スマホアプリの第三者検証フレームワーク
～au Marketにおけるプライバシー保護の取り組み～

KDDI／KDDI研究所
竹森、磯原、高野

au Marketがアプリの第三者検証役として、アプリ事業者から送信情報に関する申告を頂き、技術検証を行う。概要版／詳細版アプリプラポリを自動生成し、お客様判断を仰ぐことで、アプリの安心・安全化を目指す。

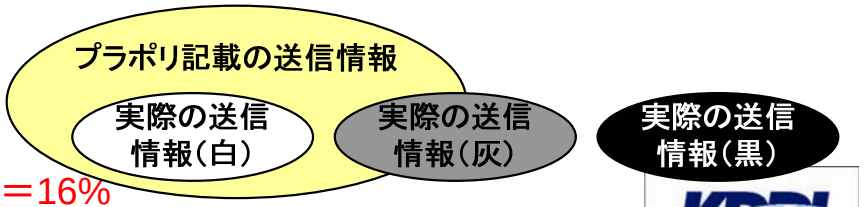
1章 スマホアプリの現状
2章 アプリとプラポリの第三者検証フレームワーク

©2013 KDDI R&D Laboratories Inc.
KDDI R&D LABS

2011/8, 2012/4, 2013/2 スマホアプリ調査（KDDI研調べ）

	2011.8–2012.1 調査(400件)	2012.4–2012.5 調査(100件)	2013.2–2013.3 調査(100件)
情報収集ﾓｼﾞｭｰﾙを組み込んだｱﾌﾟﾘ	56.9%*1 (558件)	82% (82件)	63% (63件)
利用者情報を送信するｱﾌﾟﾘ	45.3%*2 (181件)	81% (81件)	63% (63件)
ﾌﾟﾗﾎﾟﾘに送信情報が正しく記載のｱﾌﾟﾘ(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%
ﾌﾟﾗﾎﾟﾘに送信情報が誤って記載のｱﾌﾟﾘ(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%
ﾌﾟﾗﾎﾟﾘが無く利用者情報を送信するｱﾌﾟﾘ(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件のｱﾌﾟ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。



■ 2013年5月：直近100件のauスマートパス向け投稿アプリを調査
◆ アプリ本体を含め、利用者情報を送信するアプリ数　16/100件＝16%

©2013 KDDI R&D Laboratories Inc.
KDDI R&D LABS

プラポリSPI 8項目とアプリの記載状況（KDDI研調べ）

■ 2013年2月の100アプリ調査

◆ アプリプラポリ（24件）＋事業者プラポリ（29件）＝53件のSPI*対応状況

* SPI: スマートフォン プライバシー イニシアティブ by 総務省

①	情報を取得するアプリ提供者等の氏名又は名称	53/53件=100%
②	取得される情報の項目	49/53件=92%
③	取得方法の記載の有無（自動送信、手入力、Web側での閲覧履歴）	39/53件=74%
④	利用目的の特定・明示	52/52件=98%
⑤	通知・公表又は同意取得の方法、利用者関与の方法（送信の停止、情報削除）	32/53件=60%
⑥	1)外部送信・第三者提供の有無 2)情報収集モジュールの有無	47/53件=89% 12/53件=23%
⑦	問い合わせ窓口の情報	36/53件=68%
⑧	プライバシーポリシー変更の手続きの説明	32/53件=60%

間違いだらけ

■ 総務省SPI 8項目

◆ SPI 8項目の全を記載しているアプリ 4/100件、うち送信情報が正しく書けている 0/4件。

©2013 KDDI R&D Laboratories Inc.

KDDI R&D LABS

プラポリの読み解き調査 日本総研（40アプリ）,KDDI研（100アプリ）

◆ 17/33件（52%）アプリで、SPI 8ヶ条の判断が分かれた（下図黄色）。
⇒ 現時点で、アプリプラポリと技術検証の整合性確認（第三者検証）は不可能。

	SPI 8項目の記載の有無（KDDI研-日本総研の比較）										プラポリに記載のあった利用者情報														
アプリ名	① 情報を取得するアプリケーション提供者等の氏名又は名称	② 取得される情報の項目	③ 取得方法の記載の有無（自動送信、利用者入力、Web閲覧履歴）	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（情報送信の停止や削除）	⑥-1 外部送信・第三者提供の有無	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	⑧プライバシーポリシー変更の手続きの説明	プラポリと送信情報との整合性	OS生成ID	IMEI	IMSI	MAC	TEL	緯度経度	電話帳	端末・アプリ利用ログ（Logcat）	インストールアプリ一覧	通信履歴	Cookie	メールアドレス	利用者入力情報	その他
	有	有	有	有	無	有	有	有	有	-	1	1		1	1	1	1	1			1	1	1	1
	有	有	有	有	有	有	有	有	無	黒		1		1					1		1	1		1
	有	有	有	有	有	有	無	有	有	-		1			1	1		1			1	1	1	1
	-	-	-	-	-	-	-	-	-	黒														
	有	有	有	有	有	有	無	無	有	白					1	1	1			1	1	1	1	
	有	有	有	有	有	有	無	有	有	-					1							1	1	
	-	-	-	-	-	-	-	-	-	-														
	有	有	有	有	有	有	無	有	有	白					1	1	1			1	1	1	1	
	有	有	有	有	無	有	無	有	有	-		1						1			1	1	1	1
	有	有	有	有	有	有	無	有	有	白		1			1		1					1	1	
	有	有	有	有	有	有	無	有	有	-											1			
	-	-	-	-	-	-	-	-	-	黒														
	有	有	有	有	有	有	有	有	無	-											1			1
	有	有	無	有	有	有	無	有	無	-					1							1		1
	有	有	有	有	有	有	無	有	有	灰		1			1	1								1
	有	有	有	有	無	有	有	有	有	-	1	1		1	1	1	1	1			1	1	1	1
	有	無	無	無	無	有	無	有	無	黒														
	有	有	無	有	有	有	無	有	無	灰					1							1		1
	有	有	有	有	無	有	有	有	有	-	1	1		1	1	1	1	1			1	1	1	1
	有	無	無	無	有	有	無	無	有	黒														
	-	-	-	-	-	-	-	-	-	黒														
	有	有	有	有	有	有	有	有	有	灰		1			1	1	1				1	1	1	1
	有	有	有	有	有	有	有	有	有	灰					1						1	1	1	1

