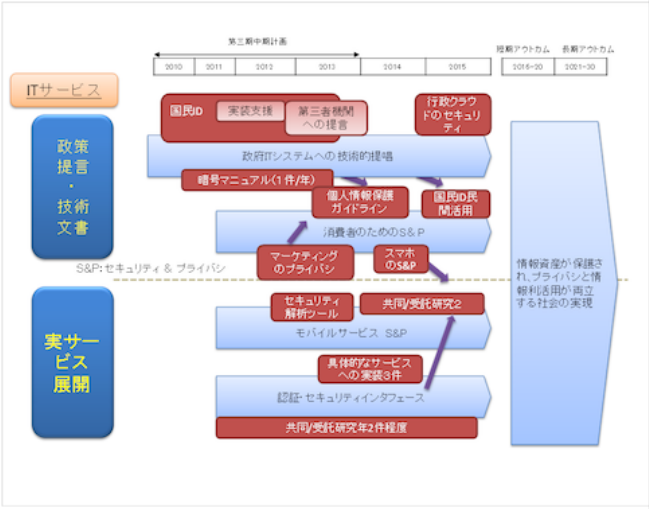
産業技術総合研究所セキュアシステム研究部門
第1回 セキュアシステムシンポジウム
2012年9月10日

スマホアプリのプライバシー問題の解決に向けて

セキュアサービス研究グループ
高木 浩光

セキュアサービス研究Gでは

- 技術開発研究の他
- 技術的知見に基づくセキュリティ分野の提言
  - スマートフォンのプライバシー保護
  - 社会保障と税の番号制度
  - 個人情報保護ガイドライン
  - 暗号マニュアル
    - ほか

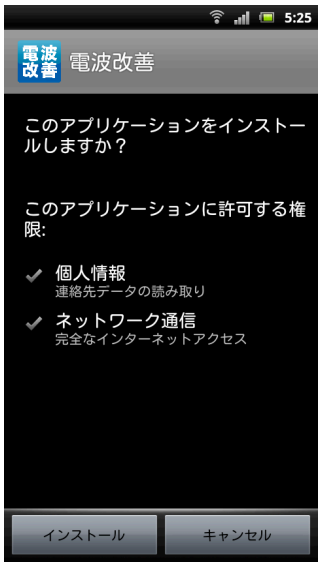


背景

- 昨年スマートフォン（スマホ）アプリが急速に普及
  - 不審なアプリが続々出回る
- 不審なアプリの例
  - 電話帳を盗むアプリ（悪意あるケース）
    - 不正指令電磁的記録の罪（刑法168条の2、3）に該当し得るものも
  - 正当な事業者が電話帳を無断でアップロードするアプリ
  - 位置情報や端末IDを無断で広告等に使うアプリ
- 総務省 利用者視点ICT諸問題研究会
  - 3月のWGのヒアリングにおいて意見陳述
  - 8月提言「スマートフォン・プライバシー・イニシアティブ」
  - 実効性のある施策の実現が課題

悪意あるアプリの事例

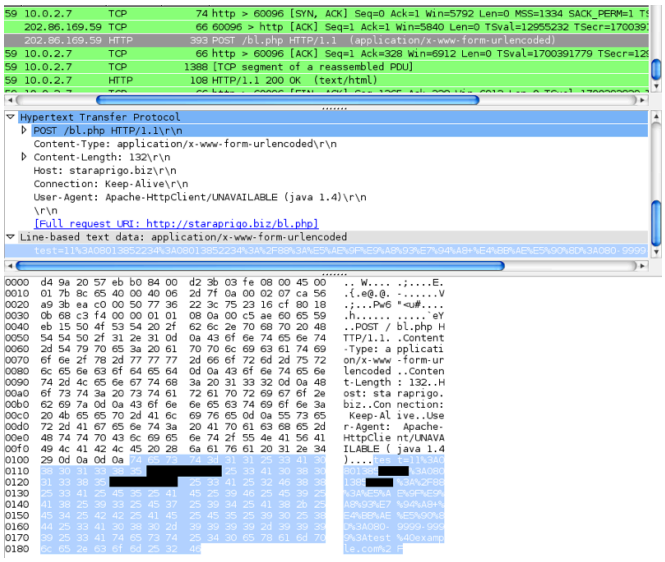
- spamメールとして受信したもの
  - 「電波改善」（2012年8月）
    - 電話帳が盗み取られる



