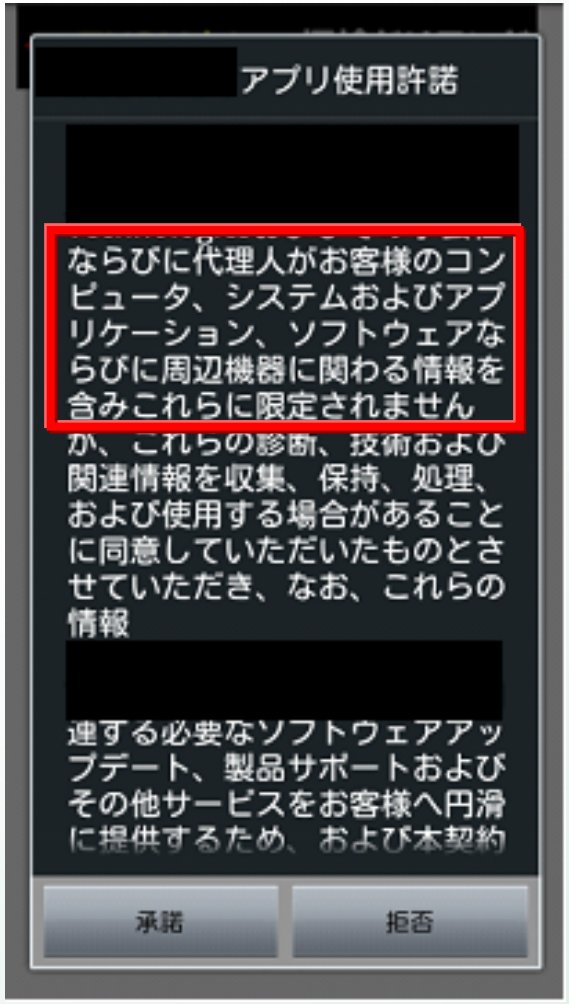
スマホ・アプリのプライバシーポリシー作成・開示についての考察

JSSEC 技術部会　アプリケーションWG
アプリ・プライバシーポリシー作成G／KDDI株式会社
リーダ　磯原 隆将

背景1　透明性が疑われるケース

■ アプリ･プライバシーポリシーに関わる問題
(1) 利用者情報を送信するにも関わらず、アプリ･プライバシーポリシーが無いもの。
(2) アプリ･プライバシーポリシーの記述内容が曖昧／誤っている／長すぎるもの。
(3) 参照までの導線が解り難いもの。

