



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>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

1

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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

2

自己紹介

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

3

2000年頃、社会人4年目

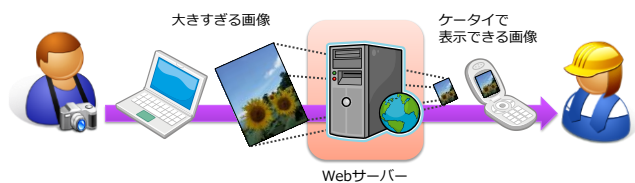
とあるメーカーで
複合機の組込技術者



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

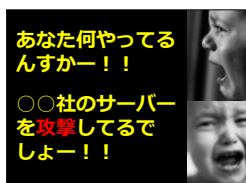


Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

4

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！

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

5

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...



Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

6

モバイルシフト

スマホアプリが流行っている理由

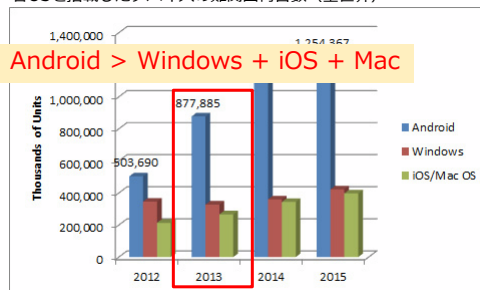
Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

7

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）



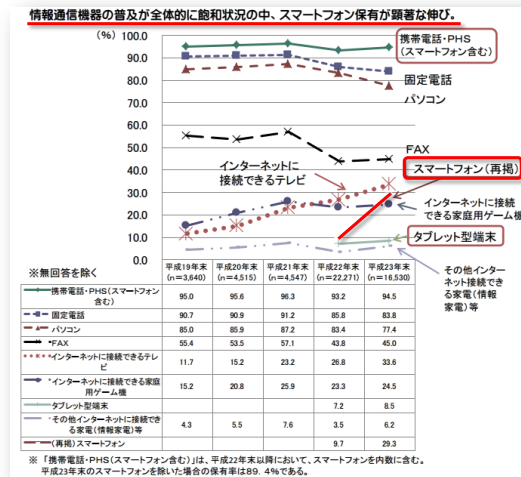
Global operating system market share based on device shipments. Source: Gartner Inc.

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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

8

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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

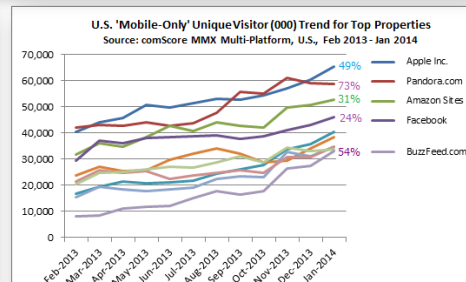
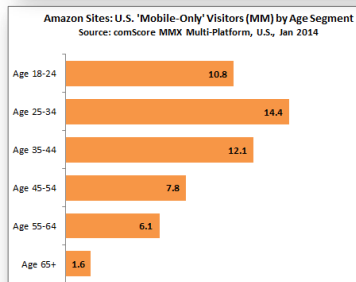
9

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/>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

10

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兼CEOの宮坂孝氏が「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。



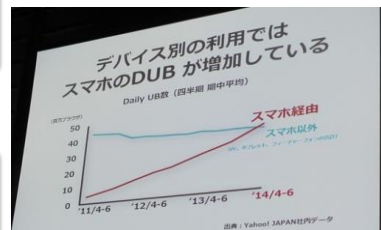
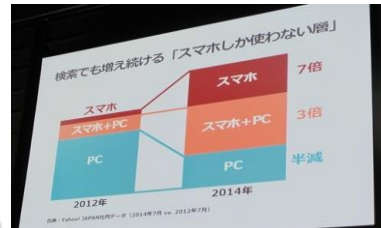
ヤフー代表取締役社長兼CEOの宮坂孝氏

