

アプリ/コンテンツ向けプライバシーポリシーの 第三者検証フレームワーク

竹森敬祐^{†1} 磯原隆将^{†1} 川端秀明^{†1} 窪田歩^{†1} 高野智秋^{†2}
可児潤也^{†3} 西垣正勝^{†3}

^{†1} KDDI 研究所 ^{†2} KDDI ^{†3} 静岡大学

情報収集モジュールなどを組み込んだスマホアプリからの勝手な情報送信が問題となる中、利用者に送信情報を説明するアプリ向けのプライバシーポリシー（以後、アプリプラボリ）の策定が求められている。我々は、情報送信を伴うアプリとアプリプラボリの実態調査を行い、63%のアプリが情報送信を行い、うち9割がアプリプラボリを持たないか、持っていたとしても送信情報を正しく記載していないことがわかった。

そこで本研究では、Market がアプリの第三者検証機関として審査役を担い、正確で解りやすいアプリプラボリを生成・提示することで、利用者判断を仰ぐフレームワークを提案する。特徴として、アプリ解析力のある技術検証機構を持つことで、誤った申告とアプリプラボリの生成を予防できる。ここで、アプリのダウンロードや利用実績に応じた報酬を支払うレベニューシェアを適用する。これにより、過剰な情報送信や目的が判然としないアプリは利用者から倦厭され、報酬が低下する経済論を働かせる。本手法をアプリ Market に実装・運用した結果、16%のアプリしか情報送信を行わないこと、アプリの趣旨に沿った必要最低限の情報送信に限られることを確認する。

Third party review framework for privacy policy of application/contents

Keisuke TAKEMORI^{†1} Takamasa ISOHARA^{†1} Hideaki KAWABATA^{†1}
Ayumu KUBOTA^{†1} Tomoaki TAKANO^{†2}
Junya KANI^{†3} Masakatsu NISHIGAKI^{†3}

^{†1}KDDI R&D Laboratories ^{†2}KDDI ^{†3}Shizuoka University

Applications in a smartphone include data collecting libraries and send user data without notifications. A privacy policy for the smartphone application, which explains “what data are sent,” “why the data are sent,” and “who uses the data,” is recommended to be written. In our investigation, 63% of applications send user data. However, about 90% of applications do not notify users of “what data are sent” or notify users incorrectly.

In this research, we propose the third party review framework for privacy policy of smartphone application to a market place. A market’s reviewer compares the application behavior with the declaration from application developer. The application privacy policy is generated by the market place and is presented to the user. The revenue share is rewarded to the application developer according to the activation records. As the suspicious data sending application is not welcomed by the users, the revenue share become decreasing. We apply the proposed scheme to the market place and investigate the application behavior. As a result, only 16% of applications send user data, which is only used for the application function.

1. はじめに

スマホアプリによる勝手な情報送信がプライバシーの観点から問題視される中で、2012年8月に総務省から、利用者のプライバシー保護の目指すべき姿として、スマホ向けアプリの透明性の向上や、アプリ事業者／Market 運営者の果すべき役割などを記載した、「スマートフォン プライバシー イニシアティブ（以後、SPI）」がリリースされた[1]。特に、送信される情報・その目的・送信先などに関して、解りやすく説明するアプリのプライバシーポリシーを策定し、利用者から承諾を得ることが推奨されている。また、2012年10月には、モバイルコンテンツフォーラム（MCF）から、SPI を参考にしたアプリプラボリの執筆例が公開された[2]。EU では忘れられる権利[3]、米国では Do Not Track[4]が提唱され、ネット上でのプライバシー保護の取り組みと利用者関与の機会が推進されている。こうした流れ