■ 技術的な観点からの考察
◆ アプリ･プライバシーポリシーの作成･開示が必要なケースの整理
◆ 開示･承諾の手順の整理



（２）曖昧な説明

（２）長すぎる説明

背景2 アプリ・プライバシーポリシーに関する世界の動向

■ PRIVACY ON THE GO（2013年1月）

http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

■ 米国カルフォルニア州司法長官から、アプリマーケット運営者へ、プライバシー保護の要請

⇒ マーケットにおけるアプリ・プライバシーポリシーの掲示

■ FTC Staff Report（2013年2月）

http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

■ 米国連邦取引委員会から、アプリ事業者へ、透明性の確保による信頼の構築

⇒ アプリ・プライバシーポリシーの作成

■ OSベンダへ、実行時通知・追跡拒否の実現を要請

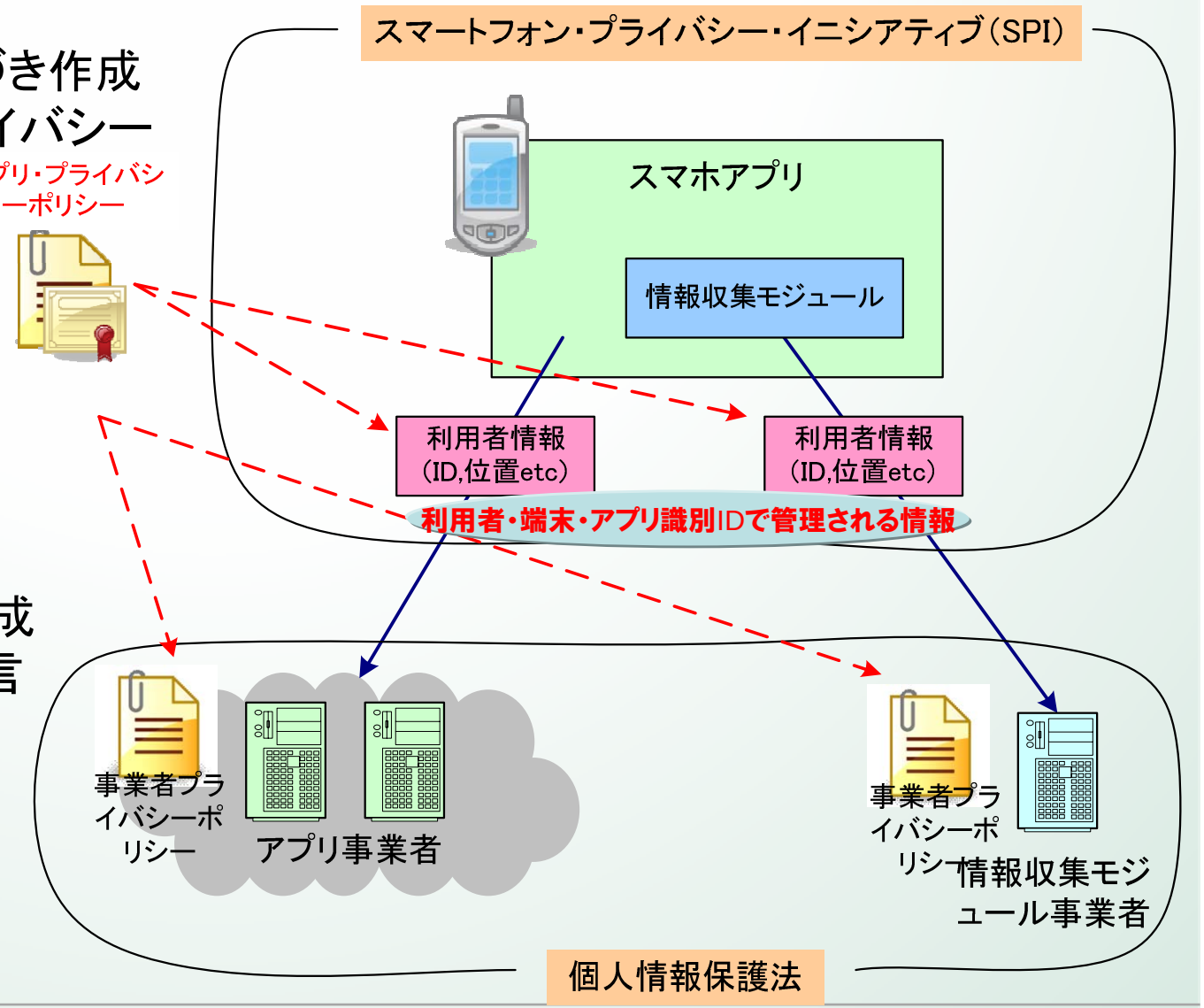
⇒ Just-in-Time Disclosures

⇒ Do Not Track（DNT）

アプリ・プライバシーポリシーと事業者プライバシーポリシーの関係性

■ アプリ・プライバシーポリシー
  ■ **総務省指針SPI/SPI IIに基づき作成**
    ⇒ アプリの透明性確保、プライバシーインパクトを説明
    ⇒ アプリ単位で作成

