スマートフォン上のアプリケーションにおける利用者情報の
取扱いに係る技術的検証等の諸問題に係る実証調査研究

プライバシーポリシー・解析結果突合手順書

平成 29 年 2 月 1 日

改訂履歴

版数	日付	変更理由	変更内容	変更者
1.0	H29/2/1	新規作成	1.0 版作成	

目次

用語の定義

用語	内容
SMS	相手先の電話番号だけで約 70 文字前後のメッセージが手軽に送受信できる、ショートメッセージサービス
契約者固有 ID(ICCID)	Integrated Circuit Card ID の略。SIM カードについている固有の ID である。
契約者固有 ID(IMSI)	International Mobile Subscriber Identity の略。契約者を一意に識別するもの
静的解析	Android アプリケーションの解析手法で、アプリケーションを実行せずに得られる情報（API:利用するアプリケーションインターフェース・バイトコード等）を基に利用者情報の送信有無・内容の解析を行うもの
端末固有 ID(IMEI)	International Mobile Equipment Identity の略。端末を一意に識別するもの
デバイス固定 ID(MAC アドレス)	Media Access Control address の略。ネットワーク機器を識別するための装置固有のアドレス
動的解析	アプリケーション実行時の挙動から得られる情報を基に、利用者情報の送信有無・内容の解析を行うもの
プライバシーポリシー	プライバシーに関する情報の取り扱いについて定めた規範のこと
プラポリ	プライバシーポリシーのこと

1　はじめに

本手順書は、平成 28 年度の総務省施策である「スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る実証調査研究の請負」として、平成 27 年度に総務省が実施した「スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る技術的検証等の諸問題に係る実証調査研究の請負」において実施したプライバシーポリシーと解析結果との突合手順についてまとめたものである。

2　概要

2.1　手順の全体像

静的解析の実行結果とプライバシーポリシー調査シート（以下、プラポリ調査シートという）、動的解析結果とプラポリ調査シートの突合手順について確認した。(「図 2.1-1 突合イメージ」にあるオレンジ色枠の手順)

