KDDI R&D LABS

スマートフォンにおけるプライバシ問題と対処の方向性

2013年2月14日

KDDI研究所

田中俊昭

本日の内容

KDDI R&D LABS

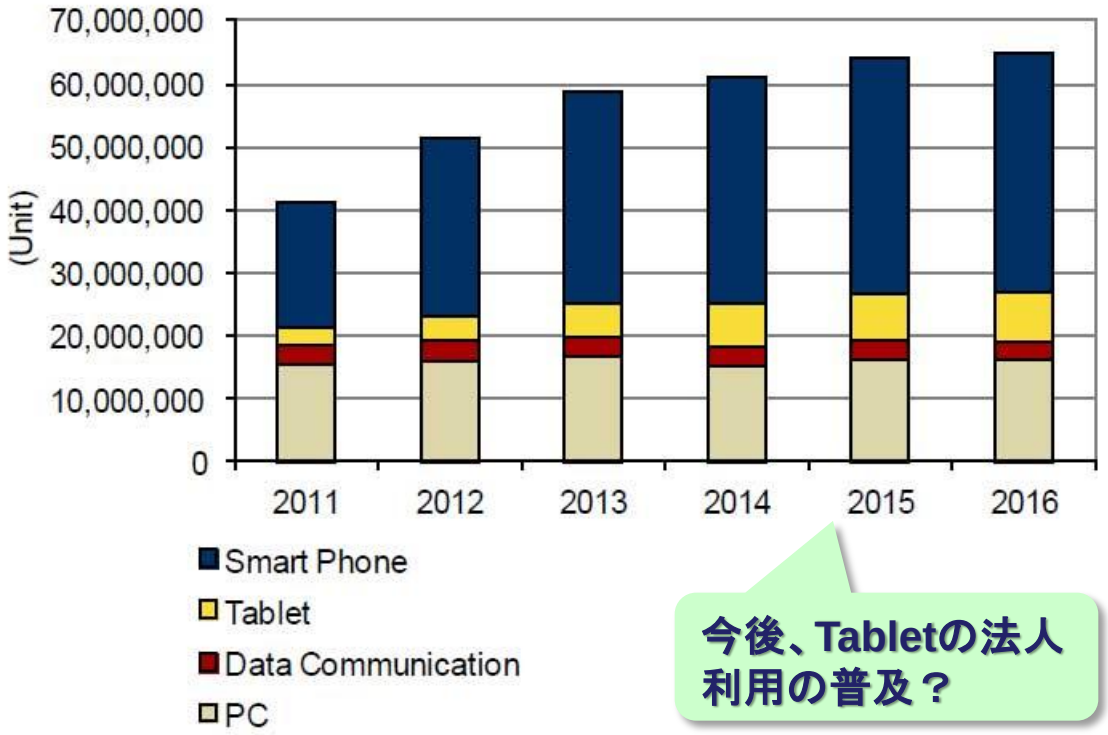
- スマートフォンの動向
- プライバシ問題
  - プライバシ問題とは
  - 米国、欧州、国際機関、日本(ICT関連)
- スマートフォンのプライバシ　課題と対策
  - 課題:
    - スマートフォンプライバシ問題の俯瞰
  - 対策:
    - アプリ審査
    - プライバシポリシー管理フレームワーク
    - 情報収集モジュール
- スマートフォンのプライバシ保護の今後の方向性

スマートフォンの動向

スマートデバイスの出荷台数予測とタブレットのOS別シェア

KDDI R&D LABS

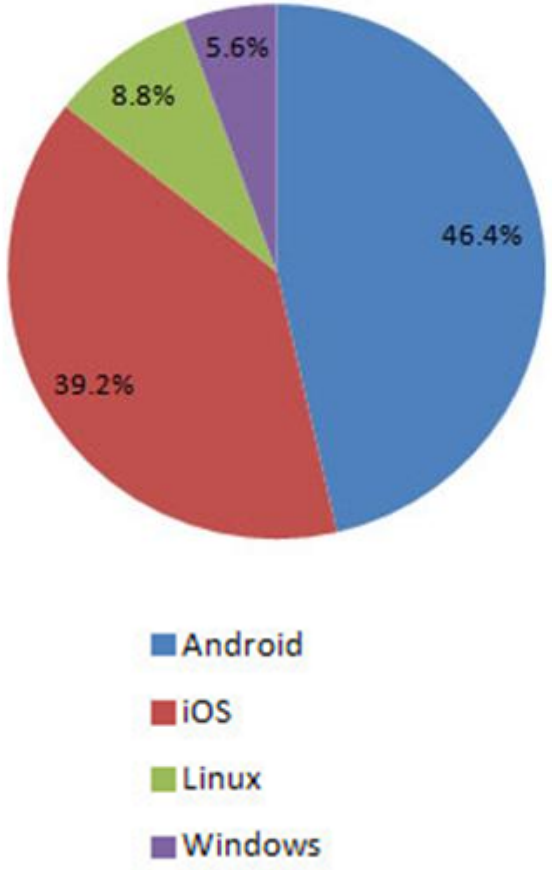
国内モバイルデバイス出荷台数予測：2011年～2016年



今後、Tabletの法人利用の普及？

Source: IDC Japan, 12/2012

タブレット出荷のOS別シェア
（2012年　第3四半期）



参照：http://www.itmedia.co.jp/promobile/articles/1212/26/news084.html

スマートフォンの概要

KDDI R&D LABS

・スマートフォンの特徴
  ・PCを小型軽量化して操作性・携帯性を向上したもの（PCの発展系）
  ・アプリをダウンロードすることで機能追加が可能（アプリの追加は、利用者の自主判断）

