スマホアプリセキュリティの現状課題と解決策

一般社団法人日本スマートフォンセキュリティ協会
技術部会　アプリケーションWG　セキュアコーディンググループ
松並　勝 <masaru.matsunami@jp.sony.com>

今日の話題

1.モバイルシフト

なぜスマホアプリが流行っているのかという話

2.Androidアプリの脆弱性問題

いまのアプリはとにかく無防備だという話

3.セキュアなAndroidアプリ開発法

忙しいアプリ開発者でも簡単にセキュアなアプリを作るうまいやり方があるという話

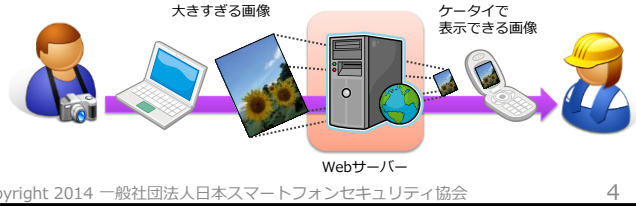
自己紹介

2000年頃、社会人4年目

とあるメーカーで
複合機の組込技術者

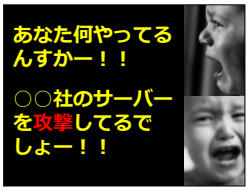
プライベートで
ケータイWebアプリ開発

送信先ケータイの機種を自動判別し、
液晶のサイズや色数、
メモリの容量に合わせて
最適な画像に自動変換



ケータイWebアプリのサーバーがハッカーの踏み台被害に遭う

仕事中にサーバー会社から電話で叱られ



サーバーが乗っ取られ、踏み台にされていた

原因：wuftpdのバッファオーバーフロー脆弱性

原理が理解できず、技術者として**悔しい**

組込機器のセキュリティは放置状態だ！

2001年からソフトウェアセキュリティの道へ

インターネットセキュリティの会社へ**転職**

IPA/ISECセキュア・プログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programmingv1/index.html

2002年、ソニーDNA（現在）へ**転職**

ソニーのソフトウェア開発で Try & Error

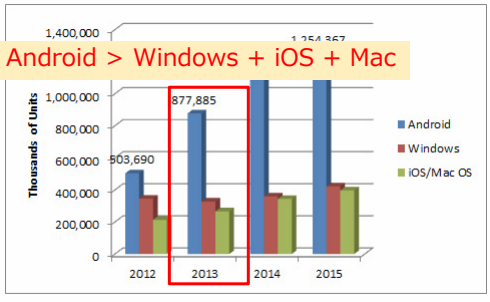
PC
CE（組込み）機器
Web
Android…

モバイルシフト
スマホアプリが流行っている理由

モバイルシフト　その１

Androidデバイスの出荷台数が、なんと他の合計を超えている → Androidスマホが急激に普及

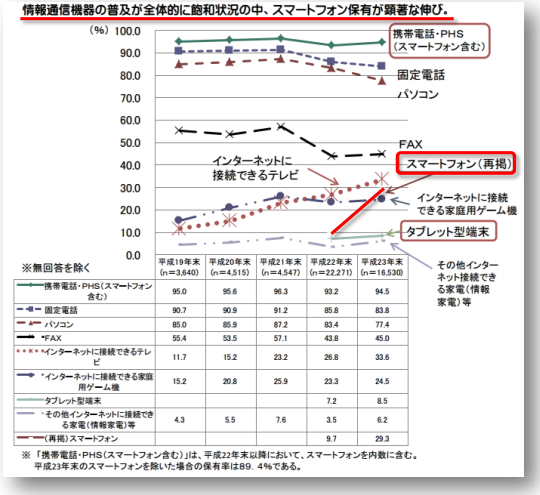
各OSを搭載したデバイスの難関出荷台数（全世界）



Global operating system market share based on device shipments. Source: Gartner Inc.

http://jp.techcrunch.com/2014/01/09/20140108androids-rise-to-platform-dominance-in-one-graph/

モバイルはまだまだ伸びしろがある



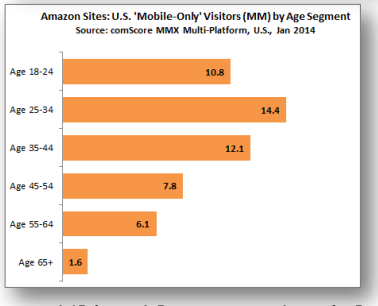
http://www.soumu.go.jp/johotsusintokei/statistics/data/120530_1.pdf

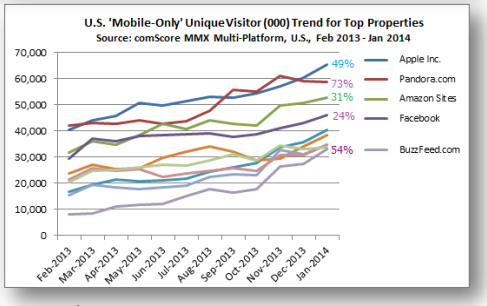
Mobile-Onlyユーザーが増加の一途

モバイル端末からしか接触しないネットユーザーが急増

2014年03月22日 12:43

デスクトップ(PC)からモバイルへ。この流れは止まりそうもない。この流れで注目したいのは、若者や新興国ユーザーを中心に、モバイルデバイス(端末)しか利用しないユーザーが急激に増え始めていることだ。





http://lite.blogos.com/article/82850/

もう完全にモバイル中心の世界に

9月16～18日にわたり開催されたデジタルマーケティングカンファレンス「アドテック東京」で、ヤフー代表取締役社長CEOの宮坂学氏が「“脱皮”のその先へ」と題した基調講演を行った。

宮坂氏は2012年にも同イベントに登壇し、「脱皮しない蛇は死ぬ」をキーワードとして、当時ヤフーが打ち出した戦略「スマートフォンファースト、PCセカンド」について説明していた。

