資料５

スマートフォンに関わる セキュリティと業界団体等の動向

一般社団法人モバイル・コンテンツ・フォーラム
理事　寺田眞治

2012,02,08

サマリー

ユーザー情報を活用することで、利用者と企業の双方が
膨大な情報の中から簡単・安価・便利に情報を整理・取捨選択できるようになる

安全・安心にできるようにするためには利用者と企業の信頼関係を構築すること

1. 実態、構造を正確に捉える
2. 課題を明確化し責任の所在を明らかにする
3. 関係者が連携して責任範囲の対策を確実に行う

ただし、ネットの世界は進化が早く新規参入者も多く構造変化も次々起こる
また、国境も無いため国内の対応だけでは足りない

1. モニタリング体制の構築
2. 国際協調の実現
3. 利用者のリテラシー向上

ユーザー情報活用の有益性

ユーザー情報を活用したサービスの概要

外部センサー
外部インターフェイス

センサーネットワーク
ライフレコーダー

端末内蔵センサー

カメラ
GPS
方位(地磁気)
加速度
照度

端末ユーザー
インターフェイス

キーボード
タッチパネル
マイク

ユーザー情報

ユーザーID
端末ID
RFID／FeliCa
端末設定
趣味・嗜好

アプリケーション
コンテンツデータ

スケジュール
アドレス帳
検索履歴
購買履歴
日記、フォトアルバム

Lifelogの収集

ユーザーのWants、Needs

マッチング
(フィルタリング／推測・・・)
↓
リコメンド
ターゲティング
：

情報／サービスの提供者

情報／サービスの提供

移動場所に合わせた店舗案内やクーポン配布
趣味に合わせた新商品、新譜発売などの案内
スケジュールに合わせた交通やイベントの案内
嗜好に合わせたサイトメニューの自動並べ替え
購買履歴から商品のお勧め
検索履歴、閲覧履歴から広告表示
健康状態に合わせたヘルスケア情報
：
：

