

SIP: スマートフォン・プライバシー・イニシアティブ
アプリプラポリ: アプリケーション向けプライバシーポリシー
事業者プラポリ: 事業者における個人情報保護方針

総務省SPI準拠 auスマパスにおけるアプリ第三者検証 アプリプラポリ作成支援ツール

KDDI 竹森敬祐



スマホアプリからの情報送信を正しく、
サービスを網羅的に説明する、プライバ
シーポリシー(アプリプラポリ)を作成する。

1章 はじめに

2章 auスマートパスにおけるアプリの第三者検証

3章 アプリプラポリ作成支援ツール

スマホアプリからの情報送信の実態調査 (KDDI研調べ)

■ 2011年～2013年の人気上位アプリ調査

◆ 動的解析による送信情報の検査。プラポリの読み解き。

調査時期		2011年8月	2012年4月	2013年2月
対象:人気上位の無料アプリ		400アプリ	100アプリ	100アプリ
利用者情報を送信するアプリ		45%(181/400)	81%(81/100)	63%(63/100)
	何らかのプラポリを開示	13%(24/181)	19%(15/81)	57%(36/63)
	アプリプラポリを開示	—	—	25%(16/63)
	送信情報を正しく説明	9%(17/181)	3%(2/81)	11%(7/63)
	説明が正しく、SPI準拠	—	—	0%(0/63)

“—” SPI公表前につき未調査



基本課題) 第三者による審査
課題1) アプリプラポリの普及
課題2) 正確な記載の促進

アプリプラポリと事業者プラポリ

■ アプリプラポリ

◆ 総務省指針SPIに基づき作成

- ⇒ アプリの透明性確保
- ⇒ アプリからの送信情報
- ⇒ 開発者が作成

au Market,
KDDI研(雛形)の
アプリプラポリ



スマートフォン・プライバシー・イニシアティブ (SPI)



スマホアプリ

情報収集モジュール

利用者情報
(ID,位置etc)

利用者情報
(ID,位置etc)

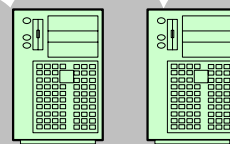
■ 事業者プラポリ

◆ 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
- ⇒ 法務／総務部が作成



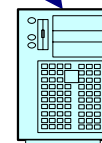
事業者
プラポリ



アプリ事業者



事業者
プラポリ



情報収集モジュール事業者

個人情報保護法

KDDI主催セミナー ～アプリ事業者の啓発～

■ auスマートパスアプリ事業者の集い

◆ KDDI主催の、アプリ開発セミナーを開催。

⇒ アプリ投稿時の送信情報に関する新申請制度(2章)

⇒ アプリプラポリ作成支援ツールの活用(3章)



