



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

2013年2月25日

日本総合研究所 総合研究部門 戦略コンサルティング部

アジェンダ

1. アプリケーションのプライバシーポリシー設置の動向
2. アプリケーションのプライバシー検証・表示の動向

1. アプリケーションのプライバシーポリシー設置の動向

■アプリケーションのプライバシーポリシーの調査概要

◆プライバシーポリシーの動向把握のため、以下の調査を行った。

調査内容

- アプリケーションの利用規約・プライバシーポリシーの記載状況の把握
 - アプリケーション内、Google Play紹介ページ内、および開発者ホームページ上での利用規約・プライバシーポリシーの有無
- プライバシーポリシーとスマートフォンプライバシーイニシアティブとの整合状況の把握
 - スマートフォンプライバシーイニシアティブにおける8項目の記載の確認

調査対象

- Google Play日本無料アプリランキング、米国無料アプリランキングより上位40のアプリを抽出
- Androidアプリ 67種(一部日米で重複が存在、また、日本ではダウンロード不可のアプリも存在)

調査イメージ

調査対象	調査項目	調査対象のプライバシーポリシー記載状況																																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32				
1	利用規約・プライバシーポリシーの記載状況	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	スマートフォンプライバシーイニシアティブとの整合状況	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
...	
67	調査対象のプライバシーポリシー記載状況	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

■アプリケーションの利用規約・プライバシーポリシーの記載状況

- ◆ プライバシーポリシーをすべてにおいて記載しているアプリ(パターン①)は9つ、逆にアプリ内、Google Playの両方にプライバシーポリシーを記載していないアプリ(パターン⑦、⑧)は16つであった。
- ◆ 日米の記載状況を比較したところ、米国の方が、全体的に利用規約、プライバシーポリシーの設置率が高かった。特にGoogle Playのページでの設置率は大きく異なった。

プライバシーポリシー設置動向(日本)

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	○	○	×	×	○	○	×	×
開発者ホームページ	○	×	○	×	○	×	○	×
アプリ数(計40アプリ)	9	0	7	2	6	0	9	7

プライバシーポリシー設置動向の比較

場所	内容	日本(計40アプリ)		米国(計37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	40.5%
	プライバシーポリシー	17	43.2%	21	56.8%
Google Play 紹介ページ	プライバシーポリシー	13	32.5%	28	75.7%
開発者ホームページ	利用規約	23	57.5%	25	67.6%
	プライバシーポリシー	32	80.0%	28	75.7%

■ プライバシーポリシーの設置とパーミッション取得状況

- ◆ プライバシーポリシーを一切記載していないアプリが多くのパーミッションを取得している事例が存在する。
- ◆ 開発者ホームページにのみ掲載しているアプリにも、同様の事例が存在する。

プライバシーポリシーを一切記載していないアプリのパーミッション		開発者ホームページにのみプライバシーポリシーを掲載するアプリのパーミッション
アプリA(カメラアプリ)	アプリB(ゲームアプリ)	アプリC(便利ツールアプリ)
<ul style="list-style-type: none"> ■ ハードウェアの制御 <ul style="list-style-type: none"> -画像と動画の撮影 ■ 現在地 <ul style="list-style-type: none"> -おおよその位置情報(ネットワーク基地局) -正確な位置情報(GPS とネットワーク基地局) ■ ネットワーク通信 <ul style="list-style-type: none"> -ネットワークへのフルアクセス ■ 電話/通話 <ul style="list-style-type: none"> -端末のステータスと ID の読み取り ■ ストレージ <ul style="list-style-type: none"> -USB ストレージのコンテンツの変更または削除/SD カードのコンテンツの変更または削除 ■ システム ツール <ul style="list-style-type: none"> -実行中のアプリの取得 	<ul style="list-style-type: none"> ■ 現在地 <ul style="list-style-type: none"> -おおよその位置情報(ネットワーク基地局) -正確な位置情報(GPS とネットワーク基地局) ■ ネットワーク通信 <ul style="list-style-type: none"> -ネットワークへのフルアクセス ■ 電話/通話 <ul style="list-style-type: none"> -端末のステータスと ID の読み取り 	<ul style="list-style-type: none"> ■ アカウント <ul style="list-style-type: none"> -この端末上のアカウントの使用 -アカウントの追加と削除 ■ ハードウェアの制御 <ul style="list-style-type: none"> -画像と動画の撮影 ■ ネットワーク通信 <ul style="list-style-type: none"> -ネットワークへのフルアクセス ■ 電話/通話 <ul style="list-style-type: none"> -端末のステータスと ID の読み取り ■ ストレージ <ul style="list-style-type: none"> -USB ストレージのコンテンツの変更または削除/SD カードのコンテンツの変更または削除 ■ システム ツール <ul style="list-style-type: none"> -実行中のアプリの取得

■ プライバシーポリシーのスマートフォン プライバシーイニシアティブとの整合状況

- ◆ プライバシーポリシーにおいて、日米ともに記載が少なかった項目は、「通知・公表又は同意取得の方法、利用者関与の方法」、「情報収集モジュールの有無」である。
- ◆ 日米間で最も記載状況に差が見られた項目は、「取得される情報の項目」であった。

番号	内容	日本(計33アプリ)		米国(計34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	33	100%	34	100%
②	②取得される情報の項目	29	87.9%	34	100%
③	③取得方法	27	81.8%	29	85.3%
④	④利用目的の特定・明示	32	97.0%	32	94.1%
⑤-1	通知・公表又は同意取得の方法	6	18.2%	7	20.6%
⑤-2	利用者関与の方法	13	39.4%	16	47.1%
⑥-1	外部送信・第三者提供の有無	25	75.8%	26	76.5%
⑥-2	情報収集モジュール(※)の有無	4	12.1%	3	8.8%
⑦	問い合わせ窓口	31	93.9%	29	85.3%
⑧	プライバシーポリシーの変更を行う場合の手続き	27	81.8%	24	70.6%