配信系技術

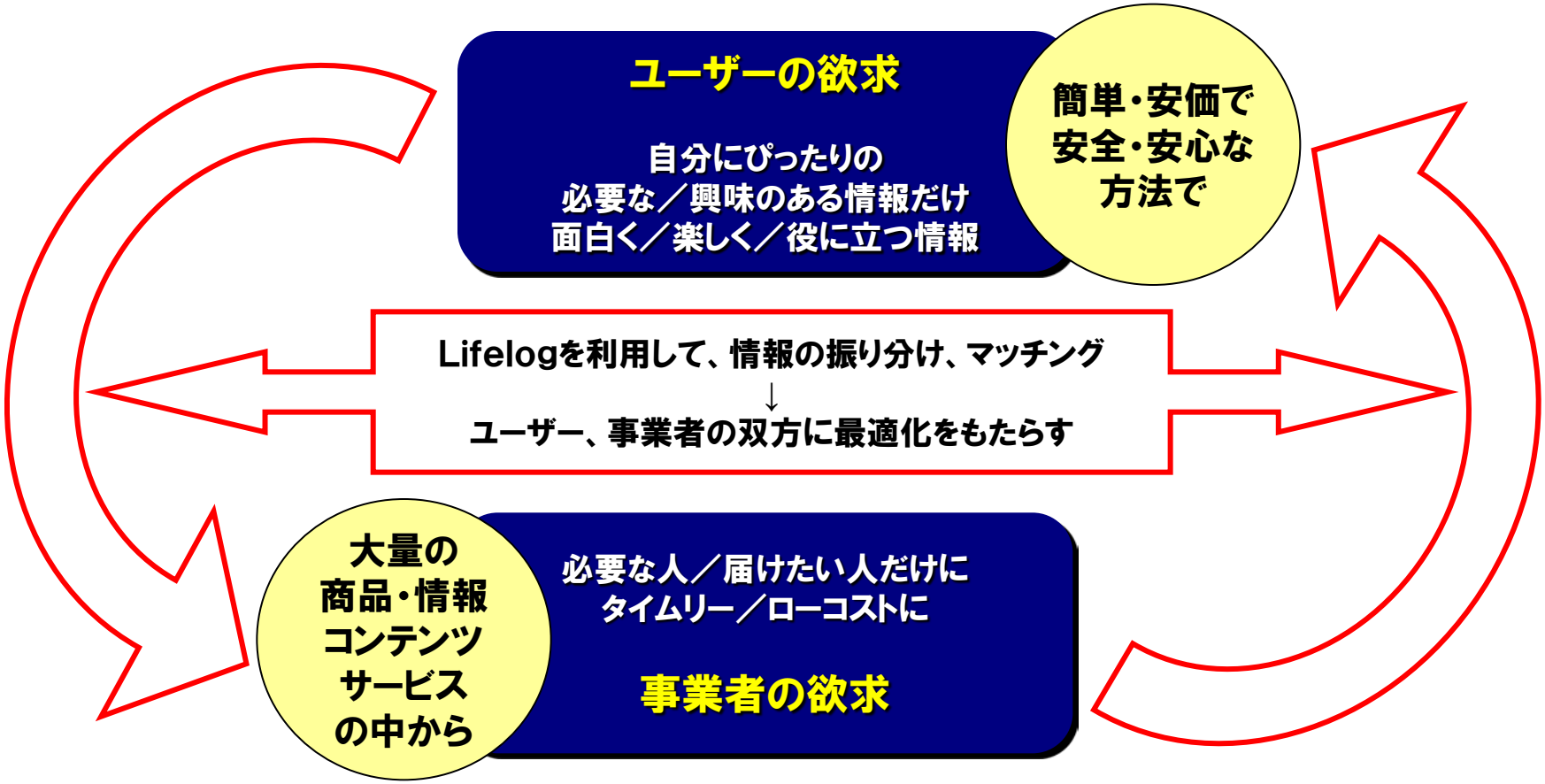
Push
マッシュアップ
クラウド

エージェント系技術

音声・画像認識
AI／感性エンジン
表現(Flash／3D)

ユーザー情報を活用したサービスのエコシステム

背景 ： ICTの進化・普及による情報の爆発的な増大と流通



ユーザーには利便性と楽しさ
事業者にはROIの最大化 ⇒ Win－Winの好循環

スマートフォンにおけるユーザー情報取得の課題

混乱する議論、錯綜する主張

個人情報、プライバシー情報は、取得が禁じられているのではなく、
取得、保存、利用などについての取り扱いが問題となる

1. 情報の取得方法や、それにともなって取得可能な情報の如何を問わずに、「ネット上の情報取得問題」とひと括りとしてしまうことによる混乱

ex. WEBブラウザーにおけるCookieによる限られたメディア内のユーザーのネット上の行動情報取得と、アプリによる端末内のユーザー情報取得は別物であるにも関わらず、全てオプトインとする議論が行われている。

2. 情報取得を可能とするシステムの構築者と、情報取得の主体者およびその情報の利用者が、同一か異なるかを考慮に入れないことによる混乱

ex. データの取得者より、データの利用者（広告主）や仲介者（広告事業者）、あるいは過去のイメージから通信事業者に責任が過度にかかっている

3. 個人情報、プライバシー情報、あるいは統計情報が混同されることによる混乱

ex. 情報の取得方法や利用方法やユーザーの意思に関係なく、情報そのものの扱いの可否が議論されている。

4. 海外プラットフォーマーの増加に伴い、国内企業と海外企業への対応についての混乱

ex. 海外での規制や活用の実態について誤った認識の下に、国内企業が誤った方法を使ったり、逆に国内企業が誤った評価をされている（米国では一般的だ or 規制されているといった表面的な認識）

実態、構造、BIZモデル等の見える化が必要
各国の実態、規制状況の把握が必要

ユーザー情報の取得方法

PCでもスマートフォン（スマートデバイス）でも基本的に同じ

1. インフラ系のネットワークプラットフォーム

1. 通信事業者が提供するIDや各種情報の取得
   ex. 各種ID、アクセスポイントの情報やそれに紐づく情報等
2. 認証決済関係プラットフォーマーが提供する情報の取得
   ex. ユーザーIDと利用データ、OpenID、SocialID、Edy ナンバー、Suicaナンバー、FeliCaナンバー等
3. トラフィックデータの取得
   ex. 通信ログ、DPIによる情報取得