■ 意見交換会の所感

◆ SPIと個人情報保護法のご理解頂けた。

⇒ アプリプラポリの重要性を認知。

⇒ **アプリプラポリを書く意識は高い。**

◆ アプリ開発の注意点についてのセミナーをもっと開催して欲しい。

◆ au Marketは、アプリプラポリを自動生成してくれるので助かる。

◆ アプリプラポリ作成支援ツールを活用してauスマートパス非対象アプリにつても作成したい。本セミナーで作成方法が解った！

総務省SPI準拠 auスマパスにおけるアプリ第三者検証 アプリプラポリ作成支援ツール

KDDI研究所 竹森敬祐／磯原隆将



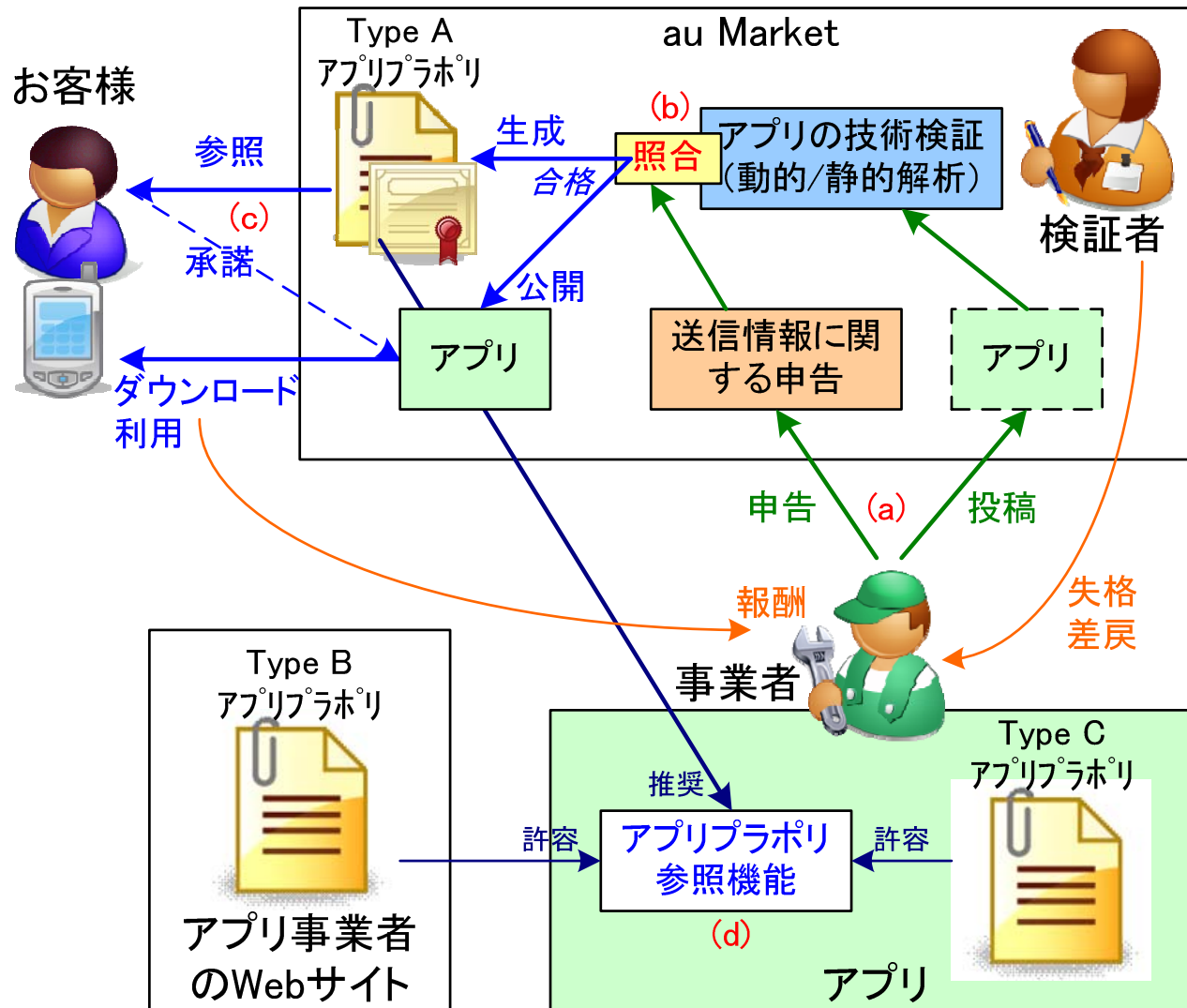
スマホアプリからの情報送信を正しく、
サービスを網羅的に説明する、プライバ
シーポリシー(アプリプラポリ)を作成する。

1章 はじめに

2章 auスマートパスにおけるアプリの第三者検証

3章 アプリプラポリ作成支援ツール

auスマートパス(KDDI研)における第三者検証



- ★ 第三者検証者のサーバに**プラホリをホスティング!**
- ★ 他Market上の同アプリから**プラホリへリンクを可能に!**
- ★ DL前と**任意のタイミング**で**プラホリを参照可能に!**

周知: 2013/7/9
実施: 2013年10月

a) プラポリ事項の申請～SPI準拠へ～

お客様情報の外部送信有無		☒ あり ☐ なし
送信するお客様情報	メールアドレス ▼	
送信元	☒ アプリ提供者 ☐ 情報収集モジュール	
事業者名	mediba ▼	
送信する目的	目的 ▼	
送信先種別	☒ アプリ提供者 ☐ 第三者提供	
送信先		
取得方法	☒ 自動 ☐ 手動	
URL		
追加		
お客様情報の送信や利用の停止		
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		

SPI 8項目への準拠

- ② 取得される情報の項目
- ① 情報を取得するアプリ提供者等の氏名又は名称
- ⑥-2 情報収集モジュールの有無
- ⑦ 問い合わせ窓口の情報
- ④ 利用目的の特定・明示
- ⑥-1 外部送信・第三者提供の有無
- ③ 取得方法の記載
- ⑤ 利用者関与の方法

