資料１－３

【P8～11は、構成員及び事務局限り】

「スマートフォン・クラウドセキュリティ研究会」の当面の検討事項及びスケジュール(案)

総務省 情報流通行政局
情報セキュリティ対策室

2011年10月19日

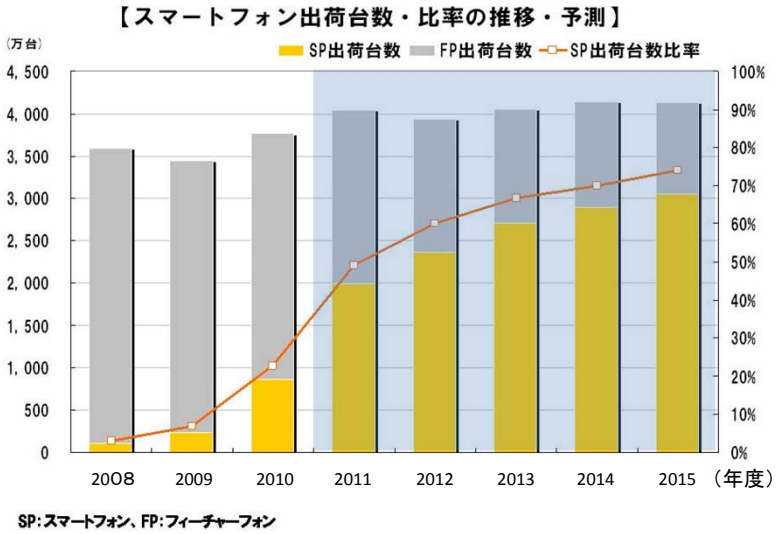
背景(1)

○ スマートフォン※及びクラウドサービスの普及の進展。

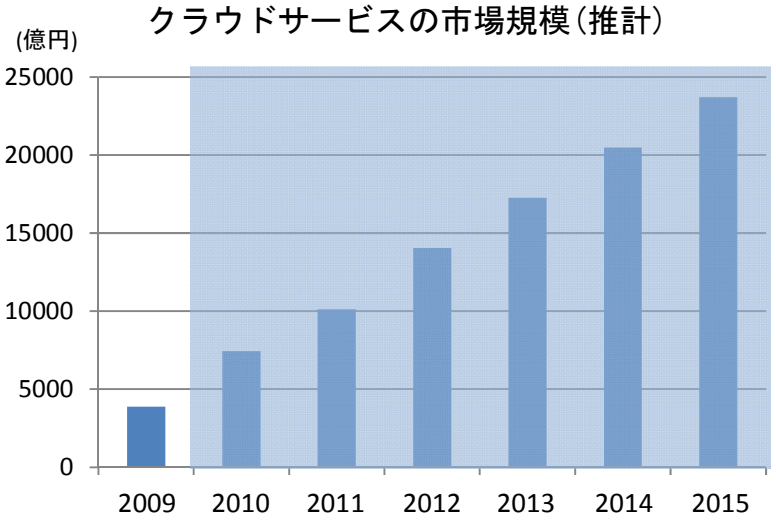
- 2010年度のスマートフォン国内出荷台数：855万台(前年度比3.7倍)
  ⇒携帯電話端末の国内総出荷台数の22.7%
- クラウドサービスの市場規模：2015年には2兆3,000億円規模に膨らむ見込み
  ⇒2009年の市場規模の6.1倍

○ 今後、スマートフォンを通じたクラウドサービスの利用の普及などクラウドサービス利用主体・形態や取り扱う情報の多様化が予想。

※スマートフォン：従来の携帯電話端末の機能に加え、PC並の高度な情報処理機能が備わった携帯端末。



出典：株式会社MM総研



出典：総務省「スマート・クラウド研究会報告書」(2010年5月17日)

背景(2)

スマートフォンをターゲットにしたマルウェア

○ 近年、スマートフォンをターゲットにしたマルウェアが出現している。
（現状、大きな被害報告はない。）

2007年10月： iOSを狙った、閲覧によりシステムのセキュリティに関する制限を一部取り除く行為(Jailbreak)を実行するウェブサイトが初めて発見。

2010年 8月： Androidを狙ったマルウェアが初めて発見。

2010年12月： Androidを狙ったボットウイルスが初めて発見。

2011年 2月： 日本語のAndroidアプリケーションにマルウェアが混入。

2011年 8月： 2011年第2四半期にAndroidを狙ったマルウェア数が前四半期比76%増。（マカフィー社調査）

これまでに見つかっているマルウェアの機能
- ○勝手に電話を発呼
- ○位置情報を無断で第三者に知らせる
- ○遠隔操作による通話の盗聴及びデータの窃取　等

2010年8月、Android向けマルウェアとして初めて発見された「TROJ_DROIDSMS.A」。映像再生ソフトを装い、有料のショートメッセージサービスを送信する機能を有する。（トレンドマイクロ社　マルウェアブログ）

