資料 2-2

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に係る実証実験の請負

成果報告書　概要版

平成 27 年 3 月 31 日
エヌ・ティ・ティ・コミュニケーションズ株式会社

目次

1 はじめに 1

2 実証実験概要 1

2.1 目的 1
2.2 実施内容 1
2.2.1 仕様検討 1
2.2.2 システム開発 1
2.2.3 アプリケーション収集 1
2.2.4 システム検証 1
2.2.5 ユーザビリティ検証 2
2.3 実施スケジュール 2
2.4 実施体制 2

3 実証実験の結果 3

3.1 アプリケーション第三者検証システムプロトタイプの仕様検討・システム開発 3
3.1.1 プライバシーポリシー解析 3
3.1.2 アプリケーション解析 3
3.1.3 アプリケーションとプライバシーポリシーの突合機能 4
3.1.4 解析・突合結果の表示機能 4
3.2 システム検証 5
3.2.1 検証対象のアプリケーションについて 5
3.2.2 プライバシーポリシー解析 5
3.2.3 アプリケーション解析 7
3.2.4 情報収集モジュールデータベースの構築 10
3.2.5 プライバシーポリシー解析とアプリケーション解析の突合 10
3.3 ユーザビリティ検証 11
3.3.1 ユーザビリティ検証（アプリケーション利用者） 11
3.3.2 ユーザビリティ検証（アプリケーション提供者） 12

4 まとめ 13

4.1 実証実験まとめ 13
4.2 今後の取り組みについて 15

5 制度についての検証 18

5.1.1 法制度面の課題、調査・検討対象等 18

5.1.2 検討結果概要　-総論-..... 18

（参考）実証実験協議会の実施概要 23

（参考）制度・運用検討会の実施概要 24

（参考）モジュールおよびアプリケーションの提供者 25

用語の定義

（アルファベット順、五十音順）

用語	定義
Activity	Android アプリケーションの画面に相当するもの。
Manifest	Android のすべてのアプリケーションのルートディレクトリにあり、アプリケーションに関する必要不可欠な情報。
SSL	Secure Sockets Layer の略。インターネットなどの TCP/IP ネットワークでデータを暗号化して送受信するプロトコルの一つ。
TaintDroid	端末内の利用者情報にテイントと呼ばれるタグを付与し、追跡できるようにした Android　OS のこと。
XML	Extensible Markup Language の略。インターネット上で様々なデータを扱う場合に有効で、多様な情報を「情報の意味」と「情報の内容」に分けてテキストで記述する方法（言語）のこと。
インテント	Android の機能の一つで、アプリケーションソフト間やソフト内の機能間を繋ぎ合わせる仕組みのこと。
情報収集モジュール	広告表示やアプリケーションの利用頻度を解析する、アプリケーション本体の機能とは独立した、第三者が作成したプログラムのこと。
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プログラミングインターフェース・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。
テイント解析	追跡したい情報にテイントと呼ばれるタグを付与してデータ依存関係を解析する手法を指す。
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。
パーミッション	Android プラットフォームのセキュリティ機能であり、アプリケーションが必要とする権限を開発者があらかじめ明示し、インストール時にユーザーがそれを確認することで、インストールの可否を判断できる仕組み。
パケットキャプチャ	パケットの形でネットワーク上に送り出された通信データをキャプチャ（捕捉）する仕組みのこと。

1 はじめに

本成果報告書概要版は、平成 26 年度に総務省が実施する「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技術的検証等に係る実証実験の請負」（以下「本実証実験」という）についての成果報告書概要版である。

2 実証実験概要

2.1 目的

本実証実験では、「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技術面から第三者が検証する仕組み（以下「第三者検証」という）」について構築・実証する。

また、本実証実験を通じて、第三者検証における様々な技術的課題の解決および解決困難な課題の明確化、第三者検証の実効性確保に係る制度・運用的諸問題の抽出を行う。

2.2 実施内容

本実証実験では、以下の項目を実施した。

2.2.1 仕様検討

第三者検証システムのプロトタイプを構築するにあたっての仕様検討を行った。

2.2.2 システム開発

「2.2.1 仕様検討」で検討したシステムの開発を行った。

2.2.3 アプリケーション収集

アプリケーション提供者から申請を受け付ける手法（以下「申請型」という）にて、アプリケーションを収集した。

2.2.4 システム検証

「2.2.3 アプリケーション収集」で収集したアプリケーションを用いて、「2.2.2 システム開発」で開発したシステムの検証を行った。

2.2.5 ユーザビリティ検証

「2.2.2 システム開発」で開発したシステムの使い勝手、表現方法、見やすさの観点から検証を行った。

2.3 実施スケジュール

本実証実験は、以下のスケジュールで実施した。

平成 26 年 11 月～平成 26 年 12 月	アプリケーション第三者検証システムプロトタイプの仕様検討
平成 26 年 12 月～平成 27 年 1 月	アプリケーション第三者検証システムプロトタイプの開発
平成 27 年 1 月～平成 27 年 3 月	システム検証およびユーザビリティ検証

2.4 実施体制

「利用者情報の適切な取扱いの推進に向けたスマートフォン等のアプリケーションにおける諸課題に関する調査研究の請負」（以下「アプリ調査」という）の請負主体と緊密な連携を行いながら、スマートフォンアプリケーションプライバシーポリシー普及・検証推進タスクフォース（以下、タスクフォース）の各種 WG、業界団体、各種関連事業者等と連携・情報共有を図り、実証実験を推進した。