⑧ プラポリ変更の手続き
⇒アプリ更新で再度プラポリ申請

注) 開発段階のため変更の可能性あり。

b) 送信情報の解析

- ◆ カーネル内部の処理ログから、サンドボックス上で動くアプリの挙動を抽出する。
(straceを実行して、断片的なログを組み上げる。)

[illegible]

b) 通信先解析 ～情報収集モジュール起動判定～

◆ 通信のあて先から、広告・情報収集サーバを検知する。

悪性アプリ認定 良性アプリ認定

	Ver.	公開鍵	端末	ファーム	カーネル	評価日時	解析日時	収集ログ	評価情報
	2.1	L8253wRs...	IS06	2.2.1	2.6.32.9...	2011/08/25 15:16	2012/08/09 20:31:06	ダウンロード	削除
	2.1		IS01	1.6	2.6.29-p...	2011/04/05 09:39	2012/08/10 14:33:36	ダウンロード	削除
→	2.1		Htc & Lfd	2.2	2.6.34.1...	2011/01/06 17:30	2012/08/10 14:00:52	ダウンロード	削除

判定結果 パーミッション マニフェスト パッケージ情報 アプリログ カーネルログ dexファイル dexパス バケット 付随情報 アソシエーション

・バケット情報

バケット量 89 KB

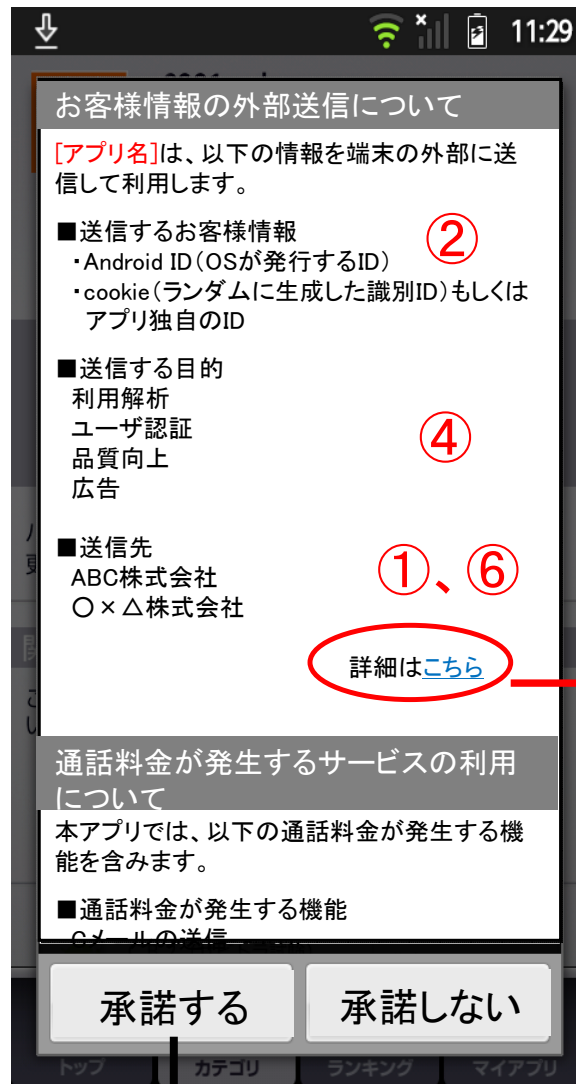
平均通信速度 723 bps

IPスキャン数 0 個

[mm.admob.com] が脅威(FQDN)に該当	外部モジュール	1	AdMob: MD5 (AndroidID)
[mm1.vip.sc1.admob.com] が脅威(FQDN)に該当	外部モジュール	1	AdMob: MD5 (AndroidID)
[r.admob.com] が脅威(FQDN)に該当	外部モジュール	1	AdMob: MD5 (AndroidID)
[www.widifu.com] が脅威(FQDN)に該当	踏み台	4	端末を攻撃の踏み台として悪用するアプリです。
[www.udaore.com] が脅威(FQDN)に該当	踏み台	4	端末を攻撃の踏み台として悪用するアプリです。
[www.frijd.com] が脅威(FQDN)に該当	踏み台	4	端末を攻撃の踏み台として悪用するアプリです。
[googleads.g.doubleclick.net] が脅威(FQDN)に該当	外部モジュール	1	AdMob: MD5 (AndroidID)

