

スマートフォンの利用者情報を巡る課題と最近の動向

～(1)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～

平成25年1月22日
事務局

1 「スマートフォン利用者情報等取扱指針」の推進フォローアップ

- ① 業界団体等の取組：各々の**業界団体の取組の進捗状況**、業界ガイドライン、**アプリケーション提供者への情報発信**、画面の工夫等に関する関係者による取組の現状等の確認
- ② アプリケーション提供者等の取組：**アプリ・プライバシーポリシー(APP)**や情報収集モジュール単位の**プライバシーポリシーの策定状況、内容、インセンティブ**等
- ③ 利用者及び専門家の取組：**通報窓口**の整備、通報について専門家が事後的に審査し改善を求める仕組みの検討
- ④ 利用者の認識向上：**ユーザーの現状認識**の状況の調査、利用者情報の取扱いに関する**消費者への注意喚起**の徹底
- ⑤ フォローアップの体制の明確化：現状把握を含む継続的なフォローアップのための体制の明確化

2 第三者におけるアプリ検証、プライバシーに係る課題解決

- ① アプリ・プライバシー・ポリシー（APP）の表示方法：利用者が必ず読めるような仕組み、**表示方法の工夫**
- ② 第三者によるアプリ検証：
 - ・ 検証の主体：**様々な民間サービス**が提供され優良事業者の差別化と利用者保護に寄与することを期待、**各機関の検証範囲**の明確化、認証の**費用負担方法**
 - ・ 検証の方法：**APPの確認方法、技術的確認方法**において留意すべき点、第三者検証の適正性の担保方法
- ③ 表示方法：**検証結果の表示方法、ホワイトリスト・ブラックリスト**の可能性、アプリ提供サイトへの記載
- ④ 一般利用者の支援：オプトインの意味、指針への適合性、第三者検証等を**自ら理解・判断するための資料作成・周知**
- ⑤ 不正・悪意のケースへの対応：不正なアプリの自動識別・削除、**通報窓口**、通報結果の第三者審査、厳正な法執行等

3 その他

- ①利用者啓発：アプリ利用者によるプライバシー侵害の可能性(盗撮・電話帳等)、**利用者啓発の重要性**
- ②**児童の情報**とそれ以外の人の情報に対する配慮の違い
- ③**情報収集モジュール**等の扱いに関する横断的整理
- ④**国際的連携**：**海外事業者と日本事業者の取組**のバランス、海外におけるルール形成との連携、海外の同種の取組の調査把握。

(参考資料)

1 国内における動向

(1) 「スマートフォン利用者情報等取扱指針」 の推進フォローアップ

(2) 第三者におけるアプリ検証、プライバシーに 係る課題解決

2 海外における動向

3 参考資料



- 利用者情報に係る利用者の不安解消は、一義的に関係事業者の役割と責任においてなされるべき。
- 業界団体未加入のアプリ提供者も含め多様な関係事業者が直接参照できる指針を提示。各業界団体が業界の実情を踏まえ、追加的事項を盛り込んでガイドラインを作成することも期待される。

6つの基本原則

- ① 透明性の確保
- ② 利用者関与の機会の確保
- ③ 適正な手段による取得の確保
- ④ 適切な安全管理の確保
- ⑤ 苦情・相談への対応体制の確保
- ⑥ プライバシー・バイ・デザイン

利用者情報取得者における取組

(アプリ提供者、情報収集モジュール提供者等による取組)

(1) プライバシー・ポリシーの作成

☞ アプリケーションや情報収集モジュールごとに分かりやすく作成。(簡略版も作成。)

- ① 情報を取得するアプリ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

(2) 適切な安全管理措置

(3) 情報収集モジュール提供者に関する特記事項

(4) 広告事業者に関する特記事項

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

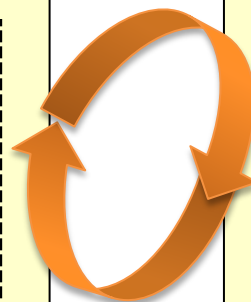
- ☞ スマートフォン販売時等
- ☞ 移動体通信事業者のアプリケーション提供サイト

(2) アプリ提供サイト運営事業者、OS提供事業者

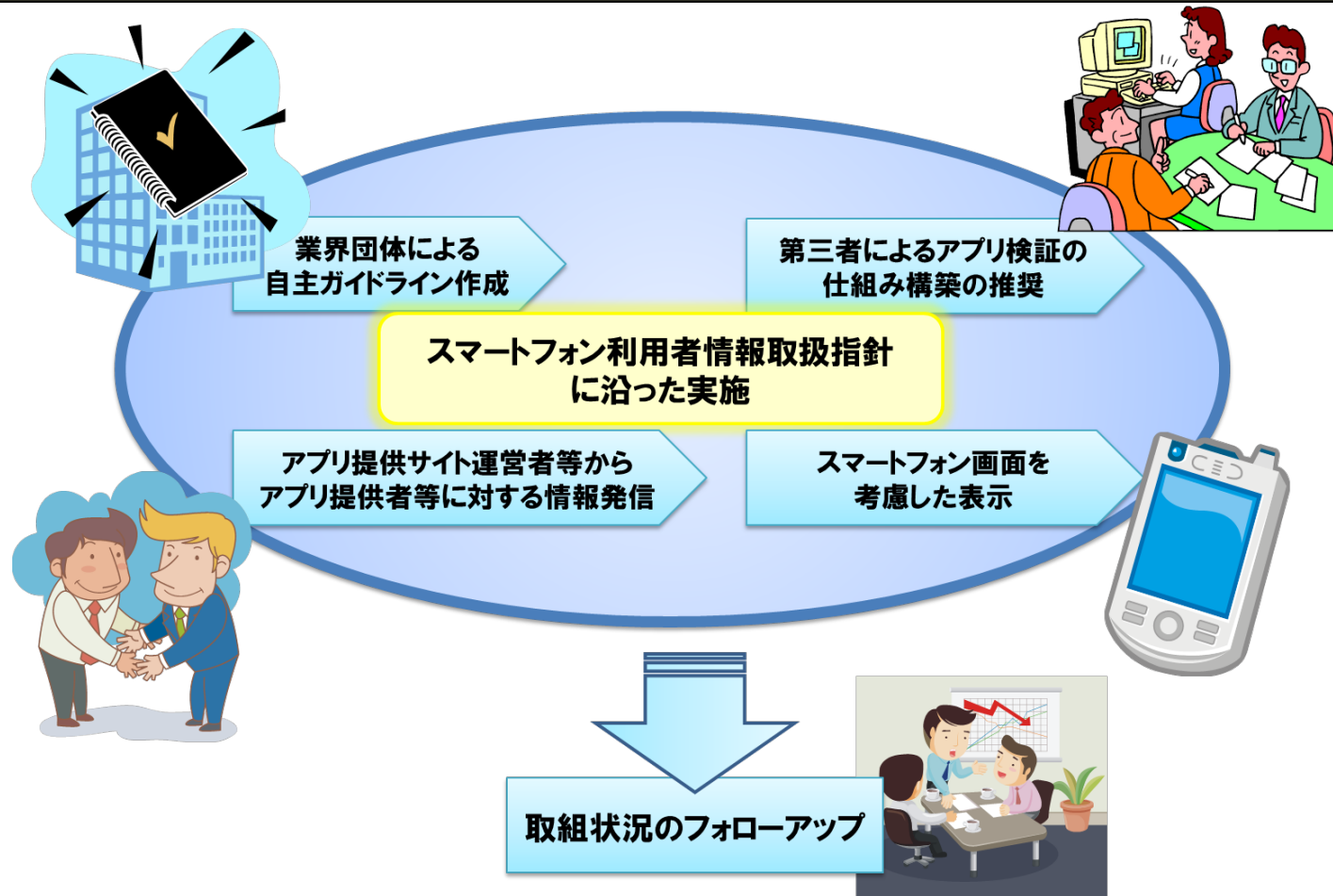
- ☞ アプリケーション提供サイト

(3) その他関係しうる事業者

- ☞ アプリケーション推薦等



「スマートフォン利用者情報取扱指針」については、関係事業者等が直接参照して適切な対応を行うほか、以下のような実効性向上のための取組が考えられる。



- 事業者・業界団体自身による取組状況のフォローアップと公表
- 本指針を踏まえた事業者・業界の取組状況をICT諸問題研等の場において一定期間後にフォローアップ
- 新たな技術・サービスへの柔軟な対応