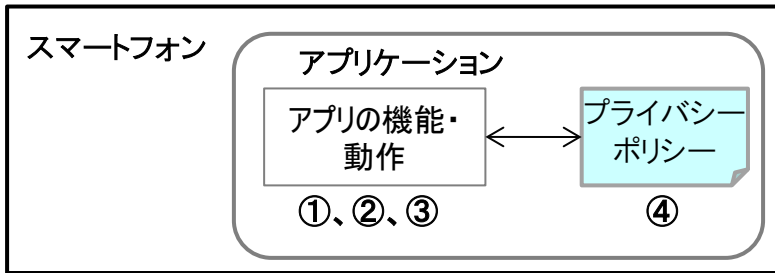
(注)*「項目⑤、⑥の評価方法」:2つの要素に分けて記載の有無の評価を行った。*「情報収集モジュール」:携帯端末に備蓄された情報の収集機能を持つプログラム。また、KDDI研究所の過去の調査(2011年1月~6月)では、980の無料アプリのうち、56.9%に情報収集モジュールが含有されていたという結果も得られた。

2. アプリケーションのプライバシー検証・表示の動向

■ 事業者別のアプリケーション検証の動向

- ◆ アプリケーション検証は「マルウェア検証」、「脆弱性検証」、「プライバシーの観点での技術検証(プライバシー技術検証)」、「プライバシーポリシー記載の検証(プライバシー非技術検証)」の4つに分かれる。
- ◆ 今回はプライバシー検証に焦点を置いて、事業者の取り組みを紹介する。

アプリケーション検証の分類



- ① マルウェア検証**
アプリケーションの動作、機能を解析し、アプリケーションがマルウェアであるかどうかを検証する。
- ② 脆弱性検証**
アプリケーションの機能・動作を解析し、アプリケーションが他アプリとの連携やファイルの保存等に脆弱性がないかを検証する。
- ③ プライバシー技術検証**
アプリの機能・動作を検証して、大量にプライバシー情報を取得していないか、送信先は適切かなどを確認する。
- ④ プライバシー非技術検証**
プライバシーポリシーが存在するか、その記載やプライバシー情報の取り扱いの方針などが適切かどうかを確認する。

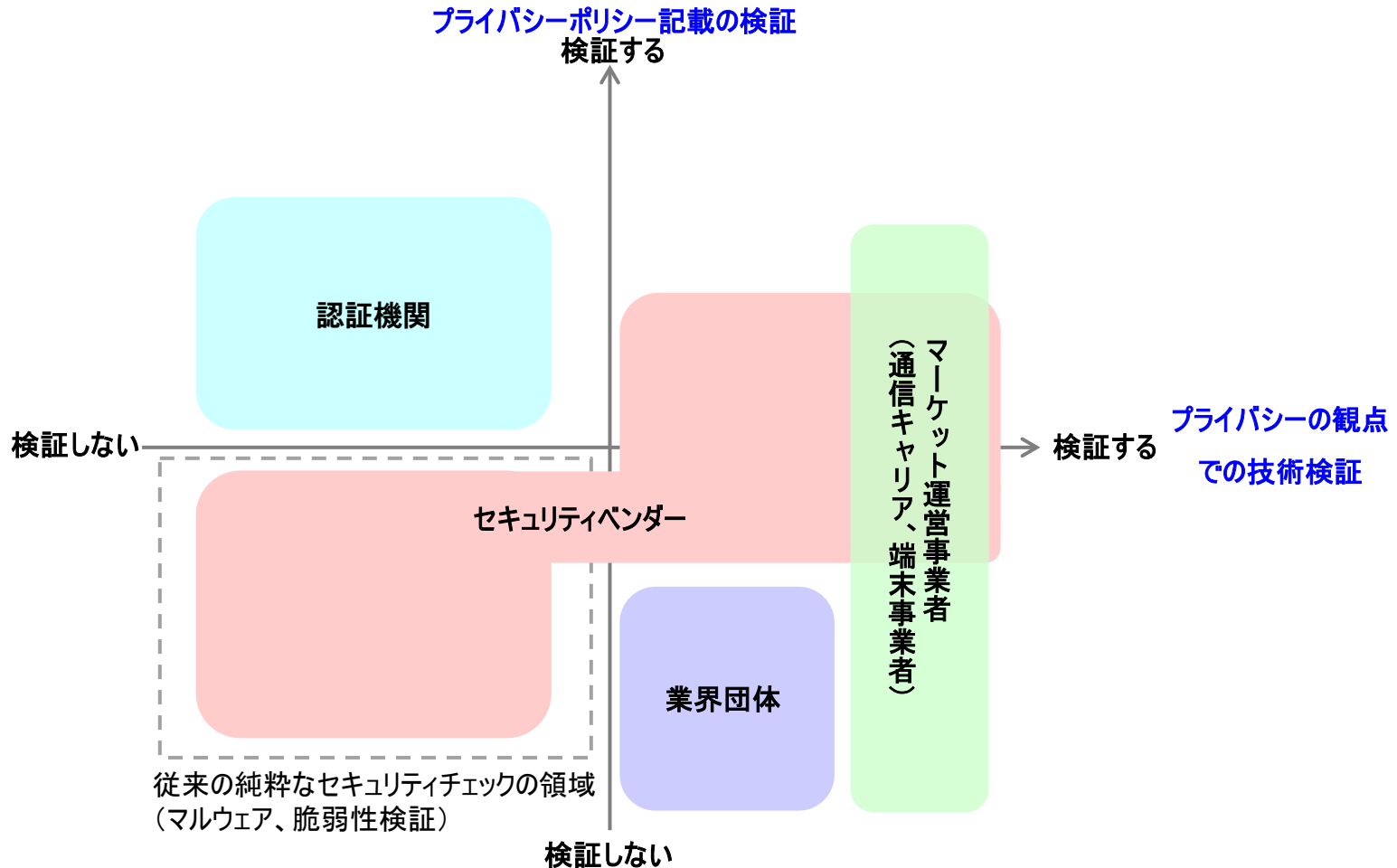
事業者別の検証の動向

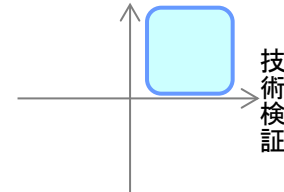
事業者	検証			
	①マルウェア検証	②脆弱性検証	③プライバシー技術検証	④プライバシー非技術検証
アプリマーケット運営者(通信キャリア、端末事業者)				
セキュリティベンダー、システム事業者			今回の対象領域	
その他機関(業界団体、研究機関等)				