DNS	送信先IPアドレス	送信先FQDN	送信先ポート	バケット数
Q	220.159.212.200	api.admob.com	53	
	220.159.212.200		53	9
Q	220.159.212.200	supl.google.com	53	
	165.193.245.41	api1.vip.sc9.admob.com	80	6
Q	220.159.212.200	mm.admob.com	53	
	70.32.132.54	mm1.vip.sc1.admob.com	80	28
Q	220.159.212.200	r.admob.com	53	
	202.239.172.82	a445.w7.akamai.net	80	144
Q	220.159.212.200	www.widifu.com	53	
Q	220.159.212.200	www.udaore.com	53	
Q	220.159.212.200	www.frijd.com	53	
Q	220.159.212.200	www.dseffects.com	53	
Q	220.159.212.200	googleads.g.doubleclick.net	53	

c) ダウンロード前の概要版プラポリ



■ 目的: 利用者に判断を仰ぐこと

◆ ダウンロード前に、承諾画面をポップアップ*

注) 情報送信しないアプリの場合、表示されません。

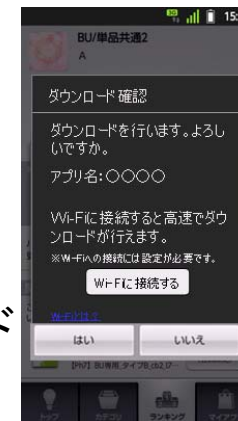
⇒ 狼少年化を避け、注目して頂きたいアプリに絞って、実際に送信される情報をご確認頂くという考え方。