KDDI R&D LABS

2013/2 情報送信63/100アプリの詳細(KDDI研調べ)

	全ｱﾌﾟﾘ(100件)	利用者情報を送信するｱﾌﾟﾘ(63件)
アプリプラポリを持つアプリ	24/100件=24%	16/63件=25% (正確5/16件=31%)
事業者プラポリを持つアプリ	29/100件=29%	20/63件=32% (正確2/20件=10%)
プラポリを持たないアプリ	47/100件=47%	27/63件=43%

重要

- アプリプラポリの普及
- アプリプラポリを正確に書く

©2013 KDDI R&D Laboratories Inc.

情報収集モジュールの送信情報の一例 ～動的解析～

©2013 KDDI R&D Laboratories Inc.

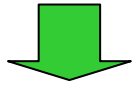
参考）ある情報収集モジュールの組込説明書の例

情報収集モジュールの
アプリ組み込みマニュアル

..... 3
..... 3
..... 3
..... 4
..... 4
..... 4
..... 5
..... 6
..... 6
..... 6
..... 6
..... 6
..... 7
..... 7
..... 7
..... 9
..... 10
..... 10
..... 10
..... 13
..... 14
..... 16
..... 16
..... 17

- Fact：IMEI,IMSI,Android IDを送信

- 説明：Manifestに追加する項目
  - android.permission.INTERNET
  - android.permission.READ_PHONE_SATATE
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.ACCESS_WIFI_STATE
- 送信情報に関する説明無し
- アプリプラポリ無し



- アプリ事業者は送信情報について理解できない。

©2013 KDDI R&D Laboratories Inc.