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 モデルプライバシーポリシー及び業界ガイドラインに関する情報交換、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 等

(具体的な活動例)

- ・スマートフォンの安心・安全な利用に向けた取組の説明 (IPA、アンドロイダー等)
- ・業界ガイドライン、モデルプライバシーポリシーの作成状況の説明 (MCF)
- ・アプリケーションに関する技術的検討状況の説明 (JSSEC)
- ・情報発信: スマートフォンの利用者情報等に関する連絡協議会のホームページ (<http://jssec.org/spsc/index.html>)

2 参加メンバー

(1) 構成員:

- 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係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准教授【議長】 森亮二 弁護士法人英知法律事務所弁護士【副議長】

(2) 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 (予定)

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。

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の作成方法についても提示。

ソフトウェア開発会社であるタオソフトウェア(株)は、平成24年10月、「スマートフォン プライバシー イニシアティブ」のAndroid開発向け解説と具体的手順を記載した「Androidスマートフォンプライバシーガイドライン by タオソフトウェア」を公表。

第1章 はじめに

第2章 スマートフォン プライバシー イニシアティブドキュメント

第3章 アプリケーションの実装(個別同意取得ダイアログ)

第4章 プライバシーポリシー作成(ドキュメントワーク)

第5章 プライバシーポリシー記載方法

第6章 プライバシーポリシーサンプル

(※利用者情報を取得する場合、情報収集モジュールを組み込む場合等に分けて例示)

第7章 まとめ

第8章 AppenDix

- 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/kamigyoo/page/0000109403.html>

プライバシーポリシーへの記載事項

項目	スマートフォン プライバシー イニシアティブ	モデル・プライバシーポリシー(MCF)
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名称	アプリケーション提供者等の名称、連絡先等	アプリケーション提供者名、アプリケーション名、連絡先を記載(連絡先は⑦を参照可能)
②取得される情報の項目	取得される利用者情報の項目・内容を列挙	②の情報の項目を利用目的(④)が分かるように記載
③取得方法	利用者の入力によるものか、アプリによるスマホ内部からの自動取得か記載	アプリケーション経由で自動的に取得するのか、利用者が登録するか記載
④利用目的の特定・明示	アプリ自体の利用者に対するサービス提供の目的/それ以外の目的(例:広告配信・表示やマーケティング目的のため)	具体的なサービス内容の提供目的、性能向上、広告表示等の別を記載
⑤通知・公表または同意取得の方法、利用者関与の方法	プライバシーポリシーの掲示場所や掲示方法、同意取得の対象・タイミング等*1、利用者関与の方法*2	個別情報に関する同意取得の方法情報の第三者提供を行う場合の同意取得の方法等について記載
⑥外部送信・第三者提供・情報収集モジュールの有無	第三者提供・情報収集モジュールの組み込みの有無等	第三者提供を行う情報の項目、同意情報収集モジュールに係る情報(提供会社、情報項目、目的、第三者提供等)を記載
⑦問合せ窓口	問合せ窓口の連絡先等(電話番号、メールアドレス等)	お問合わせフォーム、電話、メール等連絡先を記載
⑧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の変更を行った場合の通知方法	通知もしくはあらためて同意を取得

*1 個別の情報に関する同意取得: :一部のプライバシー性の高い情報(電話帳、位置情報、通信履歴、写真等)は、原則個別同意を取得
契約者・端末固有ID: 個人情報に準じた形で取り扱う(取得される項目及び利用目的を明確に記載しその目的の範囲で適正に扱う)

*2 利用者関与: 利用者がアプリによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載する。

(構成員限り)

(参考資料)

1 国内における動向

(1) 「スマートフォン利用者情報等取扱指針」
の推進フォローアップ

(2) 第三者におけるアプリ検証、プライバシーに
係る課題解決

2 海外における動向

3 参考資料

スマートフォンのアプリ評価検証について

「スマートフォン利用者情報取扱指針」の実効性向上のために、アプリケーションのプライバシーポリシーを普及させるとともに、アプリケーションのプライバシーポリシー等に表示された内容が正しいのかどうか等について、専門的知識を有する第三者が検証し、その結果を提供できる仕組みを検討することが提言されている。

《必要と考えられるアプリの第三者検証》

アプリケーションの安全性をチェックし、スマートフォンの安心安全な利用環境整備に資するため、**第三者が個々のアプリについて**、利用者やアプリ提供者からの申請をふまえ、

- ① **適切なアプリケーションのプライバシー・ポリシーが策定**されているか
- ② アプリケーションの**プライバシー・ポリシーに沿った運用が行われているか**
(プライバシーポリシー記載内容と実際の挙動の一致・不一致等)

を確認することが必要と考えられる。

具体的には、情報収集モジュールの有無・種類、外部送信される情報の内容確認等、**技術的解析**を行い、**行った結果を申請者等に伝えられる仕組み**を作ることが想定される。

【想定される利用事例】

- アプリ提供者が、**自らの提供するアプリがプライバシーポリシーと合致した動きをしている旨**、第三者によるお墨付きを得たい場合 ⇒ **ホワイトリスト作成**へ
- **プライバシーポリシーに表示された内容**（取得する情報、取得の目的、第三者提供の有無等）と**異なる挙動**をしていると疑われるアプリ等がある場合
⇒ 是正を働きかける。明かに**悪意のもの**の場合**ブラックリスト作成**へ



業界団体による
自主ガイドライン作成



第三者によるアプリ検証の
仕組み構築の推奨

アプリケーションのプライバ
シーポリシーの普及

安全安心なアプリの確認



1. 移動体通信事業者 (アプリ提供サイト運営事業者) による取組

	アプリ評価検証の現状
KDDI株式会社  (配信型)	<ul style="list-style-type: none"> ・ アプリ開発者から申請されたアプリについて、セキュリティ検査、プライバシー検査 (送信情報に関する確認) 等のアプリ審査を実施。 ・ 簡易なプライバシーポリシー作成ツールを提供
 SoftBank (紹介型)	<ul style="list-style-type: none"> ・ アプリ開発者に対し、コンテンツ提供規約 / 掲載ガイドライン等を提供

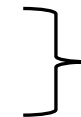
2. レビューサイト等による取組

① アン드로이드株式会社



- 利用者に対し安心なアプリについて一定の評価を与えるため、自社運営の**レビューサイトに掲載するアプリ**について、全て一定の基準で安全性の確認を行う

- ・ アプリ開発者の**実在性**を確認し、「公認デベロッパー」として認定
- ・ アプリの**パーミッションの正当性**を確認 + ウィルススキャンを実施



当該レビューサイトにおける
「公認アプリ」
 = 掲載アプリ

② 情報セキュリティ格付け制度研究会 (ISレーティング社)

- 総務省「スマートフォン プライバシー イニシアティブ」を活用し、経営者のコミットメントや体制、規程、目標、プライバシー・ポリシーといった**アプリ開発事業者のマネジメント・プロセス**を評価する**第三者証明書発行サービス**をパイロット運用予定 (アプリの動作確認等を含む格付けは今後検討)

3. 一般社団法人日本スマートフォンセキュリティ協会 (JSSEC) による取組

- アプリ解析技術タスクフォースにおいて、アプリケーション提供者から提供されたアプリ等について、
 ①**プライバシーポリシーの記載状況の読み解き**、②**実際の送信情報の検知**の両面について、複数社の参加による**トライアル**を行い、その結果について共有した。

スマートフォン安心・安全利用促進プログラム

- スマートフォンが急速に普及する中、利用者に対する必要な情報提供を推進し、プライバシーや情報セキュリティ面での課題に関係者が適切に対応し、利用者が安心・安全に利用できる環境を整備するため、総務省として以下の対策を総合的に推進する(平成24年9月公表)。