スマートフォンの概要

KDDI R&D LABS

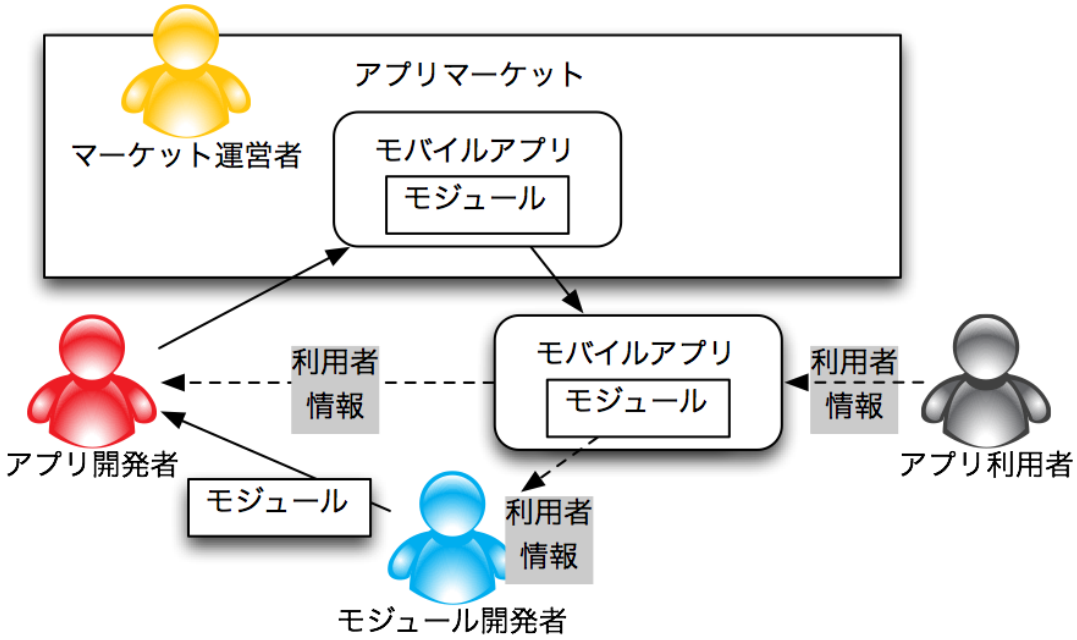
- パーソナルデバイスとして個人情報を蓄積
  - 電話番号、アドレス帳、GPS情報など

表　スマートフォンで保有・管理するパーソナル情報の一例

種別	詳細
利用者を特定する情報	氏名、アドレス帳で管理される情報、メールアドレス
個体を識別する情報（ID)	OSが生成するID(Android ID)、端末ID（IMEI）、加入者ID（IMSI）、SIMシリアルID（ICCID）、電話番号、認証チケット（AuthToken)、アプリケーションが独自に発行するID、MACアドレス、OSやサービスへのログインアカウント、IPアドレス等
ハッシュ値	IDのハッシュ値
利用履歴	位置情報、通話の内容・履歴、メールの内容・履歴、Webのブックマーク・閲覧履歴
アプリケーション	アプリケーションの一覧・利用履歴、アプリケーションの管理データ等
システム	スマートフォンのシステムログ

マーケットのビジネスモデル

- アフェリエイト型のビジネスモデル
  - 広告モジュール/情報収集モジュールを通じた報酬分配
  - 利用者の嗜好や行動を収集し、ターゲット広告、レコメンドなどに活用
  - 82%の無料Androidアプリが外部モジュールを含有（2012年4月、KDDI研　調査による）



有料アプリや、アイテム課金、定額の有料アプリサービスを提供するマーケットもある（例：KDDIのスマートパス）。

スマートフォンの動向

KDDI R&D LABS

- デバイスの多様化
  - スマートフォン、タブレット端末、STBなど
  - マルチデバイスの活用
- HTML5等新たなオープン仕様/ 新たなWebOS
  - W3C*は、2012年12月 HTML5の最終的な標準化完了
    勧告化は、2014年の第4四半期を予定
  - WebOS：FireFox(Mozilla), Tizen (Tizen Association)
- 国際標準に基づくローカルI/F（NFC)のサービス発展
  - O2O(Online to Offline)への期待
  - グローバルスタンダードによるコスト効果
- BYOD(Bring you own device)への期待
  - 企業の情報システムのコスト低減
  - 一方でセキュリティの課題

W3C: HTML5の仕様を策定している標準化フォーラム

プライバシ問題

プライバシ問題

KDDI R&D LABS

- プライバシとは
  - 他人から干渉を受けない私生活およびその権利
  - 他人に知られたくない秘密、侵害されたくない領域
- プライバシ情報に当たるかは個人の判断に従う

- インターネットを利用した経済発展に伴うビッグデータの取り扱いの中で、利用者への透明性を高めたうえで利用する必要性が高まっている。
- 個人のプライバシを保護しつつも、産業界の事業インセンティブを高める社会基盤の模索が各国で始まりつつある。