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「いつか来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く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/

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

11

モバイル経由の売上が凄いい伸び率

楽天「売上高の4割がスマホから」にアプリを強化してスマホ経由売上げ拡大へ

楽天は、スマートフォン向けアプリの強化を進めている。商品目録を載せる楽天市場アプリの強化を進めている。商品目録を載せる楽天市場アプリの強化を進めている。商品目録を載せる楽天市場アプリの強化を進めている。

GMOメイクショップ、2012年のモバイルEC売上の90.1%がスマートフォン経由

GMOメイクショップは4月22日、同社の運営するネットショップ通販サービス「MakeShop」について、2012年のスマートフォン経由の売上高に関する調査結果を発表した。

米サイバーマンデーのオンライン売上高が過去最高に、モバイル経由が前年比55%増 (2/2)

サイバーマンデーにおけるモバイル端末からのトラフィックは全オンライントラフィックの31.7%で、前年から45%増えた。このうち、スマートフォンのトラフィックは全体の19.7%、タブレット端末は11.5%だった。一方で売上高の割合はスマートフォンが5.5%、これにタブレットは11.7%と、スマートフォンの倍以上あった。注文1回当たりの平均支出金額もタブレットは126.30ドルで、スマートフォンの106.49ドルを上回った。

**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/>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

12

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

FacebookのザッカーバーグCEO、「HTML5に賭けたのは失敗」 Androidアプリも間もなくネイティブに

同氏は公式iOSアプリをHTML5からネイティブに書き直した ことについて、HTML5に賭けたことはFacebookの「最大の戦略ミス」だったと認め、iOSに続けてAndroidアプリも近いうちにHTML5ではなくネイティブに移行すると語った。



激動のスマホゲーム業界「ネイティブアプリ」の権威と敗路に立たされるソーシャルゲーム



<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！



スマホブラウザが対応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



Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

17

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…

🔔 新着通知が1件 あります。



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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

18

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	アプリ	アプリが管理する情報資産
端末の電話番号	Eメール	メアド、送受信メール本文、添付…
電話帳	SMS	送受信SMSメッセージ本文…
通話履歴（受発信の日時や番号）	Webブラウザ	ブックマーク、閲覧履歴、クッキー…
IMEI（端末固有ID）、IMSI（回線契約者ID）	カレンダー	予定、ToDo、イベント…
位置情報（GPS、WiFi、基地局…）	家計簿	残高、買い物履歴…
アカウント情報（Googleアカウント…）	Facebook	アカウント、コンテンツ…
メディアデータ（写真、動画、音楽、録音…）	Twitter	アカウント、コンテンツ…
インストールアプリ一覧	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	アプリ	アプリが管理する情報資産
端末の電話番号	Eメール	メアド、送受信メール本文、添付…
電話帳	SMS	送受信SMSメッセージ本文…
通話履歴（受発信の日時や番号）	Webブラウザ	ブックマーク、閲覧履歴 、クッキー…
IMEI（端末固有ID）、IMSI（回線契約者ID）	カレンダー	予定、ToDo、イベント…
位置情報（GPS、WiFi、基地局…）	家計簿	残高、買い物履歴…
アカウント情報（Googleアカウント…）	Facebook	アカウント、コンテンツ…
メディアデータ（写真、動画、音楽、録音…）	Twitter	アカウント、コンテンツ…
インストールアプリ一覧	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ージャー	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、同僚関係、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

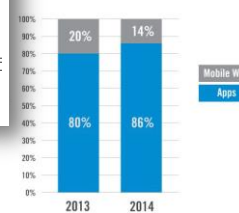
(2014/4/2 10:34)

g+ 11 8+ 70 ツイート 184 いいね! 192

米モバイルデータ解析企業のFlurry(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

Continue to Dominate the Mobile Web



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8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回以上アプリ」の数は8個だった。

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/>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