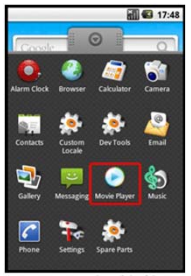


Figure 1. Screenshot of the fake Windows media player icon

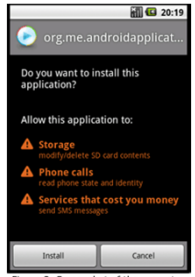
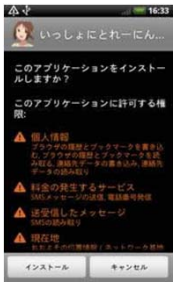


Figure 2. Screenshot of the prompt message when installing the fake app

2011年2月、日本語のAndroid アプリケーションの海賊版に「Android.Geinimi」と呼ばれるマルウェアが混入されたものが、規制されていないAndroidマーケットプレイスで発見。利用者が気づかないように、インストール済みのアプリケーションのリスト情報や、連絡先情報を、外部へ送信する可能性などがある。（シマンテック社　オフィシャルブログ）



スマートフォンによるクラウドサービス利用で懸念されるセキュリティ事項

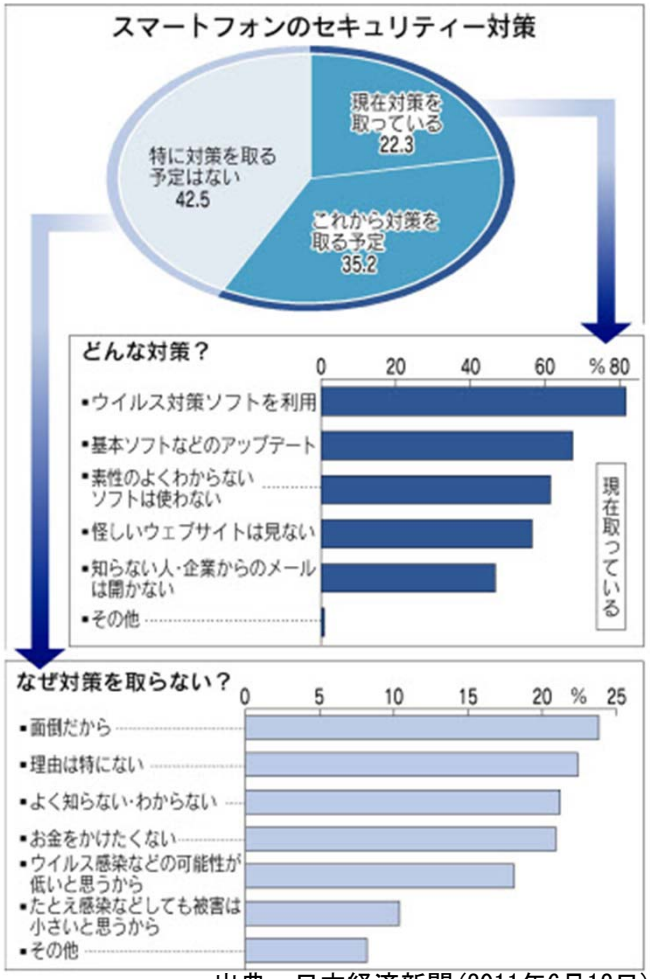
○ 利用者が意識せずにクラウドサービスを利用することが増え、情報漏えいのリスクの管理が複雑化。

○ 様々なデバイスやサービスで共通利用可能なクラウドのID・パスワードが他者に知られると、情報漏えいの被害が増大。

背景(3)

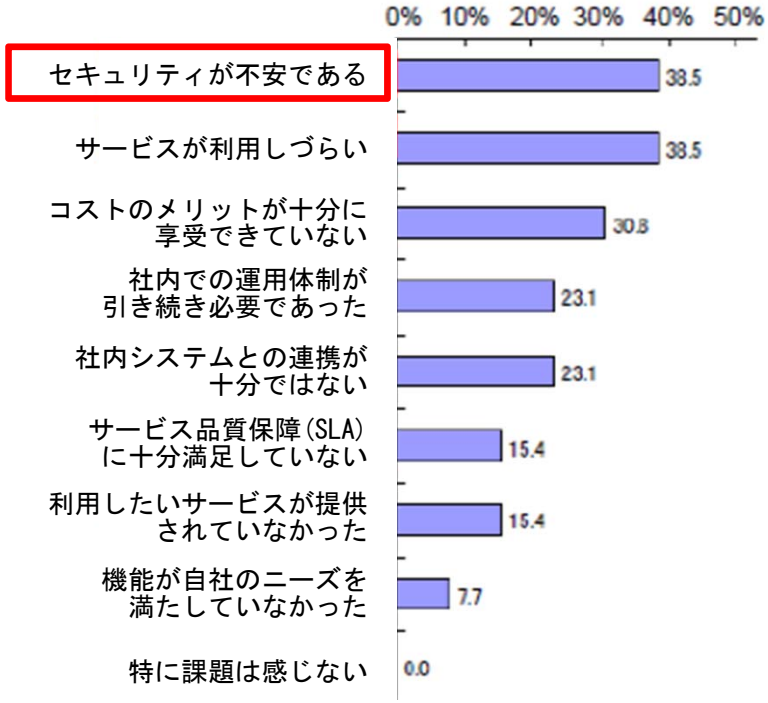
○ スマートフォン利用者のセキュリティ意識は低い。
- 安全対策を実施していない利用者：78%
- 安全対策を取る予定もない利用者：43%

