライバシーポリシー）等へのリンク）
第８条（情報の開示、提供）
第９条（取得された情報の公開、共有）
第10条（問い合わせ窓口）
第11条（変更）

（参考）アプリケーション・プライバシーポリシー概要版



パターン１



パターン２

一般社団法人電気通信事業者協会（TCA）は、2012 年（平成 24 年）10 月に移動電話委員会のもと「スマートフォンの利用者情報等の適正利用促進検討部会」を設置し、アプリケーション提供サイト運営事業者向けのガイドライン[10]の策定に向けて検討を行い、2013 年（平成 25 年）３月「スマートフォンアプリケーション提供サイト運営事業者向けガイドライン」を策定・公表[11]している。

また、「スマートフォン　プライバシー　イニシアティブ」及びMCFのガイドライン等を参照して、アプリケーションを開発・提供する側の立場から、2013年（平成25年）１月、京都市が「京都市スマートフォンアプリケーション活用ガイドライン」を策定・公表[12]している。ゲームアプリケーションの分野では、2013年（平成25年）４月、一般社団法人日本オンラインゲーム協会（JOGA）が策定・公表[13]した「スマートフォンゲームアプリケーション運用ガイドライン」の中で、「スマートフォン　プライバシー　イニシアティブ」に準拠する形でプライバシーポリシーを作成し、利用者が容易に参照できる場所に明示することとされた。

さらに、モバイル広告を含むインターネット広告のビジネスに関わる企業が加盟する　一般社団法人インターネット広告推進協議会（JIAA）がインターネット広告事業における消費者保護の観点に基づく指針をガイドライン[14]の中で定める方向で検討を進めている。

２　スマートフォンの利用者情報等に関する連絡協議会

「スマートフォン　プライバシー　イニシアティブ」において関係事業者等に求められる指針等が示されており、民間の自主的な取組を推進するために、業界それぞれの実態を踏まえた業界ガイドラインの策定が期待されている。スマートフォン市場において様々なビジネスが連携し、多様な業界団体が関係している環境を考慮し、緊密な情報交換及び相互の知見を結集してスマートフォンのプライバシーに関する業界ガイドラインの策定を促進することを目的として、2012 年（平成 24 年）10 月、35 以上の業界団体や企業・団体等が参加し「スマートフォンの利用者情報等に関する連絡協議会(SPSC)」[15]（以下「連絡協議会」という。）が設置された。

---

[10] WG 第 4 回会合資料 2「TCA におけるスマートフォンのプライバシーに関する取り組み（案）」（TCA）。同部会メンバーは、NTT ドコモ、KDDI、ソフトバンクモバイル、イー・アクセス、ウィルコムの 5 社。

[11] TCA のウェブサイトに公表されている。http://www.tca.or.jp/topics/pdf/20130329guideline.pdf

[12] 「京都市ソーシャルメディアガイドライン」及び「京都市スマートフォンアプリケーション活用ガイドライン」の策定について（2013 年（平成 25 年）1 月 10 日）。　http://www.city.kyoto.lg.jp/sogo/page/0000134264.html

[13] JOGA のウェブサイトに公表。http://www.japanonlinegame.org/pdf/JOGA130405.pdf

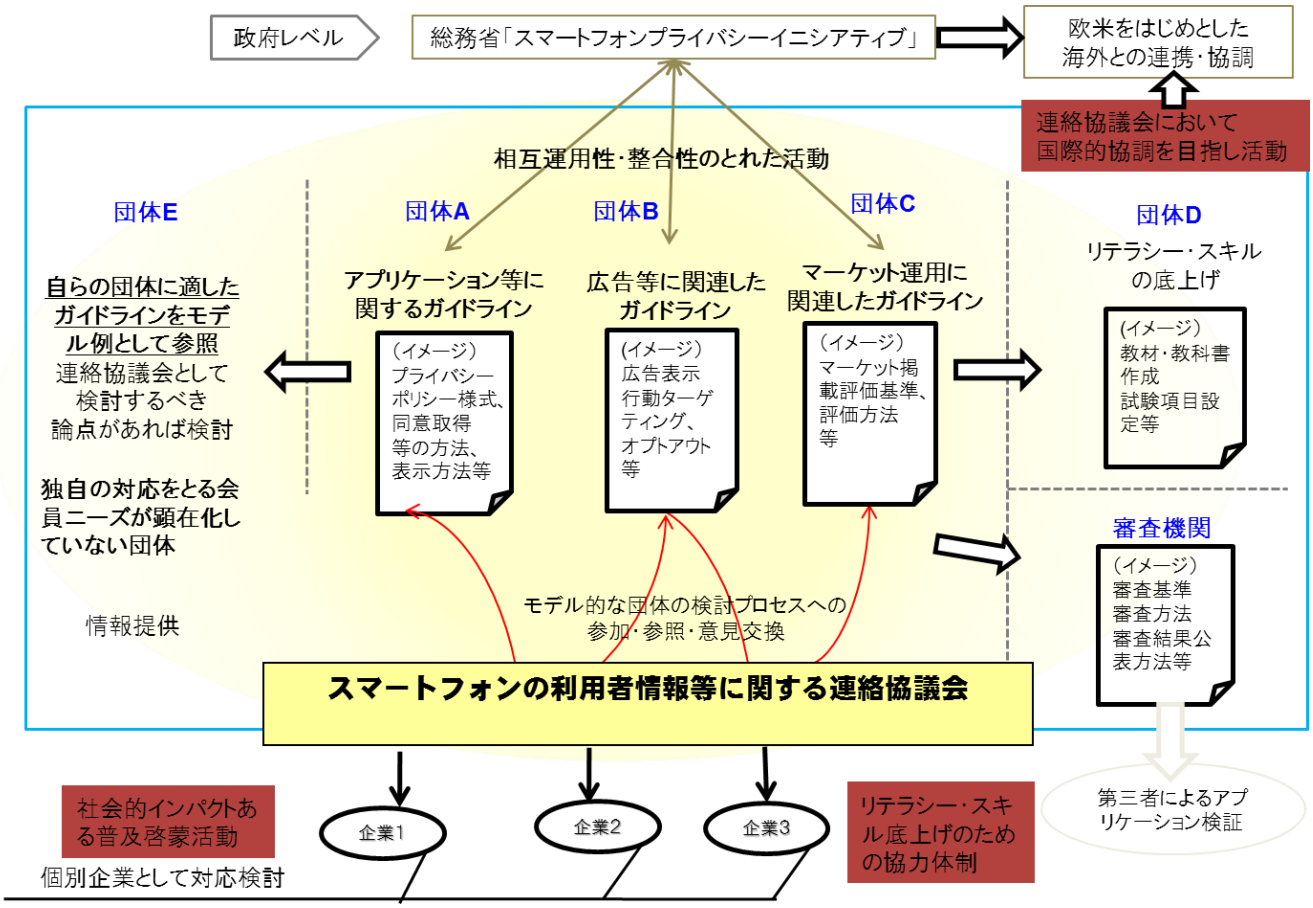
[14] 「スマートフォン時代における安心・安全な利用環境の在り方に関する WG」（以下「WG」という。）第 4 回会合資料 1「スマートフォン向け広告における利用者情報の取扱いに関するガイドラインの取組」（JIAA）。「プライバシーポリシー作成のためのガイドライン」「行動ターゲティング広告ガイドライン」について 2013 年（平成 25 年）改定を予定している。

[15] 議長：新保史生 慶應義塾大学総合政策学部教授、副議長：森亮二 弁護士法人英知法律事務所弁護士。SPSC は Smartphone Privacy and Security Council の略称。

連絡協議会は、①業界ガイドライン及びモデルプライバシーポリシーに関する情報交換、②プライバシーポリシーの効果的な表示方法等に関する情報交換及び検討、③利用者情報の取扱いに関する推奨すべき事例及び問題となり得る事例の検討、④マーケット動向及び国際的動向に関する情報交換の実施、⑤各業界における取組状況の随時把握及び普及啓発活動の実施などについて活動をしていくとしている。

これまでに、連絡協議会は、スマートフォンの利用者情報等に関わる官民の取組が一元的に把握できるよう情報集約場所（ポータルサイト）[16]を作成し、情報集約及び情報発信を開始するとともに、既に行った取組と今後の取組について中間的な取りまとめ[17]を作成し公表している。各参加団体等における活動状況や関係事業者との連携について情報共有が図られるとともに、一般利用者及びアプリケーション提供者等への周知啓発プログラムについての検討が行われている。

図表１－１－５：情報集約及び情報発信イメージ



[16] 官民の関連情報を集約したポータル（2012 年（平成 24 年）12 月 20 日発表）。http://jssec.org/spsc
[17] 「SPSC 活動報告書」を参照。http://jssec.org/spsc/report.html#spsc-work

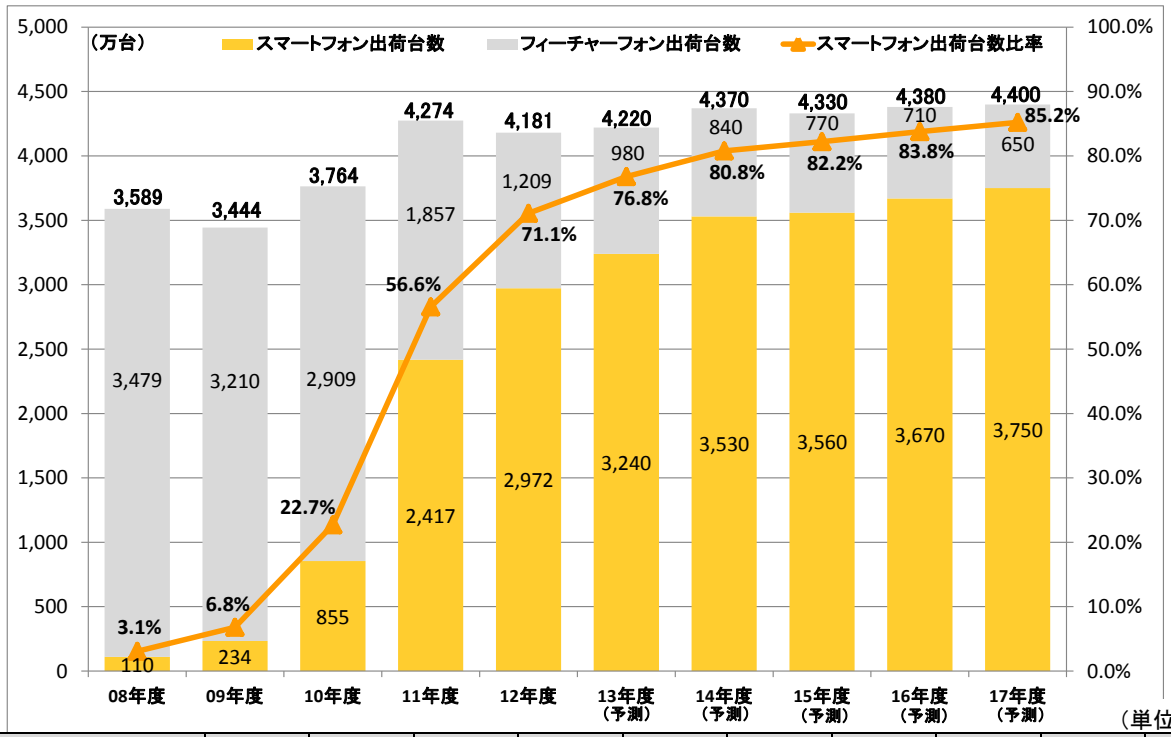
３　スマートフォンの普及の進展と利用者情報をめぐる問題

（１）　スマートフォンの普及の進展

2012 年度（平成 24 年度）については、新規出荷台数の７割以上がスマートフォンになった。2013 年度（平成 25 年度）については、新規出荷台数の約８割がスマートフォンになると予測されており、2014 年度（平成 26 年度）以降については８割以上となることが予測されている[18]。

これに伴い、スマートフォンの普及台数も増加しており、2012 年度（平成 24 年度）末において約 4,300 万台となり、普及率は約４割まで伸びると予想される。さらに、2013 年度（平成 25 年度）末には約 5,900 万台を上回り、全体としての普及率も約５割と更に増加していくと予測される。

図表１－１－６：スマートフォン国内出荷台数の推移・予測



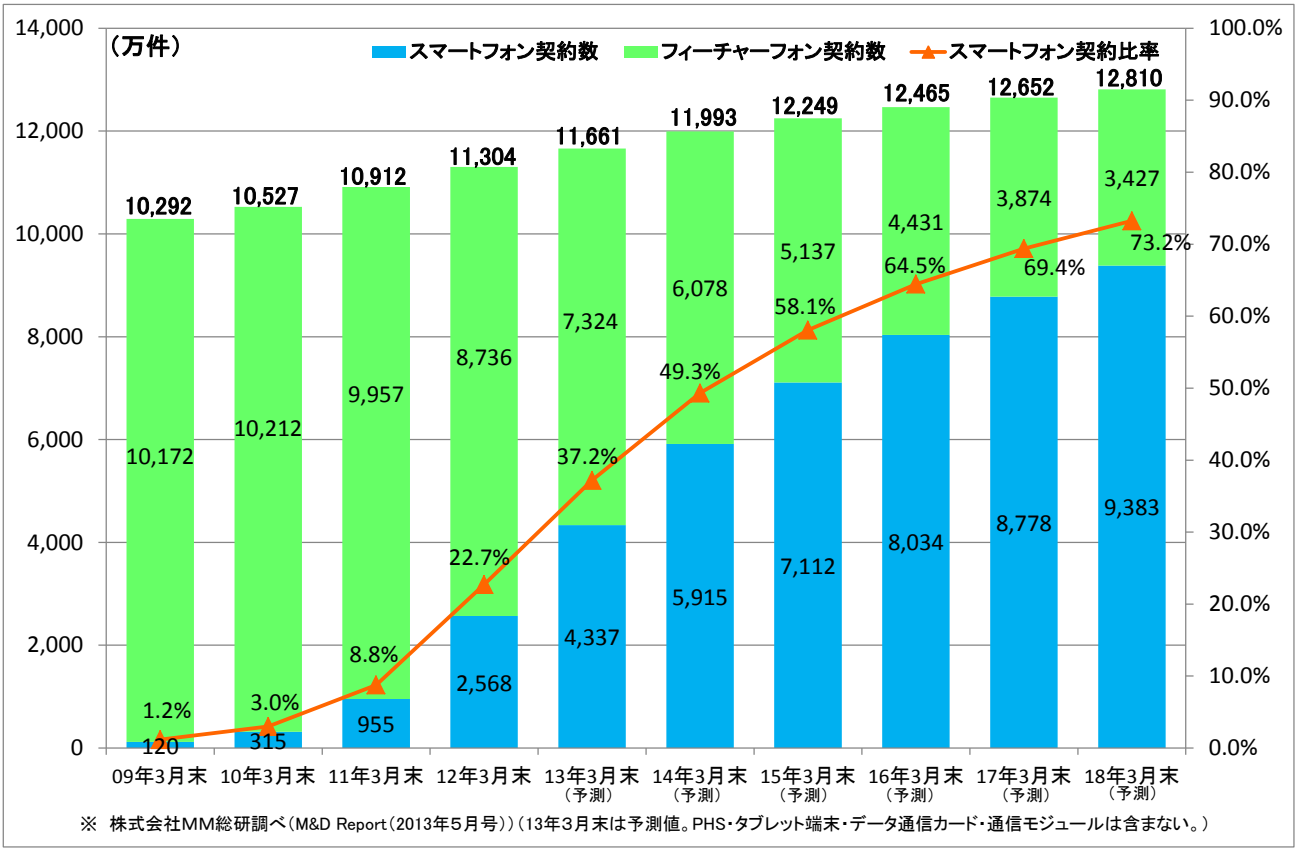
（単位：万台）

	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	2017年度
総出荷台数	3,589	3,444	3,764	4,274	4,181	4,220	4,370	4,330	4,380	4,400
うちスマートフォン出荷台数	110	234	855	2,417	2,972	3,240	3,530	3,560	3,670	3,750
スマートフォン比率	3.1%	6.8%	22.7%	56.6%	71.1%	76.8%	80.8%	82.2%	83.8%	85.2%

※　株式会社MM総研調べ（13年度以降は予測値）「2012年度通期国内携帯電話端末出荷概況」（2013年５月９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・タブレット端末・データ通信カード・通信モジュールは含まない。

[18] 株式会社 MM 総研調べ（2013 年度（平成 25 年度）以降は予測値）（「スマートフォン市場規模の推移・予測（2013 年（平成 25 年）３月）」（2013 年（平成 25 年）３月 28 日）及び「2012 年度通期国内携帯電話端末出荷概況」（2013 年（平成 25 年）５月９日））。いずれも国内メーカー製品・海外メーカー製品を含む。タブレット端末・PHS・データ通信カード・通信モジュールは含まない。

図表１－１－７：携帯電話契約数とスマートフォン契約数の推移・予測



スマートフォンの利用率は 2012 年度（平成 24 年度）末において約４割であるが、年代別で見ると、男性 20 代及び女性 20 代が約６割、男性 30 代及び男性 10 代が約５割とより高くなる一方、女性 60 代以上は約１割と大幅に低く、年代層や性別により利用率に差があることが分かる調査結果もある[19]。

世界的に見ると、米国においては 50%、韓国において 48%、英国は 51%など、スマートフォンの普及が進展しているという調査結果もあり[20]、我が国の今年度末の普及率はこれら諸国の現在の普及率と同様の水準に近づくものと予測される。

（２） 利用者情報の取得を目的としたマルウェアの増加

スマートフォンの世界的な普及に伴い、入手可能なアプリケーションの数も増加し続けている。2012 年（平成 24 年）10 月段階において Google Play が 70 万アプリケーション、App Store が 77.5 万以上のアプリケーション、Windows Phone Store

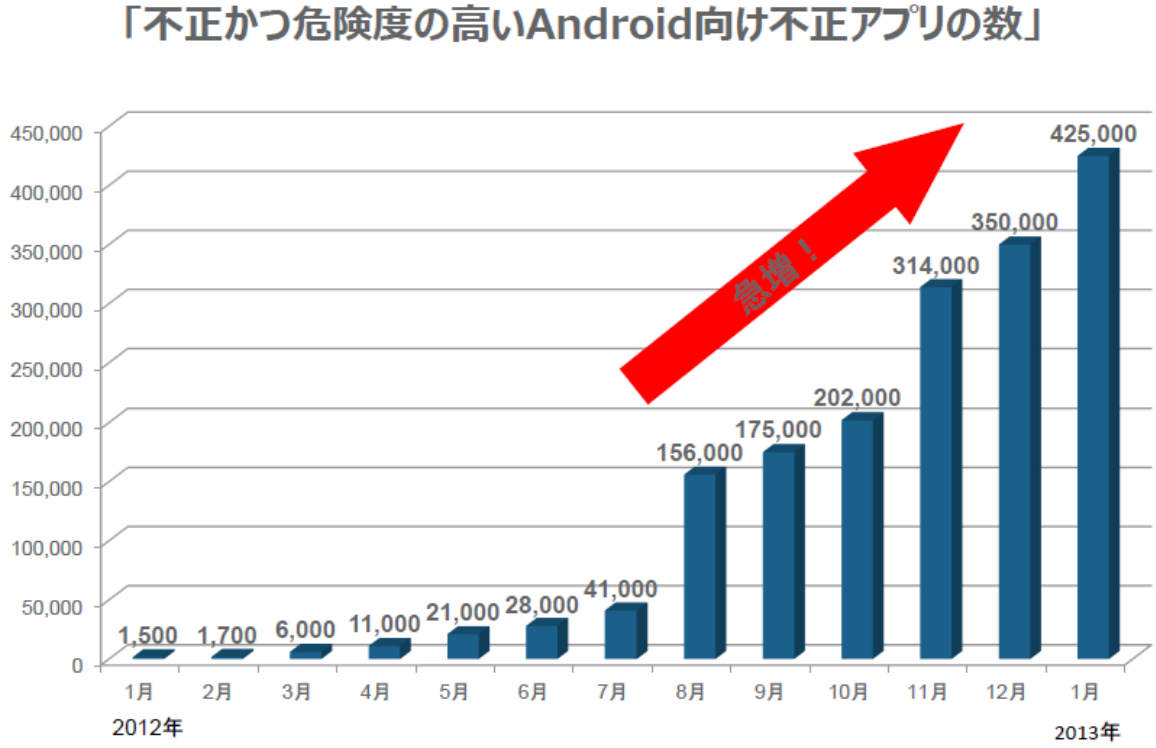
[19]「スマートフォン/ケータイ利用動向調査 2013」株式会社インプレス R&D（2012 年（平成 24 年）11 月 20 日）
http://www.impressrd.jp/news/121120/kwp2013

[20]米国：ニールセン調査（2012 年（平成 24 年）5 月）。http://japan.internet.com/allnet/20120518/4.html
韓国：放送通信委員会調査（2012 年（平成 24 年）2 月）。
http://www.yamaguchibank.co.jp/portal/special/asia/2012/busan_02.pdf
英国：Google 調査（2012 年（平成 24 年）第 1 四半期）「Our Mobile Planet スマートフォン調査」。
http://services.google.com/fh/files/blogs/our_mobile_planet_uk_en.pdf

が 12 万アプリケーション[21]を上回ると報道されている。

一方、スマートフォンの急速な普及に伴い、マルウェアの数も増加しており、金銭詐取目的のワンクリックウェアとともに、電話帳情報など利用者情報を詐取することを目的とするものも増加してきている。トレンドマイクロ株式会社によれば、不正かつ危険度の高い Android 向けアプリケーションの数は、2012 年（平成 24 年）１月の 1500 に比べ、2013 年（平成 25 年）１月には 42 万 5000 と急増している。

図表１－１－８：不正アプリケーションの数の推移



※1 2012年7月26日公開の第2四半期のセキュリティラウンドアップの作成時におけるAndroidのアプリの集計方法から変更があり、6月末の不正アプリ数を公開時の2万5千から2万8千に修正しています。

出典：2012年第3四半期セキュリティラウンドアップ、2012年第2四半期セキュリティラウンドアップ他
http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012q3.pdf
http://jp.trendmicro.com/imperia/md/content/jp/threat/report/qsr/2012q2.pdf

また、2012 年（平成 24 年）に新たに確認された利用者情報を狙うアプリケーションとして、利用者情報を読み取った上で金銭詐取目的で使用するワンクリックウェアがあり、①The Movie シリーズのアプリケーション、②電池長持ちアプリケーション・電波改善アプリケーション[22]、③わんこアプリケーションなどが挙げられ、

[21] ブルームバーグ・ビジネスウィーク（英語版）「Google Says 700,000 Applications Available for Android」（2012 年（平成 24 年）10 月 29 日）
http://www.businessweek.com/news/2012-10-29/google-says-700-000-applications-available-for-android-devices、App Store からのダウンロードが、400 億本を突破。ほぼ半数が 2012 年中に（Apple 社（米国）報道発表資料抄訳―2013 年 1 月 7 日）。
http://www.apple.com/jp/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html

[22] アプリケーション提供サイトが管理していない場所に置かれているアプリケーション（いわゆる野良アプリケーション）に不正アプリケーションも多く見られる。Facebook、twitter やスパムメッセージを通じて、これら野良アプリケーションに巧妙に誘導する導線を引く事例があり注意が必要である。

①～③のように電話帳等の利用者情報を狙う不正アプリケーションの類型及び数が増加していることが指摘されている[23]。一般利用者にとって、安心安全なアプリケーションについて見分けたり情報を得たりする必要性がますます高まっていると考えられる。

また、アプリケーション提供者が自らの提供するアプリケーションが安全であることを何らかの方法で利用者に説明し、理解してもらうことが、利用者が安心してアプリケーションを使うためには重要であると考えられる。

図表１－１－９：
ワンクリックウェア感染後の請求画面の例

トレンドマイクロ株式会社インターネット脅威マンスリーレポート(2012 年 1 月度)

図表１－１－10：不正アプリケーションの例（電池長持ち、電波改善等）

[23] WG 第 4 回会合資料 3「スマートフォンのプライバシー保護に関する取り組み」(トレンドマイクロ株式会社)。

第２章　アプリケーション等のプライバシーポリシーに関する対応状況と課題

「スマートフォン　プライバシー　イニシアティブ」において提言された「スマートフォン利用者情報取扱指針（以下「指針」という。）」において、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、情報モジュール提供者は、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、８項目[24]の事項について明記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等を行うこととされている。

このアプリケーション等のプライバシーポリシーの作成と公表は、指針における基本原則にも定められた「透明性の確保」や「利用者関与の機会の確保」等を実現するための中核となる対応であり、アプリケーション提供者や情報収集モジュール提供者による対応の進展が期待される。また、プライバシーポリシーの分かりやすい概要が作成され、利用者が容易に参照できる場所に公表されることが望ましい。

第２章においては、アプリケーションのプライバシーポリシーへの対応状況について、現状を概観し課題と対応について検討するとともに、情報収集モジュールのプライバシーポリシーについても課題を提示することとする。さらに、アプリケーション提供サイト運営事業者の対応、連絡通報窓口の設置などについても整理することとする。

１　アプリケーションのプライバシーポリシーへの対応状況

指針を踏まえ、利用者情報の取扱いに関する透明性を確保するために、アプリケーション提供者がアプリケーションのプライバシーポリシーをあらかじめ作成・公表し、利用者が容易に参照できる場所に掲示又はハイパーリンクを掲載することが望ましいとされているが、その現状を示すこととする。

（１）　アプリケーションのプライバシーポリシーの作成・掲載状況

アプリケーション提供者がアプリケーションのプライバシーポリシーをあらかじめ作成し、公表する方法としては、①アプリケーション内における表示、②アプリケーション提供サイト（Google Play 等）のアプリケーション紹介ページへの掲示（又はハイパーリンクを掲載）[25]、③アプリケーション提供者のウェブサイトへの掲載等の方法が考えられる。

---

[24] 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、②取得される情報の項目、③取得方法、④利用目的の特定・明示、⑤通知・公表又は同意取得の方法、利用者関与の方法、⑥外部送信・第三者提供・情報収集モジュールの有無、⑦問合せ窓口、⑧プライバシーポリシーの変更を行う場合の手続の８項目（「スマートフォン　プライバシー　イニシアティブ」62 ページ）。

[25] 例えば、Google Play や App Store において「プライバシーポリシー」という項目を設けて、アプリケーションのプライバシーポリシー（又はハイパーリンク）の掲載が行われている。

① 日本総合研究所[26]による調査

日本において人気の高い無料アプリケーションランキング１位～40 位のアプリケーションについて抽出し調査を行ったところ[27]、アプリケーションのプライバシーポリシーを①アプリケーション内及び②アプリケーション提供サイトの双方に記載している事例が７あった。また、①アプリケーション内又は②アプリケーション提供サイトのいずれかに記載している事例が 10 あった。