プライバシ情報の扱いに関する主な動向

KDDI R&D LABS

- EU
  - EUデータ保護規則改正案(2012.1)*
    - 従来の「指令（Directive）」から「規則（Regulation）」に格上げ
    - 個人データ保護の権利の強化（自己情報コントロール権の強化など）
      - 忘れられる権利（Right to be forgotten）
        ユーザがサービス事業に対して自身に関する情報を自由に削除できる権利
      - Privacy by Design原則
    - EU域内でのデータ保護ルールの一元化（EU域内企業にとってメリット）
    - グローバル環境でのデータ保護ルールの詳細化（第三国移転ルールの詳細化など）
- US
  - 米国プライバシー権利章典(2012.1)**
    - 個人のコントロール、透明性、コンテキストの尊重、セキュリティ、アクセスと正確性、焦点を絞った収集、説明責任（Accountability）
  - FTC：急速に変化する時代における消費者プライバシーの保護**
    - ベストプラクティス（Privacy by Design、選択の簡略化、透明性の向上）
    - Do Not Truck（DNT）の実施を勧告

* http://home.jeita.or.jp/cgi-bin/page/detail.cgi?n=376&ca=1
** http://www.i-ise.com/jp/study/EUdata_20120725.pdf

プライバシ情報の扱いに関する主な動向

KDDI R&D LABS

- OECD
  - OECDプライバシガイドライン(1980)　8原則
    - ①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、　⑥公開の原則、⑦個人参加の原則、⑧責任の原則
    - 30年を経て見直し(2013年改定予定)
      インターネット/クラウドコンピューティングの発展、個人データの増大、社会的経済価値とプライバシの脅威、個人データのグローバルな利用可能性
- GSMA
  - Mobile Privacy Principle
  - Privacy Design Guidelines for Mobile Application Development (2012.2)
    - モバイルアプリが扱うプライバシ情報を保護強化するための開発者向けの設計指針
    - Privacy by design 原則
      Transparency, Choice, and Control, Data Retention and Security, Social Networking and Social Media, Mobile Advertising, Children and Adolescents, Accountability and Enforcement

プライバシ情報の扱いに関する主な国内動向

KDDI R&D LABS

- 電気通信事業における個人情報保護に関するガイドライン(2004)
  - 通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定める
- 個人情報保護法(2005.4)
  - 個人情報の有用性に配慮しながら、個人の権利や利益を保護することを目的
  - 民間の事業者の個人情報の取扱いに関して共通する必要最小限のルールを規定「利用目的の特定」、「適正な取得」、「利用目的の通知・公表」、「安全な管理」、「従業員、委託先の監督」、「第三者提供の制限」、「保有個人データの開示」、「苦情の迅速な処理」など
- スマートフォン　プライバシー　イニシアティブ（総務省）(2012)
  - 利用者情報の適切な取り扱いと、リテラシー向上による市場の発展を目的としたスマートフォン・プライバシに関する包括的な対策の提言
  - 基本原則①透明性の確保、②利用者関与の機会の確保、③適正な手段による取得の確保、④適切な安全管理の確保、⑤苦情・相談への対応体制の確保、⑥Privacy by Design
  - プライバシポリシーの作成に関する指針として、8項目の記載事項を提示
    - 取得する情報・情報を取得する事業者や個人の名称・情報の利用目的・送信先

KDDI R&D LABS

スマートフォンのプライバシ課題と対策

スマートフォンにおける脅威

KDDI R&D LABS

スマートフォンにおけるマルウェア

- PCのような自動的なウイルス感染はない。*
  - 自動感染する通信の口（ポート）がない。
- スマホOSには、安全に利用するための機構が施されている。
  - Android™では、仮想環境（Sandbox）でアプリが稼働し、アプリがシステム領域や他のアプリにアクセスするにはユーザ承認が必要。
- マルウェア出現比　PC：Android™フォン ＝ 400：1**

スマートフォンにおける最大の脅威

- ユーザ自身がネットからマルウェアと知らずにダウンロードする。
  - マルウェアは、例えばふつうのゲームアプリの振りをして不正動作を行う。
  - 一旦、マルウェアに感染すると、常時ONのスマートフォンでは、自身や外部に対する被害が拡大する恐れがある。

*ウイルスとは、マルウェアの一種で、ファイルやネットワークを媒介して自動感染（拡大）するもの。手動感染した後は、自動感染はありうる。
**統計情報（2011年）の提供元　株式会社カスペルスキー

スマートフォン特有のプライバシ課題

KDDI R&D LABS

- プライバシ情報の不正利用防止
  - Marketからダウンロードするアプリのクオリティの問題
- プライバシ情報の利用許諾
  - Androidのパーミッション機構によるOpt-inの問題
- 情報収集モジュール
  - 無料アプリを支えるアフェリエイトモデルの情報収集モジュールにおける端末識別の課題