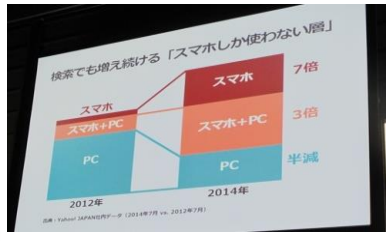
ヤフー代表取締役社長CEOの宮坂学氏

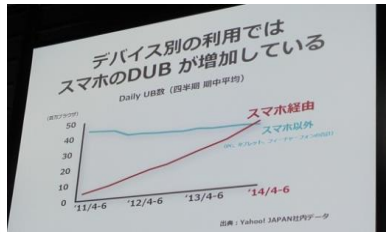
当時のヤフーはスマートデバイス向けのサービスがほとんどなく、アプリのダウンロード数は、すべてのサービスを足しても約3000万ダウンロードほどだったという。この戦略が始まっておよそ2年半が経つが、どのような変化が起きているのか。

宮坂氏によれば、PCでしか検索をしない人が半減し、その一方でスマートフォンでしか検索をしない人が7倍に増加。また、スマートデバイス向けアプリのダウンロード数は約2億件まで伸びたという。「日本のインターネット人口が1億人ということを考えると、数だけを見れば、それなりに育てることができた」（宮坂氏）。

2014年4～6月期には、Yahoo! JAPANへのスマートフォンからの流入と、PCなどスマートフォン以外からの流入が逆転した。宮坂氏は「いつかくるだろうとは思っていた。これはヤフーにとって大きな転換点ではないか」と話し、「Yahoo! JAPANの歴史の中でも、非常に大きな四半期だった」と振り返る。

「インターネット企業の中には、このクロスオーバーをとっくの昔にやっているところも多い。ただ、Yahoo! JAPANはユーザー数が多いがゆえ、日本で最も“インターネットリテラシーがそれほど高くない人”が使っているサイトだと思っている。そういったサイトでさえ、ついにPCよりもスマートフォンがアクセスの比率で上回ってきた」（宮坂氏）。





http://japan.cnet.com/marketers/sp_adtech2014/35054013/

モバイル経由の売上が凄い伸び率

スマホ対応を様子見している会社が多い中、
スマホブラウザ対応したECサイトが儲かっている

http://web-tan.forum.impressrd.jp/e/2013/08/07/15736
http://news.livedoor.com/article/detail/7622116/
http://itpro.nikkeibp.co.jp/article/NEWS/20131204/522502/

私も通勤中の隙間時間に スマホで買い物してます

隙間の可処分時間を獲得！

モバイルシフト　その２

スマホのWebブラウザ対応

→ アプリ へ取り組む企業が増加

https://play.google.com/store/apps/details?id=jp.co.rakuten.android
https://play.google.com/store/apps/details?id=jp.amazon.mShop.android
https://play.google.com/store/apps/details?id=jp.co.yahoo.android.yauction

なぜ、アプリなのか？

理由① 圧倒的な操作性、レスポンス、表現力

http://www.itmedia.co.jp/news/articles/1209/12/news032.html
http://ggsoku.com/2013/05/column-native-app/

なぜ、アプリなのか？

理由② 一等地（ユーザーに一番近い場所）を狙う

起動までのひと手間

アプリならワンタッチ起動！

スマホブラウザ対応Webサイトはブックマークの中に埋もれてしまいます

なぜ、アプリなのか？

理由②　一等地（ユーザーに一番近い場所）を狙う、誰よりも先に場所を取る

一等地は本当に狭い

左右にも一応場所はある　ホーム画面は僅か16カ所程度　左右にも一応場所はある

なぜ、アプリなのか？

理由②′二等地でも有利

プッシュ通知、バックグラウンド動作…

ホーム画面は取れなくても、アプリならばアクティブにユーザーに働きかけることができる

なぜ、アプリなのか？

理由③ 禁断のユーザー情報をビジネス活用

スマホの中にはビジネス活用したくなる貴重な情報が満載

Android OSが管理する情報資産
端末の電話番号
電話帳
通話履歴（受発信の日時や番号）
IMEI（端末固有ID）、IMSI（回線契約者ID）
位置情報（GPS、WiFi、基地局…）
アカウント情報（Googleアカウント…）
メディアデータ（写真、動画、音楽、録音…）
インストールアプリ一覧
…

アプリ	アプリが管理する情報資産
Eメール	メアド、送受信メール本文、添付…
SMS	送受信SMSメッセージ本文…
Webブラウザ	ブックマーク、閲覧履歴、クッキー…
カレンダー	予定、ToDo、イベント…
家計簿	残高、買い物履歴…
Facebook	アカウント、コンテンツ…
Twitter	アカウント、コンテンツ…
mixi	アカウント、コンテンツ…
…	

なぜ、アプリなのか？

理由③ 禁断のユーザー情報をビジネス活用

例： 位置情報、趣味嗜好からユーザーが購入しそうな商品紹介

Android OSが管理する情報資産
端末の電話番号
電話帳
通話履歴（受発信の日時や番号）
IMEI（端末固有ID）、IMSI（回線契約者ID）
位置情報（GPS、WiFi、基地局…）
アカウント情報（Googleアカウント…）
メディアデータ（写真、動画、音楽、録音…）
インストールアプリ一覧
…

アプリ	アプリが管理する情報資産
Eメール	メアド、送受信メール本文、添付…
SMS	送受信SMSメッセージ本文…
Webブラウザ	**ブックマーク**、**閲覧履歴**、クッキー…
カレンダー	予定、ToDo、イベント…
家計簿	残高、買い物履歴…
Facebook	アカウント、コンテンツ…
Twitter	アカウント、コンテンツ…
mixi	アカウント、コンテンツ…
…	

なぜ、アプリなのか？

理由③ 禁断のユーザー情報をビジネス活用

例： 電話帳に登録された知人情報から見込み顧客を探す

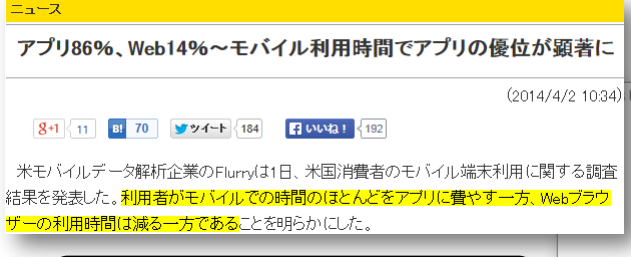
Android OSが管理する情報資産
端末の電話番号
電話帳
通話履歴（受発信の日時や番号）
IMEI（端末固有ID）、IMSI（回線契約者ID）
位置情報（GPS、WiFi、基地局…）
アカウント情報（Googleアカウント…）
メディアデータ（写真、動画、音楽、録音…）
インストールアプリ一覧
…