また、アプリ調査の請負主体と合同の検討会を概ね月 1 回程度実施した。

なお、検証対象となるアプリケーションおよびモジュールの募集に当たっては、地方自治体（全国都道府県・政令指定都市）、アンドロイダー株式会社等の協力を得た。

モジュールおよびアプリケーション提供者については、25 ページ「(参考）モジュールおよびアプリケーションの提供者」に示す。

3 実証実験の結果

本実証検証で実施した結果を以下に示す。

3.1 アプリケーション第三者検証システムプロトタイプの仕様検討・システム開発

3.1.1 プライバシーポリシー解析

プライバシーポリシーを解析し、取り込む機能を開発した。

3.1.2 アプリケーション解析

静的解析と動的解析を行うシステムを開発した。

3.1.2.1 動的解析

テイント解析（TaintDroid を活用）とパケットキャプチャ解析の 2 つの手法を用いた。

(1) テイント解析

TaintDroid 搭載の端末において、アプリケーション実行時のログを取得し、解析した。

(2) パケットキャプチャ解析

アプリケーション実行時の通信パケットをキャプチャし、解析した。

3.1.2.2 静的解析

(1) パーミッション解析

アプリケーションが必要とするパーミッション情報（利用者の許諾を必要とする端末内の情報）を抽出した。

(2) 内部 API・リソース解析

アプリケーションのバイトコードからツリー構造を解析した。
また、情報収集モジュールの利用有無を解析した。

(3) バイトコードトレース解析

利用者情報を取得し送信する機能の有無を解析した。

3.1.2.3 情報収集モジュールデータベース構築

情報収集モジュールを解析し、解析結果を格納するデータベースを構築した。

3.1.3 アプリケーションとプライバシーポリシーの突合機能

プライバシーポリシーの解析結果とアプリケーション解析結果を突合し、結果を出力する機能を開発した。

3.1.4 解析・突合結果の表示機能

(1) 解析・突合結果の表示

解析・突合結果の画面（アプリケーション利用者用、アプリケーション提供者用の 2 画面）を生成し、表示する機能を開発した。

(2) プライバシーポリシー作成支援機能

解析・突合結果をもとに、アプリケーション毎のプライバシーポリシー（概要版、詳細版、XML 版）を作成支援する機能を開発した。

3.2 システム検証

3.2.1 検証対象のアプリケーションについて

本実証実験では、アプリケーション提供者から事前申請を受けた 64 アプリケーション（Android:59、iOS:5）について、システム検証を実施した。

解析対象としたアプリケーションのカテゴリー分類を「表 3.2-1 解析対象アプリケーションのカテゴリー分類」に示す。

表 3.2-1 解析対象アプリケーションのカテゴリー分類

	ゲーム	ユーティリティ	ビジネス	情報提供	その他	合計
事業者・個人	9	25	2	1	6	43
自治体	－	－	－	18*1(4*2)	3*1(1*2)	21

*1:iOS を含む

*2： iOS

3.2.2 プライバシーポリシー解析

2013 年度の「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の現況等に関する調査研究の請負」において用いられた判断基準を活用し、プライバシーポリシーの解析を実施した。

(1) プライバシーポリシーの SPI 指針準拠度

「スマートフォン プライバシー イニシアティブ」（以下「SPI」という）に記載された 8 項目に対して準拠度を以下のように 5 段階に分けて評価した。

レベル 0：アプリケーションもしくはサービスに関するプライバシーポリシーが存在していない※
レベル 1：アプリケーションもしくはサービスに関するプライバシーポリシーが存在している
レベル 2：SPI で指定されている 8 項目のうち、重要 4 項目（項番 1,2,4,6）が記載されている
レベル 3：SPI で指定されている 8 項目が全て記載されている
レベル 4：レベル 3 に加え、プライバシーポリシーの概要版が存在している

※　ＳＰＩにおいては、スマートフォン上の利用者情報を、外部送信や蓄積を伴わない形で、端末内において一時的に取得・利用するのみの場合には、本指針の適用対象として想定していない旨が示されており、プライバシーポリシーの作成を必須としていない。

SPI で示される指針への準拠度を「表 3.2-2 SPI 指針準拠度」に示す。

表 3.2-2 SPI 指針準拠度

	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4
アプリケーション数	33	25	3	3	0

半数以上のアプリケーションにおいてプライバシーポリシーの記載がなかった。また、プライバシーポリシーの記載があったアプリケーションにおいても、重要事項の記載を満足しているものは少なかった。

(2) プライバシーポリシー解析に要した時間

プライバシーポリシー解析に要した時間を「表 3.2-3 プライバシーポリシー解析に要した時間」に示す。

表 3.2-3 プライバシーポリシー解析に要した時間

時間（分）	45	60	90	120	150	180	240
AP 数	15	11	25	4	4	4	1

大部分のアプリケーションにおいては、90 分以内に解析を完了したが、中には 4 時間近く要したものもあった。

時間を要した要因は、以下の通り。

- アプリケーション毎にプライバシーポリシーの掲載箇所（アプリケーション、Web、アプリケーションマーケット）が異なる。
- プライバシーポリシーに関わる記述が複数個所に分散されて掲載されている（利用規約、個人情報保護方針等）
- プライバシーポリシーへのリンク先が直接の掲載箇所では無い。(トップページへのリンク等)

上記要因により、プライバシーポリシーを探索する事に時間を要してしまった。

(3) プライバシーポリシー解析結果の妥当性確認

10 アプリケーションについて、複数の解析者による解析結果を比較した。比較の結果、判定が合致したものが 7 アプリケーション、判定が異なったものが 3 アプリケーションであった。判定が異なった理由は、曖昧・不明瞭な表現、記載箇所の難解さによるものであった。

3.2.3 アプリケーション解析

3.2.3.1 動的解析

(1) 実施概要

原則テイント解析を実施し、動作しなかったアプリケーションについてパケットキャプチャを実施した。また、解析手法の比較のために 12 アプリケーションについて、両手法による解析を実施した。

ただし、iOS についてはパケットキャプチャ解析のみを実施した。(TaintDroid 非対応のため)