(注)「各セルの濃淡」: 代表的な事業者がこれまで主に取り組んでいた領域を濃くした。

■ 関連事業者のプライバシー検証・表示の実施領域

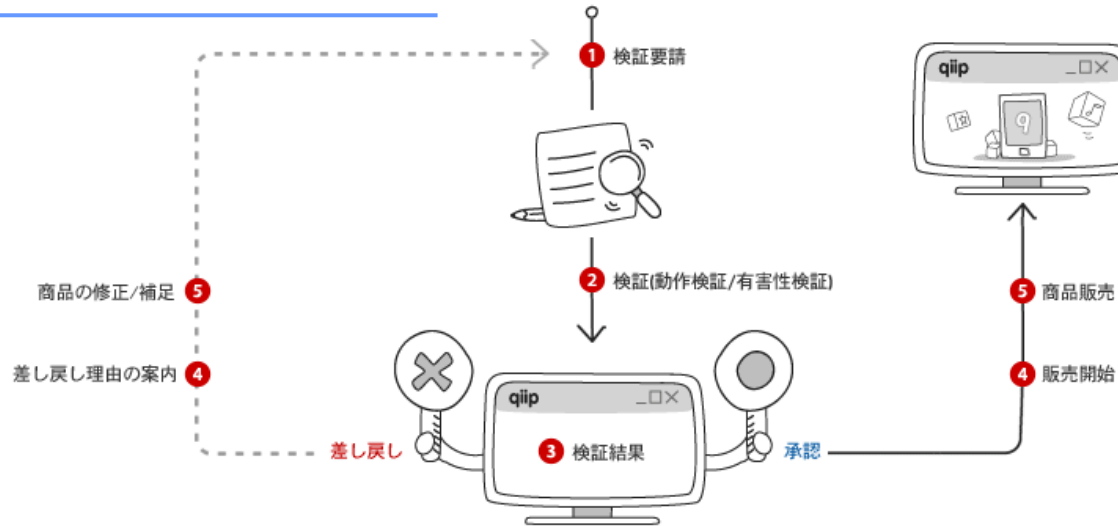
- ◆ 「プライバシーの観点での技術検証」、「プライバシーポリシー記載の検証」の実施の有無を横軸、縦軸に取り、関連する事業者をマッピングした。
- ◆ セキュリティベンダーは本来のマルウェア・脆弱性の検証から、プライバシー検証にも一部着手している。マーケット事業者についても、プライバシー検証に注力する事業者が存在する。





■ 第三者検証・表示事業者例 SK Telecom

アプリケーション検証手続きの流れ



≪検証方法≫

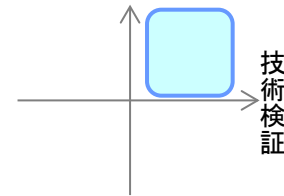
- ◆ 多様な状況と操作を想定し、アプリケーションの完成度の検証を行う

≪検証項目≫

- ◆ アプリケーションのダウンロード、インストール、削除が正常に完了するか
- ◆ アプリケーションのショートカットアイコンがコンテンツ内容と一致するか (デベロッパーセンターに登録したアプリケーションの画像および内容に沿ったものであること。)
- ◆ プラットフォーム情報、容量など、ダウンロードしたアプリ情報およびインストールした情報が一致するか
- ◆ アプリケーション内にウイルスまたは悪性コードが含まれていないか

≪プライバシー保護関連の検証項目≫

- ◆ 個人情報および位置データを収集し利用するアプリケーションの場合、ユーザに案内し同意を得る
 - ◇ ユーザ情報の収集時、利用案内および初回起動時の情報収集に関する内容をユーザが確認できるように案内をすること。
 - ◇ 個人情報収集の同意を求めるとき、ユーザに告知が必要
 - ⇒ 個人情報の利用者/個人情報の利用目的/個人情報の項目(名前、電話番号、携帯電話番号、メールアドレスなど)/個人情報の保有期間および利用期間 など
 - ◇ 同意を求めるとき、収集する情報およびその目的が含まれなければならない。
 - ◇ アプリ起動の際、初めての画面に個人情報収集についての告知および同意のプロセスが必要



■ 第三者検証・表示事業者例 KT Telecom

セキュリティ検証項目

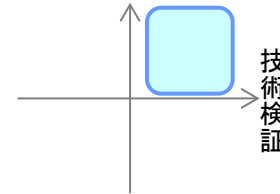
1. ウィルスおよび悪質なコードが含まれているか。
2. サービス利用において、不要な端末情報や個人情報を収集しているか。
 (同意が必要な項目について、同意を求めない&収集禁止項目を収集する場合は、×—同意必要項目:IMEI、ICCID、通話内訳、プライバシー情報/収集禁止項目:ESN、IMSI)
3. 重要情報のデータ送信の際、暗号化されるか。
 (重要情報項目:ログインID/PW、IMEI、IMSI、ICCID、電話番号など)
4. 重要情報を画面に表示する場合、暗号化表示されているか。
 (住民登録番号、口座番号、クレジットカード番号、パスワードなど)
5. 不要なAndroid権限を要求するか—114のAndroid権限のなか、主要28項目について、サービス上必要な場合のみ使用可能。個人情報、位置情報などの重要情報がサービス上必要ではない権限で使われる場合、登録不可
6. 位置情報収集・利用の場合、利用規約表示および同意のプロセスがあるか。



