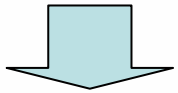
アプリケーションWG

リーダ：大輪@トレンドマイクロ　副リーダ：前田@カスペルスキー、竹森@KDDI

1.マーケットの運用TF for Android（北島@ソニーエリクソン）
2.アプリの攻撃性検査TF for Android（竹森@KDDI）
3.情報収集モジュール対応TF（岸原@MCF）
4. アプリ安全設計・セキュアコーディング（松並@ソニー）

はじめに

・スマートフォンとは、アプリケーションプラットフォームである。
・アプリの導入で高機能化を図るケータイである。



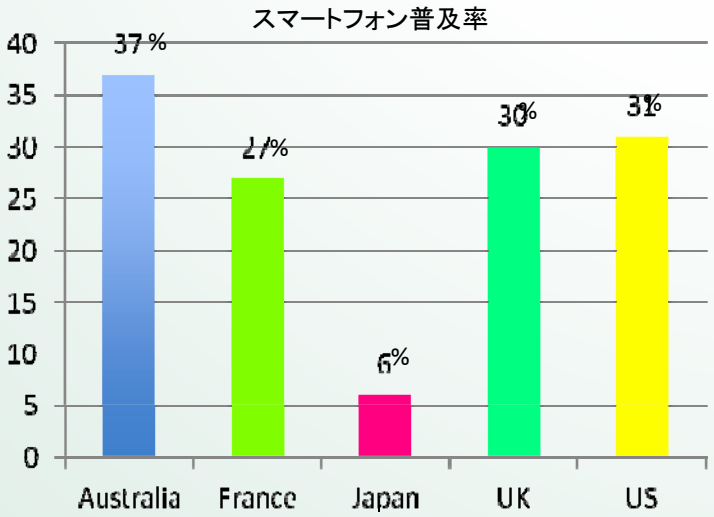
・スマートフォンの利用シーンで生じるセキュリティ事故の多くは、マーケットからアプリをダウンロードする際に生じる。

(1) 安全なマーケットを運用することが重要。
(2) 投稿されるアプリの攻撃性を事前審査することが重要。
(3) プライバシ漏洩が問題視される中、収集への指針が必要。
(4) アプリ開発が個人層まで拡がる中、安全への啓発が必要。

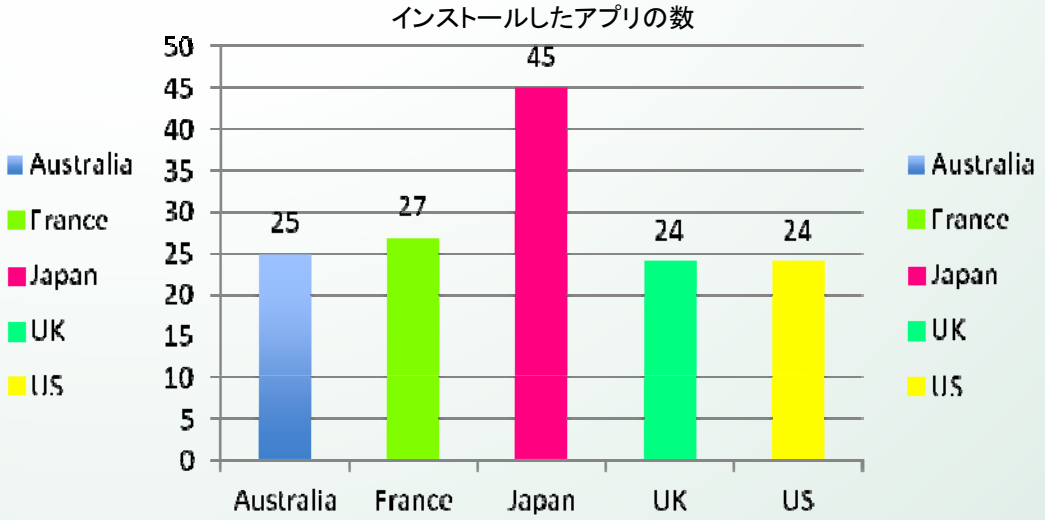
1.マーケットの運用TF

日本におけるスマートフォンユーザの特徴

1. 日本のスマートフォン普及率は6%と調査国中最低。(フィーチャフォンは除く)
2. 日本ではインストールしているアプリが平均45個で調査国中最高。
3. 広告クリック率も高く、有料アプリの普及率も高い。
4. 英語が苦手であることから、日本の大手開発元のアプリケーションが好まれる傾向がある。