電話帳内の1件のエントリに含まれるユーザーの知人の情報

情報	内容
名前	表示名、名前、苗字、ミドルネーム…
電話番号	自宅、携帯電話、仕事、FAX、MMS…
Eメールアドレス	自宅、仕事、携帯電話…
プロフィール画像	サムネール画像、大きな画像…
インスタントメッセンジャー	AIM、MSN、Yahoo、Skype、oogle Talk…
ニックネーム	略称、イニシャル、旧姓、別名…
住所	国、郵便番号、地域、地方、町、通り…
グループ	お気に入り、家族、友達、同僚…
ウェブサイト	ブログ、プロフィールサイト、自宅、会社…
イベント	誕生日、記念日、その他…
関係する人物	配偶者、子供、父、母、マネージャー、助手、同棲関係、パートナー…
SIPアドレス	自宅、仕事、その他…
…	

なぜ、アプリなのか？

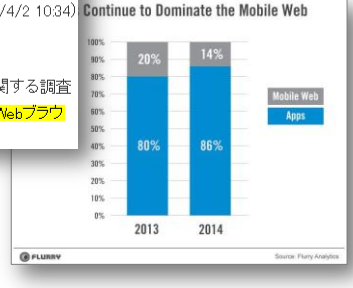
理由④ ユーザーはアプリを使い、もはやWebブラウザは使わない


ニュース

アプリ86%、Web14%～モバイル利用時間でアプリの優位が顕著に

(2014/4/2 10:34)

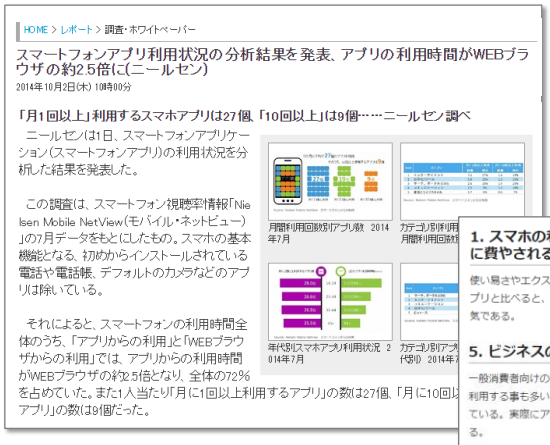
米モバイルデータ解析企業のFlurryは1日、米国消費者のモバイル端末利用に関する調査結果を発表した。利用者がモバイルでの時間のほとんどをアプリに費やす一方、Webブラウザーの利用時間は減る一方であることを明らかにした。



すでに2013年に
アプリ圧勝で決着がついている

http://internet.watch.impress.co.jp/docs/news/20140402_642413.html

もう完全にアプリ中心の世界に



HOME > レポート > 調査・ホワイトペーパー

スマートフォンアプリ利用状況の分析結果を発表、アプリの利用時間がWEBブラウザの約2.5倍に(ニールセン)

2014年10月2日(木) 10時00分

「月1回以上」利用するスマホアプリは27個、「10回以上」は9個……ニールセン調べ

ニールセンは1日、スマートフォンアプリケーション(スマートフォンアプリ)の利用状況を分析した結果を発表した。

この調査は、スマートフォン視聴率情報「Nielsen Mobile NetView(モバイル・ネットビュー)」の7月データをもとにしたもの。スマホの基本機能となる、初めからインストールされている電話や電話帳、デフォルトのカメラなどのアプリは除いている。

それによると、スマートフォンの利用時間全体のうち、「アプリからの利用」と「WEBブラウザからの利用」では、アプリからの利用時間がWEBブラウザの約2.5倍となり、全体の72%を占めていた。また1人当たり月に1回以上利用するアプリ」の数は27個、「月に10回以アプリ」の数は9個だった。

月間利用回数別アプリ数 2014年7月

年代別スマホアプリ利用状況 2014年7月

1. スマホの利用時間の87%、iPadの利用時間の76%がアプリ利用に費やされる

使い易さやエクスペリエンス面を考えると、ハイブリッドアプリやHTML5をベースとしたWebアプリと比べると、モバイルユーザー向けには、まだまだダウンロード型のネイティブ型アプリが人気である。

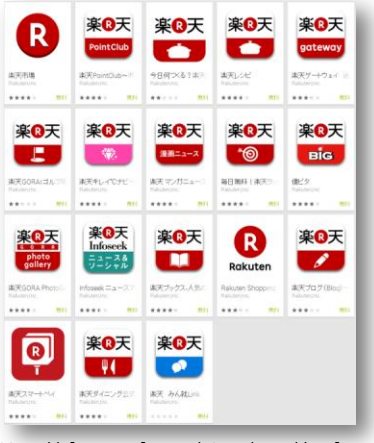
5. ビジネスのシーンにおけるモバイルアプリの利用が加速している

一般消費者向けのアプリに加え、BtoB向けアプリもどんどん増え始め、仕事でモバイルアプリを利用する事も多い。場所と時間に拘束されないモバイルアプリは新たなワークスタイルにマッチしている。実際にアメリカでは、82%のユーザーが7つ以上のモバイルアプリを仕事で活用している。

http://scan.netsecurity.ne.jp/article/2014/10/02/34929.html
http://www.fashionsnap.com/the-posts/2014-08-23/mobile/

