スマートフォン時代のセキュリティ人材育成

一般社団法人日本スマートフォンセキュリティ協会
セキュアコーディンググループ
松 並　勝
<Masaru.Matsunami@jp.sony.com>

はじめに

この講演の中ではいくつかの事例を紹介しています。

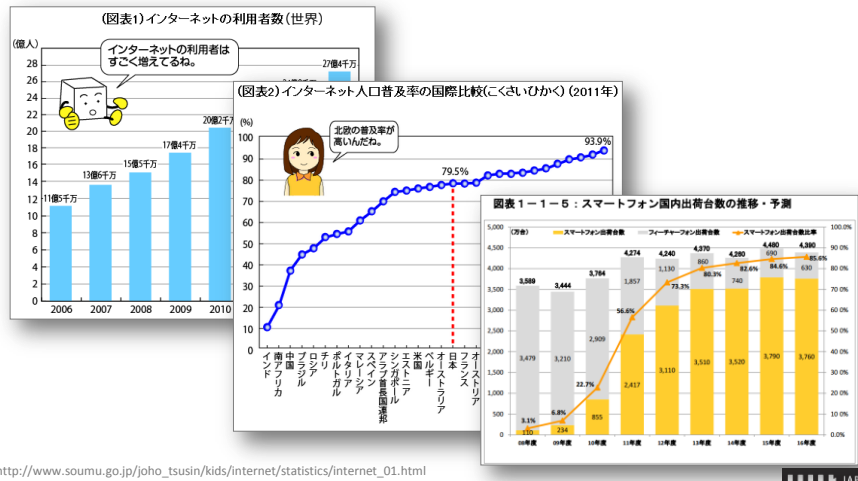
事例は主にスマートフォン、特にAndroidに関するものを紹介していますが、

事例以外の内容ついては、スマートフォンやAndroidに限らず、ソフトウェアのセキュリティ一般の話としてお聞きいただける内容となっています。

一般社団法人
日本スマートフォンセキュリティ協会

- 略称：JSSEC（ジェーセック）
- 目的：スマートフォンを安全・安心に利用できる社会をつくる
- キャリア、端末メーカー、アプリベンダー、SIer、セキュリティベンダー、ユーザー企業、等で構成
- ガイド文書などを作成して公開
- ボランティア活動
- 続きはWeb → http://www.jssec.org/

社会がインターネットに強く依存



http://www.soumu.go.jp/joho_tsusin/kids/internet/statistics/internet_01.html
http://www.soumu.go.jp/main_content/000219917.pdf

セキュリティ事件・事故は増加傾向

不正ログイン事件の影響が企業システムに及ぶ恐れ、実態調査で浮き彫りに

Webサイトの不正ログイン事件が多発したことを受け、パスワード管理の実態や企業システムへの影響の可能性についてシマンテックが調査を

プリント／PDF　ツイート 25

あらためて解説Adobe Creative Cl
情報新時代に求められるIT戦略－業

シマンテックは10月30日、個人
した。個人のパスワード利用や意
クに晒されていると警鐘を鳴らす

調査は今春頃から国内で不正ロ
企業のWebサイト管理者のパスワ
プル数はそれぞれ300件で、Web
は勤務先の業務システム利用に関

日本企業狙うサイバー攻撃、「水飲み型」に要注意

2013/10/10 23:00

小 中 大　保存　印刷　リプリント　▼共有

情報セキュリティー・サービスを提供するラックは2013年10月9日、報道機関に向けて日本の企業や団体を狙った新型のサイバー攻撃
月頃から始まったもので、重要イン
があったが日本をターゲットしたの

水飲み場攻撃とは、水飲み場に集
が狙う様から名付けられた呼称。多
用のプログラムを仕込み、特定のIP
場合にWebブラウザーの脆弱性（ソ
ホール）を突いてこれをパソコンに送
IPアドレスからアクセスしてきたWeb
ない。攻撃をするかどうかの制御は
アプリケーションで実施するのが一

Adobeへのサイバー攻撃、不正アクセスの影響は3800万人に

影響を受けたユーザーは当初290万人と発表されていたが、その後の調査で少なくとも3800万人に上ることが分かったという。

[鈴木聖子，ITmedia]