⇒ アプリ審査員は目的の妥当性の判断をし難く、これをお客様の視点でご判断頂くのが良いと考えた。

◆ 読んで頂くための簡潔化を目指し、我々がSPIで重要と考えた「送信情報」、「目的」、「宛先(第三者提供)」の概要版を提示。

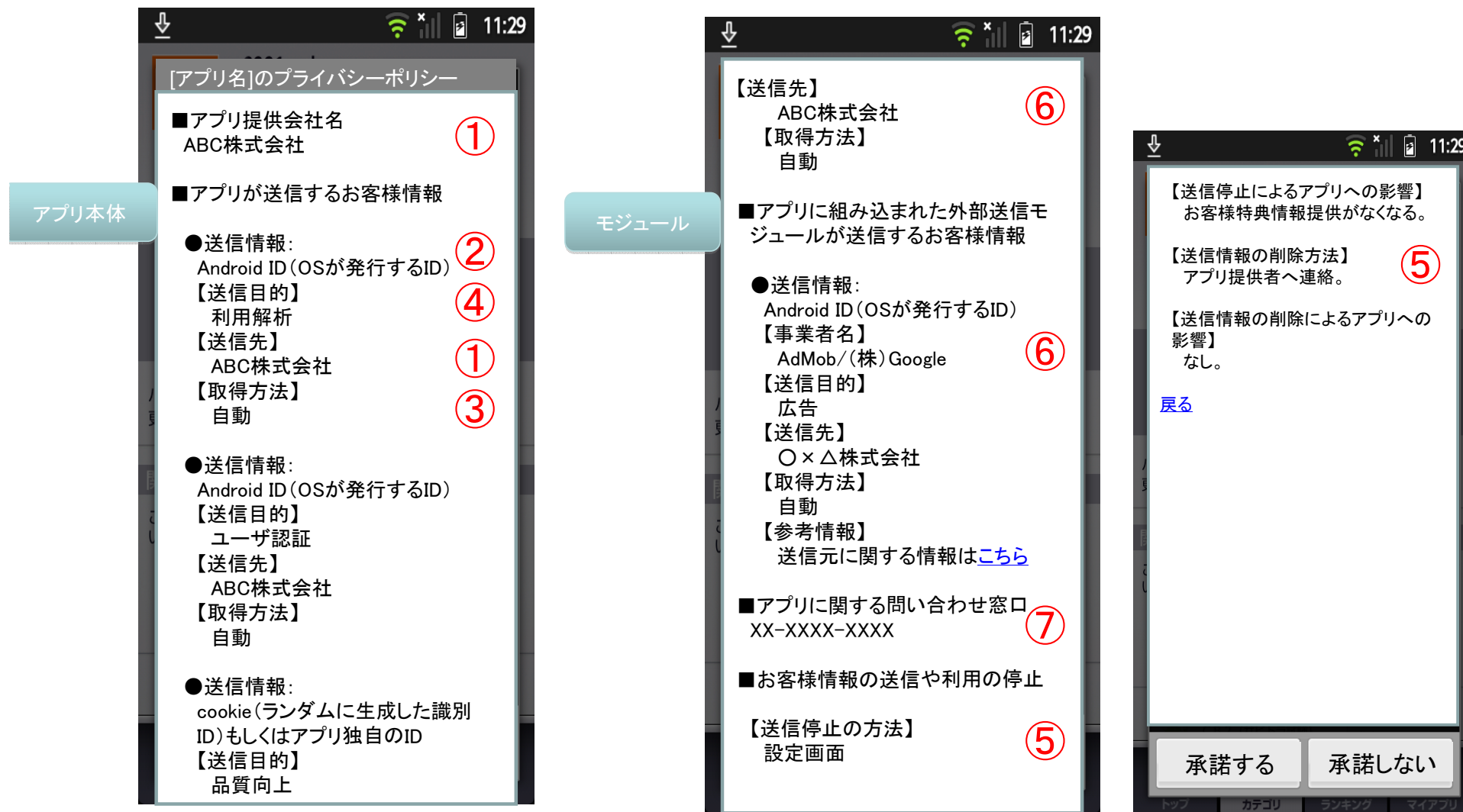
次ページへ

ダウンロード
確認画面



*auスマートパスはポップアップ
個別提供アプリは参照リンク

c) ダウンロード前の詳細版プラポリ(新規)



注) 開発段階のため変更の可能性あり。

総務省SPI準拠 auスマパスにおけるアプリ第三者検証 アプリプラポリ作成支援ツール

KDDI研究所 竹森敬祐／磯原隆将



スマホアプリからの情報送信を正しく、
サービスを網羅的に説明する、プライバ
シーポリシー(アプリプラポリ)を作成する。

- 1章 はじめに
- 2章 auスマートパスにおけるアプリの第三者検証
- 3章 アプリプラポリ作成支援ツール

d) アプリプラポリ作成支援ツールの公開 ~KDDI研から~

① アプリを開発
(数週間~数ヶ月)



アプリ開発ツール(eclipse)

② 送信情報をスキャンしてアプリ
プラポリの一部を自動生成
(数秒)



電話番号: GetLine1Number()
端末ID: GetDeviceId()

③ 必要箇所を補足、追記
(数十分)



プラグインされた「アプリ
プラポリ・エディタ」

送信情報の自動検知

送信目的の説明記入

Step 4) アプリ
プラポリ生成
(数秒)

アプリケーションのプライバシーポリシー

第1条(定義)

このアプリケーション・プライバシーポリシー(以下、本プライバ
シーポリシーといいます)は、KDDI株式会社 が提供するスマート
フォン用アプリケーション PrivacySample (以下、本アプリケーシ
ョンといいます)および本アプリケーションに関するサービス(以下、
本サービスといいます)における利用者情報の取扱いを定めたもの
です。なお、KDDI株式会社の連絡先は、第 10 条をご覧ください。

第2-1条(取得される情報の項目、利用目的、取得方法)

- 利用者識別のため(※1)、Android ID (OSが発行するID) (※2)
の情報を取得します。
なお、以下の情報については、個別の情報の取得について同
意をされた場合に限り、取得いたします。同意をいただけない
場合には、情報は提供されない代わりに、(自動的に)「機
能名を指定して下さい」の機能はご利用いただけません。
- 利用解析のため(※1)【自動送信データが有りません】(※2)の
情報を取得します。
なお、以下の情報については、個別の情報の取得について同
意をされた場合に限り、取得いたします。同意をいただけない
場合には、情報は提供されない代わりに、(自動的に)「機
能名を指定して下さい」の機能はご利用いただけません。

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

情報収集モジュールの自動検知

モジュール名	提供元	属性	プライバシーポリシー
ad4screen	Ad4Screen	利用解析	http://www.adchina.com/en/us/C...
adchina	AdChina, Ltd.	広告	http://adfonic.com/lead-user-ori
adfonic	Adfonic Ltd.	広告	