23

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



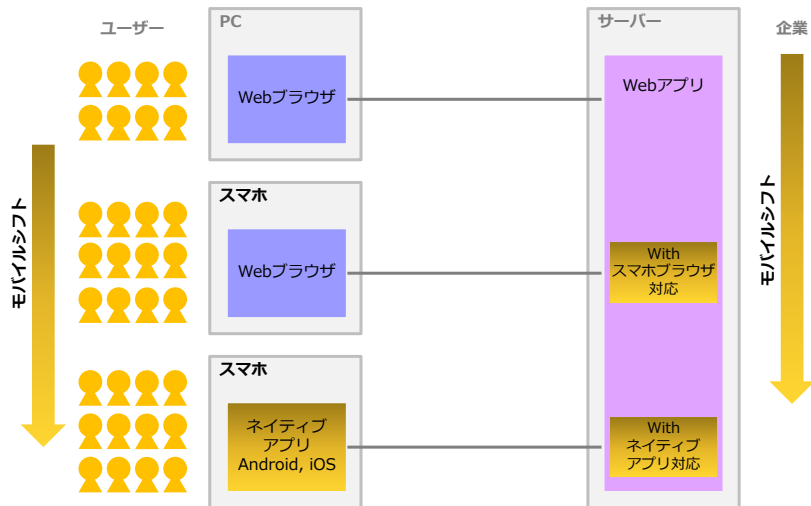
<https://play.google.com/store/apps/developer?id=Rakuten,Inc.>

<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>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

24

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



Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

25

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。

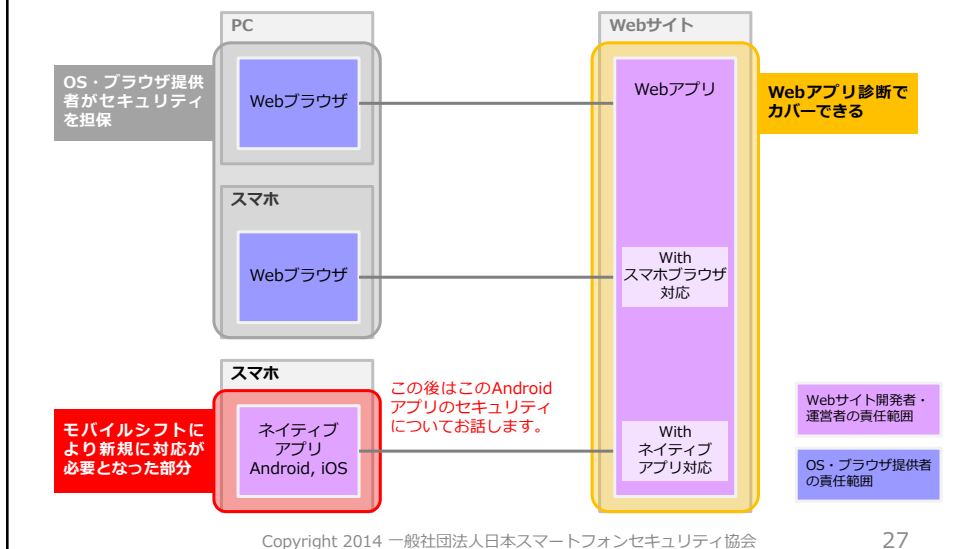
その結果、アプリ品質も安定している

- ・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。

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

26

セキュリティ対策のカバレッジ



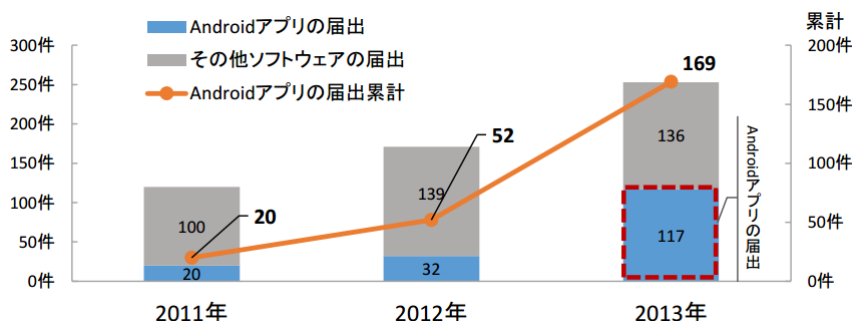
27

Androidアプリの脆弱性問題

28

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>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