KDDI R&D LABS

スマホアプリの第三者検証フレームワーク
～au Marketにおけるプライバシー保護の取り組み～

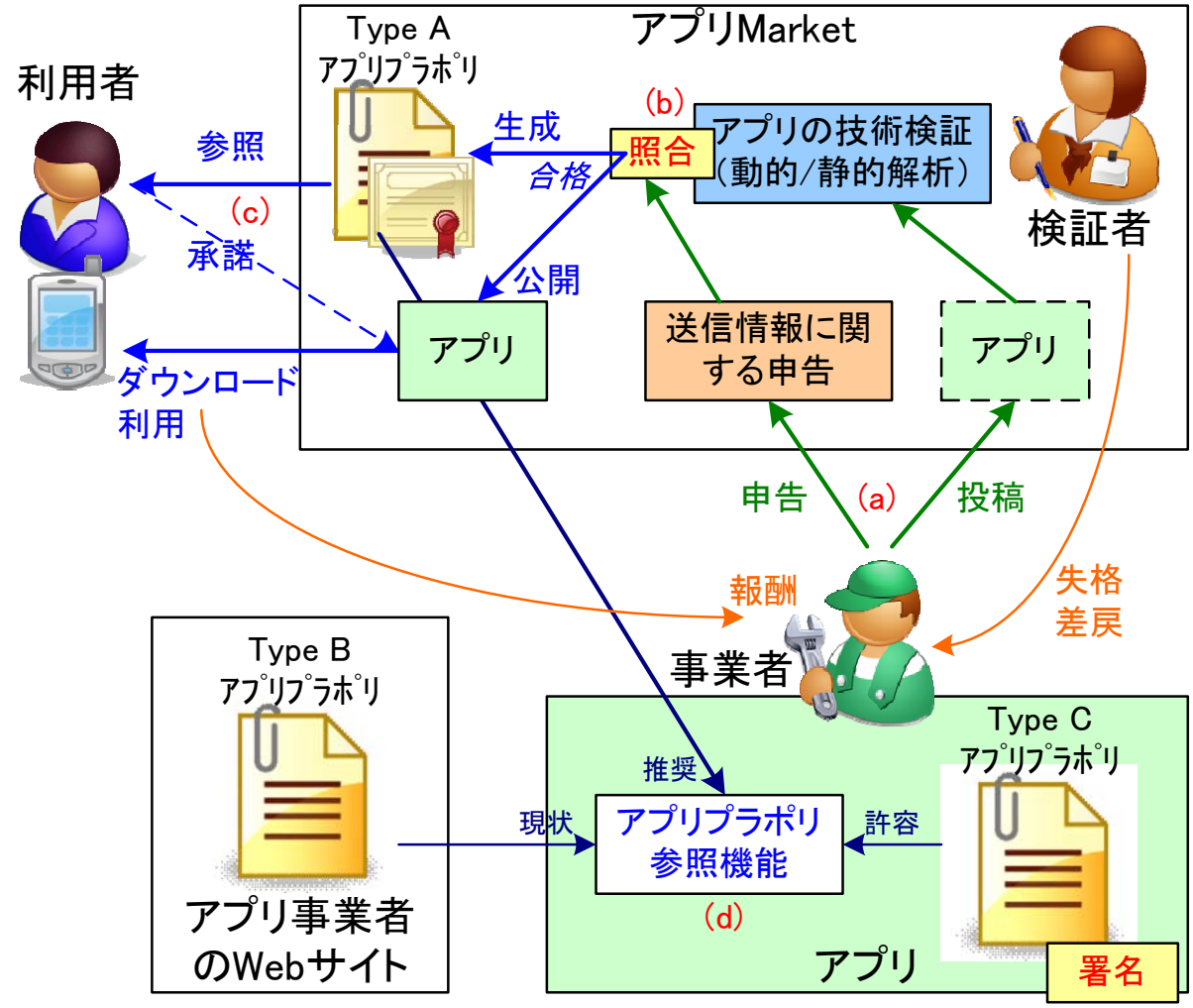
KDDI／KDDI研究所
竹森、磯原、高野

au Marketがアプリの第三者検証役として、アプリ事業者から送信情報に関する申告を頂き、技術検証を行う。概要版／詳細版アプリプラポリを自動生成し、お客様判断を仰ぐことで、アプリの安心・安全化を目指す。

1章 スマホアプリの現状
2章 アプリとプラポリの第三者検証フレームワーク

©2013 KDDI R&D Laboratories Inc.

アプリとプラポリの第三者検証フレームワーク



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

Type A,B,C
アプリの送信情報
チェックツール

Type B,C
アプリプラポリ作
成支援ツール

Type B,C
SDKプラグイン型アプリプ
ラポリ作成支援ツール

実施予定：2013年秋～

送信情報の申告・審査・公開(利用者承諾)