たくさんのアプリで顧客接点を増やす積極的な企業も増えてきた

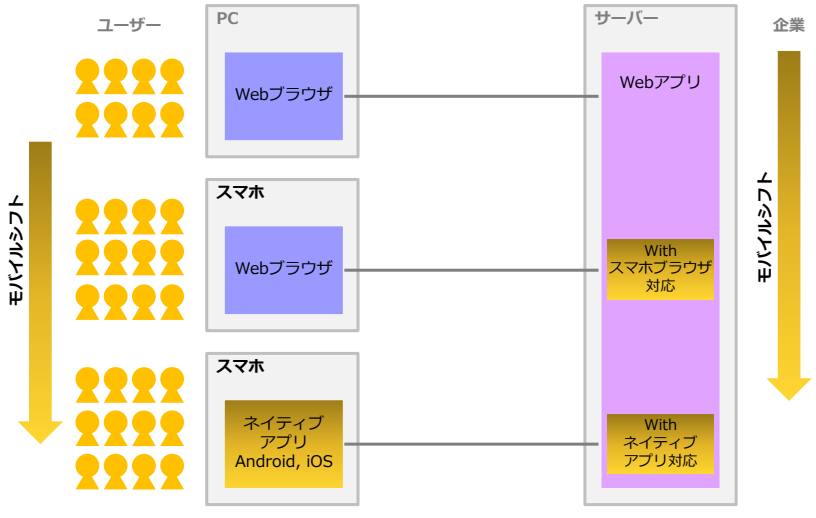
楽天株式会社



ヤフー株式会社

https://play.google.com/store/apps/developer?id=Rakuten,Inc.
https://play.google.com/store/apps/developer?id=%E3%82%BD%E3%83%95%E3%83%88%E3%83%90%E3%83%B3%E3%82%AF%E3%83%A2%E3%83%90%E3%82%A4%E3%83%AB%E6%A0%AA%E5%BC%8F%E4%BC%9A%E7%A4%BE

ユーザーが先にモバイルシフトし、企業が遅れてそれについていく状況



モバイルシフトの結果、

スマホアプリも高品質時代へ

低品質アプリがモバイルシフトを起こした

2009年頃、アイデアー発勝負の個人開発アプリやベンチャー開発アプリがスマホの人気に火をつけ、モバイルシフトの波が生じた。

この頃のアプリは低品質でよくクラッシュした。開発費も安かった。

現在、企業開発アプリが普及しアプリ品質も安定

企業がPCベースのWebシステムをスマホ対応するにあたり、企業レベルの品質でアプリを開発。

もはやアプリは安くつくれる

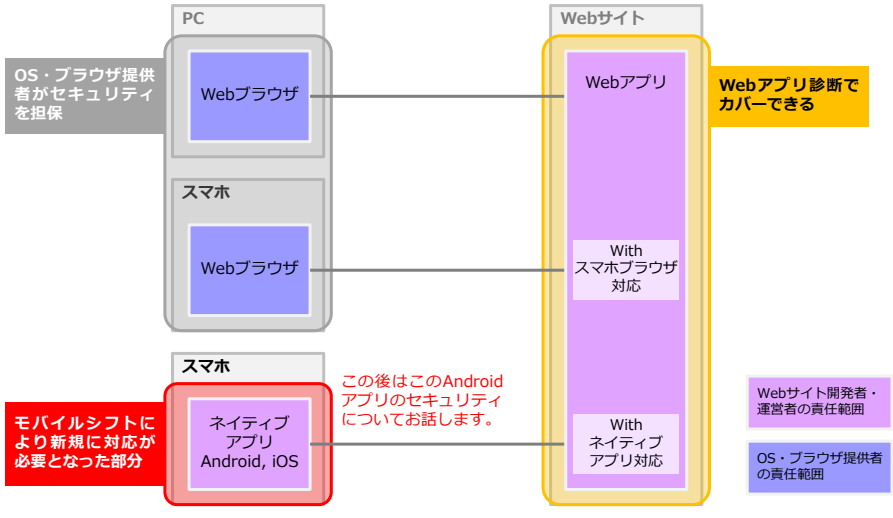
セキュリティも品質の一部として当然のように求められる。

その結果、アプリ品質 いる

- **低**品質・**低**開発費アプリ … 個人、ベンチャー企業等が開発
- **高**品質・**高**開発費アプリ … SIer、大企業等、名のある企業が開発

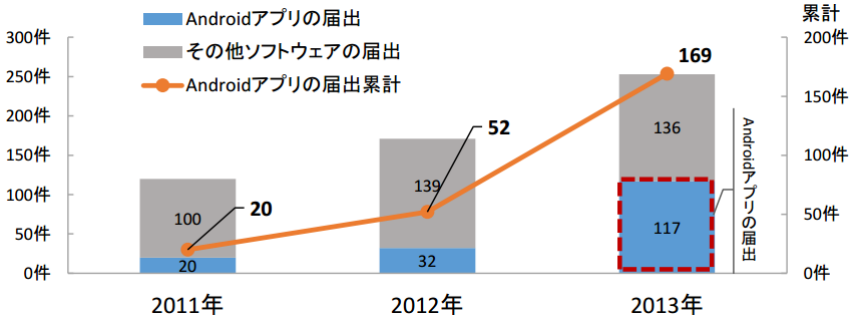
低品質アプリが多い中、高品質アプリがシェアを拡大してきている。

セキュリティ対策のカバレッジ



2013年、IPAへの Androidアプリ脆弱性の届出が急増

Androidアプリの届出件数の年別推移



http://www.ipa.go.jp/files/000036392.pdf

(JVN iPedia) 脆弱性DBに登録されたAndroidアプリの脆弱性

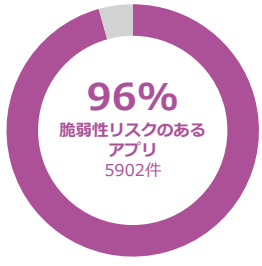
2013/08/19 Android 版 Yahoo!ショッピングにおける SSL サーバ証明書の検証不備の脆弱性
2013/08/19 ヤフオク! における SSL サーバ証明書の検証不備の脆弱性
2013/08/07 ドコモ海外利用アプリにおける接続処理に関する脆弱性
2013/06/18 サイボウズLive for Android における WebView クラスに関する脆弱性
2013/06/18 サイボウズLive for Android において任意の Java のメソッドが実行される脆弱性
2013/06/11 Galapagos Browser における WebView クラスに関する脆弱性
2013/06/11 Angel Browser における WebView クラスに関する脆弱性
2013/06/07 Android 版 ピザハット公式アプリ　宅配ピザのPizzaHut における SSL サーバ証明書の検証不備の脆弱性
2013/05/29 モバツイtouch の Content Provider にアクセス制限不備の脆弱性
2013/05/29 Sleipnir Mobile for Android におけるアドレスバー偽装の脆弱性
2013/05/27 Yahoo!ブラウザーにおけるアドレスバー偽装の脆弱性
2013/04/26 Yahoo!ブラウザーにおけるアドレスバー偽装の脆弱性
2013/04/26 Android 版 jigbrowser+ におけるアドレスバー偽装の脆弱性
2013/04/12 Sleipnir Mobile for Android において任意のエクステンション API が呼び出される脆弱性
2013/03/26 Simeji におけるアクセス制限不備の脆弱性
2013/03/26 OpenWnnフリック入力対応版におけるアクセス制限不備の脆弱性
2013/03/26 COBIME におけるアクセス制限不備の脆弱性
2013/03/26 ArtIME 日本語入力におけるアクセス制限不備の脆弱性
2013/03/29 Android 版 OpenWnn におけるアクセス制限不備の脆弱性
2013/02/14 Android 版 GREE (グリー) におけるディレクトリトラバーサルの脆弱性
2013/01/31 Android 版 ウェザーニュースタッチにおいて位置情報をログに出力する脆弱性
2012/11/04 Android 用 Groupon Redemption アプリケーションにおける SSL サーバを偽装される脆弱性
2012/11/04 Android 用 Chase Mobile Banking アプリケーションにおける SSL サーバを偽装される脆弱性