■ 事業者プライバシーポリシー
  ■ **個人情報保護法に基づき作成**
    ⇒ 取得情報の安全管理を宣言
    ⇒ 事業全体を網羅



総務省スマートフォンプライバシーイニシアティブ（SPI）

■ アプリ・プライバシーポリシーへの記載が望ましい8項目

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**	
	1) **送信停止の方法**	2) **送信された利用者情報の削除の方法**
⑥	**外部送信・第三者提供の有無、情報収集モジュールの有無**	
	1-1) **第三者提供先の事業者名**	1-2) **提供先事業者の事業者プライバシーポリシー**
	2-1) **情報収集モジュール名**	2-2) **モジュール提供者の事業者プライバシーポリシー**
⑦	**問い合わせ窓口**	
⑧	**プライバシーポリシーの変更を行う場合の手続**	

■ アプリ・プライバシーポリシーの作成と開示において留意すべき事項

- ◆ 概要版と詳細版を通じて、解りやすくかつ正確に、プライバシーインパクトを伝える。
- ◆ 送信される情報の重要度に応じて、ヘルプメニューからの参照、アプリ初回起動時の参照情報の送信直前の参照など、適切なタイミングで開示・承諾を経ること。

アプリ・プライバシーポリシーの作成・掲示手順の一例

アプリ実装	該当情報（例）	作成の要否	対応	アプリにおける対応	アプリマーケット掲載時の対応
1）利用者情報の送信を行わない場合。	---	不要	①	情報送信が無い旨、入力操作によって情報を送る旨などの説明を、アプリの説明書や利用規約に記載する。	情報送信が無い旨、入力操作によって情報を送る旨などの説明を、「アプリの説明」欄に掲載する。
2）利用者による明示的な操作によって利用者情報を送信する場合（ログイン時のID/PWDの入力やメール送信時の宛先入力等）。	---				
3）単体では利用者識別性を有さない利用者情報を送信する場合。 ※但し、サーバ側に、これら複数の情報からアクセス元を識別する処理が組み込まれている場合は、包括同意の取得（対応③）が必要。	ブラウザエージェント OS名 バージョン情報など				
利用者による取り換えが容易な利用者情報のみを送信する場合。	cookie UUIDなど ＋これらで管理される情報	必要	②	ヘルプメニューを入口とする、アプリ・プライバシーポリシーの参照機能を設ける。	アプリプライバシーポリシーへのリンクを、「アプリプライバシーポリシーURL」欄に掲載する。
利用者による取り換えが困難な利用者情報を送信する場合。	IMEI IMSI ICCID MACアドレス OSが生成するIDなど ＋これらで管理される情報		③	対応②に加え、初回起動時のアプリ・プライバシーポリシーの提示による包括同意の取得を行う。	
慎重な取扱いが求められる利用者情報を送信する場合。	位置情報 アドレス帳 電話番号 メールアドレスなど		④	対応②と③に加え、情報送信の直前や解りやすい説明による個別同意の取得を行う。	

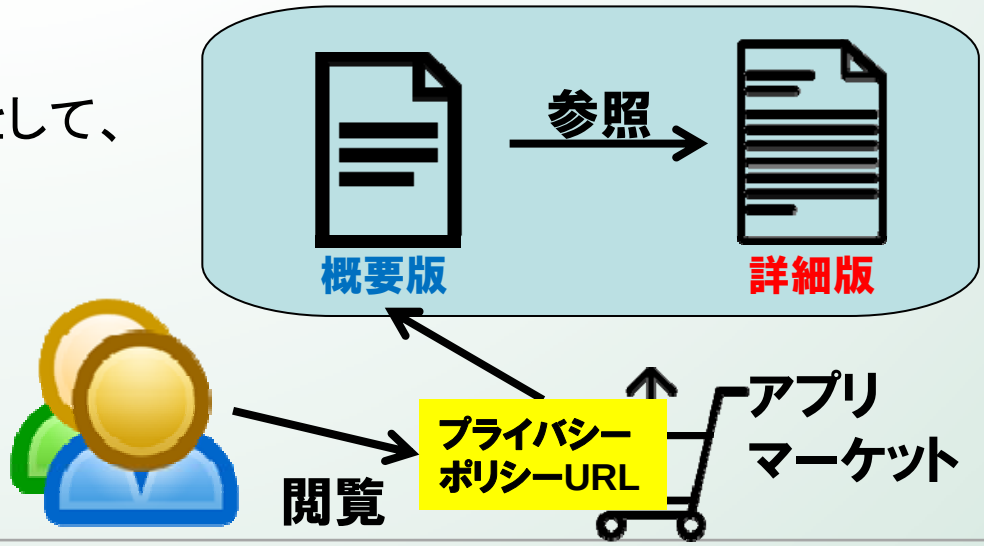
プライバシー不安は、行動・属性などの利用者情報の性質と、これを管理するIDの性質に依存する。
⇒ cookie、IMEI、電話番号などの識別子（ID）と、そのIDでどのような利用者情報が管理されるのか説明すること。