を受け、日本国内の関係者が情報共有を図る連絡協議会も設けられた[5]。

我々は、アプリから実際に送信される情報の解析とアプリプラボリ中に送信される情報に関する記載の有無について、3回/3年間の調査を実施してきた。直近の調査では、63%のアプリが端末や SIM に付随する固定の ID（以後、グローバル ID）もしくはプライバシー情報を送信することが解り、うち11%のアプリしかアプリプラボリで送信情報を正しく説明していないことが解った。送信される情報の多くは、アプリ本来の趣旨に沿わない、過剰な情報送信が目立ち、これらについてアプリプラボリに正しく記載されないことが原因である。また、SPI が推奨する8項目の記載状況や、他社が調査した結果と照合を行い、多くのアプリプラボリにおいて、SPI 8項目を満たさないこと、用語や文章が曖昧で読み解き者によって判断がばらつく問題が明らかになった。そもそも、アプリプラボリではなく、個人情報

報保護法に基づく事業者としてのプラボリ（以後、事業者プラボリ）を流用しているものも多く、アプリから送信される情報を適切に説明できていない[6]。

本研究で解決すべき課題を纏めると、(i)第三者検証機関として、実際に送信される情報とアプリプラボリの整合性を確認すること、(ii)正確で解りやすいアプリプラボリを利用者に提示すること、(iii)アプリから必要最低限の情報送信に抑えることに取り組む。

本研究では、課題(i)から(iii)を解決するために、アプリ提供者となる Market 運営者が、アプリの第三者検証機関としてアプリの審査役を担い、適切なアプリプラボリを Market 側で生成し、利用者が送信される情報に納得した上で、アプリをダウンロードするフレームワークを提案する。具体的には、アプリ事業者がアプリを Market にアップロードする際に、アプリから送信される情報について申告し、申告内容とアプリの解析結果を突き合わせる。申告内容に矛盾が無ければ、用語と様式が定型化されたアプリプラボリが生成される。あくまで、アプリ事業者からの申告に基づき生成することで、内容はアプリ事業者の責任になっている。利用者は、スマホ画面 1 ページ程度に集約されたアプリプラボリを参考に、ダウンロードの判断を行う。Market 側は、アプリ事業者にアプリのダウンロードや利用実績に応じた報酬を支払う。アプリの趣旨に沿わない過剰な情報送信を行うものは、利用者に倦厭されダウンロード数が減ることになり、報酬額が減る。これにより、アプリの趣旨に沿った必要最低限の情報送信に抑え込むことができる。我々は本フレームワークをアプリ Market に実装・運用した。評価として、アプリから送信される利用者情報が 16%に抑えられていることを確認し、課題(i)と(ii)に取り組んだことで、課題(iii)をも解決できた実績を示す。

2. 実態調査

2.1 利用者情報

表 1 に、本研究で注目する利用者情報を纏めておく[1]。スマホ特有のグローバル ID とプライバシー情報であり、利用者に直接結び付かず、利用者側で取替えが可能な cookie やアプリ独自の ID を含めていない。

表 1 スマホにおける利用者情報

グローバル ID	International Mobile Equipment Identity (IMEI)、International Mobile Subscriber Identity (IMSI)、SIM serial number (ICCID)、OS 生成 ID、電話番号、MAC アドレス
プライバシー情報	メールアドレス、電話帳、位置、インストールアプリ名、アプリ実行ログ（含：実行アプリ名、通話履歴など）

2.2 3 回／3 年の実態調査

我々は、3 回／3 年に渡り、スマホ向け無料アプリから送信される利用者情報に関する実態調査を行ってきた。アプリは、日本のドメインから参照した際の人気順にダウンロードしている。結果を表 2 に示す。プラボリとの整合性に関する調査結果も示しているが、対象にしたプラボリとして、アプリプラボリと事業者プラボリの両者を読み解いた結果であることに注意されたい。図 1 に、プラボリ記載の正誤関係を示しておく。実際に送信された情報が全てプラボリ内に記載がある場合を「白」とし、一部でもプラボリに記載が足りない場合を「灰」、そもそもプラボリを持たない場合を「黒」としている。プラボリには、実際に送信されない情報を広く記載されていても良いとしている。