外部送信 関与手段 事業者情報 ファイル情報 PrivacyPolicy.xml

説明 クラス 行

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

d) アプリプラポリ雛形.htmlの公開 ~KDDI研から~

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、^① hoge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】

- ^② AuthToken(認証チケット) を、^④ 認証・識別 のために、^① 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ありません。
- ^{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いただきます。
- 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、^③ 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ありません。
 - お客様への各種サービスのご案内にご利用させていただきます。

【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} HOGEHOG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.HOGEHOG.co.jp/>
事業者プラポリ <http://www.HOGEHOG.co.jp/corporate-privacy/>

アプリ/アプリ提供者の説明

【hoge株式会社 の個人情報保護方針】 ← ポイント2

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

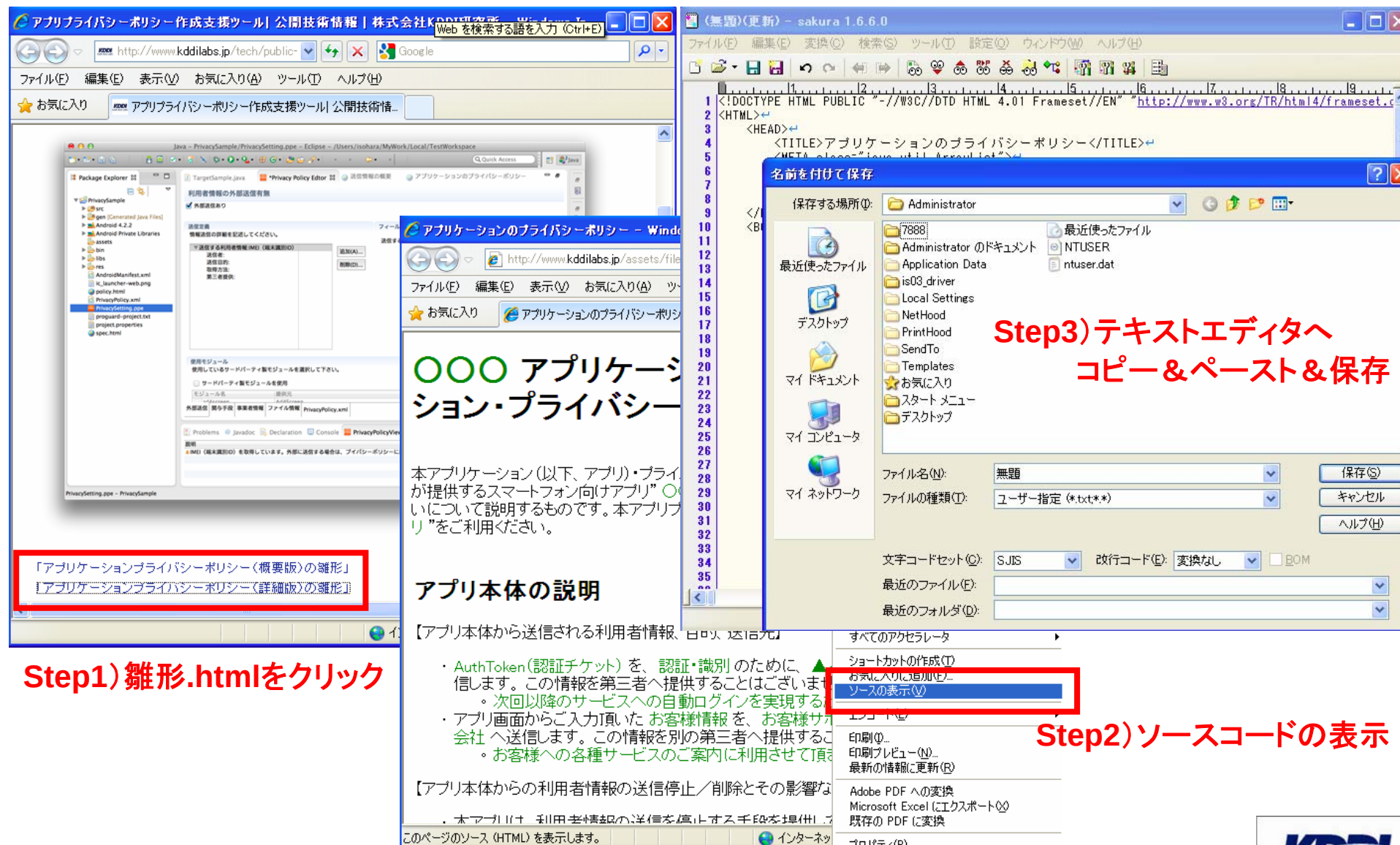
■ 特徴

- ◆ SPI8項目に沿った説明。
- ◆ アプリ本体／情報収集モジュールを分けて説明。
- ◆ 事業者プラポリを参照

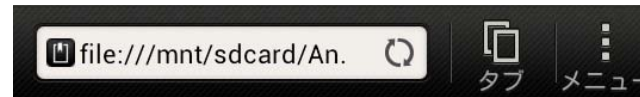


アプリからの「情報送信」について承諾
「取得情報の管理」について承諾

d) プラポリ雛形.htmlの取得



スマホ画面から見たアプリプラポリ(概要版)



送信情報の概要

〇〇〇アプリは、以下のお客様情報を外部送信します。

■送信するお客様情報

AuthToken (認証チケット)
お客様による入力情報

■送信する目的

認証・識別
お客様サポート

■送信先

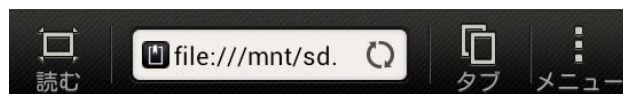
▲▲▲株式会社

より詳細なアプリケーションプライバシーポリシーを <http://www.example.co.jp/app-sample.html> でご覧いただけます。

次項の詳細版へのリンク

アプリプラポリ作成支援ツールでは、概要版＋詳細版のアプリプラポリが生成される。

スマホ画面から見たアプリプラポリ(詳細版)



〇〇〇 アプリケーションに関するアプリケーション・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、**▲▲▲株式会社**が提供するスマートフォン向けアプリ"〇〇〇アプリ"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"〇〇〇アプリ"をご利用ください。

アプリ本体の説明