Android権限主要28項目の一部抜粋

- ①位置(GPS、テスト用の位置情報提供者作成)
- ②課金サービス(SMS送信)
- ③個人情報(電話帳データ読み込み)
- ④システムツール(システムログファイル読み込み)
- ⑤項目未表示(永久的使用不可、アプリのアンインストール、位置情報提供者の設置権限)
- ⑥ハードウェアコントロール(音声録音、写真撮影)

—利用規約の必須項目 ① 位置情報事業者の商号、住所、電話番号などの連絡先 ② 個人位置情報の主体および法政代理人の権利と行使方法③位置情報事業者が位置基盤サービス事業者に提供するサービスの内容④位置情報収集資料の保有根拠および保有期間



■ 第三者検証・表示事業者例 KDDI

- ◆ KDDIは自社の運営するアプリマーケット「au Market」において、プライバシー検証を行っている。
- ◆ 利用者情報の送信において、端末から外部へ送信される情報と、プライバシーポリシーとの整合性を確認する。

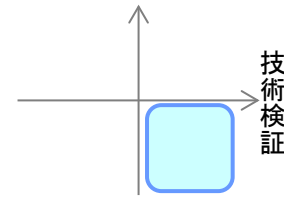
検査項目

- 機能(パーミッション)**
アプリに不必要なパーミッション(OSのパーミッション)のチェック
- 本来利用できない機能の有無**
管理者権限の利用や標準APIを回避する機能の有無のチェック
- 利用者情報の送信の有無**
端末から外部へ送信される情報のチェック この情報とアプリのプライバシーポリシーとの整合性のチェック
- 外部への不正アクセスの有無**
多量または多頻度な通信、攻撃的な通信のチェック

利用者情報の外部送信情報	R 表示 C 変更
送信する利用者情報	<input type="checkbox"/> Android ID (ハードウェアID) <input type="checkbox"/> IMEI (端末識別ID) (ハードウェアID) <input type="checkbox"/> IMSI (加入電話番号) (ハードウェアID) <input type="checkbox"/> ICCID (SIMカードID) (ハードウェアID) <input type="checkbox"/> 電話番号 (ハードウェアID) <input type="checkbox"/> Google アカウント (ハードウェアID) <input type="checkbox"/> メールアドレス (ハードウェアID) <input type="checkbox"/> アプリID (ハードウェアID) <input type="checkbox"/> MACアドレス (ハードウェアID) <input type="checkbox"/> 長短・電話番号・メールアドレス等のアドレス情報 <input type="checkbox"/> 位置情報 <input type="checkbox"/> インターネット接続のアプリ履歴 <input type="checkbox"/> カレンダー情報 <input type="checkbox"/> 通話履歴・通話相手IDリストの情報 <input type="checkbox"/> (Web)閲覧履歴 (アプリ利用履歴を基にWebサイトのアクセス履歴) <input type="checkbox"/> 送信履歴 (送信先) <input type="checkbox"/> 利用履歴の表示/非表示項目です。こちらが送信が発生するサービス・プロセスの単位で、有効無効を適宜変更しますのでこの単位で設定してください。
送信する目的	
送信先	

通信内容関連情報	R 表示 C 変更
通信内容が発生する機能	<input type="checkbox"/> 電話の発信 <input type="checkbox"/> 送信 (ICD) の操作 <input type="checkbox"/> 利用履歴の表示/非表示項目です。こちらが送信が発生するサービス・プロセスの単位で、有効無効を適宜変更しますのでこの単位で設定してください。
目的	

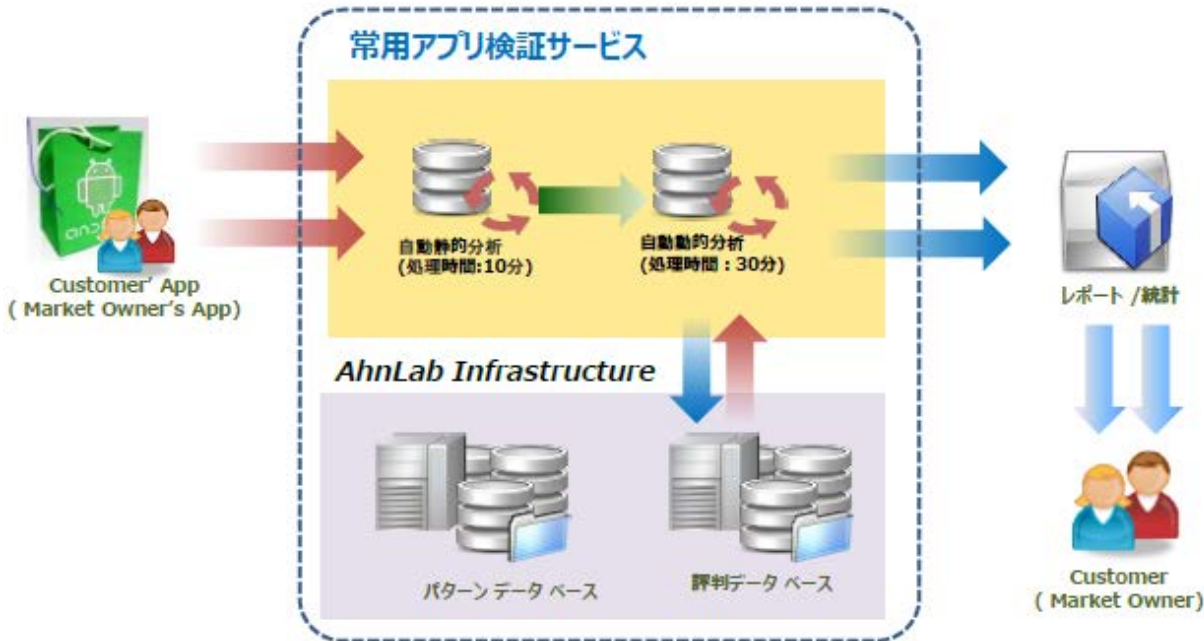
- アプリ開発者に対して、マーケットへのアプリ申請の際に利用者情報の扱いに関する説明の記入を要請
- 外部送信する情報に関して、以下の項目を申請させる
 - 送信する利用者情報
 - 送信する目的
 - 送信先
- 申請内容と実際の送信情報、送信先があることを確認して公開。