1 スマートフォンに関する総合的・重点的な周知啓発活動の全国展開

(1)関係事業者・団体、消費者団体、PTA等と連携した総合的な周知啓発活動の全国展開

- 提供する情報:スマートフォンに関する基本的事項、プライバシーに関する事項、情報セキュリティ対策
青少年・保護者や高齢者が知っておくべき事項
- 具体的な取組:①分かりやすい資料等周知啓発素材の開発と活用 ②様々なメディアの活用による総合的な周知啓発活動

(2)特にスマートフォンの普及が著しい高校生を対象とした重点的な周知啓発活動の実施

- ①高等学校PTA連合会等との連携による重点的な周知啓発活動 ②地域における推進体制の構築支援

2 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の支援

関係事業者が過去の研究会の検討成果を踏まえた対応を図り、安心・安全な利用環境が整備されるよう、取り組む。

(1)関係事業者の対応の促進

- 関係事業者・団体によるスマートフォン利用者情報取扱指針に沿った業界ガイドラインやプライバシーポリシーのモデル例の作成支援
- 関係団体によるアプリケーション提供サイト運営者等への働きかけやアプリケーション開発を取り扱う専門学校等への情報提供に対する必要な協力

(2)第三者によるアプリケーション検証の仕組みの検討への協力

3 青少年・高齢者の安心・安全な利用環境の整備

スマートフォンが青少年や高齢者にも急速に普及しつつある現状を踏まえ、必要な利用環境整備を促進する。

(1)青少年に対する利用環境整備

- ①スマートフォンのフィルタリングの改善 ②青少年のインターネットリテラシーに関する指標(ILAS)の作成・活用

(2)高齢者に対する利用環境整備

- ①契約に関する基本的情報の丁寧な提供促進 ②高齢者を意識した周知啓発活動の支援

スマートフォン関係の政府広報

特集 スマートフォンの安全な使い方

スマートフォンってどんなもの？

スマートフォンの利用が、幅広い世代の人に急速に広がっています。大きな画面でインターネットをスムーズに利用できるなど、多彩な機能が便利なスマートフォンでは、従来の携帯電話とは、いろいろな点で大きく異なっていることをご存じですか？

これまでの携帯電話と同じだと思って使っていると、思わぬトラブルに出くわすことも……。ここでは、スマートフォンの性質や、利用にあたっての注意事項をまとめました。

ツール：電話の機能もベースにして、パソコンの機能をベースにして、電話機能も取除かれる。アプリインストールすることで機能の追加が可能。

画面：ほとんどのスマートフォンより画面が小さい。

操作：数字のボタンを押して操作する。画面も操作するタッチパネル方式。

インターネット：携帯サイズに特化、パケット向けサイトは多い。

メール：これまでのSMSに加え、画像も送れるMMSが使用可能。

電話：ここが従来の携帯電話と異なる点。

ワンセグ・赤外線・決済機能：日本独自の機能もあり、ほとんどの携帯電話にはない。

出典：総務省広報誌4月号 MIC April 2012

総務省広報誌4月号

スマートフォンの中にある大切な情報を守るために

スマートフォン プライバシーガイド

スマートフォンは多種多様なアプリをダウンロードして利用することができますが、それには利用者の個人情報を守るための注意が必要です。スマートフォンを安心して利用するために、心当たりがない点を確認しましょう。

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さまざまな利用情報が蓄積されます。アプリによってはこれらの情報が不正に第三者に提供される場合があります。

事前に、アプリの信頼性に関する情報を入手し、理解するように努めましょう。

3 利用者情報の許諾画面等を確認しましょう

アプリの信頼性の確認は、利用者情報などの必要も同様であるため、必要以上に収集されていないように確認してください。

アプリのインストール時や利用時（起動）する時点で、収集する利用者情報に関する利用許諾を求められる画面が表示されます。この画面を確認し、必要な情報を提供することを確認してください。

出典：総務省広報誌6月号 MIC June 2012

総務省広報誌6月号

政府インターネットテレビ

スマートフォンを安心して使うために！～守ろう 情報セキュリティ3か条

安心・安全にスマートフォンをご利用ください！

番組一覧表

字幕OFF せひ 安心安全にスマートフォンをご利用ください！

政府インターネットテレビ

スマートフォンを安心して使うために！
<http://nettv.gov-online.go.jp/prg/prg6690.html>

政府広報オンライン

暮らしに役立つ政府広報ポータルサイト

トップ 特集 お役立ち情報 各府県からのお知らせ 政府広報

お役立ち情報

国の行政施策の中から、暮らしにかかわりの深いテーマ、暮らしに役立つ情報型ピックアップ、分かりやすくまとめて提供しています。

スマートフォンを安心・安全に使うために情報セキュリティ対策をしましょう

平成24年7月27日掲載

OutLine

- インターネット利用に伴うスマートフォンは、従来の携帯電話とは違っています。パソコンと同様、利用者自身の情報セキュリティ対策が必要です
- 実際に、ウイルスに感染したり、電話帳のデータを不正に抜き取られるなどの被害が出ています

スマートフォンを安心・安全に使うために
情報セキュリティ対策をしましょう
<http://www.gov-online.go.jp/useful/article/201207/2.html>

電気通信サービス Q&A

知っているれば安心! 便利! 電気通信サービス

スマートフォンってなに?

携帯電話 スマートフォン

インターネット

困ったことも知りたいことも、わたしたちがお答えします!

電気通信サービスの電話サービス

電気通信サービスQ&A

(参考資料)

1 国内における動向

(1) 「スマートフォン利用者情報等取扱指針」
の推進フォローアップ

(2) 第三者におけるアプリ検証、プライバシーに
係る課題解決

2 海外における動向

3 参考資料

2012年2月23日、ホワイトハウスが、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、政策大綱を発表。なお、政策大綱で示す「消費者プライバシー権利章典」は、明確な消費者保護のベースラインとなると共に、企業にとってもより確実性を与えるものであるとしている。また、ホワイトハウスは、利害関係者に、マルチステークホルダープロセスにより策定された「行動規範」を通じて権利章典を実行し、その後、連邦議会と共に、これらの権利を法制化するよう作業することとしている。

4つの重要事項(Key elements)

I. 「消費者プライバシー権利章典」(A Consumer Privacy Bill of Rights)

- 1 個人による管理 : 消費者は、自分の個人データを企業が収集し、それを使用する方法について管理する権利を有する。
- 2 透明性 : 消費者は、プライバシー及びセキュリティの企業実務に関する情報に容易に理解しアクセスできる権利を有する。
- 3 経緯の尊重 : 消費者は、企業が、自分の個人データを、自分が情報を提供した経緯に沿う方法で、収集、使用、開示することを期待する権利を有する。
- 4 セキュリティ : 消費者は、個人データを保護し、責任持って処理する権利を有する。
- 5 アクセス及び正確性 : 消費者は、使用可能な形式で、また、データの機微性及びデータが不正確であった場合に消費者に悪影響を与える危険度に応じた方法で、個人データにアクセスし訂正する権利を有する。
- 6 対象を絞った収集 : 消費者は、企業が収集及び保持する個人データに合理的な制限を設ける権利を有する。
- 7 説明責任 : 消費者は、この権利章典の遵守を保証するための適切な措置を講じる企業によって個人データが処理される権利を有する。

II. 執行可能な行動規範を策定するための、関係者間のプロセスの強化

- 政府は、今後、行動規範を策定するため、オープンで透明性のある会合を開催し、行動規範について議論することとしている。
- 行動規範を採用するかどうかは企業の最終判断に委ねられる。ただし、遵守を公言した企業が違反した場合、連邦取引委員会(FTC)は行動規範に基づき、執行することができる。

III. 連邦取引委員会(FTC)の執行能力の向上

- FTCは、企業に対する調査や執行において、当該企業の行動規範への遵守を評価すべき。

IV. 国際的な相互運用性の促進

- ユーザー本位及び分散的なインターネット環境では、個人情報のため、整合性のとれた、低い障壁のルールが必要。
- 国際的な相互運用性については、①相互認証及び②執行協力の2原則を提示。