一方、調査対象の最も人気の高いアプリケーション 40 の中でも、一般の利用者が通常参照し得ると思われる①アプリケーション内及び②アプリケーション提供サイトのいずれにもアプリケーションのプライバシーポリシーの記載がないものは 23 あった。このうち、③開発者ウェブサイトにおいて会社のプライバシーポリシーについても掲載がない場合も約２割程度あった。どんな情報を何のために取得しているのか何ら説明がないこれらのアプリケーションの中には、Android のパーミッションを見る限り GPS 位置情報、契約者・端末固有 ID 等を外部に送信し得るものもあった。

図表１－２－１：アプリケーションのプライバシーポリシーの作成・公表状況[28]

記載場所	記載パターン							
	①	②	③	④	⑤	⑥	⑦	⑧
アプリ内	○	○	○	○	×	×	×	×
Google Play 紹介ページ	○	○	×	×	○	○	×	×
開発者 ウェブサイト	○	×	○	×	○	×	○	×
アプリ数(計40アプリ)	7	0	6	1	3	0	16	7

また、米国において人気の高い無料アプリケーションランキング 1 位～40 位のアプリケーションについても同様に調査を行い[29]、日米比較を行ったところ、①のアプリケーション内における記載の割合は、米国が約５割弱、日本は約４割弱であった。また、②のアプリケーション提供サイトにおける掲載又はハイパーリンクの記載割合が米国は高く約５割強であり、一方、日本は約 2.5 割と米国の方が２倍以上の高い割合であった。

---

26 株式会社日本総合研究所（以下同じ。）

27 WG 第 4 回会合資料 4「スマートフォンアプリケーションの表示・検証に関する国内・海外動向」（日本総合研究所）。Google Play 日本無料アプリケーションランキング、米国無料アプリケーションランキングより上位 40 位のアプリケーションを抽出（2013 年 2 月 5 日時点)。

28 図表 1-2-1 及び 1-2-2 において、アプリケーション内及び Google Play 紹介ページは、アプリケーションのプライバシーポリシーを計上。開発者ウェブサイトは、主として会社全体のプライバシーポリシーを計上。

29 WG 第 4 回資料 4「スマートフォンアプリケーションの表示・検証に関する国内・海外動向」（日本総合研究所）。人気が高く、ダウンロード数の多いアプリケーションを中心に調査するため、Google Play 日本無料アプリケーションランキング、米国無料アプリケーションランキングより上位 40 位のアプリケーションを抽出（2013 年 2 月 5 日時点）。ただし、4 つのアプリケーションについては、日本からダウンロードまたはインストールできなかったため、実際に調査したアプリケーションは 36 個となった。

図表１－２－２：アプリケーションのプライバシーポリシーの作成・公表の日米比較

場所	内容	日本(計40アプリ)		米国(計36アプリ)	
		対象アプリ数	比率	対象アプリ数	比率
アプリ内	利用規約	18	45.0%	15	41.7%
	プライバシーポリシー	14	35.0%	17	47.2%
Google Play 紹介ページ	プライバシーポリシー	10	25.0%	19	52.8%
開発者ホームページ	利用規約	23	57.5%	21	58.3%
	プライバシーポリシー	32	80.0%	25	69.4%

② KDDI 研究所による調査

KDDI 研究所によれば、2013 年（平成 25 年）２月に収集した 100 個のアプリケーションのプライバシーポリシーについて調査を行った結果[30]、アプリケーション内にアプリケーションのプライバシーポリシーの記載があるものは 24 個、アプリケーション提供サイト紹介サイトに記載があるものは 16 個であった。一方、アプリケーション内に何らプライバシーポリシーの記載がないものが 47 個、アプリケーション提供サイトに何らプライバシーポリシーの記載がないものが 74 個あったとしている。

図表１－２－３：アプリケーションのプライバシーポリシーの作成・公表状況

場所	アプリケーションのプライバシーポリシー	関連しそうな事業者のプライバシーポリシー	プライバシーポリシーの記載なし
アプリケーション内	24	29	47
アプリケーション提供サイト	16	10	74
開発者ウェブサイト	19	39	42

またアプリケーションについて技術的検証を行った結果、アプリケーション本体あるいは第三者の情報収集モジュールを含め情報を外部送信するアプリケーション数は 63 個(63%)であり、このうちアプリケーションのプライバシーポリシーを作成していたのは 17 個（27%)、事業者のプライバシーポリシーを作成していたのは 19 個（30%）であり、何ら説明がないものが 27 個（43%）であった。2012 年(平成 24 年) ４月に収集した 100 個のアプリケーションについては情報を外部送信するアプリケーション 81 個(81%)のうち何ら説明がないものが 66 個(81%)、2011 年(平成 23 年）８月に収集した 400 個のアプリケーションについては情報を外部送信するアプリケーション 181 個(45.3%)のうち何ら説明がないものが 157 個(86.7%)であったことと比べると、何らかのプライバシーポリシーが作成・公表され透明性が向上してきていることが定量的に把握できる[31]。

30 第 10 回 WG 資料１ 「au Market におけるプライバシー保護の取り組み」

31 ただし、実際に送信された情報に関して記述が全て正しいと判断されるものは、2013年２月の場合も７個(11%)でありとなっており、実際に送信される情報とプライバシーポリシーの記述の整合性を確認する第三者検証の重要性が指摘されている（第 10 回 WG 資料１ 「au Market におけるプライバシー保護の取り組み」)。

図表１－２－４：利用者情報を外部送信するアプリケーションにおける
プライバシーポリシーの作成・公表状況[32]

調査時期	アプリケーションのプライバシーポリシー	関連しそうな事業者のプライバシーポリシー	プライバシーポリシーの記載なし
2011 年 8 月調査[33]（181 個）	24（13%）		157(87%)
2012 年 4-5 月調査（81 個）	15（19%）		66（81%）
2013 年 2-3 月調査(63 個)	16(25%)	20（32%）	27（43%）

③　独立行政法人産業技術総合研究所による調査[34]

アプリケーションのプライバシーポリシー掲載の現状について、産業技術総合研究所セキュアシステム研究部門において調査が行われている。アプリケーション提供サイトの「プライバシーポリシー」のリンク先などに存在したプライバシーポリシーの体裁について６段階に分類して評価を行ったところ、アプリケーションに関して明確な記述があるプライバシーポリシーが掲載されていた比率は約２割であったとされる。

（２）　記載内容

①　日本総合研究所による調査

アプリケーションのプライバシーポリシーを作成しているものについて、日米それぞれ指針の８項目に該当する内容の記載があるか否かについて確認を行った。その結果、①アプリケーション提供者の氏名等については日米ともすべて記載があった。また②取得される情報の項目、④利用目的については、日米ともにすべてに記載があった。③取得方法については日米ともに約８割に記載があった。⑤外部送信・第三者提供の有無、⑦問い合わせ窓口及び⑧プライバシーポリシーの変更を行う場合の手続きについて日本側は 100%記載があり、米国側も約９割に記載があった。

一方、利用者関与の方法については、日本側は約７割の記載に留まり、米国側も５割強の記載であった。また、情報収集モジュールの有無等については、日本側は２割強の記載であり、米国側も１割弱の記載と記載割合そのものが少ない状況であった。情報収集モジュールについては、実際に情報収集モジュールが含まれているアプリケーションの中でプライバシーポリシーに記載していないものも多い可能

32 アプリケーション内に存在するプライバシーポリシーを中心に検証を実施。

33 調査時期：2011 年 8 月～2012 年 1 月

34 産業技術総合研究所において 2013 年（平成 25 年）4 月において無料アプリケーショントップ 500 から 100 個を抜粋し、有料アプリケーショントップ 500 から 50 個を抜粋、「あ」で検索した結果のアプリケーションから先頭の 50 個を抜粋し、アプリケーションのプライバシーポリシー（APP）の策定状況について 6 段階の評価基準を用いて調査を実施。;「スマホアプリにおけるアプリケーション・プライバシーポリシー掲載の現状調査」情報処理学会研究報告
一般的な Web サイトのプライバシーポリシーや会社としての抽象的なポリシーのみしか存在しないケースは、外国製と推定されるアプリケーションに少なく、日本製と推定されるアプリケーションに多いとしている。

性が指摘されている[35]。

図表１－２－５：アプリケーションのプライバシーポリシーの項目別記載動向の日米比較

番号	内容	日本（計17アプリ）		米国（計22アプリ）	
		対象アプリ数	比率	対象アプリ数	比率
①	情報を取得するアプリケーション提供者等の氏名または住所	17	100%	22	100%
②	取得される情報の項目	17	100%	22	100%
③	取得方法	13	76.5%	18	81.8%
④	利用目的の特定・明示	17	100%	22	100%
⑤-1	通知・公表又は同意取得の方法	2	11.8%	5	22.7%
⑤-2	利用者情報関与の方法	12	70.6%	12	54.5%
⑥-1	外部送信・第三者提供の有無	17	100%	21	95.5%
⑥-2	情報収集モジュール（※）の有無	4	23.5%	2	9.1%
⑦	問合わせ窓口	17	100%	20	90.9%
⑧	プライバシーポリシーの変更を行う場合の手続き	17	100%	21	95.5%

② KDDI 研究所による調査

KDDI 研究所によれば、2013 年（平成 25 年）２月に収集した 100 個のアプリケーションのプライバシーポリシーについて調査を行った結果[36] アプリケーション内あるいは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のプライバシーポリシーのあった 28 個のアプリケーションのうち、①情報を取得するアプリケーション提供者の氏名、②取得される情報の項目、④利用目的の特定・明示は 95%以上に記載があった。③取得方法、⑥外部送信・第三者提供の有無は８割以上記載があるが、利用者情報関与の方法については半分しか記載がなかった。

[35] KDDI 研究所によれば 2011 年（平成 23 年)8 月に 980 個のアプリケーションについて分析を行った結果、約 56.9%のアプリケーションに情報収集モジュールが含有されていたとされる。(「スマートフォン　プライバシーイニシアティブ」P16 第 2 章)。また、2013 年（平成 25 年）2 月に 100 個のアプリケーションについて分析を行った結果、約 63%のアプリケーションに情報収集モジュールが含有されていたとされる。（第 10 回 WG 資料 平成 25 年 5 月 17 日「au Market におけるプライバシー保護の取り組み」（KDDI 研究所））

[36] 第 10 回 WG 資料 1 「au Market におけるプライバシー保護の取り組み」等

図表１－２－６：アプリケーションのプライバシーポリシーの項目別記載動向[37]

番号	内容	日本（計 28 アプリケーション）	
		対象アプリケーション数	比率
①	情報を取得するアプリケーション提供者等の氏名または住所	27	96.4%
②	取得される情報の項目	26	92.9%
③	取得方法	23	82.1%
④	利用目的の特定・明示	26	92.9%
⑤	通知・公表又は同意取得の方法、利用者情報関与の方法	13	46.4%
⑥-1	外部送信・第三者提供の有無	22	78.6%
⑦	問合わせ窓口	19	67.9%
⑧	プライバシーポリシーの変更を行う場合の手続き	18	64.3%

（３）　概要の掲載

指針においては、アプリケーションのプライバシーポリシーについては、分かりやすい概要を作成して掲示することが望ましいとされ、詳細についてはリンク等で表示できるようにすることが有用であるとされている。業界ガイドラインにおいてアプリケーションのプライバシーポリシー概要案等[38]が既に示されている。また、アプリケーション提供者が申請した内容を踏まえ、アプリケーション提供サイトからダウンロードする際に簡単な説明画面を作成・表示している事例[39]もある。

全般的にはイラストを活用したり一部項目のみの概要を表示したりする概要版を表示する事例は一部あるものの、まだ割合は少ない状況である。業界ガイドライン等も参照しつつ、各アプリケーション提供者やアプリケーション提供サイト運営者等による概要版の作成・公表の取組が進むことが望ましい。

37 アプリケーション内又はアプリケーション提供サイトにおいて掲載されたアプリケーションのプライバシーポリシーについて検証を実施。

38 2012 年（平成 24 年）11 月にモバイル・コンテンツ・フォーラムが公表したアプリケーション・プライバシーポリシーのモデル案の中の概要案参照（8 ページ パターン 1、パターン 2 参照）。

39 P36-37②アプリケーション提供サイト運営事業者による検証事例を参照。

２　アプリケーションのプライバシーポリシーに関する課題と対応

アプリケーションによる利用者情報の取扱いに関する透明性を高めていくためには、アプリケーションのプライバシーポリシーや概要版の作成を促進し、利用者がこれらを見て容易に判断できる環境を整えていくことが有用である。

しかしながら、１でみたようにアプリケーションのプライバシーポリシーの作成率は必ずしも高くないこと、また作成していた場合も一部記載項目について記載が十分行われていないなどの課題が見られることから、今後適切なアプリケーションのプライバシーポリシーの策定を更に強力に推進していく必要がある。

なお、米国においても、後述のようにアプリケーションのプライバシーポリシーの作成が求められており[40]、また、それらアプリケーションのプライバシーポリシーには、指針において求められている８項目について何らかの記載がなされている場合が多い。このように、指針に示す内容は国際的に見ても調和のとれたものであると考えられる[41]。また、スマートフォンの一画面に示せるような簡略な通知についてもマルチステークホルダーの会合において検討[42]が行われている。

（１）　アプリケーションのプライバシーポリシーの作成促進

指針の内容を踏まえ、我が国におけるアプリケーションのプライバシーポリシーの作成・公表を促進することがスマートフォンの利用者情報の取扱いの透明性向上のために必要であると考えられる。

既に 2012 年（平成 24 年）８月の「スマートフォン　プライバシー　イニシアティブ」の公表から 10 カ月以上が経過する中、関係事業者や業界団体において一定の取組の進展は見られるものの、現段階において、アプリケーションのプライバシーポリシーの策定状況は十分な水準が既に達成されたとは言えない[43]。既存のアプリケーションで対応が未了のものについては、早急に移行計画を検討し対応を推進するほか、今後作成されるアプリケーションについては、あらかじめアプリケーションのプライバシーポリシーを作成するなど、業界全体として更なる取組の加速が

---

40 FTC スタッフレポート”Mobile Privacy Disclosures – Building Trust through Transparency”（2013 年（平成 25 年）2 月）、カリフォルニア州司法長官提言 ”Privacy on the GO - Recommendations for the Mobile Ecosystem”（2013 年（平成 25 年）1 月）等においてアプリケーションのプライバシーポリシーを作成し、アプリケーションマーケットに示し、利用者に明示的にアクセス可能とすること等が求められている。

41 プライバシーポリシーの作成言語に着目し、英語のみのアプリケーション（海外製の可能性が高い）の方が日本語のみのアプリケーション（日本製の可能性が高い）よりもアプリケーションのプライバシーポリシーの作成比率が高いという調査結果もある（産業技術総合研究所「スマホアプリにおけるアプリケーション・プライバシーポリシー掲載の現状調査」（情報処理学会研究報告,Vol.2013-CSEC-62, No.62）http://staff.aist.go.jp/takagi.hiromitsu/paper/ipsj-csec62-62-ichinose-dist.pdf）

42 P59①商務省 NTIA によるマルチステークホルダー会合参照。

43 産業技術総合研究所の前出の調査によれば、スマートフォンアプリケーションに関する記述がある APP の策定比率は無料トップ 500 で 16%、有料トップ 500 で 21%程度であったとされる。;「スマホアプリにおけるアプリケーション・プライバシーポリシー掲載の現状調査」情報処理学会研究報告,前掲脚注 34。

期待される。

総務省等関係省庁においても、アプリケーションのプライバシーポリシーや概要の作成・公表の促進が図られるように、国際的動向も踏まえつつ、官民連携し関係事業者に働きかけていくことが望ましい。

（２） 分かりやすい掲載・表示方法

アプリケーションのプライバシーポリシーの掲載場所については、上述のとおり、①アプリケーション内、②アプリケーション提供サイト（ハイパーリンク等）のアプリケーション紹介サイト、③アプリケーション提供者のウェブサイトへの掲載等の方法がある。このうち、一般利用者が一般的な導線で見ることが可能であるものは、①か②であり、このいずれかがアプリケーションのプライバシーポリシーの掲載場所として標準的なものとして採用されることが期待されると考えられる。

また、①アプリケーション内の場合も、アプリケーション内の奥深い画面にのみ記載がある場合には呼び出すことが困難な場合もあり得るため、アプリケーションの初回起動時等に表示するなどの方法が採用されることが望ましい。

「スマートフォン　プライバシー　イニシアティブ」の指針においては、電話帳、位置情報、通話記録、写真等のプライバシー性の高い情報について、プライバシー侵害を防止する観点から、個別の情報を取得することについて例えばポップアップ等で表示し同意を取得することとしている。利用者が必ず読んで確認の上同意の有無を表明できる仕組みが重要であり、ポップアップ等による同意取得については、当該情報を取得・送信する前の分かりやすいタイミングで出すことが望ましい。

（３） 標準的な様式・形式

アプリケーション提供者は、アプリケーションのプライバシーポリシーを指針や業界ガイドライン等に基づき策定し、この中に記載が期待される８項目等を標準的な様式に基づき記載することが望ましい。利用者が真に知りたいことを、透明性が高い形で示すために、アプリケーションのプライバシーポリシーについては原則として企業全体のプライバシーポリシーやアプリケーションの利用規約と別に策定されることが望ましい。また、アプリケーションのプライバシーポリシーを策定する際には、企業全体のプライバシーポリシーや当該アプリケーションの利用規約との整合性について確認し、必要に応じて調整を行うことが期待される。

（４） 概要版の作成

アプリケーションにより取得される利用者情報の項目、利用目的、第三者提供・情報収集モジュールの有無等について、スマートフォンの画面で一覧できるように

簡潔に記載した概要版は、適切な様式により分かりやすく作成されれば幅広い層の利用者にとって理解しやすいものであり、利用者情報の取扱いの可視化や透明性を高め、プライバシー保護を高める観点からも有用であると考えられる。

各アプリケーション提供者は、業界ガイドラインや先行事例等も参考にしつつアプリケーションのプライバシーポリシーの概要版の作成と掲載を進めることが期待される。

また、今後も国際的議論の動向や一般利用者の意見などを参考にしつつ、必要とされる事項を分かりやすく示す概要版の表示方法などについては、検討を行い、開発を進めることが有用である。アイコン表示を含む分かりやすい表示方法の在り方について検討し、必要に応じてフィールドトライアル等を実施したり、消費者団体、事業者、学識経験者等の幅広いマルチステークホルダーの意見を聞くこと等を通じて検討を進め、その結果を業界共通的なガイドラインの策定・見直し・充実などにつなげることも、より分かりやすい概要版の普及の加速につながることが期待される。

（５） 利用者に対する周知・啓発

利用者に対して、アプリケーションによる利用者情報の取扱いがアプリケーションのプライバシーポリシーにより説明されていること、概要版の提示も推奨されていること、電話帳等プライバシー性の高い情報についてはポップアップ等で個別情報取得に関する同意が求められるため確認が重要であること等について、業界として周知啓発を推進する必要がある。

最近注意すべき利用者情報の取得を目的としたマルウェアの増加等も踏まえ、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である「スマートフォン　プライバシー　ガイド」を改定し、本ＷＧの中間取りまとめにおいて既に公表している[44]。今後も、関係事業者、関係省庁、業界団体、スマートフォンの利用者情報等に関する連絡協議会など幅広く協力・連携をしながら、利用者に対して必要な情報を周知・啓発していくことが求められる。

（６） 青少年に関する情報の取扱い

スマートフォンのアプリケーションによる青少年からの利用者情報の取得事例も増加している。判断力や経験が乏しい場合もある青少年の特性を考慮して、十分に配慮した取扱いを行う必要性がある。国際的動向等も踏まえ検討を深め、関係事業者、関係省庁、業界団体などが幅広く協力・連携をしながら、必要とされる対応を行っていくことが望ましい。

---

44 スマートフォン　プライバシー　ガイドの概要版等を公表（http://www.soumu.go.jp/main_content/000227662.pdf）

（７）定期的なアプリケーション調査の実施とフォローアップ

人気上位 100－200 程度のアプリケーションについて、定期的にアプリケーションのプライバシーポリシーの策定・公表状況について調査を行う。この調査は、「第三章　４　今後の具体的措置」にある「（７）定期的なアプリケーション調査の実施」と合わせて行い、取りまとめた調査結果について公表する。

調査結果を踏まえ、「スマートフォン　プライバシー　イニシアティブ」の実施状況を継続的にフォローアップし、考察する。また、調査結果を踏まえ必要がある場合には、取るべき追加的措置等について検討を行う。

３　情報収集モジュールに関する課題

（１）　「指針」において期待される内容

指針において、情報収集モジュール提供者は、情報収集モジュールのプライバシーポリシーを作成・公表するものとされており、これら内容について変更があった場合にはプライバシーポリシーを更新するものとされている。

また、指針において、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は、アプリケーションのプライバシーポリシーにおいて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について記載することとされている。アプリケーション提供者による正確な説明に資するため、指針において、情報収集モジュール提供者は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ととされており、これら内容について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されている。

（２）　情報収集モジュールに関する状況と対応

情報収集モジュールは、アプリケーション本体以外のモジュールで、何らかの情報を外部送信するプログラムである。広告配信、アプリケーションの利用解析、クラッシュレポート等のために使われていることが多い[45]。民間事業者の調査結果によれば、情報収集モジュールの多くは契約者・端末固有 ID[46]等を送付しており、また、位置情報等を送付するものも見られるとされる。

45　第10回WG資料　平成25年5月17日「au Marketにおけるプライバシー保護の取り組み」（KDDI株式会社）、Software Development Kit（SDK）としてコンパイルされたJavaバイトコードや画像などをZIP圧縮したファイル（Java Archive File:jar ファイル）で配布されることが多い。

46　契約者・端末固有ID（AndroidID、IMEI、MACアドレス）等

日本において提供されているアプリケーションに含まれる情報収集モジュールについては、何らかのプライバシーポリシーがあるものは多く見られたが、半数以上が英文で記載されており、一般利用者に分かりやすい説明が行われているとは言えない状況である[47]。情報収集モジュールによる利用者情報の取扱いの透明性を高める観点から、関係する業界団体等が連携して情報収集モジュール提供者への働きかけを行い、協力を受けつつ、情報収集モジュール毎に分かりやすいプライバシーポリシーの作成を促すことが必要である。

また、アプリケーション提供者は内包する情報収集モジュールについてアプリケーションのプライバシーポリシーに記載して説明することが求められるが、この記載率については、１～２割程度に留まっている[48]。情報収集モジュールが組み込まれているアプリケーションの比率については、約 63%という調査結果[49]があり、情報収集モジュールが組み込まれているにもかかわらず、説明を行っていないアプリケーションも多いと考えられる。アプリケーション提供者が情報収集モジュールについて正確に把握しプライバシーポリシーに記載するよう促すことが必要である。

さらに、情報収集モジュールについてのリストを作成し共有していくことが共通的基盤として有用である。このリストは、アプリケーション提供者によるプライバシーポリシーへの記載、一般利用者への情報提供、第三者検証等の実施等を推進するためのデータベース等としても活用されることが期待される。

４　関係事業者における取組

（１）　移動体通信事業者・端末提供事業者

「スマートフォン　プライバシー　イニシアティブ」における指針において、移動体通信事業者に対し、スマートフォンの利用者情報等の適正な利用を促進するため、アプリケーション提供サイト運営者として①アプリケーション提供者に対する対応、②アプリケーション利用者に対する周知啓発の両面から対応が期待されている。

これを受けて、2012 年（平成 24 年）10 月に、電気通信事業者協会（TCA）の移動電話委員会のもとに、「スマートフォンの利用者情報等の適正利用促進検討部会[50]」が設置され、2013 年（平成 25 年）３月「スマートフォンアプリケーション提供サ

47 参考資料の 54 個について調べたところ 51 個にプライバシーポリシーがあったが、半数以上の 28 個については英文であり、日本語で書かれているものは 23 個に過ぎなかった。

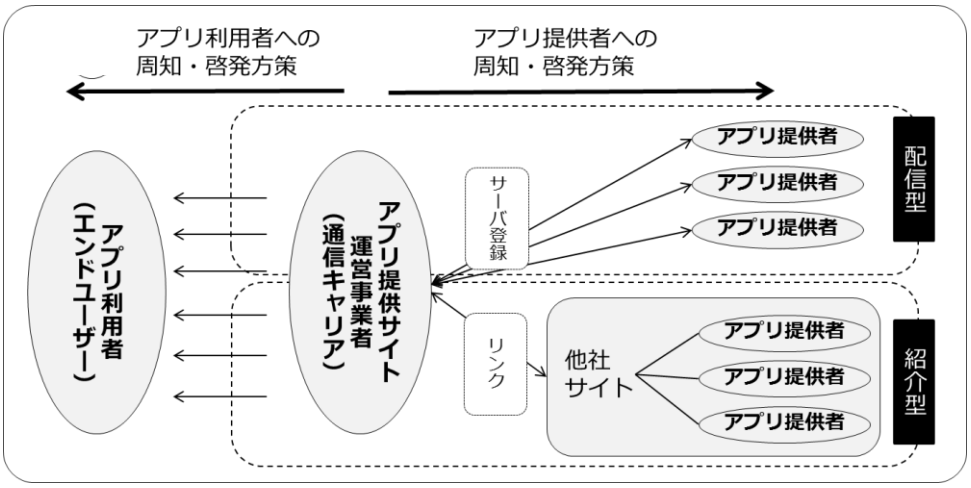
48 2013 年 1 月　日本総合研究所調査

49 第 10 回 WG 資料 1 「au Market におけるプライバシー保護の取り組み」等

50 WG 第 4 回会合資料 2「TCA におけるスマートフォンのプライバシーに関する取り組み」（TCA）。

イト運営事業者向けガイドライン（以下「電気通信事業者協会ガイドライン[51]」という。）」が策定・公表された。

図表１－２－７：アプリケーション提供サイト運営事業者の取る方策案



① アプリケーション提供サイトの運営者としての活動

【アプリケーション提供者等に対する支援】

電気通信事業者協会ガイドラインにおいて、各アプリケーション提供サイト運営事業者は、「スマートフォン　プライバシー　イニシアティブ」に沿ったアプリケーションの掲載ガイドライン等を作成しアプリケーション提供者にあらかじめ提示し、アプリケーション提供者等が適切なアプリケーション・プライバシーポリシー（APP）を作成できるように支援すること、アプリケーション提供者との関係を通じてアプリケーション・プライバシーポリシーが守られるように働きかけることが期待されている。アプリケーションを自社のサーバーに一旦蓄積した上でそこから配信する配信型[52]の場合、アプリケーション提供者等から事前申請を受けて検査を実施した上で配信することが期待されている。

また、アプリケーションを自社のサーバーに蓄積することなく他事業者のサーバーから直接配信する紹介型[53]の場合であっても配信型の場合であっても、自社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作成したアプリケーション・プライバシーポリシーに対するハイパーリンクを掲載する等することが期待されている。