悪意あるアプリの事例

悪意あるアプリの事例

- このときの通信内容：電話帳を盗まれている



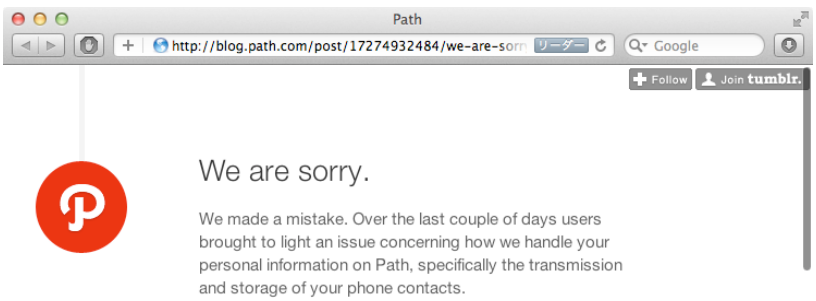
- test=11:0801385[redacted]:0801385[redacted]:/88:実験用 仮名:080-9999-9999:test@example.com/

悪意あるアプリの問題解決

- 報道例
  - 「スマホアプリで情報流出か 数百万人分 自動的に外部送信」
    読売新聞2012年4月14日朝刊
    - 「問題となっているのは、人気ゲームなどを動画で紹介するアンドロイド用の無料アプリ。タイトルは、実在するゲーム名などに「the Movie」とつけられ、少なくとも16種類が確認された。」
  - 「アプリ作成者特定へ スマホ情報流出 警視庁が調査」
    読売新聞2012年4月14日夕刊
    - 「スマートフォン（略）の電話帳に登録された個人情報を外部に送信してしまうアプリが出回っていた問題で、警視庁が情報収集を始めたことが、捜査関係者への取材でわかった。同庁は（略）刑法のウイルス作成罪にあたるかどうかを慎重に検討する。」
- IPAでは
  - 「コンピュータウイルス・不正アクセスの届出状況」で事例公表

正当な事業者による場合

- 報道例：米国「Path」の例
  - iPhoneの連絡先データ無断収集のPathが謝罪 アプリをアップデート, ITmediaニュース, 2012年2月9日
    - 「米Pathのデイブ・モリンCEOが2月8日（現地時間）、ソーシャルメディアサービスPathのiPhoneアプリでユーザーに無断で連絡先データを収集していたことを謝罪した。」
  - We are sorry. - Path, 2012年2月8日



- 日本にも類似の例あり

適切な例

- facebookアプリ「友達を検索」機能での電話帳の利用

なぜ今これが問題か

- ウェブからスマホアプリへ
  - ウェブ
    - セキュリティ制約による厳しい機能制限
      - どのサイトを不意に訪れても問題が生じないよう機能を制限
      - 収集できるのは利用者が自発的に入力した情報に限られる（同意確認不要）
      - 端末ID的な機能（super cookie）は徹底排除されている
      - 位置情報の使用はサイト単位でオプトイン方式（ブラウザ機能2009年～）
    - 少数のブラウザベンダにより事実上の標準が確立していた
      - 結果としてコンテンツプロバイダはその上で可能なことは何でも無断でやってよい
    - しかし利便性に限界
  - スマホアプリ
    - 中間的な緩さの機能制限
      - 一般のPCのプログラムのようには自由でない（マルウェア蔓延の防止）
        - 例：他のアプリのデータを参照することはできないが、アドレス帳は読める等
      - 「iアプリ」よりは制限が緩い
        - 例：任意のサイトと通信できる、同意確認なしにアドレス帳を読める等
    - 個々のアプリ提供者の裁量 → 新しい問題が発生