【アプリ本体から送信される利用者情報、目的、送信先】

- **AuthToken（認証チケット）** を、**認証・識別**のために、**▲▲▲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ありません。
 - **次回以降のサービスへの自動ログイン**

組み込まれた外部の情報収集モジュール(※1)の説明

【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。

- **▲▲▲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.example.co.jp/>
事業者プラポリ <http://www.example.co.jp/corporate-privacy/>

※1:情報収集モジュールとは、広告表示やアプリの利用頻度を解析する、アプリ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です。

アプリ／アプリ提供者の説明

【**▲▲▲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.example.co.jp/corporate-privacy.html>

アプリ／アプリ提供者の説明

【**▲▲▲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.example.co.jp/corporate-privacy.html>

【**▲▲▲株式会社**の問い合わせ窓口】
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
<mailto:contact@example.co.jp>
tel:03-xxxx-xxxx

【本アプリプラポリの変更について】
本アプリのバージョンアップに伴って、送信される利用者情報、目的、送信先が変更される場合があります。変更内容などは、新バージョンのアプリに付随するアプリプラポリをご参照ください。

以上

アプリプラポリ作成・公開の世界的な流れ



■ PRIVACY ON THE GO(2013年1月)

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

- ◆ 米国カリフォルニア州司法長官から、アプリMarket運営者へ、プライバシー保護の要請。
- ⇒ Market上でのアプリプラポリの明示

■ FTCスタッフレポート(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。
- ⇒ アプリプラポリの作成
- ◆ 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)

<http://japanese.engadget.com/2012/02/22/google-ms-6/>

Google Play／AppStoreでのアプリプラポリ欄



Google Play「プラポリURL」欄



AppStore「プラポリURL」欄

Marketでのアプリプラポリの掲載方針の案

アプリからの 情報送信	説明文の作成	説明文の提示方法
無し	利用者情報を外部送信しない旨を説明する文書を作成	「アプリの説明」欄に説明文を記載
操作を伴う自 明な送信のみ (ログイン、SNS)	利用者情報が送信されうる ログインやSNSについての 機能説明を作成	「アプリの説明」欄に説明文を記載
有り (特に自動送信)	総務省SPI準拠のアプリプラ ポリを作成	「アプリプラポリURL」欄に、 アプリプラポリ参照用のリン クを記載