2. メディア系のネットワークプラットフォーム

メディア、CP等のプラットフォームが提供する情報の取得
①SocialAPI、SocialGraph等による情報の取得
②ECサイトのプラットフォームが提供する情報の取得
ex. 購買履歴、商品DB、ポイント等のAPI等

3. アプリケーションプラットフォーム（OS、JAVA、Flash等）

1. アプリケーションによる情報の取得
   ①端末内に記録されている情報
   ②端末のデバイスを利用して取得する情報
   ③端末による通信の履歴や内容
   ④端末の通信機能を利用した他の端末やサーバの情報
   ⑤他のアプリケーションの情報や実行内容
2. アプリケーションの機能を活用する情報の取得
   ex. ブラウザーのCookie・・・メディアがユーザー識別のために発行した識別子を利用
3. 機能を強化する追加アプリ等による情報の取得
   ex. Toolbar、WEBヘルパー・・・機能強化が主な目的だがブラウザーのアクセス内容等を取得するものもある

4. 外部からネットワークを通じての明示的な情報取得

1. 会員登録型サイト、懸賞サイト、アンケートサイト等によるユーザー情報収集
2. メール、IM等によるアンケート等のユーザー情報取得

5. 外部からネットワークを通じての明示的でない情報取得

1. フィッシングサイト
2. OS、ミドルウェアやアプリの脆弱性をついたサイト
3. 無差別メールによるメアド収集
4. ウィルス添付メール

6. 外部からネットワークを通じてのサーバーからの情報取得

サイトクローリング、SocialGraphを利用したクローリング等

7. ネットワークを通じての製品やソフトウェアのフィードバック

OS，端末、デバイス自身
ex. 製品登録、バージョンアップ、不具合修正のための情報取得

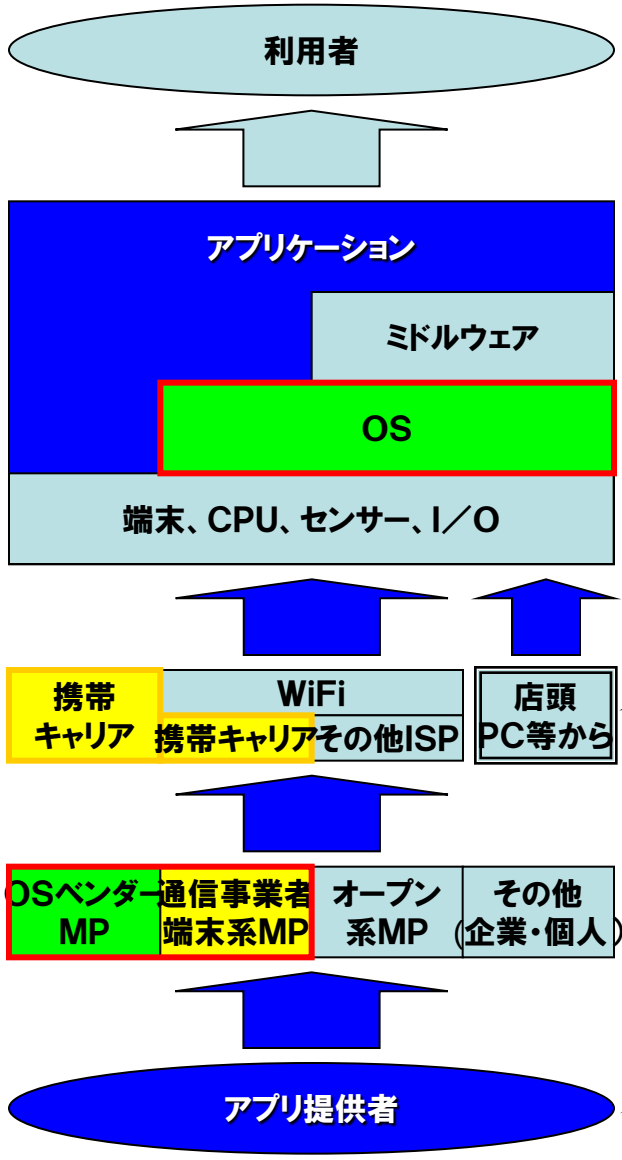
8. デバイス間通信による情報取得

PAN（Bluetooth、IrDA、ZigBee等）
非接触ICカード（NFC、FeliCa等）
USB

9. その他

端末購入時、回線契約時、製品登録カード等

アプリケーションの流通の構造



現在、スマートフォンにおけるアプリケーションの流通は、オンラインではiOS、Windows PhoneはOSベンダーのマーケットプレイスに限られるが、Androidでは、ほぼPCと同じで極めて多様。

プリインストール・アプリケーション
（端末購入時にあらかじめ組み込まれているアプリ）
- ・ハードウェア系（端末メーカー、デバイス・ベンダー等）
- ・ソフトウェア系（OSベンダー、ミドルウェア・ベンダー等）

アプリを端末にデータとして送り込む主な方法
- ・事業者無線系（キャリア、WiFi事業者）