■ 第三者検証・表示事業者例 Samsung

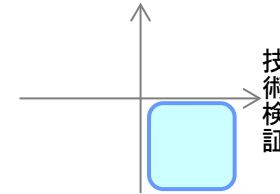
- ◆ Samsung社は、アンラボ社のアプリ検証セキュリティソリューション「AhnLab モバイルスマートディフェンス」をSamsung Appsのセキュリティ審査自動化ソリューションに導入。Samsung Appsで提供されるすべてのアプリケーションに事前検証を行っている。
- ◆ 動的解析、静的解析、専門家による検証の3種類を行う。
- ◆ アプリの検証項目として、プライバシーに関する検査項目が存在する。

AhnLab モバイルスマートディフェンス



プライバシーに関する検証項目

- 利用者を騙すための警告を行うなどの、暗号・クレジットカード番号などのデータを入手する悪意的手段を使うことを禁じる。
- アプリがオーディオストリームや個人情報を記録・モニタリングすることを禁じる。
- 利用者の同意を得ない限り、有料サービスは提供できない。
- 利用者の個人情報を使用、収集、修正、転送する場合、アプリの初回起動の際、予め通知し、同意を得なければならない。
- 強制的メッセージや広告など、利用者は要請していない情報を表示・提供する場合、アプリの初回起動の際に、予め通知し、同意を得なければならない。



■ 第三者検証・表示事業者例 トレンドマイクロ

- ◆ 2012年9月より、トレンドマイクロ社はアプリのプライバシーリスクを一目で確認できる新機能「プライバシースキャン」機能を新たに搭載。
- ◆ アプリの危険性を「問題なし」「低」「中」「高」の4段階で表示するとともに、どのような情報が収集される可能性があるかを通知する。

検査項目

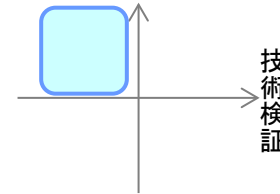
- アプリの挙動
- 配信元、通信先のURL
- 署名
- 携帯電話機識別番号(IMEI)、連絡先電話帳、ショートメッセージ(SMS)、ログインアカウント、位置情報、通話履歴などの情報を収集するかどうか



■ 第三者検証・表示事業者例 情報セキュリティ格付け制度研究会

◆ 同研究会は、スマートフォン プライバシーイニシアティブに対する企業の実施状況について評価を行い、第三者としての証明書を発行する。

プライバシーポリシー検証



検査項目

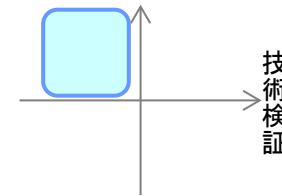
確認事項	詳細
1.基本原則	①透明性の確保 ②利用者関与の機会の確保 ③適正な手段による取得の確保 ④適切な安全管理の確保 ⑤苦情・相談への対応体制の確保 ⑥プライバシー・バイ・デザイン
2.プライバシーポリシー項目	① 情報を取得するアプリケーション提供者等の氏名又は名称 ② 取得される情報の項目 ③ 取得方法 ④ 利用目的の特定・明示 ⑤ 通知・公表又は同意取得の方法、利用者関与の方法 ⑥ 外部送信・第三者提供・情報収集モジュールの有無組込みの有無を記載する。 ⑦ 問合せ窓口 ⑧ プライバシーポリシーの変更を行う場合の手
3.アピールポイント	業界団体のガイドラインを加味したアピールポイント (ex.蓄積データの漏えい防止策等)

左記の3つの確認事項に対して、
企業の実施策を記載・確認し、証明書を発行



第三者証明書





■ 第三者検証・表示事業者例 Mozilla

- ◆ Webサービス上でのプライバシーに関する表示例として、Mozilla社は自社ブラウザ(Firefox)のアドイン型での、表示ツールの導入試験を行っている。
- ◆ プログラムがウェブサイトのプライバシーポリシーを読み込み、自動でプライバシーに関するアイコンを表示する。
- ◆ 現状はPCを対象としているが、今後モバイルへの導入も検討している。

表示項目



- ◆ 来訪データ保存期間(※再訪までの時間)
ユーザーの訪問記録を何か月前まで保有するか



- ◆ サードパーティーへの情報提供
ウェブサイトが個人情報を取得して、それ外部に伝えているか、を他者に販売しているかどうか



- ◆ アドネットワーク
個人情報をアドネットワーク事業所に提供しているか



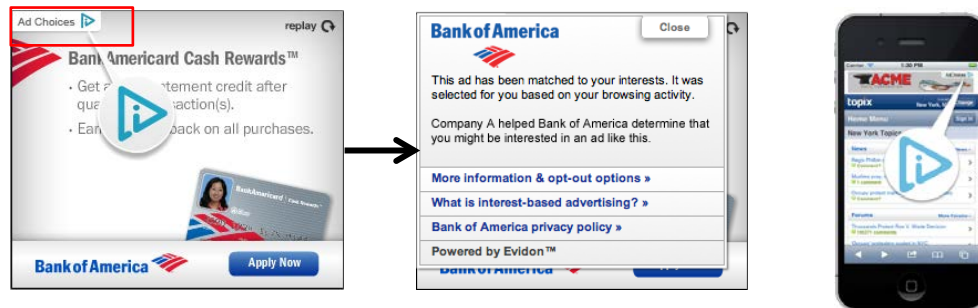
- ◆ 法的・政府機関への情報提供
法的機関政府機関から要求が来た場合に、ユーザーの個人情報を提供できるか

