今日の話題

1. **IoTとAndroid**
   IoTでAndroid OSが採用される
2. **Androidの脆弱性問題を振り返る**
   脆弱性とはどのようなもので、どのような原因で生じるのか
3. **IoTセキュリティの悪寒**
   歴史を振り返り、今後のIoTセキュリティを考える
4. **IoT時代に備えよう、Androidセキュリティ技術**
   Androidなら、IoTにも活用できる良いセキュリティ対策がある

IoTとAndroid

IoTでAndroid OSが採用される

モノのインターネット

IoT（Internet of Things）

これまでインターネットはPCや携帯などいわゆるコンピュータ的なものが接続するネットワークとされてきたが、これからはありとあらゆるモノがインターネットに繋がってさまざまな新しいサービスを実現していく。このような現象にInternet of Thingsと名前が付けられた。

スマホで色や明るさを変えられるライト

スマホで制御できるコンセント

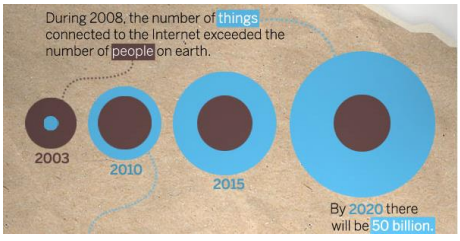
屋外の気温、湿度、気圧を継続観測

植物の状態を監視・診断し、適切にアドバイス

さまざまなアイデア商品が市場を賑わし始めてきており、IoTがポストスマートフォンの有力候補だと言われるようになってきた。

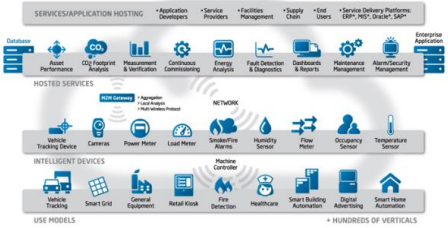
http://www.exchangewire.jp/2014/01/24/wirecolumn-thinkjam-arai-maeda-5/
http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/
http://www.netatmo.com/ja-JP/product/station

IoTデバイスが凄い勢いで増える



すでに2008年にはIoTデバイスの数が人類の全人口を超えた

2020年には500億台を超える勢い



家庭から社会までいたるところにIoTデバイスが浸透して人類の生活が豊かなものになる

http://readwrite.com/2011/07/17/cisco_50_billion_things_on_the_internet_by_2020
http://www.trentonsystems.com/applications/machine-to-machine

UIを持つIoTデバイスではAndroid採用が進む

1. Androidは安定したOSであり無料で手に入る
2. 大量のアプリ資産もIoTデバイスに活かせる
3. Android OSはIoTデバイスに合わせて自由にカスタマイズできる
4. Android OSは既に主要な技術をサポートしている
5. Android OSはwatchからTVまで大小様々なプラットフォームに対応している
6. Java/Androidのプログラマは既に大量にいるので人材調達に困らない

http://www.hsc.com/research-innovation/newsletter/issue-1/android-internet-of-things
http://gpad.tv/develop/pioneer-cycle-android/
http://monoist.atmarkit.co.jp/mn/articles/1305/15/news030.html
http://gpad.tv/develop/seraku-smart-plantfactory/
http://www.ys-consulting.com.tw/news/46043.html

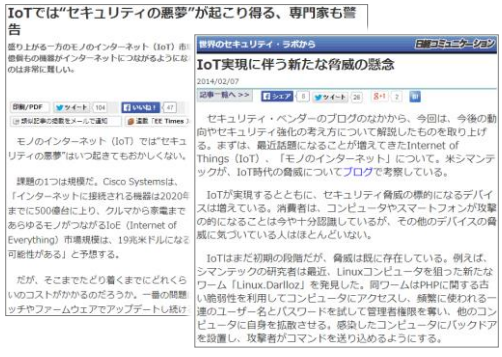
Android搭載
サイクルコンピュータ

Android搭載カーナビ

Android搭載スマート野菜工場

IoT最大の懸念事項はセキュリティ

多くの専門家が警鐘を鳴らしている


IoTでは“セキュリティの悪夢”が起こり得る、専門家も警告

モノのインターネット（IoT）では“セキュリティの悪夢”はいつ起きてもおかしくない。

課題の1つは規模だ。Cisco Systemsは、「インターネットに接続される機器は2020年までに500億台に上り、クルマから家電まであらゆるモノがつながるIoE（Internet of Everything）市場規模は、19兆米ドルになる可能性がある」と予想する。

だが、そこまでたどり着くまでにどれくらいのコストがかかるのだろうか。一番の問題はパッチやファームウェアでアップデートし続け

世界のセキュリティ・ラボから

IoT実現に伴う新たな脅威の懸念

2014/02/07

セキュリティ・ベンダーのブログのなかから、今回は、今後の動向やセキュリティ強化の考え方について解説したものを取り上げる。まずは、最近話題になることが増えてきたInternet of Things（IoT）、「モノのインターネット」について。米シマンテックが、IoT時代の脅威についてブログで考察している。