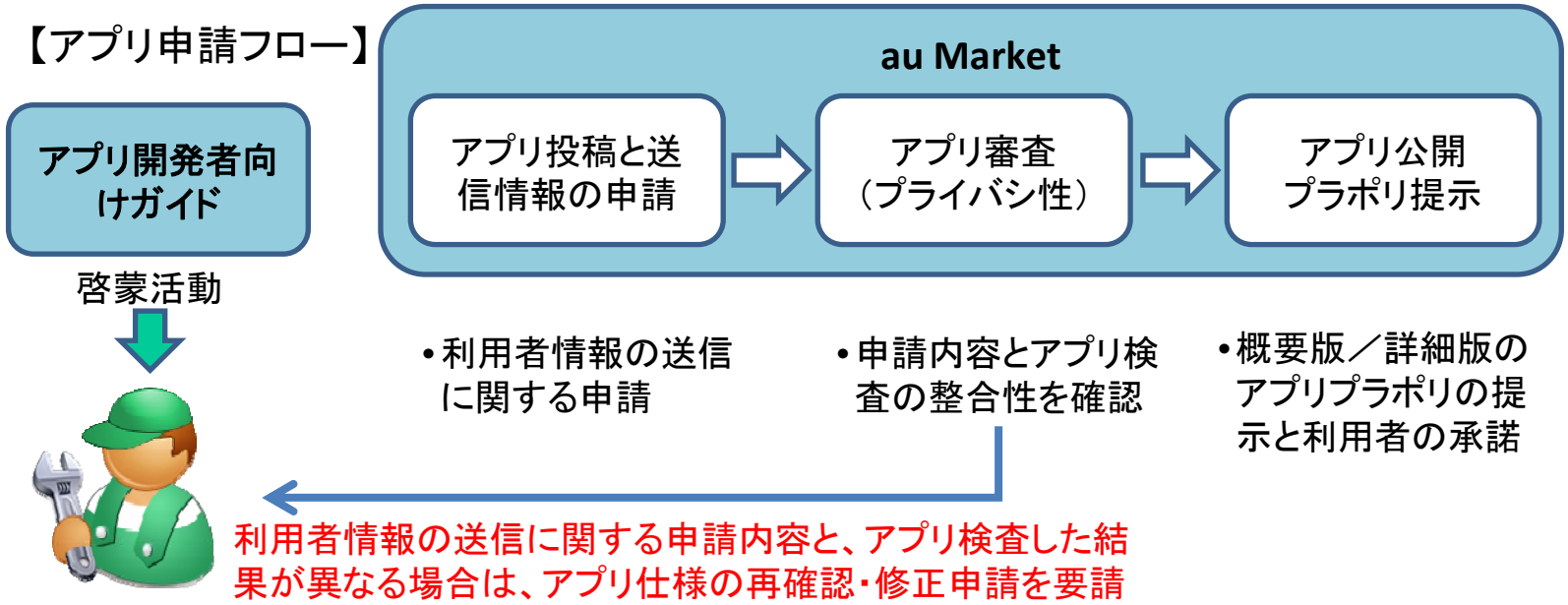
■ アプリ投稿・審査・掲載の流れ

◆ アプリ事業者に扱う情報を申請して頂き、au Market側で動的・静的解析を実施。

◆ 整合性の取れたアプリプラポリを、au Marketから提示・承諾して頂く。

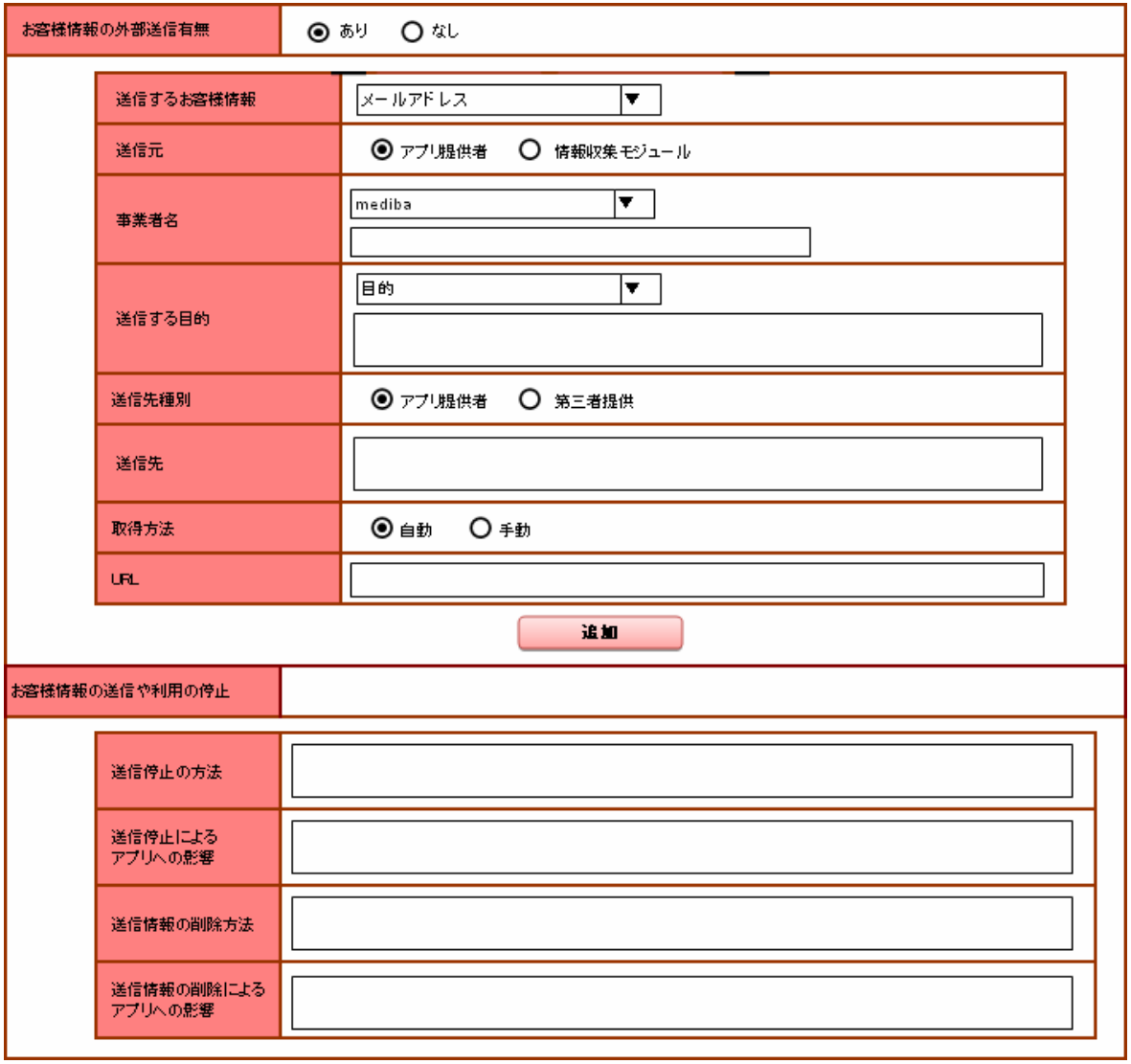
⇒ アプリプラポリ内容はアプリ事業者の責任

⇒ au Marketは、ダウンロード前に、正確かつ解り易い説明を支援。



©2013 KDDI R&D Laboratories Inc.