Japan smartphone penetration data excludes feature phones



「世界のスマートフォン利用に関する調査-OUR MOBILE PLANET 10/27/2011 By Google
「スマートフォンユーザーの利用動向調査-By ディーツーコミュニケーションズ
2011/3～7月調査、 日本の有効回答数＝2000名

1.マーケットの運用TF ～Androidのみ～

Android Marketの現状とアプリ開発者の声

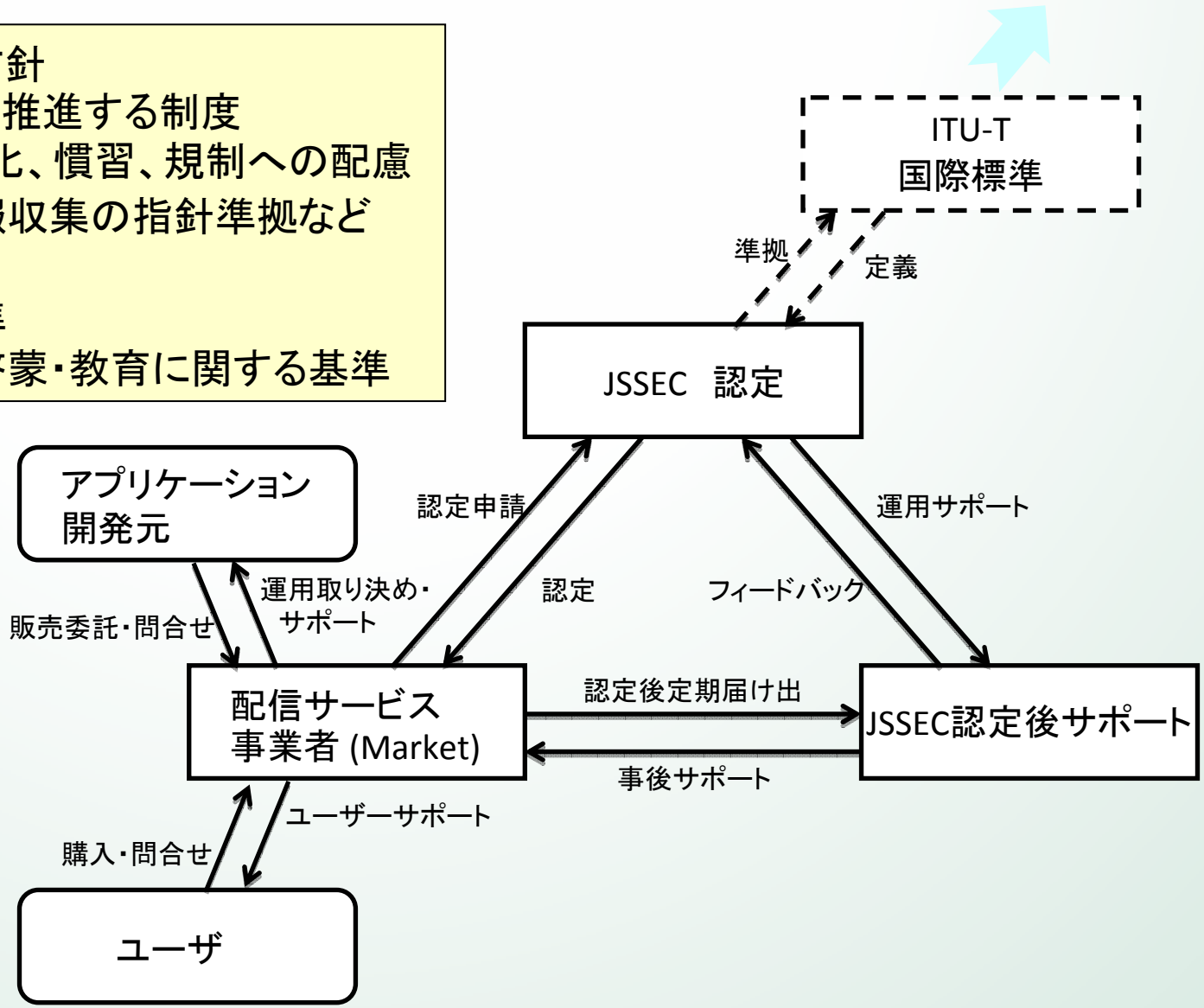
- 海賊版の無い所で売りたい。
- 素人アプリに埋もれさせたくない。
- 手数料など、自分たちで決めたい。
- 適正価格で売りたい。
- キャンセルポリシを独自に決めたい。
- 法的にも文化的にも国や地域合った方法で売りたい。
- 安全な課金スキームを持ちたい。
- 攻撃性が無いことをアピールしたい。