解析手法毎のアプリケーション数を「表 3.2-4 解析手法毎のアプリケーション数」に示す。

表 3.2-4 解析手法毎のアプリケーション数

適用した動的解析手法	アプリケーション数
テイント解析のみを実施	36
パケットキャプチャ解析のみを実施	10(5*1)
テイント解析とパケットキャプチャ解析の両方を実施	18(6*2)

*1: iOS のアプリケーション数

*2：テイント解析だけでは網羅できない一部機能をパケットキャプチャにて補完したアプリケーション

外部送信を検出したものは 11 アプリケーション（Android:10、iOS:1）であった。

(2) 解析手法の比較

① 解析時間

解析に要する時間については、両手法共に平均 55 分程度であり、解析手法による差異はなかった。

② 外部送信の検出

両手法の解析を実施した 12 アプリケーションについて、外部送信の検出結果を「表 3.2-5 解析手法毎の外部送信検出数」に示す。

表 3.2-5 解析手法毎の外部送信検出数

適用した動的解析手法	アプリケーション数
テイント解析とパケットキャプチャ解析の両方で検出	3
テイント解析のみで検出	1
パケットキャプチャ解析のみで検出	0

③　解析手法の比較

テイント解析とパケットキャプチャ解析の特徴を「表 3.2-6 テイント解析およびパケットキャプチャ解析の特徴」に示す。

表 3.2-6 テイント解析およびパケットキャプチャ解析の特徴

比較項目		テイント解析	パケットキャプチャ解析
情報取得・送信の検出	外部送信の検出	○	△（情報加工時は不可）
	インテントの検出	○	×
	ファイルへの書き出しの検出	○	×
通信環境	キャリア通信	△（キャリアが限定される）	○
	Wi-Fi 通信	○	○
	暗号化通信（SSL）	○	△（プロキシを介さない通信は不可）
解析環境	OS バージョンへの依存度	△（動作しないものがある）	○
	端末への依存度	△（動作しないものがある）	○

(3) 到達率の検証

ユーザインタフェースとして定義される Activity の数を用いて、到達率の検証を行った。その結果を、「表 3.2-7 到達率」に示す。

表 3.2-7 到達率

アプリケーション	実行した Activity 数	Manifest にある Activity 数	到達率
A:情報提供	11	12	92%
B:ユーティリティ	10	13	77%
C:ユーティリティ	4	5	80%
D:情報提供	3	3	100%
E:その他	1	1	100%
F:情報提供	8	9	89%
G:その他	20	22	91%

C、F、G において外部送信を検出しており、外部送信した Activety の実行タイミングを「表 3.2-8 外部送信した Activity の実行タイミング」に示す。

表 3.2-8 外部送信した Activity の実行タイミング

アプリケーション	外部送信までに要した Activity 数	Manifest にある Activity 数	外部送信時の到達率
C:ユーティリティ	3	5	60%
F:情報提供	7	9	78%
G:その他	13	22	59%

3.2.3.2 静的解析

すべてのアプリケーション(iOS を除く)に対して静的解析を実施した結果、11 アプリケーションにおいて情報を取得・送信する可能性を検出した。

(1) 解析時間

解析に要する時間の平均が約 120 分であり、約 69%が 90 分以内に完了した。一方で、5 時間以上要したものが一部あった。解析に要した時間について以下に示す。

表 3.2-9 静的解析に要した時間

時間（分）	30	45	60	75	90	120	150	180	300	301 以上
AP 数	6	10	4	5	16	2	3	1	8	4

(2) 解析手法の比較

情報の送信について、静的解析および動的解析の結果比較（iOS を除く）を以下に示す。

表 3.2-10 静的解析および動的解析の結果比較（iOS を除く）

	動的解析で検出	動的解析で未検出
静的解析で検出	6	5
静的解析で未検出	4	-

動的解析で検出し、静的解析で検出できなかったものについては Google の API に渡すものや難読化されていたものがあった。

3.2.4 情報収集モジュールデータベースの構築

構築した情報収集モジュールデータベースについて、情報収集モジュールを構成するプログラム単位であるライブラリおよび、アプリケーションから呼び出す命令であるメソッドの登録数を「表 3.2-11 情報収集モジュールデータベースの内訳」に示す。

表 3.2-11 情報収集モジュールデータベースの内訳

収集方法		事業者数	ライブラリ数	メソッド数
A	SPI II 掲載情報および JSSEC 公開情報を基に調査*1	19	25	13071
B	実証実験協力事業者からの提供*2	7(3)	11(1)	14927(493)
C	アプリケーション解析（静的解析）により検出	12	15	846
合計		35	50	28351

（*1）SPI II 掲載情報および JSSEC（一般社団法人日本スマートフォンセキュリティ協会）公開情報には 103 事業者が掲載されていたが、リンク切れやすでに存在しない事業者を除き、特定できた 72 事業者を母数とする。

（*2）カッコ内に A との重複を示す。

3.2.5 プライバシーポリシー解析とアプリケーション解析の突合

プライバシーポリシー解析と動的解析の突合結果を「表 3.2-12 プライバシーポリシー解析と動的解析の突合結果」に示す。

表 3.2-12 プライバシーポリシー解析と動的解析の突合結果

		アプリケーション解析（動的解析）	
		送信あり	送信なし
プライバシーポリシーあり（レベル 1 以上）		6	25
	「送信あり」に関する記載あり	2	5
	「送信なし」に関する記載あり	0	6
	「送信あり」「送信なし」に関する記載なし	4	14
プライバシーポリシーなし		5	28