IoTが実現するとともに、セキュリティ脅威の標的になるデバイスは増えている。消費者は、コンピュータやスマートフォンが攻撃の的になることは今や十分認識しているが、その他のデバイスの脅威に気づいている人はほとんどいない。

IoTはまだ初期の段階だが、脅威は既に存在している。例えば、シマンテックの研究者は最近、Linuxコンピュータを狙った新たなワーム「Linux.Darlloz」を発見した。同ワームはPHPに関する古い脆弱性を利用してコンピュータにアクセスし、繰り返しの一連のユーザー名とパスワードを試して管理者権限を奪い、他のコンピュータに自身を拡散させる。感染したコンピュータにバックドアを設置し、攻撃者がコマンドを送り込めるようにする。


IoT端末の70%に脆弱性--ヒューレット・パッカードが警鐘

Larry Dignan（ZDNet.com） 翻訳校正： 編集部 2014年07月30日 09時40分

センサーやコネクテッドインフラストラクチャを含むモノのインターネット（IoT）端末の70%に、悪用につながり得る脆弱性が存在すると、Hewlett-Packard（HP）が指摘する。

HPのFortify部門が、最も普及しているIoT端末10種（テレビ、ウェブカメラ、サーモスタット、リモート電源管理ユニット、スプリンクラー制御装置、ドアロック、住宅用警報機、ガレージ開閉機など）を調査した結果、1端末あたり平均25の脆弱性があることが分かった。

レポートで明かされた論点は以下の通り。

- クラウドアプリやモバイルアプリを含む端末の80%が、堅牢なパスワードを要求しない。
- 端末の8割が、プライバシー上問題があるという足るだけの情報を収集している。
- 通信を暗号化しない端末が7割、ソフトウェアアップデートの取得に暗号化を利用しない端末が6割存在した。

http://eetimes.jp/ee/articles/1404/04/news073.html
http://itpro.nikkeibp.co.jp/article/COLUMN/20140205/534564/
http://japan.zdnet.com/article/35051569/

IoTが実際に攻撃できる事例も


テスラの電気自動車に遠隔ハッキング

2014/08/07

記事一覧へ >>

98 2 5 13 31

おすすめ 共有 ブックマーク Pocket ツイート シェア

世界のセキュリティ・ベンダーのブログから、興味深い記事を紹介する。今回はInternet of Things（IoT）関連の話題を3本紹介する。このところ、IoTのセキュリティが取り上げられるケースが目立ってきている。

最初に紹介するのは、電気自動車のハッキング実験に関する話題。中国の研究チームが、米テスラモーターズの「Model S」のハッキング実験に成功した。スロバキアのイーセットがブログで紹介している。遠隔操作でドアやサンルーフの開閉、ヘッドライトの点灯、クラクションの鳴動を実行したという。

ブログによると、このハッキングは、セキュリティカンファレンス「SyScan」で行われたコンテストの一環。同研究チームは、ドアロックやワイパー、ライトなどのシステム制御を乗っ取り、賞金の1万ドルを獲得した。同チームは攻撃方法の詳細を明らかにしていない。

テスラはコンテストの公式スポンサーではないが、責任あるセキュリティ研究者の力を借りて潜在的脆弱性を特定するという主旨に賛同し、「今後、問題の脆弱性を調査する」としている。これまでも複数のセキュリティ研究者がさまざまなネット接続可能な車両へのハッキングを実証してきたが、動いている車両に対する無線経由の攻撃はほとんどなかった。


Hikvision製のDVRに深刻な脆弱性、IoTデバイスは「90年代のOS状態」

HikvisionのDVRに脆弱性がみつかり、「モノのインターネット」製品に見つかる脆弱性は、90年代のOSやサーバの脆弱性を彷彿とさせると米SANS Internet Storm Center。

[鈴木聖子，ITmedia]

印刷/PDF ツイート 22 いいね！ 32 チェック 0 Pocket 8 通知

PR バチカン図書館がCIO来日 約4千万ページのデジタル文献化事業
PR 無料トライアル実施中－クラウド版プロジェクト管理ツール

セキュリティ企業のRapid7は、監視カメラや入退室管理システムを手掛ける中国Hikvision製のデジタルビデオレコーダー（DVR）に、リモートからコードを実行されてしまう脆弱性が複数見つかったと伝えた。パッチはまだ公開されておらず、同社は脆弱性検査ツールMetasploitにこの脆弱性を突くモジュールを追加した。

Rapid7の11月19日のブログによると、Hikvisionの「DS-7204」などのモデルで、RTSPリクエストの処理コードにバッファオーバーフローの脆弱性が3件見つかった。悪用された場合、リモートの攻撃者にDVRを完全に制御される恐れがあるという。