総務省研究会WG

- 「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」
  - 2010年 第二次提言
    - 「ライフログ活用サービスに関する検討について」
      - Webの行動ターゲティング広告について、業界に自主的ガイドラインの取組みを促す
        - このときは、オプトアウト手段の提供でよしとするものだった
  - 2012年 スマートフォン・プライバシー・イニシアティブ
    - 「スマートフォンを経由した利用者情報の取扱いに関するWG」
    - 2012年1月～8月
    - 8月に最終取りまとめを公表
      - 副題「利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション」

WGでの意見陳述

- 背景
  - 一部事業者の主張として
    - オプトアウト方式でかまわないとする主張
    - Permission機構による同意をとっているとする主張
- 我々の主張
  - オプトアウト方式で受容できるのは限定的なケース
    - Webのアドネットワークの特殊性に依拠
  - Permission機構では同意にならない
  - 取得する情報によってはオプトイン方式をとるべき
  - オプトイン方式にもいろいろある
    - 包括的選択と、個別的選択など

Permission機構は有効な同意？

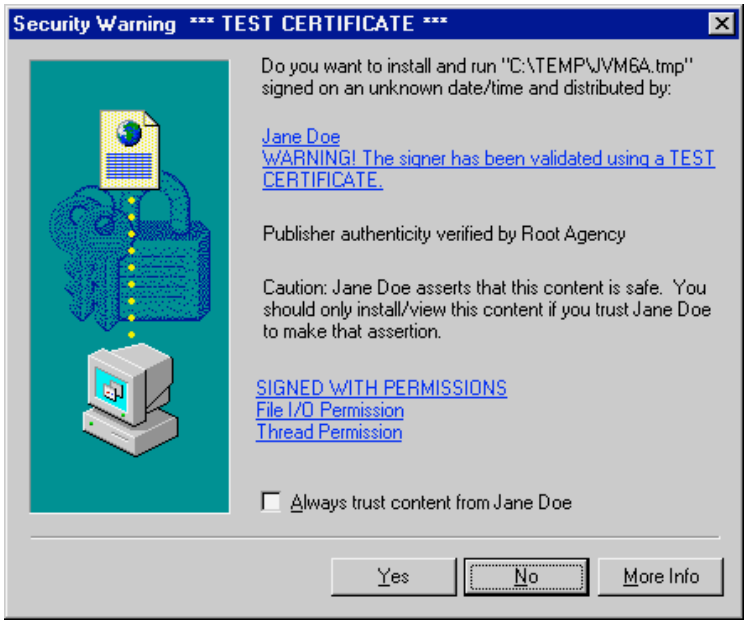
- Androidの場合
  - 「同意してダウンロード」とのボタン
    - これをもって利用者の有効な同意があると言えるか / 何への同意か