29

(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 ビザハット公式アプリ 宅配ビザの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!ブラウザにおけるアドレスバー偽装の脆弱性
2013/04/26 Yahoo!ブラウザ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
2013/04/26 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 (グリーン) におけるディレクトリトラバーサル脆弱性
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

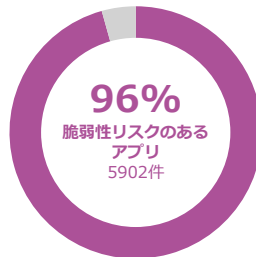
Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

30

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



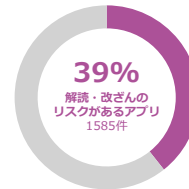
人気アプリ6170件の…



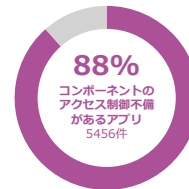
(ソニーデジタルネットワークアプリケーションズ調べ)

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

HTTPS通信するアプリの…



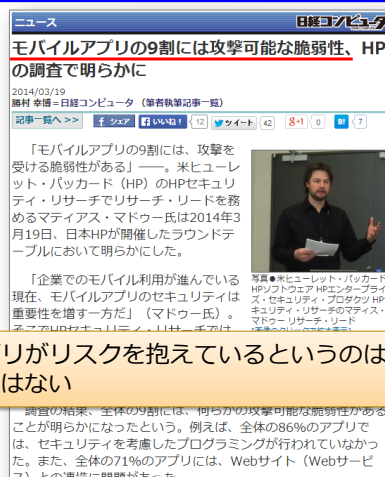
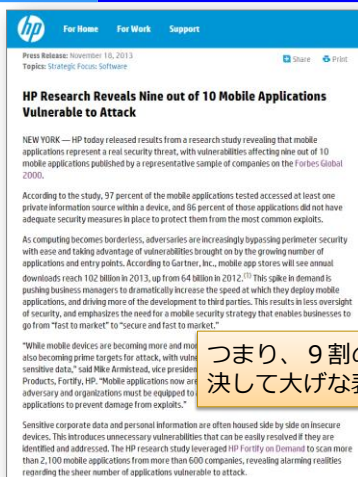
人気アプリ6170件の…



Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

31

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/>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

32

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**は見えていない。
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>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