外部への送信が検出された 11 アプリケーションの内、プライバシーポリシーに情報送信の有無を記載せずに、情報送信を行うものが 9 アプリケーションあった。

3.3 ユーザビリティ検証

3.3.1 ユーザビリティ検証（アプリケーション利用者）

(1) 実施概要

検証結果の表示機能に関するユーザビリティ検証のために一般消費者（20 代～50 代男女 24 人）へのフォーカスグループインタビュー（以下「FGI」という）を行い、検証を実施した。

FGI では、事前説明を行った上で、プライバシーポリシーと解析結果を突合した結果画面に関してヒアリングを実施した。

(2) 総括

FGI でのコメントを「表 3.3-1 解析・突合結果画面（アプリケーション利用者用）に対するコメント総括」に示す。

表 3.3-1 解析・突合結果画面（アプリケーション利用者用）に対するコメント総括

分類	コメント総括
わかりにくい表現	専門用語が多く、理解が難しい サイトの目的、利用方法の解説がないと理解できない 項目間の関連性が分かりにくい
表示項目の過不足	表示をみてどうすればよいかアドバイスが欲しい 解析結果が 2 つ（静的解析、動的解析）あるとどちらで判断してよいか混乱する
画面構成の問題	一目で見て、評価結果が伝わってこない 画面スクロールが煩わしい 概要、詳細のどちらがメインの内容かわかりにくい

3.3.2 ユーザビリティ検証（アプリケーション提供者）

(1) 実施概要

本実証実験に参加したアプリケーション提供者に、プライバシーポリシーと解析結果を突合した結果画面を提示するとともに、突合結果を元にプライバシーポリシーの作成を支援する機能を提供し、アンケートを行った。

(2) 回答結果

29 件のアンケートを回収した。画面のわかり易さ、操作性、利用意向についての回答結果を以下に示す。

表 3.3-2　解析・突合結果画面（アプリケーション提供者用）のわかり易さ

わかり易い	ややわかり易い	普通	ややわかりにくい	わかりにくい
8	3	9	5	3

●コメント総括
・プライバシーポリシーに不足している項目が一目でわかる
・どうすれば改善できるかなどアドバイスも表示してくれるとよい
・表記、用語などでわからないものがある
・静的解析、動的解析の結果が異なる場合、どうすればよいかわからない

表 3.3-3　プライバシーポリシー作成支援機能の操作性

使い易い	やや使い易い	普通	やや使いにくい	使いにくい
8	7	6	3	3

●コメント総括
・わかり易く現状のもので十分利用できる
・用語説明を追加して欲しい
・利用者情報の送信についてどの単位でかけばよいかわからない

表 3.3-4　プライバシーポリシー作成支援機能の利用意向

利用する	どちらともいえない	利用しない
19	5	3

●コメント総括
・プライバシーポリシーの作成が簡単になる
・自社でツールを用意するよりも効率的になる
・項目漏れが防げる
・このままのユーザーインターフェースでは利用しにくい

※各質問項目に対する未回答の件数は省略した。

4 まとめ

4.1 実証実験まとめ

(1) プライバシーポリシー解析

プライバシーポリシーの解析においては、掲載箇所が一定ではないために、掲載の有無、掲載箇所の探索・特定に時間を要した。

また、事前にプライバシーポリシー解析時の判断基準を明確にしていたものの、曖昧・不明瞭な表現がある場合に、前後の文章の読み解き方によって判定が異なる場合があった。

(2) アプリケーション解析

静的解析は、アプリケーションのバイトコードを解析するため、アプリケーションに記述されている情報送信機能の有無を幅広く検出することができる。ただし、情報送信機能の有無を検出した場合でも、実際にはその機能を利用しないケースもあるため、確実に情報送信を行うとは言い切れない。

また、バイナリコードや難読化されたコードが含まれるアプリケーションにおいては、情報送信機能の有無を検出できない場合がある。

動的解析は、アプリケーションを動作させた結果をもとに解析を行うため、実際の情報送信そのものを検出することができる。ただし、すべての機能を網羅的に動作させることを担保する事が課題となる。

情報送信までの到達率の結果より、動的解析において情報送信を検知するには一定の操作が必要であることを確認した。

また、動的解析における各手法毎の特徴を確認した。

・テイント解析：暗号化通信や情報の加工、端末内の送信等、捕捉できる情報送信が多い
・パケット解析：捕捉できる情報送信は限られるものの環境への依存性は低い

(3) 情報収集モジュールデータベース

各モジュールの公開情報、各提供者より申請されたモジュールの情報、申請されたアプリケーションの解析結果をもとに、情報収集モジュールデータベースを構築した。

一方で、モジュールの入手に申請・登録が必要なものは対象より除いた。

(4) プライバシーポリシー解析とアプリケーション解析の突合

動的解析において外部への送信が検出された 11 アプリケーションの内、プライバシーポリシーに情報送信の有無を記載せずに、情報送信を行うものが 9 アプリケーションあった。

(5) ユーザビリティ検証

① アプリケーション利用者向け表示画面について

アプリケーション利用者向けに表示する画面としては、「表現方法がわかりにくい」「表示項目に過不足がある」「画面構成が最適でない」等の課題があり、改善が必要であることが示された。

② アプリケーション提供者向け表示画面について

アプリケーション提供者向けの表示画面について、多くの提供者から「問題がない」との回答を得たものの、一部「用語説明が欲しい」「アドバイスが欲しい」等の指摘があり、利用者向けと同様の課題があった。

プライバシーポリシー作成支援機能については、「効率的」「簡単」「漏れを防げる」等の好意的な意見が多く、利用意向が高いことがわかった。

4.2 今後の取り組みについて

(1) プライバシーポリシー解析

プライバシーポリシー探索・特定の所要時間を短縮するためには、プライバシーポリシーの掲載に関するルール作りが必要である。例えば、以下の対策が有効と考えられる。

・プライバシーポリシーをアプリケーションダウンロードページに掲載する

・アプリケーションダウンロードページ外への掲載の場合は、直接のリンクを記載する

曖昧・不明瞭な表現による判定結果の差異を解消するためには、プライバシーポリシーの定型化が必要である。本実証実験で試作した「プライバシーポリシー作成支援機能」の利用を促すことで、判定結果の精度向上が期待される。