表 2 スマホアプリからの利用者情報の送信状況

	2011.8-2012.1 調査(400件)	2012.4-2012.5 調査(100件)	2013.2-2013.3 調査(100件)
情報収集モジュールを組み込んだアプリ	56.9%*1 (558件)	82% (82件)	63% (63件)
利用者情報を送信するアプリ	45.3%*2 (181件)	81% (81件)	63% (63件)
プラボリに送信情報が正しく記載のアプリ(白)	17/181件=9% 17/400件=4%	2/81件=3% 2/100件=2%	7/63件=11% 7/100件=7%
プラボリに送信情報が誤って記載のアプリ(灰)	7/181件=4% 7/400件=2%	13/81件=16% 13/100件=13%	29/63件=46% 29/100件=29%
プラボリが無く利用者情報を送信するアプリ(黒)	157/181件=87% 157/400件=39%	66/81件=81% 66/100件=66%	27/63件=43% 27/100件=27%

*1 この調査のみ980件のアプリを対象としている。

*2 2011.8-2012.1の調査ではSSL通信で送信される利用者情報を対象外。

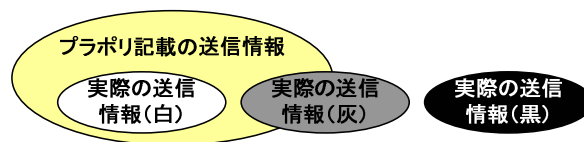


図 1 プラボリ記載内容の正誤関係

SPI は 2012 年 8 月に公開された。表 2 の 2011、2012、2013 年の 3 列は、それぞれ空白期、SPI 公開前、SPI 公開後の状態であることを勘案して参照すると解りやすい。

2012 年 4-5 月の情報収集モジュール[7]-[13]の組み込み率と利用者情報の送信率が 8 割を超えているのに対して、2013 年 2-3 月では、6 割程度になっており、SPI のリリースによって、素行が良く解らない外部の情報収集モジュールの組み込みや、不必要な利用者情報の収集を控えるアプリ事業者が現れてきたことが伺える。また、アプリもしくは事業者プラボリを持たずに勝手な情報送信をするアプリ(黒)が、87%→81%→43% へと減少している。送信情報が誤って記載されているものの、プラボリを通じて利用者に説明しようと努力が伺えるアプリ(灰)が、4%→16%→43% へと増加している。特に、SPI 公開前後で減少と増加の変化量が著しい。これより、SPI[1]や MCF ガイド[2]を参考にプラボリを書く流れが起きていることが伺える。

<Optional Permission>

android.permission.ACCESS_COARSE_LOCATION or
android.permission.ACCESS_FINE_LOCATION

また、Flurry Agent に位置情報を取得させたい場合には、
FlurryAgent.setReportLocation(false/true)

の API を true に設定して利用するよう説明がある。さらに、
事業者のホームページ (HP) にアプリプラポリが掲載され
ており、Android ID と位置情報を利用する旨が記されてい
る。アプリ事業者が本モジュールから送信される利用者情
報を把握することは可能であり、透明性が確保された情報
収集モジュールと言える。

我々の動的解析で、Android ID、IMEI、IMSIを送信することを確認したある広告モジュールについて、アプリへ組み込むまでの設定・解説書の状況を紹介します。まず、アプリのマニフェストファイルに、以下のパーミッションを書くよう述べられている。

android.permission.READ_PHONE_STATE

3. アプリ Market が担う第三者検証フレームワークの提案

利用者がアプリプラボリを参照・承諾する主なタイミングは、**Market** からアプリをダウンロードする前とアプリの利用時である。我々は、アプリのセキュリティ品質に一定の役割が期待される **Market** に注目し、アプリを利用者に届ける **Market** 運営者が第三者検証役を担うプライバシー審査のフレームワークを提案する。

2 章の議論から本研究で解決すべき課題を以下に纏める。

- (i) 第三者検証機関として、実際に送信される情報とアプリプログラムの整合性を確認すること
- (ii) 正確で解りやすいアプリプログラムを利用者に提示すること
- (iii) アプリから必要最低限の情報送信に抑えること