脆弱性問題を指摘されたHikvision

Hikvisionの製品には今回の脆弱性のほかにも別の脆弱性が指摘されていたが、Rapid7はこの脆弱性もまだ修正されていないことを確認したとしている。さらに、同社製品のデフォルトの管理者アカウントに「admin」「12345」という安易なユーザー名とパスワードが使われている問題も以前から指摘されていた。

この問題についてRapid7は2014年9月にHikvisionに報告したが、まだ返答はないという。パッチが公開されるまでは、HikvisionのDVRなどの製品を無防備な状態でインターネットに接続しないようRapid7は呼び掛けている。

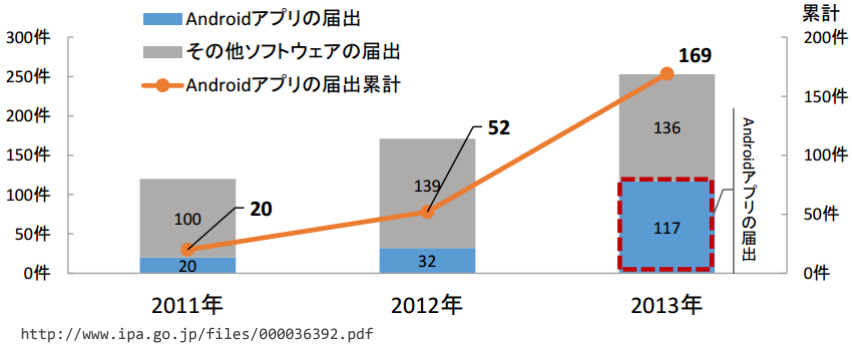
http://itpro.nikkeibp.co.jp/atcl/column/14/264220/080500006/
http://www.itmedia.co.jp/enterprise/articles/1411/25/news056.html

Androidの脆弱性問題を振り返る

脆弱性とはどのようなもので、どのような原因で生じるのか

2013年、Androidアプリの脆弱性の届出が急増

- セキュリティ研究者が脆弱性を発見するとIPAに届け出する仕組みがある
- モバイルの市場拡大に伴い、アプリの脆弱性が多数届け出られている



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

届け出されたアプリの脆弱性は公表される

- アプリの脆弱性はJVN iPediaというデータベースに登録公開され、誰でも検索可能
- 企業のブランドイメージにも影響がある

・・・
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・・・
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 Android 版 jigbrowser+ におけるアドレスバー偽装の脆弱性
・・・

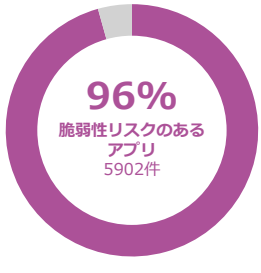
http://jvndb.jvn.jp/search/index.php?mode=_vulnerability_search_IA_VulnSearch&lang=ja&keyword=android

アプリの96%は セキュリティを考慮せずにつくられている

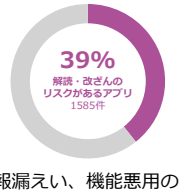
- 人気アプリ6170件を集めて、脆弱性を調べてみたところ

Androidアプリ脆弱性調査レポート

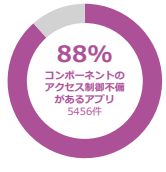
何らかの脆弱性がある アプリの割合



暗号通信が破られる アプリの割合



情報漏えい、機能悪用の リスクがあるアプリの割合



（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

世界的に有名なセキュリティ研究機関のあるHP社も同様のレポートを公開

- 決して大げさな話ではなく、
  アプリの脆弱性は誰もケアしていないという現実

For Home For Work Support

Press Release: November 18, 2013
Topics: Strategic Focus: Software

Share Print

HP Research Reveals Nine out of 10 Mobile Applications Vulnerable to Attack

NEW YORK — HP today released results from a research study revealing that mobile applications represent a real security threat, with vulnerabilities affecting nine out of 10 mobile applications published by a representative sample of companies on the Forbes Global 2000.

According to the study, 97 percent of the mobile applications tested accessed at least one private information source within a device, and 86 percent of those applications did not have adequate security measures in place to protect them from the most common exploits.