（付録）アプリ・プライバシーポリシーの概要版と詳細版の活用

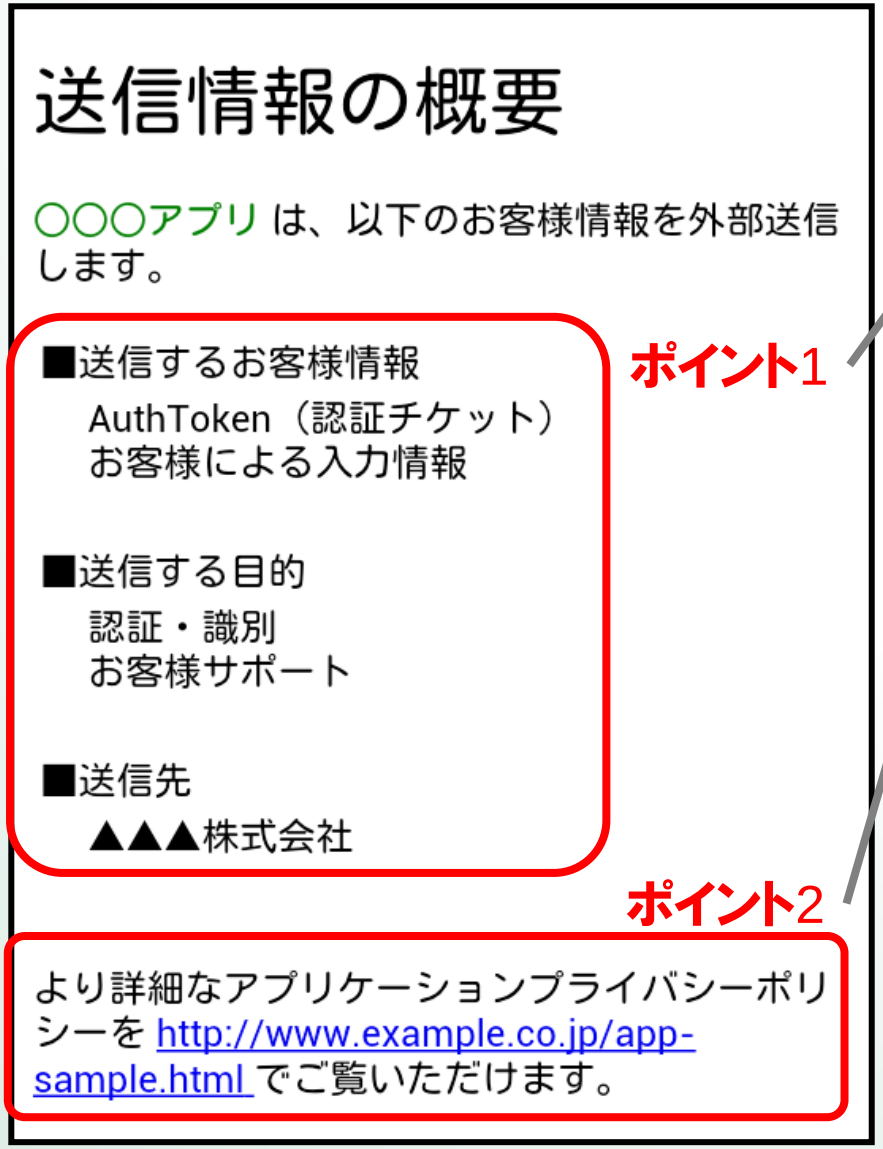
- アプリ・プライバシーポリシーは、「**概要版**」と「**詳細版**」の作成・活用が望ましい
  - **簡潔明瞭な実態の通知**と**正確な実態の通知**の両立をはかるため