<u>安心・安全なマーケットの運用に関する指針と、認定制度が必要</u>

USマーケットで「テトリス or Tetris」を検索した例
※日本では版権の関係で発売元がEAではありません。

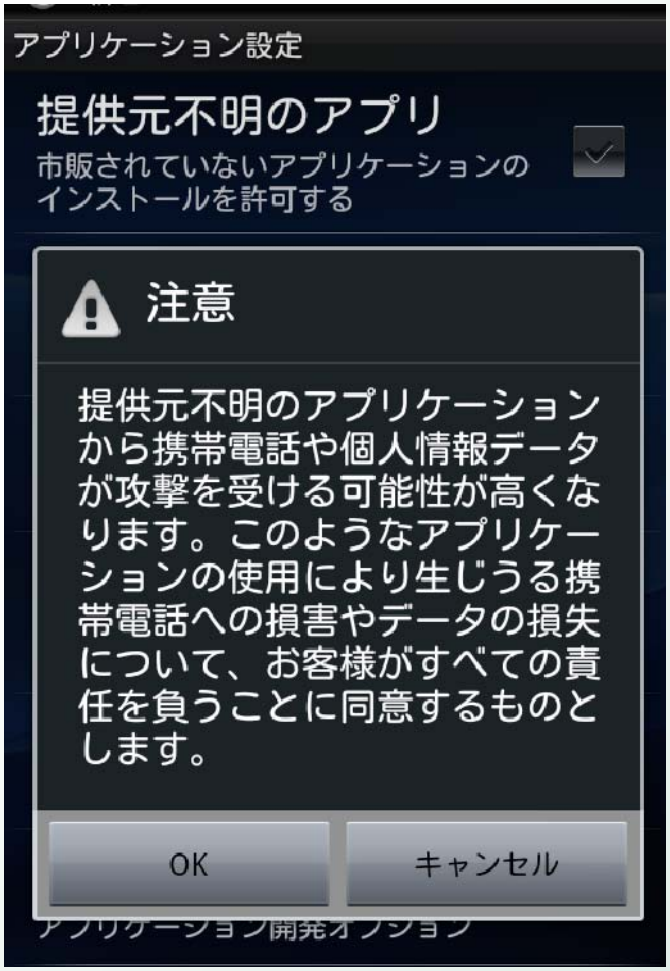
1.マーケットの運用TF ～認定制度(案)～

・認定マーケット制度の基本方針
  -配信サービスの適正運用を推進する制度
  -法令遵守、地域・業界の文化、慣習、規制への配慮
  -攻撃性への事前審査、情報収集の指針準拠など
・運用に関する基準
・ユーザサポートに関する基準
・開発サポート、開発元への啓蒙・教育に関する基準