As computing becomes borderless, adversaries are increasingly bypassing perimeter security with ease and taking advantage of vulnerabilities brought on by the growing number of applications and entry points. According to Gartner, Inc., mobile app stores will see annual downloads reach 102 billion in 2013, up from 64 billion in 2012.[1] This spike in demand is pushing business managers to dramatically increase the speed at which they deploy mobile applications, and driving more of the development to third parties. This results in less oversight

ニュース 日経コンピュータ

モバイルアプリの9割には攻撃可能な脆弱性、HPの調査で明らかに

2014/03/19
勝村 幸博＝日経コンピュータ （筆者執筆記事一覧）

記事一覧へ >> シェア いいね！ 12 ツイート 42 +1 0 B! 7

「モバイルアプリの9割には、攻撃を受ける脆弱性がある」――。米ヒューレット・パッカード（HP）のHPセキュリティ・リサーチでリサーチ・リードを務めるマティアス・マドゥー氏は2014年3月19日、日本HPが開催したラウンドテーブルにおいて明らかにした。

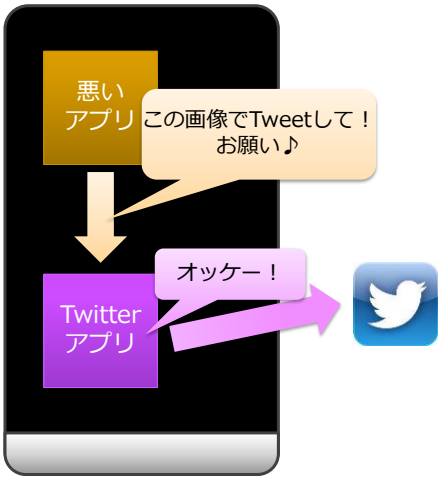
「企業でのモバイル利用が進んでいる現在、モバイルアプリのセキュリティは重要性を増す一方だ」（マドゥー氏）。そこでHPセキュリティ・リサーチでは、

写真●米ヒューレット・パッカード HPソフトウェア HPエンタープライズ・セキュリティ・プロダクツ HPセキュリティ・リサーチのマティス・マドゥー リサーチ・リード
[画像のクリックで拡大表示]