図 4 に、アプリ Market が主体となって課題(i)から(iii)を解決する第三者検証フレームワークを提案する。

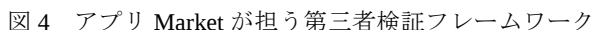
図3 情報収集モジュールから送信された利用者情報

情報収集モジュールが扱う情報についてアプリ事業者への説明の事例を2つ紹介する。

アプリの利用統計を調査するモジュールとして Flurry がある[7]。我々が調べた Android アプリ向け Flurry Agent は、Android ID と位置情報を送信する機能を持っていた。Flurry Agent をアプリに組み込むまでの設定に関する説明として、アプリの Manifest ファイルに、以下のパーミッションを書くよう述べられている。

<Required Permission>

© 2013 Information Processing Society of Japan



- ### 3.3 (a) アプリ申告

尚、「⑧プライバシーポリシー変更の手続きの説明」については、アプリがバージョンアップ・投稿される度に、送信情報を申告し、新アプリプラポリが新アプリとセットで公開されるため、既に⑧を満たしており、記載はない。そもそも、個人情報保護法に基づく事業者プラポリについては、様々な事業を手がける事業者の実態に合わせて柔軟

お密着情報の外部送信有無		☒ あり ☐ なし								
②	送信するお密着情報	メールアドレス								
⑥-2	送信元	☒ アプリ提供者 ☐ 情報収集モジュール								
①	事業者名	medika								
⑦										
④	送信する目的	目的								
⑥-1	送信先種別	☒ アプリ提供者 ☐ 第三者提供								
	送信先									
③	取得方法	☒ 自動 ☐ 手動								
	URL									
		追加								
⑤	お密着情報の送信や利用の停止									
<table border="1"> <tr> <td>送信停止の方法</td> <td> </td> </tr> <tr> <td>送信停止によるアプリへの影響</td> <td> </td> </tr> <tr> <td>送信情報の削除方法</td> <td> </td> </tr> <tr> <td>送信情報の削除によるアプリへの影響</td> <td> </td> </tr> </table>			送信停止の方法		送信停止によるアプリへの影響		送信情報の削除方法		送信情報の削除によるアプリへの影響	
送信停止の方法										
送信停止によるアプリへの影響										
送信情報の削除方法										
送信情報の削除によるアプリへの影響										

図5 送信情報に関する申告画面

もし申告内容に不備があれば、アプリを不合格として、アプリ事業者に再申告を促す。ここでのポイントとして、アプリプラポリの様式／枠を **Market** 運営者が用意したとしても、申告やその修正を全てアプリ事業者が主体となっていくことで、内容の責任元がアプリ事業者になっていることである。