(参考) 米国における検証・表示例

- ◆ 2010年の米国連邦取引委員会(FTC)以降、米国ではターゲティング広告に対する取組が行われている。
- ◆ Webサービスに対するプライバシーの動向として、米国のEvidon社は、米国、EUを中心に、オンライン広告に対する自主規制ツールの「Evidon InForm」、ブラウザベースでのモニタリングサービス「Ghostery」を提供している。

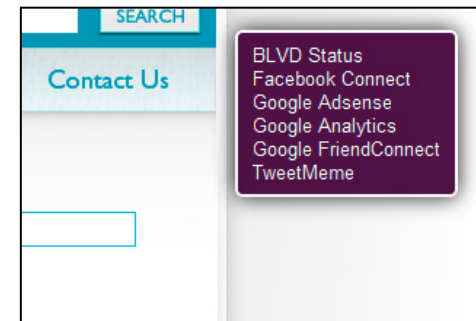
オンライン広告アイコンサービス「Evidon InForm」

- 広告主が米国のオンライン広告の自主規制や、EUの ePrivacy Directiveの順守をサポートするサービス。
- 広告上にアイコンを掲示して、広告主に対する詳細情報、情報を取得しているサードパーティーの一覧を掲示、それぞれのオプトアウトの選択肢等を提供する。
- ホームページ掲載前に、情報の取得に関する同意画面を掲示させたり、同意の状態をわかりやすく掲示させたりする。
- 1日に40か国以上の1.5億人のユーザーにアイコンを表示している。
- Mobile版でも同サービスを展開



ブラウザベースモニタリングサービス「Ghostery」

- ブラウザ上でユーザーのトラッキングを監視、把握するサービス。
- アドネットワークや、行動データの収集者等の、1,200の企業のトラッカーを把握し、ユーザー側でオプトアウトを選択できる。
- iPhoneアプリでもサービスを展開。



トラッカー表示例
















iPhoneアプリ版

(参考) 欧州における検証・表示例

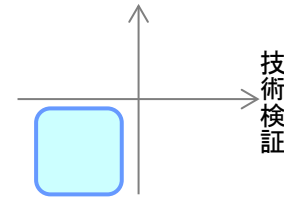
- ◆ 欧州でも、ターゲティング広告に対する議論により、Webサービスでのプライバシーに関して先行的に着手している。
- ◆ Interactive Advertising Bureau (IAB) Europeにおいて、ホームページ「your online choices」において行動ターゲティング広告のために情報を取得する事業者が一覧化されており、ユーザー側で選択して、情報の取得を拒否することが可能。

Turn on or off individual companies

Company	On/Off	Info
ad4mat®	<input checked="" type="radio"/> On <input type="radio"/> Off	
Adatus	<input checked="" type="radio"/> On <input type="radio"/> Off	
Adcloud	<input checked="" type="radio"/> On <input type="radio"/> Off	
Adconion Direct	<input checked="" type="radio"/> On <input type="radio"/> Off	
AddThis (formerly Clearspring)	<input checked="" type="radio"/> On <input type="radio"/> Off	
AdDynamics	<input checked="" type="radio"/> On <input type="radio"/> Off	
Adform	<input checked="" type="radio"/> On <input type="radio"/> Off	
adGENIE	<input checked="" type="radio"/> On <input type="radio"/> Off	
AdLantic	<input checked="" type="radio"/> On <input type="radio"/> Off	
Admeta	<input checked="" type="radio"/> On <input type="radio"/> Off	
AdServerPub	<input checked="" type="radio"/> On <input type="radio"/> Off	
AdTiger	<input checked="" type="radio"/> On <input type="radio"/> Off	
Affectv	<input checked="" type="radio"/> On <input type="radio"/> Off	

個社名、詳細情報の取得、個別オプトイン・アウトの選択が可能

your online choices
 a guide to online behavioural advertising



■ 第三者検証・表示事業者例 神戸デジタル・ラボ

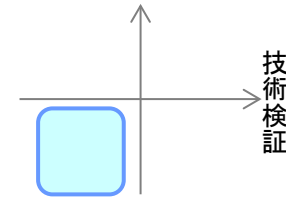
- ◆ Androidアプリの脆弱性に対して、安価かつ高速な簡易診断サービスを提供する。
- ◆ アプリ内だけでなく、アプリがアクセスするサーバー側の脆弱性についても検証を行う。

アンドロイド(Android)アプリの診断の観点

1. 認証
認証処理を介さずに認証が必要なコンテンツにアクセスされたり、認証情報が外部に漏洩したりすることがないか
2. 不適切な権限
アプリに必要以上のパーミッションが割り当てられていたり、各アプリ用に用意されたディレクトリに機密情報を保存している場合に他のアプリからアクセスできたりしないか
3. 不適切なプロセス間通信
コンテンツプロバイダ機能やインテント機能などが悪用されることによりアプリ内部の情報が漏洩することがないか
4. コマンドの実行
不正なパラメータを送信することにより、アプリの機能を悪用したり、アプリ内DBの内容を不正操作できないか
5. 情報漏えい
アプリのソースコードやロジックの構造などにより機密情報・個人情報・認証情報などの重要な情報が漏洩することがないか
6. その他

サーバーサイドの診断の観点

1. 認証
認証処理を介さずに認証が必要なコンテンツにアクセスされたり、認証情報が外部に漏洩したりすることがないか
2. 承認
アクセスするために一定の権限が必要となるコンテンツについて、その権限を持たないユーザが不正にアクセスすることができないか
3. インジェクション系攻撃
不正なパラメータを送信することにより、サーバ側で実行されるSQLやOSコマンドなどのコマンド内容を任意に改ざんし、データベースやサーバ内部の情報を閲覧・改ざん・削除することができないか
4. 情報漏洩
サーバが出力するレスポンスやエラーなどからサーバの内部情報が取得できたり、任意のパスを指定してサーバにアクセスすることで公開を意図していない情報にアクセスできたりしないか
5. その他