a）プラポリ事項の申請～SPI準拠へ～



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

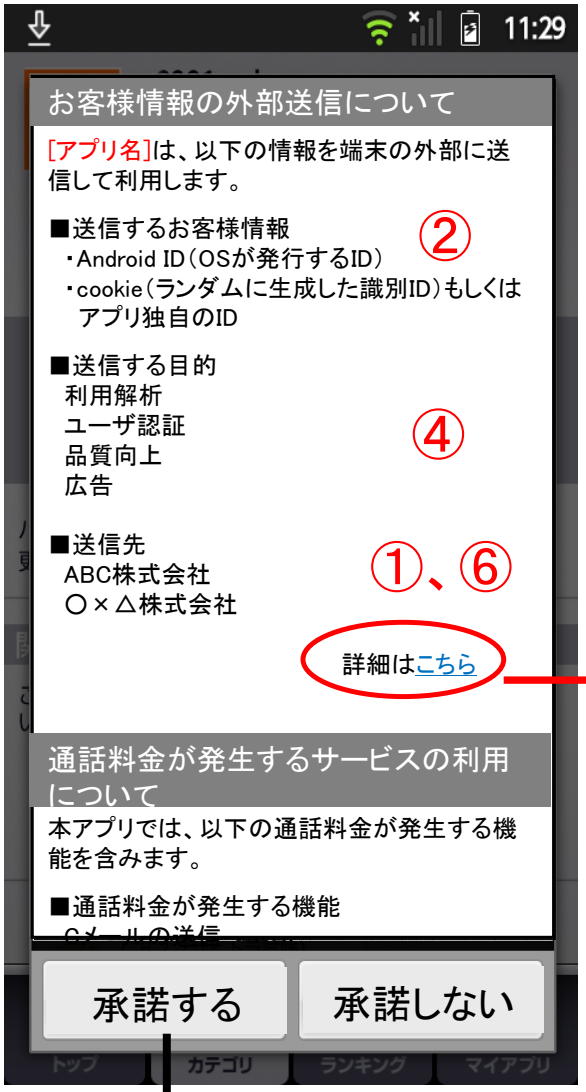
⑧ プラポリ変更の手続き
⇒アプリ更新で再度プラポリ申請

注）開発段階のため変更の可能性あり。

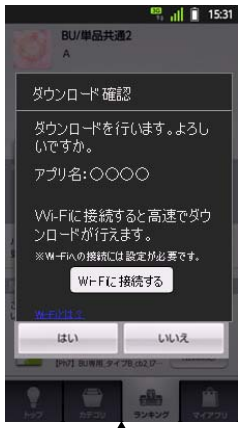
©2013 KDDI R&D Laboratories Inc.

KDDI R&D LABS

c) ダウンロード前の概要版プラポリ



次ページへ



ダウンロード確認画面

■ 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。

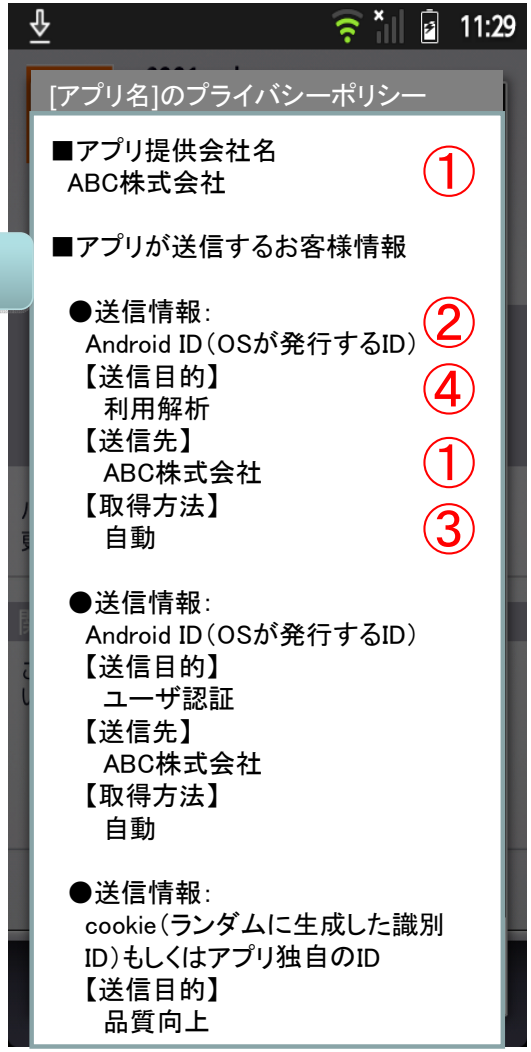
◆ 読んで頂くための簡潔化を目指し、我々がSPIで重要と考えた「送信情報」,「目的」,「宛先（第三者提供）」の概要版を提示。

*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

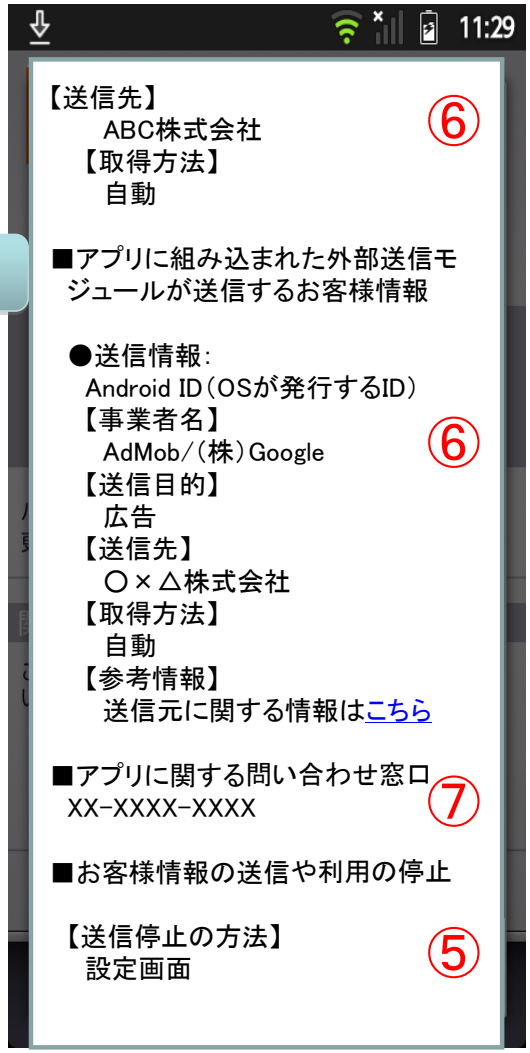
©2013 KDDI R&D Laboratories Inc.

