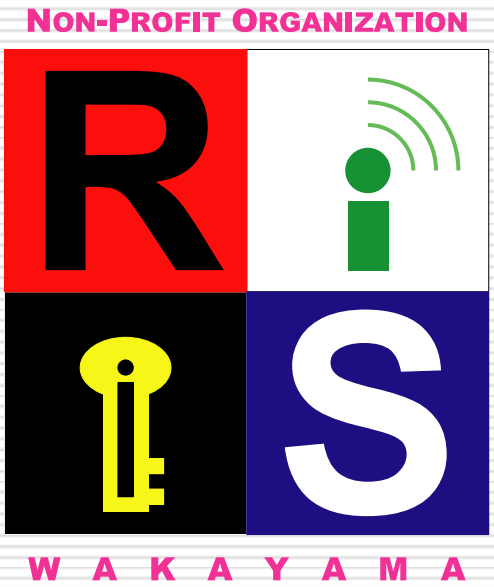
国立情報学研究所オープンハウス
「スマホ持ち込みのセキュリティ対策」

スマートフォンが引き起こすセキュリティ＆プライバシー脅威



2012年6月7日
NPO情報セキュリティ研究所
上原哲太郎
http://uehara.tetsutaro.jp

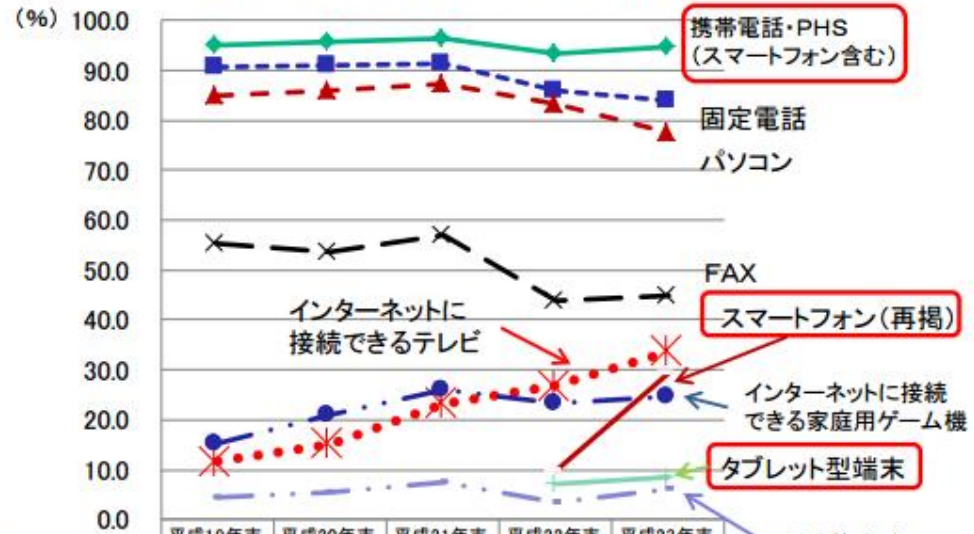
NON-PROFIT ORGANIZATION

RIS WAKAYAMA

スマホ・タブレットの爆発的普及

主要情報通信機器の世帯保有の状況

情報通信機器の普及が全体的に飽和状況の中、スマートフォン保有が顕著な伸び。



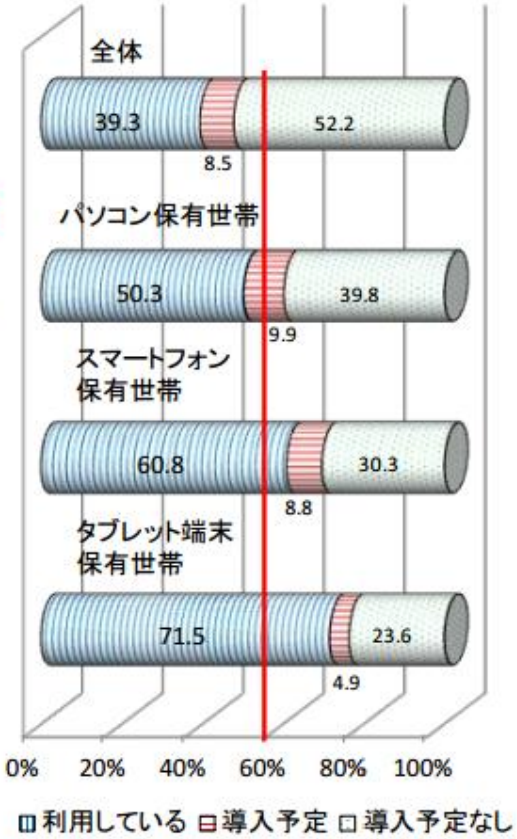
※無回答を除く

	平成19年末（n＝3,640）	平成20年末（n＝4,515）	平成21年末（n＝4,547）	平成22年末（n＝22,271）	平成23年末（n＝16,530）
携帯電話・PHS（スマートフォン含む）	95.0	95.6	96.3	93.2	94.5
固定電話	90.7	90.9	91.2	85.8	83.8
パソコン	85.0	85.9	87.2	83.4	77.4
・FAX	55.4	53.5	57.1	43.8	45.0
・インターネットに接続できるテレビ	11.7	15.2	23.2	26.8	33.6
・インターネットに接続できる家庭用ゲーム機	15.2	20.8	25.9	23.3	24.5
タブレット型端末				7.2	8.5
・その他インターネットに接続できる家電（情報家電）等	4.3	5.5	7.6	3.5	6.2
（再掲）スマートフォン				9.7	29.3

※「携帯電話・PHS（スマートフォン含む）」は、平成22年末以降において、スマートフォンを内数に含む。
平成23年末のスマートフォンを除いた場合の保有率は89．4%である。