33

Androidアプリ脆弱性 ～ よくある事例 ～

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

34

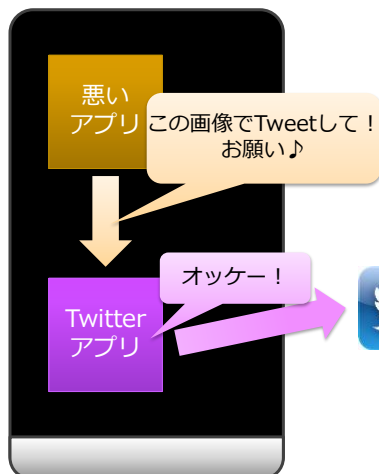
事例 1

勝手にツイートされて しまうTwitterアプリ

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

35

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。

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

36

勝手にツイートされてしまうTwitterアプリ

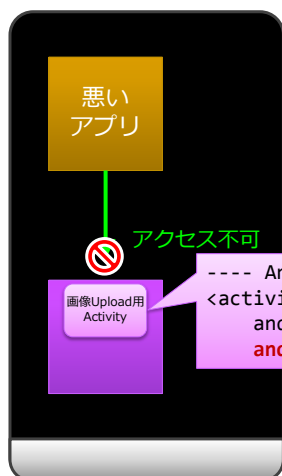


【原因】

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

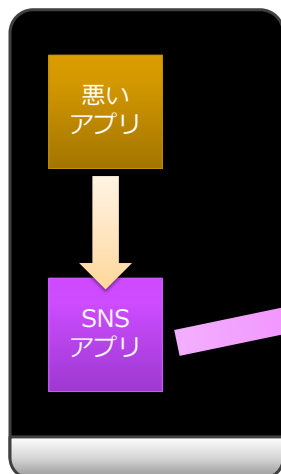
Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

39

メッセージが盗み見られてしまうSNSアプリ

【問題】

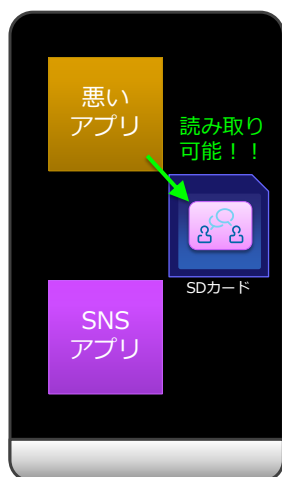
アプリが一時保存したファイルの内容を他のアプリに盗み見られてしまう問題があった。



Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

40

メッセージが盗み見られてしまうSNSアプリ

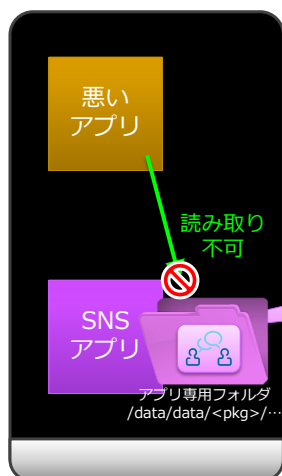


【原因】

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

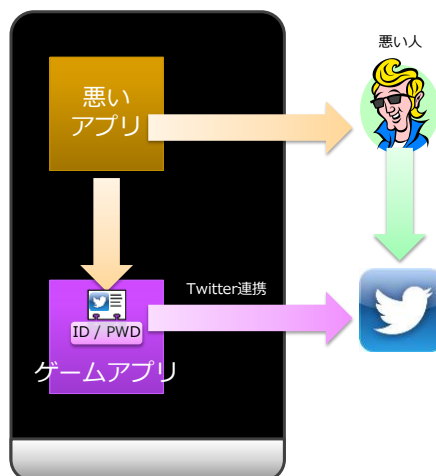
事例 3

Twitterアカウントが 乗っ取られてしまう ゲームアプリ

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

43

Twitterアカウントが乗っ取られてしまうゲームアプリ



【問題】

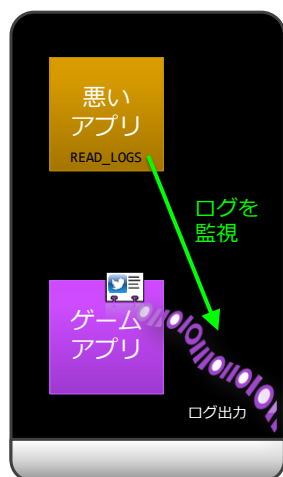
Twitter 連 携 用 の
ID/PWDが他のアプ
リに盗み見られてし
まう問題があった。