日本で開発されているであろうアプリだけに絞っています。

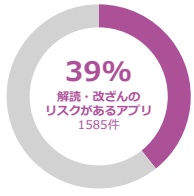
http://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&keyword=android

ほとんどのアプリがまったくセキュリティを考慮せずにつくられている

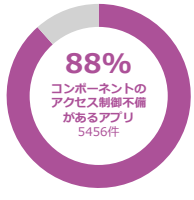
人気アプリ6170件の…



HTTPS通信するアプリの…



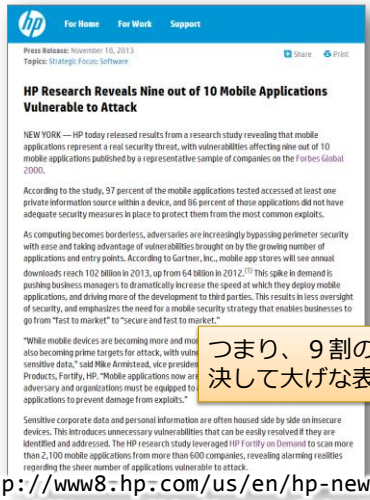
人気アプリ6170件の…

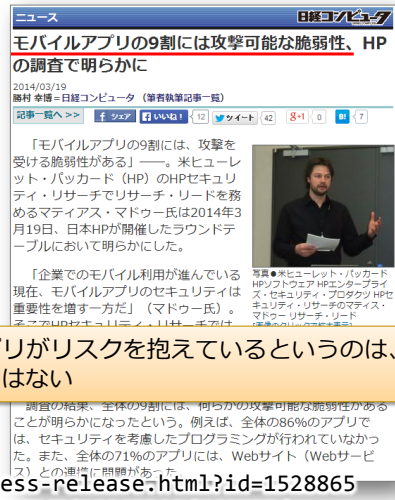


（ソニーデジタルネットワークアプリケーションズ調べ）

http://www.sonydna.com/sdna/solution/android_vulnerability_report_201310.pdf

世界的に有名なHP社も同様のレポートを公開





つまり、９割のアプリがリスクを抱えているというのは、決して大げな表現ではない

http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865
http://itpro.nikkeibp.co.jp/article/NEWS/20140319/544723/

iOSアプリにも脆弱性はある

App Store審査があるので「iOSは安全」と信じられているが、App Storeは**脆弱性**は見ていない。

ウィルス、迷惑アプリはしっかり調べている。

現状、Androidに比べればそれほど緊急性は高くない。

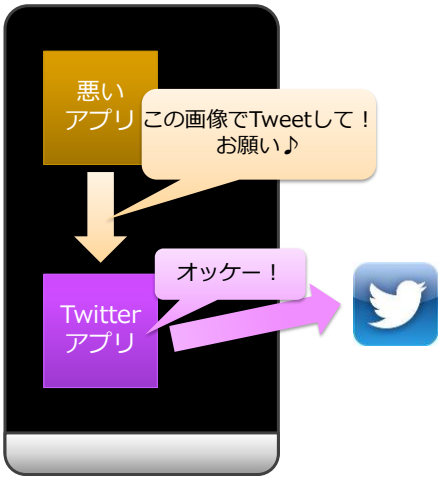
http://www.itnews.com.au/News/381803,hacker-holds-key-to-free-flights.aspx
http://www.engadget.com/2014/01/15/starbucks-app-security/
http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html

Androidアプリ脆弱性
～ よくある事例 ～

事例１

勝手にツイートされてしまうTwitterアプリ

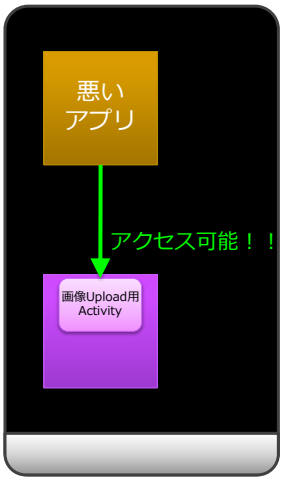
勝手にツイートされてしまうTwitterアプリ



【問題】

ユーザーが知らないうちに、端末の中のプライベートな写真が勝手にTwitterにアップロードされてしまう問題があった。

勝手にツイートされてしまうTwitterアプリ

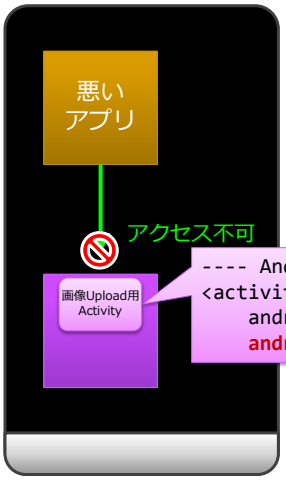


【原因】

画像アップロード用Activityが他のアプリからアクセス可能であった。

つまり他のアプリからのIntentを受理して処理してしまっていた。

勝手にツイートされてしまうTwitterアプリ



【対策】

Activityを非公開に設定する。

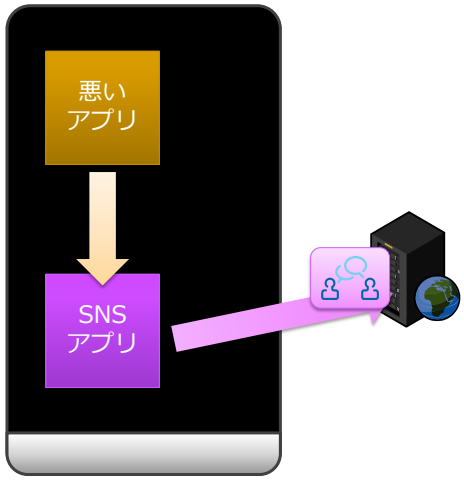
```
---- AndroidManifest.xml ----
<activity
    android:name=".UploadActivity"
    android:exported="false" >
```