○ クラウドサービス導入後にセキュリティに不安を感じている利用者が38.5%。



出典：日本経済新聞(2011年6月12日)

クラウドサービス導入後に不満に、感じている点



出典：総務省「スマート・クラウド研究会報告書」(2010年5月17日)

スマートフォンに関するこれまでの検討(1)

◇ 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（総務省）

○ 電気通信サービス利用者ＷＧ　提言(案)の概要について
(2011年9月28日 第10回会合・資料1)
「安全・安心サービスの提供の在り方」のうち、スマートフォンに係る今後の方向性

- 従来の携帯電話端末とスマートフォンでは、利用できるサービスに差異があることについて、カタログ等へ具体的に記載したり、端末購入時に説明を行ったりすることにより、利用者が認識できるようにすること。

- セキュリティや事業者対応の限界等のスマートフォンの普及に伴って新たに発生する問題点を整理し、利用者自ら対応すべき事項、問題発生時に携帯電話事業者として対応が可能な事項と対応困難な事項、対応困難な場合の相談先等を、予め利用者に対し周知。

- 今後のスマートフォンを標的としたマルウェアの出現状況やそれに対する対策の状況等を注視しつつ、必要に応じ、関係者と協力しつつ、専門家による適切な場を設置するなどして、これらの点に関する検討を進めていく。

スマートフォンに関するこれまでの検討(2)

◇ 日本スマートフォンセキュリティフォーラム(JSSEC)

○ スマートフォン&タブレットの業務利用に関するセキュリティガイドラインβ版(2011年8月31日)

- ビジネスユース（BYODを含む。）における管理者向けガイドライン（利用者向けではない。）。
- デバイス毎ではなく4種のOSにより分類（タブレットも対象。）。
- 端末、アプリケーション及びネットワークの特徴を組み合わせた利用形態と脅威の認識。
- アドレス帳、電話、メール等の利用シーン別に、セキュリティ上の脅威とその対策を解説。
- 計画、導入、運用及び廃棄のライフサイクルの各フェーズにおける留意点を解説。
- セキュリティコストがメリットを上回る場合には、導入の先送りも視野。

○ 構成員

幹事会員（26社）：アイ・ティー・シーネットワーク株式会社、株式会社インフォセック、NRIセキュアテクノロジーズ株式会社、株式会社エヌ・ティ・ティ・ドコモ、株式会社カスペルスキー、 KDDI株式会社、サイバーソリューションズ株式会社、サイバートラスト株式会社、株式会社シーイーシーソリューションズ、シスコシステムズ合同会社、株式会社システナ、株式会社シマンテック、シャープ株式会社、ソニーデジタルネットワークアプリケーションズ株式会社、ソフトバンクモバイル株式会社、株式会社ソリトンシステムズ、株式会社ディアイティ、トレンドマイクロ株式会社、日本ヒューレット・パッカード株式会社、日本電信電話株式会社、株式会社ネクストジェン、株式会社日立システムズ、富士ソフト株式会社、株式会社ProVision 、マカフィー株式会社、株式会社ラック