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。

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

44

Twitterアカウントが乗っ取られてしまうゲームアプリ

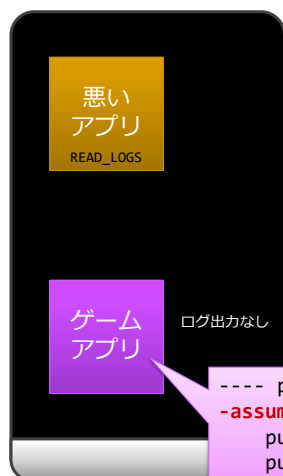


【原因】

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 ～

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

47

脆弱性の傾向

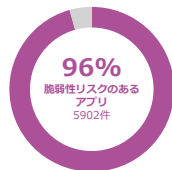
初歩的な問題ばかり

- exported
- ファイルの扱い
- ログ出力

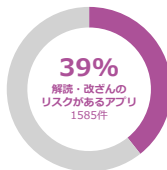
知っていれば防げた

JSSEC セキュアコーディングガイドを読んでいたれば防げた

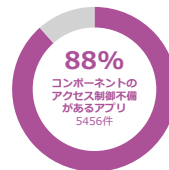
何らかの脆弱性があるアプリの割合



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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

48

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えます。

<http://securityblog.sonydna.com/blog/news/20140925/>

http://www.theregister.co.uk/2014/09/23/app_devs_suck_at_security_says_trainer/

80 PER CENT of app devs SUCK at securing your data, study finds

Ignore that, look at my shiny-shiny

By Darren Park, 23 Sep 2014

Follow 5,522 followers

23 Likes and 461 Retweets

Developers are experts in spinning wonderfully shiny, horribly insecure apps, according to research from Aspect Security.

Social media meeting before and go live dates are far higher with app developers than the need to ensure the security of private data.

Worse, devs couldn't secure apps if they wanted to, according to the company's year-long study.

The majority of some 1,400 random devs from 750 businesses flunked a set of multiple-choice application security tests covering 53 topics, obtaining a 60 per cent mark and a "C" rating.

The most terrible carnage was found in the protection of sensitive data, which 80 per cent of developers flunked.

Module 420 - Threat Modeling and Security Architecture Review

Where is the vulnerability in this illustration?

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

Who is doing the Hackers Shake

Home Depot opened call center, all security fail hourly fail

Comprehensive guide to obtaining web apps published

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



セキュアな Androidアプリ開発法

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

51

すべて解決しました！

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



Copyright 2014 Sony Digital Network Applications, Inc.