---

51 TCA のウェブサイトに公表されている。http://www.tca.or.jp/topics/pdf/20130329guideline.pdf

52 例えば、KDDI の au Market や NTT ドコモのスゴ得コンテンツは配信型サービスであるとされている。

53 例えば、NTT ドコモの d メニュー及び d マーケット（アプリ&レビュー）、ソフトバンクモバイルのメニューリストなどについては、紹介型サービスであるとされている。

さらに、必要に応じて、他の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等に対する啓発活動を実施することが望まれている。

② アプリケーション利用者に対する周知啓発等

【契約時等における利用者に対する周知啓発】

電気通信事業者協会ガイドラインにおいて、移動体通信事業者は、既存の販売チャンネルを通じて、スマートフォン契約時あるいは機種変更時に利用者に対して自らが提供するサービス条件の概要を説明することが求められている。この際、スマートフォンをこれまで利用していない方も容易に理解できるように①スマートフォンと従来型の携帯電話端末の違い（スマートフォンの特性やサービスの構造)、②スマートフォンにおける様々な利用者情報の取扱いと注意点、③スマートフォンにおける情報セキュリティ対策等について、書面に記載の上、丁寧な説明をすることが望まれている。また、契約後も利用者からの問合せに対応することとされている。

【様々なリテラシーの消費者への対応】

青少年向けに利用機能を制限したスマートフォン端末（例：NTT ドコモのスマートフォン for ジュニア等（KIDS 向け））や高齢者向けに、見やすさ、分かりやすさを訴求した端末（例：NTT ドコモのらくらくスマートフォン、ソフトバンクモバイルのシンプルスマホ）を開発し、アプリケーションのダウンロード対象を制限するなどの取組が行われている。これらは、利用者の特性やリテラシーを考慮し、セキュリティやプライバシー上の配慮をあらかじめ行ったスマートフォンと言える。

電気通信事業者協会ガイドラインにおいて、青少年や高齢者向けのスマートフォン利用に関する自主セミナーの開催を継続的に行っていくことが望まれている（例：NTT ドコモのケータイ安全教室[54]、KDDI のケータイ教室等)。

（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する支援】

指針において、アプリケーション提供サイト運営事業者、OS 提供事業者に対し、スマートフォンの利用者情報等の適正な利用を促進するため、アプリケーション提供サイト運営者としてアプリケーション提供者に対する対応等が期待されている。

54 例えば、NTT ドコモが作成しているケータイ安全教室の教材（保護者・教員編）において、「スマートフォンプライバシー ガイド」についても分かりやすく説明し周知している。
http://www.nttdocomo.co.jp/binary/pdf/corporate/csr/social/educational/safety/manual_download/adult_text_04.pdf

主要なOS事業者が運営するアプリケーション提供サイト[55]のアプリケーション紹介ページにおいて、2012年（平成24年）、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へのハイパーリンクを設置する場所が設けられている。

（３） その他関係し得る事業者

指針において、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はないアプリケーションが判明した場合の対応を検討したりするなど、指針の内容を考慮しつつ取組を協力して進めることが期待されている。

例えば、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（アンドロイダー）において、①物理的、運用的に実在していることが確認できたアプリケーション開発者のみを「公認デベロッパー」とし、②公認デベロッパーが開発したアプリケーションについて独自に「パーミッション（利用許諾）の正当性」、「ウィルスのスキャン」について確認し、当該アプリケーションが利用しようとする利用者情報の危険度や利用目的の正当性等を確認した上で、安全性の確認がとれたものだけを「公認アプリ」として掲載している事例がある。

「公認アプリ」については、利用しようとする利用者情報の項目（パーミッション）を列挙した上で、それぞれの利用者情報の利用目的等についてアプリケーション提供者自身に記載してもらい分かりやすく透明性を高める工夫がなされている。

さらに、アンドロイダーとして確認したアプリケーションのみを紹介するアンドロイダーAPIを各種Webサイトや MDM、各種媒体等向けに提供するサービスも開始している[56]。

[55] Apple社の運営するApp Store及びGoogle社の運営するGoogle Play。

[56] アプリケーションフィルタリングやセキュリティアプリケーションのオプション機能として提供されている事例もある。

図表１－２－８:レビューサイトにおけるアプリケーションに係る検証情報紹介例

５　アプリケーション提供サイト等における連絡通報窓口

（１）　移動体通信事業者のアプリケーション提供サイト

指針において、移動体通信事業者のアプリケーション提供サイトは、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こととされている。

既に、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、連絡通報窓口が設置されている。また、一般に利用者からの電話による問い合わせの受付窓口なども用意している。

指針内容を踏まえ、電気通信事業者協会ガイドラインにおいて、利用者が容易に到達できるような分かりやすい連絡窓口を設置し、プライバシーやセキュリティ上利用者情報の取扱いが適切ではないアプリケーション等についての情報を積極的に収集し、不適切なアプリケーションが判明した場合には、当該アプリケーションの削除、利用者への注意喚起、関係事業者間の情報共有等の対応をすることが求められている。

（２）　OS 事業者等のアプリケーション提供サイト

指針において、OS 提供事業者等のアプリケーション提供サイトは、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こととされている。

既に、OS 事業者等のアプリケーション提供サイトにおいて、連絡通報窓口が設置されており、アプリケーションに問題があった場合、当該アプリケーション名及び問題のカテゴリー等を示しつつ通報することが可能となっている。

（３）　連絡通報窓口間の連携について

①　掲載基準の明確化

それぞれのアプリケーション提供サイトにおいて、当該アプリケーション提供サイトへのアプリケーション掲載基準を有しており、その掲載基準に該当しないと認められる場合には、当該アプリケーションについてあらかじめ掲載しないあるいは事後的に掲載を取りやめるという形をとることが一般的である。

まず、法令を遵守していることが求められており、通報等により違法である可能性を指摘されたものについては、法令を踏まえ対応するものとされている。また、全般的にはアプリケーション掲載基準を満たしているかどうかといった観点から判断が行われていると考えられる。ただし、アプリケーション掲載基準につ

いては、個人情報やプライバシー保護の観点からは、一義的に判断が定まるほど具体的であるかどうかというと、必ずしもそうではない場合がある。

アプリケーション提供サイト運営事業者が、利用者のプライバシーの取扱いやセキュリティ上適切ではないとされるアプリケーションについて掲載の取りやめ等の個別判断を行う場合の基準について、アプリケーション市場の性質やオープンなイノベーション等に配慮しつつ、あらかじめ一定の基準を明らかにすることが望ましい。

適切な掲載基準、運用基準や掲載取りやめの実績等が明らかにされることにより、当該基準に沿ったアプリケーションの作成が促進されることが期待されものであり、また、利用者に対する透明性が高まることが期待される。

② 連携について

上記のように移動体通信事業者や OS 提供事業者において連絡通報窓口が設けられるとともに、セキュリティベンダー等において、独自の連絡通報窓口を有している。

利用者情報の取扱いの観点から問題のあるアプリケーションについて、アプリケーション提供サイトやセキュリティベンダー等の連絡通報窓口間において、情報共有を図るための連絡体制を検討することが望ましい。

また、連絡通報窓口に対する情報提供のうち、共有可能なものについて関係団体・機関や技術・法律の専門家がこれをチェックするとともに、アプリケーション提供サイト運営事業者と情報共有を行い、必要な対応を推進できることが望ましい。

第３章　アプリケーションの第三者検証の在り方

第１章においても示されたように、利用者情報を狙う不正アプリケーションが増加しているとともに、利用者情報の取扱いが適正でないアプリケーション等も存在することが指摘されている。このため、実際に個々のアプリケーション等について、利用者情報の適切な取扱いが行われているかどうか等を、運用面・技術面から第三者が検証する仕組みが民間主導により整えられることが望ましい[57]。

本章においては、「スマートフォン利用者情報取扱指針（以下、「指針」という。）」の実効性を高める上で有効と考えられる、アプリケーションの第三者検証の在り方について、具体的に検討を行うこととする。

本章の構成は大きく４つに分かれており、第一に、アプリケーションの第三者検証の実施内容及び在り方について選択肢を示しつつ基本的な考え方について検討を行うこととする。第二に、スマートフォンのビジネス構造に関わる様々な主体による安心安全な利用環境を目指すための取組において、既にアプリケーション検証が開始されている事例を踏まえて全体像を見ることとする。第三に、第一及び第二における検討結果を踏まえ、第三者検証の検証主体、検証の具体的方法と基準について取りまとめる。第四に、これらの検討を踏まえ、今後取り組むべき具体的措置を提言することとする。

１　概要

（１）アプリケーションの第三者検証の意義

アプリケーションの第三者検証は、「スマートフォン プライバシー イニシアティブ」に示された指針の実効性を高める上で、次のような意義を持つと考えられる。

①　アプリケーション提供者にとっては、その提供するアプリケーションについて、適正なアプリケーションのプライバシーポリシー（以下、「APP」という。）が作成・公表されており、それに合致した運用をしていることが客観的に確認され、当該アプリケーションに対する信頼が醸成されることがその利用促進にもつながり得る。

②　利用者にとっては、当該アプリケーションが適正な APP の下、適正な運用がなされているかどうかが第三者によって客観的に確認されることにより、それを利用するかどうかの有効な判断基準となり得る。

（２）アプリケーションの第三者検証の実施内容

アプリケーションの第三者検証は、アプリケーション提供者又は利用者から、検証を行う主体に対して申出がなされた等の場合や第三者検証を行う者が自ら選定

[57] 「スマートフォン　プライバシー　イニシアティブ」第 5 章「2　指針の実効性を上げるための様々な取組み」等を参照。

して行う場合があり、検証を行う機能・能力を行う者が以下のいずれか又は両方を行うことが想定される。

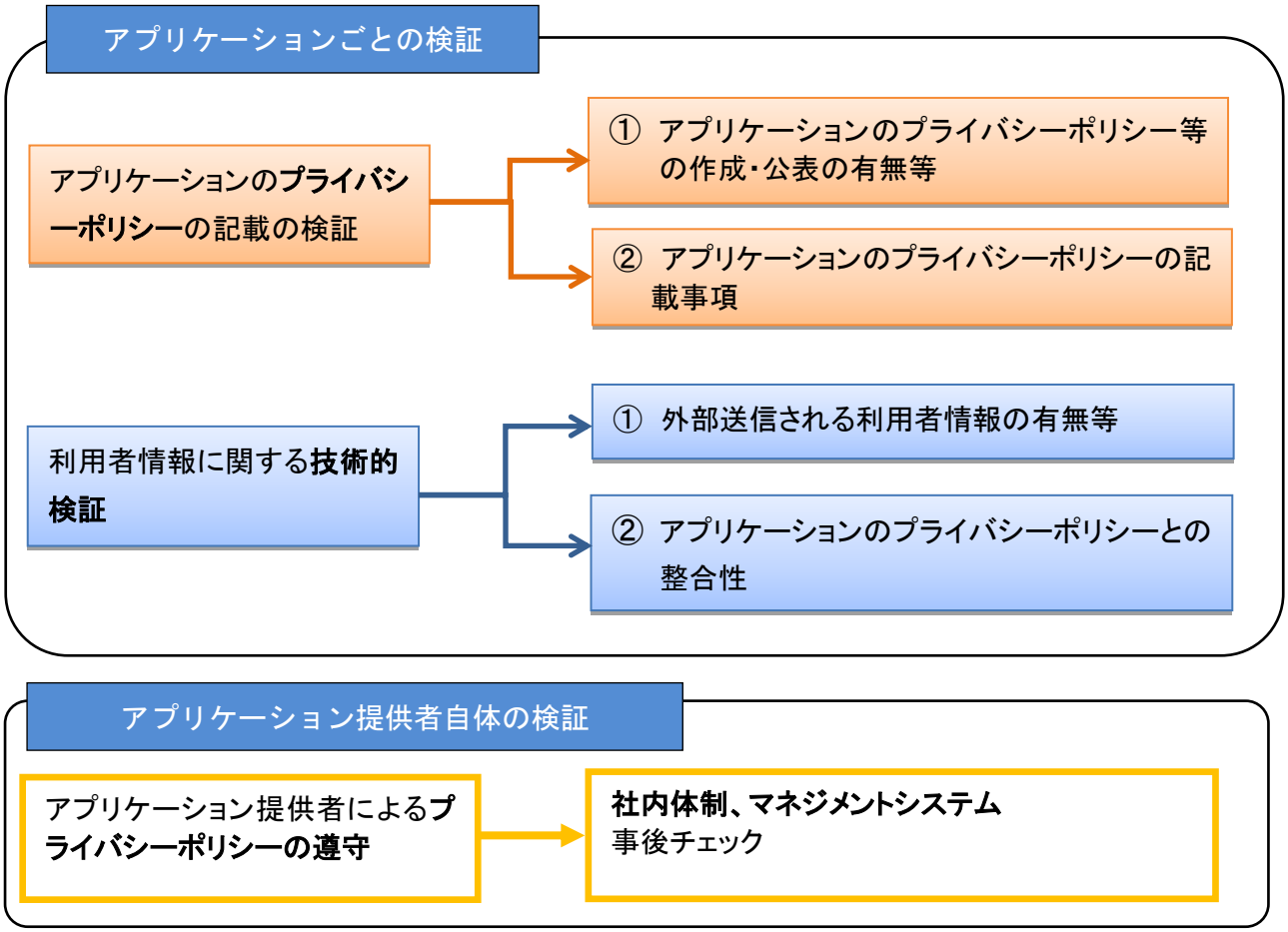
① APP の記載の検証（APP 等の作成・公表の有無等、APP の記載事項）

② APP の動作に関する技術的検証（外部送信される利用者情報の有無等、APP との整合性）

この検証結果は、あくまで第三者検証が行われた時点でのものであり、その後の利用者情報の管理・運用状況や、利用者情報の取扱いの変更によって変動するものであることから、事後的な確認や更新を可能とすることも重要である。

なお、個々のアプリケーションの記載や動作が「スマートフォン　プライバシー　イニシアティブ」の求める内容に合致しているかとは別に、アプリケーション提供者そのものの信頼性やマネジメントシステムについて確認することも付加的な方策として一定の有用性がある。

図表１－３－１：アプリケーション検証の体系



（３）アプリケーションの第三者検証の在り方

①　第三者検証の在り方の選択肢

このようなアプリケーションの第三者検証の在り方には、以下のような選択肢が考えられる。

ア　第三者検証を行うための機能・能力を有する単一の主体が、APP の記載の検証から技術的検証までを一括して行い、そのために必要な検証基準等についても、当該単一主体が作成し運用する。

イ　第三者検証を行うための機能・能力を複数又は多数の主体が分散的に保持・提供することを許容し、それらの機能・能力に応じて APP の記載の検証や技術的検証を行う。ただし、そのために必要な検証基準等については、多数の関係者が受け入れ可能な共通的なものを作成し、運用する[58]。

ウ　第三者検証を行うための機能・能力を複数又は多数の主体が分散的に保持・提供することを許容し、それらの機能・能力に応じて APP の記載の検証や技術的検証を行う。そのために必要な検証基準等についても、各主体が作成したものを活用する。

②　検討

以下の事項を総合的に考慮すれば、上記のうちイによる対応を推進することが適当であると考えられる。

・　何らかの形でアプリケーションの検証を行う民間事業者や団体がすでに存在しており、それらの能力や知見を活用することが適切と考えられること。

・　第三者検証を利用するアプリケーション提供者や一般利用者が求める検証の内容やレベルに応じて、多様な検証サービス（「簡易な検証」[59]を含む）を選択的に利用できる環境を整備することが適切と考えられること。

・　ただし、どのような主体による検証を活用した場合にも、検証結果に対する信頼感のレベルについて、利用者にある程度共通した認識が得られるためには、どのような基準でどのような検証が行われたかについて、一定の信頼性ある共通的な物差しに拠っていることが適切と考えられること。

③　留意すべき事項

また、上記①イの枠組みによる第三者検証が行われ、その利用が普及するためには、以下の点に留意する必要がある。

ア　検証を行う主体が、そのビジネスモデルの中に適切に位置づけ、持続的・

58　第三者検証を実施するそれぞれの者が、共通的な検証基準等を踏まえ、具体的には、個別の基準に対する実施細目を設定したり、推奨基準を活用して検証を行うこと等が想定される（本提言 P47「②検証の基準」参照）。

59 ハイレベルな検証はコストが高く、中小零細のアプリケーション開発者にはコスト負担ができない可能性があるため、多くのアプリケーション開発者が受けることが可能な「軽い検証」の仕組みの仕組みについて検討すべきとの指摘があった。例えば、「スマートフォン　プライバシー　イニシアティブ」に基づくアプリケーションのプライバシーポリシーの作成の有無等を中心に検証を受ける方法などもある。

継続的に提供することが求められること。

イ　検証に必要な基準等については、検証の利用者の幅広い信頼を得るためにも、アプリケーション提供事業者、移動体通信事業者、OS 事業者、携帯電話メーカー、セキュリティベンダー、格付け関係事業者及びこれらの団体、消費者団体、法律・プライバシー等の専門家等からの広範なインプットを受けた本ＷＧとして、提示すべきこと。

ウ　アプリケーションの検証結果の表示については、検証を申し出た者に分かりやすいものであるべきことはもとより、特に APP の記載や動作に問題がないことや、何らかのグルーピングや段階の設定によりアプリケーションの信頼の度合を示す場合については、一般利用者にとっても分かりやすく表示する方法が早期に検討・提示されるべきであること。

以下、本章においては、アプリケーションの検証等に関する取組の現状や実例を踏まえ、第三者検証の在り方に関連し、検証主体、検証方法と検証基準、検証後の対応、今後の具体的措置等について詳細な検討を行うこととする。

２　アプリケーションの検証・透明性向上等を通じた安心安全強化の取組

現在、スマートフォン等の OS は上位２つを合計すると約９割のシェアを有している[60]とされ、アプリケーションの検証・透明性等を通じた安心安全強化の取組についてもこれらのプラットフォームを前提として行われる場合も多く想定される。

今後端末発売が予定される新たなモバイル OS[61]においても、プライバシー・バイ・デザインの観点からアプリケーション提供サイトや OS の仕様などが設計され、適正な利用者情報の取扱いを組み込んだ設計とされることが期待される。

（１）利用者情報の取扱いに関する様々な主体による検証

スマートフォンの OS 提供事業者や移動体通信事業者等が提供するアプリケーション提供サイトはプラットフォームとしてアプリケーションに関する掲載ガイドラインを策定し、確認・検証を行う場合が多い[62]。一定基準の検証のみを行ったアプリケーションのみを掲載するアプリケーション紹介サイトもある。

また、スマートフォンの端末あるいは OS は、利用者情報に関する一定の制御を

60　ガートナー調査によれば世界的には Android が約 7 割、iOS が約 2 割であり、MM 総研によれば日本国内においては Android が約 6 割、iOS が約 3.5 割のシェアを有するとの調査結果がある。
ガートナー：“Market Share Analysis: Mobile Phones, Worldwide, 1Q13.”
http://www.gartner.com/document/2482415?ref=QuickSearch&sthkw=G00252860
株式会社 MM 総研：2012 年度通期国内携帯電話端末出荷概況
http://www.m2ri.jp/newsreleases/main.php?id=010120130509600

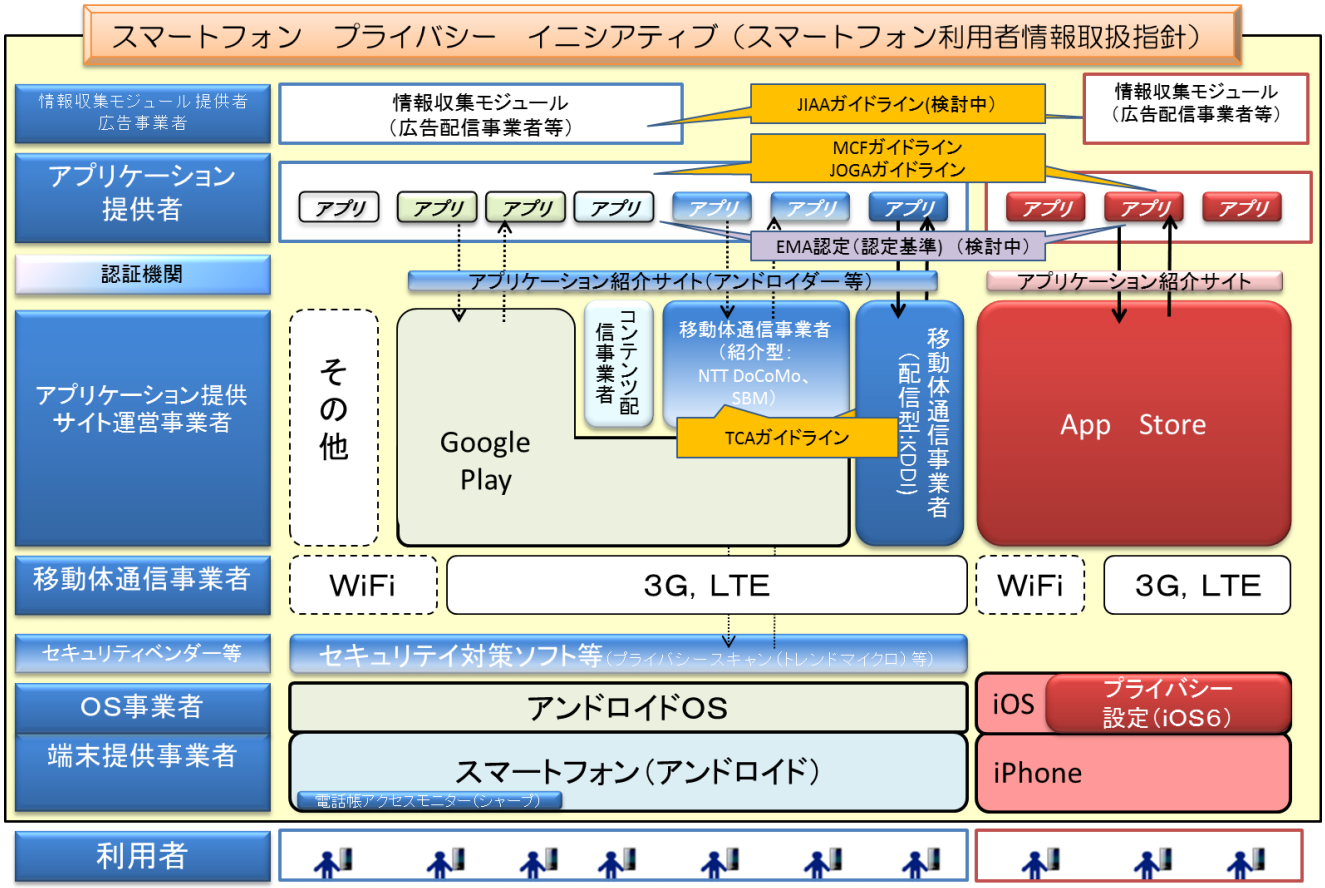
61 Tizen 及び Firefox OS 等新たなモバイル OS を用いた端末が日本国内においても発売予定であるとされている。

62　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。

提供するものである[63]。セキュリティ対策ソフト等は、当該対策ソフトによる検証結果を利用者端末に表示等可能とする。

さらに、認証機関（一般社団法人モバイルコンテンツ審査・運用監視機構（EMA）等）が行う認証において透明性確保等の観点から一定の検証を行う可能性もある。

図表１－３－２：アプリケーションの検証・透明性向上に関わる主な関係事業者等



（参考）実線矢印は、事前審査を行っているもの。点線矢印は事前又は事後に一定の検証を行っているもの

（２） 各レイヤーにおけるアプリケーション検証の事例

① アプリケーション提供サイト・OS 提供事業者による検証事例

アプリケーションが電話帳や位置情報等のプライバシー性の高い利用者情報を取得しようとする場合に、利用者に知らせて同意を取得した上で利用者情報を取得する仕組みをプラットフォームとして導入している事例[64]がある。

---

63 「スマートフォン　プライバシー　イニシアティブ」に記載されているように、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おり、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）が定められており API を通じて利用者情報が収集される「スマートフォン　プライバシー　イニシアティブ」P11　第二章 2（1）。

64 例えば、Apple 社の iOS6 の場合、アプリケーションが電話帳情報、位置情報、写真等へアクセスしようとした際、ポップアップ表示により、当該利用の可否の確認を利用者に求める（参考資料 P78「iOS6 におけるプライバシー設定」）。同様に、Firefox OS の場合、電話帳情報、位置情報についてはすべてのアプリケーションについてアクセスしようとした際、ポップアップ表示により利用の可否の確認を利用者に求める予定としており、

また、アプリケーションがアクセスする利用者情報の種類をワンストップで一覧性を持って把握できる「ダッシュボード」[65]を用意したり、実際に利用者情報にアクセスした際にアイコンその他の方法で通知したりする仕組みをプラットフォームとして導入している事例もある。

これらは、プライバシー性の高い情報へのアクセスを利用者に確実に知らせることにより可視化を進めるものであり、利用者による同意や管理を可能にする分かりやすい仕組みであると考えられる[66]。

この他、一定のマーケット審査を受けたアプリケーションのみに電話帳などのプライバシー性の高い情報へのアクセス権限を付与する仕組みとするOSもある[67]。

② アプリケーション提供サイト運営事業者による検証事例

加入者向けのアプリケーション提供サイト（au Market）[68]を運営するKDDIは、アプリケーション提供者から利用者情報の取扱いに関する申請を受け付けた上で、動的解析及び静的解析などによる技術的検証を行い掲載前にアプリケーションについて利用者情報の取扱いの適正性を判断している。

また、透明性を高める観点から、au Market からアプリケーションをダウンロードする際に、どのような利用者情報が外部送信されるか利用者がスマートフォンの画面で確認できる説明画面[69]を作成している。

次回以降も毎回確認するかどうか利用者が選択できるとしている（第10回WG 資料8「Firefox OS-Security」）。

65 例えば、Apple社のiOS6の場合、電話帳情報、位置情報、写真等へアクセスしようとするアプリケーションを一覧表示させるとともに、当該情報の利用を個別のアプリケーション毎に管理することができる仕組みを導入。同様に、Firefox OSの場合も、OSの設定画面でアプリケーションごとに利用者情報へのアクセスを管理できる予定であるとしている（第10回WG 資料8「Firefox OS-Security」一般社団法人Mozilla Japan 浅井智也氏）。