さらに上記の対策を実施する事により、プライバシーポリシー探索・解析の自動化・効率化が見込める。

(2) アプリケーション解析

3 種類の解析方式（静的解析、動的解析（テイント解析・パケット解析））を併用し、アプリケーション解析を実施した。

精度向上のためには、各方式により特徴が異なるため、アプリケーションの実態に合わせた使い分け・併用が望ましい。今後更なる精度向上に向けては、新たな方式の調査・検討も必要となる。

また、将来の第三者検証における実運用に向けて、解析の効率化を行う必要がある。

現状において、静的解析は既に解析の多くをソフトウェアに任せる事ができるが、動的解析ではアプリケーションを操作する工程で多くの人的リソースを要している。

解決の方向性として、端末（アプリケーションを含む）の操作を自動実行するツール等の活用が考えられる。しかし、一般的なツール類は

- ランダム操作を行うツールは、網羅性の担保が難しい
- 操作内容の初期登録を求めるツールは、初期登録に人手を要するため自動化・効率化が難しい

等の問題があり、本実証実験での利活用のためには新たな方式等の調査・検討が必要である。

(3) 情報収集モジュールデータベースの構築

情報収集モジュールデータベースの完成度を高めるためには、継続的にアプリケーション解析を行いデータベースを拡充させていく必要がある。

また、動的にアプリケーションの部品をダウンロードする事によって、情報送信に関わる動作を変化させる情報収集モジュールへの対応が新たな課題である。

しかしながら、このような情報収集モジュールの動作変化は無限では無く、一定範囲での動作変化を示すと想定されるため、継続的にアプリケーション解析を行いデータベースを更新・拡充させていくことで、捕捉率を高めることが期待される。

(4) プライバシーポリシー解析とアプリケーション解析の突合

半数以上のアプリケーションがプライバシーポリシーを有していないことから、プライバシーポリシー作成のさらなる普及・啓発が必要と考えられる。ただし、動的解析の結果、アプリケーションの大半は利用者情報を外部に送信しておらず、プライバシーポリシーの掲載が必須ではないことには留意が必要である。アプリケーションのプライバシーポリシー作成状況については、アプリ調査で行われたプライバシーポリシーの作成状況に関する調査結果も踏まえて、考察が必要である。

また、プライバシーポリシーを有する場合において、ほとんどのアプリケーションでは情報送信を正しく記載できていない。アプリケーション提供者が、利用する情報収集モジュールの動作を十分に把握しきれないケースもあると考えられる。

今後、第三者検証サービスを提供することでアプリケーション提供者に対し、想定外の情報送信への気付きを促すことが可能である。さらに、「プライバシーポリシー作成支援機能」の普及・啓発により、情報送信の記載漏れを防ぐ効果が期待される。

(5) 解析・突合結果の表示

アプリケーション利用者向け、アプリケーション提供者向け画面に示された課題に対し、改善の方向性を決めるにあたっては、伝える手段を改善する（「表現方法」）、伝える内容の過不足を精査する（「表示項目」）、それらをふまえたトータルな最適化（「トータル構成」）という評価視点で検討していく必要があると考えられる。「表 4.2-1　解析結果の表示画面への改善方向性」に今後の検討項目を示す。

表 4.2-1　解析結果の表示画面への改善方向性

評価視点	改善方向性
表現方法	視覚的表現の利用
	平易な表現の利用
	補足説明の追加・表示
表示項目	評価結果の総括・アドバイスの追加
	検証結果の掲載内容・方法の変更
トータル構成	項目間の関連性が分かる構成に変更
	詳細情報の表示場所・表示方法の変更

(6) その他

① 非申請型アプリケーションの収集・解析

本実証実験では、申請型でのアプリケーション収集を実施したが、申請型の場合にはサンプル数が限られるため、市場で流通するアプリケーションの傾向を十分に把握することは困難である。

アプリケーション利用者に対して、より有益な情報・サービスを提供するためには、非申請型アプリケーションを解析対象として拡充することが必要である。

②　アプリケーションのアップデートへの対応

将来の第三者検証における実運用を念頭においた場合、アプリケーションのアップデート検知、アップデートから解析が完了するまでのタイムラグ等に関する対策について検討を行うべきである。

5 制度についての検証

5.1.1 法制度面の課題、調査・検討対象等

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第三者検証を実施するにあたっては、検証対象アプリケーションの静的解析および動的解析が必要となり、当該検証結果の表示・公開方法等、関連する法制度面での課題解決と第三者検証にあたっての現実的な運用方法が求められる。

当該第三者検証の実施および利用者が安心・安全にスマートフォン上のアプリケーションを利用する環境整備を実施するためには、マーケット運営事業者、キャリア、アプリケーション開発事業者、モジュール提供事業者、解析事業者等、多様な主体（マルチステークホルダー）の参画による多角的検討が必要であるとともに、

・通信の秘密
・個人情報保護
・プライバシー保護
・著作権法
・実務レベルで想定されるリスクの整理および手続きについての体系的整理

等の総合的な法制度の検討が必要である。

また、法制度面の検討の前提として、想定されるシステムの要件・環境を設定し、それに則った法制度面の検討が求められることとなる。

そのため、本検討会では本調査研究の実証実験に係るシステムの要件・環境および実証実験に係るプロセス、データを踏まえて、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第三者検証を実施するにあたって、以下の事項