- ・自営無線系（自宅のWiFi／ISP経由）
- ・その他店頭でのインストールやPCからのインストール

iOS、Windows Phoneのアプリはベンダーのマーケットのみ
Andoroidは
- ・Android Market（OSベンダー）
- ・通信事業者、端末ベンダー等の独自マーケット
- ・勝手マーケット
- ・その他企業や個人のダウンロードサイト

開発会社や開発者（個人やチーム）だけでなく、開発を他に依頼している場合やアグリゲーターなどの仲介者がいる場合もある。

アプリケーションの流通過程での課題

OSベンダーや携帯キャリアでの対策には限界がある

＜OSベンダー＞

OSの機能の利用についてOSベンダーで規制するためには、アプリケーションがマーケットプレイスに提出されなければならない。

Androidでは、キャリアや端末ベンダーによるマーケットプレイス、いわゆる勝手マーケットプレイスや企業や個人でのアプリケーション配布が可能。

またOSベンダーは国内事業者ではないため、日本の国内事情の反映に限界がある。

各国でプライバシー情報の取り扱いについては法制度や規制が異なり、また、OSベンダーによってアプリケーションの審査方法や基準が異なり、一律で対応してもらうことは困難。

＜携帯キャリア＞

アプリケーションへの関与度は低く、できることは限定的。

アプリケーションのマーケットプレイスは他にも存在するだけでなく、WiFiでの接続ではキャリアの通信網を経由しない場合も多いため、キャリアによるアプリケーションへの関与は少ない。

キャリアへの責任押し付けは垂直型ガラパゴス化の再現。

キャリアがアプリケーションに責任を持つためには、アプリケーションの一元管理が必要となり、端末とネットワークのキャリア管理が前提となるため、SIMロックの復活（端末とネットワークの一体化）、WiFiネットワークの指定（自由なWiFi事業者の選択や家庭内におけるWiFiを通じた自由なISPの選択を阻害）等、様々なレイヤーの自由競争に悪影響を及ぼす。

アプリケーションの開発・配布元での課題

**問題のあるアプリケーションの第一の責任は、開発者や配布者にあることは論を待たないが
アプリケーションの配布元や開発者への対策には限界がある**

＜アプリケーションの開発、配布元＞

アプリケーションの開発者や配布元はあまりにも多様であるため、全てを網羅することは不可能であり、特に海外のベンダーに日本の仕様を守らせることは現実的ではない。

1. プリインストールタイプ（ネットワークからの配布含む）
   デバイスベンダー／端末ベンダー／OSベンダー／ミドルウェアベンダー／キャリア／端末販売者
2. インストールタイプ
   企業、アプリケーションプロバイダーからサンデーエンジニアや学生まで
3. 特定国向けではなく全世界に同時に広がる流通システム