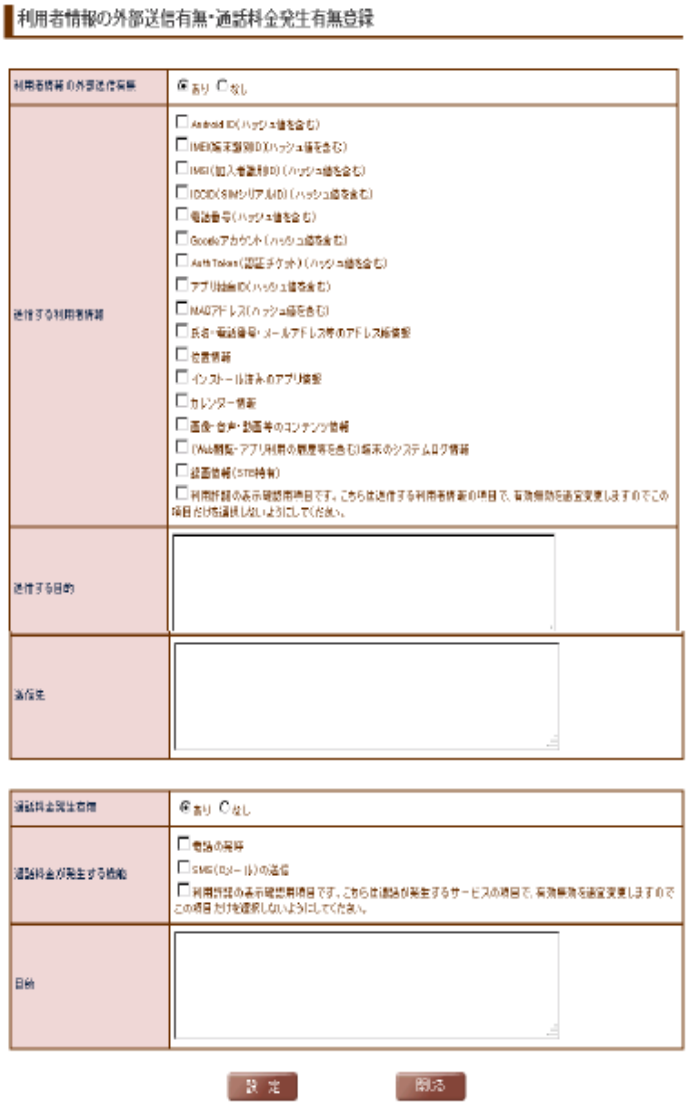
66 FTCスタッフレポート「モバイル・プライバシー・ディスクロージャーズ」（2013年2月）において、Apple, Google, Microsoft等を例示し、プラットフォーム事業者（OS事業者）がセンシティブ情報へのアクセスを利用者に知らせ同意取得すること、ワンストップで利用者情報へのアクセス状況を利用者に知らせるダッシュボード、送信を示すアイコンの開発の検討を提言している。

67 WG第10回 資料8「Firefox OS - Security」。プライバシー性の高い情報へのアクセス権限を求めるアプリケーションについては、任意のWebサイトからJavaScriptを直接読み込んで実行することはできなくなっている。マーケットで審査されたJavaScriptだけが実行されることにより、安全性を確保する仕組みであるとしている。

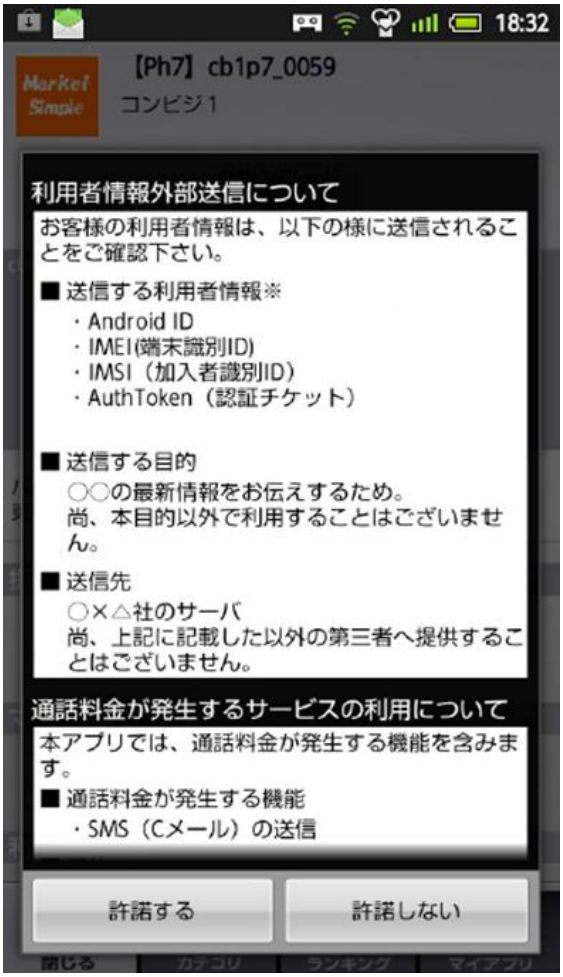
68 電気通信事業者協会ガイドラインにおける配信型の類型。

69 送信する利用者情報、送信目的、送信先等を簡易にスマートフォン画面上に表示する。

図表１－３－３：
利用者情報の扱いに関する申請画面の例
（au Market）



図表１－３－４：
ダウンロード時の利用者向け説明画面の例
（au Market）



③ 端末提供事業者による検証事例

端末提供事業者が、アプリケーションがどのタイミングでスマートフォンの電話帳情報へアクセスするのか可視化するとともに、アプリケーション開発者や通信事業者、OS 事業者に影響が出ない方法で管理する方法を実装した事例もある[70]。

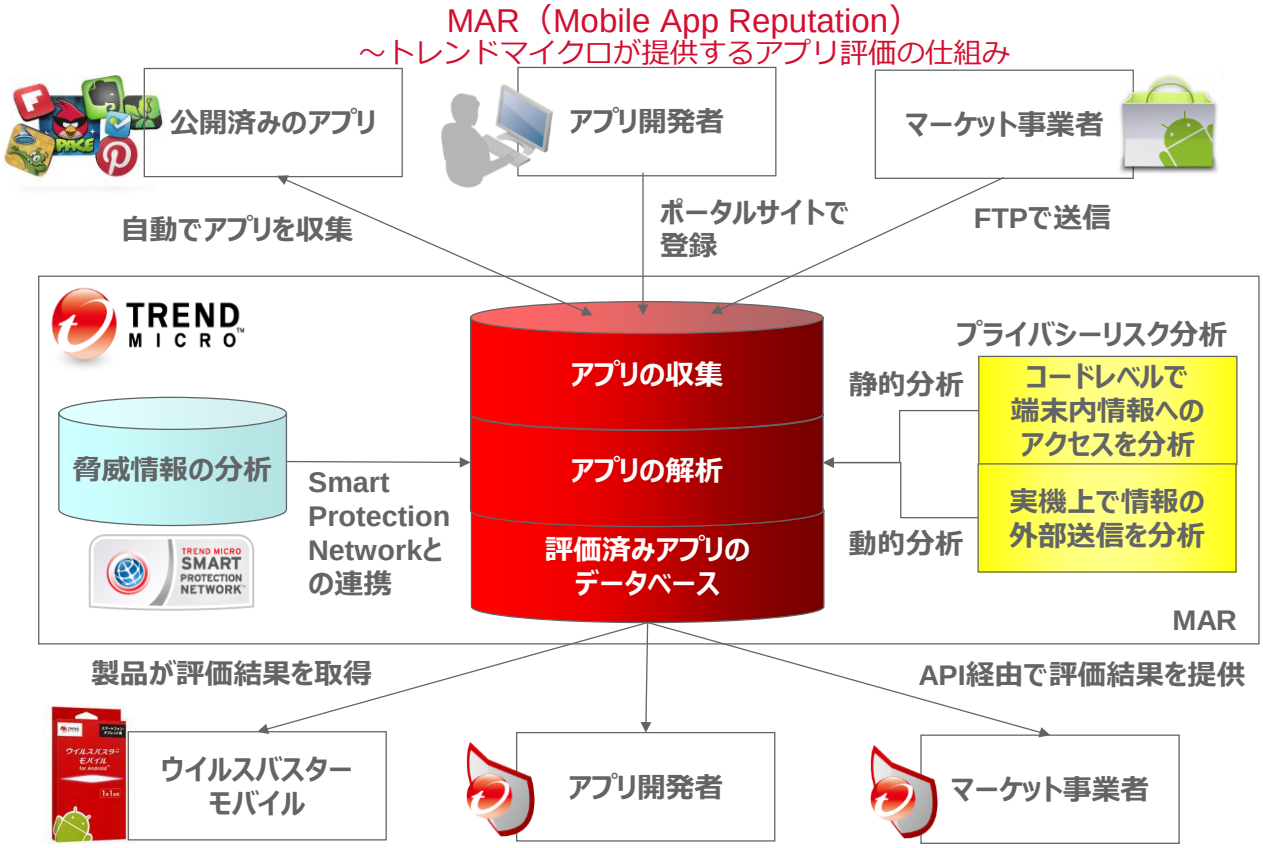
電話帳などのプライバシー性の高い情報へのアクセスを利用者に確実に知らせることにより可視化を進めるものであり、また利用者による同意や管理を可能にするものである。

70　第 7 回 WG 資料 2「電話帳アクセスモニターのご紹介」（シャープ株式会社）

④ セキュリティ関係事業者による検証事例

トレンドマイクロ株式会社は、100 万以上のアプリケーションについて静的解析[71]及び動的解析[72]を行った上で評価点（レピュテーションスコア）とレポートを生成し、MAR（Mobile App Reputation）というデータベースとして運用しており、①不正な挙動の分析（アプリケーションの不正な振る舞いの有無、不正な署名情報による改造アプリケーションや海賊アプリケーションの分析・評価）、②プライバシーリスク（外部に送信しようとするプライバシー情報に関するリスク分析・評価）、③システムリソースの消費についての情報を取りまとめている。特にプライバシーリスクについては、この MAR を活用し、データ外部送信について積極的に検出しており、契約者・端末固有 ID(IMEI/IMSI/SIM_SN 等)、電話番号・アカウント、位置情報、電話帳（着信履歴・連絡先）、利用者入力情報、データベース情報（写真・動画、音楽ファイル、ボイスレコーダー）等に着目し、４段階に区分し、リスクを分析しているとしている[73]。

図表１－３－５：トレンドマイクロ社のアプリケーション評価の仕組み



[71] 外観から判断できる情報（ハッシュ値など）とソフトウェア解析。
[72] アプリケーションを実機上で動作させ実際の動作を分析。
[73] WG 第 4 回会合資料 3「スマートフォンのプライバシー保護に関する取り組み」(トレンドマイクロ株式会社)。

また、ネットエージェント株式会社は、大量のアプリケーションについて継続的にクローリングにより収集し静的な自動解析[74]を行った上で、一定の基準を定めて、それぞれのアプリケーションが利用者情報の取扱いの観点からどのような性質を持っているのか、独自のリスクレベルに応じて色分けするなどして分析結果を一般向けにサイト等で公表するとともに、事業者向けに詳細な分析結果を提供している[75]

タオソフトウェアは、アプリケーションの実行ファイル[76]を静的解析により分析し、脆弱性、品質とともに、利用者情報の関係でパーミッションと対応するAPIや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フェース（API[77]）関連、第三者モジュール等を分析しレポートを作成するサービス[78]を提供している。

⑤ レビューサイト運営事業者による検証事例

レビューサイトであるアンドロイダーは、2012 年（平成 24 年）10 月以降、「安全なアプリのみを紹介するプラットフォーム」にリニューアルしたとしている。アプリケーション開発者の実在性を確認した「公認デベロッパー」が開発したアプリケーションのうち、パーミッションの妥当性の確認とウィルススキャンを行ったアプリケーションのみを「公認アプリ」としてレビューサイトに掲載するという仕組みである[79]。また、2013 年（平成 25 年）2 月から、アンドロイダーの運用で蓄積されたセキュリティ審査済みのアプリケーション情報を無償提供するサービスを開始している[80]。

⑥　認証機関[81]

プライバシーポリシーの記載の検証について、EMA のサイト表現運用管理体制認定基準及びコミュニティサイト運用管理体制認定基準において、サイト運用事業者が利用者情報を取得する際に、利用者のプライバシーに配慮した対応を行うことを

---

74 WG 第 7 回 WG 資料 1「secroid の目指す スマートフォン環境の安全」（ネットエージェント）。平成 25 年 4 月 4 日現在で約 47 万 5000 のアプリケーションを分析しデータベースを構築しているとしている。

75 WG第7回WG資料1「secroidの目指す スマートフォン環境の安全」（ネットエージェント）独自の判定基準に基づき、個人情報・ユーザ識別情報などを収集する可能性の有無を判定するとしている（例えば電話番号や電話帳にアクセスするものは危険度がHIGHとし、GPSによる位置情報にアクセスするものは危険度LOW等と出すこととしている）。広告モジュールの一覧や詳細な分析結果については有償にて提供している。

76 APK ファイル（application package file）

77 Application programming interface の略。

78 第 10 回 WG 資料 3「利用者情報に関する取組」（タオソフトウェア株式会社）Tao Risk finder として提供。アプリケーション開発会社、アプリケーション販売会社、アプリケーション検査会社等を利用者として想定し分析結果を提供するとしている。

79 WG 第 1 回会合資料 7「スマートフォンセキュリティ時代！「アンドロイダー」の取り組み」（アンドロイダー株式会社）。

80 企業向けのモバイル端末管理（MDM）連携などビジネス向けにも利用可能となっている。

81 何らかの認証を付与する機関。例えば、青少年の利用に配慮したモバイルサイトの審査・認定及び運用監視業務を行う一般社団法人モバイルコンテンツ審査・運用監視機構（EMA）等も一般的には該当する。

目的として、透明性の確保の観点から充足すべき水準を示している[82]。

情報セキュリティ格付け研究会（株式会社アイ・エス・レーティング）はアプリケーション提供組織（企業・団体）からの依頼に基づき、「スマートフォン　プライバシー　イニシアティブ」を踏まえた組織単位のマネジメント等について第三者として確認することを予定しているとしている[83]。

（３）アプリケーション検証の現状に関するマッピング

・　プライバシーポリシーの検証及び利用者情報に関する技術検証の両方を行う者（右上領域）は現段階において多くはないが、アプリケーション提供サイト運営者、セキュリティベンダー、レビューサイト等の中に、技術検証とともに、プライバシーポリシーについて何らか確認や検証を検討している場合がある。

・　アプリケーション等に関する認定機関等が、プライバシーポリシーを作成していること等も視野に入れて認定を行う事例があり、この場合技術検証を伴わない認定となることが想定される（左上領域）。

・　また、アプリケーション等についてマルウェア検証[84]及び脆弱性検証[85]等を行う能力を有する者は多くおり、これらの者（主に左下領域）が既存の技術検証を行う際に併せて利用者情報に関する技術検証等を行うことも可能であると考えられる（右領域）。

---

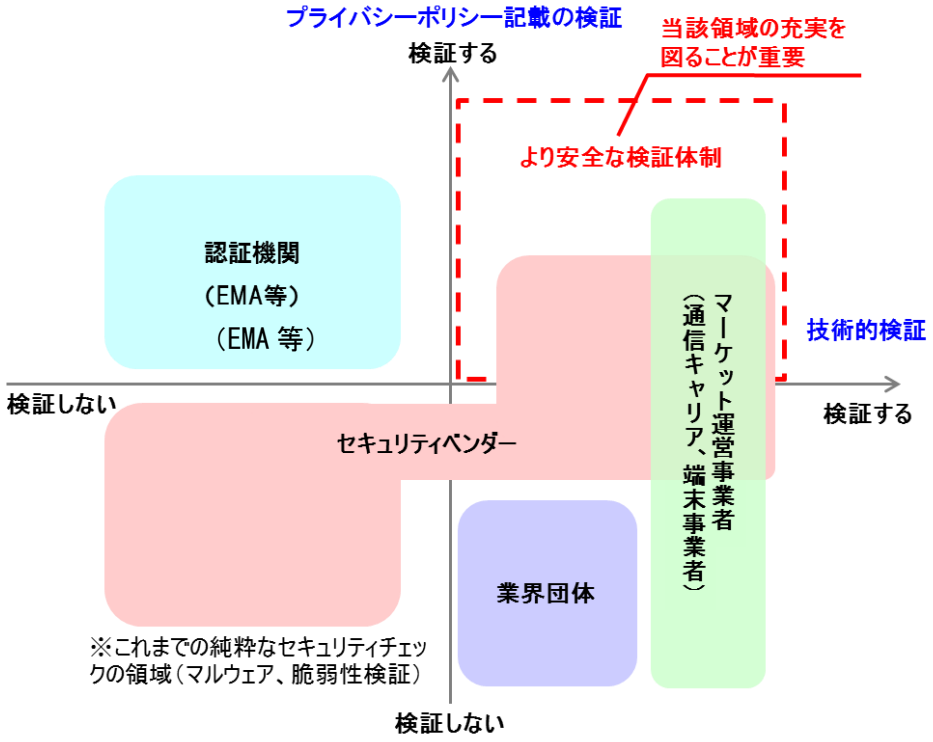
82 http://www.ema.or.jp/press/2013/0530_01.pdf　スマートフォンのアプリケーションを利用して利用者情報を取得する場合には、サイト運営事業者は、「スマートフォン　プライバシー　イニシアティブ」のスマートフォン利用者情報取扱指針に定められている 8 項目を利用者に周知しなければならないこととされている。その理由として、スマートフォンのアプリケーションを利用したユーザー情報の取得については、青少年を含むユーザーのプライバシー保護の観点から対応の必要があるものと判断したとしている。

83 WG 第 2 回会合 資料 6「スマートフォン・アプリケーション格付け準備状況」（株式会社アイ・エス・レーティング）。

84 マルウェア検証は、アプリケーションの動作や機能を解析・分析し、アプリケーションがマルウェアなのかどうか検証することであり、セキュリティベンダーが自らのセキュリティ対策ソフト等へのサービス等にも活用するため一般的に実施したり、アプリケーション提供サイト運営者が自ら運営するアプリケーション提供サイトに掲載するアプリケーション等について自らの技術で又はセキュリティベンダーの技術支援を受けるなどして実施する場合が多い。さらに、情報セキュリティ分野の業界団体や研究機関等もスマートフォンのアプリケーション等に関するマルウェア検証について実施している場合がある。

85 脆弱性検証については、一般社団法人日本スマートフォンセキュリティ協会は脆弱性対応を含むアンドロイドアプリケーションのセキュアコーディングガイドを発表。「Android アプリのセキュア設計・セキュアコーディングガイド」（2012 年 11 月 1 日版）http://www.jssec.org/dl/android_securecoding.pdf 等が公表されている。アプリケーションの動作や機能を解析・分析し、スマートフォンやアプリケーション内情報利用、他アプリケーションとの連携やサーバーとの通信等を行う際などに攻撃されやすい脆弱性がないかどうか等を検証する場合が多い。セキュリティベンダーやセキュリティ診断・調査事業者等により、アプリケーションの動作確認や脆弱性検証のサービスが提供されつつある。

図表１－３－６：利用者情報に関する検証の現状



出典：WG 第４回資料４　スマートフォンのアプリケーションの表示・検証に関する国内・海外動向
（株式会社　日本総合研究所）

３　利用者情報に関する第三者検証

（１） 検証主体

１（３）においても検討されているように、第三者検証の枠組みの検討においては、広く関係事業者や関係機関等を視野に入れ、事業者による自主的な取組や創意工夫を生かしつつ取り組むことが重要である。

第三者検証の主体としては、OS 提供事業者や移動体通信事業者及びゲーム等のコンテンツ配信事業者がアプリケーション提供サイトを運営し利用者との接点となるプラットフォームを提供する場合、大きな役割を果たすことが期待される。

また、セキュリティベンダー、レビューサイト等もアプリケーションについて技術的検証等を行った結果を利用者に提供する機能を既に有しており今後も大きな役割を果たすことが期待される。

さらに、プライバシー等に関する認証を行う機関において、スマートフォンのアプリケーション等について扱う場合には、「スマートフォン　プライバシー　イニシアティブ」を取り入れて認定・認証基準を考慮することは、スマートフォンの利用者情報に関して、業界横断的な取組を推進していく観点からも有効である。

アプリケーション等の事前審査、認定、格付けなど様々な民間サービスが提供され、優良事業者の差別化が図られるとともに、問題のあるアプリケーションについてはその旨が明らかにされることにより、利用者保護に寄与することが望ましい。

（２）検証の具体的方法と基準

１（２）にも記載されているように、アプリケーションごとの利用者情報に関する検証は、大きく分けて、「アプリケーション等のプライバシーポリシーの記載の検証」と「利用者情報の観点での技術的検証」の２つに分類される。

プライバシーポリシーの記載の検証と技術的な検証を並行して行うことにより、プライバシーポリシーへの記載内容に一致した形でアプリケーションが動作しているかどうかについて検証することが可能となると考えられる。

なお、アプリケーション提供者自体の検証として、アプリケーション提供者によるプライバシーポリシーの遵守や会社全体としてのコミットメント体制が確保されることについての検証を行うことも付加的方策として一定の有効性がある。

これら全てが一括して行われ結果として検証の基準を全て満たす場合には、そのアプリケーションは信頼性が相対的に最も高いということができる。また、その一部が行われ、その基準を満たす場合は、相対応の信頼性があるものということができる。

①　検証の具体的方法

ア　アプリケーションのプライバシーポリシーの記載の検証の基準（APP検証）

「スマートフォン　プライバシー　イニシアティブ」は、アプリケーションのプライバシーポリシー（APP）を作成し、利用者情報の取扱いの透明性の確保を図ることを目指しており、この APP の検証は中核的な位置づけとなる。

APP 検証にあっては①アプリケーション等のプライバシーポリシー作成・公表の有無の確認、②当該プライバシーポリシーの記載事項に係る確認が必要であると考えられる。

イ　利用者情報に関する技術的検証の基準

技術的検証は、利用者情報の外部送信の有無や APP との整合性を検証するため、アプリケーション等を技術的見地から専門的に検証・確認するものであり、①動的解析（アプリケーションを実際に動かし、その挙動を検査）、②静的解析（アプリケーションの構成ファイルを分析し問題を抽出、可能性（能力・権限）を検査）等の検証手法により、求められる検証内容に応じて実施[86]するものである。

なお、以下②の検証の基準において、「●」の事項はいわば必須項目であり、これらの項目が満たされている場合には、一定の信頼性あるアプリケーションということができる。一方、「・」の事項については推奨項目であり、これらが併せて満たされている場合は更に透明性や信頼性の高いアプリケーションであると考えられる。

86　使用する検証手法による検証可能範囲の違いを把握した上で、求められる検証内容に応じて検証を行う。

② 検証の基準

【アプリケーションのプライバシーポリシーの記載の検証の基準（APP 検証）】

① アプリケーションのプライバシーポリシー等の作成・公表の有無等
- ●アプリケーションのプライバシーポリシー（APP）を作成していること
- ●APP を利用者が容易に参照可能な場所に掲載しているか（ハイパーリンク記載含む）。アプリケーション内で容易に参照可能であること
  - ・概要版を作成・公表していること、APP と整合性があること（※推奨）

② アプリケーションのプライバシーポリシーの記載事項
- ●「スマートフォン　プライバシー　イニシアティブ」においてプライバシーポリシーに明示することとされている８つの事項（参考）について必要な内容を記載していること
  - （参考）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、②取得される情報の項目、③取得方法、④利用目的の特定・明示、⑤通知・公表又は同意取得の方法、利用者関与の方法、⑥外部送信・第三者提供・情報収集モジュールの有無、⑦問合せ窓口、⑧プライバシーポリシーの変更を行う場合の手続き
- ●取得される利用者情報とサービス内容、目的の関係が示していること。
- ●情報収集モジュールが含まれる場合、情報収集モジュールの名称、提供者等が記載しているか。また、取得される情報の項目、利用目的、第三者提供の有無が記載しているか（これら事項が明記された情報収集モジュールのプライバシーポリシー等へのリンク先等の提示を含む）
  - ・オプトアウトの方法についての記載があること（※推奨）

③ 同意取得に関する事項
- ●プライバシー性の高い情報（参考）を取得するアプリケーションの場合、個別に同意を取得していること
  - （参考）「スマートフォン　プライバシー　イニシアティブ」P64-65 において個別の情報を取得することについて同意を取得するとされている、電話帳、GPS の位置情報、通信履歴、アプリケーションの利用履歴、スマートフォンに保存された写真・動画等
- ●第三者提供を行う場合、あらかじめ本人の同意取得をすること

【利用者情報に関する技術的検証の基準】

①外部送信される利用者情報の有無等
- ●アプリケーションにより外部送信される利用者情報があるか否か
- ●外部送信される利用者情報の項目、内容
  - ※動的解析・静的解析を実施。静的解析のみに基づく場合には、実際には外部送信されない利用者情報も幅広く指摘し得ることに十分留意し検証する。
- ●外部送信される利用者情報の送信先

②アプリケーションのプライバシーポリシーとの整合性
- ●当該アプリケーションを通じて取得すると APP に記載される利用者情報の項目と、実際に外部送信される利用者情報の項目が合致していること
- ●外部送信される利用者情報の利用目的が明示されていること
- ●実際のアプリケーションの内容と提供サービス・目的に一定の整合性があること
- ●情報収集モジュールが組み込まれている場合、組込まれている情報収集モジュールの名前、提供者、送信情報等が合致していること

※　検証後の対応

検証の結果はあくまで検証を行った時点で基準に合致しているかどうかを示すものであるので、検証後にアプリケーションのバージョンアップ等に伴い利用者情報の取扱いを変更する場合は、APP の変更の履歴を残すとともに利用者が容易に閲覧できるようにすることで検証結果との対応関係を確認できるようにすることが望ましい[87]。また、新たにプライバシー性の高い情報取得や第三者提供をする場合の同意取得等が行われることが必要である。

③　アプリケーション提供体制の確認の基準

アプリケーション提供事業者が利用者情報を取得した後も、プライバシーポリシーに沿って適切に当該利用者情報を管理・運用しているかについての実態と、管理・運用の体制について確認することは、付加的な方策として一定の有用性を持つと考えられる。

① アプリケーション提供者の所在確認・信用度確認
・アプリケーション提供者の連絡先等が把握できること
・アプリケーション提供者の提供実績など

② 指針を踏まえた利用者情報の取扱い体制
・アプリケーションのプライバシーポリシーを策定・公表する体制があること
・事実に即し APP を策定し、これを遵守する体制があること
・他の検証や認証などにおいて、上記②が確認されていること
※ 他の認証機関（EMA 等）において、確認されている場合には、その結果を援用することが可能である。

87 なお、配信型のアプリケーション提供サイトなどにおいて、常に新しいバージョンのアプリケーションとそれに合致したアプリケーションのプライバシーポリシーが掲載される場合には、当該バージョンについての検証結果だけを掲載する場合も想定される。