プライバシ情報の不正利用による問題

KDDI R&D LABS

- 透明性の確保、適切な手段による取得の確保

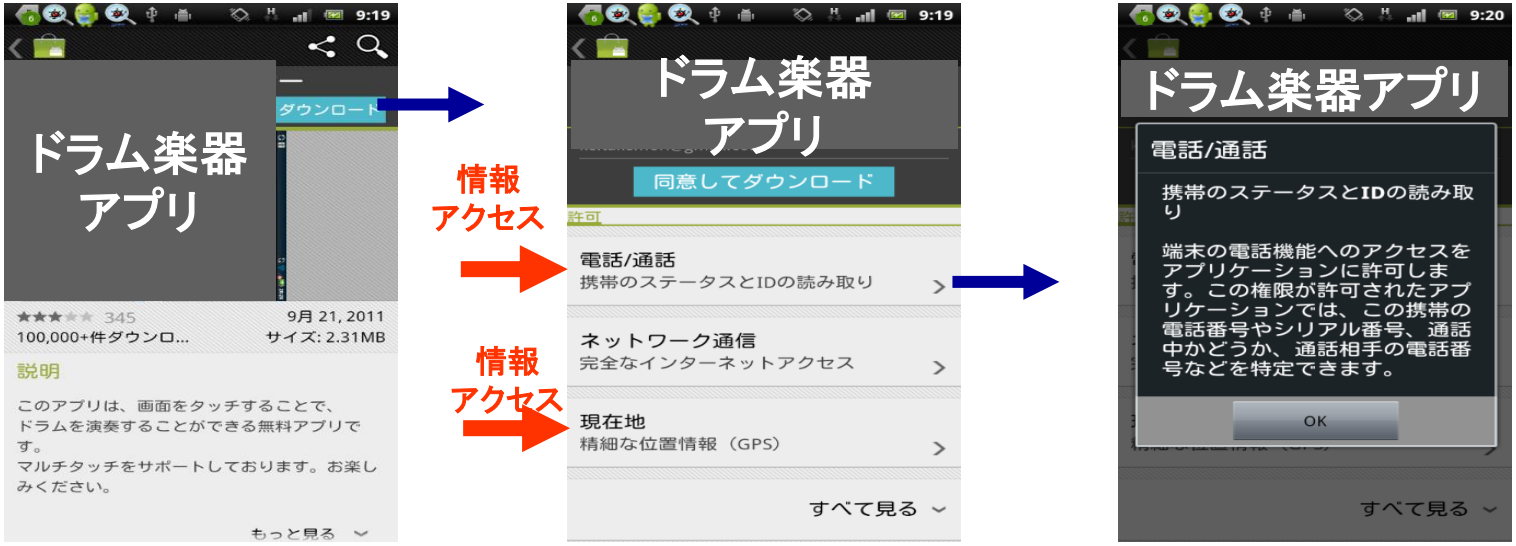
分類	原因	事例	頻度
OSの機能	OSにプリインされた機能がプライバシ情報を収集	Carrier IQ(ネットワーク診断ソフトウェア)がiPhone, Android端末内の利用者情報をCarrier IQ社へ送信	稀
アプリの機能	正当な事業者のアプリによるプライバシ情報漏えい	Pandola Media(インターネットラジオ視聴アプリ)が複数の広告会社へ利用者情報を送信していた。	ややあり
不正アプリ	アプリの不正動作によるプライバシ情報の漏えい	Exprespam 「バッテリー・キーパー」「スマホワンセグ」「迷惑メールブロック」などの名称のアプリとして流通。端末の電話番号や連絡先の名前とメールアドレスなどの個人情報を、リモートサーバへ送信	多数

プライバシ情報の利用許諾の問題

KDDI R&D LABS

- 透明性の確保、利用者関与の機会の確保
  - Opt-in, Out-outによる利用者の選択権の付与
  - Permission機構の課題
    - 過剰な権限要求、使用目的の説明不足等

ドラム楽器アプリでは不要なパーミッション（IDの読み取り、位置情取得等）を要求　⇒ 情報漏えいの可能性



実態調査

～2011/8アプリ vs 2012/4 100アプリ～

KDDI R&D LABS

■ 2011年8月収集: 400個のスマホ向け無料アプリを調査
- ◆ 第三者の情報収集モジュールの組込み組み率　56.9% /980件
- ◆ アプリ本体を含め、何らかの端末情報を送信するアプリ数　181件（45.3% /400件）
- ◆ 適切な説明*1を経て情報収集しているアプリ　白17/400件（4.3%）　9.4%/181件
- ◆ 不適切な説明のまま情報収集しているアプリ　灰7/400件（1.8%）　3.9%/181件
- ◆ 勝手に情報送信しているアプリ　黒157/400件（39.3%）　86.7%/181件

■ 2012年4月収集：100個のスマホ向け無料アプリを調査
- ◆ 第三者の情報収集モジュールの組込みアプリ数　82% /100件
- ◆ アプリ本体を含め、何らかの端末情報を送信するアプリ数　81件（81% /100件）
- ◆ 適切な説明*2を経て情報収集しているアプリ　白 2/100件（2%）　3%/81件
- ◆ 不適切な説明のまま情報収集しているアプリ　灰 13/100件（13%）　16%/81件
- ◆ 勝手に情報送信しているアプリ　黒 66/100件（66%）　81%/81件
- ◆ 70種の情報収集モジュールが組み込まれていた。
  - ⇒ 65種の広告、5種のアクセス解析モジュール

増加*

*新たにSSL送信を検知

減少

*1 2012/1月のau Marketの基準を満たしていないもの。
*2 2012/10月のau Marketの基準を満たしていないもの。より厳密化と事前許諾を課している。
尚、総務省「スマートフォン プライバシー イニシアティブ」の8ヶ条＋提示方式を参考にしている。
但し、総務省公開は、6/28β、8/7ver1のため、イニシアティブの公開前のアプリ。

通信事業者としての取り組み

KDDI R&D LABS

- スマートフォンプライバシ問題の対策基本方針
  - プライバシ情報の主観性を踏まえ、国内外の客観的な基準(コンセンサス)を規範としたプライバシ情報の扱い。
  - 特に、総務省　スマートフォン　プライバシ　イニシアティブのガイドラインを配慮