1.マーケットの運用TF　～今後～

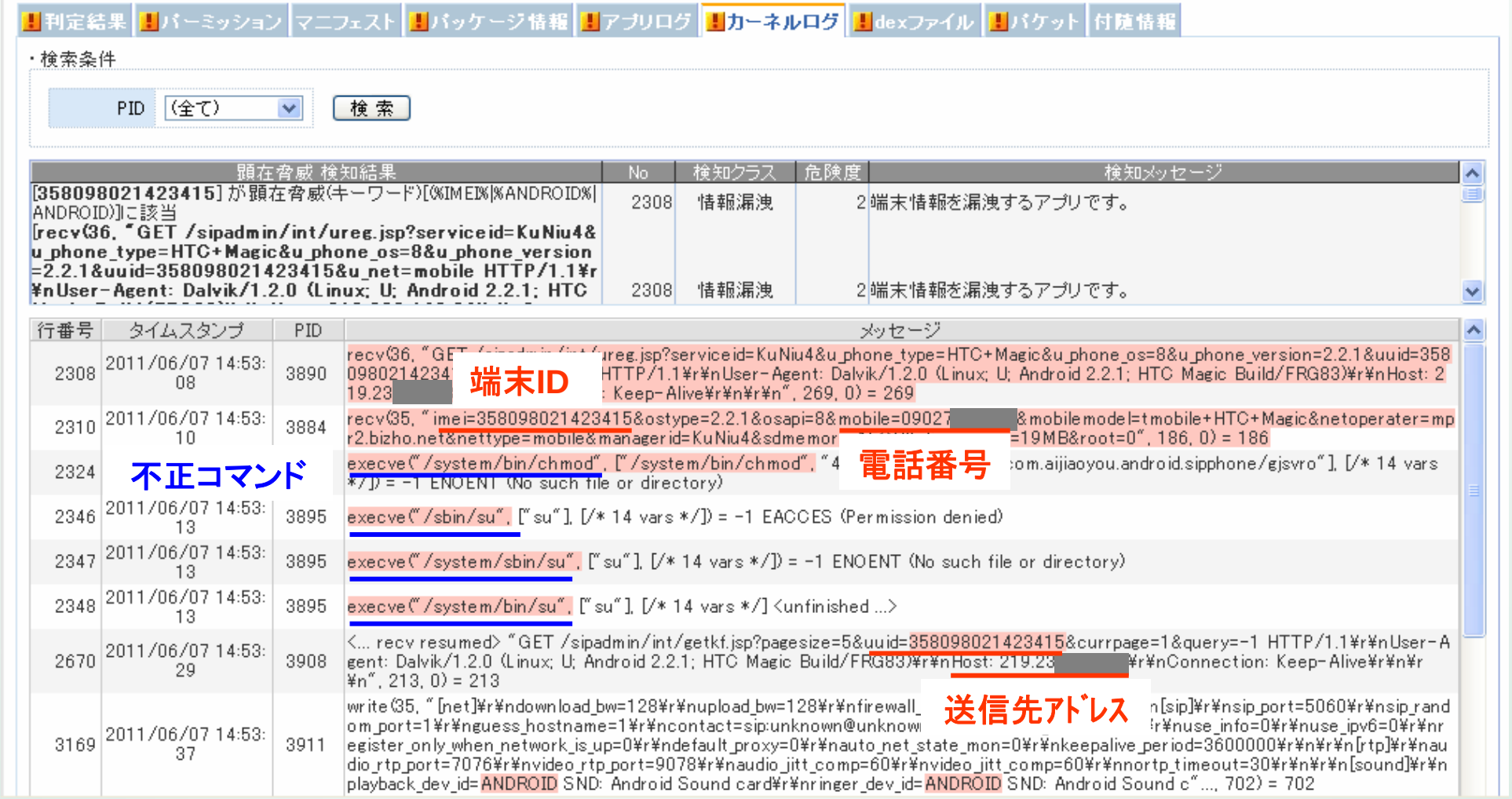
- 2011年12月
  - マーケット認定基準β版リリース
  - 関係者・有識者よりコメント聴取
- 2012年1月 ～
  - 認定制度運用準備
  - フィードバックを元にレビュー
- 2012年2月
  - マーケット認定基準をITU-Tへ提起
- 2012年?～
  - マーケット認定基準正式版リリース
  - JSSECマーケット認定制度運用開始