保有端末別家庭内無線LANの利用率（世帯）

スマートフォン・タブレット端末保有世帯の利用率は6割を超える。

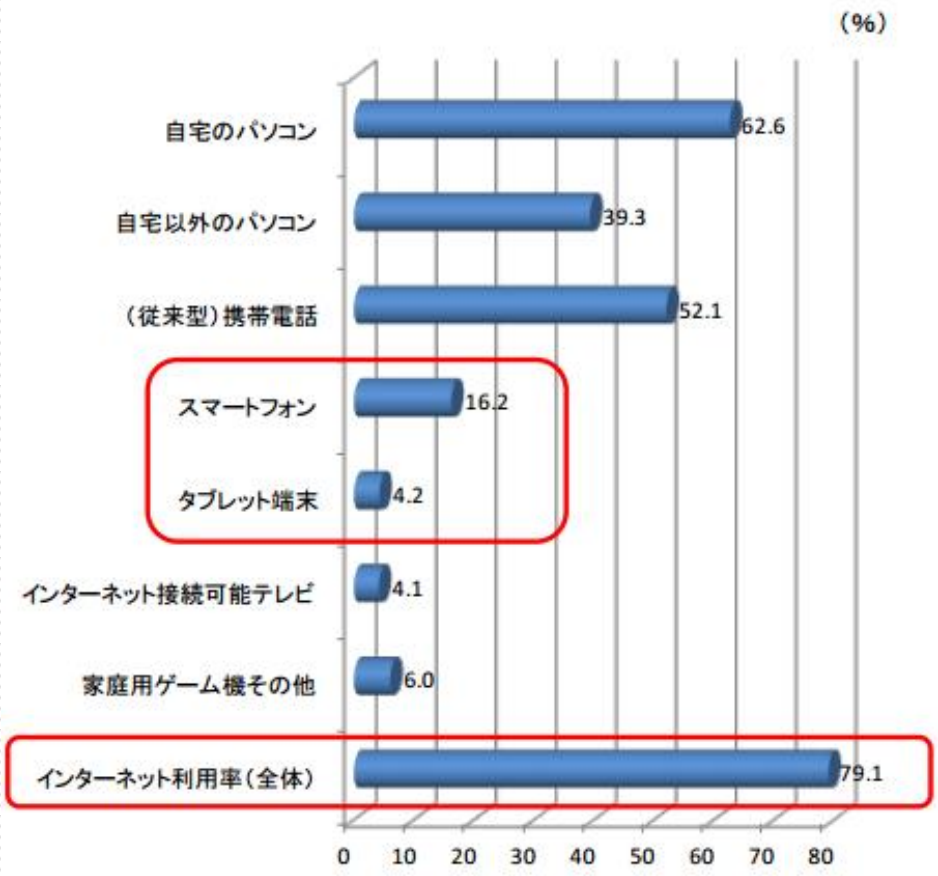


※無回答を除く

平成23年度通信利用動向調査（総務省）より

全体的には、パソコン及び携帯電話によるインターネット利用が多く、主として利用する端末としても両者が家庭内外で7割を超える。

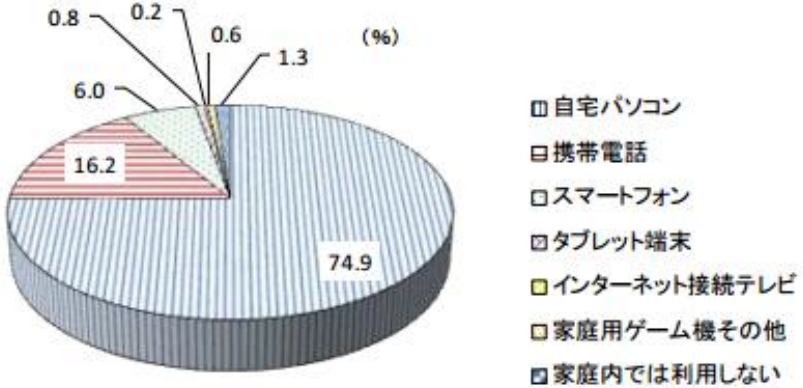
端末別インターネット利用（人口普及率）



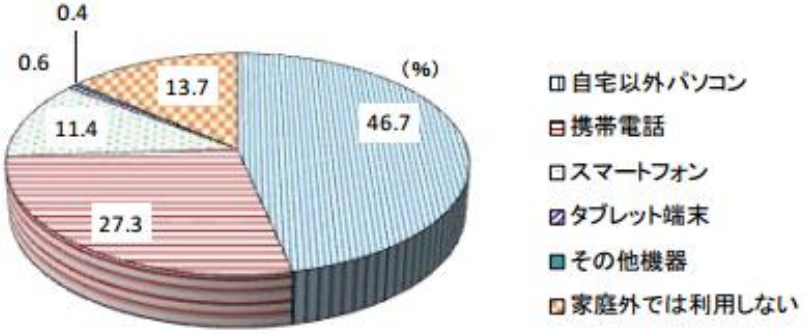
※当該端末を用いて平成23年の1年間にインターネットを利用したことのある人の比率を示す（無回答を除く）。

家庭内外で主としてインターネット接続に使う端末（インターネット利用者に占める比率）

家庭内インターネット利用



家庭外インターネット利用



※平成23年の1年間にインターネットを利用したことのある人に占める当該端末を主として利用する人の比率を示す（無回答を除く）。

平成23年度通信利用動向調査（総務省）より

NON-PROFIT ORGANIZATION
WAKAYAMA

BYOD:Bring Your Own Device 私物デバイスの業務活用

- かつては「先進的」ユーザを中心に常態化
  - 私物PCの職場持ち込み・活用・自宅持ち帰り…
- しかし（残念ながら）事故が多発→禁止へ
  - 特にWinny+Antinny案件で深刻な事故が
  - PCは支給＆私用禁止＆持ち帰りは厳禁へ
- ここへ来て揺り戻し
  - BYODの方が業務効率の向上が望める
  - どうせ「隠れて使う」人がいるなら…
  - 震災を機に在宅勤務態勢の見直しへ

スマホ普及を機にリスクマネジメントをした上での
BYOD一部容認が大きな流れになった

スマホ・タブレットBYODのリスクを考えるポイント

- ポイント1：スマホ（やタブレット）はOSによってリスクがかなり異なる
- ポイント2：スマホ単体のリスクとクラウドサービス利用のリスクを混同しない
- ポイント3：技術的対策はまだ未熟な上個人所有の機器に導入する必要があるため大きくは頼れないセキュリティポリシーを中心に考えるべき