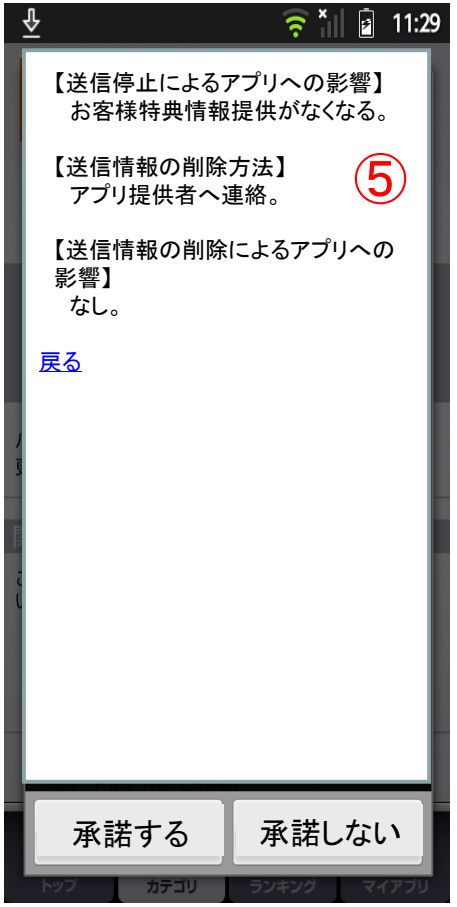
c) ダウンロード前の詳細版プラポリ（新規）

アプリ本体



モジュール





注）開発段階のため変更の可能性あり。

©2013 KDDI R&D Laboratories Inc.

まとめ

■ 提案と効果
- ◆ アプリ事業者から、送信情報や取り扱いに関する申告をして頂く。
  - ⇒ 総務省SPI準拠、曖昧な表現の排除
- ◆ アプリ審査（第三者検証）による申告内容の確認。
  - ⇒ 送信情報の正確率：11% → 100%
- ◆ 生成されたアプリプラポリをau Market側でホスティング。
  - ⇒ 情報送信を伴うアプリのプラポリ所有率：25% → 100%
- ◆ ダウンロード前に利用者のアプリプラポリの提示・承諾を経る。

■ アプリ事業者の役割
- ◆ 申告・修正に関わる手続きは、全てアプリ事業者に担って頂く。
  - ⇒ アプリプラポリの内容は、アプリ事業者の責任に帰す。

■ 総合的な効果
- ◆ 「申請と第三者検証」、「情報送信アプリのDL前プラポリの提示によるお客様判断」で、アプリから必要最低限の情報送信に抑える。
  - ⇒ 情報送信アプリ率：63% → 16%