- KDDI研究所の取り組み
  - 1. プライバシ情報の不正な漏えいを防ぐアプリ審査(商用化)
  - 2. プライバシ情報の利用許諾のためのポリシー管理フレームワーク
  - 3. プライバシを考慮した情報収集モジュールの提案

au Marketのアプリ評価

KDDI R&D LABS

■ 安全性検査

◆ アプリ配信サイトが安全であれば、脅威の多くを取り除ける。

⇒ 事前検査と掲載中検査：auスマートパス向けアプリの全検査

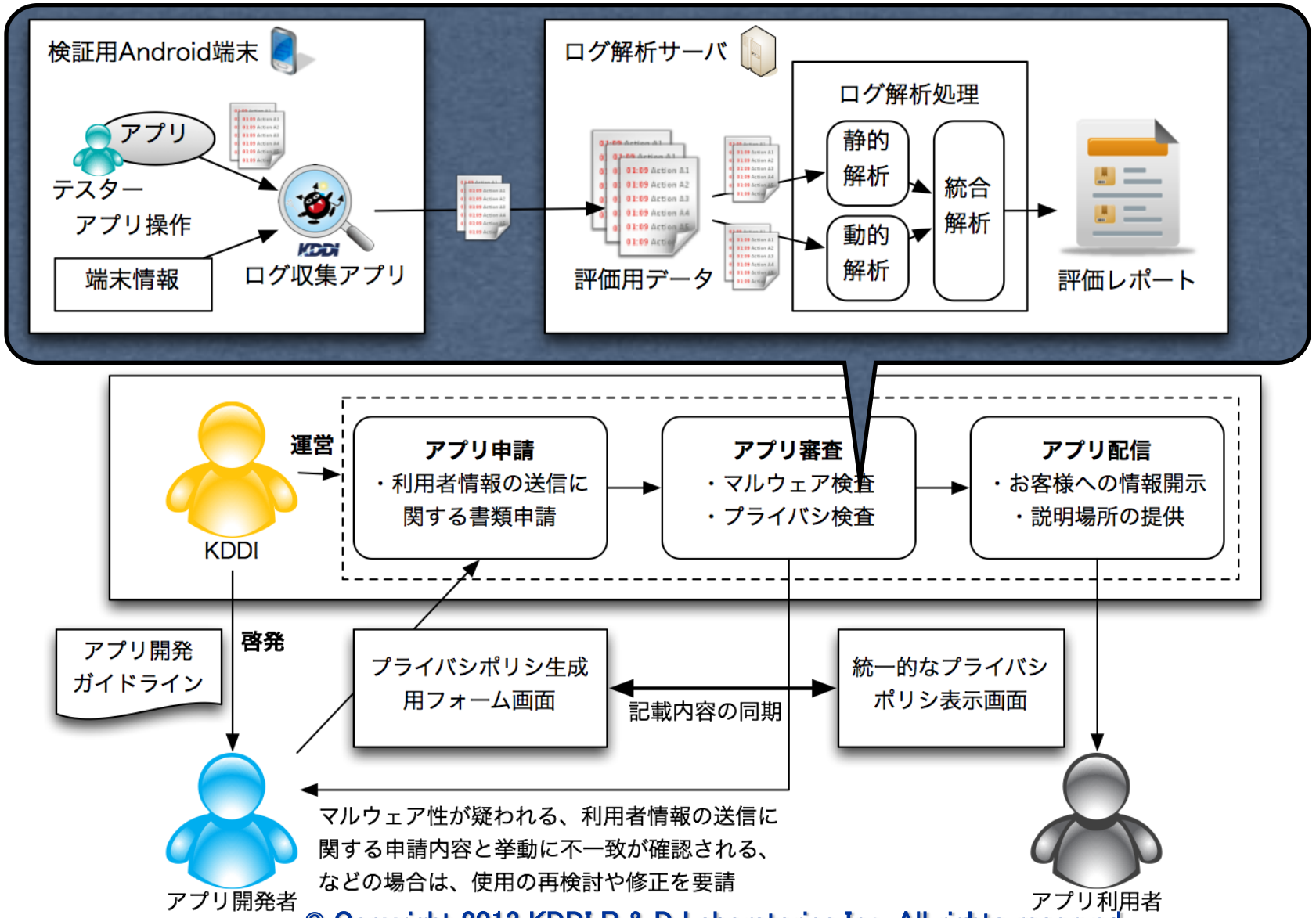
⇒ 静的解析と動的解析： アプリの機能や実行ログを確認

チェックのポイント

1. 機能（パーミッション）
2. 本来利用できない機能の有無
3. 利用者情報の勝手な送信の有無