・第三者検証が通信の秘密を侵害する可能性についての検討
・第三者検証（動的解析および静的解析）の実施に際しての著作権法上の検討
・第三者検証が利用規約に反する可能性についての検討（同意取得に関する課題等）
・第三者検証結果の表示・公開方法に関する検討（信頼性設計におけるリスク等）
・第三者検証（第三者認証）の在り方に関する検討
・第三者検証におけるその他課題の検討

について調査・検討を行い、アプリケーション第三者検証を実現するための業務フローを確立するべく、法制度面からの論点整理を行った。なお、以下に記載された見解は、本検討会の見解であり、法解釈に関する総務省の見解を示すものではないことを念のため申し添える。

5.1.2 検討結果概要　-総論-

上記の論点等の整理では、

・憲法第 13 条、第 21 条第 2 項
・電気通信事業法第 2 条、第 4 条、第 5 条
・個人情報保護法第 2 条第 1 項、第 15 条、第 16 条、第 18 条、第 20 条、第 23 条
・民法第 709 条

・特許法第 69 条
・著作権法第 30 条 4 項、第 47 条 6 項
・工業標準化法第 28 条（平成 16 年改正前）

の解釈およびその解釈に基づく運用を検討し、アプリケーション第三者検証を実現するための業務フローを確立するために、実質的な制度的障壁の解決を図った。

検討に際し、本実証実験での法制度面からの検討に加え、実験後の第三者検証機関における実運用を想定した場合についても同様の検討を行い、将来に係る課題の抽出を行った。

検討の結果、

1）一般的な権利制限規定の存在しない現行の著作権法のもとで、アプリケーションの第三者検証の為の静的解析が許されるか（いわゆるリバースエンジニアリングに係る問題）についての論点が挙がったが、本実証実験においては、アプリケーションの不適切な外部への情報送信の有無を分析することは、アプリケーションの機能を適切に享受するために必要なものとして、著作権法第 30 条 4 項「技術の開発又は実用化のための試験の用に供する場合」に該当し、著作権法上の支障が生じないように実施することが可能と解する結果を得た。しかしながら、実運用の場合は、同条は適用されないことになるが、当該解析がアプリケーションの著作物としての利用の促進に資することを考慮すれば、そもそも、損害賠償発生の可能性は低いか、あったとしても低いと考えられる。なお、差し止めについて言えば、著作権者は自らが著作権を有するアプリケーションについて著作権侵害を主張できるのみであり、本プロジェクト全般の差し止めを請求することはできないから、仮に、特定のアプリケーションの著作権者からの静的解析に対する差し止めが認められたとしても、第三者検証全般に影響するものとは考えにくい。

加えて、その前提としてのアプリケーションのダウンロードに関しては、一般にアプリケーションが公開されている場合、その利用のためにはアプリケーションのダウンロードが必須であることからすれば、アプリケーションの著作権者は、第三者による複製を予想し、許諾しているものと考えられ、少なくとも、黙示の許諾があると考えてよく、検証目的でのアプリケーションのダウンロードも許諾の範囲に含まれていると解釈してよいものという結論を得た。

しかしながら、著作権法上の問題が解決されたとしても、アプリケーション利用におけるライセンス契約等、アプリケーション利用に関する規約中に、リバースエンジニアリング行為が禁止されている場合が殆どであり、第三者検証が利用規約に反する可能性についての検討を実施した。その結果、

2）規約の同意そのものの有効性について、第三者検証主体が規約への同意があったものとして考えた場合においても、アプリケーションにおいて不適切な情報の外部送信がなされていないかどうかを確認するための動的解析・静的解析およびそのためのダウンロードがかかる規約の効力によって禁止されるとすれば、悪意のあるプログラム開発者に、当該プログラムの不正性の発覚を防ぐ手段を与えてしまうことに他ならず、このような禁止行為まで、法的保護に値するものとは考えられず、本実証実験での静的解析・動的解析が規約の違反である旨の訴えが提起されたとしても、裁判所としては、規約の趣旨を限定して解釈するか、かかる禁止を無

効又は同意の内容とならないと解釈するなどを行う可能性があり、かかる静的解析・動的解析行為の差止又は損害賠償を認める可能性は極めて低いものと考えられるという結論を得た。

次に、第三者検証結果の表示・公開方法に関して、専用のホームページ等を通じた一般への公表が想定されているが、スマートフォンアプリケーションの構造やサービスモデルが複雑化しており、常に技術的およびビジネスモデル面での進展がなされているため、技術的限界等によって検証結果とアプリケーションの動作とが異なる可能性が一定程度不可避的に存在する。そして、当該技術的限界や、検証過程での何らかの誤りのため、検証結果に示されない送信先に利用者情報が送信されるような場合も起こり得る。また、表示・公開方法によっては、特にアプリケーションや外部モジュールの提供者の許諾を得ないまま、低評価の検証結果をアプリケーションの名称等を明示して公表した場合に、提供者との間で紛争となるといった可能性も考えられる。以上、検証機関に生じ得る法的リスクとこれを低減させるための対処について検討を行った結果、

3)「一般利用者に対する法的責任」としては、特定のアプリケーション等を明示して公表した検証結果が客観的に誤っていた場合の検証機関の一般利用者に対する法的責任について考えられる。しかしながら、専門的知見による第三者検証機関が、信義則上、誠実公正に評価を行うべき義務を一般利用者に対して負い、この義務に反しない限り、結果として公表した検証結果と客観的事実との間に齟齬があったとしても、検証機関が一般利用者に対する法的責任を問われる可能性は低いという結論を得た。