- ホワイトハウスの政策大綱※の中で掲げられた「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、NTIA(米国商務省・国家電気通信情報庁)はマルチステークホルダー会合を開催(企業、業界団体、消費者団体等が出席し各者がそれぞれの立場から自由に発言)。
- 2012年3月に実施したパブリックコメントの結果を踏まえ、NTIAは「モバイル・アプリの透明性」に関する行動規範をまず策定することとし、マルチステークホルダー会合2012年7月12日から2013年1月17日までに計8回開催。(今後4回の会合(2013年1月31日、2月21日、3月14日、4月4日)が予定されている。)

会合回数	開催日	概要
第1回	2012年7月12日	参加者が自由に発言を行い、これら意見について挙手により重要度の記録を行った。
第2回	8月22日	本会合の運営方法等手続き面について議論が行われた。
第3回	8月29日	第1回会合で多くの指示を集めた意見の紹介がNTIAより行われ、追加の意見募集が行われた。ワーキンググループの設置や事業者からの技術的なブリーフィングの必要性につき議論された。
第4回	10月16日	<ul style="list-style-type: none"> ・行動規範ドラフト: 法律事務所Venableが作成した行動規範の討議ドラフトを一部修正して当面用いることを決定。 ・次の2つのサブグループを設置して作業を進めることを決定 <ul style="list-style-type: none"> ①個人が特定される可能性のあるモバイル・アプリが利用するデータ構成要素・機能リスト、②簡略な告知開発
第5回	11月7日	<ul style="list-style-type: none"> ・行動規範ドラフト: Venable案、Center for Democracy & Technology(CDT)等の案の双方を議論 ・データ構成要素・機能のリスト作成: 競争的テクノロジー協会(ACT)とTRUSTeが作成したリストの説明を実施 ・簡略な告知の開発: 簡略な告知に何を含めるべきか、簡略な告知が有効かどうかの評価が検討課題とされた
第6回	11月30日	<ul style="list-style-type: none"> ・行動規範ドラフト: 3つの討議ドラフト(①Venable+CDT/Future of Privacy Forum(FPF)、②Consumer Federation America(CFA)、③アプリ開発者協会(ADA))が発表され議論が行われた ・簡略な告知の開発: ①TRUSTe(Mozillaアイコン)、②Association for Competitive Technology(ACT)(プライバシーダッシュボード)、③ADA/米国市民的自由連合(ACLU)/World Privacy Forum(WPF)等(簡略な告知モデル)を説明
第7回	12月17日	<ul style="list-style-type: none"> ・行動規範ドラフト: アプリ開発者協会(ADA)他団体による討議ドラフトについて、アジェンダに列挙された質問項目に沿って議論。これらの結果が次回会合のアジェンダに反映される予定。 ・簡略な告知の開発: ①ACT(プライバシーダッシュボード)、②ADA等団体(簡略な告知モデル)について議論
第8回	1月17日	<ul style="list-style-type: none"> ・行動規範ドラフトについて、拘束力はないが覚書として重要との意見を明記するとともに、金融情報、健康情報等のセンシティブ情報について、それらに含まれる内容の詳細を明記。また、第三者との情報共有が通知なく実施可能な場合についても追記。

※:「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:グローバルデジタルエコノミーにおけるプライバシー保護及びイノベーション促進に向けた枠組み」

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)

2012年11月29日付けのアプリ開発者協会(ADA)他団体(参考)による討議ドラフト「モバイルアプリの自主的透明性向上画面(VTS)」について、アジェンダに列挙された質問項目に沿って議論が行われ、項目ごとに表現の見直しや削除、議論の継続といったことが決定された。

(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)
 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)

モバイルアプリの自主的透明性向上画面(VTS: Voluntary Transparency Screen)

I アプリケーションの透明性に向けた導入及び原則

- モバイルアプリの自主的な透明性向上画面(VTS)は、簡略化された通知であり、モバイルアプリ提供者により導入されることにより、アプリケーションの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。利用者情報の取扱いの点から各アプリを比較した上で選択可能とする。VTSを通じた透明性の確保は利用者の信任につながる。
- 原則
 - ・アプリ提供者は、アプリ産業の成長のために重要である利用者の信任を得られるように努力
 - ・アプリのバージョンアップにより利用者情報の取扱いが変わる場合には説明も変更する
 - ・簡略版通知によってアプリの透明性と利用者の理解が向上するようにしなければならない
 - ・業界として共通化された取組を推進
 - ・この行動規範に拠るアプリ開発者は、ベストプラクティスを実施しているということになる 等
 →拘束力はないが覚書として重要という意見を明記。



II 簡略版通知への記載事項

(1) 利用者から取得される情報

例: 電話帳、利用履歴(ブラウザー利用)、位置情報、金融情報、年齢、バイオメトリックス、健康情報、他のアプリからのデータ等
 →金融情報、健康情報等のセンシティブ情報について、詳細を明記。

(2) 第三者との情報共有

例: 広告ネットワーク、通信事業者、プラットフォーム、ソーシャルネットワーク等
 →社内の他部署との情報共有、第三者との間の契約でサービス提供に必要な範囲に用途が限定されている場合や更なる第三者との共有が禁止されている場合等については、明示しなくとも構わない旨を追記。

(3) 新しいタイプの情報取得や情報共有

III 簡略版の記載方法(デザイン)

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

※簡略版の通知は、法的に求められるデータ利用・利用条件、又は全体版プライバシーポリシーへのリンクを提供すること。
 これらのリンクは、利用者がデータ消去を求める方法に関する説明を含む。

TRUSTeによるMozillaアイコンの紹介

Overview **Icons** Sites

We developed the privacy icons in partnership with a [Mozilla-led working group](#), the images were designed by [Ocupop](#). The icons are a work in progress — [share your feedback](#) or [start our forum](#). Or, you can [start](#)

利用範囲 (Expected Use) **第三者提供 (Third Party Sharing)** **法執行機関への提供 (Sharing with Law Enforcement)** **データ保存 (Data Retention)**

限定的再利用 (limited Reuse) →

意図された利用のみ (Intended Use Only)

Hover over an icon to read their definitions.

The image shows a row of nine icons: 1. A person with a downward arrow (Expected Use). 2. A person with an upward arrow (Third Party Sharing). 3. A dollar sign with an upward arrow (Sharing with Law Enforcement). 4. A dollar sign with a circular arrow (Data Retention). 5. A shield with a star and upward arrow (Sharing with Law Enforcement). 6. A shield with a star and circular arrow (Data Retention). 7. A calendar icon with the number 3. 8. A calendar icon with the number 18. 9. A calendar icon with an infinity symbol. Red circles highlight the first four icons. A red arrow points from the text '限定的再利用 (limited Reuse)' to the first icon. Another red arrow points from the text '意図された利用のみ (Intended Use Only)' to the second icon.

ACT(競争的テクノロジー協会)による「プライバシー・ダッシュボード」案

PRIVACY DASHBOARD
Short form Full policy

DATA ACCESSED

USER	SENSITIVE	USAGE	LOCATION	CONTACTS	PHOTOS
YES	YES	YES	YES	NO	YES

DATA SHARING

ANALYTICS	ADS	SOCIAL
YES	YES	YES

The image shows a 'PRIVACY DASHBOARD' with two sections: 'DATA ACCESSED' and 'DATA SHARING'. Each section contains icons for different data types and their status (YES/NO). A red circle highlights the 'PHOTOS' icon in the 'DATA ACCESSED' section, with a red arrow pointing to the right towards the next screenshot.