■ 第三者検証・表示事業者例 viaForensics、Plynt

◆脆弱性に関しては、海外のセキュリティ関連企業も検証、表示サービスを提供している。

viaForensics

- viaForensicsはモバイルセキュリティサービスを提供する企業
- 同社の「Mobile Application Security - appSecure」で認可されたアプリケーションに対して、認証を提供する
- 評価基準は以下の通り(一部抜粋)
 - 1.ウェブ履歴とキャッシュの取扱い
 - 2.ログイン情報の安全な取扱い
 - 3.人の仲介による攻撃の回避
 - 4.センシティブな情報の安全な送信
- 認証を得たアプリに関しては、viaForensicsのホームページ上で紹介
- また、アプリケーション内部、ホームページなどに掲載する用の画像イメージを提供する(下図参照)



Plynt

- Plyntはアプリケーションセキュリティを提供する会社
- 12 の基準を満たすモバイルアプリケーションに対して提供される認証
- 評価基準は以下(一部抜粋)
 - 1.センシティブなデータをセキュアなストレージに保管しているか(またはストレージが無い)
 - 2.(キャッシュ、ログ等の)データ流出を防止しているか
 - 3.サーバー側への攻撃を防いでいるか
 - 4.脅威に対する防御を行っているか
 - 5.セキュアでない方法で、外部サイト・他アプリケーションにセンシティブなデータを送信していないか
 - 6.OS関連機能を安全に導入しているか
 - 7.センシティブなアクティビティに対して承認を要求しているか
 - 8.承認されていないデバイスリソースの利用に対して防御を行っているか
- Plynt社のエンジニアがハッカーとしてアプリの内部データに侵入できるかを検証する



■ プライバシー検証・表示事業者のまとめ

- ◆ 技術検証、プライバシーポリシー記載の検証の両方を行っている事業者は現状では少ない。しかし、ヒアリング等から、ユーザーに対する安全性を高めるためには、同2項目での検証が今後重要であると考える。
- ◆ 検証体制の充実のためには、各団体での評価基準の統一、事業者間連携等の取組が必要と推測される。

プライバシーポリシー記載の検証

検証する

当該領域の充実を
図ることが重要

より安全な検証体制

認証機関

マーケット運営事業者
(通信キャリア、端末事業者)

プライバシーの観点
での技術検証
検証する

セキュリティベンダー

業界団体

※これまでの純粋なセキュリティチェックの領域(マルウェア、脆弱性検証)

検証体制の拡充に向けて

- ① 評価基準に関する情報共有と検討
各事業者の評価基準を、部分的に統一する、もしくは共有することで、検証の効率化を促進し、体制の拡充を見込む
- ② 事業者間連情報共有、連携の強化
プライバシーポリシー、技術の検証のみを行っている事業者がそれぞれ連携して検証を行うことで、検査体制の拡充、安全なアプリケーションのための検証を目指す

(参考) 韓国におけるプライバシーの動向

◆韓国では2011年に個人情報保護法が施行され、アプリ近年アプリケーションを対象としたプライバシーに対する取組が行われている。

年次	概要
1997年1月	<ul style="list-style-type: none"> • <u>位置情報保護法が制定。</u> <ul style="list-style-type: none"> ➢ 2012年2月にGoogle社のプライバシーポリシーが①個人情報利用目的の包括的記載及び明示上同意手続きの不備、②情報通信網法上の必須明示事項の脱落、③プライバシーポリシーを受け入れない利用者にも選択権を保障すること等について不十分であることから、改善を要求した。 • 2011年8月には、iPhoneが位置情報サービスをオフに設定した際にも位置情報が収集されていたことに対して、<u>同法違反を認定。</u>
2011年9月	<ul style="list-style-type: none"> • <u>個人情報保護法が施行。</u> <ul style="list-style-type: none"> ➢ 個人情報を「生きている個人に関する情報であり、個人を識別できる情報」と定義。<u>通信情報(電子メール、通話、インターネット接続IPアドレス、ログなど)も対象となる。</u>
2012年3月	<ul style="list-style-type: none"> • 韓国情報保護振興院(KISA)が、<u>アプリ事業者向けのガイドラインとして、「アプリ開発者向けプライバシーガイド」を公表。</u> <ul style="list-style-type: none"> ➢ 個人情報保護の観点から留意すべき事項を示したもので、法的拘束力はない。 ➢ <u>「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、センシティブな個人情報の収集の原則禁止、個人情報の第三者提供の制限等を内容に含む。</u> ➢ 国内通信事業者を通じ、同ガイドを周知・啓発中。 • KISAは、<u>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。</u>
2012年6月	<ul style="list-style-type: none"> • 韓国情報保護振興院(KISA)は、放送通信委員会による「安全な位置情報利用環境造成事業」の一環として、<u>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。</u> <ul style="list-style-type: none"> ➢ アプリ事業者が個人情報の流出の危険のないアプリを開発し、それを消費者が選択できるようにするための仕組み。 • <u>2012年内にパイロットプロジェクトの実施を予定。</u>