NON-PROFIT ORGANIZATION
R i
S
WAKAYAMA

スマホ・タブレットのOS

- 多くがアプリに対しサンドボックスモデルを採用
  - Windowsの「管理者権限」にあたるものは
    アプリには与えられない（あれば脆弱性である）
  - APIも制限され、利用者の許可なく使えない場合も
  - アプリ間のデータ交換手段がごく限られる
- 多くはアプリが「マーケット」限定で配布される
  - そこである程度の審査を受ける
- よって基本的には「マルウェア」が作りにくい
  - 例外的なのがAndroid
  - JailBreak（JB）した場合も別
- 同時に「アンチウィルス」も作りにくい

NON-PROFIT ORGANIZATION
WAKAYAMA

主なスマホ・タブレット用OS

OS名	主な機器	公式マーケット外アプリ導入	アプリ審査
iOS	iPhone, iPad iPod touch等	不可能 （JBした場合除く）	全審査 （半自動？）
Android	多数	可能（マーケット自体公式Google Play以外にも多数ある）	Google Playは自動審査 キャリアは別審査
Windows Phone	現在日本ではau IS12Tのみ	不可能	全審査 （半自動？）
BrackBerryOS	ドコモ BrackBerry	不可能（企業利用の場合アプリ導入そのものも禁止可能）	全審査 （BIS）

その他 Windows Mobileは「PC並み」 Windows 8 RTが今後登場予定

NON-PROFIT ORGANIZATION
R i
S
WAKAYAMA

スマホ向けOSとマルウェア

- Androidを除くと報告例は少ない
- Androidにしても…
  - 脆弱性を突くものは少ない
  - 『錯誤』や『不注意』を狙い、こっそりと裏で必要な情報を詐取するものが多い
- ただ、内部データの「標準化」が事態を深刻に