４　今後の具体的措置

（１）アプリケーションのプライバシーポリシーの策定推進と様式の共通化

現段階では、第２章において記述した通り、アプリケーションのプライバシーポリシーの普及率が必ずしも高くないことから、各業界はスマートフォンの利用者情報等に関する連絡協議会（SPSC）の活動等を参考にしつつ、まずはアプリケーションのプライバシーポリシーの策定を強力に推進していく必要がある。

その際、記載様式の共通性が高くないため、利用者にとって把握しにくく読み解く手間がかかることも指摘されており[88]、プライバシーポリシーについて記載様式や記載場所を共通化することが、今後の検証の効率化と普及のために重要であると考えられる[89]。プライバシーポリシーの記載様式のフォーマットなど一定の基準が定まると、マーケット運営事業者やセキュリティベンダーなどの検証者による検証も容易になる。

アプリケーションの審査や配信に関わるアプリケーション提供サイト運営事業者や OS 提供事業者等がプライバシーポリシーの記載（プライバシーポリシーの記載形式・記載方法・記載場所についての一定の基準）について示すことが有用である[90]。検証を確実かつ効率的に実施するのに適した実装[91]が可能となるように、あらかじめ技術的なツールを配布し普及させることは検証を効率化し業界全体の取組の推進につながるため有用である[92]。

APP の記載項目の共通的な記載様式に合致しているアプリケーションについては、簡便な APP に関する第三者検証が受けられることとなる場合、これら様式を導入するインセンティブも働くと期待されるものであり、利用者にとっても、より読みやすく分かりやすい APP となる可能性が期待される。

（２）第三者検証の実施主体の公表・リスト化

第三者検証を実施する主体について利用者及びアプリケーション提供者に分かりやすく把握可能とするため、第三者検証を行っている者は自ら名称、連絡先、実施している検証内容・検証基準について、公表を推進する。また、業界団体・関係機関等は第三者検証を行っている者についての情報をリストとして取りまと

---

88 WG 第 2 回会合資料 5「JSSEC アプリ解析技術タスクフォース活動のご紹介」（JSSEC）。プライバシーポリシーについて、記載様式や記載場所が標準化されることが検証の効率化のために重要であり必要であるとしている。

89 アプリケーション等のプライバシーポリシーの検証については、現在試行的な検討がいくつか行われている。例えば、一般社団法人日本スマートフォンセキュリティ協会技術部会アプリケーション解析技術タスクフォースにおいて、アプリケーションのプライバシーポリシーの読み解きの試行が行われた。（WG 第 2 回会合資料 5「JSSEC アプリ解析技術タスクフォース活動のご紹介」（JSSEC））

90 第 10 回 WG 資料 4「スマートフォンの安心・安全な利用環境整備のためのエコシステムについての考察」（日本総合研究所 東博暢氏）

91 共通の名称のファイルに共通の書式（共通のタグを持つ XML 等）で記載する方法等が想定される。

92 WG 第 10 回資料 1「au Market におけるプライバシー保護の取り組み」（KDDI 研究所　竹森敬祐氏）KDDI において、「スマートフォン利用者情報取扱指針」の 8 項目に対応したアプリケーションのプライバシーポリシーを共通の書式（XML 文書）でアプリケーション提供者が容易に作成できるように、SDK へのプラグイン型プライバシーポリシー作成支援ツールを開発し、アプリケーション提供者へ提供予定としている。

めた上で公表する。

（３）第三者検証の結果の表示の検討

消費者の信頼を得るために、第三者検証のシステム又は個別の結果について分かりやすく「「スマートフォン　プライバシー　イニシアティブ」準拠（以下「SPI準拠」と記載。）」のような表示を用いる場合には、一定の要求事項の充足を求める[93]ことが考えられる。

一方、このようなSPI準拠マークについては、利用者がこれを参考にしてアプリケーションをダウンロードする点から大変有効な手段であるが、一方、当該マークを導入する際には、改ざんのおそれや、不適切なものまでSPI準拠マークを付してしまうおそれなども指摘されることから、どのような形であれば実効性がありかつ安心安全なSPI準拠マークを発行・運用可能であるかも含め、引き続き検討を行うことが望ましい。

（４）各アプリケーション提供サイト運営事業者等の連絡通報窓口の連携

利用者情報の点で問題があるアプリケーションの判断基準を明らかにしていくために、各アプリケーション提供サイト運営事業者やセキュリティベンダー等の連絡通報窓口間における連携を図り、情報共有や対応方法の共有等を推進するとともに、判断基準について、関係事業者間で議論をした上で検討することが望ましい。

また、危険性のあるアプリケーション、情報漏えいのリスクのあるアプリケーション及びその事例について、データベース化する。

さらに、データベースを活用し、問題あるアプリケーションを発見できるアプリケーション、問題あるアプリケーションリスト公開なども進められることが望ましい。また、利用者に緊急で伝達すべき内容のものがあった際の伝達方法を検討する。

（５）情報収集モジュールのリスト化・共有

アプリケーション提供者は、アプリケーションのプライバシーポリシーにおける記載において、アプリケーション自体として取得・利用する情報とともに、情報収集モジュールにより取得･利用する情報について適切に記載する必要がある。また、情報収集モジュール提供者も適切な説明が期待される。

一方、アプリケーション提供者側が情報収集モジュールについて十分に理解していないため、正確に記載できない場合もあり、利用者にとっても情報収集モジュールのプライバシーポリシーが分かりにくい場合も多く見られる。

各情報収集モジュールについて、アプリケーション提供事業者や第三者検証を

93　第10回WG資料5「SPIと第三者認証の在り方」（森亮二構成員）

行う主体を支援する観点から、業界関係者向けに情報収集モジュールについての共通的なデータベース（情報収集モジュール提供会社、プライバシーポリシーの記載の有無、取得される情報の種類等）や業界関係者向けの一覧表・カタログの作成などを検討することが望ましい（また危険な情報収集モジュールが今後出てきた場合には、そのリスク情報共有を行うことも望ましい）[94]。

（６）利用者支援・検証支援のためのアプリケーションやウェブサイト等の検討

一般利用者や検証を行う者が簡易にアプリケーションについての検証結果を確認できるよう支援する観点から、アプリケーションの検証結果について簡単に確認できるアプリケーションやウェブサイト等について検討を進める。

その際、既に利用者がスマートフォンにインストール済みのアプリケーションについても確認し、問題が発見された場合アプリケーションのアンインストールを含めた対応ができるように支援できることが望ましい。

（７）定期的なアプリケーション調査の実施とフォローアップ

アプリケーション調査を実施する上での基準を検討・策定し、その基準を踏まえ少なくとも人気上位 100－200 程度のアプリケーション(及びランダム抽出したアプリケーション等）について、定期的に、アプリケーションのプライバシーポリシーの策定・公表状況、利用者情報の技術的検証等について行い、取りまとめた調査結果について公表する。

調査結果を踏まえ継続的にフォローアップを行うとともに、その結果を踏まえ必要がある場合には、取るべき追加的措置等について検討を行う。

（８）共通的事項の実施体制の確保

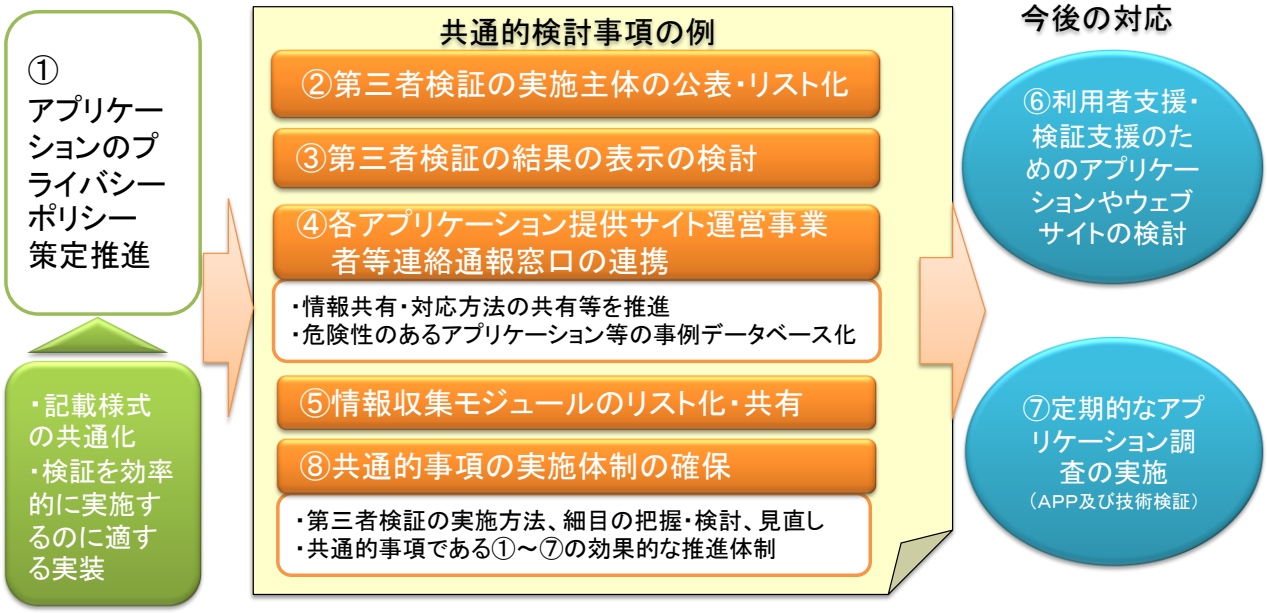
「スマートフォン　プライバシー　イニシアティブ」に基づく取組の実効性を確保していくために、第三者検証の仕組みが重要であり、共通的事項について実施できる体制について検討する必要がある。第三者検証の実施方法や実施細目の在り方について共通的に把握・検討すること、必要に応じ基準の見直しについて検討すること、また第三者検証の結果の表示方法の検討、アプリケーションや事業者の登録[95]、情報収集モジュールのリスト化、連絡通報窓口間の連携など前出の課題のうち共通的事項について関係事業者や業界団体の協力を得つつ効果的かつ効率的に推進されるような体制を検討する。

---

94 第 10 回 WG 資料 4「スマートフォンの安心・安全な利用環境整備のためのエコシステムについての考察」（日本総合研究所 東博暢氏）JSSEC においても情報収集モジュールに関する検討に着手している。

95 アプリケーション（APK ファイル等）及びアプリケーション提供者の情報について、アプリケーション提供者が了承し特定の場所に登録し場合、検証・審査機関間で情報共有を行うことも有用であるとの指摘がある。

図表１－３－７：共通的検討事項の例



これら事項について対応を進め諸問題研究会の下にフォローアップのためのＷＧ又はＴＦを維持（設置）し、今後の進捗状況について継続的に確認し、当面の間半年に１回程度報告を行うこととする。

その際、例えば第三者提供に関し提供先についても個別に記載すべきである等、個人情報・パーソナルデータ保護に係る全体的なルールの見直し・作成に関する議論において、「スマートフォン　プライバシー　イニシアティブ」におけるアプリケーションのプライバシーポリシーの記載事項にも影響を与え得るような消費者保護強化の議論が強まった場合には、諸外国の状況も踏まえ、第三者検証の基準等の見直しも視野に入れた柔軟な対応を図るべきである。

第４章　利用者及びアプリケーション提供者のリテラシーの向上

１　基本的考え方

急速に普及が進むスマートフォンは、青少年から高齢者まで、誰もが安心して使いやすいものであるべきである。サービスについて知見を有する関係事業者等が自らの責任として、「スマートフォン　プライバシー　イニシアティブ」第６章等の内容も踏まえつつ、利用者への情報提供・周知啓発を推進し、利用者のリテラシー向上を図っていくことが重要である。

本提言を踏まえ、今後アプリケーションのプライバシーポリシーの策定、スマートフォン画面を考慮した表示（概要版）、プライバシー性の高い情報取得時におけるポップアップによる同意取得等の導入の推進が期待される、更には第三者検証についての実施が進むと期待されることから、利用者に対してこれらについて分かりやすく説明し認知度と理解を高めることが望ましい。

また、さらに、アプリケーション提供サイト運営事業者等から、アプリケーション提供者に対する周知啓発を進めることにより、適正なアプリケーションのプライバシーポリシーの策定や利用者情報取得時の同意取得などが推進され、業界全体としての取組が進展することを目指すこととする。

２　一般利用者向けの情報提供・周知啓発

（１）情報提供・周知啓発の推進

「スマートフォン　プライバシー　イニシアティブ」第６章にあるように、引き続き、①スマートフォンと従来型携帯電話の違い、②利用者情報の取扱いの注意点、③情報セキュリティ対策、④青少年・高齢者に必要な情報について利用者に情報提供し、周知啓発を進めることとする[96]。

様々なリテラシーの利用者が増えるとともに、利用者のリテラシーに応じた情報提供を行うことも重要となっている。①端末・サービス開発時の取組（例：青少年・高齢者向けスマートフォンの提供等）や②サービス利用時の取組（例：自主セミナーの開催）などについても引き続き推進していくことも重要である。

例えば、NTT ドコモの場合、青少年、高齢者向けのスマートフォンを提供（スマートフォン for ジュニア/らくらくスマートフォン）を発売するとともに、スマートフォンの設定・操作等に関する問い合わせを遠隔でサポートするサービスを開始（スマートフォンあんしん遠隔サポート）、また、「ケータイ安全教室」を実施し（2013 年３月末に受講者数が 500 万人を突破）しているとしている[97]。ソフトバンクモバイルの場合にも、シンプルスマホなどを販売するとともに、青少年向けにス

96 「スマートフォン　プライバシー　イニシアティブ」第 6 章

97 第 7 回 WG 資料 3（NTT ドコモ）

マホ安心サービスを提供している。情報モラル授業プログラムにおいてスマートフォンやアプリケーションについて考える啓発に努めているとしている[98]。

また、各事業者において実施されている様々な周知啓発資料について取りまとめ、スマートフォンの利用者情報等に関する連絡協議会（SPSC）等の業界横断的なマルチステークホルダーが集う場においてワンストップで分かりやすく情報提供や発信を行っていくことも有用であると考えられる。

（２）「スマートフォン　プライバシー　イニシアティブⅡ」を踏まえた周知啓発

最近の事例を含めて採り入れ、分かりやすく「スマートフォン　プライバシーガイド」を改定しており、パンフレットやPDF版[99]も作成していることから、今後このガイドについて幅広く周知し認知度を高めることが有用である。

また、今後アプリケーションのプライバシーポリシーの策定、スマートフォン画面を考慮した表示（概要版）、プライバシー性の高い情報取得時におけるポップアップによる同意取得等の導入の推進が期待される利用者に対してこれらについて分かりやすく説明し認知度と理解を高めることが望ましい。

また、第三者検証についての実施が進むと期待されることから、利用者が適正なAPPの下、適正な運用がなされているアプリケーションを客観的に確認し、アプリケーションを利用するかどうかの有効な判断基準等とすることができるように、第三者検証の実施内容と理解・活用の仕方について関係事業者や業界団体等が分かりやすい周知啓発を行うことが期待される。

98 WG第10回資料2

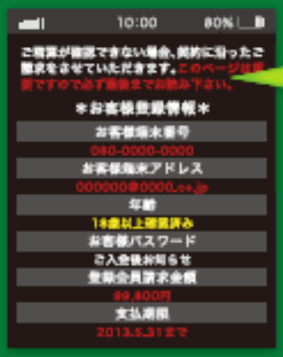
99「スマートフォン　プライバシー　ガイド」のパンフレット http://www.soumu.go.jp/main_content/000227662.pdf

図表１－４－１：「スマートフォン　プライバシー　ガイド」のパンフレット

最近の注意!!

1 不正アプリの増加と多様化

- スマートフォンの急速な普及に伴い、不正アプリも増加、多様化しています。
- 動画を再生するアプリに見せかけ、インストールするとメールアドレス・電話番号等の個人情報を取得し、**架空の料金請求画面を出す、金銭搾取を目的としたワンクリックウェア**が報告されています。
- スマホの機能改善ツールを装い、**電話帳情報等の詐取等を目的としたアプリ**も増加しています。
- 人気ゲームを動画で紹介するとしたアプリが利用者の電話帳情報を外部に送信していた事例もありました。



●ワンクリックウェアをインストールしてしまった場合、慌てず端末から削除しましょう。

●身に覚えのない請求の場合、決して支払わないようにしましょう。

●機能改善をうたうアプリをインストールすると、電話帳情報が外部へ送信される可能性があります。

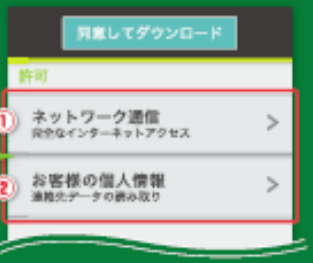
2 不審なメールやSNSの投稿等に記載されたURLからアプリをダウンロードしないように注意しましょう

- 機能改善ツールを装ったアプリなどには、利用者に対して送られた不審なメールやSNSの投稿を通じて、**不正アプリ配布サイトに誘導**するものが多くあります。
- 不審なメールやSNSの投稿で紹介されたURLを安易にクリックしてアプリをダウンロードしないように注意しましょう。

3 電話帳情報を外部に送信し得る利用許諾(パーミッション)を求めるアプリには注意しましょう

- アプリの提供する機能には明らかに不要であるにもかかわらず、**電話帳情報を外部に送信し得るパーミッション**を求めるアプリがあった場合は十分注意しましょう。

①ネットワーク通信-完全なインターネットアクセス
②個人情報-連絡先データの読み取り
上記2つのパーミッションを取得するアプリは電話帳に記録された情報(氏名、電話番号、メールアドレス、住所等)を外部に送信する可能性があります。



３　アプリケーション提供者向けの周知啓発

関係事業者の中のアプリケーション提供者が、適正な対応を行うことができることを可能とするため、アプリケーション提供サイト、OS 提供事業者、業界団体、研究機関等の関係事業者等はアプリケーション提供者への情報発信・周知啓発を充実することが期待される。

（１）アプリケーション提供サイト運営事業者等

「スマートフォン　プライバシー　イニシアティブ」においてアプリケーション提供サイト運営者側からアプリケーション提供者等に対する情報提供を行うことが、指針の実効性を上げるために重要であるとされている。

アプリケーション提供サイト運営事業者からは、アプリケーション提供サイト掲載ガイドライン等を通じて、アプリケーションのプライバシーポリシーの作成を促すことが重要である。

さらに、適切なベストプラクティスを共有するとともに、アプリケーション提供者への研修や説明会などにおける啓発活動を通じて、周知を行うことが重要である。

（２）業界団体等による周知啓発

業界団体等において、アプリケーション提供者向けのガイドライン等を作成している場合、そのガイドラインを分かり易くアプリケーション提供者に対して周知啓発していくことが重要である。

また、スマートフォンの利用者情報等に関する連絡協議会（SPSC）等の業界横断的なマルチステークホルダーが集う場において、各業界団体の作成しているガイドラインやアプリケーション提供サイトの掲載ガイドライン等を含め、ワンストップで分かり易く情報提供や発信を行っていくことも有用であると考えられる。

第５章　国際協調に向けて

世界的にスマートフォンの普及が進展しており、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が、諸外国においても政策課題となっている。

「スマートフォン　プライバシー　イニシアティブ」において提言されているように、プラットフォーム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が多いことから、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取組を推進する必要がある。

１　米国

（１）　インターネットエコノミーに関する日米政策協力対話

インターネットの経済的側面に焦点を当てた政策全般について、総務省情報通信国際戦略局長と米国国務省大使の間で定期的に実施しているインターネットエコノミーに関する日米政策協力対話[100]（第４回）が 2012 年（平成 24 年）10 月米国ワシントンD.C.で開催され、日本側からは「スマートフォン　プライバシー　イニシアティブ」について総務省から紹介を行い、米国側からは商務省・国家電気通信情報庁（NTIA[101]）よりホワイトハウスの政策大綱を踏まえ、モバイルアプリケーションの透明性向上のための行動規範について議論が行われていることについて紹介があった。

政府間共同記者発表において、消費者のデータ保護については、「双方は、スマートフォンの利用者のプライバシーに関するスマートフォンのアプリケーションの透明性の重要性と、リテラシー向上について議論を行った。双方は、安心安全な ICT の利活用の環境を確保し、移動体通信市場の継続的な発展を確保するため、引き続き、消費者のデータ保護に関するベストプラクティスとアップデートを共有していくことで一致した。」と発表されている。

[100] この対話は、日米首脳会談(2012 年（平成 24 年）4 月 30 日)で、日米関係の強化・拡大を目指す「日米協力イニシアティブ」の一環として位置づけられている。第 4 回会合には、米側からは、国務省、連邦政府 CIO、商務省（NTIA)、国土安全保障省、連邦通信委員会（FCC: Federal Communications Commission)、連邦取引委員会（FTC)等が参加。

[101] NTIA; National Telecommunications and Information Administration

（２） 米国内における検討の動き

① 商務省 NTIA によるマルチステークホルダー会合

ホワイトハウスの政策大綱(消費者プライバシー権利章典等)を踏まえ、NTIA が企業、業界団体、消費者団体等が一同に出席するマルチステークホルダー会合を開催している。パブリックコメントの結果を踏まえ、2012 年（平成 24 年）７月より「モバイルアプリケーションの透明性」に関する行動規範の策定に向けた議論を開始している。

2013 年（平成 25 年）７月までに 16 回の会合が開催され、アプリケーション開発者協会（ADA[102]）等が起草した行動規範の討議ドラフトに基づき簡略な通知への記載事項等に関する議論が行われ[103]、７月 25 日に開催された第 16 回会合で行動規範ドラフトの編集作業はひとまず終了し、今後はその行動規範に従うアプリが消費者にもたらす効果をテストする局面へ移行するとしている。

なお、政策大綱において、連邦取引委員会（FTC）は企業が遵守を宣言した行動規範に基づき執行が可能と言及されているが、今後、これら権利の法制化についても検討することとしている。

② 連邦取引委員会（FTC）

ア スタッフレポート：モバイル・プライバシー・ディスクロージャーズ：透明性の確保による信頼の構築

2013 年（平成 25 年）２月、FTC スタッフレポートが公表され、同レポートに示す提言において、モバイルにおけるプライバシーの説明をきちんと行い、透明性を確保していくことが求められている[104]。具体的には、アプリケーション提供者、アプリケーション提供者の業界団体、プラットフォーム事業者（OS 事業者）、広告ネットワーク事業者等の各関係主体が果たすべき役割が示されている。

アプリケーション提供者に対して、プライバシーポリシーを作成しアプリケーション提供サイトにおいて示すこと、位置情報、電話帳、写真、カレンダー、録画等のセンシティブあるいはセンシティブとなり得る情報を取得する場合、速やかに利用者に知らせ同意を取得することが提言されている。さらに、アプリケーション提供者の業界団体に標準化されたアプリケーションのプライバシーポリシーの策定を促進すること、簡潔な情報提供の方法を開

102 ADA: Application Developers Alliance

103 ドラフトに対しカリフォルニア州司法長官室等からコメントが寄せられている。また、4 月 4 日会合において、FTC スタッフからスタッフレベルの非公式コメントとしていくつかの点で懸念が示された。

104 FTC が引用する調査結果によれば、利用者情報の取扱いに不安があるためアプリケーションを削除あるいはアプリケーションのインストールをやめた事例が 57%あるとされる。Pew Internet & American Life Project, Privacy and Data Management on Mobile Devices（2012 年（平成 24 年）9 月 5 日）。http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

発することが提言されている。また、プラットフォーム事業者に対して、アプリケーションがアクセスする情報の種類をワンストップで把握できるダッシュボード、利用者情報の送信を示すアイコンの開発が提言されている。また、アドネットワーク等によるトラッキングの可否を選択できるようモバイル向けの「Do Not Track」の仕組みを検討することが提言されている。

FTC は同提言が上記①の米国商務省 NTIA によるマルチステークホルダー会合の議論への有益なインプットとなることを期待するとしている。

イ　スタッフレポート：子供向けのモバイルアプリケーション

2012 年（平成 24 年）12 月、FTC は「子供向けのモバイルアプリケーション：情報公開水準は未だ合格水準にない」を２回目のスタッフレポートとして発表した。この中で、多くのアプリケーションがどのような情報をどのような目的のために取得し誰がこの情報を共有するのか十分な説明を行っていないこと、機器の ID や位置情報、電話番号などが両親に知らされないまま第三者によって取得されている場合があること等を問題点として指摘しており、2012 年２月のスタッフレポート時に比べ状況が改善されたとは言えないとしている[105]。

FTC はモバイルアプリケーションの関係事業者（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者、広告配信事業者等）に対して、保護者が子供のためにアプリケーションをダウンロードするか判断をするために必要な情報が確実に提供することを推進することを求めている。また、FTC 報告書（2012 年（平成 24 年）３月）を踏まえたプライバシー・バイ・デザイン、シンプルな選択肢の提供、透明性の増進を促している。また、FTC は、保護者を対象としたリテラシー向上に向けた取組を行うこととしている[106]。

また、FTC はモバイルアプリケーションの関係事業者による、児童のオンラインプライバシー保護法（COPPA）の遵守状況について調査を開始するとしており、「子供向けのモバイルアプリケーション」に係る第３回目の調査を実施予定としている。

ウ　FTC 児童のオンラインプライバシー保護法（COPPA[107]）規則改正

---

105 子供向けカテゴリーのアプリケーションを Android OS 又は iOS のそれぞれ 200 ずつ調査した結果、約 60%が契約者・端末固有 ID、位置情報、電話番号等をアプリケーション提供者あるいはアドネットワーク等に送信しており、約 20%のアプリケーションのみが十分な説明を行っていたとしている。

106 2012 年 12 月の子供のモバイルアプリケーションに関するスタッフレポートを踏まえ、2013 年 3 月、FTC は保護者等がどの子供向けのモバイルアプリケーションをダウンロードするか意思決定をするために役立つ図解のツールとして、「子供のアプリについて知っておくために（”Keeping Up With Kids’ Apps”）」を公表。
http://www.ftc.gov/opa/2013/03/kidsapps.shtm

107 COPPA: Children’s Online Privacy Protection Act

FTC はオンライン上における児童（13 歳未満）のプライバシー保護の強化をめざして 2010 年（平成 22 年）より児童オンラインプライバシー保護法規則のレビューを開始し、2012 年（平成 24 年）12 月に児童オンラインプライバシー保護法（COPPA）規則の改正案を採択、2013 年（平成 25 年）７月に発効している。保護者への通知及び同意なしに収集できない「個人情報」として、「位置情報、子供の顔や声が含まれる写真、ビデオ、オーディオ」も含める案となっている。また、IP アドレスや携帯端末 ID など、異なるウェブサイトやオンラインサービスをまたいで利用者の識別が可能な ID についても COPPA の対象範囲として拡大、データセキュリティ保護・保存・削除についても対応を求めている。さらに、FTC による自主規制セーフハーバープログラムに対する FTC の監督権限が強化されている。