しかしながら、法的責任を問われる可能性が皆無ではない以上、当該法的責任を低減させる措置を講ずることは重要であり、例えば、「検証結果の利用に関する規約や、検証結果を見る者の目にとまりやすいホームページ上の場所に、最善の注意を払って検証をしているが、検証結果が完全に正しいことや、プライバシーポリシーの内容に全く問題が無いこと、個人情報の取扱いが完全にプライバシーポリシーに記載された通りであることを保証するものではない、公表した内容はあくまで参考であり検証機関はこれを信頼したことにより生じた利用者の損害に一切責任を負わない」等の免責文言を明示する（個別の事案で完全に免責されるというわけではないが）などの対策を講じることが重要である。

また、検証の正確性（精度）の限界について一般の理解を得るため、検証の仕組み、方法、技術的限界ないし精度、プロセス、評価基準、検証結果や公表された内容の意味するところについて、典型的な問答集（FAQ）や図解を用いるなどによりその意味合いを正確にかつ分り易く表示し、透明性を確保することも、検証結果への信頼性を高め、紛争を予防する点から重要である。

「アプリケーション提供者、外部モジュール提供者に対する法的責任」については、マーケットから問題視され、社会的評価を低下させる名誉毀損であるとの主張されることも想定されるが、当該第三者検証の結果の公表が一般利用者のプライバシーの保護といった大きな社会的意義を有することを考えれば、公共性と公益性を充たし、その内容が合理的な根拠に基づく限り（真実性）、名誉毀損は成立しないと考えられる。また、検証結果が客観的に誤っていた場合も、上述した一般利用者に対する法的責任と同様の考え方が適応される。ただし、アプリ

ケーション開発事業者等に許諾を得ずに検証結果を公表する場合に、アプリケーション等提供者との紛争予防や法的リスクをさらに低減させるために、手続面について検討することは重要であり、検証結果を公表する前に、その内容を当該アプリケーション等の提供者に知らせ、そこに表れたプライバシーポリシーやアプリケーションの問題点を改善し、再検証を受けたり、検証過程での誤認の指摘を受けたりするなどの機会を設けることで、検証の精度向上、信頼性向上に資するとともに、提供者の評価結果に対する理解と受容も得やすくなり、検証結果の公表を巡る紛争のリスクを低減させることができると考える。また、第三者検証の実施と結果の公表を周知し、オプトアウト方式によって、希望しない提供者については検証や公表を取りやめる等の措置を講じることも考えられる。

以上、本実証実験でアプリケーション第三者検証を実施する場合においては、上記 1）～3）の検討結果により、以下の結論に至った。

専門的知見による第三者検証主体が、信義則上、誠実公正に評価を行うべき義務を一般利用者、アプリケーション提供者事業者等に対して負い、本検証結果の表示・公開については、技術的限界等によって検証結果とアプリケーションの動作とが異なる可能性が一定程度不可避的に存在し、法的責任を問われる可能性が皆無でない。しかしながら、当該第三者検証の実施および結果の公表が一般利用者のプライバシーの保護といった大きな社会的意義を有することを考えれば、公共性と公益性を充たし、その内容が合理的な根拠に基づく限り（真実性）、検証結果の表示・公開方法についても、技術的限界等の免責文言の明示、一般利用者にとっての分り易さと正確性や精度、基準の明確さ、Q&A の設置等、アプリケーション開発事業者等に対する適切な手続き等、法的リスク低減策を講じつつ選択することにより、法的リスクが吸収可能な程度にあると考えられることから本実証実験および実運用においてもアプリケーション第三者検証を実施することは可能という結論を得た。

最後に、実験後の第三者検証機関における実運用を想定した場合について、第三者検証（第三者認証）の在り方に関する検討を行った。

第三者検証（第三者認証）のそもそも目的は、アプリケーションの安全な利用環境の構築であり、消費者に対して十分にして正確な情報を提供できなければ、この目的を達することができない。故に、審査の結果、明らかにできたことしか保証してはいけないのは当然のことであり、審査対象外の事項について、消費者にとって理解が困難な留保を付けることは消費者に対して十分かつ正確な情報を提供したことにならないことに留意が必要であり、十分かつ正確なことに加え、消費者にとって分かりやすいものでなければならない。

また、基準を設けて第三者認証を行うことには、第一に、アプリケーションの安全性に関する情報を提供することはアプリケーションユーザーの保護に資するものであり、第二に、関係事業者が安心・安全なアプリケーションを作成し販売・頒布することの動機付けにもなるといったメリットを見出すことができる。そのような、第三者認証の組織・手続きの要求事項として、(a)透明性の確保、(b)公平性・中立性の確保、(c)十分なリソース、(d)正確性の確保な

どが求められているため、ユーザー情報の取扱いに関するアプリケーションの安全性の第三者認証について、上記要請を具体化するものとしては様々な組み合わせが考えられるが、その一例は以下が考えられる。

- ✓ 明確な審査基準を有しており、それが公表されていること。
- ✓ 審査のための十分なリソースがあること 、具体的には、関連法規やスマートフォンアプリケーションの実情に通じており、審査能力のある審査員を擁すること。
- ✓ 認証の対象となる事業者からの独立性・中立性を確保する仕組みが確立されていること。
- ✓ 適正な審査手続きを有しており、それが公表されていること。
- ✓ 定期的に再審査・認証を行うこと。

また、第三者検証（第三者認証）において未解決の問題としては、以下の二点が今後の検討課題として挙げられた。

第一に、認証（保証）の有効期間の問題がある。原則として、アップデート等によるアプリケーションの同一性が失われた場合には、認証は失効しなければならない。この点を留保事項として処理することは適切ではない。この問題を解決するためには、アプリケーションの同一性と認証の有効性を連動させる仕組みが必要である。

第二に、アプリケーションそのものには変更はなくとも、サーバーと連携して機能することによりアプリケーションの振る舞いが変わる場合をどうするかという問題がある。この場合も、認証の有効性を維持することはできないというべきであり、留保事項としての処理も不適切である。