(参考) 各国の通信キャリアのスマートフォン向けアプリマーケット、アプリ検証体制

国	キャリア名	アプリマーケットの提供状況	アプリ審査の実査状況	備考
米国	AT&T	【提供している】 <ul style="list-style-type: none"> 2012年1月からアプリマーケットと開発環境を提供開始 	【実施している】 <ul style="list-style-type: none"> アプリがセンシティブな情報を送信・保存する際に暗号化されているかなどをチェックしている 	<ul style="list-style-type: none"> API呼び出し数はOTT系APIと比較して圧倒的に少なく、アプリマーケットのDL数や売上高に関する記事や決算資料での説明も見当たらないため、利用されていない。
	Verizon	【提供していた(2013年1月に撤退)】 <ul style="list-style-type: none"> 2010年3月からアプリマーケットであると開発環境を提供開始 2013年1月にアプリマーケットを閉鎖 	【実施していた】 <ul style="list-style-type: none"> 詳細不明 	
日本	NTTドコモ	【提供している】 <ul style="list-style-type: none"> Google Playのリンクを掲載したアプリマーケットを提供 	【一部実施】 <ul style="list-style-type: none"> マルウェアかどうかのチェック、動作チェックを行っている。 	<ul style="list-style-type: none"> 自社のアプリマーケットに掲載するアプリのデータは保持していない
	KDDI	【提供している】 <ul style="list-style-type: none"> 有料アプリが使い放題というアプリマーケットを提供している 	【提供している】 <ul style="list-style-type: none"> プライバシーポリシーのチェック、技術的なセキュリティチェックを行っている。 	<ul style="list-style-type: none"> 自社のアプリマーケットに掲載するアプリのデータはKDDIのサーバー上に存在
	SoftBank	【提供している】 <ul style="list-style-type: none"> Google Playのリンクを掲載したアプリマーケットを提供 	【一部実施】 <ul style="list-style-type: none"> 自社のアプリマーケットで紹介する上で、適正なコンテンツかどうかのチェックは実施 	<ul style="list-style-type: none"> 自社のアプリマーケットに掲載するアプリのデータは保持していない
韓国	SKテレコム	【提供している】 <ul style="list-style-type: none"> アプリマーケットと開発環境を提供 	【実施している】 <ul style="list-style-type: none"> マルウェアかどうかのチェック、動作チェック、個人情報収集における同意の有無などをチェック 	
	KT	【提供している】 <ul style="list-style-type: none"> アプリマーケットと開発環境を提供 	【実施している】 <ul style="list-style-type: none"> マルウェアかどうかのチェック、動作チェック、個人情報収集における同意の有無、不要なパーミッションの取得の有無などをチェック 	
	LG U+	【提供している】 <ul style="list-style-type: none"> アプリマーケットと開発環境を提供 	【実施している】 <ul style="list-style-type: none"> 詳細不明 	

(参考) 韓国におけるゲームに関する規制とアプリマーケットへの影響

- ◆ 韓国では、ゲームの販売前の事前審査を義務付けた法律の影響により、2010年3月から2011年11月までの約1年半の間、Google Play、App Storeにおいてゲームカテゴリが存在しなかった。現在では、法律の改正により、ゲームカテゴリが存在している。

韓国におけるゲーム規制のアプリマーケットへの影響

年月	概要
2010年 3月	<ul style="list-style-type: none"> 韓国政府側からApple、Googleに対して、スマートフォンのアプリマーケットで無審査でゲームを流通させていることが、「ゲーム産業振興法」を違反しているとして、是正を求めた
2010年 3月、4月	<ul style="list-style-type: none"> Apple、Googleともに自社のアプリマーケットからゲームカテゴリを削除することを決定 <ul style="list-style-type: none"> 韓国でのゲーム提供のためだけに、ゲーム開発者に韓国の事前審査を受けさせることを義務付けることは、デメリットが大きい ただし、韓国の事前審査を受けたゲームはエンターテインメントのカテゴリの中で提供 韓国の通信キャリアのアプリマーケットでは、韓国の事前審査に対応させる仕組みを作り、スマートフォン向けゲームを提供し続ける
2011年 4月～7月	<ul style="list-style-type: none"> 2011年4月に法律が改正され、7月から施行され、モバイルゲームを事前審査なしで、自主審査により提供可能になった <ul style="list-style-type: none"> Apple、Googleは、韓国政府とゲームカテゴリ開放に関して協議を開始
2011年 11月	<ul style="list-style-type: none"> Apple、Googleともに自社のアプリマーケットからゲームカテゴリを新設し、ゲームアプリの提供を開始

韓国におけるゲーム規制の概要

項目	概要
法律名	<ul style="list-style-type: none"> ゲーム産業振興法
規制の概要	<ul style="list-style-type: none"> 氏名を照会して本人確認を行う実名確認制度 ゲームの事前審査による年齢等級制度 リアルマネートレードや不正アクセスの禁止 青少年の長時間プレイの制限
ゲームの事前審査の詳細	<ul style="list-style-type: none"> 「ゲーム物等級委員会(Game Rating Board)」の事前審議を受けていないゲームコンテンツは販売できない。 審議により青少年への有害性、射幸性を判断し、すべてのゲームを「全体利用可」・「12歳利用可」・「15歳利用可」・「青少年利用不可」にレーティングする。
ゲーム物等級委員会	<ul style="list-style-type: none"> ゲームを審査する公的な機関 ゲームを評価する委員会は大学教授、弁護士、NGOなど様々な背景を持つ15名で構成される 機能テスト、プログラムの分析など技術的なアドバイスをする委員会やゲームのテスター部隊なども存在している。
2011年の法律改正の内容	<ul style="list-style-type: none"> 制作主体・流通過程の特性などにより、等級委員会の事前等級分類が適切ではないゲームのうち、青少年利用不可のゲーム物を除いたゲーム物に対しては、ゲームを流通する者などが等級委員会と協議した、別途の基準により、自発的に等級分類できる。

(参考) 韓国のスマートフォン向けアプリマーケット

- ◆ 韓国では、韓国最大のモバイルキャリアのSKテレコム提供する「T Store」が、ダウンロード数ではGoogle Playに一步譲るものの、売上面ではGoogle Playをしのいで、国内ナンバーワンの実績を持っている。「T Store」はキャリアフリーのマーケットであり、他のモバイルキャリアの契約者も利用可能である。

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)	<ul style="list-style-type: none"> アプリのダウンロード数ではGoogle Playに一步譲るものの、売上面ではGoogle Playをしのいで国内ナンバーワンの実績を持つという。そのため韓国のアプリメーカーの多くは、まず「T Store」でアプリを配信し、それからGoogle Playで配信する。 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)	

(参考) 世界でのアプリマーケット

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
Google Play (Google)	n.a	n.a	70万 (2012年10月)	250億 (2012年9月)	<ul style="list-style-type: none"> グローバルでの数値 Google Apple共に、韓国でのアプリの月間ダウンロード数は伸び悩んでいる
App Store (Apple)	31,600万台 (iOSデバイスの累計販売台数:2011年末)	n.a	70万 (2012年10月)	400億 (2012年12月)	