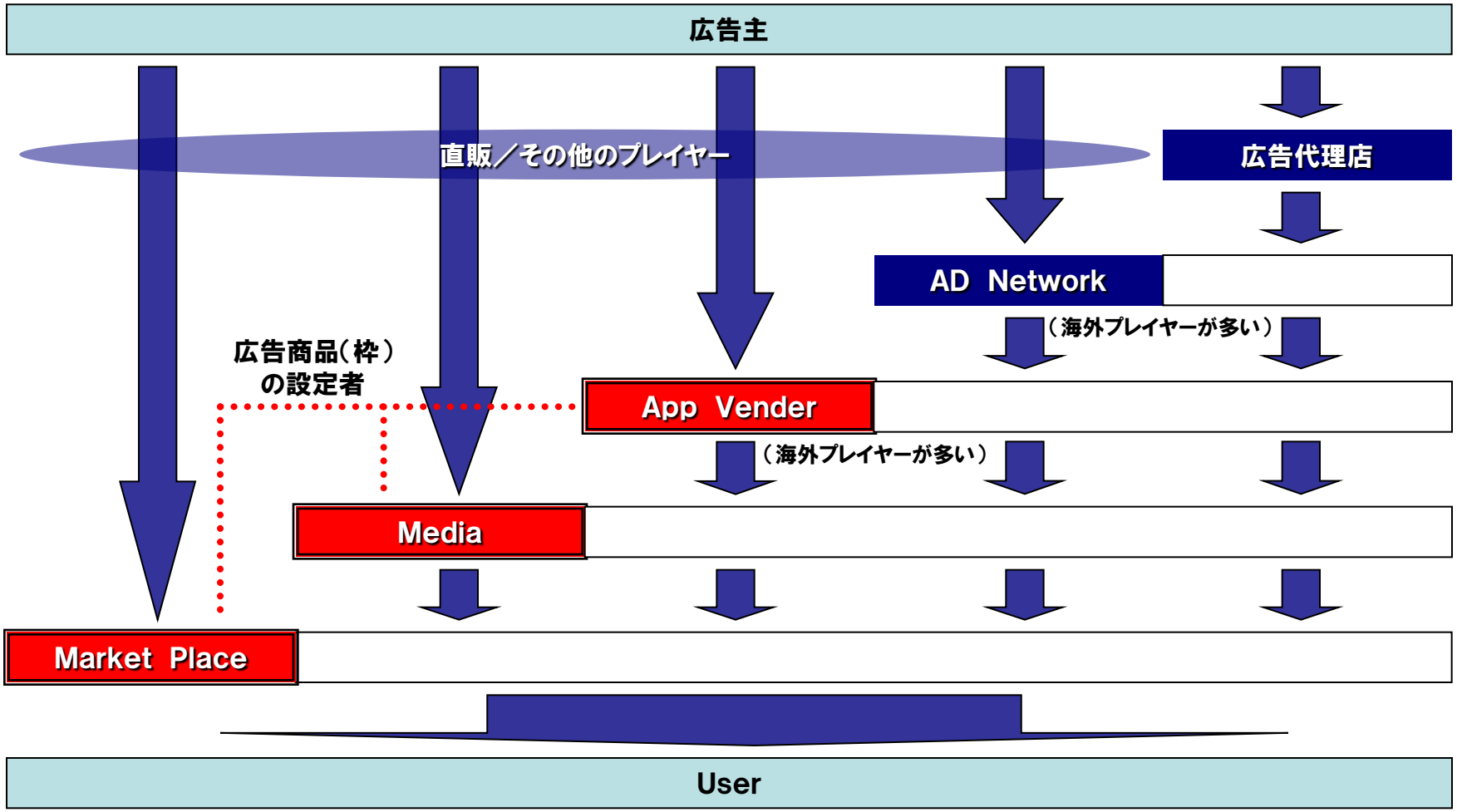
＜モジュール組み込みアプリケーションの課題＞

開発者以外の第三者が配布する、いわゆる情報収集モジュールを組み込んだアプリケーションが存在する

1. アプリケーションに広告を配信するAdnetworkを実装するためのものが大多数（米国のシェアが大）
   これを組み込む場合には、各Adnetworkはアプリケーションベンダーに対して利用者への表示や参照元Linkについて掲載するよう要請しているが、英語での説明であるため日本のアプリケーションベンダーは遵守していない場合が多い
2. 部品として流通しているものもあるが仕様を十分に理解していない場合も少なくない