これらの点について解決ができない場合には、消費者に対する認証（保証）という本実証実験で想定する第三者認証を行うことは困難である。

今後、上記第三者認証の組織・手続きについて更なる検討を進めるとともに、実証実験期間内に第三者検証のシステム設計をさらにアップデートし、上記未解決の問題についても解消し、実運用につなげていく取組を行う必要がある。

加えて、次年度以降の実証実験や実運用に向けて、以下の提言があった。

- **アプリケーション提供者向けに特化したサービスの提供**
  - アプリケーション提供者向けの具体的なサービスとして、情報収集（広告）モジュールの第三者検証、アプリケーションのプライバシー面の確認項目・検証方法の標準化、アプリケーション提供者向けの相談窓口などが挙げられた。
- **第三者検証の結果に応じて付与されるマーク等の不正利用対策**
  - 認証マークのモジュール等の作成による技術面からの対策、認証マークの商標登録を行い訴訟などで対応する法制度面からの対策などが存在するものの、海外事業者に不正利用された際に権利行使をどのように行うかという課題が指摘されている。

（参考）実証実験協議会の実施概要

有識者を招き、実証実験協議会を 2 回実施した。
各協議会の日程、テーマ、構成員は次のとおりである。

【テーマ】
スマートフォンアプリケーションの第三者検証プロトタイプシステムの仕様検討

【構成員】

所属	氏名（敬称略）
ソニーデジタルネットワークアプリケーションズ	松並　勝
KDDI 研究所	川端　秀明
NTT セキュアプラットフォーム研究所	名雲　孝昭
NTT ソフトウェア	奥地　優雅
総務省　総合通信基盤局　消費者行政課	神谷　征彦、渡邊　涼介、 齋藤　彰夫
日本総合研究所	東　博暢、小竹　庸平
NTT コミュニケーションズ	本間　康嗣、長谷川　昌寿、 斎藤　良輔

【各協議会の議題】

	日程	実施内容
第 1 回	平成 26 年 11 月 25 日	・本実証実験についての説明 ・第三者検証プロトタイプシステムの仕様説明 ・意見交換
第 2 回	平成 26 年 12 月 15 日	・前回コメントへの対応方針 ・修正版第三者検証プロトタイプシステムの仕様説明 ・検証・評価項目案について説明

（参考）制度・運用検討会の実施概要

今年度は、制度的な検討に加え、運用面での検討も同時に実施した。各検討テーマに合わせて上記制度検討会の構成員に加え、外部から有識者を招き、合計 4 回の検討会を開催した。各検討会の日程、テーマ、参加者は次の通りである。

	日程	テーマ	構成員※50 音順、敬称略
第 1 回	平成 26 年 11 月 17 日、18 日 ※1 部と 2 部に分けて実施	● 第三者検証が通信の秘密を侵害する可能性 ● 第三者検証の実施に際しての著作権法上の検討 ● 第三者検証が利用規約に反する可能性	● 東博暢（日本総合研究所） ● 上沼紫野（弁護士 虎ノ門南法律事務所） ● 森亮二（弁護士 英知法律事務所） ● 山田卓（弁護士 ユアサハラ法律特許事務所）
第 2 回	平成 26 年 12 月 18 日	● 第三者検証が利用規約に反する可能性 ● 第三者検証（第三者認証）の在り方 ● 民間部門における第三者検証機関の持続的な運営体制 （主に運営資金の獲得方法について）	● 東博暢（日本総合研究所） ● 上沼紫野（弁護士 虎ノ門南法律事務所） ● 佐藤進（アンドロイダー） ● 高木浩光（産業技術総合研究所） ● 三好眞（アイ・エス・レーティング） ● 森亮二（弁護士 英知法律事務所） ● 谷田部茂（日本スマートフォンセキュリティ協会） ● 山田卓（弁護士 ユアサハラ法律特許事務所）
第 3 回	平成 27 年 1 月 20 日	● 第三者検証結果の表示・公開方法 ● 民間部門における第三者検証機関の持続的な運営体制 （第三者検証機関の役割）	● 東博暢（日本総合研究所） ● 上沼紫野（弁護士 虎ノ門南法律事務所） ● 岸原孝昌（モバイル・コンテンツ・フォーラム） ● 竹森敬祐（KDDI 研究所） ● 森亮二（弁護士 英知法律事務所） ● 山田卓（弁護士 ユアサハラ法律特許事務所
第 4 回	平成 27 年 3 月 6 日	● 第三者検証の結果に応じて付与されるマーク等の不正利用対策 ● 検討会の報告書の取り纏め	● 東博暢（日本総合研究所） ● 上沼紫野（弁護士 虎ノ門南法律事務所） ● 森亮二（弁護士 英知法律事務所） ● 山田卓（弁護士 ユアサハラ法律特許事務所）

（参考）モジュールおよびアプリケーションの提供者

アンドロイダー株式会社の協力により、本実証実験に参加いただいたモジュール提供者、アプリケーション提供者は以下の通り（本成果報告書への掲載に同意いただいた提供者について、アルファベット順、50 音順に掲載）。

モジュール提供者

Glossom 株式会社
株式会社 アイモバイル
株式会社オルトプラス
カイト株式会社
株式会社ファンコミュニケーションズ
ライヴエイド株式会社
株式会社レボラボ

アプリケーション提供者

Busey
ElitApps, Ltd.
Fotor
GMO　Media（株）　スタンリーン　イエンハオ
Kuniyuki Nakagomi
Mtk Fujiu.jp
TEAM DAMOMO
UNI-UNI
株式会社 woodsmall
YILABO
株式会社エフ・ディー・シー
スターツ出版株式会社
株式会社トビオ
ピノ・アソシエイツ株式会社
ペンギンソフト
山川 武志
山本　徹
株式会社ライドアンドコネクト
株式会社ワーカービー