⬅非公開

事例２

メッセージが盗み見られてしまうSNSアプリ

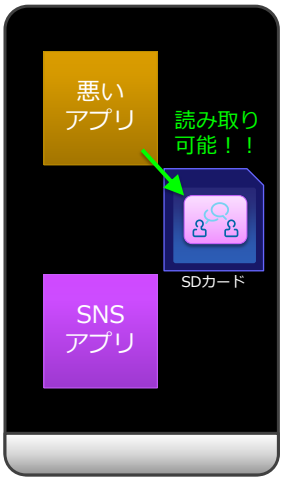
メッセージが盗み見られてしまうSNSアプリ



【問題】

アプリが一時保存したファイルの内容を他のアプリに盗み見られてしまう問題があった。

メッセージが盗み見られてしまうSNSアプリ

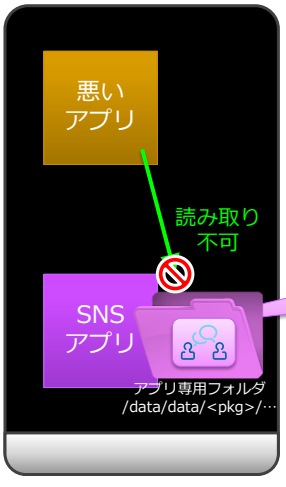


【原因】

SDカード上にファイルを作成していた。

SDカード上のファイルはすべてのアプリから読み取り可能である。

メッセージが盗み見られてしまうSNSアプリ



【対策】

アプリ専用フォルダに非公開ファイルとしてファイルを作成。

```
---- DataManager.java ----
fos = openFileOutput(FILE_NAME, MODE_PRIVATE);
```

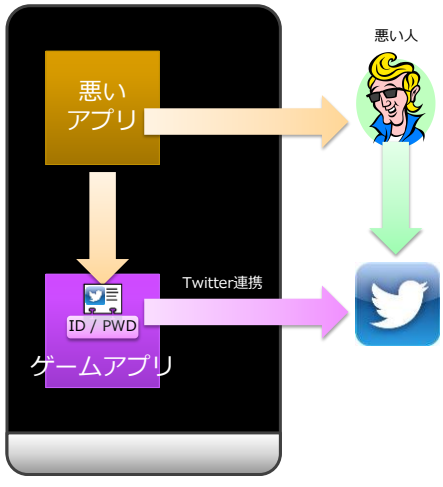
アプリ専用フォルダにファイル作成

非公開

事例３

Twitterアカウントが乗っ取られてしまうゲームアプリ

Twitterアカウントが乗っ取られてしまうゲームアプリ

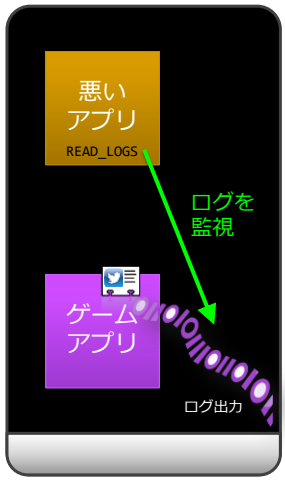


【問題】

Twitter 連 携 用 の ID/PWDが他のアプリに盗み見られてしまう問題があった。

ID/PWDが攻撃者に渡ると攻撃者がユーザーとしてTwitterにログインできた。

Twitterアカウントが乗っ取られてしまうゲームアプリ

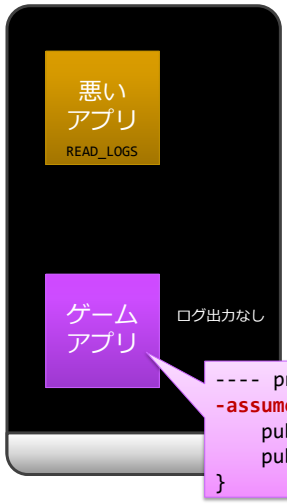


【原因】

ID/PWDをログ出力してしまっていた。

デバッグ時のログ出力を残したままアプリをリリースした。

Twitterアカウントが乗っ取られてしまうゲームアプリ



【対策】

ログ出力しない。

リリースビルドではLog.d(), Log.v()をProGuardで自動削除するなど。

```
---- proguard-project.txt ----
-assumenosideeffects class android.util.Log {
    public static int d(...);
    public static int v(...);
}
```

⬅ 削除指定

脆弱性 の 原因
～ なぜ脆弱性が多いのか ～

脆弱性 の 傾向

初歩的な問題ばかり

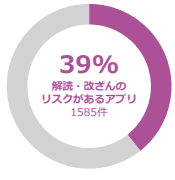
- exported
- ファイルの扱い
- ログ出力

知っていれば防げた

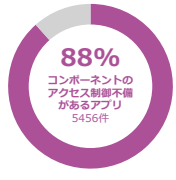
JSSEC セキュアコーディングガイドを読んでいれば防げた

何らかの脆弱性があるアプリの割合

コンポーネントが悪意あるアプリから悪用されるアプリの割合



HTTPS暗号通信が盗聴・改ざんされるアプリの割合



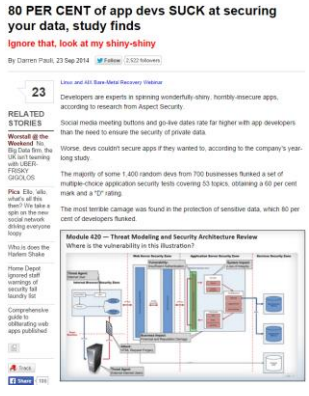
http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf

アプリ開発者、セキュリティの知識が不足

アプリ開発者の 8割は、あなたのデータをきちんと守れない

(80 PER CENT of app devs SUCK at securing your data, study finds)
http://www.theregister.co.uk/2014/09/23/app_devs_suck_at_security_says_trainer/
(The Register 9月23日)

Aspect Security社の調査で、アプリプログラマーのほとんどがセキュリティに無頓着であることが明らかになってしまいました。しかも、やる気の問題だけでなく、セキュリティに関する知識も乏しいそうです。セキュリティに関する様々なトピックについて選択式の問題を出題したところ、大事なデータの保護についての設問には 80% の回答者が不正解、脅威分析やセキュアアーキテクチャの質問には 74% が不正解、などとなっています。これでは今後ますます増えていく IoT などの製品のセキュリティ品質が危機的な状況になってしまいます。ソフトウェアのセキュリティは、できてしまった穴を探してふさぐよりも、最初から穴をできるだけ作らないようにすることが望ましいので、開発者の皆さんへのセキュリティ教育が急務です。弊社も日本スマートフォンセキュリティ協会(JSSEC)の活動などを通じてこの方面で貢献して行きたいと思います。

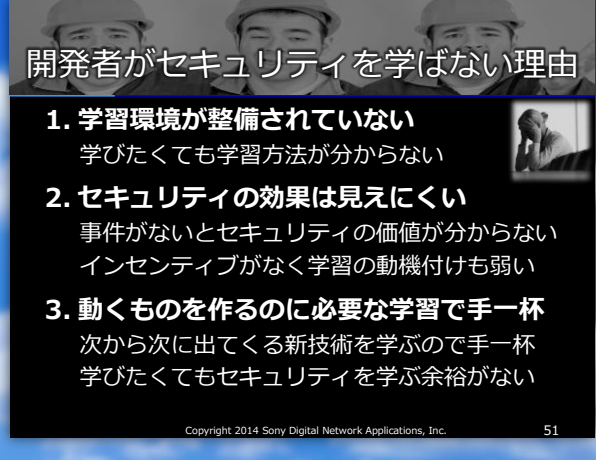


http://securityblog.sonydna.com/blog/news/20140925/
http://www.theregister.co.uk/2014/09/23/app_devs_suck_at_security_says_trainer/

開発者がセキュリティを学ばない理由

1. **学習環境が整備されていない**
   学びたくても学習方法が分からない
2. **セキュリティの効果は見えにくい**
   事件がないとセキュリティの価値が分からない
   インセンティブがなく学習の動機付けも弱い
3. **動くものを作るのに必要な学習で手一杯**
   次から次に出てくる新技術を学ぶので手一杯
   学びたくてもセキュリティを学ぶ余裕がない

すべて解決しました！



1. 学習環境の整備

知っていれば防げたというノウハウで構成されている。

Androidアプリセキュリティのノウハウ集

通称：JSSECセキュアコーディングガイド
PDF文書とセキュアなサンプルコード一式（無償）
http://www.jssec.org/report/securecoding.html
「Android セキュアコーディング」と検索

デファクトスタンダードなガイド・基準

総務省も推奨のガイド。
通信キャリアや
多くのアプリベンダーでも活用。
受入基準にするアプリ発注会社もある。

総務省 MIC Ministry of Internal Affairs and Communications

http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000043.html

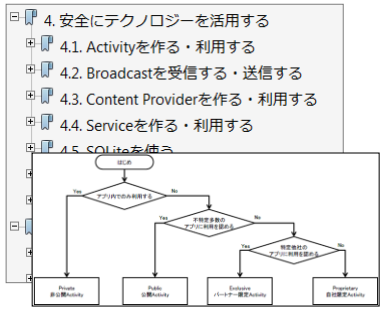
開発者が便利に使えるガイド

アプリ開発者のやりたいこと に即したセキュアな作法

- セキュアなやり方を先に説明するので、忙しい開発現場にもすぐに役立つ

コピペ歓迎！ セキュアなサンプルコード

- コピーペーストされるほどセキュアなコードが解説文も含めて社内に広まる



その始まりは 2011年11月

JSSEC技術部会にてキックオフ。ボランティアを募集して作業開始。

ガイドの歴史

年1回から2回のペースで改訂

2012年6月

28人

2012年11月

41人

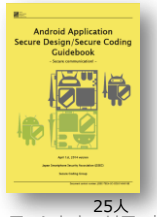
2013年4月

34人

2014年7月

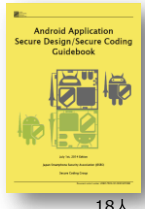
18人

2014年4月



25人

2014年8月



18人

2014年、英語版リリース

広く活用されるようになった


総務省
MIC Ministry of Internal Affairs and Communications

総務省トップ > 広報・報道 > 報道資料一覧 > スマートフォンの情報セキュリティに関する最新動向と今後の方向性

報道資料

平成25年3月29日

スマートフォンの情報セキュリティに関する最新動向と今後の方向性

【最新動向】

JSSEC のセキュアコーディンググループでは、「Android アプリのセキュア設計・セキュアコーディングガイド」初版を平成２４年６月に公表したのち、同年１１月に改訂するなど、Android 向けアプリケーションのぜい弱性の動向を踏まえた見直し・拡充等の取組を継続的に実施している。同ガイドは多くの関係者に参照されており、複数の携帯電話事業者やアプリケーション開発企業において、社内アプリケーション開発者への教育や自社提供アプリの設計・自己診断に活用されているほか、ＫＤＤＩ株式会社が運営するアプリケーション提供サイトにおいて、平成２５年３月より、提携先のアプリケーション開発者への推薦資料としても活用されるようになっている。