©2013 KDDI R&D Laboratories Inc.
KDDI R&D LABS

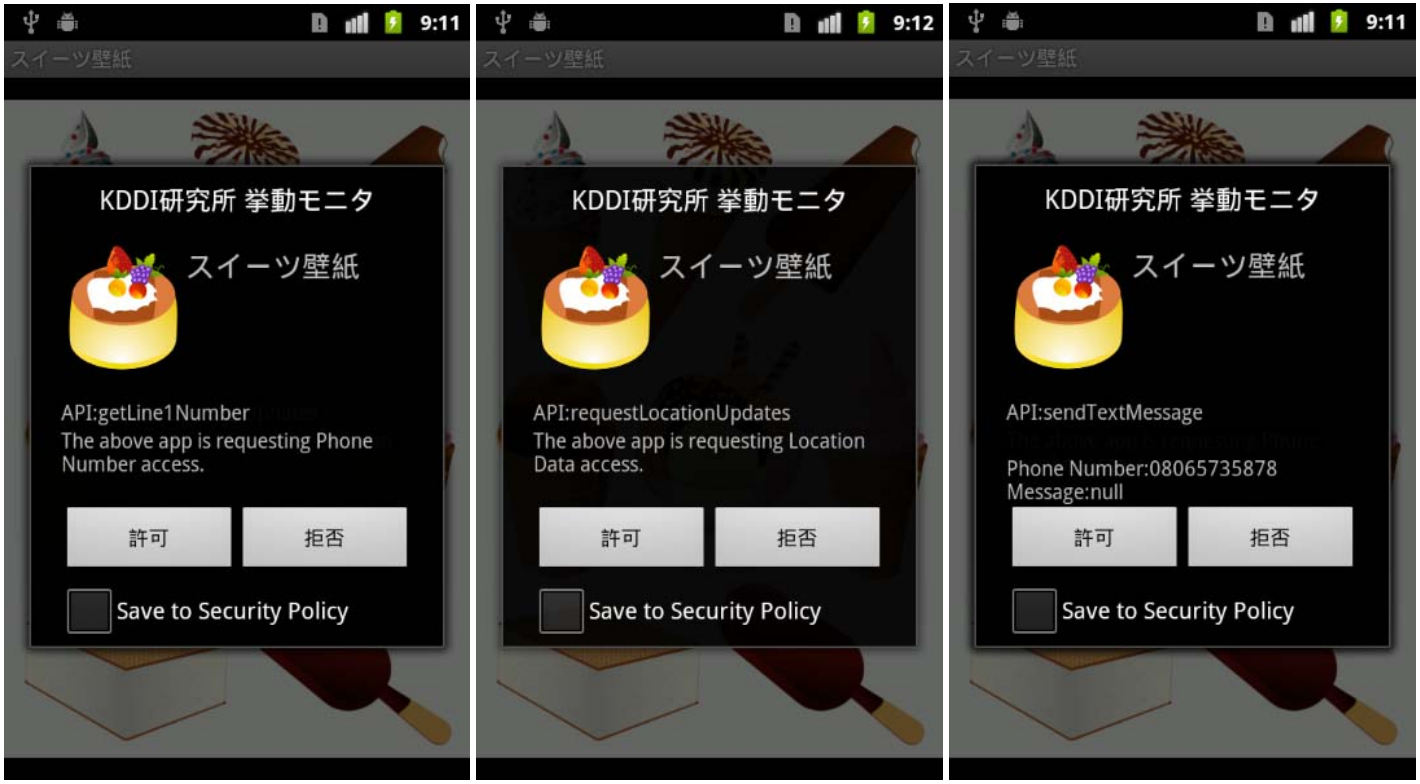
参考：au Market解析技術 ～アプリ挙動のモニタ端末

■ 利用者情報の取得APIへのフック

◆ APIをフックして、アプリの処理を停止し、ユーザ承認を反映する。

⇒ 情報アクセスのログ出力へと応用し、アプリ審査に利用している。

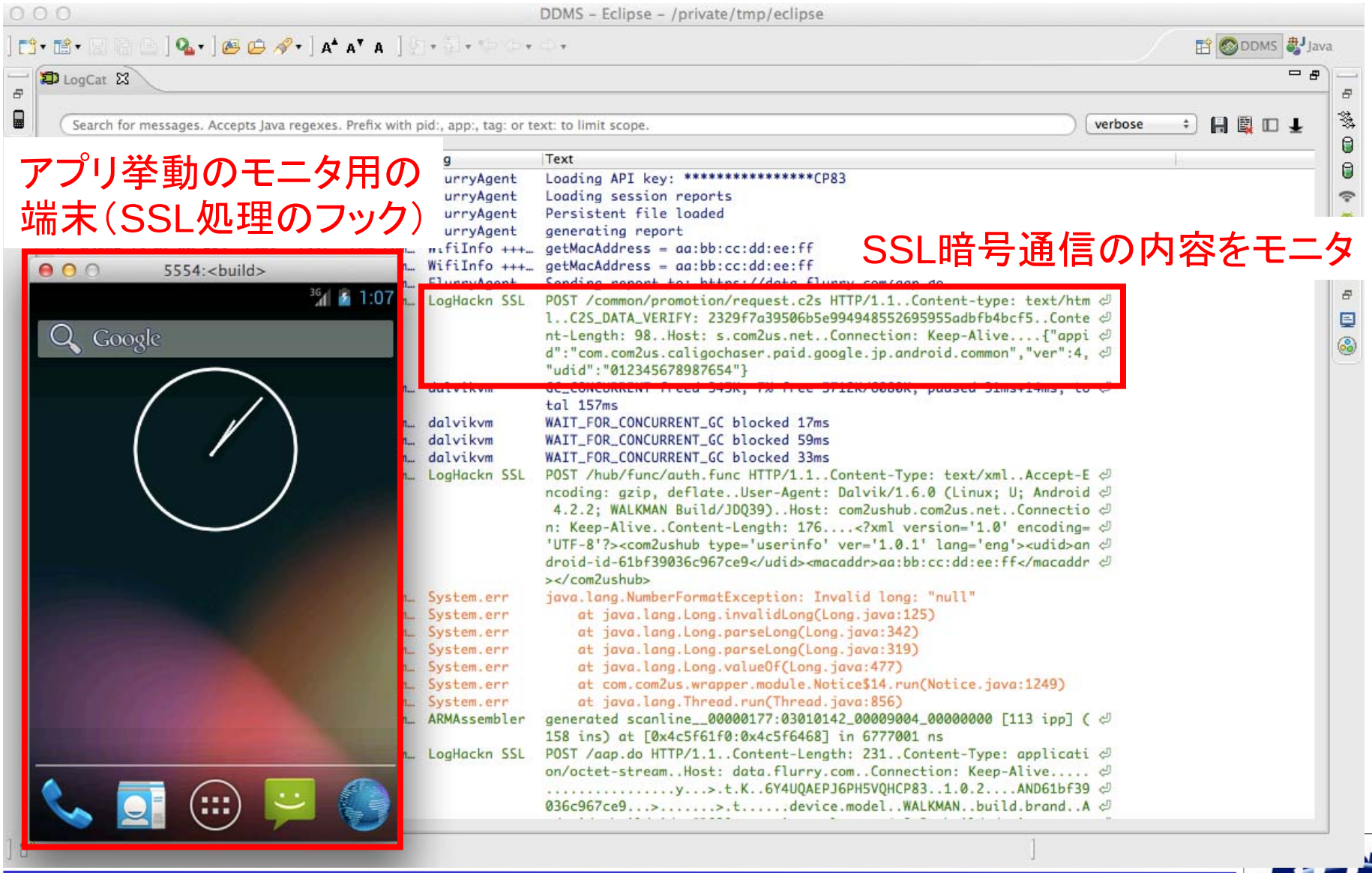
【CSS2011 優秀論文賞】KDDI研、静大、“Android OSにおける機能や情報へのアクセス制御機構の提案”、情報処理学会、コンピュータセキュリティシンポジウム2011.