「提供元不明のアプリ」とあっても
しっかり運営のマーケットはあるんです！

2.アプリの攻撃性検査TF ～Androidのみ～

マルェアを実行したときの挙動ログ：情報漏洩＋不正コマンド実行



2.アプリの攻撃性検査TF ～Androidのみ～

- パーミッション機構

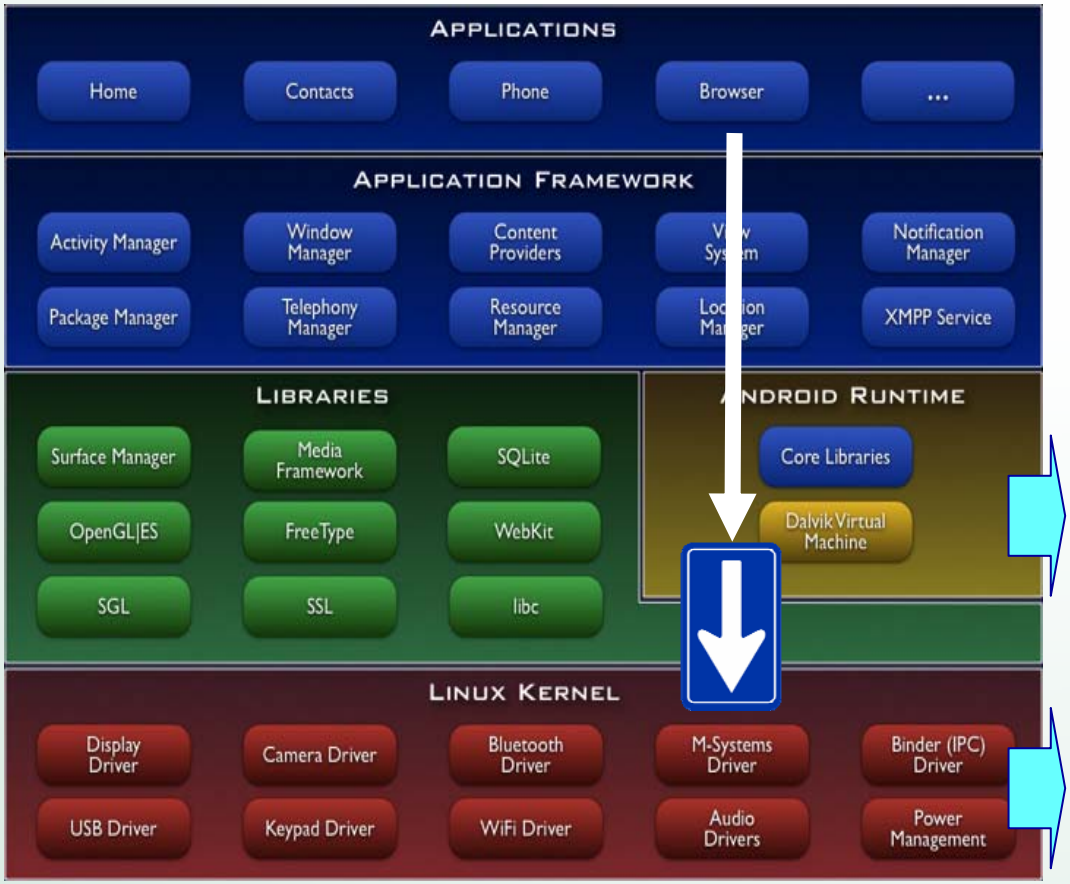
  Android™OSから、アプリが利用する機能や情報を表示して、ユーザ承認を求める。

  ⇒ 機能や情報を利用する目的が記されていない。総合的な作用の推測は難しい。

  ⇒ 脆弱性を突いて管理者権限を奪うアプリの場合、パーミッションを必要としない。

2.アプリの攻撃性検査TF　～Androidのみ～

- Linux OS + パーミッション可変型のサンドボックス
  ⇒ 安全性と利便性のトレードオフをユーザに委託。
- 端末実装、Linux層、Android層の脆弱性が混在し、サンドボックスが崩れる。



・ユーザがマルウェアを見抜くことは困難
⇒ 投稿アプリに対する事前審査が必要

◆ マルウェア（A）**パーミッション悪用型**
原因：機能や情報へのアクセスAPIが豊富

◆ マルウェア（B）**脆弱性攻撃型**
原因：端末実装、Linux層、Android層の脆弱性

2.アプリの攻撃性検査TF　～Androidのみ～

・パーミッション悪用型
　⇒ 情報漏洩、不正課金、踏み台（なりすまし、ボット）
・脆弱性攻撃型
　⇒ 情報漏洩、踏み台（なりすまし, ボット）、管理者権限（奪取, 利用, 改造）

攻撃性検査のチェックポイント

	潜在脅威	顕在脅威
解析対象の一例	パーミッション	システムログ、通信ログ、構成ファイル、コード
情報漏洩	未検出 検出　情報漏洩を引き起こす可能性があります。	未検出 検出　ユーザ承認なく個人情報を漏洩しています。
不正課金	未検出 検出　料金の発生するサービスを利用する可能性があります。	未検出 検出　ユーザ承認なく料金の発生するサービスを利用しています。
踏み台 （なりすまし、ボット等）	未検出 検出　外部から指令を受ける可能性があります。	未検出 検出　迷惑メールを送信します。
管理者権限 （奪取、利用、改造等）	未検出 検出　システム権限を利用する可能性があります。	未検出 検出　管理者権限を奪います。端末を改造します。