③　カリフォルニア州の司法長官「モバイル端末におけるプライバシーに関する提言」

2013 年（平成 25 年）１月、カリフォルニア州の司法長官が「モバイル端末におけるプライバシーに関する提言」を公表した。同提言において、モバイルアプリケーションにおけるプライバシー保護に向けて、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者、モバイル広告ネットワーク事業者、移動体通信事業者の各関係主体が果たすべき役割が示されている。

アプリケーション提供者に対しては、アプリケーションの基本機能に不要な個人情報の収集を回避又は制限すること、明確で正確なプライバシーポリシーを作成し、利用者に明示的にアクセス可能とすること、利用者の注意を引く通知方法を用いること等を提言している。また、アプリケーション提供サイト運営事業者には、アプリケーション提供サイトからアプリケーションのプライバシーポリシーへアクセスできるようにすること、利用者へモバイルプライバシーについて周知啓発することとされた。さらに、モバイル広告ネットワークに対しては、アドネットワークに関するプライバシーポリシーを作成しアプリケーション提供者に提供すること、アプリケーション独自の一時的 ID を使うこと等が提言された。移動体通信事業者に対しては、モバイルプライバシーと児童のプライバシーについて利用者に周知啓発を行うことが提言された。

２　欧州

（１）　日 EU・ICT 政策対話

総務省と欧州委員会（通信ネットワーク・コンテンツ・技術総局）との間で、ICT 政策全般について、定期的に実施している政策対話である日 EU・ICT 政策対話（第

19 回）が 2012 年（平成 24 年）11 月東京において開催され、日本側からは「スマートフォン　プライバシー　イニシアティブ」について紹介を行い、EU 側からは e プライバシー指令に基づく取組等について紹介が行われた。

2012 年（平成 24 年）11 月 15 日総務省報道発表資料[108]において、青少年のインターネット利用環境整備、ブロードバンド普及促進、スマートフォンにおける利用者情報の取扱い等 ICT サービスにおける利用者情報・プライバシーについて、日 EU 双方の政策動向やベストプラクティスの共有など、情報交換・意見交換が行われ、これらの議題についても、引き続き情報交換・意見交換を行うこととしていると発表されている。

（２）　二国間の政策協議

①　日仏 ICT 政策協議

総務省とフランスにおける情報通信政策担当省庁（現在は生産復興省）との間で、ICT 政策全般について、定期的に実施している政策対話である日仏 ICT 政策協議（第 16 回）[109]が 2013 年（平成 25 年）２月パリにおいて開催され、日本側からは「スマートフォン　プライバシー　イニシアティブ」について紹介を行い、仏側（CNIL[110]）からは EU 個人データ保護規則案に関する動向等について紹介があった。

②　日フィンランド ICT 政策協議

総務省とフィンランド運輸通信省との間で、ICT 政策全般について、定期的に実施している政策対話である日フィンランド ICT 政策協議（第 13 回）が 2013 年（平成 25 年）６月東京において開催され、日本側からは「スマートフォン　プライバシー　イニシアティブ」について紹介を行い、フィンランド側からは e プライバシー指令等を含むプライバシー保護に係る動向等について紹介があった。

（３）　EU 域内における検討の動き

EU における個人データ保護に関する基本法令である 1995 年個人データ保護指令を改正するため、2012 年（平成 24 年）1 月に欧州委員会により個人データ保護規則案が発表され、欧州議会の主管委員会である市民の自由委員会（LIBE[111]）は、同

---

[108] 2012 年 11 月 15 日総務省報道発表資料「日 EU・ICT 政策対話（第 19 回）及び日 EU インターネット・セキュリティフォーラムの結果」。　http://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000041.html

[109] 仏側からは、生産復興省競争力・産業・サービス総局、ARCEP（電子通信・郵便規制機関）、CNIL（情報処理及び自由に関する国家委員会）ほかが参加。

[110] CNIL: Commission nationale de l'informatique et des libertés

[111] LIBE: Civil Liberties, Justice and Home Affairs

原案に対する改正案について議論を実施している。また、2009 年（平成 21 年）に改正されたｅプライバシー指令に基づき、クッキーの利用や位置情報の利用に当たっては、原則として、内容を明示しオプトインによる利用者同意を求めることとされている。

スマートフォン等に焦点を当てた動きとしては、民間レベルでは 2012 年（平成 24 年）１月に世界的な携帯通信事業者の業界団体 GSM 協会（GSMA）が携帯端末向けのプライバシー原則、プライバシーデザインのガイドラインを発表している[112]。

また、2013 年（平成 25 年）2 月、EU の第 29 条作業部会[113]が、スマートフォン等のアプリケーションに関する意見書[114]を公表している。スマートフォンには電話帳や位置情報、写真やビデオなど様々な利用者情報が存在しており利用者はこれらの情報をコントロールできる必要があるが、スマートフォンアプリケーションが急速に普及する中で、利用者への透明性のある説明や有効な同意の欠如、不十分なセキュリティ措置、利用目的や流通範囲の限定が講じられないままの個人データ取得等を問題点として指摘している。その上で、個人データ保護指令やｅプライバシー指令に基づく義務及び推奨事項について、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者、OS・端末開発者及び第三者利用者（サードパーティー）等の関係事業者ごとに取りまとめている。例えば、アプリケーション提供者については、利用者情報の取扱いについて必要な情報（収集者、内容、目的、第三者提供の有無、利用者の権利等）についてプライバシーポリシーを提示すること、アプリケーションが情報収集等を開始する前に情報の種類（注）ごとに有効な同意を求めること、必要以上の情報を収集しないこと、利用目的を明示し個別の同意なく変更しないこと、子供向けアプリケーションを厳格に取り扱う[115]こと等が義務として記載されている。

（注）位置情報、契約者・端末固有 ID、個人情報、電話帳、クレジットカード番号、通話・SMS・電子メール、閲覧履歴等

３　韓国における検討の動き

韓国においても、スマートフォンにおける個人情報の流出が問題となっていることを背景として、2012 年（平成 24 年）３月に韓国情報保護振興院（KISA[116]）は「アプ

112 「スマートフォン　プライバシー　イニシアティブ」39 ページ　第 3 章

113 第 29 条作業部会は、現行 1995 年データ保護指令第 29 条に基づいて設置された諮問機関であり、欧州委員会（司法総局）、加盟国規制機関等から構成され、同指令に関する法的解釈等を行っている。

114 “Opinion 02/2013 on apps on smart devices” Article 29 Data Protection Working Party（2013 年 2 月 27 日採択）http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

115 収集情報の最小化、ターゲティング広告への利用自粛等

116 韓国語は、인터넷진흥원。KISA は、Korea Internet and Security Agency の略。

リケーション開発者向けプライバシーガイド[117]」を公表した。独自のアプリケーション提供サイト、アプリケーション開発者支援ホームページウェブサイト、アプリケーション開発者センター等を運営する国内通信事業者を通じ、同ガイドの周知・啓発が行われている。このガイドの中で、アプリケーション提供者は、個人情報の収集を最小限に抑えるべきであり、必須項目以外利用者が個人情報を提供しないことを理由にサービスの利用を禁止してはならないとされている。また、個人情報の収集・利用に関して同意取得、位置情報の収集・利用・提供に関して同意取得、センシティブな情報の収集の原則禁止、第三者提供の制限、個人情報の収集目的範囲内の利用の確保などが示されている。

また､KISA はスマートフォンの中でモニター機能を果たすようなアプリケーション（SS チェッカー）を開発・公開するほか、放送通信委員会（KCC[118]）の「安全な位置情報利用環境造成事業」の一環として、スマートフォン用個人情報保護マーク（プライバシーマーク）を開発すると発表している(2012 年６月)。加えて、パイロットプロジェクトの実施等が予定されている[119]。

なお､「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、韓国放送通信審議委員会(KCSC[120])が主催する「2012 国際ラウンドテーブル」(2012 年（平成 24 年）８月）において、総務省から紹介を行っている。

４　国際連携の推進に向けて

プライバシー保護に係る法規制は、各国・各地域により様々な違いもあるものの、スマートフォンの利用者情報の取扱いに関する検討については、主要先進国において透明性を高める方向で検討や取組が進んでおり、方向性はほぼ合致している。

今後も我が国から「スマートフォン　プライバシー　イニシアティブ」及びそれを踏まえた取組などの状況について、積極的に二か国の枠組みに対して説明を行うことが有用である。更に、プライバシー問題等についてこれまでも議論されている経済協力開発機構（OECD）の情報・コンピューター・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､「スマートフォン　プライバシー　イニシアティブ」について WPISP の新保副議長より 2013 年（平成 25 年）４月に説明を行ったところである。

---

117 本ガイドは、個人情報保護の観点から、情報通信網法（情報通信網利用促進及び情報保護に関する法律）及び位置情報の保護及び利用に関する法律（位置情報保護法）等の適用関係を明確化しアプリケーション提供者が留意すべき事項を示すものである。

118 韓国語は、방송통신위원회。KCC は、Korea Communications Commission の略。

119 「스마트폰 앱 `개인정보보호 마크` 나온다」(「スマートフォンのアプリケーションの『個人情報保護マーク』が登場」)（etnews.com）（韓国語）(2012 年（平成 24 年）6 月 27 日)。
http://www.etnews.com/news/computing/security/2606734_1477.html

120 韓国語は、방송통신심의위원회。KCSC は、Korea Communications Standards Commission の略。

今後も、多国間連携の場として、OECD、国際電気通信連合（ITU）やアジア太平洋電気通信連合（APT)、アジア太平洋国際協力（APEC)、東南アジア諸国連合（ASEAN）などの国際的機関や地域連合の場においても、「スマートフォン　プライバシー　イニシアティブ」やそれを踏まえた我が国における取組を説明し、多国間連携を進め、これらの枠組みに参加する諸国における検討や取組等とも連携しつつ対応を進めていくことが期待される。

（参　考　資　料）

業界団体等による自主ガイドライン作成の状況

一般社団法人モバイル・コンテンツ・フォーラムは平成24年11月13日、アプリケーション提供者にとって喫緊の課題であるアプリケーション毎のプライバシーポリシーの作成や掲出方法について、必要要件、推奨要件やモデル案を記載した**「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」**を公表。

第1部：充足すべき必要要件

総務省「スマートフォン プライバシー イニシアティブ」スマートフォンにおける利用者情報の取扱いの在り方（第5章）を提示。

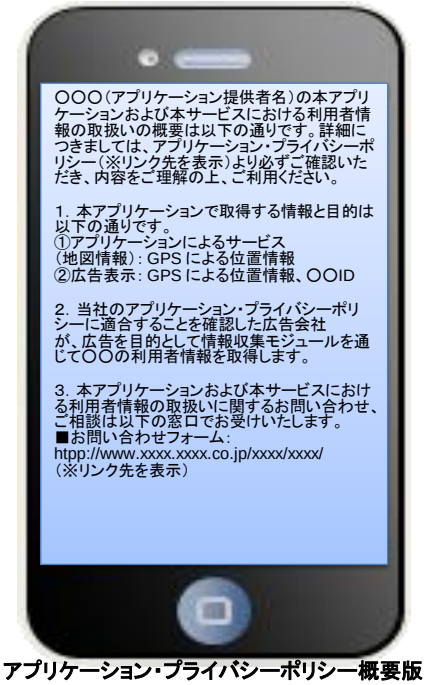
第2部：実装にあたっての推奨要件

「アプリケーション・プライバシーポリシー」の実装にあたって**推奨される要件**を提示。指針では触れられていない**具体的な方法や実態に合わせた追加事項**等。

1 アプリケーション・プライバシーポリシーの名称について
2 通知又は公表及び同意取得等のタイミングについて
3 アプリケーション・プライバシーポリシーを提示する場所について
4 アプリケーション・プライバシーポリシーの変更について
5 同意が得られなかった場合に制限される事項について
6 取得した利用者情報の取扱いについて
7 必要要件以外の同意取得について
8 日本語以外での説明に対する対応について
9 既存のアプリケーションのホンガイドラインへの対応について

第3部：実装にあたってのモデル案

「アプリケーション・プライバシーポリシー」のモデル案と作成ガイドを提示。**詳細な本編**だけでなく**概要版**の作成方法についても提示。



アプリケーション・プライバシーポリシー概要版

電気通信事業者協会（TCA）「スマートフォンアプリケーション提供サイト運営事業者向けガイドライン」の概要

1. 目的・背景

- 利用者の同意を適切に得ることなくプライバシー情報を外部送信する等、問題のあるアプリケーションが流通する事例が発生し、利用者に不安を与える状況が生じている。
- そのような中、**アプリケーション提供サイトを運営する移動体通信事業者**が、**プライバシーやセキュリティの観点から安心・安全なアプリケーションが流通するよう適正に運用**を行い、**利用者に対してスマートフォン利用時の注意事項を周知啓発し、リテラシーの向上を図る**ためにガイドラインを策定。

2. 対象範囲

- 移動体通信事業者が運営するアプリケーション提供サイト
  （①アプリケーションを自社サーバに登録して配信する配信型、②自社サイトにアプリケーション提供者へのリンクを掲載する等の紹介型）

3. 概要

アプリケーション提供者等に対する支援

① **アプリケーション提供者等によるプライバシーポリシーの作成・公表の促進**
特に配信型事業者の場合には、アプリケーションが取得/送信する利用者情報について、アプリケーション提供事業者等からの事前申請を受け、検査を実施した上で自社サーバに登録し、配信する。

② **アプリケーションに関するセキュリティの確認**
アプリケーション登録等の前に、セキュリティ上の確認を行い、事後的にも定期的にチェックする。

③ **適切ではないアプリケーションが判明した場合の対応**
自社サイトからの削除、利用者への注意喚起、関係事業者間の情報共有等を行う。

利用者に対する周知啓発等

スマートフォンをこれまで利用していない方々にも容易に理解してもらえるよう、次の各項目について、書面に記載の上、丁寧に説明する。

① **スマートフォンと従来型の携帯電話端末との違い**
自動通信による課金、アプリによる動作不良等

② **スマートフォンにおける様々な利用者情報の取扱いと注意点**
蓄積された利用者情報に基づく嗜好・趣味に応じた広告の表示等

③ **スマートフォンにおける情報セキュリティ対策**
OS更新、ウィルス対策ソフトの利用、無線LAN利用時の注意等

京都市スマートフォンアプリケーション活用ガイドライン

- 京都市は、平成25年１月10日に「京都市スマートフォンアプリケーション活用ガイドライン」を策定※1。
- 同ガイドラインは、スマートフォンのアプリケーションを提供する京都市の各組織（一部対象外）を対象とし、「スマートフォン　プライバシー　イニシアティブ」を参考に、アプリ利用者の情報を取得する場合の留意点等を提示。
- 京都市は今後、本ガイドラインを利用した研修を職員に対し実施する予定。

ガイドラインの構成

アプリの現状

１　アプリを取り巻く状況･･･スマートフォンの普及及びアプリケーションの多様性について記載
２（１）　アプリのメリット･･･インターネット接続機能、GPS位置情報等の活用例を紹介
２（２）　アプリを活用する場合の注意事項･･･利用者情報の取得によるプライバシー侵害等に言及

京都市スマートフォンアプリケーション活用ガイドライン策定

３　ガイドライン策定の目的･･･
京都市の情報発信・行政サービス提供の推進と情報セキュリティの確保を目的

４　アプリの積極的な活用

（１）アプリを提供するまでの手続
（２）アプリの利用促進
･･･正規のアプリストア（Google Play、App Store等）への登録及び京都市市HPへの掲載等

５　アプリの安全な活用

（１）利用者情報を取得する場合の留意点
･･･利用者情報の種類及びプライバシー侵害の危険性並びに利用者情報を取得する場合の判断基準を記載。
（２）プライバシーポリシーの作成・掲載

※1：http://www.city.kyoto.lg.jp/sogo/page/0000134264.html
※2：平成24年８月「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」提言　http://www.city.kyoto.lg.jp/kamigyo/page/0000109403.html

スマートフォンの利用者情報等に関する連絡協議会　SPSC

平成24年10月にスマートフォンの利用者情報等に関する連絡協議会（SPSC）が、**利用者情報等の適正な取扱いを通じ、安心安全なスマートフォンの利用環境を整備するため、**30以上の関係業界団体、関係機関、関係事業者が参加し設立。

１　活動概要

（１）業界ガイドライン及びモデルプライバシーポリシーに関する情報交換、業界ガイドライン等を策定するためのサポート
（２）プライバシーポリシーの効果的な表示方法等に関する情報交換
（３）利用者情報の取扱いに関する推奨すべき事例及び問題となりうる事例の検討・共有
（４）マーケット動向及び国際的動向に関する情報交換
（５）各業界における推進状況の把握
（６）情報集約及び情報発信（SPSCポータルサイトhttp://jssec.org/spsc/）　等

２　参加メンバー

（１）スマートフォンのプライバシーに関する業界ガイドラインの検討・策定を進める意向がある業界団体、スマートフォンの利用者情報の取扱いに関係する業界団体及び関係機関
※(一社)日本スマートフォンセキュリティ協会（JSSEC）、(一社)モバイル・コンテンツ・フォーラム（MCF）、(社)電気通信事業者協会（TCA）による共同事務局
（２）学識経験者：
新保史生　慶應義塾大学総合政策学部教授【議長】　森亮二　弁護士法人英知法律事務所弁護士【副議長】
（３）オブザーバ：
①関係省庁（総務省、経済産業省、消費者庁）
②関連個別事業者（移動体通信事業者、広告事業者、レビューサイト　等）

３　スケジュール

平成24年　10月　４日 第1回連絡協議会、　11月　６日 第2回連絡協議会、　12月11日 第3回連絡協議会
平成25年　 1月30日 第4回連絡協議会、　 3月18日 第5回連絡協議会 、　 5月16日　第6回連絡協議会

スマートフォン関係事業者による安心・安全な利用環境整備

スマートフォンの利用者情報等に関する連絡協議会(Smartphone Privacy & Security Council)への参加状況

関係業界団体及び関係機関

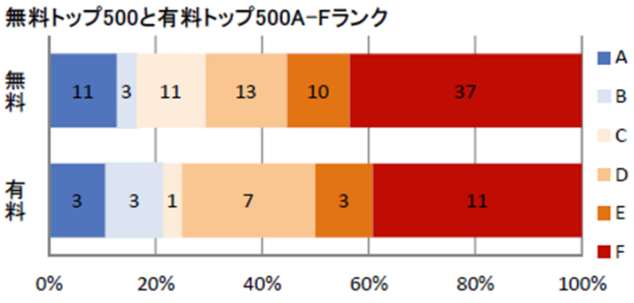
独立行政法人産業総合研究所(AIST)
ビジネス　ソフトウェア　アライアンス(BSA)
一般社団法人情報通信ネットワーク産業協会(CIAJ)
一般社団法人コンピューターソフトウェア協会(CSAJ)
一般社団法人モバイルコンテンツ審査・運用監視機構(EMA)
独立行政法人　情報処理推進機構(IPA)
一般社団法人　IPTVフォーラム(IPTVFJ)
一般社団法人 日本広告業協会 (JAAA)
一般財団法人　日本データ通信協会(JADAC)
社団法人　日本インターネットプロバイダー協会(JAIPA)
一般社団法人ソーシャルゲーム協会(JASGA)
社団法人日本ケーブルテレビ連盟(JCTA)
一般社団法人　インターネット広告推進協議会(JIAA)
一般財団法人日本情報経済社会推進協会(JIPDEC)
安心ネットづくり促進協議会(JISPA)
一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
一般社団法人　情報サービス産業協会(JISA)
一般社団法人　日本オンラインゲーム協会(JOGA)
JPCERTコーディネーションセンター(JPCERT/CC)
一般社団法人モバイル・コンテンツ・フォーラム(MCF)
モバイルコンピューティング推進コンソーシアム(MCPC)
独立行政法人　情報通信研究機構(NICT)
一般社団法人日本ソフトウェア産業協会(NSA)
セキュリティ対策推進協議会(SPREAD)
社団法人電気通信事業者協会(TCA)
一般社団法人テレコムサービス協会(TELESA)
安心ネットづくり促進協議会
日本Androidの会　　等

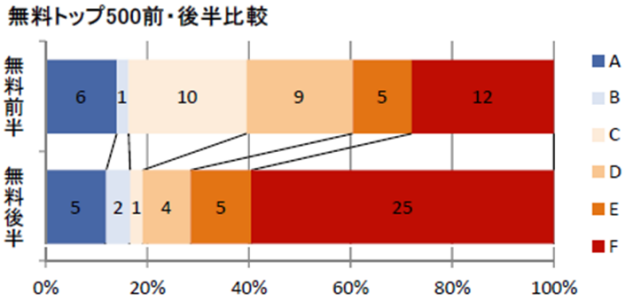
関係事業者

株式会社NTTドコモ
KDDI株式会社
ソフトバンクモバイル株式会社
株式会社日本総合研究所
株式会社電通
株式会社博報堂
アンドロイダー株式会社
情報セキュリティ格付け制度研究会　　等

アプリケーション・プライバシーポリシー掲載の現状調査(産業技術総合研究所調査)

産業技術総合研究所において、2013年4月に無料アプリトップ500から100個を抜粋し、有料アプリトップ500から50個を抜粋し、アプリケーションのプライバシーポリシーの策定状況について6段階の評価基準を用いて調査を行った結果。





評価基準

- A～F 評価
  - A: 個々のスマホアプリ専用のプライバシーポリシーが用意されている
  - B: サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述がある
  - C: サービス全体のプライバシーポリシーがあり、その中に個々のスマホアプリに関する記述がない
    - 利用者情報の取得に関する記述があっても、各アプリによる送信で取得するものなのか書かれていない
      - 例えば、「端末IDを取得する場合がある」と書かれていても、何によって送信されるのか明らかにされていない場合は、C評価
  - D: サービスのプライバシーポリシーとは言えない一般的なWebサイトのプライバシーポリシーがあるだけ
    - 利用者情報に関する個別の記載がない
  - E: 会社としての抽象的なポリシー（個人情報保護方針）があるだけ
  - F: リンクがない又はリンク先にそれらしきものが見つからなかった

（参考）アプリケーション提供サイトに関する連絡通報窓口の例①

（参考）アプリケーション提供サイトに関する連絡通報窓口の例②

（参考）アプリケーション提供サイトに関する連絡通報窓口の例③

※ 第10回WG KDDI説明資料より抜粋

この他、カスタマーサポートセンタへ直接伝える窓口（157）もあり、お客様からのご意見はWeb、電話の両方からいただけます。

（参考）アプリケーション提供サイトに関する連絡通報窓口の例④

※ 第10回WG ソフトバンクモバイル説明資料より抜粋

メニューリスト内のアプリに限らず、Google Play上のアプリの通報を受付

※PC版もあり

アプリケーション提供サイトの掲載基準及び連絡通報方法等

アプリケーション提供サイト	アプリケーション掲載基準	連絡通報方法
Google Play **【Google Inc.】**	アプリケーション提供者は、Google Playデベロッパープログラムポリシー及びAndroidマーケットデベロッパー販売/配布契約書*1に基づきアプリケーションを提供することが求められている。(Googleはこれらにポリシーや契約書を踏まえGoogle Playからアプリを削除する場合があり、深刻な違反や違反を繰り返す場合アカウントが停止される場合がある。)	アプリケーション提供サイト(Google Play)等において不適切なアプリケーション等について、カテゴリー*2を示して通報を受けつけている
App Store **【Apple Inc.】**	App Storeレビューガイドライン*3を踏まえ審査が行われている(非公表)。 Apple Developer Program加入契約書を締結	HP経由で購入したコンテンツの品質に問題がある場合Appleサポートへの通報を受けつけている
Marketplace(Windows7) **Windows Phone ストア(Windows8)** **【Microsoft Corporation】**	**App Policies for Windows Phone※**等を踏まえ審査。(※①位置情報を利用する場合、②利用者の電話帳、写真、電話番号などプライバシー性の高い情報を取得する場合又は第三者と共有する場合、③契約者・端末固有IDを第三者と共有する場合には、利用者の同意を取得し、プライバシーポリシーに記載)	アプリケーション提供サイト(Marketplace/Windows Phone ストア)等において不適切なアプリケーション等についてカテゴリー*4を示し通報を受けつけている
dメニュー、dマーケット **【株式会社NTTドコモ】**	**dメニュー・メニューリスト掲載基準** 1-3-6個人情報保護法のその他の適用法令ならびに関連規則等に基づいて、個人情報を適切に管理すること	スマートフォン画面からメールにての問い合わせ、又は電話窓口による問い合わせを行うことが可能。
au Market **【KDDI株式会社】**	**au Marketコンテンツ掲載に関するガイドライン** 4. 個人情報の取扱いについて 5. 利用者情報の外部送信有無・通話料金発生有無について*5	アプリケーション提供サイト(au Market)から各アプリケーションについて、問題を指摘*6したり、提供者に連絡することが可能。また、電話(157)による問い合わせも可能。
メニューリスト **【ソフトバンクモバイル株式会社】**	**メニューリスト掲載規約*7**	スマートフォン及びPCから不適切アプリ通報窓口*8を設けている。

＊1 Android マーケットデベロッパー販売/配布契約書4.3において、**「デベロッパーは、マーケットを使用して対象製品を販売/配布するにあたり、ユーザーのプライバシー及び法的権利を保護するものとします。」「ユーザー名、パスワード、またはその他のログイン情報または個人情報が提供される、またデベロッパーの対象製品によってそのような情報へのアクセスまたは使用が行われる場合、デベロッパーは、情報がデベロッパーの対象製品に提供されることをユーザーに認識させ、当該ユーザーについてプライバシーに関する法的に十分な通知および保護を行わなければなりません。」「当該情報の仕様については、ユーザーがデベロッパーに対して許可した、限定された目的のための使用のみが認められます。」**とされているhttps://developer.apple.com/jp/appstore/guidelines.html

＊2 性的なコンテンツ、暴力的な画像、差別的または攻撃的な内容、端末やデータに悪影響がある、レーティングが不適切、その他の問題のカテゴリーに分けて連絡通報が可能。

＊3 App Store Review Guidelines(内容についてはDeveloper Program参加者のみに開示)。https://developer.apple.com/jp/appstore/guidelines.html

＊4 不快な内容、児童搾取、マルウェア又はウィルス、プライバシーの侵害、誤解を招くアプリ、パフォーマンス低下

＊5 **ID情報またはプライバシー情報を取得し、外部へ送信する場合、ユーザーに表示する許諾画面で、何の情報を何の目的で、どこへ送信するかに関して分かり易く表示するために、送信する情報、送信する目的、送信先を具体的且つ分かり易くau Market管理画面に登録することを必須とします。送信先は送信先企業・団体等の名称を明示してください。**

＊6 自由記入欄にコメントを記載することが可能。また、不正種別として、URLのリンク先が謝っている、カテゴリーが謝っている、アプリに不具合がある、記載料金が誤っている等を選択することが可能。