Permission確認方式の限界

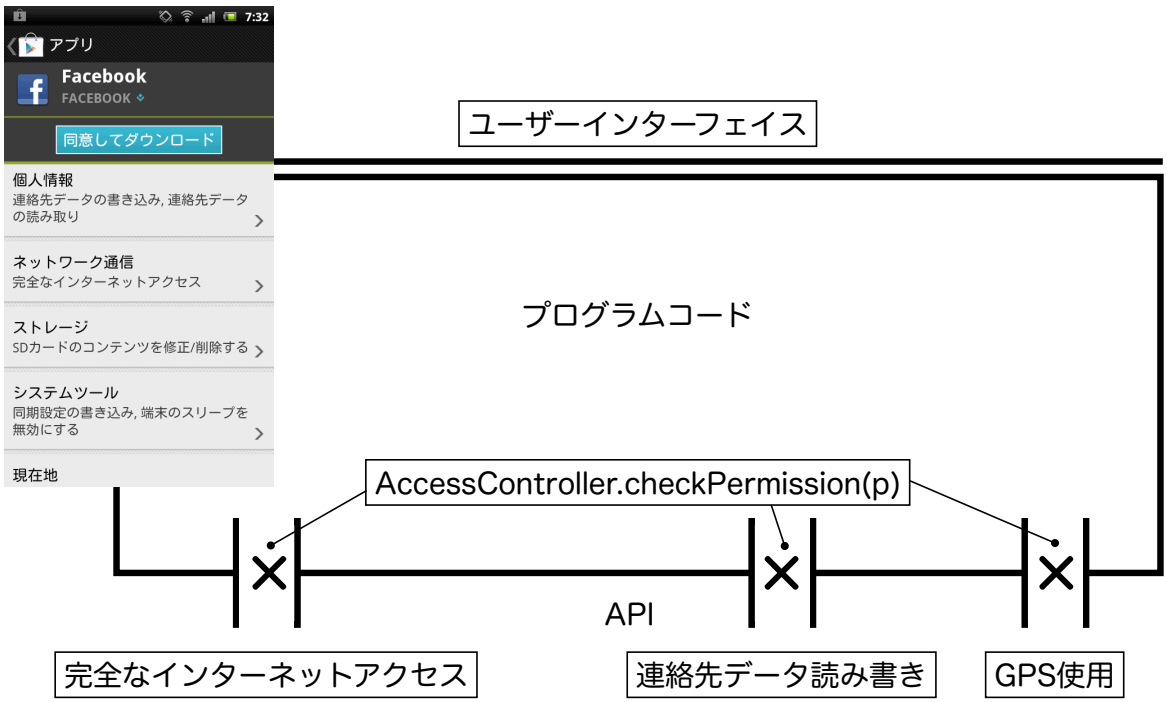
- PermissionはJavaの基本機能（J2SE 1.2 1998年〜）
  - ウェブ用Appletでpermissionを利用者が確認するという方式が採用されることはなかった
    - WindowsのActiveXコントロールで一時期近い方式はあったが廃止になった（利用者に見せても判断できずナンセンス）
  - Androidがそれを採用
- 説明がわかりにくい？（そういう問題ではない）
- 使用と送信の許可が独立
  - 例：位置情報を使用することと、何かを外部に送信することは別々のpermissionで制御される
  - 「送信しない使用」と「送信する使用」を区別できない
    - これを区別して許可するpermissionモデルは技術的に実現不可能
  - 各情報の送信に同意したことにはならない

過去の例

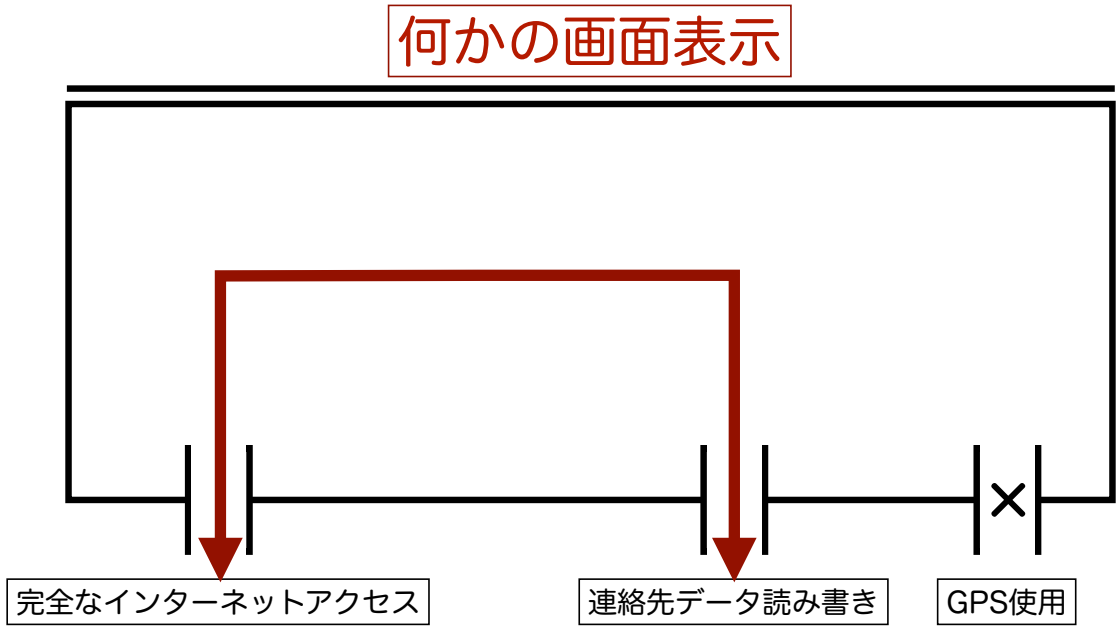
- ActiveXによるPermissionの確認（2000年）
  - Visual J++ によるもの