灰色文字は、安全性評価レポートのコメント例です。

3.情報収集モジュール対応TF

- 発端： Android OSのパーミッション・承認機構
  利用する機能や情報の通知のみ。ユーザ説明を十分果たしきれていない。

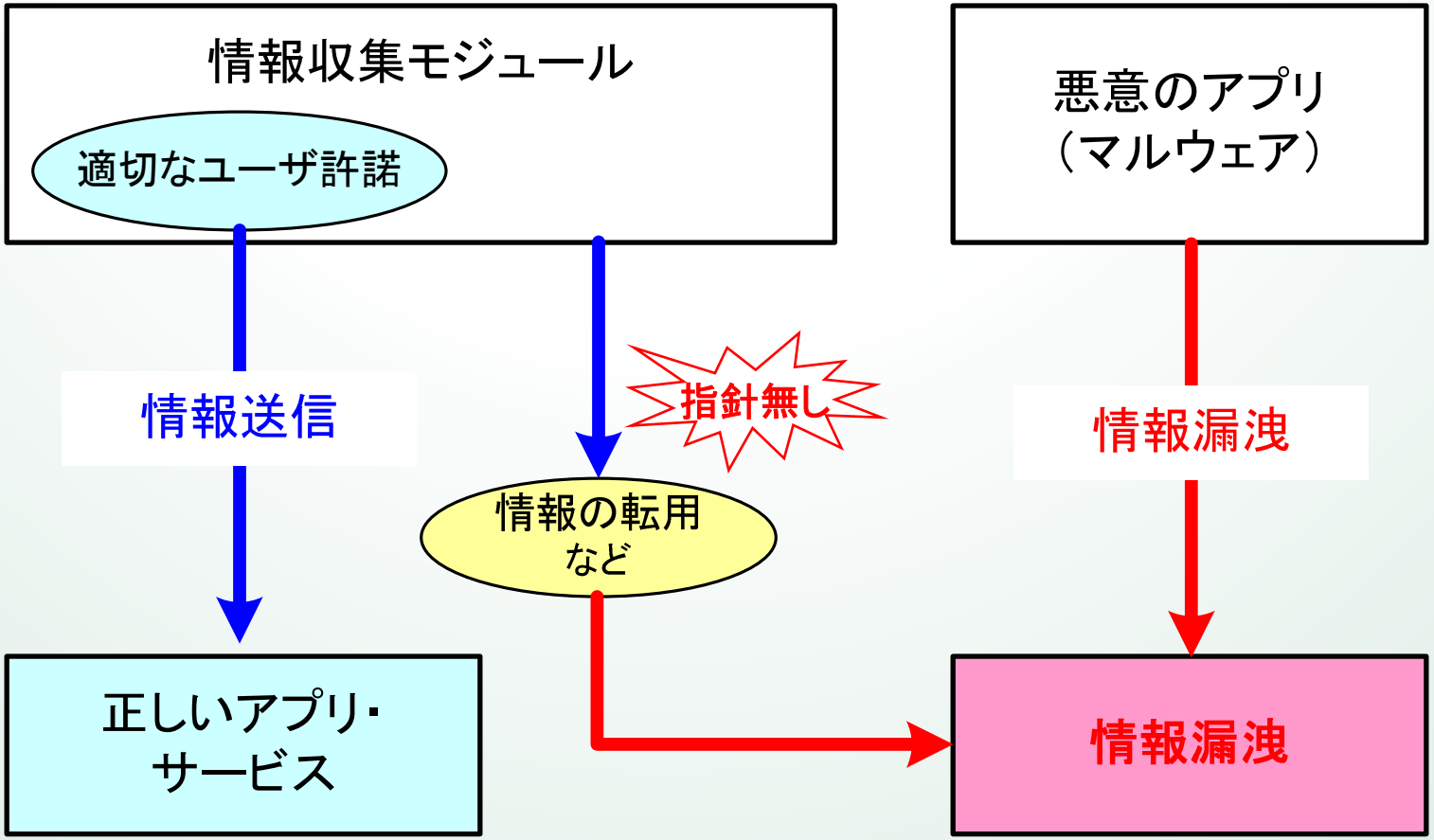
- 問題(1)
  情報収集モジュール提供者が、アプリ開発者に特性を説明していないケースがある。

- 問題(2)
  アプリ開発者が、情報収集モジュールに関する特性を理解しないままアプリに組み込み、適切なユーザ許諾を得ていないケースがある。

- 今後（2012年12月）
  MCF（モバイルコンテンツフォーラム）、JIAA（インターネット広告推進協議会）のご支援の下、JSSECとしてスマートフォン向けアプリ開発者向への情報収集のあり方に関する指針β

3.情報収集モジュール対応TF

・アプリの画面上にターゲット広告を表示するために、個人情報（ID＋趣向）を収集
・見守り、ネットアルバムなどのサービス提供のために、個人情報（ID+位置など）を収集
⇒ スマートフォン向けの情報収集のあり方に関する指針がない！