スマートフォンアプリの広告に関する構造

広告枠、広告手法の多様化と広告型ビジネスを展開するプレイヤーの増加に伴い
広告代理店が広告主側を統括する従来モデルが崩れており
広告事業の規範化が難しくなっている



関係者の責任

アプリケーションの開発・配布元	配慮原則やガイドラインの遵守 ※特にパーミッション等の取り方に留意
アプリケーションの配布者 （ダウンロードサイト、インストール者等）	1．配慮原則やガイドラインに則した審査 ※スクリーニング、審査の透明性 2．アプリケーションの開発者、配布元が配慮原則やガイドラインに則した対応を可能とする仕組みの提供 ※アプリ紹介やDL時等での表示
OS、ミドルウェアベンダー	アプリケーションの開発者、配布元が配慮原則やガイドラインに則した対応を可能とする仕組みの提供 ※API利用の説明詳細化や容易化 ※パーミッション等の取得方法の改善
ユーザー情報収集モジュールの提供者	配慮原則やガイドラインの遵守 ※モジュールを利用する者へのユーザー説明の徹底化 ※特にパーミッション等の取り方に留意
ユーザー情報の提供を受ける事業者	提供元への指導、確認
端末販売者 （端末ベンダー、キャリア含む）	1．正当なアプリケーション以外を検知、排除できる仕組みの提供 ※セキュリティアプリの普及 2．利用者への説明
利用者（ユーザー）	正しい知識と対応の習得

全体で検討すべき事項

●パーミッション等の取り方についてガイドライン（基準や例示）必要？

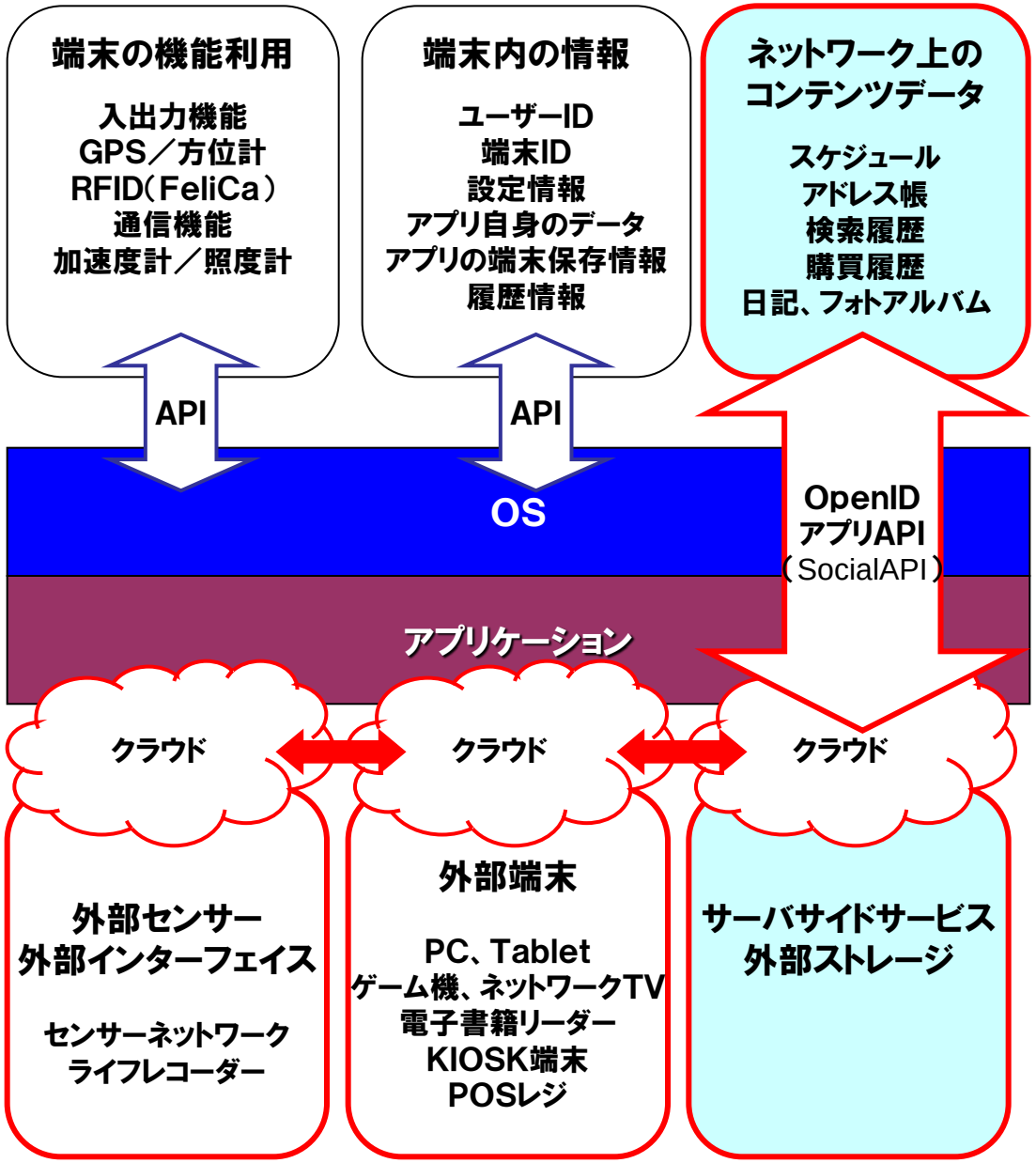
●レイヤーの異なる事業者や官庁、海外事業者も含めた関係者間の調整を円滑に進める仕組みができないか？