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

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

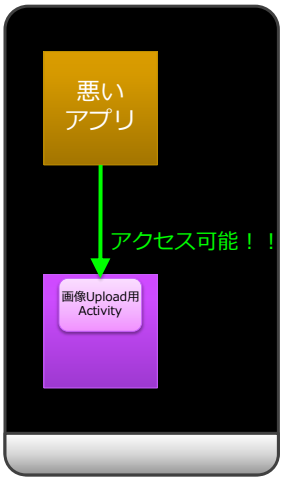


【問題】

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。

つまりプライベートな情報の漏えいが発生。

勝手にツイートされてしまうTwitterアプリ

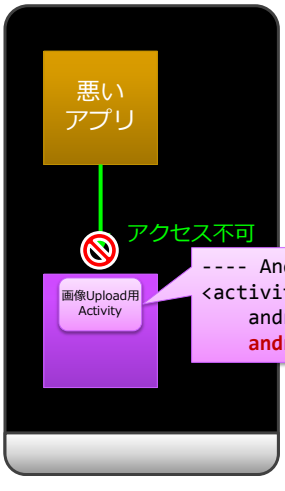


【原因】

画像アップロード用の部品が他のアプリから（意図せず）アクセス可能な状態となっていた。

つまり他のアプリから画像アップロード機能を勝手に利用することができてしまった。

勝手にツイートされてしまうTwitterアプリ



【対策】

部品（Activity）を非公開に設定する。

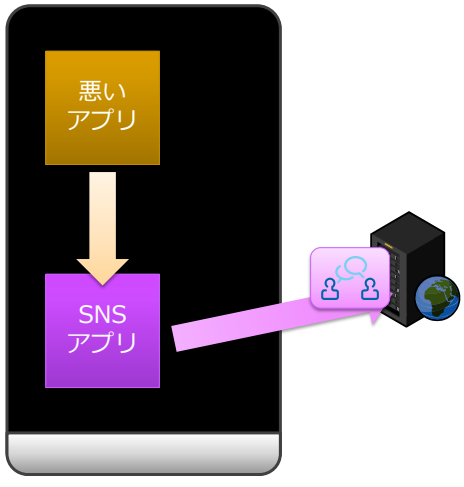
アプリの開発者（プログラマ）が知っていれば防げた問題。

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

⬅ **非公開**

事例２
会話が盗聴されてしまうSNSアプリ

会話が盗聴されてしまうSNSアプリ

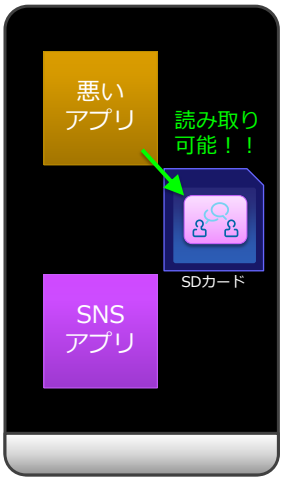


【問題】

SNSアプリが一時保存した会話データのファイルの内容を、他のアプリに盗み見られてしまう問題があった。

つまりプライベートな情報の漏えいが発生。

会話が盗聴されてしまうSNSアプリ

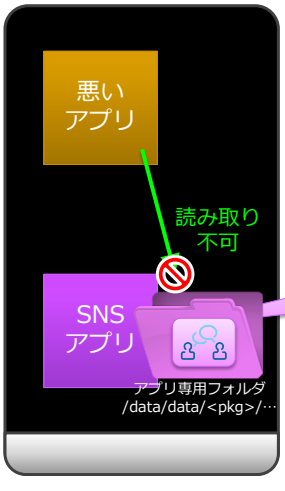


【原因】

SDカード上に会話データのファイルを保存していた。

SDカード上に保存したファイルの内容はすべてのアプリから読むことができるので、他のアプリがSNSの会話データを読み取ることができた。

会話が盗聴されてしまうSNSアプリ



【対策】

アプリ専用フォルダに会話データのファイルを非公開ファイルとして保存。

アプリの開発者（プログラマ）が知っていれば防げた問題。

```
---- 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**

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

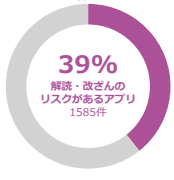