3.情報収集モジュール対応TF

- PC・モバイルのマルウェア種類の総計（2011年1月～2011年10月観測）のべ1,300,000種類、約4,300種類／日の検体を観測。

- Androidのマルウェア種類の計（2011年1月～6月観測）のべ200種類、約1.1種類／日の検体を観測。

マルウェア出現数　PC : Android™フォン ＝ 4000 : 1

情報漏洩の主原因は、情報収集モジュールの誤用です。

マルェア対策ソフトの検知対象外

統計情報の提供元
株式会社カスペルスキー

3.情報収集モジュール対応TF

- ターゲット広告
  アプリ内の広告をユーザがクリックすることで、アプリ開発者に報酬が入る。
  ⇒ ID情報：　端末ID(IMEI)、電話番号などからユーザを識別
  ⇒ プライバシ情報：　場所に応じた広告を表示

- Android™OSのパーミッション機構が十分と言えない中、情報収集モジュールを組み込んだアプリ開発者が責任を持って、ユーザに対して収集する情報、利用目的や範囲などをアプリの中で承認を得るべき。

- 情報収集モジュールの含有実態
  Android Market™の14カテゴリ×70個＝980個の無料アプリを対象に含有する情報収集モジュールを調査。

	含有数	含有率
アプリ総計	558/980	56.9%
情報収集モジュール総計	1065/558	1.91個

某社の乗換案内アプリ

3.情報収集モジュール対応TF

・Android Marketから14カテゴリ×70件＝980個のアプリを収集・調査した。
注）下記は、KDDI研究所が挙動ログから抽出したものであり、抜けや誤りがある場合もある。
注）ユーザ許諾を適切に得ているアプリと、得ていないアプリが混在することに注意されたい。

情報収集モジュール一覧	外部送信される情報	対象アプリ 件数	980アプリ 利用比率
com/	AndroidId, 国名, 端末名	269	27.45%
com/ /ads	AndroidId, AndroidId(ハッシュ値), IMEI, 国名, 端末名	212	21.63%
com/	AndroidId, IMEI, 位置, 端末名	86	8.78%
com/ /apps/analytics	国名, 端末名	83	8.47%
com/	AndroidId(ハッシュ値), 国名	58	5.92%
com/	–	58	5.92%
com/ /android	IMEI, 国名, 端末名	44	4.49%
net/	–	40	4.08%
com/ id	–	39	3.98%
com/ l/sdk	AndroidId, IMEI, 国名, 端末名	38	3.88%
jp/co ker	AndroidId(ハッシュ値), 国名, 端末名	24	2.45%
com/ ndroid	電話番号, AndroidId, 端末名	23	2.35%
com/	AndroidId(ハッシュ値), 端末名	16	1.63%
com/ dk	AndroidId, 国名, 端末名	16	1.63%
com/	IMEI, 国名, 端末名	12	1.22%
com/	–	12	1.22%
com/ id/ads	AndroidId, 国名,端末名	10	1.02%
com/	AndroidId, 位置, 端末名	8	0.82%
com/ id/sdk	IMEI	7	0.71%
com/ android	電話番号, AndroidID	6	0.61%
com/	–	3	0.31%
com/	–	1	0.10%

3.情報収集モジュール対応TF

・個人情報収集に関するアプリ開発者への啓発
何の情報を、なぜ収集し、どの範囲まで、いつまで、利用するのかなど、明確にユーザ許諾を得て頂きたい。

表　ユーザ許諾が必要と考える情報の例

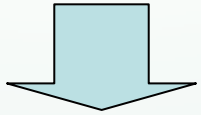
種別	IDの例
ID	Android ID、端末ID(IMEI)、SIM ID(IMSI)、SIMシリアルID、電話番号、Googleアカウント、AuthTokenなど
加工したID	上記IDのハッシュ値など
プライバシ	アドレス帳、位置情報、通話の内容・履歴、メールの内容・履歴、アプリ一覧、利用履歴、カレンダ、写真など

◆ スマートフォンにおける利用者許諾の基準が無い中で、下記が参考資料になる。
参考：JIAAの「行動ターゲティング広告ガイドライン」
http://www.jiaa.org/dbps_data/_material_/common/release/bta_guideline_release_100624.pdf