Back PHOTOS AND FILES

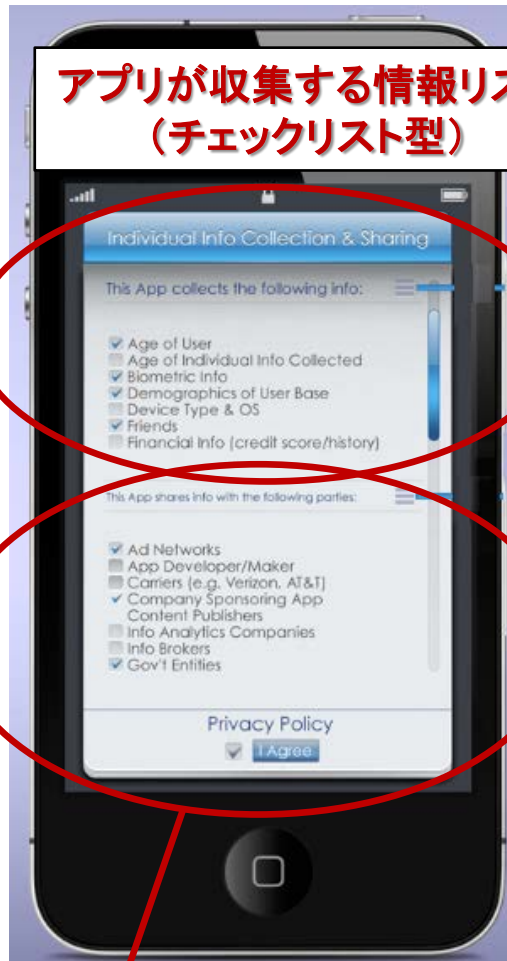
This app can access the photos and files stored on the device. This data includes:

- PHOTOS - This app accesses the photos you have stored on your device.
- FILES - This app accesses the documents and other files that are stored on your device.

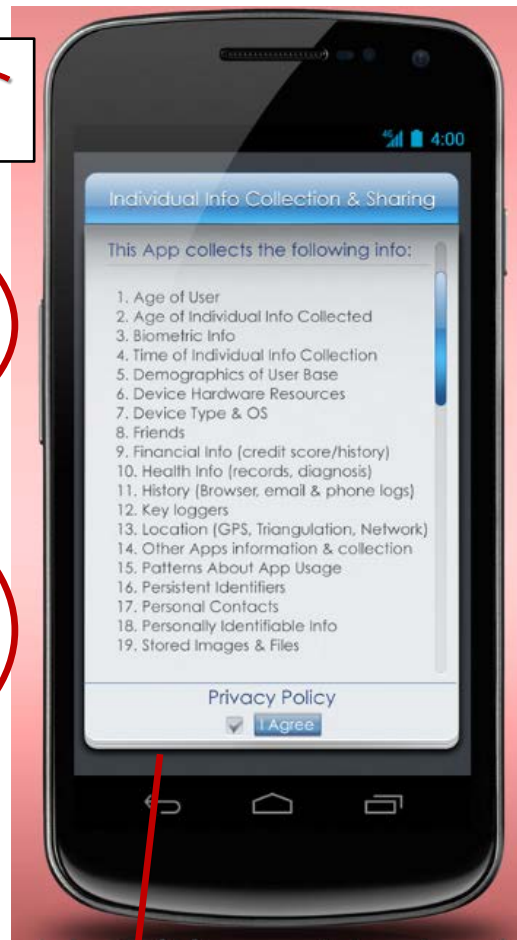
The image shows a mobile app interface with a 'Back' button and a 'PHOTOS AND FILES' header. A red circle highlights the notification text, and a red arrow points from the 'PHOTOS' icon in the previous screenshot to this notification.

ADA他による簡略な告知画面案

アプリが収集する情報リスト (チェックリスト型)



アプリが情報を
シェアする第三者
(チェックリスト型)



アプリが収集する情報リスト
(リストアップ型)

(ブラックベリー・カテゴリ別型)



アプリが収集する情報

アプリが情報をシェアする第三者



アプリケーション提供サイト運営事業者6社

(アップル社、グーグル社、マイクロソフト社、リサーチ・イン・モーション社、アマゾン社、ヒューレッド・パッカード社)

※2012年6月にフェイスブック社も参加

共同声明 (2012年2月)

カリフォルニア州司法長官 カマラ・ハリス氏

アプリケーション提供者

提供

・当該アプリケーションに係るプライバシーポリシーを提示
(個人データの収集方法・利用目的・提供先を示す)

・サービス条件や法令に従わないアプリの通報方法の確保、
通報されたサービス違反や法令違反の事案へのレスポンス

アプリケーション提供サイト運営事業者

購入

・アプリケーション提供者が、アプリケーションを提出する際、当該アプリのプライバシーポリシーへのハイパーリンク又はテキストを提出可能とする

・利用者がアプリケーション提供サイトにて、**アプリケーション購入時前にアプリケーションのプライバシーポリシーを確認**できるようにする

消費者

司法長官と協力し、
・プライバシーに関するベストプラクティス、
・モデルプライバシーポリシーを開発することに取り組む

- 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。





- 2012年7月、Lookout社(米国のモバイルセキュリティ会社)が、主としてモバイル・アプリ向け広告提供者(Ad Providers)及びアプリ提供者(App Publishers)を対象として、プライバシーを保護すると同時に、オンライン広告の信頼性を確保することを目的として、個人情報の取扱い及びオンライン広告の在り方に関するガイドラインを公表。
- ガイドラインにおいては、広告提供者と一体的にサービスを提供する場合、利用者に対しては、アプリ提供者がプライバシー、セキュリティ及び使いやすさについて適切に周知する責務を有する旨を明示。

○ 主な内容

1. 透明性と明確性(Transparency and Clarity)

- ・ 収集したデータについて、アクセスしやすく、簡単に分かりやすく、平均的な利用者が選択しやすいような形で情報提供すべき。
- ・ モバイルアプリ向けプライバシー・ポリシー作成に合意するべき
- ・ 特定のデータについては、収集前にプライバシー・ポリシーを提示するのみでは十分ではなく、利用者からインフォームド・コンセントを得ることが求められる場合もある

2. 個人のコントロールの拡充(Enable Individual Control)

- ・ アプリ提供者は、利用者参加のツールを簡便に利用できるようにしなければならない。
- ・ 特にいつでも同意を取下げ、収集されたデータにアクセスできるようにしなければならない。



3. 新たな広告表示の際の背景説明及びコントロール(Ad Delivery Behavior)

- ・ 個々のアプリ外で表示される広告等、新たな方法で広告が表示される場合、利用者はその広告の出所やコントロール方法を知る権利がある。
- ・ 従って、①プッシュ型広告の場合、広告提供者はどのアプリの広告なのか明示しなければならず、②アプリ提供者は、デスクトップにプッシュ型広告のアイコンなどが作成される際には、事前に通知しなければならない。

4. 利用者端末からのデータ収集・保存の限定(Focused Data Collection)

- ・ 広告提供者は、利用者端末から収集するデータの収集・保存について、合理的な制限を設けるべきである。
- ・ 従って、広告提供者は、①不変の端末IDを用いずに、行動ターゲティング広告上同様の機能性を提供できる独立した／一時的な端末識別IDを用いるべきであり、また、②MSIやMSISDNといった加入者特定IDを収集すべきではない。

5. トランスポートレイヤーの暗号化及びフォワードハッシュ化(Enable Individual Control)

- ・ 端末固有ID等を収集する際には、広告提供者は当該IDをハッシュ化しなければならない。
- ・ メールアドレスや電話番号等個人情報の収集の際には、広告提供者はトランスポートレイヤーのセキュリティ(TLS/SSL)を利用しなければならない。

- 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

2011年12月モバイルマーケティングアソシエーション(MMA)は、アプリケーション開発者が消費者にプライバシーポリシーを伝えられるように「モバイル・アプリケーション・プライバシーポリシー」を発表。アプリケーション開発者がプライバシーポリシーを作る際の参考となるように作成。それぞれ記載事例を示している。(※実際の作成時には専門家への確認を推奨)

【モバイル・アプリケーション・プライバシーポリシーにおける記載項目】

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

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

- 対象: アプリケーションとモバイル端末に関連するプライバシーデザイン(アプリ開発者、機器製造事業者、プラットフォーマー、OS事業者、通信キャリア、広告や情報分析事業者など関連する全ての主体に適用)
- 目的: “Privacy by Design”アプローチを採用し、モバイル・アプリケーションの開発時にユーザーのプライバシーや個人情報の尊重や保護に関する確認の手助けとなること。
- 個人情報(Personal information): 個人に関連づけられた情報であり、個人を識別するために利用されるもの。ユニークな識別子を利用しても個人を識別することができる。

1 透明性とユーザーによる選択とコントロール(TCC)

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

2 データの保存とセキュリティ(DRS)

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

3 教育(E)

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

4 ソーシャルネットワークとソーシャルメディア(SNS)

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

5 モバイル広告(MA)

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

6 位置情報(L)