- exported
- ファイルの扱い
- ログ出力

知っていれば防げた

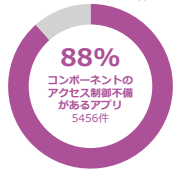
JSSEC セキュアコーディングガイドを読んでいれば防げた

何らかの脆弱性があるアプリの割合

暗号通信が破られるアプリの割合



情報漏えい、機能悪用のリスクがあるアプリの割合



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

アプリ開発者は セキュリティをほとんど知らない

- これがアプリの96%に脆弱性があるという根本的な原因

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

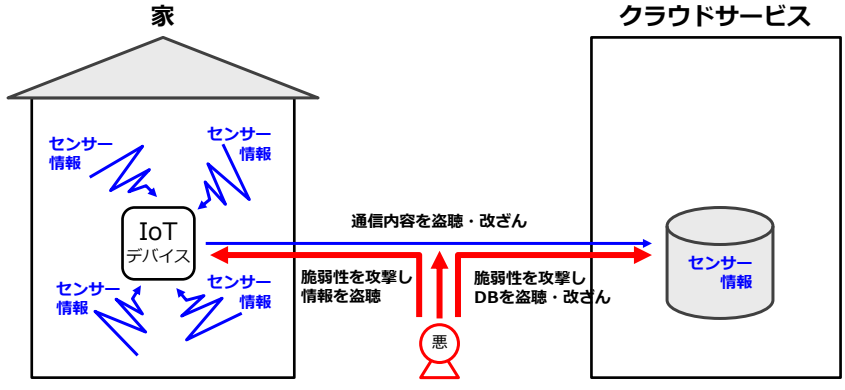
脆弱性が繰り返されてきた歴史

ネットの危険を知らない開発者が製品を無邪気にネット接続させ脆弱性問題を起こしてきた。

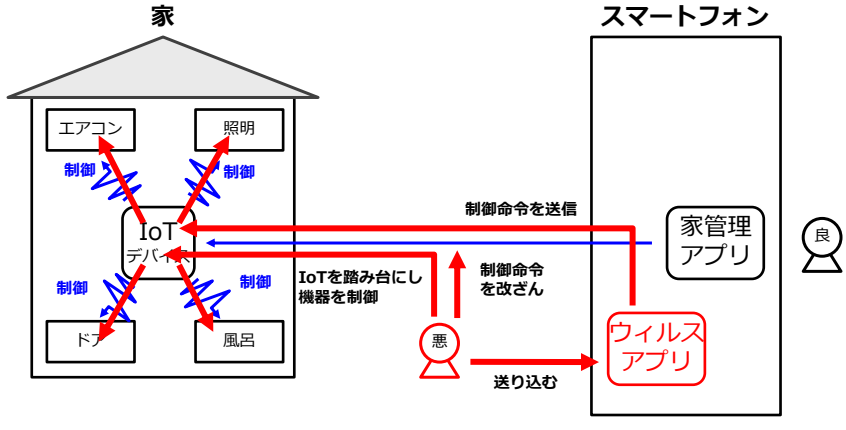
バッファオーバフローやパストラバーサルなど、同種の脆弱性が製品ジャンルを跨いで繰り返され、教訓は生かされてこなかった。

2000年～	2005年～	2010年～	2015年～
サーバー／PCアプリ	同様の脆弱性が問題になった		
	ネット家電	同様の脆弱性が問題になった	
		スマートフォンアプリ	恐らく同様に…
			IoTデバイス

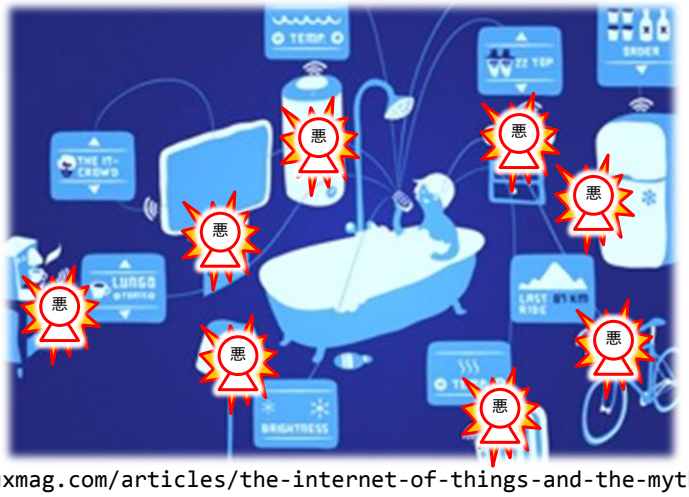
「情報」が狙われる



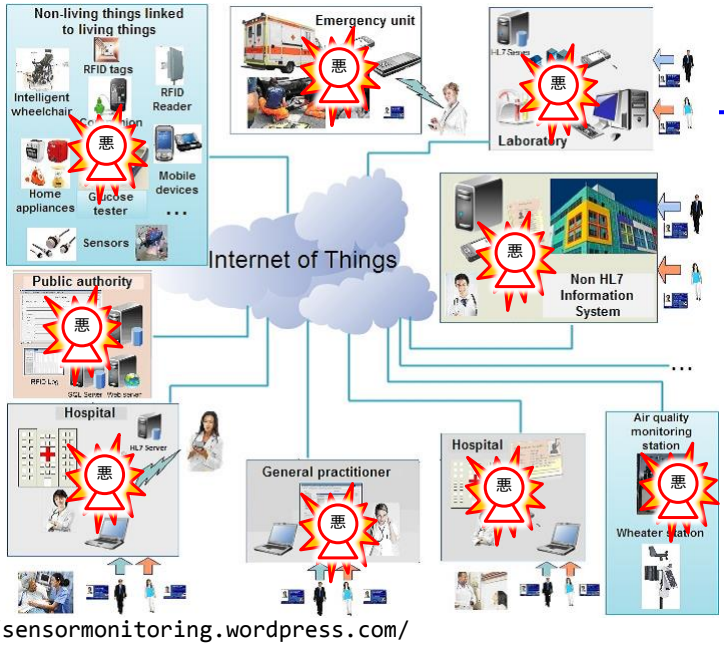
「機能」が狙われる



気が付くと包囲されている！



http://uxmag.com/articles/the-internet-of-things-and-the-mythical-smart-fridge



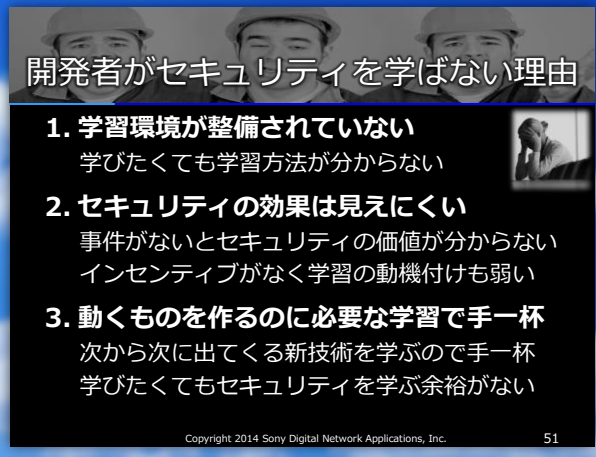
http://sensormonitoring.wordpress.com/

IoT時代に備えよう、Androidセキュリティ技術

【朗報】Android IoTデバイスには脆弱性の連鎖を断ち切る解決策がある！

2000年～	2005年～	2010年～	2015年～
サーバー／PCアプリ	同様の脆弱性が問題になった		
	ネット家電	同様の脆弱性が問題になった	
		スマートフォンアプリ	連鎖を断ち切る！
			IoTデバイス

3つの問題、すべて解決済み！