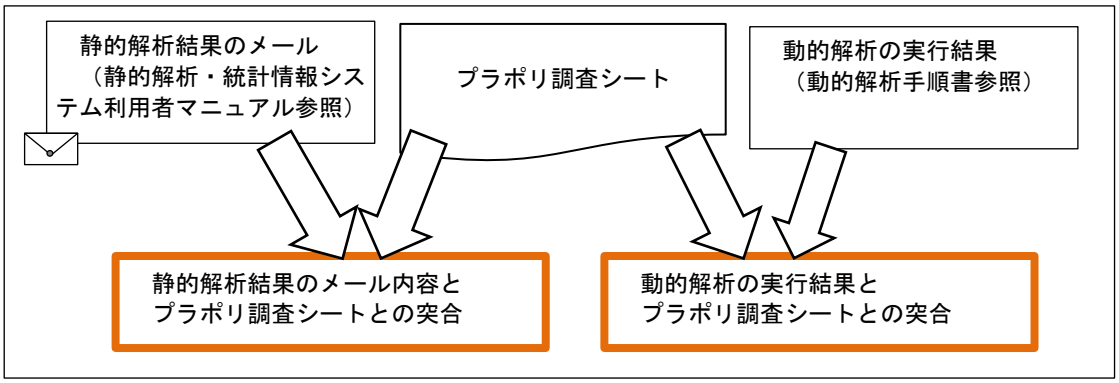

図 2.1-1 突合イメージ

2.2　前提条件

突合を行う上で必要な以下の解析結果を準備する。

- プラポリ調査シート（Excel）
- 静的解析結果のメール
- 動的解析の実行結果

静的解析結果および動的解析結果は、以下の手順書を参照のこと。

- 静的解析・統計情報システム利用者マニュアル
- 動的解析手順書

3　解析結果突合

解析結果の突合は、プラポリ調査シートに記載された対象項目との比較により実施する。

3.1　突合項目について

解析の対象となる項目について以下に示す。
解析対象が(〇)となる項目に対して突合を行う。

項番	プラポリ調査シートに記載されている項目	解析対象		
		静的解析	動的解析	
			送信有無	送信先
1	OS 生成 ID (AndroidID)	〇	〇	〇
2	端末固有 ID (IMEI)	〇	〇	〇
3	契約者固有 ID (IMSI, ICCID)	〇	〇	〇
4	デバイス固有 ID (MAC アドレス)	〇	〇	〇
5	TEL 番号	〇	〇	〇
6	メールアドレス (Gmail アドレス)	〇	〇	〇
7	位置	〇	〇	〇
8	アドレス帳	〇	×	×
9	マイク	〇	×	×
10	カメラ	〇	×	×
11	加速度センサー	〇	×	×
12	SMS	〇	×	×

〇: 解析対象、×: 解析および突合対象外

3.2　静的解析結果との突合手順

以下の２つを利用して突合を行う。

・プラポリ調査シート
・静的解析結果のメール

3.2.1　プラポリ調査シートの確認

プラポリ調査シートのうち「②「スマートフォン プライバシー イニシアティブ」で示される 8 項目の記載状況」エリアの「2.取得される情報の項目」(「図 3.2-1 プラポリ調査