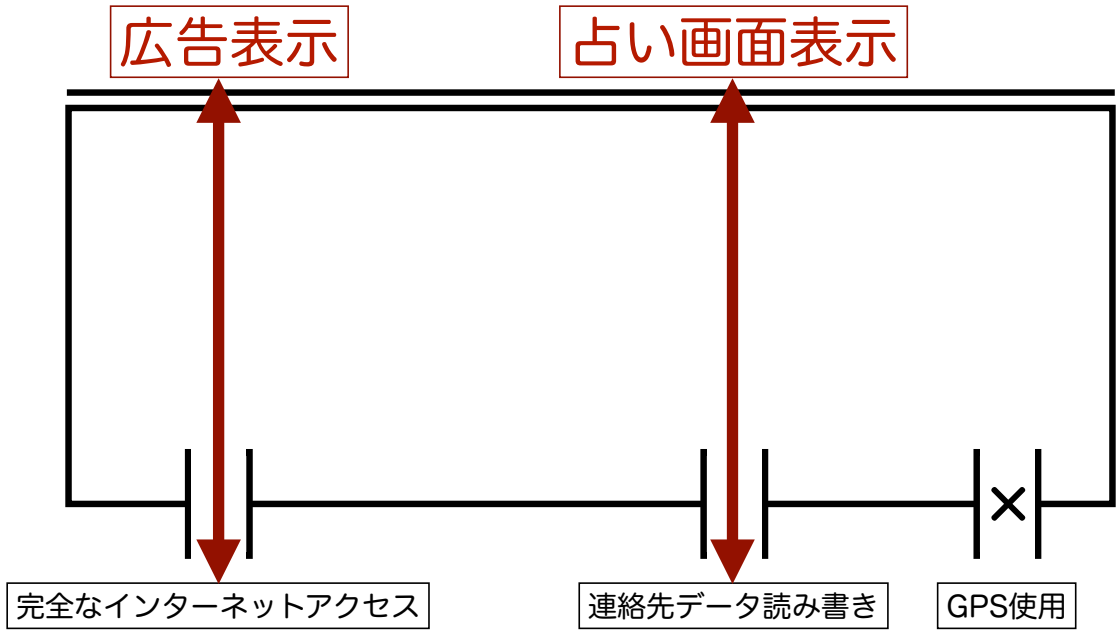
Permission機構 概念図



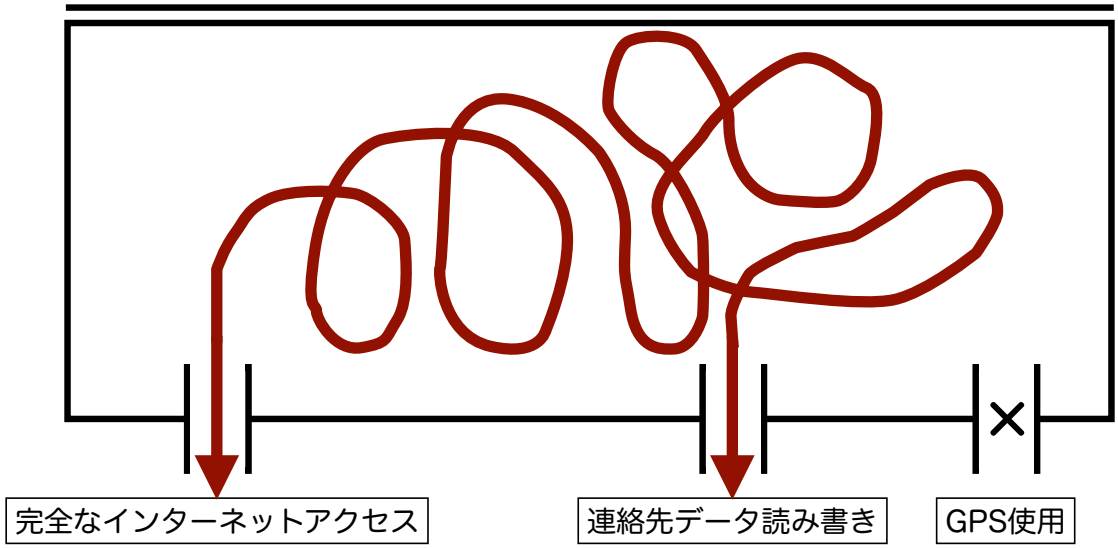
使って送信する場合



使うが送信しない場合



機械的検出は容易でない



つまり

- 機械式の同意確認には無理がある
  - うまくいくのは一部のケース
  - OSによる機械式の同意確認は補助的なもの
- アプリ提供者による同意確認のための作り込みが必要
  - アプリ提供者の自己申告で
  - 自然言語による説明で
  - 個別のプログラムによる同意確認処理で

基本的な考え方

- 利用者の意図に反した動作とならないようにする
  - 不正指令電磁的記録に関する罪（刑法168条の2 ）との関係
  - 個人情報保護法17条 偽りその他不正な手段によらない取得
  - 当該機能の存在を利用者が予見できるか
- 歴史的経緯（国際的な）を踏まえる
  - 意図に反するか否かは、社会通念に照らしその機能につき一般に認識すべきと考えられるところを基準とする
  - 例：Webのアクセスログは20年前にWebが始まったときから
- サービス実現のための技術的必然性があるか
  - 利用者が期待するところのサービスの実現にとって
  - 必要最小限の技術手段を用いるのが望ましい

総務省提言の内容(1)