- 一方Root化されたAndroidやJailBreakされたiOSは「PC並みに危険」

NON-PROFIT ORGANIZATION
R i
S
WAKAYAMA

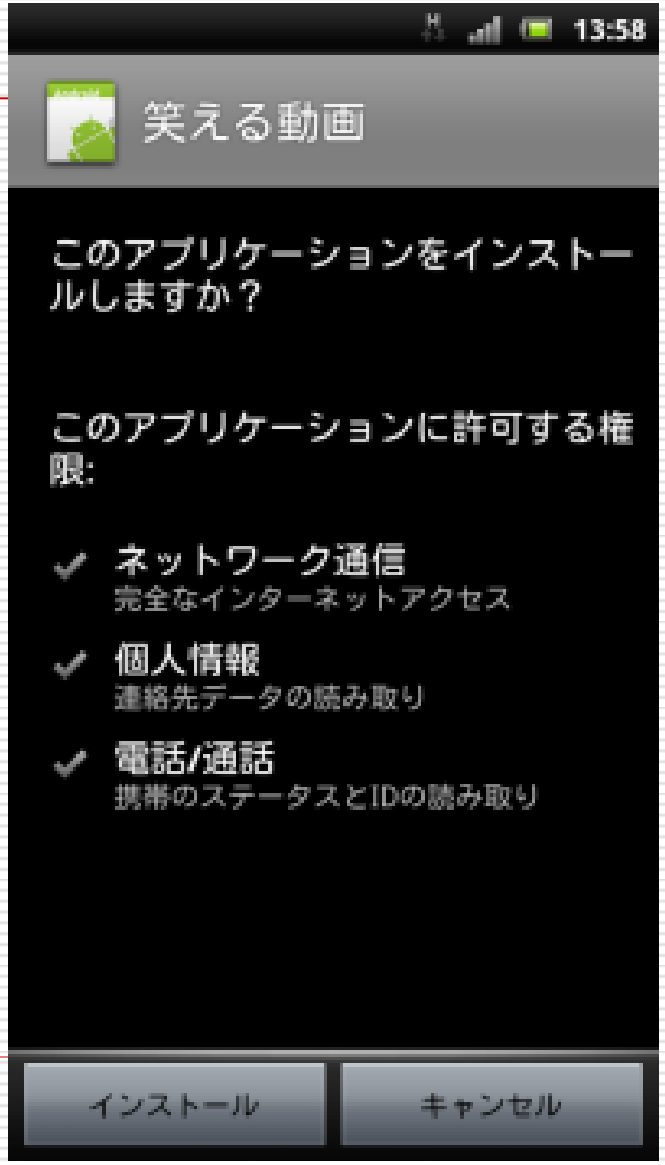
Androidのパーミション

- Androidは100以上のAPIに関して
  利用者に使用許可を得る仕組みがある
  - インストール時にアプリが許可を得る
    ただし許可を得ないとインストール自体できない
    後で設定変更もできない(iOSとの違い)
- 主なもの
  - 個人情報関係への読み書き
    - 連絡先情報、カレンダー、発着信履歴、ブラウザ履歴
      ブックマーク、SMS、位置情報、アカウント、ID類
  - ハードウェアの操作
    - カメラ撮影、録音、SDカードへの読み書きなど
  - ソフトウェアの操作
    - ネットワークの通信、アラーム設定、各種設定変更など
- 問題:「何を」得るかは判っても「どう使うか」が判らない

NON-PROFIT ORGANIZATION
R i
i S
WAKAYAMA

「the Movie」事件

- 人気ゲームのプレイ動画などが見られるだけのアプリが大量に（29種）Google Playにアップロードされる
- コレをインストールすると連絡先データと携帯ID等が外部に送信される



NON-PROFIT ORGANIZATION
R i
i S
WAKAYAMA

スマホアプリの「個人情報詐取」問題

- The Movieに限らず「連絡先」を取るアプリがSNS中心に大量にある
  - Facebook, LINE…
  - iOS版ですらある
    - iOSの場合は連絡先パーミションの仕組みがなかったのでさらに深刻に
- 事前に許可を得ているか？（何に使う？）
- そもそも「連絡先データ」は「だれのものか」

NON-PROFIT ORGANIZATION
R i
i S
WAKAYAMA

IDだけでも問題？

- 携帯IDやSIMのID（IMSI）、UDID（デバイス固有ID）などはターゲティング広告を中心に格好の「名寄せ」道具となっている
- なので「携帯IDの読み取り」だけでもプライバシ漏洩につながる可能性
- ただし組織セキュリティとの関係は要検討

他の問題：ロケーションプライバシ

- カレログ問題

- 同様の仕組みを「社員管理」に使うツールもある
- 一方で位置情報を積極的に公表させるアプリ
  - 「チェックイン」、Foursquare、コロプラ…
- 位置情報を他人に知らせる／知られることはセキュリティとプライバシー上どうあるべきか

NON-PROFIT ORGANIZATION
R i
i S
WAKAYAMA

ではどうするのか

- BYODの視点で見た場合
  - 「連絡先データ」の扱いをポリシーで決める
    その上で連絡先データの扱いがポリシーを
    超えないかチェック
  - その他の個人情報（発着信記録）についても
    チェック
    - 「こっそり」提供することはAndroidでは難しい
    - iOSではパーミションでなくアプリ審査で行うが
      抜けがありうることを意識する
  - いずれにせよパーミションだけでは判らないことが
    残っていることに要注意

NON-PROFIT ORGANIZATION
WAKAYAMA

クラウドサービスの問題

- クラウドサービスと併用されることにより「組織内情報流出」の経路が出来てしまう問題
  - 特にクラウドストレージサービス
    - Evernote, Dropbox, Skydrive, Google Drive…
  - その他グループウェア系
- SNSなどがコミュニケーション経路となりメールなどの監視網の外となる問題
  - スマホメールの公私混同問題も同じ
- スマホだけでなくPCでも同じ

対策はフィルタ導入かポリシー

NON-PROFIT ORGANIZATION
R i
S
WAKAYAMA

おまけ：脆弱性問題はあるか？

- OSの脆弱性問題はあるが
  攻撃はいわゆるroot化・JBがほとんど
  - root化やJBされたものを狙うマルウェアはあり
- もちろん脆弱性はあれば防ぐべきだが…
  - 必ずしも対策は早くない
  - Androidのバージョン分岐問題