4. 外部への不正アクセスの有無 etc

Androidアプリ安全性評価システム

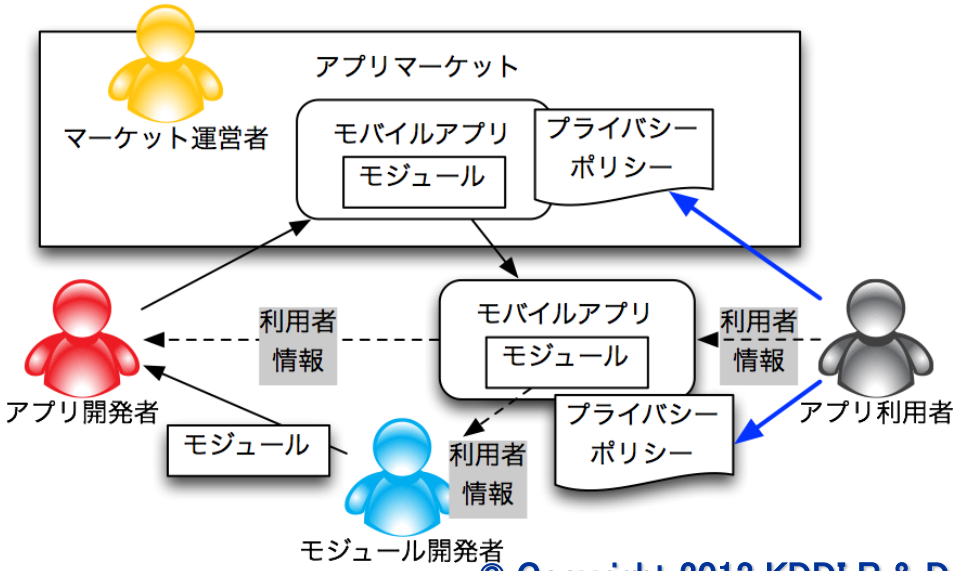
KDDI R&D LABS

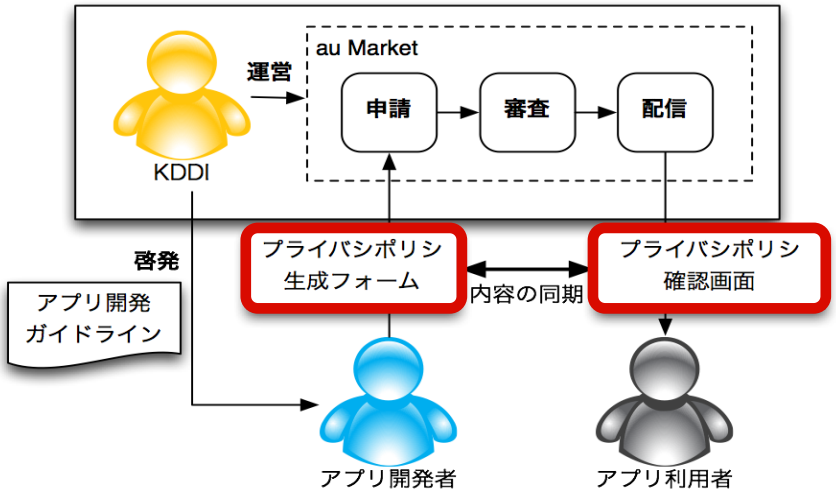


プライバシポリシー管理フレームワーク

KDDI R&D LABS

- 目的
  - アプリによる利用者情報の取り扱いの透明性を確保する
- 概要
  - 透明性を確保する手段として、適切な「プライバシーポリシー」を用いて、アプリの利用者の承諾を得る利用形態を定着させる
- プライバシーポリシーの作成指針
  - プライバシーポリシーの作成に関する指針として、スマートフォン プライバシー イニシアティブ（総務省）の以下の8項目を配慮