4.アプリの安全設計・セキュアコーディング

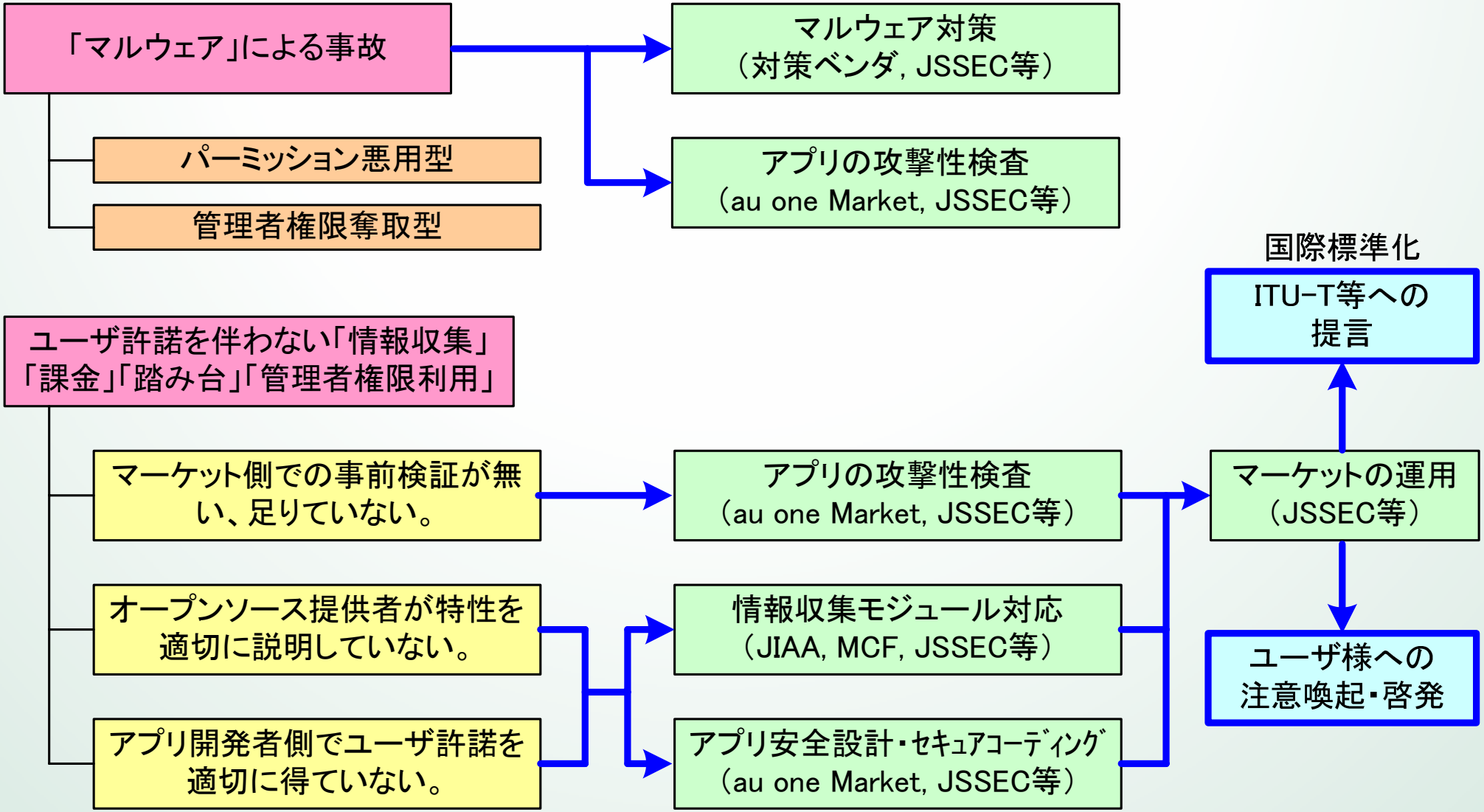
・ユーザ保護視点での安心・安全なアプリ開発の啓発が必要。
- アプリプラットフォームの遵守に関する啓発 など

・開発者視点での安心・安全なアプリ開発の情報が必要。
- オープンソース ソフトウェア ライセンスの考え方の浸透
- 不正コピー、認証処理に対する保護（難読化 など）
- セキュアコーディング



2011年11月頃からTFスタート

アプリWGのまとめ


「マルウェア」による事故
パーミッション悪用型
管理者権限奪取型
マルウェア対策
（対策ベンダ, JSSEC等）
アプリの攻撃性検査
（au one Market, JSSEC等）
国際標準化
ITU-T等への
提言
ユーザ許諾を伴わない「情報収集」
「課金」「踏み台」「管理者権限利用」
マーケット側での事前検証が無
い、足りていない。
オープンソース提供者が特性を
適切に説明していない。
アプリ開発者側でユーザ許諾を
適切に得ていない。
アプリの攻撃性検査
（au one Market, JSSEC等）
情報収集モジュール対応
（JIAA, MCF, JSSEC等）
アプリ安全設計・ｾｷｭｱｺｰﾃﾞｨﾝｸﾞ
（au one Market, JSSEC等）
マーケットの運用
（JSSEC等）
ユーザ様への
注意喚起・啓発