- 推奨される記載内容と関係性
  - **概要版**
    - アプリが取得する利用者情報の項目、利用目的、第三者提供・情報収集モジュールの有無等を、スマホ端末の1画面で一覧できるよう記載する
  - **詳細版**
    - 総務省SPIの定める8項目に準拠した内容をすべて記載する

アプリマーケット等に掲載の**概要版**を導入として、
詳細版へのリンクを設けることが望ましい



（付録）概要版アプリ･プライバシーポリシーの記述例と特徴

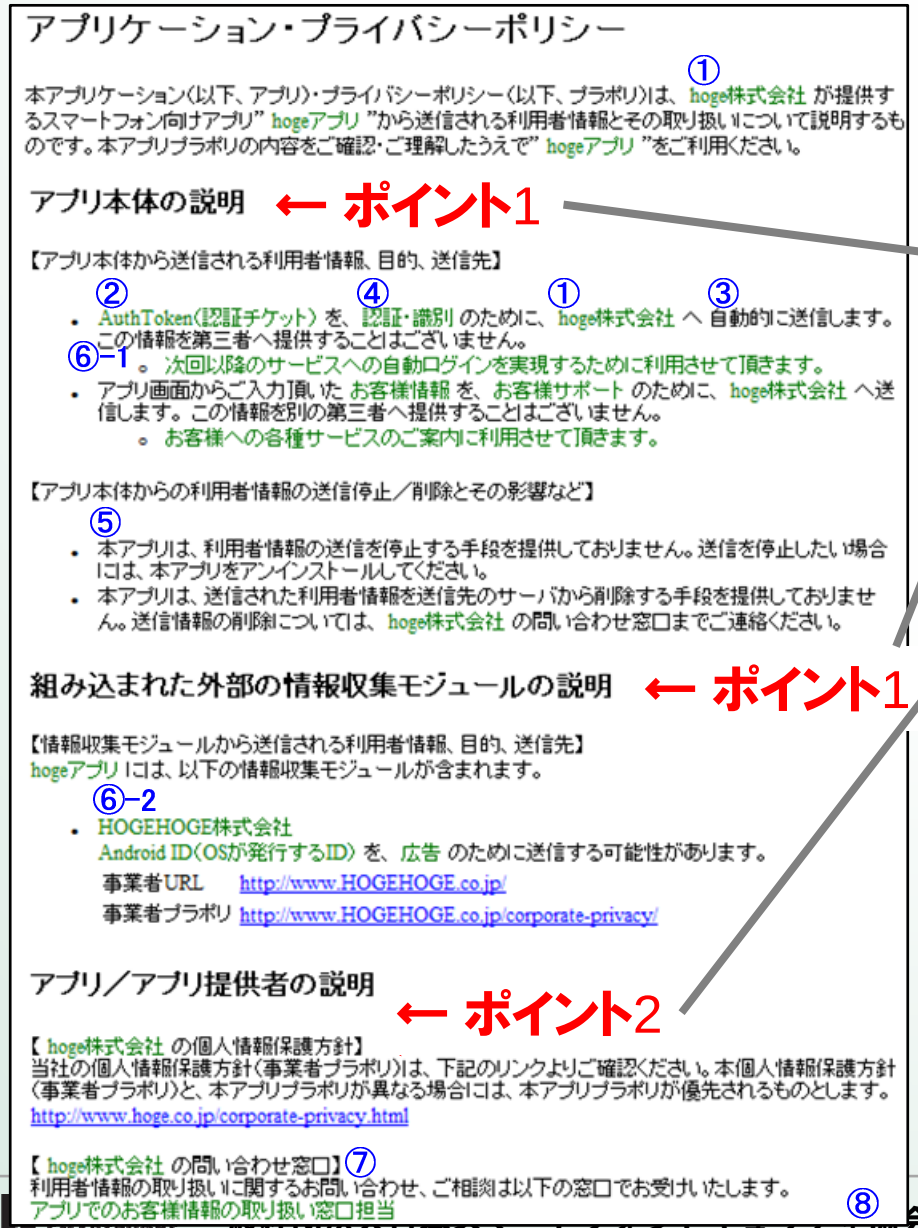


【特徴】

- ■ スマホ画面での一覧性を考慮した厳選された記載内容（ポイント1）
- ■ 詳細版アプリ･プライバシーポリシーを参照（ポイント2）

（参考）KDDI研究所、アプリ･プライバシーポリシー概要版雛形HTMLファイル、
http://www.kddilabs.jp/assets/files/pub-tech/app-sample-abst.html

（付録）詳細版アプリ･プライバシーポリシーの記述例と特徴



アプリケーション･プライバシーポリシー

本アプリケーション(以下、アプリ)･プライバシーポリシー(以下、プラポリ)は、①hoge株式会社 が提供するスマートフォン向けアプリ" hogeアプリ "から送信される利用者情報とその取り扱いについて説明するものです。本アプリプラポリの内容をご確認･ご理解したうえで" hogeアプリ "をご利用ください。

アプリ本体の説明 ← ポイント1

【アプリ本体から送信される利用者情報、目的、送信先】

②④①③
- AuthToken(認証チケット) を、認証･識別 のために、hoge株式会社 へ 自動的に送信します。この情報を第三者へ提供することはございません。

⑥−1
。次回以降のサービスへの自動ログインを実現するために利用させて頂きます。
- アプリ画面からご入力頂いた お客様情報 を、お客様サポート のために、hoge株式会社 へ送信します。この情報を別の第三者へ提供することはございません。
  - お客様への各種サービスのご案内に利用させて頂きます。