左：電話番号アクセス
中：位置情報アクセス
右：勝手なSMS送信

©2013 KDDI R&D Laboratories Inc.

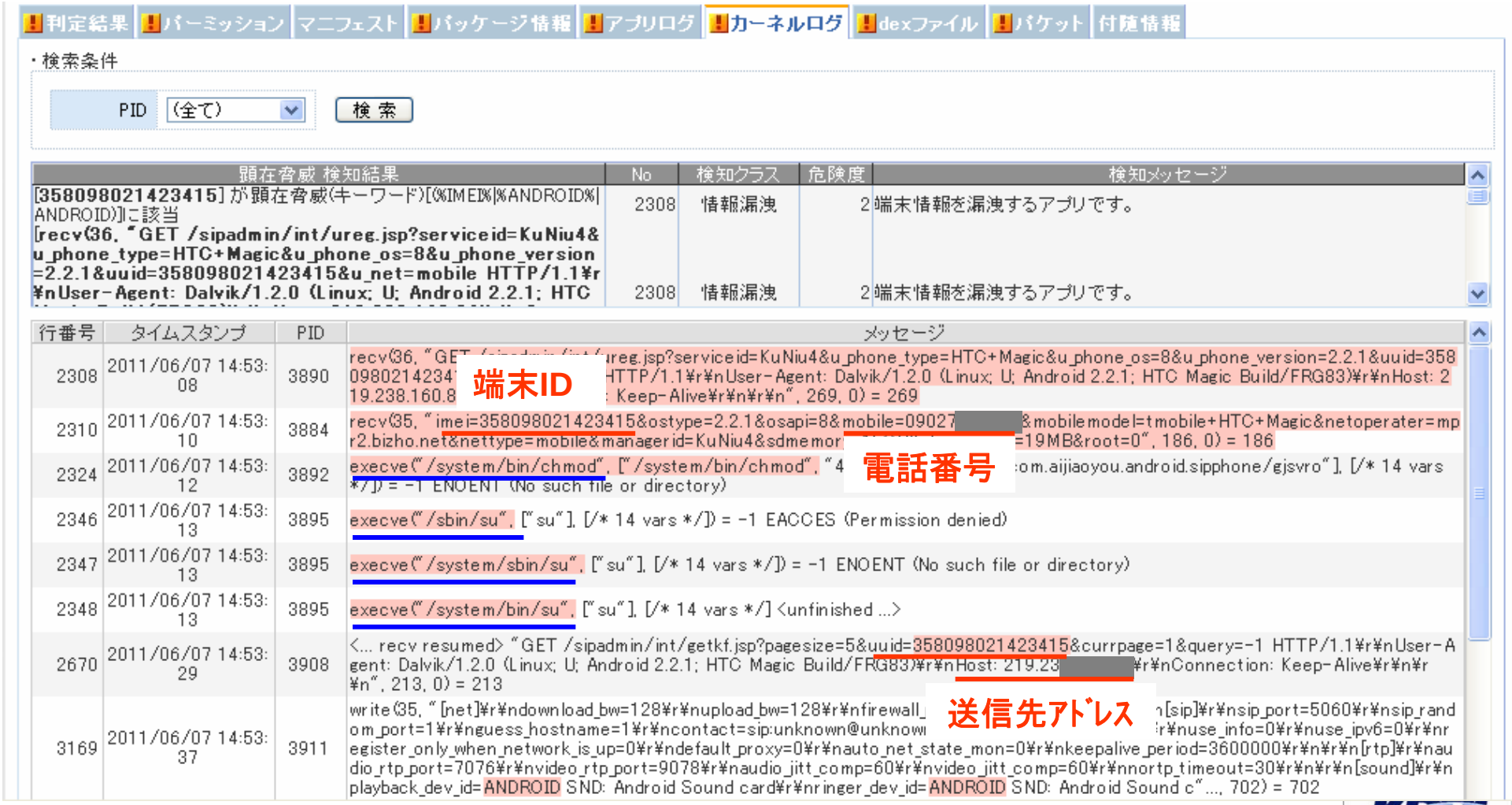
参考：au Market解析技術 ～SSL通信のモニタ～



©2013 KDDI R&D Laboratories Inc.
KDDI R&D LABS

参考：au Market解析技術 ～挙動ログ解析サーバ～

◆ 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。
（断片的なログを組み上げる。）



©2013 KDDI R&D Laboratories Inc.