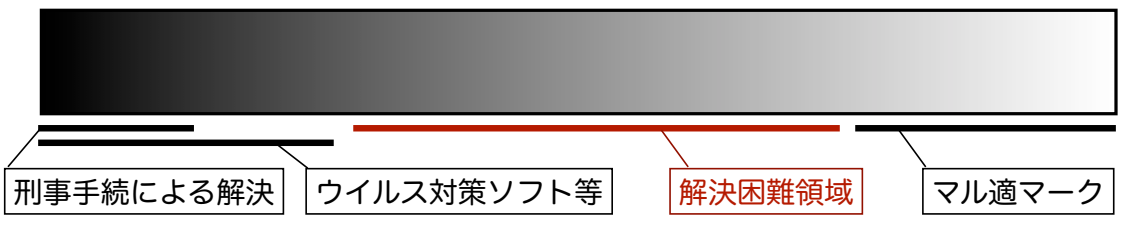
- オプトイン方式（事前に個別の同意を求める）を基本に
  - プライバシー性が高いと考えられる代表的なもの
    - 電話帳、GPSの位置情報、通信内容・履歴、メール内容・送受信履歴等の通信履歴、アプリの利用履歴、保存された写真・動画
    - 「これらの取得に当たっては個別の情報に関する同意を取得する」
- 端末IDは「個人情報に準じた形で取り扱う」
  - 「取得される項目及び利用目的を明確に記載し」
- アプリ単位でのプライバシーポリシーの作成と表示
  - 取得する情報の項目、取得方法、利用目的の特定・明示、通知・公表又は同意取得の方法、利用者関与の方法、外部送信・第三者提供・情報収集モジュールの有無、問い合わせ窓口、ポリシーの変更を行う場合の手続

総務省提言の内容(2)

- 関係事業者における取組
- 実効性を上げるための様々な取組み
  - (1) 業界団体によるガイドライン作成
  - (2) アプリ提供者等への情報発信
  - (3) スマホ画面を考慮した表示
  - (4) 第三者によるアプリ検証の仕組みの検討
    - 確認がなされたアプリに「何らかのマーク等」を表示
      - 本指針や業界団体ガイドラインに沿っているか
  - (5) 関係者の取組状況に関するフォローアップ