技術検証で合格した場合は、アプリプラボリの概要版（図 6）と詳細版（図 7）が生成され、アプリが公開される。利用者がアプリをダウンロードする前に、送信される利用

者情報を確認できるようになっている。

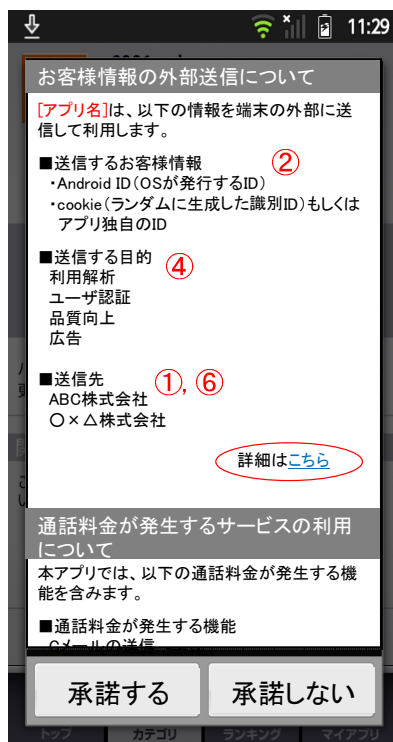


図6 概要版アプリブラボリ

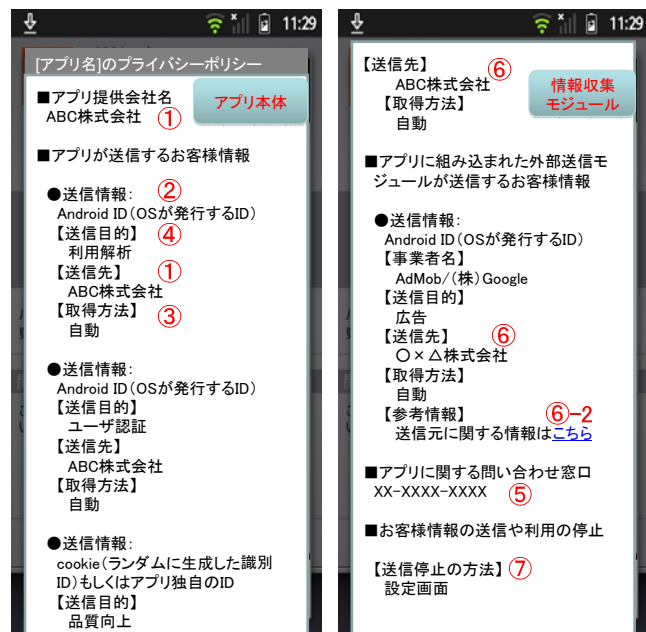


図7 詳細版アプリブラボリ

図6の概要版アプリブラボリでは、SPI 8項目のうち、②送信される情報、④目的、①、⑥送信先を、箇条書きすることで、判断に欠かせない重要事項をスマホ画面の1ページ程度で参照できるようになっている。

図7の詳細版アプリブラボリでは、①アプリ本体に関する説明部と、⑥第三者提供（含：情報収集モジュール）の

説明部に分けた構成になっている。両者とも、②送信される情報ごとに、④目的・①、⑥送信先、③自動/手動を結び付けて説明する。ここで、④目的や①、⑥送信先が複数に分かれる場合には、全ての組み合わせを②送信される情報を主語にして列挙する。尚、⑥-2 情報収集モジュールに関してアプリブラボリがある場合には、そのURLを記載する欄を設けている。

ここでのポイントとして、情報送信を行うアプリに限って、図6,7の承諾画面がポップアップ形式で利用者に通知されるようにすることである。この理由として、

- 情報送信を伴わないアプリについても承諾画面が表示されると、利用者に慣れが生じてしまい、内容の確認が疎かになることを防ぐためである。狼少年化を避け、情報送信をとまなうアプリに絞って、正しく読みやすいアプリブラボリを提示し、利用者の判断を仰ぐことが重要である。
- Market側の技術検証者は、②送信される情報、④目的、①、⑥送信先について、記載の有無や整合性は確認できるが、その妥当性については判断が難しい。そこに、利用者側の判断が入るよう、概要版ブラボリで端的に解りやすく、詳細版ブラボリで正確に伝える。不安や不信を感じるアプリはダウンロード数が低下し、Market運営者からアプリ事業者へ支払われる報酬額が減少する。これにより、もしアプリ本来の機能に利用者情報が不要な場合には、ポップアップの承諾画面が表示されないよう、情報送信を取りやめる判断に至る。必要最低限の情報送信に抑える経済論を働かせるモデルである。

3.6 (d)アプリブラボリ参照機能

SPIでは、アプリから任意のタイミングでアプリブラボリを参照できることが推奨されている。そこで、情報送信をとまなうアプリについては、アプリ内にアプリブラボリを参照できる機能を持つことを必須化する。

参照先として、Marketが生成したアプリブラボリへのリンク、アプリ内に組み込まれたアプリブラボリのファイル、アプリ事業者HPにあるアプリブラボリへのリンクがある。ポイントとして、第三者検証機関であるMarketで生成されたアプリブラボリへのリンクを推奨することである。この理由として、