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

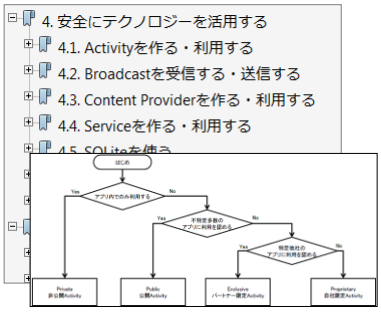
開発者が便利に使えるガイド

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



JSSECガイドは永遠のベータ版

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

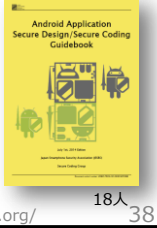
2014年7月

18人

2014年4月

25人

2014年8月



18人

2014年、英語版リリース

1つ目を解決！

開発者がセキュリティを学ばない理由

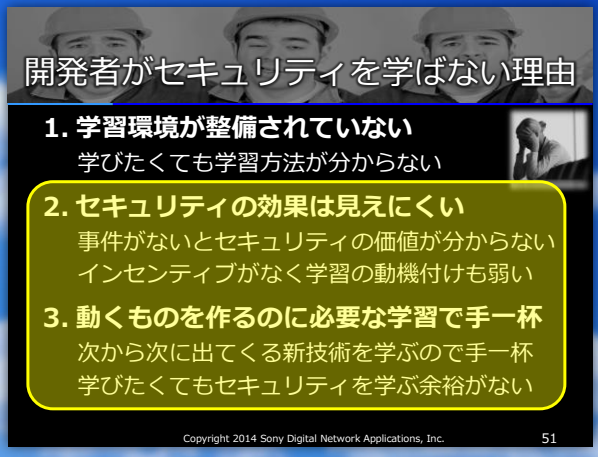
1. **学習環境が整備されていない**
   学びたくても学習方法が分からない

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

ただ、分厚い。忙しい開発者に「コレ読んで♪」とは言えない。

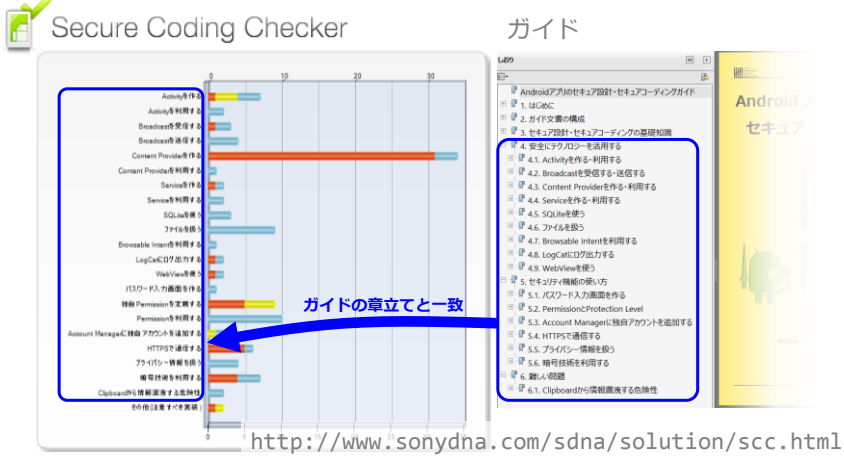
400ページ超

残りをツールで解決！



2. セキュリティの効果の可視化

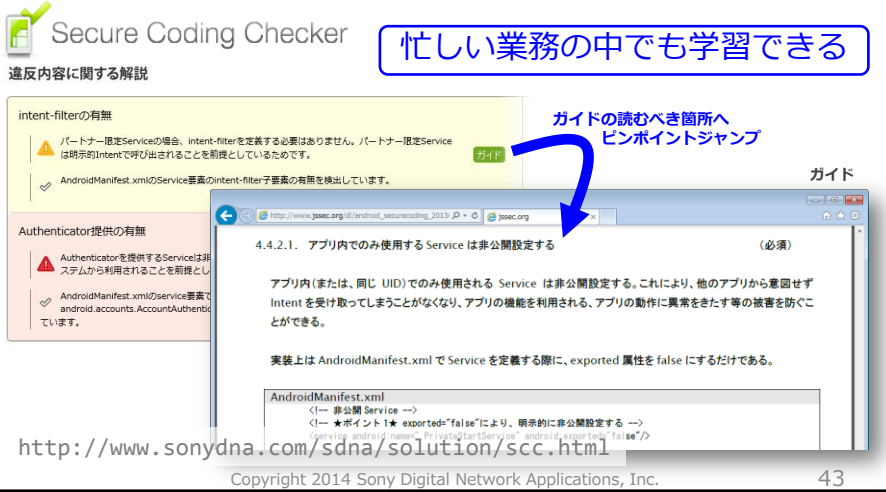
アプリを自動解析して脆弱性をグラフ表示するツール



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

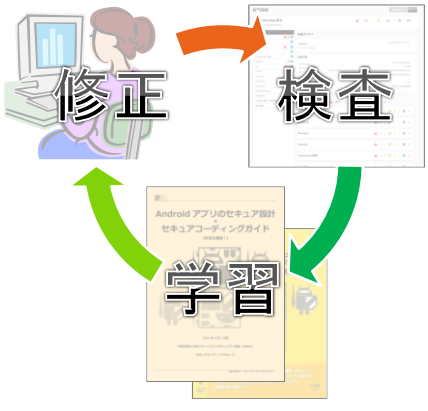


http://www.sonydna.com/sdna/solution/scc.html

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

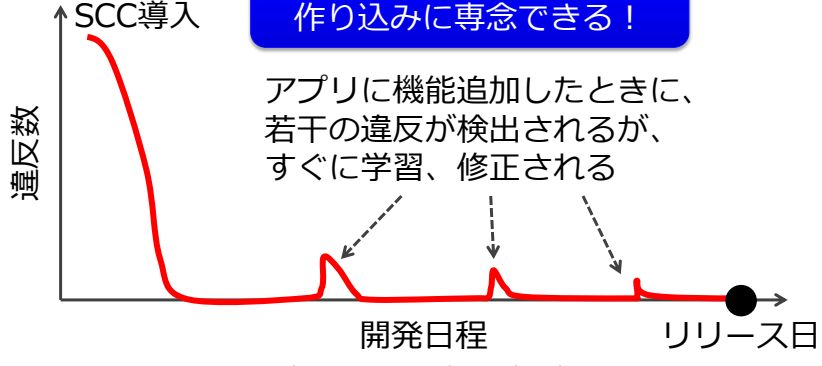
【メリット２】
見つかる問題には必ず解決方法があり、業務が滞ることがない

【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

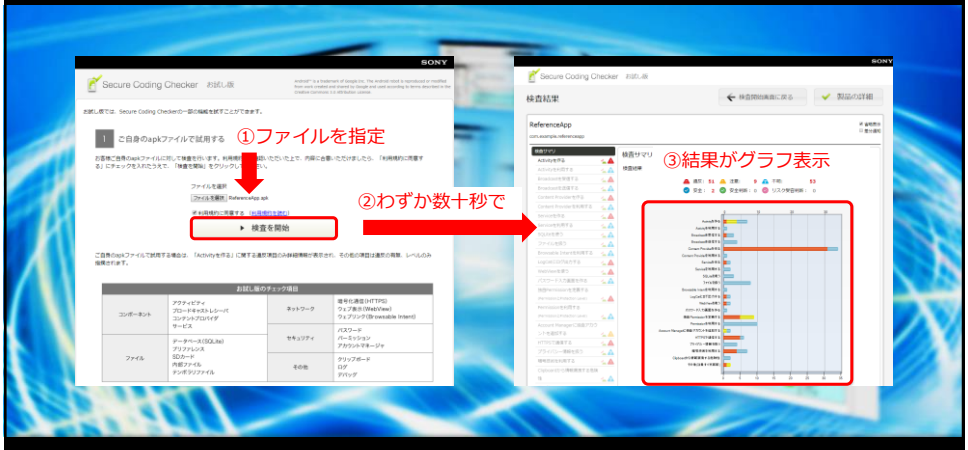
SCCの一般的な利用状況

３日程度の対策で０件を実現したあとは、アプリのリリース日まで０件をキープ！

最後の最後までアプリの作り込みに専念できる！



一度、あなたのアプリを検査してみてください(無償)