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

7 青少年(CA)

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

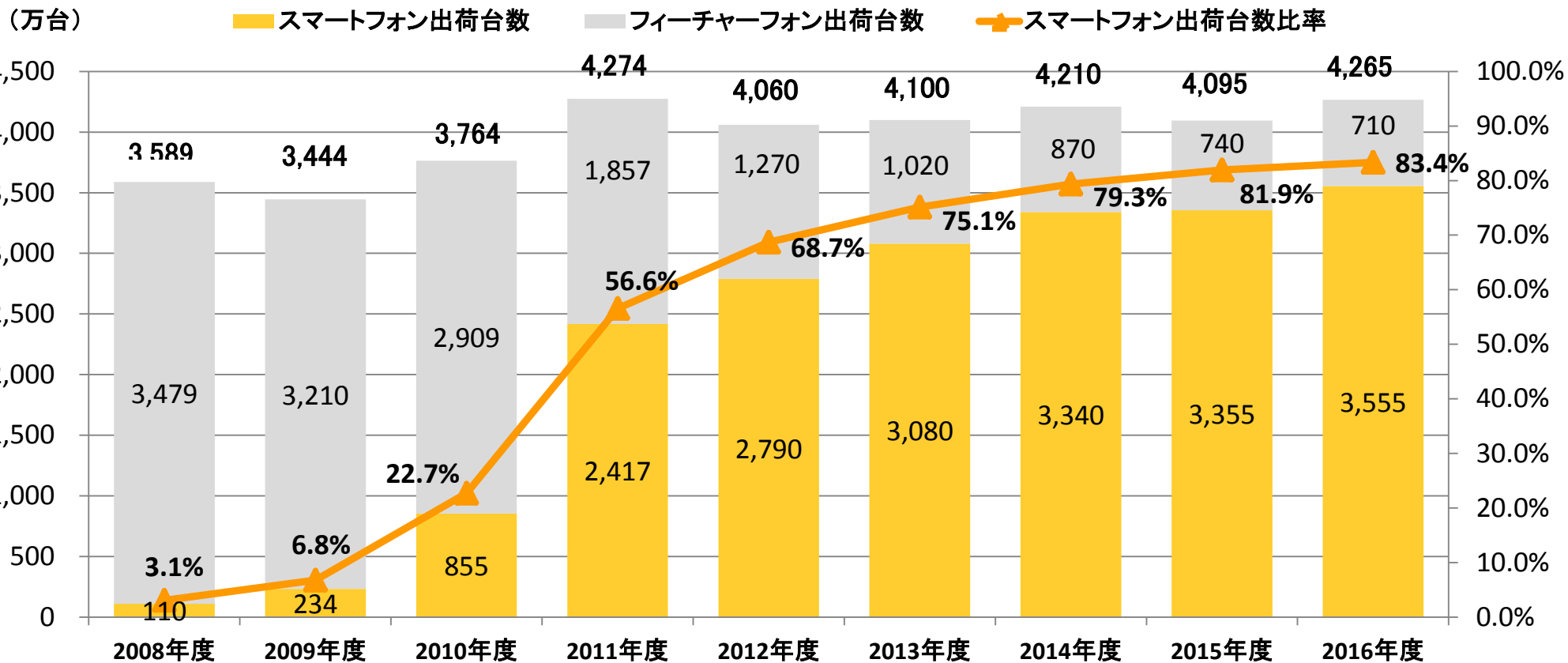
8 説明責任等(AE)

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

(参考資料)

- 1 国内における動向
- 2 海外における動向
- 3 参考資料

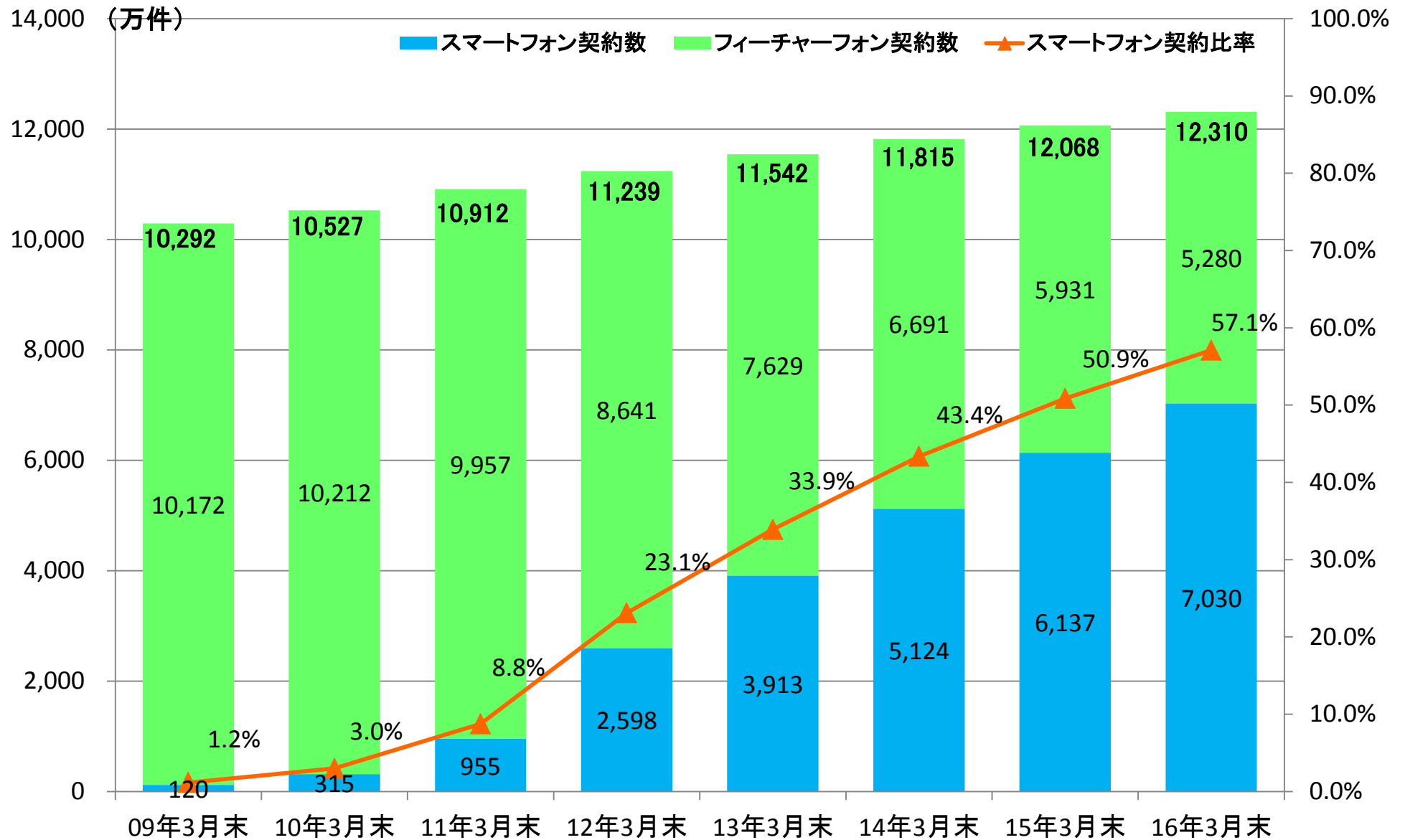
携帯電話端末の国内における年間出荷台数のうち、スマートフォンの占める比率が急速に上昇を続けており、2012年度には70%近くまで達するとの見通しもある。



(単位: 万台)

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

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



※ 株式会社MM総研調べ(11年度以降は予測値)

(「スマートフォン市場規模の推移・予測(11年7月)」(2011年7月7日)及び「2011年度上期国内携帯電話端末出荷概況」(2011年10月27日))