- 整合性が検証されたアプリブラボリであり、一定の正確性が期待できるためである。
- アプリブラボリは、アプリの保証書の役割を果たすものであり、アプリ事業者が任意のタイミングで書き換えられる状況は好ましくない。Market生成のアプリブラボリは勝手な書き換えはできない。アプリ内にファイル形式で持つ場合も、署名によって担保される。
- 正確性が期待されるMarket生成のアプリブラボリと、アプリ内ファイルやアプリ事業者HPのアプリブラボ

リの記載に食い違いがでることで、矛盾を生じる。

- アプリプラポリは、アプリ事業者の法的保護の役割を果たす側面を持ち、Market 運営者は、アプリ事業者が自ら作成したアプリプラポリの矛盾や不備に対してコメントし難い。Market 運営者が申告内容に沿って生成したものであれば、Market への投稿ルールとして、コメントバック可能である。

追記として、本 Market で生成されるアプリプラポリは、グローバルに公開されるものである。よって、本 Market から配布されるアプリの参照先として利用できるだけでなく、他の Market に投稿された同じコード・動作のアプリであれば参照先として利用しても良い。

4. 評価

我々は、3章の提案手法を実際のアプリ配信 Market に適用し、運営してみた。ここで、図5の申告内容は、図6の概要版アプリプラポリに沿った簡略化されたものを利用し、図7の詳細版アプリプラポリは未適用である。この運営で得られた結果を本論文の評価として、以下に述べる。

4.1 利用者情報を送信するアプリ

2013年5月1日からさかのぼって投稿された直近100件のアプリに注目し、表1に示す利用者情報の送信アプリ数を調査した。

結果、16/100件=16%のアプリが利用者情報を送信していた。表2より、2013年2-3月の一般のMarketでは63%のアプリが情報送信を行うのに対して、1/4程度に抑えられていることがわかる。適用されたMarketには、

- a) Market から利用実績に応じて報酬を支払うコース
→ 利用者情報を送信する広告モジュールを禁止
- b) Market からの支払の無いコース
→ 情報収集モジュールに関する禁止事項なし

が設けられている。多くのアプリがa)に登録されており、広告モジュールによる情報送信がb)に限られることが主因である。但し、b)コースのアプリについても、広告モジュールを組み込まず、ポップアップ・承諾画面がでないものもある。次に、利用統計を把握するモジュールは、a)、b)ともに適用できるが、情報送信を伴うアプリは、ポップアップ・承諾画面が入るため、アプリ本体が情報送信をともなわない場合には、極力ポップアップを避けたい傾向があるようである。的確に送信情報を検知する技術検証フェーズを持つMarketにおいては、アプリプラポリとの整合性を確認し、申告ミスの指摘や利用者承諾を設けることで、アプリ本来の機能に必要な利用者情報の送信に抑制される様子が伺える。

4.2 検証で失格したアプリのその後

2013年5月1日からさかのぼって、一旦は申告ミスを指摘され不合格になった後に、合格となって公開されたアプ

リ10件について追跡した。

- ・ 6/10件が、②送信される情報、①,⑥-2送信先のいずれかの申告ミスが修正された。
- ・ 4/10件が、情報収集モジュールを停止/削除するというアプリ仕様が修正された。

10件中5件は、アプリの利用統計を収集するモジュールを組み込んだものであり、1件が前者の申告ミスの修正で、4件が停止/削除のアプリ仕様の修正の対応であった。このことから、アプリプラポリの申告ミスの主因は、外部の情報収集モジュールを組み込むことで生じていることがわかる。また、アプリ本来の機能に必要な情報のみ送信されるよう促されている様子がわかる。