【アプリ本体からの利用者情報の送信停止／削除とその影響など】

⑤
- 本アプリは、利用者情報の送信を停止する手段を提供しておりません。送信を停止したい場合には、本アプリをアンインストールしてください。
- 本アプリは、送信された利用者情報を送信先のサーバから削除する手段を提供しておりません。送信情報の削除については、hoge株式会社 の問い合わせ窓口までご連絡ください。

組み込まれた外部の情報収集モジュールの説明 ← ポイント1

【情報収集モジュールから送信される利用者情報、目的、送信先】
hogeアプリ には、以下の情報収集モジュールが含まれます。

⑥−2
- HOGEHOGE株式会社
  Android ID(OSが発行するID) を、広告 のために送信する可能性があります。
  事業者URL http://www.HOGEHOGE.co.jp/
  事業者プラポリ http://www.HOGEHOGE.co.jp/corporate-privacy/

アプリ／アプリ提供者の説明 ← ポイント2

【 hoge株式会社 の個人情報保護方針】
当社の個人情報保護方針(事業者プラポリ)は、下記のリンクよりご確認ください。本個人情報保護方針(事業者プラポリ)と、本アプリプラポリが異なる場合には、本アプリプラポリが優先されるものとします。
http://www.hoge.co.jp/corporate-privacy.html

【 hoge株式会社 の問い合わせ窓口】⑦
利用者情報の取り扱いに関するお問い合わせ、ご相談は以下の窓口でお受けいたします。
アプリでのお客様情報の取り扱い窓口担当 ⑧

【特徴】

- SPI8項目に沿った説明（図中①～⑧）
- アプリ本体／情報収集モジュールを分けて説明（ポイント1）
- 事業者プライバシーポリシーを参照（ポイント2）

アプリからの「情報送信」について承諾
「取得情報の管理」について承諾

（参考）KDDI研究所、アプリプライバシーポリシー詳細版雛形HTMLファイル、
http://www.kddilabs.jp/assets/files/pub-tech/app-sample.html