●進化スピードが速く、国内外含めて新たな参入者が急増することを考えると何らかのモニタリングの仕組みが必要ではないか。

●正しくやっている者を守り、不良な事業者を排除する環境を整備するためにはエンフォースメントについても検討する必要があるのでは？

●制度面では国や国際機関レベル、自主規制では海外の業界団体レベルで整合性を取るために、国際協調の仕組みが作れないか。
※今後、セキュリティ意識の低い新興国からのアプリ流入も増えるため、欧米だけでなく新興国との関係作りも重要

スマートフォンに依存しない情報取得と流通



端末やOS、ネットワークに依存しない プライバシー情報の取得・流通

OSやミドルウェアのAPI等を利用するのではなく、サーバサイドのAPI等を利用するもの
- ※SNSのアプリケーション
- ※ストレージサービスを利用するアプリケーション

サーバ同士でAPI等を通じてユーザー情報が流通するもの
- ※パブリッククラウドのサービス

この場合のアプリの多くは単なるデータビューアー(ブラウザ)でしかない。
また、プライバシー情報の多くはユーザー自身が提供したものである。

スマートフォンのセキュリティという枠では検討が難しい。

今、何をすべきか？

個別の課題 ： 個々の課題の抽出 → 責任の明確化 → 個別の対策の実現

同時進行

構造的課題 ： 全体構造のシンプル化 → 関係者横串での情報共有 → 共通対策

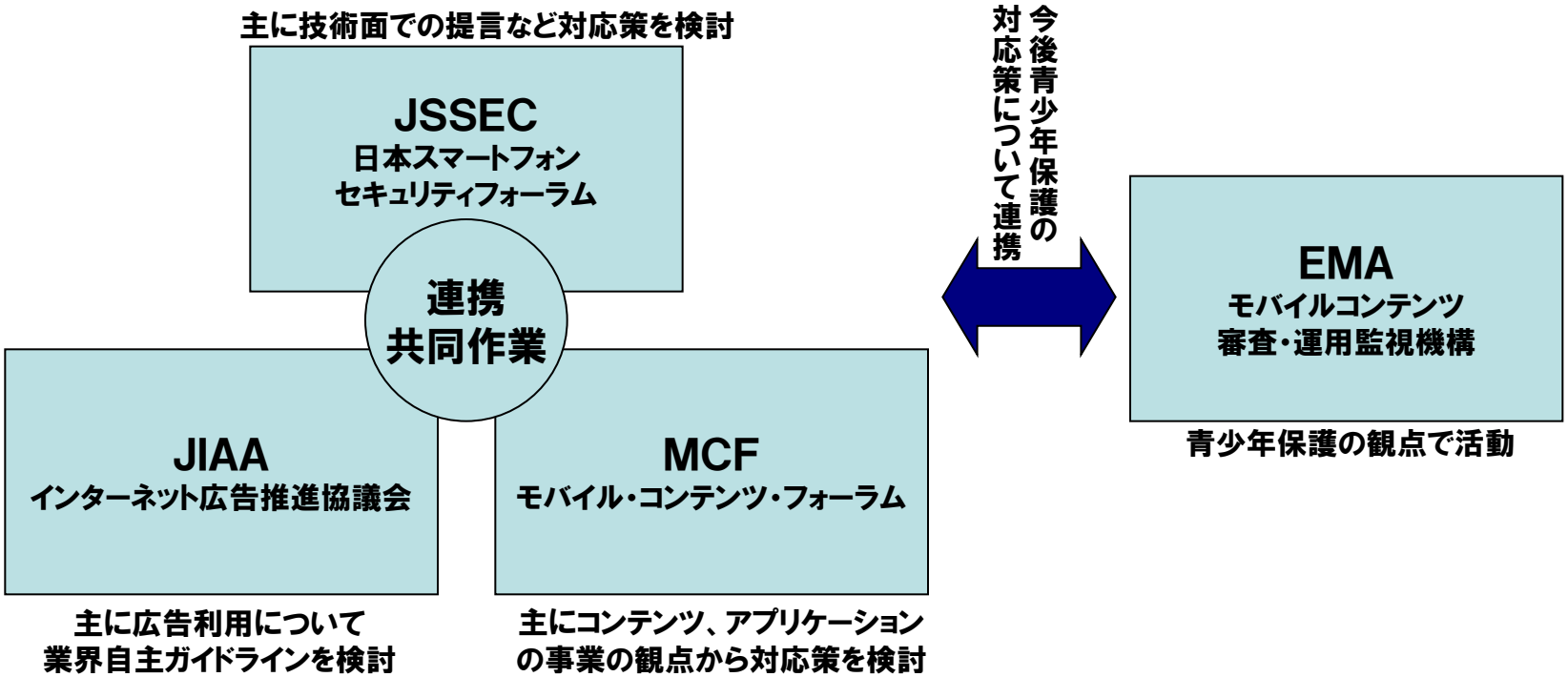
議論が迷走しないために、また議論が一部の利害関係者内で閉じてしまわないために
広く関係者間での議論と情報の公開が重要

加速度的に新たな問題が頻発する虞があるため、
問題を察知し即応できるモニタリングの仕組みを構築する必要性