https://scc-mini.sonydna.com/



アプリのファイル(.apk)をUploadするだけですぐに結果がでます。

Facebook や Twitter のように、

世界を変える

製品やサービスを作りたい人？

自分には**できる**と思う人？

できると思った人へ

頑張ってください！

他のみんなも応援すると思いますよ。

むつかしいと思った人へ

そんなあなたに
とっておきの話があります

ゴールドラッシュ

その昔、アメリカの川で砂金が見つかり、アメリカ全土から10万人以上の人が集まった。

シャベルとバケツを販売した人が大儲けした。

送金・輸送・郵便サービスを提供した人が大儲けした。

ジーンズを販売した人が大儲けした。

そして、金の採掘者に成功者はいなかった。

金を採掘するのではなく、
金を採掘する人たちを支えた人たちが大儲けしたという話。こっちならできそうな気がしませんか？

Internet of Things

すべてのモノはどんどんネットへ

ネットには世界を変える力がある

ネットには危険もある

個人情報やプライバシーが奪われる製品やサービスを使いたいと思いますか？

セキュリティはインターネットで世界を変える人たちを支える技術

すごい製品・サービスを作ろうという人たちは多いが、同じ土俵で競争に勝つのは幸運が必要

すごい製品・サービスはネット前提なのでセキュリティの確保は必須条件

成功したい（＋成功している）人たち全員が必要とするセキュリティの仕事は儲かるはず

なのに、セキュリティを志す人は少ない

いまこそ、セキュリティ技術を身につけるとき！

まとめ

1. **IoTとAndroid**
   IoTでAndroid OSが採用される
2. **Androidの脆弱性問題を振り返る**
   脆弱性とはどのようなもので、どのような原因で生じるのか
3. **IoTセキュリティの悪寒**
   歴史を振り返り、今後のIoTセキュリティを考える
4. **IoT時代に備えよう、Androidセキュリティ技術**
   Androidなら、IoTにも活用できる良いセキュリティ対策がある
5. **セキュリティ技術を身につけて金持ちになろう！**

一度、あなたのアプリを検査してみてください(無償)
https://scc-mini.sonydna.com/

アプリのファイル(.apk)をUploadするだけですぐに結果がでます。

ブログにて
セキュリティの時事情報を発信中

ソフトウェアセキュリティの気になる話

http://securityblog.sonydna.com/

「SDNAセキュリティブログ」で検索！