正会員(83社)：株式会社RSP、株式会社ACCESS、合同会社アビニシオ・リサーチ 、アルバネットワークス株式会社、アルプスシステムインテグレーション株式会社、株式会社アンラボ、株式会社イーグリッド、伊藤忠テクノソリューションズ株式会社、イノパスソフトウェア株式、インサイトインターナショナル株式会社、株式会社インターナショナル・ストラテジック・リーダーズ、インヴェンティット株式会社、株式会社インテック、ウィアー・エンジニアリング株式会社、ウェブルート・ソフトウェア株式会社、株式会社ウェブレッジ、株式会社Ａ３セキュリティ、 NECネッツエスアイ株式会社、 NHN Japan株式会社、株式会社NSD 、株式会社エヌジェーケー、エヌ・ティ・ティ・コミュニケーションズ株式会社、エヌ・ティ・ティ・ソフトウェア株式会社、株式会社NTTデータMSE 、エヌ・ティ・ティ・データ先端技術株式会社、エフセキュア株式会社、エレコム株式会社、キヤノンITソリューションズ株式会社、グローバルセキュリティエキスパート株式会社、株式会社ケイ・テック、株式会社KBIZ 、株式会社ゲネシスコンマーズ、株式会社神戸デジタル・ラボ、株式会社コネクトワン、サムスン電子株式会社、 GMOグローバルサイン株式会社、ジュニパーネットワークス株式会社、一般社団法人情報セキュリティ相談センター、新日本無線株式会社、セコムトラストシステムズ株式会社、ソニー・エリクソン・モバイルコミュニケーションズ株式会社、ソフォス株式会社、ソフトバンク・テクノロジー株式会社、大日本印刷株式会社、株式会社大和総研ビジネス・イノベーション、チェック･ポイント･ソフトウェア･テクノロジーズ株式会社、株式会社ディー・ディー・エス、デジタルアーツ株式会社、株式会社テラス、株式会社Doctor Web Pacific 、ドコモ・システムズ株式会社、凸版印刷株式会社、トヨタ自動車株式会社、株式会社ナバヨアジア、日本CA株式会社、日本システムウエア株式会社、日本データコム株式会社、日本電気株式会社、日本電子専門学校、日本ベリサイン株式会社、日本ユニシス株式会社、株式会社ネットマークス、ノミナムジャパン株式会社、伯東株式会社、パナソニック株式会社、株式会社バリューエンジン、バルテス株式会社、ハンドリームネット株式会社、BizMobile株式会社、株式会社日立製作所、ファルコンシステムコンサルティング株式会社、フェリカネットワークス株式会社、フォーティネットジャパン株式会社、フォーマルハウトテクノソリューションズ、株式会社富士通四国システムズ、株式会社富士通ソーシアルサイエンスラボラトリ、富士通東芝モバイルコミュニケーションズ株式会社、株式会社富士通ビー･エス･シー、株式会社ブランコ・ジャパン、ベライゾン ビジネス、丸紅OKIネットソリューションズ株式会社、株式会社ユーエヌアイ研究所、ユニアデックス株式会社、リアルコム株式会社、レノボ・ジャパン株式会社

特別会員：Androidセキュリティ部、一般社団法人Open Embedded Software Foundation 、一般社団法人情報通信ネットワーク産業協会(CIAJ) 、データベース・セキュリティ・コンソーシアム(DBSC) 、特定非営利活動法人日本ネットワークセキュリティ協会(JNSA) 、一般社団法人モバイル・コンテンツ・フォーラム(MCF)

オブザーバー：内閣官房情報セキュリティセンター(NISC) 、総務省、経済産業省、独立行政法人情報通信研究機構(NICT) 、独立行政法人情報処理推進機構(IPA) 、公益財団法人金融情報システムセンター(FISC) 、一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)

本研究会の当面の検討事項

当面の検討事項

○ スマートフォンの情報セキュリティ上の課題抽出（課題の例）

- アプリケーションの作成、提供、利用に関する課題。
- 通信路の多様性に伴う課題。
- マルウェア対策ソフトの有効性に関する課題。
- 個人に関する情報が、一つの通信端末に集約されることの課題。
- リバースエンジニアリング※1に関する課題。
- ソーシャルハッキング※2に関する課題。

○ 重点的な検討課題

- 利用者の情報セキュリティ意識の向上やセキュリティ対策を取ることを促すガイドライン。
- 事業者が導入を検討されるべきセキュリティ対策。
- 他の枠組みで検討・対処することが望まれる事項。

※1 リバースエンジニアリング：機器を分解、動作を観察、又はソフトウェアの動作を解析するなどして、製品の構造を分析することにより、製造方法や動作原理、設計図、ソースコードなどを調査すること。

※2 ソーシャルハッキング：ユーザーIDやパスワードを盗み出すために、技術的な手段を利用せず、直接本人の口から聞き出す、タイプ内容を盗み見る、書類やメモを入手するといった手段を利用する行為。

スケジュール（案）

○ スマートフォン（スマートフォンによるクラウド利用を含む。）に関するセキュリティ対策について検討を集中的に行い、当面の対策につき中間報告としてとりまとめ予定。

○ その後、最近の技術進歩等に伴う課題を含め、中長期的な対策等につき検討の上、報告をとりまとめ。

年内の進め方

第1回（10月19日）：○ 研究会の背景・検討対象等の確認
○ スマートフォンに関するセキュリティ対策の現状及び課題の整理

第2回（11月 4日）：○ 当面の対策につき議論①

第3回（11月29日）：○ 当面の対策につき議論②

第4回（12月19日）：○ 中間報告案とりまとめ予定