プライバシポリシーの利用者への告知

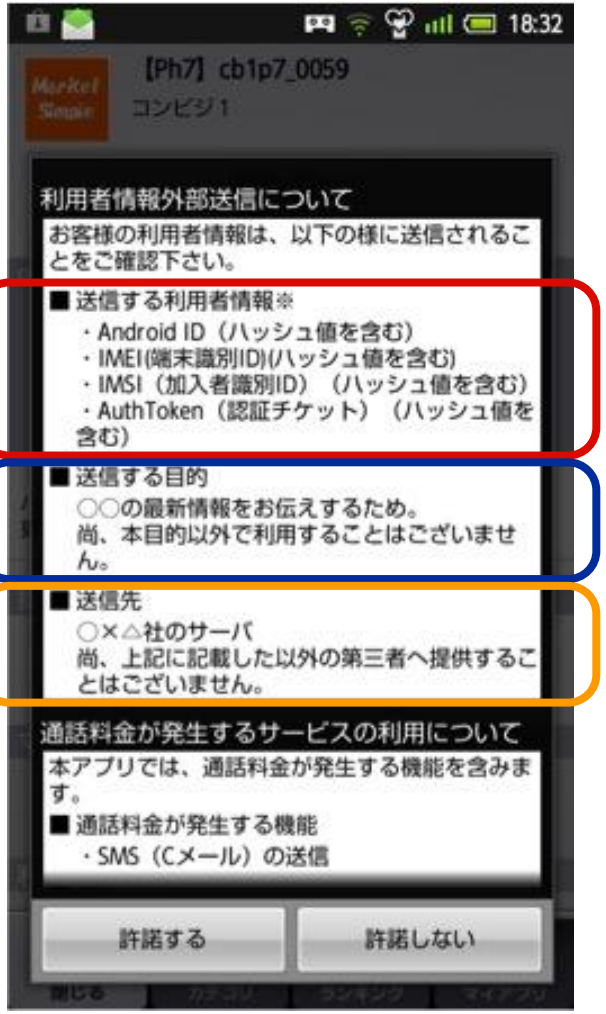
KDDI R&D LABS

許諾文を読む文化のない日本のユーザ向けに、読みやすさを考慮した1ページの画面で重要な3項目を説明！！

取り扱う情報

取り扱う目的

情報の送信先



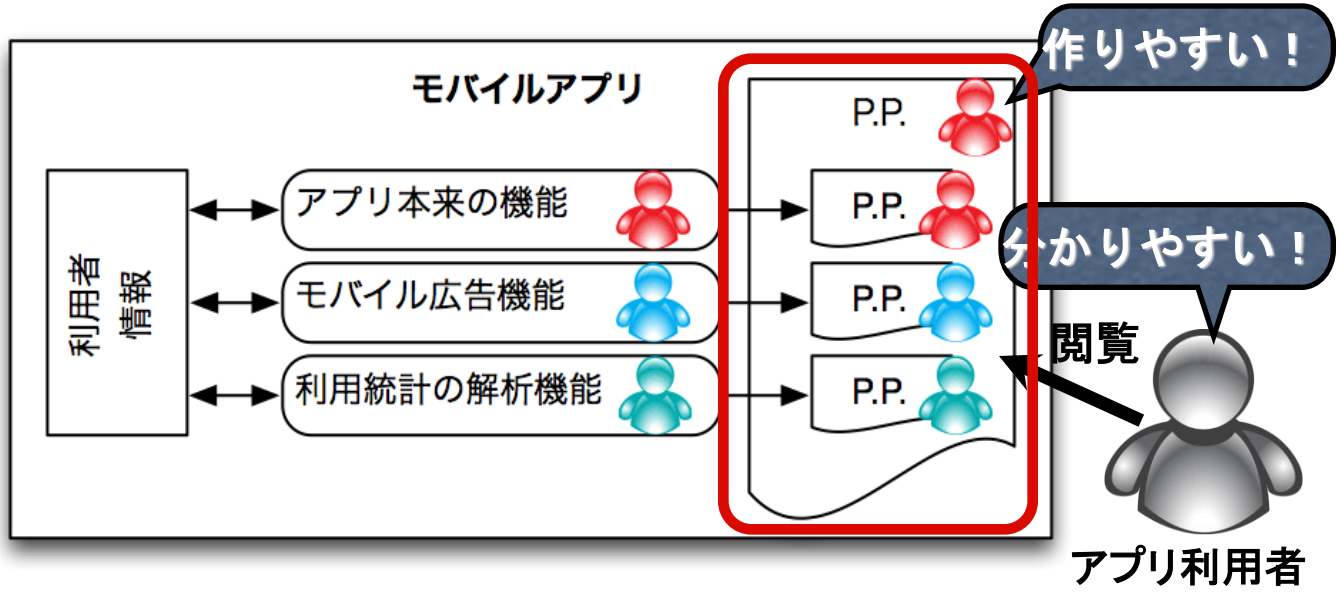
利用者情報の取り扱いに関する申請画面

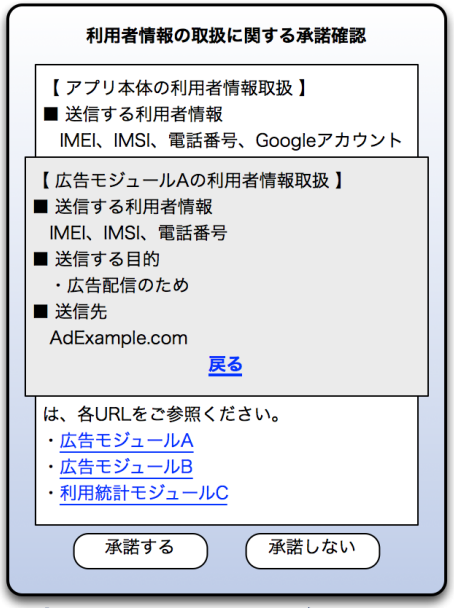
利用者情報の取り扱いに関する告知画面

プライバシポリシー
～　外部モジュールを含むアプリ　～

KDDI R&D LABS

- 要件
  - アプリを構成する機能モジュール毎の責任分界点の明確化
  - アプリの利用者が記載内容とモジュール毎の責任の範囲を容易に理解できること
- プライバシーポリシーの管理運用手段
  - アプリを構成する各モジュールの作成者がプライバシーポリシーを作成する
  - アプリ開発者が、自身の提供するアプリを構成する全てのモジュールに関する内容を含むプライバシーポリシーを作成し、アプリ利用者に提示する





責任分界点を明確化した
プライバシポリシーの画面例

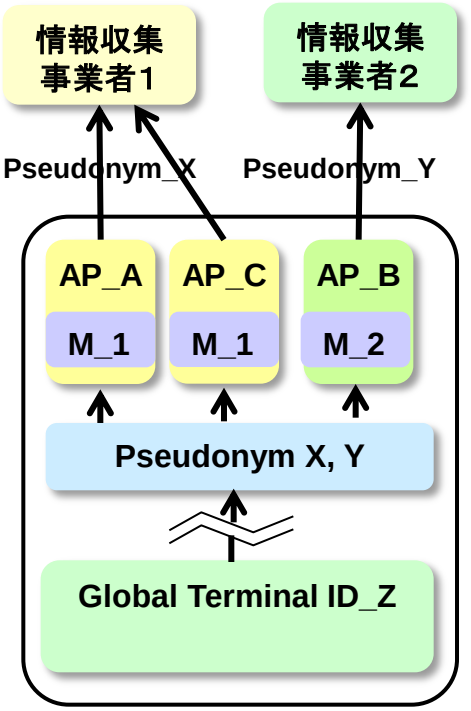
プライバシを考慮した情報収集モジュールの提案

KDDI R&D LABS

- 目的
  情報収集事業者による利用者アクセス履歴の収集・活用が行われる際に、過度なプライバシ情報の流出を回避する仕組みを提供

- 要件
  - 機能要件:
    - 情報収集事業者が端末を一意に識別できること
  - プライバシ要件:
    - ①端末の識別では、実端末への到達性は持たないこと
    - ②情報収集機能の許諾を利用者が関与できること
    - ③忘れられる権利が保障されること
    - ④名寄せによる行動追跡を回避できること