51

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

52

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。



http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_0200043.html

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

53



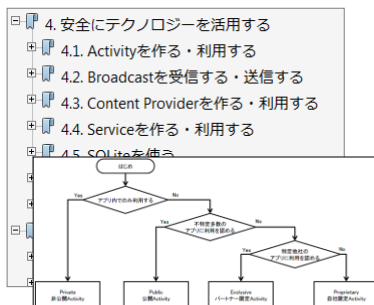
開発者が便利に使えるガイド

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

コピー歓迎！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



```
AndroidManifest.xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.privacynotify"
    android:versionCode="1"
    android:versionName="1.0">

    <uses-sdk android:minSdkVersion="8" />

    <!-- ★ポイント1★ taskAffinity を用いてアフィニティを指定しない -->
    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name">

        <!-- ★ポイント2★ Activity に taskAffinity を指定せず、値をデフォルトのまま "standard" とする -->
        <activity
            android:name=".PrivacyNotifyActivity"
            android:label="@string/app_name">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>

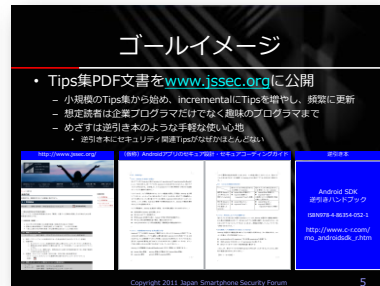
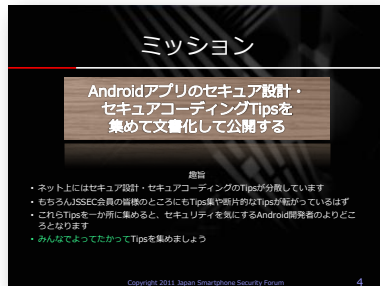
        <!-- 非公開 Activity -->
        <!-- ★ポイント1★ taskAffinity を用いてアフィニティを指定しない -->
        <!-- ★ポイント2★ Activity に taskAffinity を指定せず、値をデフォルトのまま "standard" とする -->
        <!-- ★ポイント3★ exported="false"により、明示的に非公開設定する -->
        <activity
            android:name=".PrivacyNotifyActivity"
            android:label="@string/app_name"
            android:exported="false">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

54

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



広く活用されるようになった

総務省
MIC
Ministry of Internal Affairs
and Communications

Google "カスタム検索" サイ内 関連サイト
ここに検索語句を入力 検索

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く。

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

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会 57

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/>

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

59

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

1. はじめに.....
 - 1.1. スマートフォンを安心して利用出来る社会へ.....
 - 1.2. 常にβ版でタイムリーなフィードバックを.....
 - 1.3. 本文書の利用許諾.....
 - 1.4. 2012年11月1日版からの訂正記事について.....
2. ガイド文書の構成 ... **DVDで一気に学習**
 - 2.1. 開発者コンテキスト.....
 - 2.2. サンプルコード、ルールブック、アドバンスト.....
 - 2.3. ガイド文書のスコープ.....
 - 2.4. Androidセキュアコーディング関連書籍の紹介.....
 - 2.5. サンプルコードのEclipseへの取り込み手順.....
3. セキュア設計・セキュアコーディングの基礎知識.....
 - 3.1. Androidアプリのセキュリティ.....
 - 3.2. 入力データの安全性を確認する.....
4. 安全にテクノロジーを活用する.....
 - 4.1. Activityを作る・利用する.....

分かる！

- 4.2. Broadcastを受信する・送信する.....
- 4.3. Content Providerを作る・利用する.....
- 4.4. Serviceを作る・利用する.....
- 4.5. SQLiteを使う.....
- 4.6. ファイルを扱う.....
- 4.7. Browsable Intentを利用する.....
- 4.8. LogCatにログ出力する.....
- 4.9. WebViewを使う.....
5. セキュリティ機能の使い方.....
 - 5.1. パスワード入力画面を作る.....
 - 5.2. PermissionとProtection Level.....
 - 5.3. Account Managerに独自アカウントを追加する.....
 - 5.4. HTTPSで通信する.....
6. 難しい問題.....
 - 6.1. Clipboardから情報漏洩する危険性.....

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

60

1つ目を解決！

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

Copyright 2014 Sony Digital Network Applications, Inc.

51

Copyright 2014 一般社団法人日本スマートフォンセキュリティ協会

61

残りはソニーの立場で解決！

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

Copyright 2014 Sony Digital Network Applications, Inc.

51

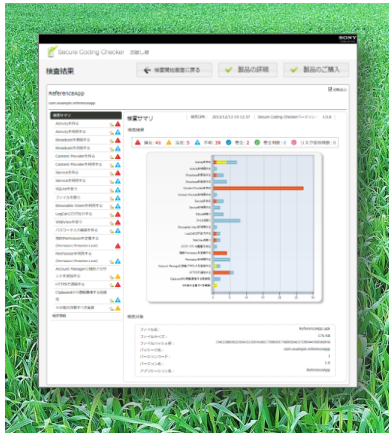
Copyright 2014 Sony Digital Network Applications, Inc.

62



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！



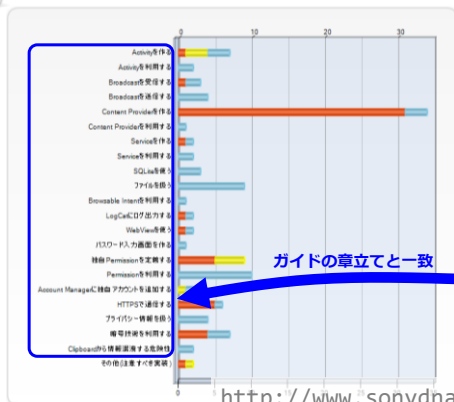
2. セキュリティの効果の可視化

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



- Androidアプリのセキュア設計・セキュアコーディングガイド
- 1. はじめに
- 2. 54件の文書の構成
- 3. セキュア設計・セキュアコーディングの基礎知識
- 4. 安全にアプリ/ロガーを適用する
- 4.1. Activityを作る・利用する
- 4.2. Broadcastを受信する・送信する
- 4.3. Content Providerを作る・利用する
- 4.4. Serviceを作る・利用する
- 4.5. SQLiteを使う
- 4.6. ファイルを使う
- 4.7. Broadcast Intentを利用する
- 4.8. LogCatに出力する
- 4.9. WebViewを使う
- 5. セキュア機能の使い分け
- 5.1. JKS/ロード入力量を高める
- 5.2. Permission Protection Level
- 5.3. Account Managerに独自アカウントを追加する
- 5.4. HTTPSで通信する
- 5.5. ファイバー・接続を使う
- 5.6. 暗号技術を利用する
- 6. 基本知識
- 6.1. Clipboardから情報漏洩する危険性



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

セキュリティを 3. 動くものを作る過程で学習

見つけた脆弱性についてセキュリティ学習を促す



Secure Coding Checker

違反内容に関する解説

忙しい業務の中でも学習できる

intent-filterの有無

パートナー指定Serviceの場合、intent-filterを定義する必要はありません。パートナー指定Serviceは明示的Intentで呼び出されることを前提としているためです。

AndroidManifest.xmlのService要素のintent-filter子要素の有無を検出しています。

Authenticator提供の有無

Authenticatorを提供するServiceは非公開から利用されることを前提として、AndroidManifest.xmlのService要素でandroid.accounts.AccountAuthenticatorActivityを指定する必要があります。

ガイドの読むべき箇所へ
ピンポイントジャンプ

ガイド

4.4.2.1. アプリ内でのみ使用する Service は非公開設定する (必須)

アプリ内(または、同じ UID)でのみ使用される Service は非公開設定する。これにより、他のアプリから意図せず Intent を受け取ってしまうことがなくなり、アプリの機能を利用される、アプリの動作に異常をきたす等の被害を防ぐことができる。

実装後は AndroidManifest.xml で Service を定義する際に、exported 属性を false にするだけである。