＊7 メニューリスト提供規約第32条第2項:**個人情報の収集「プロバイダーは、前項に定めるほか、個人情報の収集、管理、利用にあたっては、個人情報の保護に関する法律等の関連法令、政府等が公表する指針、業界の自主ガイドライン等を遵守するものとする」とされている。また、第33条個人情報の利用・管理、第36条位置情報、第37条位置情報取得に係る顧客の同意などを規定。**

＊8 不適切理由のカテゴリー(性的なコンテンツ、暴力的画像、差別的または攻撃的な用、その他の問題)についてコメントも示した上で送信することが可能。

政策大綱を踏まえた行動規範策定に向けて

ホワイトハウスの政策大綱の発表（2012年2月）

- 2012年2月ホワイトハウスは、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**として、**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**。
- 政策大綱において、プライバシーに関する消費者の７つの権利を示す**「消費者プライバシー権利章典(A Consumer Privacy Bill of Rights)（注）」**が示された。
- 消費者プライバシー権利章典の具体化を目的とした**行動規範を策定**するため、多様な利害関係者（**マルチステークホルダー）**が参加するオープンな議論を行う。**連邦取引委員会（FTC）**は**企業が遵守を宣言した行動規範に基づき執行可能**。権利の法制化についても今後検討。

（注）消費者プライバシー権利章典　（A Consumer Privacy Bill of Rights）
消費者が自らの個人データに関して有する７つの権利として、1個人による管理（自分の個人データを企業が収集・使用する方法について管理できる権利）、2透明性（容易に理解できる形でプライバシー等に関する情報を入手できる権利）、3経緯の尊重（自分の個人データが、自分が情報を提供した経緯に沿う方法で、収集・使用・開示される権利）、4セキュリティ、5アクセス及び正確性、6対象を絞った収集、7説明を示した。

モバイル・アプリの透明性に関する行動規範の検討（2012年7月～）

- ホワイトハウスの政策大綱を踏まえ、**NTIA（米国商務省・国家電気通信情報庁）**が企業、業界団体、消費者団体等が一同に出席するマルチステークホルダー会合を開催。2012年3月にNTIAが実施したパブリックコメントの結果を踏まえ、まずは**「モバイル・アプリの透明性」に関する行動規範の策定に向けた議論**が行われることとなった。
- 2012年7月から2013年6月までに「モバイル・アプリの透明性」に関する行動規範策定に向けて**NTIAはマルチステークホルダー会合を計15回開催**（7月9日に第16回会合を開催予定。）
- **最近の検討状況**
  - ・第14回会合（5月23日）に、**NTIAのストリックリング長官**が出席。これまでの成果を賞賛しつつ**1日も早い手続き完了を要請**（NTIA担当課長が１名か２名の反対は必ずしもコンセンサスの形成を阻害するものではないと発言）
  - ・アプリ開発者協会（ADA）等の起草者が、FTC等から提示された懸念等に対応し**行動規範討議ドラフトを修正。**
  - ・参加者から寄せられた未解決の問題についてNTIAからリストが公表された。
  - （簡略版に関する行動規範であると明示すべきか、第三者のモジュールによる情報収集の扱いをどうすべきか等）
- 簡略な通知の開発に関して、学識経験者が今後調査予定

（参考）モバイル・アプリの透明性に関する行動規範（ADA他団体による討議ドラフト）

- アプリ開発者協会（ADA）他団体による討議ドラフト「モバイル・アプリの透明性」について、FTCから提示された懸念等も踏まえ起草者がドラフトを修正。現段階における討議ドラフトの内容は下記のとおり（※討議中であり、今後も会合における議論等に基づき変更予定）
  （参考）米国市民的自由連合（ACLU）、Consumer Action、世界プライバシー・フォーラム（WPF）

モバイル・アプリの透明性に関する行動規範（Code of Conduct on Mobile APP Transparency）

Ⅰ　前文
○ マルチステークホルダープロセスを経て検討されたモバイルアプリに関する簡略な通知のための自主的な行動規範。
○ **簡略な通知は、消費者に対してアプリケーションによるデータ取得や第三者提供などに関する透明性を向上させるためのもの。**
○ **アプリケーション提供者は、本行動規範に関らずカルフォルニアのオンラインプライバシー保護法や他の法令を踏まえ、詳細なプライバシーポリシー作成の義務を負う。**

Ⅱ　簡略な通知
下記の事項について、簡易版通知において、**できる限り一画面内に表示する。**
（1）利用者から取得される情報
例：電話帳、ブラウザー利用履歴、通信履歴、位置情報、金融情報、バイオメトリックス、医療健康情報、ユーザ保存ファイル　等
（2）詳細なプライバシーポリシーへのアクセス方法
（3）第三者との利用者を特定する情報の共有　　例：広告ネットワーク、通信事業者、**消費者情報再販事業者**、データ分析事業者、政府機関、OS提供事業者・プラットフォーム提供者、ソーシャルネットワーク、その他
※アプリ開発者が第三者の情報収集を了解しておらず、情報収集されるまで知らなかったが、その後直ちに適切な措置をとる場合は除く。
※当該アプリのサービス提供や**運用**に必要な範囲に使途が限定されており、更なる第三者との共有が禁止される場合等については除く
（4）アプリケーションの提供事業者名

※　非識別化された情報については記載する必要はない：①非識別化され、②再識別化しないと約束し、③第三者にも再識別化させない場合
※　運用目的のために情報を収集する場合は除く：アプリの維持管理、利用者の識別、セキュリティ、法令順守等

Ⅲ　簡略な通知の記載方法
・Ⅱ（1）、（3）の内容については文書で表示されていること（適宜アイコンやシンボルも活用可能）、必要事項を見やすく一つのスクリーンに記載
・アプリケーションからいつでも見られること、利用者情報の取得について、取得する情報の範囲を拡大するような変更を行う場合には、FTC法第5条に基づき改めて同意取得を行う

Ⅳ　データ利用・利用条件、又は全体版プライバシーポリシーへのリンク
簡略な通知を行うとともに、利用者情報の利用ポリシー、利用規約、法的に求められる詳細なプライバシーポリシーへのアクセスを提供すること。これらのリンクには、利用者がデータ消去を求める方法に関する説明、第三者提供される事業者名、データ保存期間等を含む。

FTCスタッフレポート「モバイル・プライバシー・ディスクロージャーズ」

- 2013年2月1日FTC（米連邦取引委員会）は、「モバイル・プライバシー・ディスクロージャーズ：透明性の確保による信頼の構築」を**FTCスタッフレポート**として発表。**プラットフォーム事業者（OS事業者）、アプリ開発者、広告ネットワーク事業者、アプリ開発事業者の業界団体及び関係有識者等に対しそれぞれの果たすべき役割を示した。**
- FTCは同スタッフレポートが**NTIA（米国商務省・国家電気通信情報庁）によるマルチステークホルダー会合における議論への有益なインプット**となることを期待するとしている。

Ⅰ　モバイルテクノロジーの利便性とリスク

・スマートフォンやタブレッドが急速に普及し、多数のアプリが提供されている（例：Google Play80万アプリ、App Store70万アプリ）。
・利用者に多くの利便性を提供。一方、複雑な業界構造の下、**位置情報を含む利用者情報の取扱いに係るプライバシー上の課題が大きい。**
　＊　約６割の利用者がプライバシー上の懸念からアプリ利用を断念した経験。大半の利用者は自らの利用者情報を十分管理できないと考えている。

Ⅱ　FTCによる活動と検討

・2012年3月に報告書「急速の変化する時代における消費者プライバシー保護」を発表し、**同年5月にモバイル環境におけるプライバシーに関するワークショップを開催**。また、**モバイルプライバシーに係る執行**、**アプリ開発者の啓発**等を実施。

Ⅲ　FTCによる提言

A.プラットフォーム事業者（OS事業者）※ Apple, Google, Amazon, Microsoft, Blackberryを例示
・**センシティブ情報（例：位置情報）**及び場合によっては**センシティブとなりうる情報（例：電話帳、写真、カレンダー、録音、録画）を取得**する際には、**速やかに利用者に知らせ、同意を取得（affirmative express consent）**
・アプリがアクセスする情報の種類を**ワンストップで把握できる「ダッシュボード」**、**利用者情報の送信を示すアイコン**の開発を検討
・**アプリ開発者によるベストプラクティスを推進**
・アドネットワーク等によるトラッキングの可否を選択できるよう、**モバイル向け「Do Not Track」の仕組みを検討**

B. アプリ開発者
・**プライバシーポリシーを作成**し**アプリマーケットに示す。センシティブ情報を取得する前**に、利用者の**同意を取得**（OS事業者の対応と要調整）
・**広告ネットワーク事業者等と連携**し利用者への正確な情報提供に努める。**業界として簡潔なプライバシー情報提供のガイドライン等**を策定。

C. 広告ネットワーク事業者等
・**アプリ開発者と連携**し正しい情報を利用者に提供、**モバイル向け「Do Not Track」**を効果的に実行できるプラットフォームと協力

D. アプリ開発事業者の業界団体及び関係有識者等
・**標準化されたアプリ・プライバシー・ポリシーの策定促進**、アプリ開発者を教育、**簡潔な情報提供の方法を開発（例：標準化されたアイコン等）**

PRIVACY ON THE GO-モバイル・エコシステムに向けた提言-

○2013年1月、**カルフォルニア州の司法長官**は、**モバイル端末におけるプライバシーに関する提言を発表**。アプリ提供者、アプリケーション提供サイト運用者、アドネットワーク、OS提供者、移動体通信事業者などの関係する各主体が、モバイルアプリにおけるプライバシー保護に向けて実施すべき事項について提言。
○多様な利便性を提供するアプリケーションのイノベーションを維持しつつ、適切にプライバシー保護を行っていくため、**スマートフォンの利用者情報に関するプライバシー・ポリシーを提供**し、消費者の予見可能性を高め、有効で選択できる情報を提供することが必要としている。

1　アプリケーション提供者（APP Developers）
・情報チェックリストにより、アプリが取得・利用しうる個人情報を確認し、取扱いについて意志決定すること。
・アプリの**基本的機能に不要な個人情報の収集を回避もしくは制限**すること。
・**明確で正確なプライバシーポリシーを作成**し、利用者又は潜在的利用者に明示的に**アクセス可能**とすること。
・情報の取扱いについてユーザーの注意を引く通知方法を用いるとともに、ユーザーに意味のある選択権を与えること。

2　アプリケーション提供サイト運営者（App Platform Providers）
・ユーザーがアプリをダウンロード前に確認できるように、**アプリケーション提供サイトからアプリケーション・プライバシーポリシーへアクセス**できるようにすること。アプリケーション提供サイトを通じ利用者へ**モバイルプライバシーの教育**をすること。

3　モバイル広告ネットワーク（Mobile Ad Networks）
・アプリ外部の広告のために、ブラウザ設定を変更したり、モバイルデスクトップのアイコンを置いたりしないこと。アドネットワークに関するプライバシーポリシーを作成し、アドネットワークを用いるアプリ提供者に開示しなさい。
・端末固有IDの利用をやめて、**アプリ独自の一時的ID**を使うこと。

4　OS提供事業者（Operating System Developers）
・グローバルなプライバシー設定を開発し、利用者が**アプリがアクセスできる機器の性質や情報をコントロール**できるようにしなさい。

5　移動体通信事業者（Mobile Carriers）
・**モバイルプライバシーと子供のプライバシー**について、利用者を教育する。

児童オンラインプライバシー保護法(COPPA)規則改正

■ 子供のインターネット使用に関して親により広範な管理権を与えることで、子供のプライバシー保護の強化を目指し、米連邦取引委員会(FTC)は、2010年に米児童オンラインプライバシー保護法(COPPA)規則のレビューを開始。2012年12月19日に最終改正案を採択し、2013年7月1日より発効。

○ COPPAの概要

- 1998年10月、オンライン上における児童(13歳未満)のプライバシー保護に特化した連邦法として成立。
- 13歳未満の児童を対象とするか、13歳未満の児童から実際に個人情報を収集するウェブサイトやオンラインサービスは、個人情報の収集開始前に保護者に対して通知し、有効な同意(varifiable parental consent)を取得することが必要。

○ 規則改正案のポイント

- 保護者への通知及び同意なしに収集できない「個人情報」のリストを修正し、**位置情報、子供の顔や声が含まれている写真、ビデオ、オーディオが保護者への通知及び同意なしに収集できない**ことを明確化
- 企業に対し、**新たに保護者の同意を取得する、合理化された、自発的かつ透明性のある承認プロセス**(※1)を提示
  (※1)電子的にスキャンされた署名付きの親の同意書やビデオによる確認の利用も可能に
- 児童向けアプリ及びウェブサイトが、**第三者**(広告ネットワーク等)**が保護者への通知及び同意なしに児童から個人情報を収集することを防止するための合理的な措置を講じるべき**旨定め、これまでの抜け穴を防止
- 追加で情報を収集する第三者はCOPPAを遵守しなければならない範囲を拡大
- **IPアドレスや携帯端末ID**など、異なるウェブサイトやオンラインサービスをまたいで利用者の識別が可能なIDをカバーするよう、COPPAの対象範囲を拡大
- 対象となるウェブサイト運営者やオンラインサービス提供者による児童の個人情報の提供先は、**個人情報を安全かつ秘匿した形で保管できる企業にのみ提供**することを求める、データセキュリティ保護に係る規定を強化
- 対象となるウェブサイト運営者は、**データ保存及び削除について合理的な手続きを定めること**を要求
- FTCによる自主規制セーフハーバープログラム(※2)の**FTCの監督を強化**
  (※2)業界団体等が策定し、FTCが承認した自主規制プログラムを遵守する事業者はCOPPAルールを充足するとの規定

他方で、米Googleの「Google Play」や米Appleの「App Store」等のプラットフォームは、児童向けアプリへのアクセスを提供しているのみであるとして対象外とされたほか、米Facebookは外部サイトに設置された「Like」ボタンについて、児童向けサイトから情報収集している事実上の認識がなければ同法に問われることはないとされたため、改正の影響は限定的な可能性(米メディア報道)。

EUにおける個人データ保護に関する制度

個人データ保護指令(1995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)」

(主な内容)
(1)データ内容に関する原則(特定された明示的かつ適法な目的のための取扱い等)
(2)データ取扱いの正当性の基準(データ主体の明確な同意等)
(3)センシティブデータ※の取扱い ※人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入、健康又は性生活に関するデータ
(4)データ主体のデータへのアクセス権
(5)取扱いの機密性及び安全性
(6)第三国への個人データの移転に関する規律(第三国が十分なレベルの保護措置を確保していることを条件とする等)
(7)独立した監督機関

e-プライバシー指令(2002年、2009年改正)

「電子通信部門における個人情報の処理とプライバシーの保護に関する指令(2002/58/EC)」

(主な内容)
(1)Cookieの利用に当たって内容を明示しオプトインによる利用者同意を求める
(2)ロケーションデータを利用する際にオプトインによる利用者同意を求める

◆ 急速な技術進展
◆ 情報の共有・収集規模な急増

EU個人データ保護規則案 ※2012年1月25日公表

立法手続きを開始

(主な内容)
(1)EU域内における規制の単一化・簡素化(※国内法制化の不要な「規則」に変更)
(2)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)
(3)データ保護に関するグローバルな課題への対応(EU域内居住者向けにサービスを提供する場合等には、域外事業者による個人データ取扱いにも効力を及ぼすための規定)
(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)、「欧州データ保護ボード」の設置等)

EU第29条作業部会による意見書概要（スマートフォン等アプリ）

■2013年2月、EU第29条作業部会（※）は、スマートフォンアプリが急速に普及する中で、①利用者への透明性のある説明や有効な同意の欠如、②不十分なセキュリティ措置、③利用目的や流通範囲の限定が講じられないまま個人データが取得されている点を踏まえ、スマートフォンアプリに関する意見書を公表。

※ 1995年データ保護指令第29条に基づき設置された諮問機関。欧州委員会、加盟国規制機関等から構成され、同指令の法的解釈を行っている。

■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用者、OS・端末開発者等の関係する各主体について、個人データ保護指令やeプライバシー指令に基づく義務及び推奨事項を記載。

1 アプリケーション開発者の義務

・アプリが情報収集等を開始する前に**情報の種類（注）毎に有効な同意を求める**こと。当該同意を撤回可能とする
（注）位置情報、契約者・端末固有ID、個人情報、電話帳、クレジットカード番号、通話・SMS・電子メール、閲覧履歴等
・**利用目的を明示し、個別の同意なく変更**しないこと。**必要以上の情報を収集**しないこと。**第三者提供する場合明示**。
・必要な情報（収集者、内容、目的、第三者提供の有無、利用者の権利等）について**プライバシーポリシーを提示**すること
・データ管理者としての義務を履行する（外部委託時に監督義務を含む）、設計段階から、個人データ保護のための対策を講じる。
・**子ども向けアプリを厳格に取り扱うこと**（収集情報の最小化、行動ターゲティング広告への利用自粛等）　等
（この他、eプライバシー指令に準拠したデータ侵害時の情報提供、データ保存期間のカスタマイズツール等の提供が推奨される）

2 アプリケーション提供サイト運営者の義務

・アプリ開発者に対し**アプリが収集可能な情報の種類や目的等に係る情報提供義務を遵守**させる、提出されたアプリケーションに対する審査結果の公表
（この他、OS提供者と協力し情報へのアクセス状況を示すマーク等の管理ツールを開発、全ての掲載アプリケーションのプライバシー保護レベルに関する評価、連絡通報窓口の設置、プライバシーに配慮したアンインストールツールの提供等が推奨される）

3 OS・端末開発者の義務

・利用者が有効な同意を行えるようにAPIや保存ルールを最新のものとする。**アプリケーションの初回起動時や機微情報への初回アクセス時に同意ツールを作動**させる。悪意あるアプリの拡散防止、アプリ開発者が必要最低限の情報にのみアクセス可能とする。
（この他、利用者によるアプリのアンインストール、セキュリティ措置の更新、利用者に対する詳細な情報提供（どのデータが利用されているか）が可能となるツールを開発すること等が推奨される）

4 第三者（サードパーティー）の義務

・eプライバシー指令に基づく同意取得義務を履行すること、Do　Not　Track機能を迂回しない
・トラッキングの目的のために契約者・端末固有IDを用いることを避ける、子どもの情報の行動ターゲティング広告への利用自粛　等

韓国・アプリ開発者向けプライバシーガイド

■ 韓国においても、スマートフォンにおける個人情報の流出が問題となっていることを背景として、2012年3月、**韓国情報保護振興院（KISA）**が**「アプリ開発者向けプライバシーガイド」**を公表
■ 国内通信事業者（※）を通じ、同ガイドの周知・啓発を実施　（※ 独自のマーケット、アプリ開発支援HP、アプリ開発教育センター等を運営）

○ 法的位置づけ

個人情報保護の観点から、
①情報通信網利用促進及び情報保護などに関する法律（情報通信網法）、
②位置情報の保護及び利用などに関する法律（位置情報法）
に基づき、アプリ開発者が留意すべき事項を示すもの（ガイド自体に法的拘束力はなし）

○ 主な内容

○ 個人情報の収集を最小限に抑えるべきであり、必須項目以外、利用者が個人情報を提供しないことを理由にサービスの利用を禁止してはならない旨規定
○ 信頼できるアプリ開発ツールを利用すべき旨規定（放送通信委員会（KCC）及びKISAが運営する「スマートアプリ開発支援センター」や各事業者が運営するアプリ開発支援HPを参照することを推奨）
○ 法規に準拠し、アプリ開発すべき旨規定。ガイドにおける主な規定は次のとおり。

ガイドにおける規定
「個人情報保護方針」の作成・公開義務
個人情報の収集・利用に関する同意取得
位置情報の収集・利用・提供に関する同意取得
センシティブな個人情報の収集の原則禁止
個人情報の取扱いの委託時の利用者の同意取得
個人情報の第三者提供の制限
未成年者の場合の法定代理人の同意取得
個人情報の収集目的範囲内の利用の確保
会員情報の閲覧・訂正等、利用者の権利保障
技術的保護措置の実装義務

（参考）利用者情報に係る韓国の取組

○ 周知・啓発等取組

・国内通信事業者が運営する独自のマーケット、アプリ開発支援HP、アプリ開発教育センター等を通じ、KISA発表のアプリ開発者向けプライバシーガイドを周知・啓発

・国内通信事業者はアプリの個別チェックは行わず、KISAがツールを使ったり、直接ダウンロードしたりすることにより、ツールによる自動チェック及び利用者の同意を取得しているか等の状況をモニタリング
→ 来年の目標はアンドロイド上のアプリ、再来年の目標はiPhone上のアプリ（各一万個程度）

・このほか、KISAは、スマートフォンの中でモニター機能を果たすようなアプリ（**SSチェッカー**）を開発

SSチェッカー

（参考）韓国のスマートフォン向けアプリマーケット

マーケット名（事業者名）	ユーザー数	1日平均利用者数	掲載アプリ数	累計ダウンロード数	備考
T Store（SKテレコム）	1,856万人（2012年12月）	260万人/日（2012年12月）	20万以上（2011年11月）	10億8,000万（2012年12月）	• アプリの売上面で国内ナンバーワンの実績。 • 他の携帯電話事業者の契約者も利用可能。
Olleh Market（KT）	600万人（2012年4月）	n.a	4万（2011年11月）	2億2,000万（2012年12月）	
U+ストア（LGU+）	n.a	34万人/日（2011年12月）	4万4,000（2012年9月）	1億3,800万（2012年10月）	
Samsung Apps（Samsung）	n.a	n.a	4万（2011年9月）	1億（2011年9月）	

＊株式会社日本総合研究所による調査（平成25年2月）

プライバシー・バイ・デザイン

プライバシー・バイ・デザイン（PbD：Privacy by Design）

○カナダオンタリオ州　情報プライバシー・コミッショナーのアン・カブキアン博士が1990年代に開発した概念

7つの基本原則

1. 事後対応ではなく、事前対応/予防的
2. デフォルト設定でプライバシー保護
3. 設計時に組み込むプライバシー保護
4. すべての機能に対して：ゼロサムではなく、ポジティブサム
5. 個人情報のライフサイクル全体における保護
6. 可視性と透明性：オープンにする
7. 個人のプライバシー尊重：個人を主体に考える

プライバシー・バイ・デザイン
プライバシー情報を守るための世界的新潮流
堀部政男/JIPDEC編
PbD：アンカブキアン著

第３章にてスマートフォン　プライバシー　イニシアティブを日本の代表的プライバシー・バイ・デザイン事例として紹介

プライバシー影響評価（PIA：Privacy Impact Assecement）

個人情報の収集を伴う情報システムの導入にあたり、プライバシーへの影響度を「事前」に評価し、その構築・運用を適正に行うことを促す一連のプロセス

プライバシー保護強化技術（PETs：Privacy Enhancing Technologies）

プライバシー保護を向上させるために利用される技術の総称（代替的PET、補完的PET（DNT等））

プライバシー・バイ・デザイン概念の国際的浸透

○データ保護・プライバシー・コミッショナー国際会議決議（第32回：2010年10月）
○EU個人データ保護規則案（2012年1月）
○携帯通信事業者の業界団体GSMA「携帯端末向けのプライバシー原則」（2012年1月）
○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3月）

（参考）モバイルＯＳの比較表

	Android	i OS	Windows Phone	Tizen	Firefox OS
開発元	Google	Apple	Microsoft	Linux Foundation	Mozilla
シェア（世界）	69.7%	20.3%	3.2% （IDC）	–	–
発売時期（日本）	2009年7月～	2008年7月～	2011年8月～	2013年内予定	2014年以降
サポート企業	Open Handset Allianceパートナー（世界各国の通信事業者、端末メーカー、チップメーカー等85社以上を含む）	–	【通信事業社】KDDI(WP7.5), 米AT&T, 英Vodafone, 仏Orange, 独T-Mobileなど 【チップメーカー】クアルコム 【端末メーカー】富士通(WP7.5),ノキア,HTC,サムスン,ファーウェイなど	【通信事業社】docomo、英ボーダフォン、韓国KTなど6社 【チップメーカー】インテル 【端末メーカー】サムスン、ファーウェイ、富士通など5社	【通信事業社】KDDI、米America Movil、チャイナユニコム、ドイツテレコムなど18社 【チップメーカー】クアルコム 【端末メーカー】LG、ファーウェイ、ソニーモバイルなど5社
アプリ入手先	**Google Play**(Google) その他制限なし（第三者によるアプリ提供サイト等）	**App Store**(Apple)のみ	**Windows Phone Store** (Microsoft) のみ	**Tizen Store**(サムスン、インテル)、 各キャリアによるアプリ提供サイト	**Firefox Marketplace**(Mozilla) その他制限なし（第三者によるアプリ提供サイト等）
アプリの審査体制	アプリケーション開発者と締結する契約とアプリケーション掲載者の自己審査,Bouncer によるマルウェア検出	Appleによる事前審査	Microsoftによる事前審査	サムスンとインテルが共同で審査	Mozillaのスタッフ等による事前審査
OSレベルでのアプリへの対応	ネイティブアプリ / Webアプリ※(HTML5) ※ブラウザアプリによりWebアプリ（HTML5）も利用可	ネイティブアプリ / Webアプリ※(HTML5) ※ブラウザアプリによりWebアプリ（HTML5）も利用可	ネイティブアプリ / Webアプリ※(HTML5) ※ブラウザアプリによりWebアプリ（HTML5）も利用可	ネイティブアプリ / Webアプリ(HTML5)	Webアプリ(HTML5)
HTML5アプリへの対応	●標準のブラウザ経由でWebアプリ（HTML5）を利用可能(端末利用者情報へのアクセスは原則ない) ●ネイティブアプリ内Webviewは、アプリのパーミッション範囲内	●標準のブラウザ経由でWebアプリ（HTML5）を利用可能(端末利用者情報へのアクセスは原則ない) ●ネイティブアプリ内Webviewの場合、通常のアプリケーションと同様（位置情報等を取得しようとする場合ポップアップを表示し同意取得）	●標準のブラウザ経由でWebアプリ（HTML5）を利用可能(端末利用者情報へのアクセスは原則ない) ●ネイティブアプリ内WebBrowserコントロールは、アプリのパーミッション範囲内	●Webサーバーに接続するHostedアプリ、Appストアからダウンロードするアプリ等がある。 ●Webアプリは原則TizenStoreから各キャリアによるアプリ提供サイトのみから提供	●Webサーバーに接続するHostedアプリ、Appストアからダウンロードするアプリ等がある。 ●位置情報や電話帳*等を利用する場合ポップアップで同意取得。 (*Marketplaceによる審査を受けたアプリのみ利用可能)