課題解決の困難性

- マル適マーク制度の限界
  - 基準の妥当性
    - 厳しい基準とすれば、利用者はマークのないものを使う
      - 結果として対策にならない
    - 利用者を増そうとすれば緩い基準となりがち
- 適切か否かは利用者各々の価値観や判断により異なる
  - 悪用しない保証があれば無断で取得してよいとは限らない
    - 何をもって「悪用」でないと言えるか、一律に決まらない



10年前との類似性

- 10年前、ソフトウェアの脆弱性の解決が課題に
  - 技術者が発見、開発元に知らせても対応されない
    - 脆弱性対策の重要性が広く認識されていなかった
  - 技術者個人が脆弱性情報を告発する例はごく僅かだった
    - 諸外国では発見者の指摘で修正される例が報道されていたのと対照的
- 脆弱性届出制度（2004年）
  - 経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」
  - 「情報セキュリティ早期警戒パートナーシップガイドライン」
- 現在の課題
  - 正当な事業者がプライバシー情報を無断収集している場合
    - これは脆弱性情報ではない / ウイルスでもない
  - 誰が問題提起できるか / 個人による指摘の限界

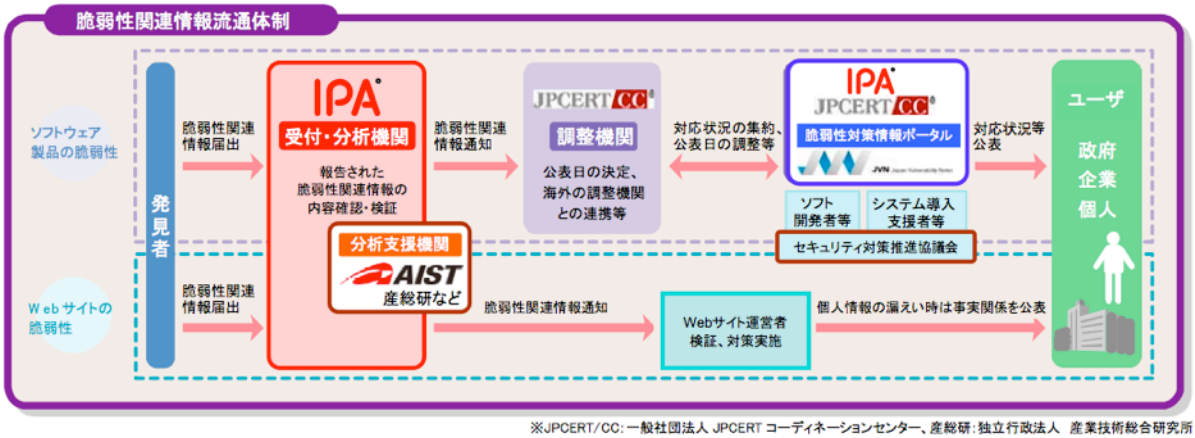
脆弱性届出制度

・脆弱性関連情報流通の基本枠組み

独立行政法人情報処理推進機構（IPA）では、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）の告示を踏まえ、2004 年 7 月からソフトウエア製品及びウェブアプリケーションの脆弱性に関する届出を受け付けています。

http://www.ipa.go.jp/security/vuln/report/index.html

「情報セキュリティ早期警戒パートナーシップ」



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人　産業技術総合研究所

不審アプリ届出(仮)制度の提案

- 発見者からの通報を受付
  - 指摘のあったものについて対応する
  - 指摘の例「掲示されたポリシーに反した送信がある」
  - 取り扱う案件か否かの判断基準が必要
- 事実か開発元に問い合わせる
  - 開発元の自主的な対応を促す
- 事実を公表する
  - そのプログラムが何を送信しているか
  - 公表方法に関する基準が必要
- スマホに限らず一般PC向けプログラムも対象とする

取組みへの期待

- 間接的な改善効果
  - 自主的な取組みの促進
  - 網羅的に解決できるわけではないが
- 他の取組みと平行して
  - マル適マーク方式、ウイルス対策ソフトによる解決
  - 業界団体のガイドライン
- 目標と期待
  - コンピュータプログラムに対する社会の信頼を確保
  - 同時にソフトウェア開発の自由を保障
  - 業界の健全で持続可能な発展を促すことができると期待
    - 焼畑農法に陥るのではなく