```
AndroidManifest.xml
<!-- 非公開 Service -->
<!-- ★ポイント1★ exported="false"により、明示的に非公開設定する -->
<service android:name="PrivilegedService" android:exported="false"/>
```

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

Copyright 2014 Sony Digital Network Applications, Inc.

65

セキュアなアプリを簡単に作るデモ

SONY

Sony Digital Network Applications, Inc.

会社概要 | 採用情報



ソリューション

製品情報

お知らせ

お問い合わせはこちら

セキュアコーディングチェッカー Secure Coding Checker

Androidアプリケーション脆弱性チェックツール

～ 開発中のAndroidアプリの脆弱性を指摘し、修正方法を表示 ～



開発者のメリットはこちら



発注者のメリットはこちら

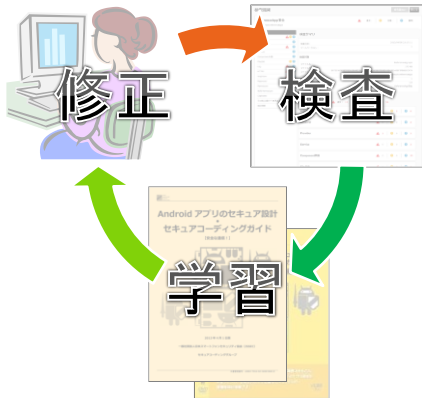


<http://www.sonydna.com/sdna/solution/scc.html>

Copyright 2014 Sony Digital Network Applications, Inc.

66

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