孤立しないための国際協調を念頭に置いた海外との連携システムの構築も重要

連携して対応する業界の動向

関連する業界団体が連携・共同で春頃を目処に対応を検討中



提言・ガイドライン等の策定を通じて、自主規制、啓発・教育の実施

※各団体は、社会全体のバランスや国際協調等に留意するため
国内外のそれぞれの関連業界団体やクラウド関連の団体等とも情報交換を進めている

Privacy by Design

ライフログを活用したサービス、ビジネスを行うにあたって念頭に置くべき新たな概念

- アン・カブキアン(Ann Cavoukian)博士：オンタリオ州の情報・プライバシー・コミッショナー
- 様々な技術に関する設計仕様の中に、プライバシーを組み込むという考え方。
- 適用分野：(1)技術、(2)事業活動、(3)物理的設計
  1 プライバシーの利益を承認し、懸念は事前に対処しなければならない。
  2 プライバシー保護に関して普遍的な立場で表現されている基本的な諸原則を適用すること。
  3 情報技術及びシステムを開発する際に、情報のライフサイクル全体を通じて、プライバシーの懸念を早期に緩和すること。
  4 有能なプライバシーの指導者及び/又は専門家の助言を求めること。
  5 プライバシー促進技術(privacy-enhancing technologies, PETs)を採用し、統合すること。

日本ではほとんど知られていない

**事業者とユーザーの両方にとって不利益で不毛な追いかけっこ状態に陥る前に、
あらゆる場面に適応しうる「Privacy by Design」のような基本的な考え方を関係者に啓発・普及し、
事前にトラブルの芽を摘むことを意識する環境（風土）を作り出すことが重要**