※　日経コミュニケーション(2013年5月号)等を元に総務省作成

（参考）ネイティブアプリはJava、Objective-C、C/C++等で開発されている。Webアプリ（HTML5）は、HTML、CSS、JavaScript等で開発されている。HTML5において、端末機能や位置情報等を制御できるAPI（アプリケーション　プログラミング　インターフェース）が規定され、Webアプリであってもネイティブアプリ並の機能が実現できるようになってきている。

iOS6におけるプライバシー設定

- Apple社が2012年９月20日に「iOS6」をリリースした。
- 「iOS6」では、従来のiOSに比べ、**プライバシー保護に向けた機能が強化**されており、個別のアプリケーションが初めて電話帳情報等を利用しようとした際、**ポップアップ表示により、当該利用の可否の確認を利用者に求める（図１）。**
- **アプリケーションによる電話帳情報等の利用を個別のアプリケーションごとに管理**することができる。（図２）

※「iOS」とは、Apple社が提供する、OS（Operating System：パソコンやスマートフォン等のデバイスが基本的な機能を実現するために必要なソフトウェア。）の名称。他社製品ではMicrosoft社の「Windows」等。

図１：電話帳利用に関する同意確認

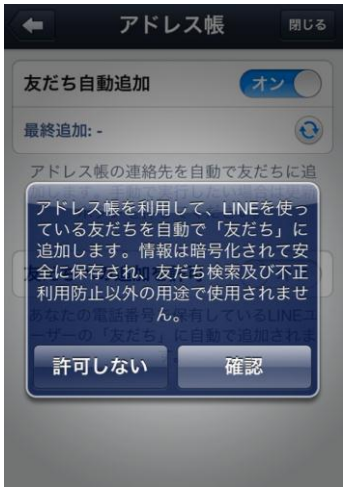


図２：プライバシー設定画面

Firefox　OSにおけるプライバシー設定

- 「**Firefox　OS**」では、個別のアプリケーションが初めて電話帳情報、位置情報等を利用しようとした際、**ポップアップ表示により、当該利用の可否の確認を利用者に求める（図１）。**
- **アプリケーションによる電話帳情報等の利用を個別のアプリケーションごとに管理**することができる。（図２）
- Firefox　Marketplaceにおいて、プライバシーポリシーは必須であるとしている。

※「**Firefox　OS**」とは、Mozilla Foundationが提供するOS（Operating System：パソコンやスマートフォン等のデバイスが基本的な機能を実現するために必要なソフトウェア。）の名称。

図１：位置情報利用に関する同意確認

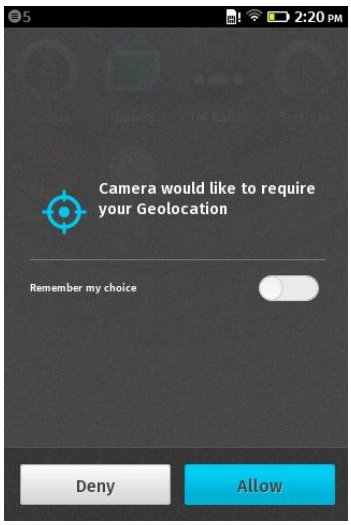
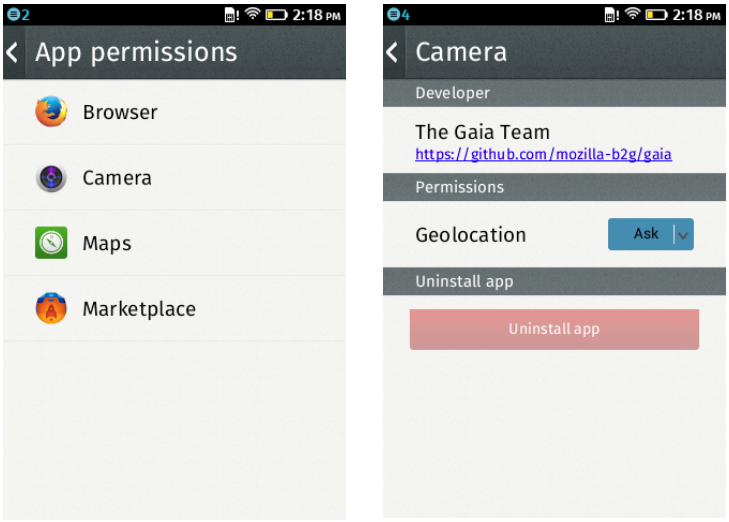


図２：プライバシー設定画面



シャープ(株)の電話帳アクセスモニター

- 機能搭載の背景
  - Androidのパーミッション確認の仕組みに係る事故の発生
    - 利用者が意図しないうちに、あるアプリが電話帳データを外部に送信した等。
- 課題
  - アプリがいつ端末の機能を使うか、顧客にはわからない。
- 解決方針
  - アプリがいつ端末の機能を使うかの可視化及び使用をブロックする手段を提供。(当面まず電話帳データの読み書きから対応。)
- 機能(2012年冬モデルの機種から搭載。)
  - アプリによる電話帳データへのアクセスを検出するごとにアプリ名を通知領域に表示。
  - 電話帳データへのアクセス時の動作をアプリ単位で設定可能。

※電話帳には、利用者が登録した名前、電話番号、メールアドレス、住所、顔写真等の幅広い項目が含まれる。

各国におけるスマートフォン等における利用者情報保護に関する提言の比較

	スマートフォン プライバシー イニシアティブ（H24年8月・日本諸問題研提言）	モバイル・プライバシー・ディスクロージャーズ（H25年2月・米FTCスタッフレポート）	PRIVACY ON THE GO-モバイル・エコシステムに向けた提言（H25年1月・米カリフォルニア州）	携帯端末向けのプライバシー原則及びプライバシーデザインのガイドライン（※※）（H24年1月・GSM協会）
対象				
アプリ提供事業者	・個別のアプリについて８項目（※）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こと ※ ①情報取得者の名称、②取得される情報、③取得方法、④利用目的、⑤通知・公表又は同意取得の方法、⑥利用者関与の方法、⑦外部送信・第三者提供・情報収集モジュールの有無、⑧問合せ窓口、⑨プライバシーポリシーの変更を行う場合の手続き	・プライバシーポリシーを作成しアプリマーケットに示すこと ・センシティブ情報を取得する前に、利用者の同意を取得すること（OS事業者の対応と要調整） ・広告ネットワーク事業者等と連携し利用者への正確な情報提供に努めること（業界として簡潔なプライバシー情報提供のガイドライン等を策定）	・情報チェックリストにより、アプリが取得・利用しうる個人情報を確認し、取扱いについて意志決定すること ・アプリの基本的機能に不要な個人情報の収集を回避または制限すること ・明確で正確なプライバシーポリシーを作成し、利用者又は潜在的利用者に明示的にアクセス可能とすること ・情報の取扱いにつき利用者の注意を引く通知方法を行うほか、利用者に意味のある選択権を与えること	○透明性と利用者による選択とコントロール ・利用者に個人情報の収集項目、利用目的、利用方法等を事前に通知すること ・情報の取得者を利用者に通知すること ・利用者にプライバシーに係る説明を行うこと ・最小限の情報収集・限定利用とすること ・必要な場合、利用者の積極同意を得ること 等 ○データの保存とセキュリティ ・識別子を適切に管理すること ・送信等の際、データの安全性を確保すること ・可能な限り、リスクに応じ、利用者の認証を行うこと ・データの保管及び削除期間を定めること ○教育 ・プライバシー管理の設定や手法について、利用者を教育すること ○ソーシャルネットワークとソーシャルメディア ・登録時に任意提供である情報は明示するとともに、利用者関与の機会を付与せず、公開プロフィール等に公開しないこと ・初期設定がプライバシー保護的であること、各自情報が簡単にコントロール可能であること 等 ○モバイル広告 ・広告配信機能を利用者に通知すること ・ターゲティング広告の利用者同意を得ること ・ターゲティング広告は合法的に取得された情報を利用すべきこと ・バイラルマーケティングもプライバシーに配慮すること 等 ○　位置情報 ・利用者に位置情報の利用を通知し選択権を与えること ・位置情報の利用につき適切な同意を得ること ○　青少年の保護 ・次項目参照 ○　説明責任等 ・ビジネスプロセス全体を通じ利用者のプライバシー確保のための責任を明確化すること ・アプリの問題を報告するための手法を利用者に提供すること
モバイル広告ネットワーク	・提供する情報収集モジュールに関するプライバシー・ポリシーを定め公表すること ・当該情報収集モジュールを組み込もうとするアプリ提供者へ必要な情報を提供すること ・プライバシー・ポリシーの内容に変更があった場合、その旨を通知すること	・アプリ開発者と連携し正しい情報を利用者に提供、モバイル向け「Do Not Track」を効果的に実行できるプラットフォームと協力すること	・アプリ外部の広告のために、ブラウザ設定を変更したり、モバイルデスクトップのアイコンを置いたりしないこと ・アドネットワークに関するプライバシーポリシーを作成し、アドネットワークを用いるアプリ提供者に開示すること ・端末固有IDの利用をやめて、アプリ独自の一時的IDを使うこと	
OS提供事業者	・アプリ提供者等に対し、適切なプライバシーポリシーの作成・公表等を促すこと ・プライバシー・ポリシー等の表示場所を提供するなど、アプリ提供者等に対し、適切な対応を行うように支援すること ・アプリ提供者や情報収集モジュール提供得者等に対し、啓発活動を進めること ・説明や情報取得の方法が適切ではないアプリ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こと ・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こと	・センシティブ情報及び場合によってはセンシティブとなりうる情報を取得する際には、速やかに利用者に知らせ、同意を取得すること ・アプリがアクセスする情報の種類を把握できるダッシュボード、利用者情報の送信を示すアイコンの開発を検討すること ・アプリ開発者によるベストプラクティスを推進すること ・アドネットワーク等によるトラッキングの可否を選択できるよう、モバイル向け「Do Not Track」の仕組みを検討すること	・グローバルなプライバシー設定を開発し、利用者がアプリがアクセスできる機器の性質や情報をコントロールできるようにすること	
アプリ提供サイト運営者		ー	・ダウンロード前に確認できるよう、アプリ提供サイトからアプリ・プライバシー・ポリシーへアクセスできるようにすること ・アプリ提供サイトを通じ利用者へモバイル・プライバシーの教育をすること	
移動体通信事業者	・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こと ・リテラシーに応じたスマートフォンのサービス設計や周知を端末提供事業者との協力も考慮しつつ検討すること	ー	・モバイル・プライバシーと子供のプライバシーについて、利用者を教育すること	
業界団体・関係有識者等	・業界ごとのガイドラインを策定すること、利用者への情報提供・周知啓発等を推奨	・標準化されたアプリ・プライバシー・ポリシーの策定促進、アプリ開発者を教育、簡潔な情報提供の方法を開発すること	ー	
青少年に特化した規定				
	「インターネットの利用を前提するスマートフォンについては、･･･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」と記載。	ー （FTCは、H22年に児童オンラインプライバシー保護法（COPPA）規則のレビューを開始し、H24.12月に最終案を採択）	・移動体通信事業者が子供のプライバシーについて利用者を教育すること等を規定	・年齢層に応じ、適切なアプリを作成することと ・プライバシー保護的な初期設定とすること ・子供を保護する法令を遵守すること ・適切な場合には年齢確認を行うこと

スマートフォンのアプリケーションに組み込まれるモジュールの例

No	モジュール名（SDK）	事業者名	言語	プライバシーポリシーURL
1	adclr	株式会社ライブレボリューション	日本語	http://adcounter.jp/privacy_policy/
2	AdColony	AdColony	英語	http://adcolony.com/legal/privacy/
3	Adlantis	株式会社アトランティス	日本語	http://atlantiss.jp/privacy/
4	AdMarge	株式会社 ディマージシェア	日本語	http://www.dimage.co.jp/privacy/index.html
5	AdMarvel	AdMarvel, Inc	英語	http://www.admarvel.com/AdMarvel_Privacy_Policy_2012.pdf
6	AdMob	グーグル株式会社	英語	http://jp.admob.com/home/privacy
7	AdMobOld	グーグル株式会社	英語	上記に同じ
8	AdWays	株式会社アドウェイズ	日本語	http://www.adways.net/privacy.html
9	AdWhirl	グーグル株式会社	－	－
10	AMoAd	株式会社AMoAd	日本語	http://www.amoad.com/privacy/
11	aMoBee	Amobee, Inc.	英語	http://www.amobee.com/privacy/
12	burstlyAd	Burstly	英語	https://www.burstly.com/Home/Privacy
13	CARewardAck	株式会社CAリワード	日本語	http://www.ca-reward.co.jp/company/privacy.html
14	chartBoost	Chartboost	英語	https://help.chartboost.com/legal/privacy
15	DaumAd	deviantART, Inc.	英語	http://about.deviantart.com/policy/privacy/
16	DimageAd	株式会社 ディマージシェア	日本語	http://www.dimage.co.jp/privacy/index.html
17	fiksuMart	Fiksu, Inc.	英語	http://www.fiksu.com/privacy-policy
18	flurry	Flurry, Inc.	英語	http://www.flurry.com/privacy-policy.html
19	glamAd	Glam Media, Inc/Glam Media Japan	英語	http://www.glammedia.com/about_glam/legal/privacy-security/
20	gmoSeo	GMOインターネット株式会社	日本語	http://seo.gmo.jp/privacypolicy.html
21	GoogleAnalytics	グーグル株式会社	日本語	http://www.google.co.jp/intl/ja/policies/privacy/
22	GreystripeAd	ValueClick, Inc.	英語	http://www.greystripe.com/user-privacy-policy
23	greeReward	グリー株式会社	日本語	http://corp.gree.net/jp/ja/privacy/
24	imobile	株式会社アイモバイル	日本語	http://i-mobile.co.jp/privacy.aspx
25	inmobi	インモビジャパン株式会社	英語	http://japan.inmobi.com/terms/privacy-policy/
26	INTERSPACE	株式会社インタースペース	日本語	http://www.interspace.ne.jp/privacy.html
27	jumptapAd	Jumptap, Inc.	英語	http://www.jumptap.com/privacy-policy/
28	Kiip	Klip,Inc.	英語	https://app.kiip.me/privacy
29	leadBoltAd	LeadBolt	英語	http://www.leadbolt.com/privacy.php
30	lotarisAnly	Lotaris	日本語	http://static.onlotaris.com/isv/common/doc/LOTARIS_PP_V1.1_JP.pdf
31	MAIST	アキナジスタ株式会社	日本語	http://www.maist.jp/policy/index.html
32	mdotmAd	MdotM	英語	http://mdotm.com/privacy-notice/
33	mediaLetsAd	Medialets, Inc.	英語	http://www.medialets.com/privacy/
34	medibaAd	株式会社 mediba	日本語	http://medibaad.com/privacy/
35	MicroAd	株式会社マイクロアド	日本語	http://www.microad.co.jp/utility/privacy.php
36	Mobclix	Mobclix	英語	http://www.mobclix.com/privacy.html
37	mobfoxAd	MobFox	英語	http://www.mobfox.com/privacy
38	mopubAd	MoPub Inc.	英語	http://www.mopub.com/legal/mopub-ads-privacy-policy/
39	nend	株式会社ファンコミュニケーションズ	日本語	http://www.fancs.com/privacy
40	omiture	Adobe Systems Inc.	日本語	http://www.adobe.com/jp/privacy.html
41	OpenXadserver	OpenX	英語	http://www.openx.com/about/privacy-policy
42	ormma	ORMMA .org	日本語	http://www.google.com/policies/privacy/
43	poncan	株式会社ドリコム	日本語	http://www.drecom.co.jp/privacy/
44	rhythm	Rhythm NewMedia Inc.	英語	http://rhythmnewmedia.com/privacy-policy/
45	smartiAd	株式会社アイメディアドライブ	日本語	http://i-mdrive.co.jp/privacy/
46	SponsorPay	SponsorPay	英語	http://sponsorpay.com/
47	tapitAd	TapIt	英語	http://jp.tapit.com/privacy-policy/
48	Tapjoy	Tapjoy, Inc.	英語	http://info.tapjoy.com/about-tapjoy/privacy-policy/
49	tremorAd	Tremor Video	英語	http://www.tremorvideo.com/about-us/privacy/
50	w3iAd	W3i Mobile Solutions, LLC(nativeX)	－	－
51	yahooAd	Yahoo! JAPAN	日本語	http://advertising.yahoo.co.jp/ad/privacy/
52	Yicha	株式会社　YICHA	－	－
53	ZestADZ	ZestADZ(a division of komli)	英語	http://www.komlimobile.com/static/komli_static/privacy
54	zucksAd	株式会社Zucks	日本語	http://zucks.co.jp/privacy/

（※第 10 回ＷＧ資料より）

（別紙）

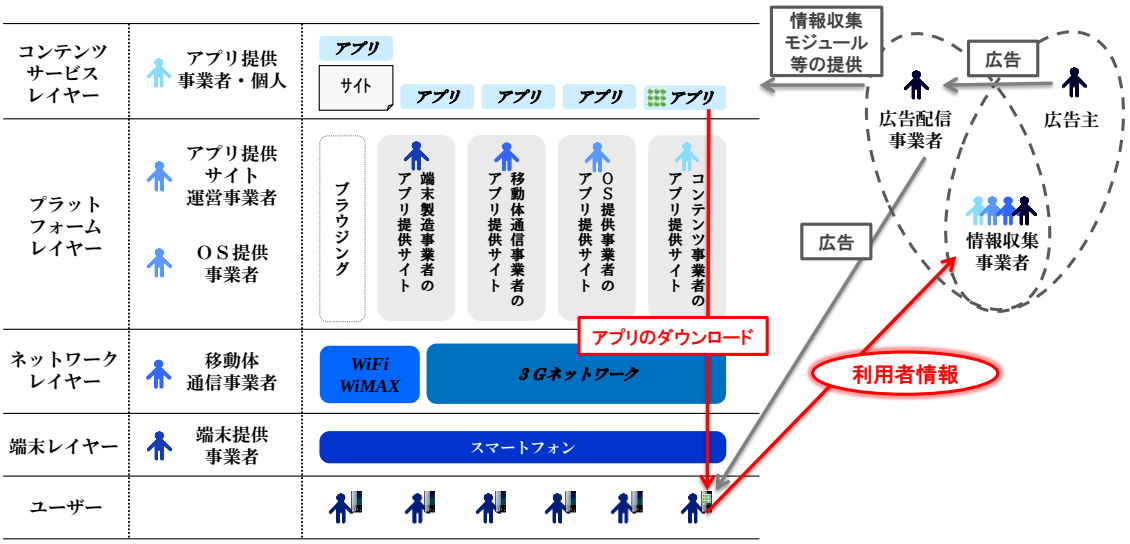
スマートフォン プライバシー ガイド

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」としてとりまとめました。

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。

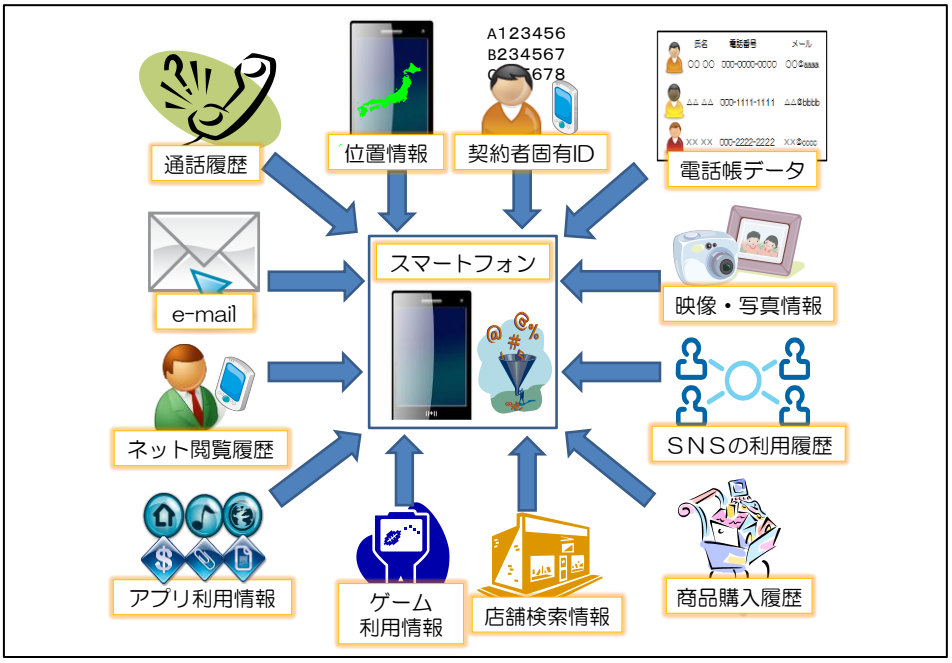
【スマートフォンのサービス構造】



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（パーミッション）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】

【利用者情報の利用許諾画面の例】 【アプリ提供サイト上でのプライバシーポリシー表示例】

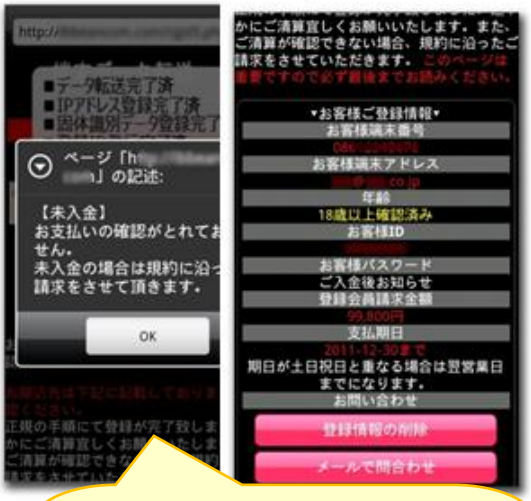
（※Google Play 及び App store から入手したアプリをもとに総務省作成）

最近の注意すべき事項

1　不正アプリの増加と多様化

- スマートフォンの急速な普及に伴い、**不正アプリも増加、多様化**しています。
- 例えば、動画を再生するアプリケーションに見せかけ、インストールするとメールアドレス・電話番号等の個人情報を取得し、料金請求画面を出して**金銭詐取を目的とするワンクリックウェア**が 2012 年1月以降報告されています。

ワンクリックウェアの例



- ワンクリックウェアをインストールしてしまった場合、**慌てず端末から削除**し、利用しないようにしましょう。
- **身に覚えのない請求**の場合、執ような請求があっても、**決して支払わないように**しましょう。

- また、人気ゲームを動画で紹介するアプリケーションが、利用者の電話帳情報を外部に送信していた事例がありました。
- 2012 年 8 月以降、「Power Charge」、「電池長持ち」、「電波改善」、「app 電話帳リーダー」、「無料電話」などスマホの機能改善ツールを、9 月には「安心ウイルススキャン」というセキュリティソフトや「SUN POWER」、「電池持ち改善」、「電波改善！」という**機能改善ツールを装ったアプリケーションに偽装し、電話帳情報など利用者情報の詐取を目的とするアプリ**なども増加しています。

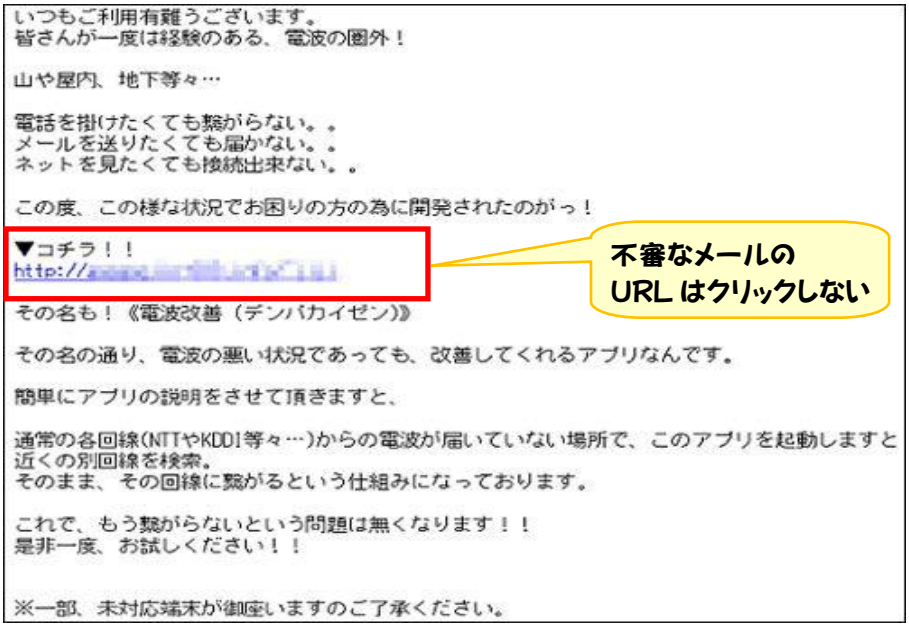
偽装したアプリの例

- インストールすると、お使いのスマートフォン**電話帳のデータが外部転送される可能性**があります。
- 下記２．３の事項に注意して、**インストールしないように注意**しましょう。（セキュリティベンダー等が最新の情報について発表する場合もあります。）

2　不審なメールやSNSなどに記載されたURLからアプリをダウンロードしないように注意しましょう

- 「電池長持ち」、「電波改善」等の機能改善ツールを装ったアプリケーション、「安心ウイルススキャン」というセキュリティソフトの多くは、**利用者に対して不審なメール**が送られ、**メールを通じ不正アプリの配布サイトへ誘導**する事例として報告されています。

- 不審なメールを受けとっても、記載されたURLをクリックして、**信頼性が確認されていないアプリの配布サイトからアプリをダウンロードしないように注意**しましょう。



不正アプリに誘引する手段の例

- また、SNSを利用して拡散するアプリケーションも報告されています。SNSの投稿などに記載されたURLをクリックして、**信頼性が確認されていないアプリの配布サイトからアプリをダウンロードしない**ように注意しましょう。

不正アプリに誘引する手段の例

3　電話帳を外部に送信する利用許諾（パーミッション）を使う場合には注意しましょう

✓ 「電池長持ち」、「電波改善」等の機能改善ツールを装ったアプリケーション、「安心ウイルススキャン」というセキュリティソフトの多くは、**利用者のスマートフォンから、電話帳のデータを外部に送信**していたことが事例として報告されています。

> 電話帳を外部に送信する場合、「スマートフォン　プライバシー　イニシアティブ」では、使用目的を示して個別にポップアップ等で分かりやすく示して同意をとることを推奨しています。ただし、これらの不適正なアプリでは、電話帳取得に関する個別のポップアップ等による同意取得はありませんでした。

✓ **アプリケーションの提供するサービスには明らかに不要**であるにもかかわらず、次のような**電話帳を外部に送信し得るパーミッションを取得**しようとするアプリケーションがあった場合には、**十分注意**しましょう。

> **①　個人情報-連絡先データの読み取り**
> **②　ネットワーク通信-インターネットアクセス**

パーミッション取得確認の画面の例