スマートフォンにおける利用者情報の収集事例①（カレログ）

サービス概要

スマートフォン端末の所在地等の情報を当該端末のGPS位置情報等を基に、サービス利用者（端末所有者以外の第三者も含め）がPCで遠隔で把握することができるサービス。



サービス提供システム（平成23年8月30日～10月上旬まで）

（1）登録方法



- ①「カレログ」をダウンロード
- ②スマートフォン端末より利用者登録を実施。

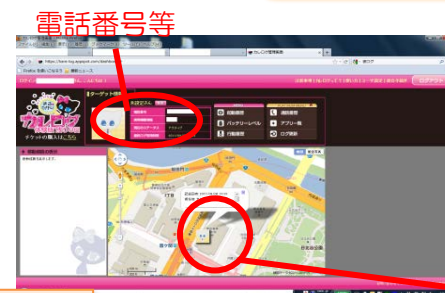


- ③PC用のログインID、パスワードを登録されたメールアドレスに送信

（2）利用方法



- ④位置情報等の情報を自動収集し、送信。



- ⑤PCより端末の位置情報等の情報を閲覧可能

課題と改善点（「カレログ2」平成23年10月16日サービス提供開始）

- 1 登録に係る同意
端末所有者が知らないうちに登録されてしまう。
→登録メールアドレスに定期的にメールマガジンを送付。（端末所有者が知らないうちに登録されていた場合でも、後から気づくことが可能。）
- 2 情報収集時の表示
位置情報等の情報を取得されていることを端末所有者が認識できない。
→位置情報取得開始時及び取得中に、携帯端末画面上にその旨表示。
- 3 収集した情報の範囲
位置情報等に加えて通話記録を取得。→通話記録の取得を取りやめ。

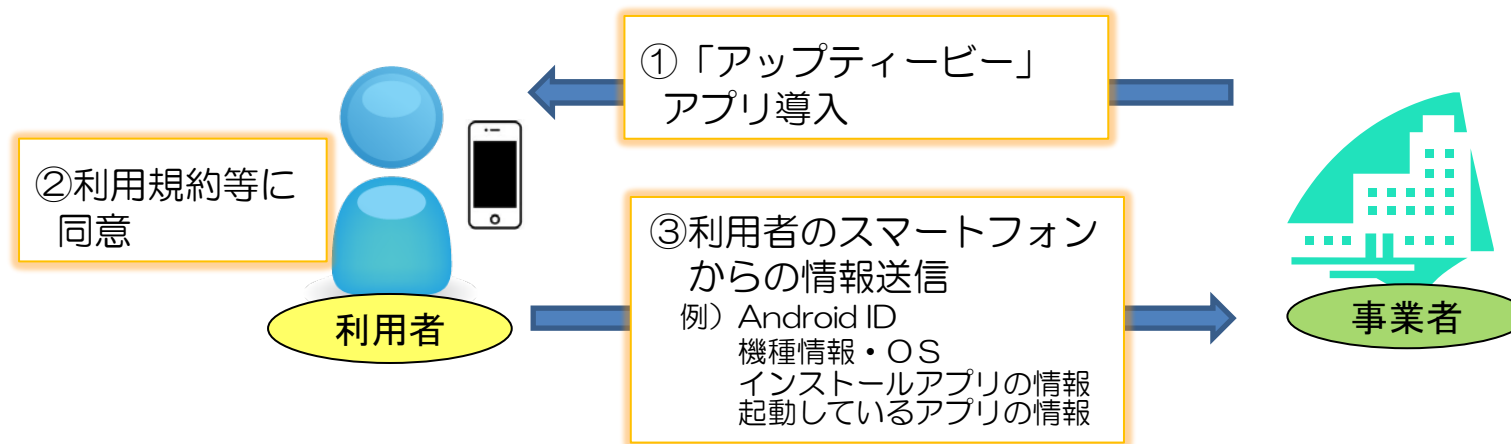


スマートフォンにおける利用者情報の収集事例②（アップティービー）

「アップティービー」の概要

- アニメ等の映像視聴用アプリ「アップティービー」は2011年7月からAndroidスマートフォン向けに、提供されていたところ。
- 「アップティービー」アプリを導入した利用者の端末において、他に導入しているアプリ等の情報を収集し、当該アプリを提供していた事業者へ送信していたもの。
- 同事業者は、利用者の「承諾を得ない段階で情報を取得送信しているという重大な瑕疵が発見され」とし、同年10月10日にサービスを停止。

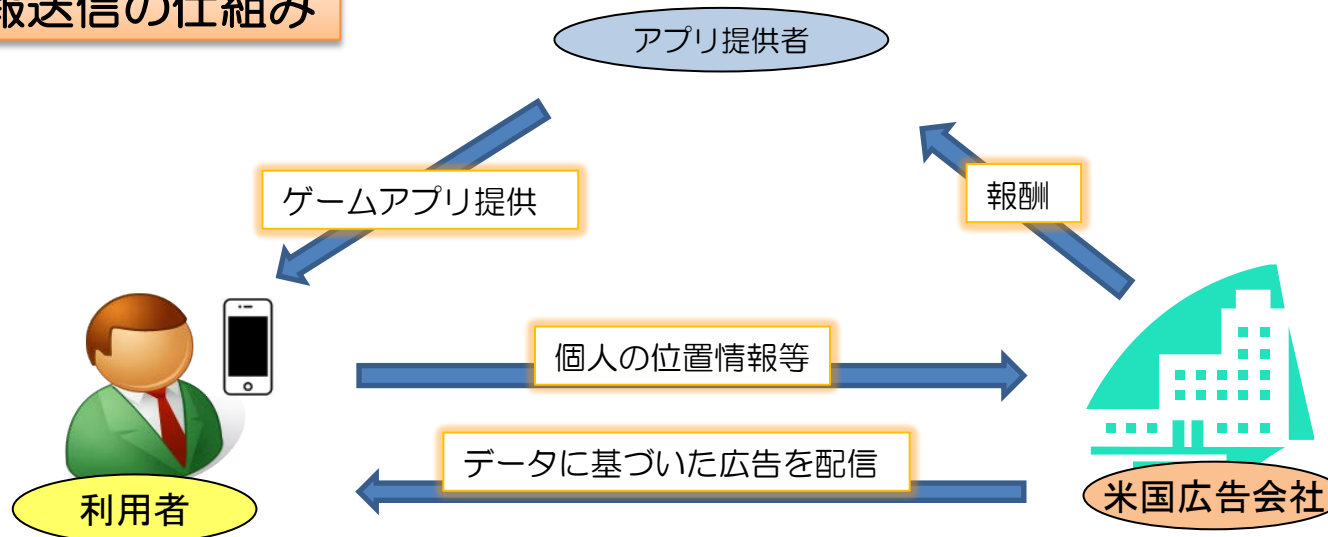
「アップティービー」の仕組み



情報収集モジュールを通じた情報収集

- Androidスマートフォン向けに、200種類以上の無料ゲームアプリ（例：金魚すくい等）をサービス提供。
- 一部のアプリについて、アプリに組み込まれた情報収集モジュールを通じて、GPS等によるスマートフォンの位置情報を1分間に1回、米国の広告会社に送信されていた。
- 収集した位置情報は、アプリ利用者の所在地と関連性の高い広告を表示するために利用されていた。