シートのイメージ（静的）」参照）を確認する。プラポリ調査シートの具体的な内容は、別途配布されているプラポリ調査シートを参照のこと。

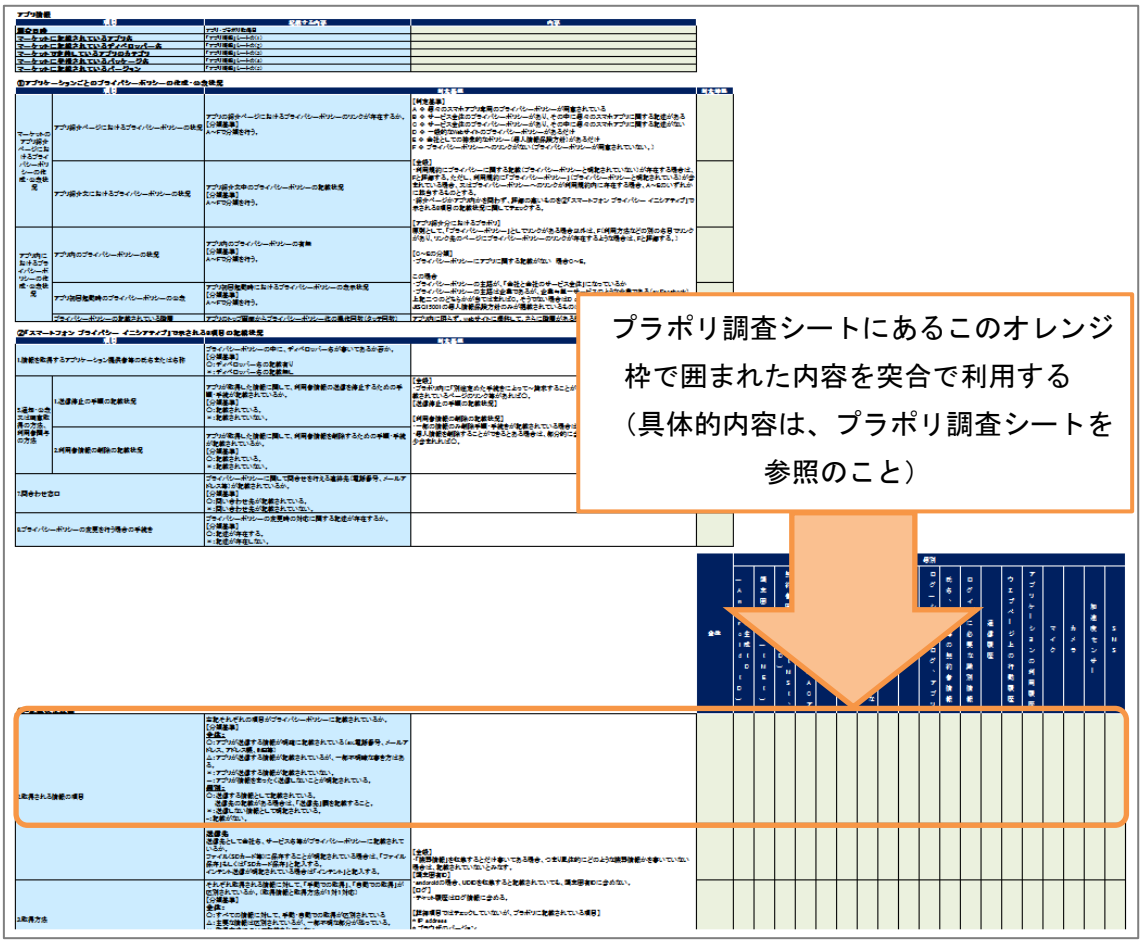

図 3.2-1 プラポリ調査シートのイメージ（静的）

3.2.2　静的解析結果の確認

静的解析ツールから届いた静的解析結果のメールに記載された【利用者情報送信】(「図 3.2-2 静的解析結果のメールにある【利用者情報送信】のイメージ」参照) を確認する。

【利用者情報の送信】

解析項目名	送信検出
OS生成ID	無
端末固有ID (IMEI)	有
契約者固有ID(IMSI)	無
契約者固有ID(ICCID)	無
デバイス固有ID(MACアドレス)	無
電話番号	有
メールアドレス	無
位置	無
アドレス帳	無
マイク	無
カメラ	無
加速度センサー	無
SMS	無

図 3.2-2 静的解析結果のメールにある【利用者情報送信】のイメージ

3.2.3　突合方法

「3.2.1 プラポリ調査シートの確認」で確認した内容と、「3.2.2 静的解析結果の確認」で確認した内容に対し突合を行う。突合は、以下の「表 3.2-1 突合項目 (静的)」に記載されている各項目について、「表 3.2-2 突合結果確認方法 (静的)」を参考に、結果が一致しているか、不一致かを確認する。

表 3.2-1 突合項目（静的）

プラポリ調査シート	メール(静的解析結果)	備考
OS 生成 ID（Android ID）	OS 生成 ID	
端末固有 ID（IMEI）	端末固有 ID（IMEI）	
契約者固有 ID（IMSI、ICCID）	契約者固有 ID(IMSI)	
契約者固有 ID（IMSI、ICCID）	契約者固有 ID(ICCID)	
デバイス固有 ID（MAC アドレス）	デバイス固有 ID(MAC アドレス)	
TEL 番号	電話番号	
メールアドレス（Gmail アドレス）	メールアドレス	
UUID（cookie など）	－	突合対象外
位置	位置	
アドレス帳	アドレス帳	
ログ（システムログ、アプリログ）	－	突合対象外
氏名、住所等の契約者情報	－	突合対象外
ログインに必要な識別情報	－	突合対象外
通信履歴	－	突合対象外
ウェブページ上の行動履歴	－	突合対象外
アプリケーションの利用履歴	－	突合対象外
マイク	マイク	
カメラ	カメラ	
加速度センサー	加速度センサー	
SMS	SMS	

表 3.2-2 突合結果確認方法（静的）

プラポリ調査シート	メール(静的解析結果)	突合結果
○(送信)	有	一致
○(送信)	無	不一致
×(非送信)	有	不一致
×(非送信)	無	一致
－(記載無し)	有	不一致
－(記載無し)	無	一致

※静的解析結果のメールで解析結果が「成功」ではない場合は、静的解析結果が「無」の場合でも、情報が外部へ送信されている可能性があります。

例えば、以下の場合は、突合結果が『不一致』となり、プライバシーポリシーに記載さ

れていないが、電話番号情報を外部へ送信している可能性があります。

・プラポリ調査シートの TEL 番号：×

・解析結果メールの電話番号：有

3.3 動的解析結果との突合手順

以下の２つを利用して突合を行う。

・プラポリ調査シート

・動的解析の実行結果

3.3.1 プラポリ調査シートの確認

プラポリ調査シートのうち「②「スマートフォン プライバシー イニシアティブ」で示される 8 項目の記載状況」エリアにある以下の 2 つの情報（「図 3.3-1 プラポリ調査シートのイメージ（動的)」参照）について確認する。