http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000043.html

ただ、分厚い。忙しい開発者に「コレ読んで♪」とは言えない。

400ページ超

JSSECガイドの解説DVD

ネットですぐ買えます！

http://www.contentsbrain.co.jp/jssec_dvd/
http://www.amazon.co.jp/dp/B00ECW3CG6/

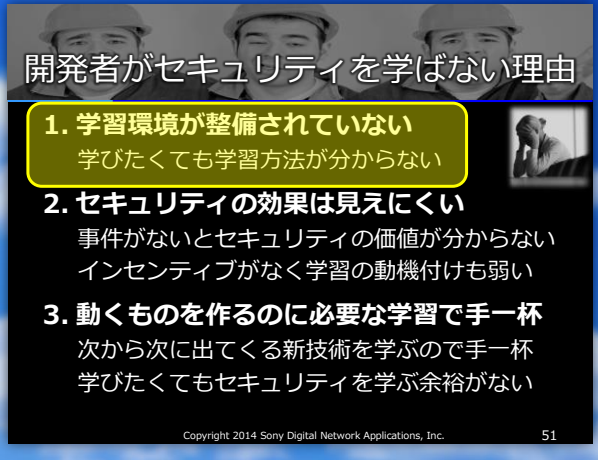
JSSECガイドの解説DVD

一通りDVDを見ると（90分）、ガイドのどこを読んでもすぐに理解できるようになります

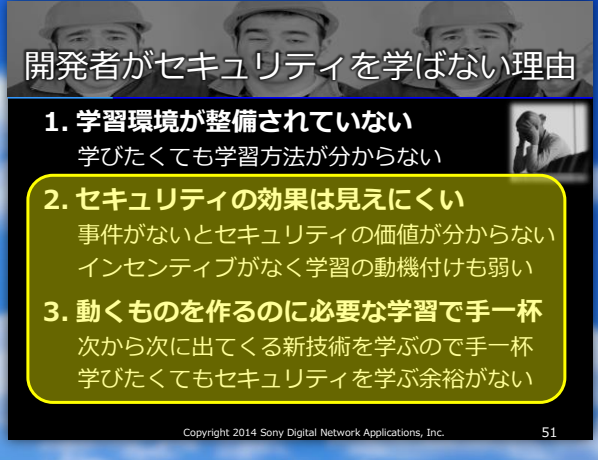
DVDで一気に学習

分かる！

1つ目を解決！



残りはソニーの立場で解決！



Secure Coding Checker

Androidアプリに特化した解析・教育ツール

【特徴】

1. 総務省推奨の基準に則った検査ツール

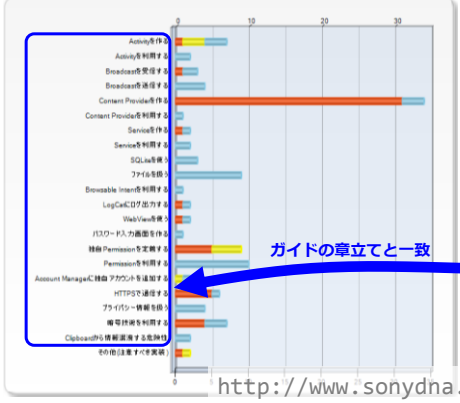
2. アプリ開発者が脆弱性を自己解決できる

アプリ完成時にはセキュアで総務省推奨基準に準拠したアプリができる！

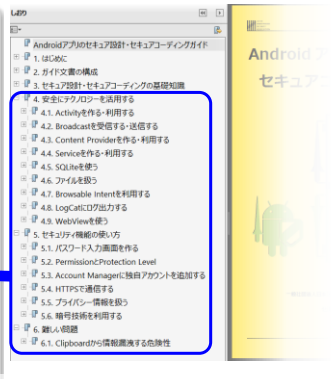
2. セキュリティの効果の可視化

アプリを自動解析して脆弱性をグラフ表示するツール

Secure Coding Checker



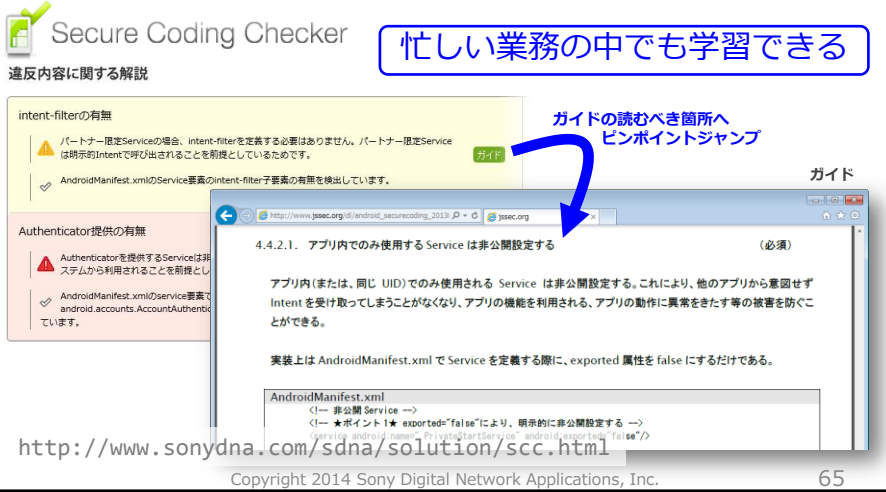
ガイド



http://www.sonydna.com/sdna/solution/scc.html

3. 動くものを作る過程でセキュリティを学習

見つかった脆弱性についてセキュリティ学習を促す

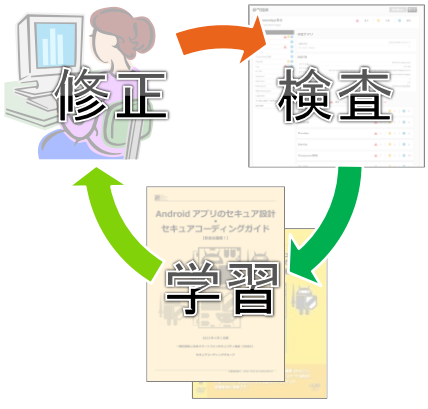


http://www.sonydna.com/sdna/solution/scc.html

セキュアなアプリを簡単に作るデモ

http://www.sonydna.com/sdna/solution/scc.html

業務を通じて良質の学習を！



【メリット１】
いまの業務に必要な最小限の学習で、学習効果がすぐに業務に活かされる

【メリット２】
見つかる問題には必ず解決方法があり、業務が滞ることがない

【メリット３】
自分のアプリの脆弱性という具体例を題材に学習できるため、理解が深まり学習効果が高い

まとめ

1.モバイルシフト

なぜスマホアプリが流行っているのかという話

2.Androidアプリの脆弱性問題

いまのアプリはとにかく無防備だという話

3.セキュアなAndroidアプリ開発法

忙しいアプリ開発者でも簡単にセキュアなアプリを作るうまいやり方があるという話