- 提案手法
  - Pseudonym(仮名ID)を利用（要件①, ③, ④）
    - Web Cookieライクの端末に紐づかないID
  - 許諾状態、Pseudonymを共通モジュールで管理(要件②)
    - オプトアウト対策



スマートフォン

AP_*j* ：アプリ
M_*i* ：情報収集モジュール

情報収集モジュール提案詳細

KDDI R&D LABS

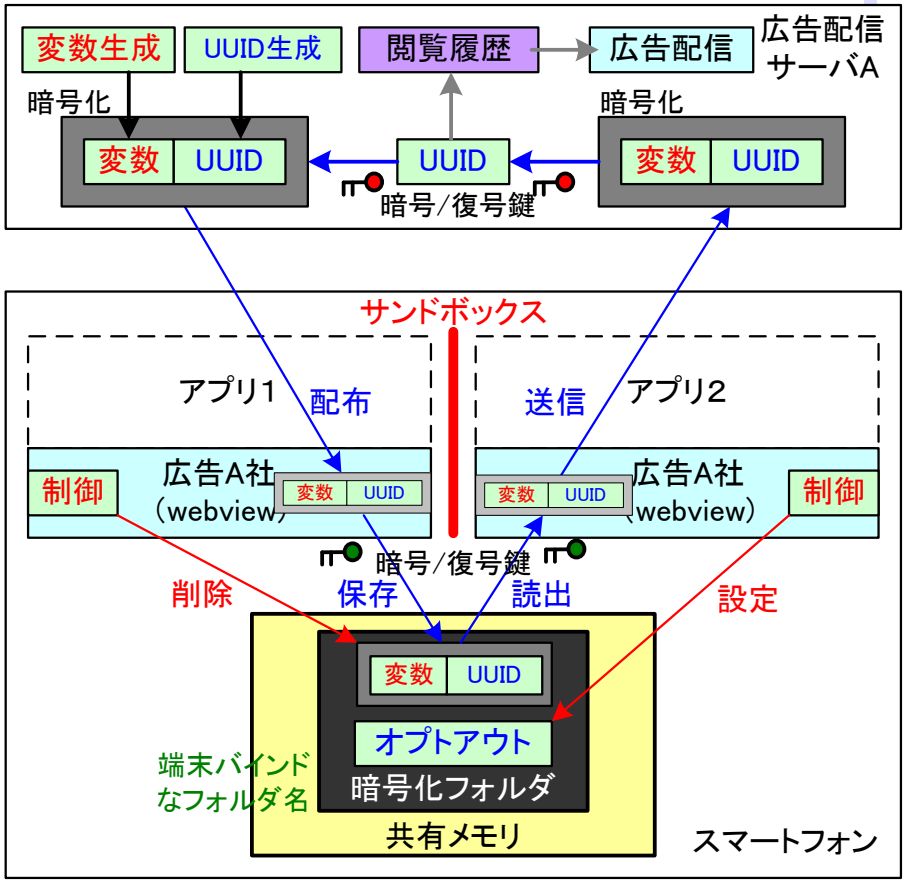
動作手順

①広告配信サーバは、暗号化（変数＋UUID）し、アプリ1の広告モジュールへ送信。

②暗号化（変数＋UUID）を、共有メモリへ保存する。

③ アプリ2の広告モジュールは、暗号化（変数＋UUID）を広告配信サーバへ送信。

④ 広告配信サーバは、復号してUUIDを取り出す。



スマートフォンのプライバシ保護の今後の方向性

スマートフォンのプライバシ保護 ～今後の課題～

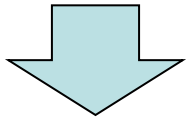
KDDI R&D LABS

- アプリの検証
  - ブラックボックステストの限界
- Opt-inのコンセンサス
  - Consentの解釈
  - NFCのローカルI/Fにおける許諾手続きと利便性のバランス
- 新たなプラットフォームへの対応・検証
  - HTML5, WebOS
    W3CではDNTの検討を実施
- スマートフォンに対する信頼性向上
  - OS, プラットフォームの完全性検証
    (SIM, TPM, SoCのトラストデバイスなどの活用)

スマートフォンのプライバシ保護 ～今後の課題～

KDDI R&D LABS

- プライバシ情報のライフサイクル管理
  - 現状、プライバシ情報の収集と一次利用に関する議論が中心
  - 今後、プライバシ情報の二次利用やRetentionやDisposalをどのように透明性を持って実践できるかの議論が必要



- スマートフォンプライバシ問題の対策基本方針
  - プライバシ情報の主観性を踏まえ、国内外の客観的な基準(コンセンサス)を規範としたプライバシ情報の扱い
  - PIMS(Privacy Information Management System)等の国際標準のフレームワークに基づいた評価
  - PdDを実践するためのコストエフェクティブな研究・開発を推進
    フォーマルな理論の客観的な指標としての実世界への展開も期待

KDDI R&D LABS

ご清聴ありがとうございました。