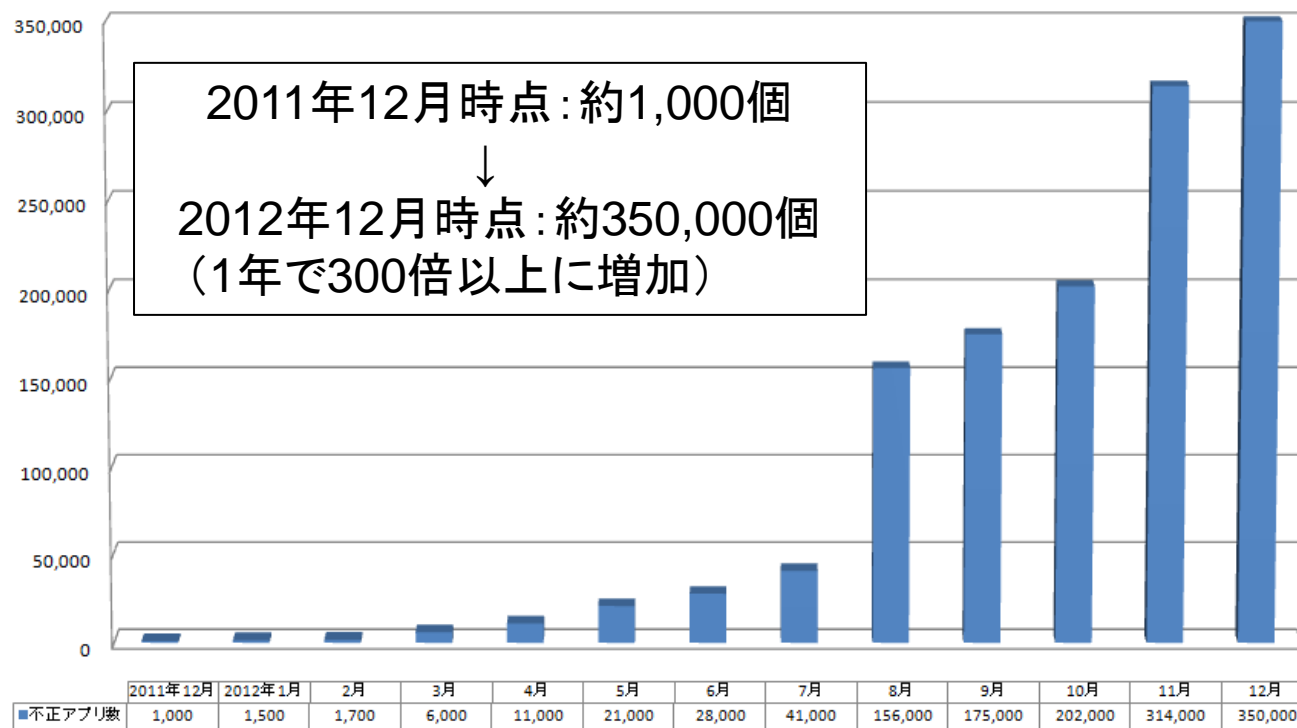
位置情報送信の仕組み



2012年における不正アプリの傾向

トレンドマイクロ(株)によれば、スマートフォンにおける不正アプリは、2012年の上半期まではゲームやアダルト、動画コンテンツの再生などユーザの興味を引くアプリに偽装するものが主であった。一方、2012年の下半期にはスマホの普及を背景に、電池を長持ちさせるアプリやセキュリティソフトを偽装するなど不正アプリが偽装するカテゴリが増加し、ユーザを騙すソーシャルエンジニアリングの手法が広がりました。

Android端末に感染する不正アプリ数 2011年12月～2012年12月(累計)

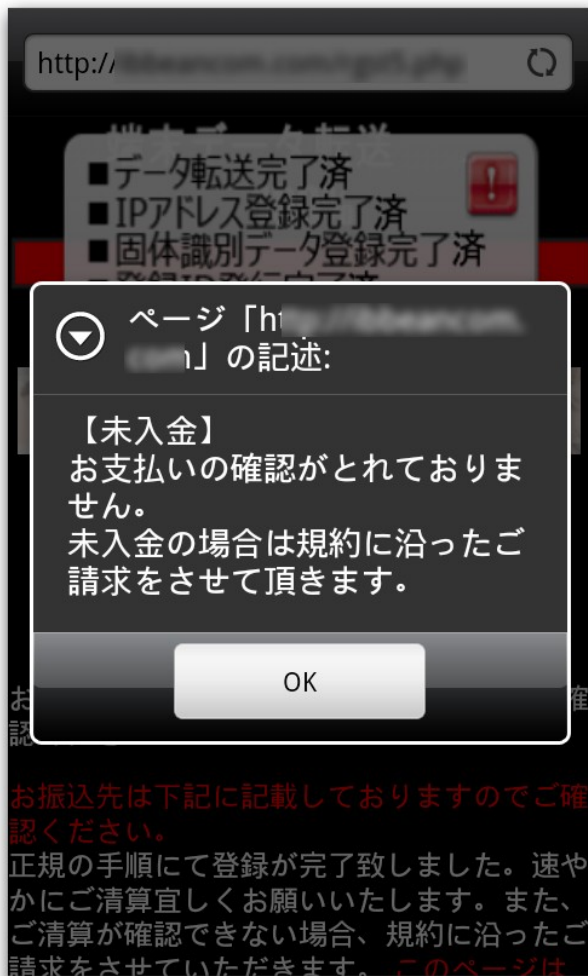


出典: 2012年度インターネット脅威年間レポート(2013年1月10日、トレンドマイクロ株式会社)
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20130107041500.html

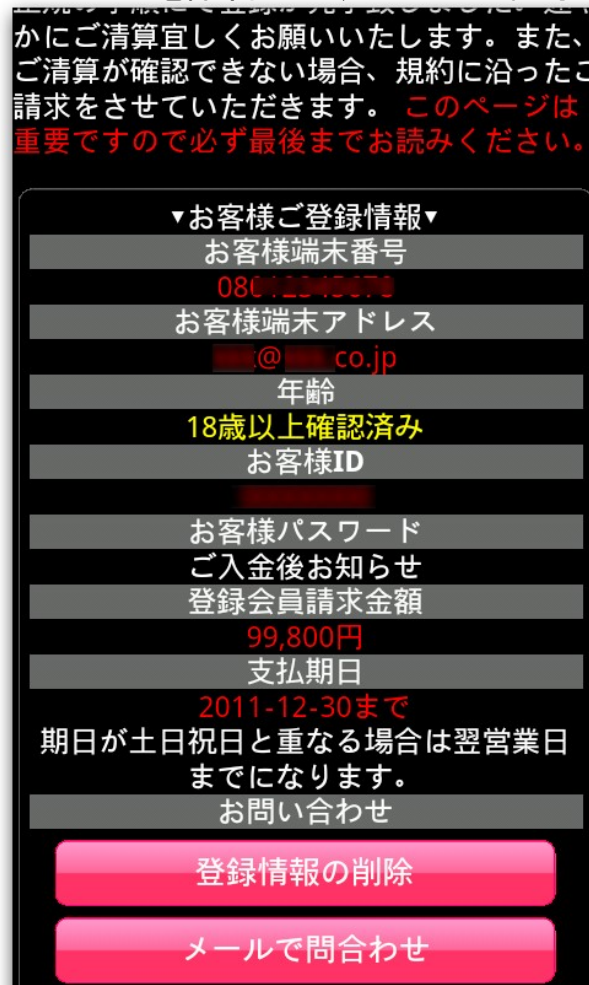


動画を再生しようとしてアプリをダウンロードすると感染し、定期的に金銭の請求画面を表示するワンクリックウェア。

ワンクリックウェア感染後の請求画面のポップアップ



ユーザの電話番号が表示される請求画面



電話帳情報を外部に送信するアンドロイドのアプリケーション

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等を外部に送信していたことが判明。

【アプリケーションの概要】

○アプリケーションは、グーグル社が運営する公式の提供サイトであるGoogle Playで、2月頃から無料配布されていた。(グーグル社は、外部からの通報により、4月13日に掲載ポリシー違反を認知、同アプリを削除)

○アプリケーションをインストールする際、「連絡先データの読み込み」について、利用者に対する許諾が求められる。許諾のボタンを押すことによりインストールが実施される。

○起動すると、動画が再生されるが、同時に端末所有者の電話番号や、電話帳に登録された個人名、電話番号、メールアドレスなどを外部のサーバに送信する機能を持つ。

○この種のアプリケーションは少なくとも16種類存在し、6万6,000人から27万人がインストールし、延べ数10万人から数100万人の個人情報が流出した可能性。

【アプリケーションが提供されていた画面】



電話帳情報等を外部に送信するアンドロイドのアプリケーション

平成24年8月、「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不正アプリが確認された。

概要

- 平成24年8月頃から、スマートフォンの機能を改善するアプリケーションを装って、複数の不正なアプリがスマートフォン利用者に配布された。
- 当該アプリは、機能改善を実現せず、実際は当該アプリをインストールした端末から電話帳情報等を抜き出し、外部へ送信するものであることが判明。
- これらアプリはGoogle Playでは配布されず、当該不正アプリ作成者等が作成したWebサイト等で配布され、当該サイト等に利用者を誘導するため、Facebook等SNSへの書き込みやメール等でURLの紹介が行われるなどしていたもの。

【不正アプリの例】



【不正アプリに誘引する手段の例】