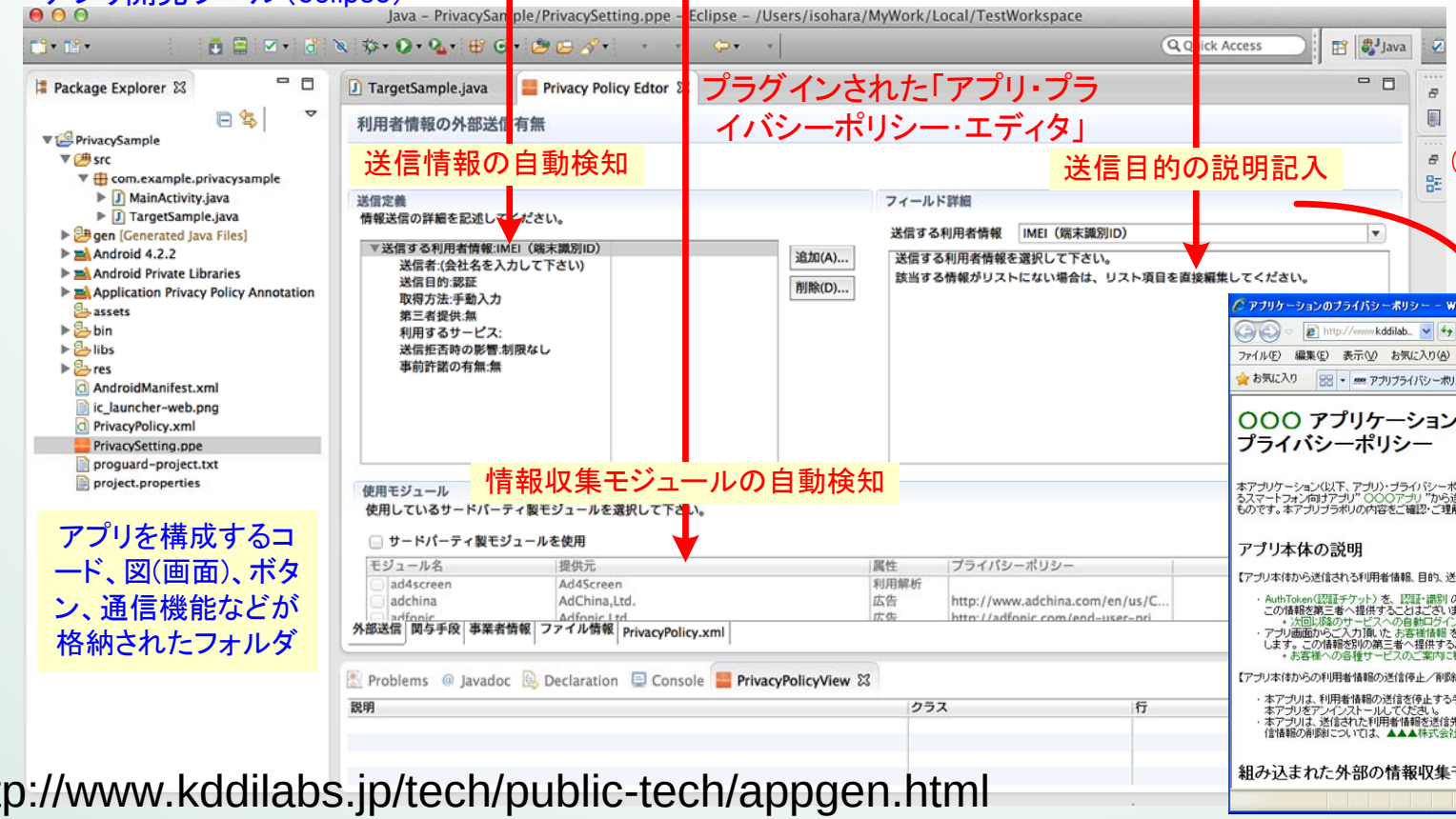
（付録）アプリ・プライバシーポリシー作成支援ツールの利用例

① アプリを開発
（数週間～数ヶ月）

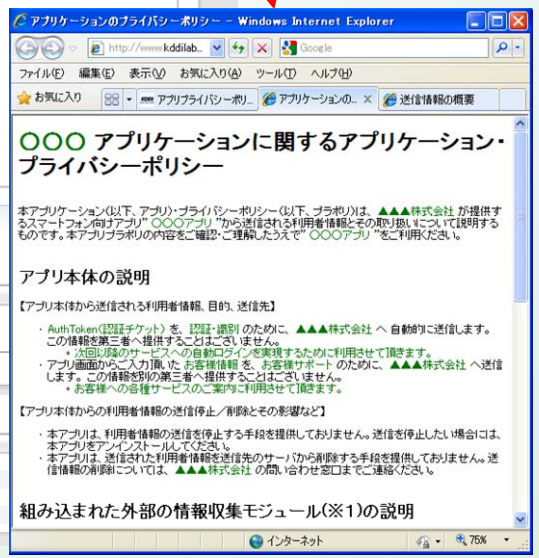
② 送信情報をスキャンしてアプリ・プライバシーポリシーの一部を自動生成
（数秒）

③必要箇所を補足、追記
（数十分）

アプリ開発ツール（eclipse）



④ アプリ・プライバシーポリシーの生成（数秒）



アプリを構成するコード、図(画面)、ボタン、通信機能などが格納されたフォルダ

http://www.kddilabs.jp/tech/public-tech/appgen.html

（付録）用語解説

用語	解説
事業者プライバシーポリシー	事業者における個人情報保護方針を記したプライバシーポリシー。個人情報保護法に基づき作成。
アプリ・プライバシーポリシー	アプリケーション向けプライバシーポリシー。総務省SPIの指針に基づき作成。概要版と詳細版での解りやすい説明が望まれる。
概要版アプリ・プライバシーポリシー	アプリが取得する利用者情報、取得目的、第三者提供の有無などを簡潔に記述した文書。
詳細版アプリ・プライバシーポリシー	総務省SPIの定める8項目に準拠した詳細な内容を記述した文書。
利用者による取り換えが容易な利用者情報	cookie、UUIDなど
利用者による取り換えが困難な利用者情報	IMEI、IMSI、ICCID、MACアドレス、OSが生成するIDなど
慎重な取り扱いが求められる利用者情報	位置情報、アドレス帳、電話番号、メールアドレスなど

参考文献

- 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/main_content/000236366.pdf
- 総務省、スマートフォン プライバシー イニシアティブ II、
  http://www.soumu.go.jp/main_content/000247654.pdf
- モバイルコンテンツフォーラム（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
- JIPDEC プライバシーマーク推進センター “（スマートフォン等のアプリケーション配信事業者対象）利用者情報の取扱い、アプリケーション・プライバシーポリシーについて”、
  http://privacymark.jp/news/2014/0114/
- Tao software, ″アンドロイドスマートフォンプライバシーガイドライン by タオ″
  http://www.taosoftware.co.jp/android/android_privacy_policy/
- KDDI研究所、アプリプライバシーポリシーリ雛形HTML（詳細版・概要版）、
  http://www.kddilabs.jp/assets/files/pub-tech/app-sample-abst.html （概要版）
  http://www.kddilabs.jp/assets/files/pub-tech/app-sample.html （詳細版）
- KDDI研究所、 Androidアプリ向けプライバシーポリシー作成支援ツール、
  http://www.kddilabs.jp/tech/public-tech/appgen.html
- 日本スマートフォンセキュリティ協会、JSSECセキュアコーディングガイド、
  http://www.jssec.org/dl/android_securecoding.pdf