・2.取得される情報の項目

・6.外部送信・第三者提供・情報収集モジュールの有無

プラポリ調査シートの具体的な内容は、別途配布されているプラポリ調査シートを参照のこと。

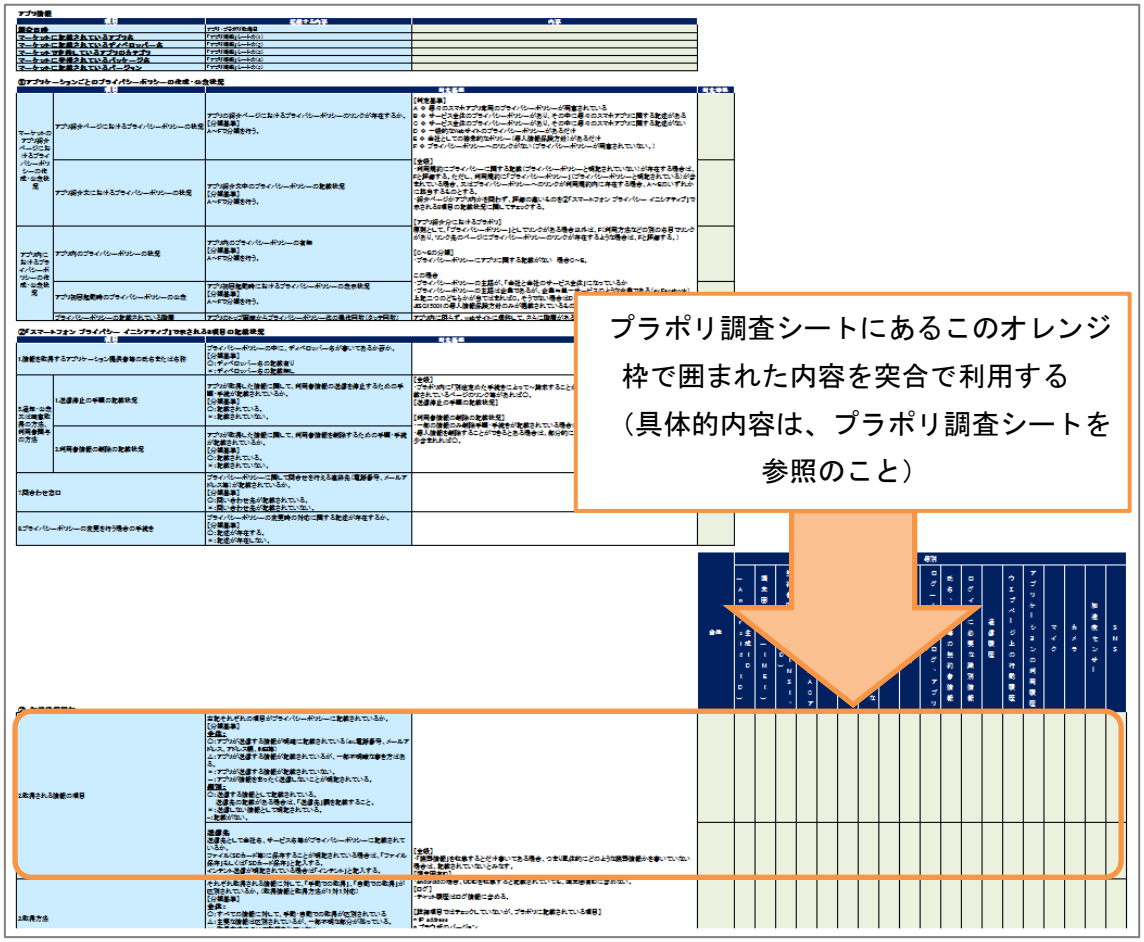

図 3.3-1 プラポリ調査シートのイメージ（動的）

3.3.2 動的解析結果の確認

proxy サーバーで実行した動的解析ツールの実行結果(「図 3.3-2 実行結果のイメージ(動的)」を参照）を確認する。

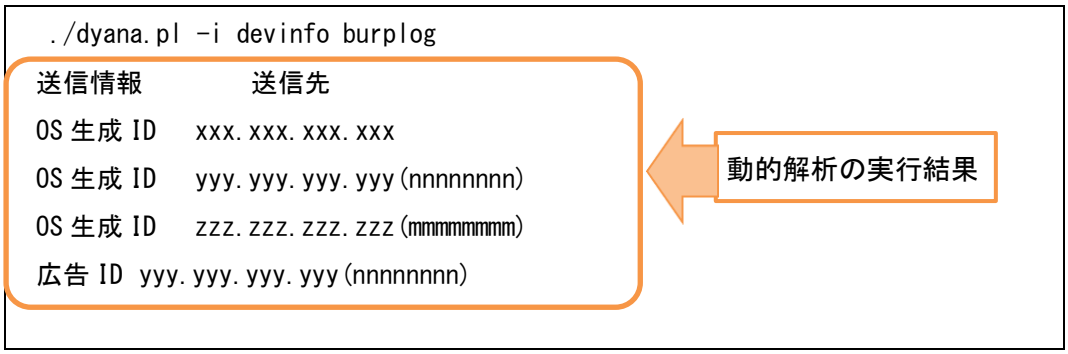

図 3.3-2 実行結果のイメージ（動的）

3.3.3 突合方法

以下の「表 3.3-1 突合項目（動的）」にある項目について、「表 3.3-2 突合結果確認方法（動的）」を参考に結果が一致しているか、不一致かを確認する。

動的解析ツールの IP アドレスの横には、whois コマンドで取得した情報のうち「Organization」の項目が表示される。この内容がプラポリ調査シートと等しい場合は一致とし、異なる場合は不一致とした。なお、Organization がホスティングの場合があり、全く異なるとは言い切れない場合があるが、本実証実験では一律不一致とした。

表 3.3-1 突合項目（動的）

プラポリ調査シート	動的解析の実行結果	備考
OS 生成 ID（Android ID）	OS 生成 ID	
端末固有 ID（IMEI）	端末固有 ID（IMEI）	
契約者固有 ID（IMSI、ICCID）	契約者固有 ID（IMSI、ICCID）	