5. まとめと期待

スマホアプリからの勝手な利用者情報の送信が問題になる中、アプリMarketが主体となって、正確で解りやすいアプリプラポリを生成・提示し、利用者判断を仰ぐ第三者検証フレームワークを提案した。ここに至るまでに、自らプラポリの実態調査を行い、多大な工数を要する割には的確に読み解けない状況を認識し、現時点でアプリ事業者が書いたアプリプラポリに基づく第三者検証を妥当なコストで運用することは不可能であると結論付けた。そこで、アプリ事業者にSPI 8項目を申告して貰い、これと実際の送信情報との整合性を確認する検証モデルを考案した。申告に基づき、概要版と詳細版のアプリプラポリを生成し、利用者に内容の妥当性の判断を仰ぐ。ここに、アプリのダウンロードや利用実績に応じて報酬を支払うレベニューシェアを適用する。過剰な情報送信や目的が判然としないアプリについては、利用者から倦厭されるため、必要最低限の情報送信になるような経済論を働かせている。本スキームをアプリMarketに実装・運用した結果、16%のアプリしか情報送信を行わず、送信される情報もアプリの趣旨に沿ったものに限られることがわかった。追記として、今回のMarketへ投稿されたプラバシー対策済みのアプリが、世界的なアプリMarketにそのまま投稿されているケースを確認している。本Market検証が、グローバルMarket上のアプリにも良い影響を与え始めている現われである。また我々は、情報送信をともなうアプリについては、アプリ内にアプリプラポリを参照する機能を持つことを必須化する。その参照先として一定の正確性が期待されるMarket側で生成されるアプリプラポリを推奨している。

経済論を働かせることができるMarketに第三者検証機能を担わせる効果は高く、本手法を業界のデファクトへと導くことで、スマホアプリ市場全体の信頼向上が期待される。我々はその期待に応えたいと思う。

謝辞

本研究の2章の実態調査を纏めるにあたり、読み解き結

果を共有頂けた日本総研(株) 東氏、前田氏に深謝する。また、アプリブラポリと事業者プラポリの区分をアドバイス頂けた産業総合研究所 高木氏、渡辺氏に深謝する。

参考文献

- 1) 総務省, “スマートフォン プライバシー イニシアティブ”,
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
http://www.soumu.go.jp/main_content/000171224.pdf
- 2) MCF, “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”,
http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf
- 3) European Commission, April 2010, “A comprehensive approach on personal data protection in the European Union: Right to be Forgotten,” COM(2010) 609 final, Brussels.
http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
- 4) Federal Trade Commission (FTC), 2010, “Endorses ‘Do Not Track’ to facilitate consumer choice about online tracking,”
<http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.
- 5) スマートフォンの利用者情報等に関する連絡協議会(SPSC),
http://www.mcf.to/press_comment/pdf/spsc_press_20121004.pdf
- 6) 一瀬, 高木, 山口, 渡辺, “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”, 情処, CSEC62-61, 2013 年 7 月.
- 7) FLURRY, <http://www.flurry.com/>,
<http://www.flurry.com/privacy-policy.html>,
<http://support.flurry.com/index.php?title=Analytics/GettingStarted/TechnicalQuickStart/Android>,
<http://support.flurry.com/index.php?title=Analytics/Code/Doc/Android>.
- 8) Google Analytics, <http://www.google.com/analytics/>.
- 9) AdLantis, <http://sp.www.adlantis.jp/>.
- 10) i-mobile, <http://i-mobile.co.jp/en/index.aspx>.
- 11) nend, <http://nend.net/>.
- 12) Admob by Google, <http://www.google.com/ads/admob/>.
- 13) AMoAd, <http://www.amoad.com/>.
- 14) 竹森敬祐, 他 5 名, “スマートフォンアプリ向け独自 ID の生成・管理”, 情処, CSEC59-8, 2012 年 12 月.
- 15) 磯原, 川端, 竹森, 窪田, “XML を用いたモバイルアプリのプライバシーポリシーの運用”, 信学, SCIS シンポジウム, 2013 年 1 月.
- 16) 磯原, 川端, 竹森, 窪田, “Android アプリの静的解析を用いた利用 API と外部モジュール検知によるプライバシーポリシー作成支援機構”, 情処, CSEC62-63, 2013 年 7 月.