デバイス固有 ID（MAC アドレス）	デバイス固有 ID(MAC アドレス）	
TEL 番号	電話番号	
メールアドレス（Gmail アドレス）	メールアドレス	
UUID（cookie など）	－	突合対象外
位置	位置	
アドレス帳	－	突合対象外
ログ（システムログ、アプリログ）	－	突合対象外
氏名、住所等の契約者情報	－	突合対象外
ログインに必要な識別情報	－	突合対象外
通信履歴	－	突合対象外
ウェブページ上の行動履歴	－	突合対象外
アプリケーションの利用履歴	－	突合対象外

マイク	－	突合対象外
カメラ	－	突合対象外
加速度センサー	－	突合対象外
SMS	－	突合対象外

表 3.3-2 突合結果確認方法（動的）

プラポリ調査シート	動的解析結果	送信先	突合結果
○(送信)	検出有	調査シートと同一	一致
		調査シートと異なる	不一致
○(送信)	検出無	－	不一致
×(非送信)	検出有	－	不一致
×(非送信)	検出無	－	一致
－(記載無し)	検出有	－	不一致
－(記載無し)	検出無	－	一致

例えば、以下の場合は、突合結果が『不一致』となり、プライバシーポリシーに記載されていない組織へ、OS 生成 ID を送信している可能性があります。

・プラポリ調査シートの OS 生成 ID：○
・動的解析の実行結果に OS 生成 ID（AndroidID）が出力されている：検出有
・動的解析の実行結果にある OS 生成 ID の送信先（IP アドレスや「Organization」情報）に、プラポリ調査シートに記載されていない送信先がある。：調査シートと異なる