プリント／PDF　ツイート 147　いいね！ 135　チェック　+1 8　投稿　メール　アラート

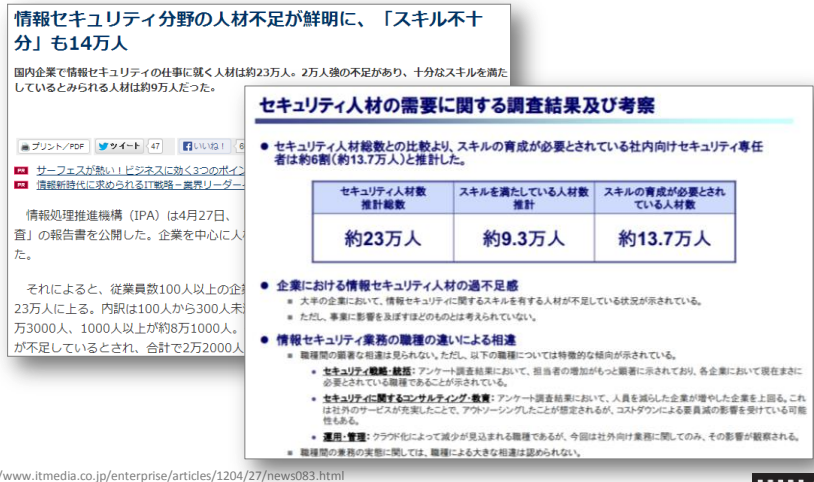
あらためて解説Adobe Creative Cloud
情報新時代に求められるIT戦略－業界リーダーインタビュー

米Adobe Systemsのユーザー情報などが不正アクセスされた事件で、米セキュリティ情報サイトの「Krebs on Security」は10月29日、影響を受けたユーザーは少なくとも3800万人に上ることが分かったと伝えた。Adobeはこの問題が発覚した10月3日の時点で、「影響を受けたユーザーは290万人」と発表していた。

http://www.itmedia.co.jp/enterprise/articles/1310/30/news144.html
http://www.nikkei.com/article/DGXNASFK1001P_Q3A011C1000000/
http://www.itmedia.co.jp/enterprise/articles/1310/30/news044.html

JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュリティ人材が慢性的に不足



情報セキュリティ分野の人材不足が鮮明に、「スキル不十分」も14万人

国内企業で情報セキュリティの仕事に就く人材は約23万人。2万人強の不足があり、十分なスキルを満たしているとみられる人材は約9万人だった。

プリント／PDF　ツイート 47　いいね！

サーフェスが熱い！ビジネスに効く3つのポイン
情報新時代に求められるIT戦略－業界リーダー

情報処理推進機構（IPA）は4月27日、
査」の報告書を公開した。企業を中心に人
た。

それによると、従業員数100人以上の企
23万人に上る。内訳は100人から300人未
万3000人、1000人以上が約8万1000人。
が不足しているとされ、合計で2万2000人

セキュリティ人材の需要に関する調査結果及び考察

- セキュリティ人材総数との比較より、スキルの育成が必要とされている社内向けセキュリティ専任者は約6割（約13.7万人）と推計した。

セキュリティ人材数推計総数	スキルを満たしている人材数推計	スキルの育成が必要とされている人材数
約23万人	約9.3万人	約13.7万人

- 企業における情報セキュリティ人材の過不足感
  - 大半の企業において、情報セキュリティに関するスキルを有する人材が不足している状況が示されている。
  - ただし、事業を及ぼすほどのものとは考えられていない。
- 情報セキュリティ業務の職種の違いによる相違
  - 職種間の顕著な相違は見られないただし、以下の職種については特徴的な傾向が示されている。
    - **セキュリティ戦略・統括：** アンケート調査結果において、担当者の増加がもっと顕著に示されており、各企業において現在まさに必要とされている職種であることが示されている。
    - **セキュリティに関するコンサルティング・教育：** アンケート調査結果において、人員を減らした企業が増やした企業を上回る。これは社外のサービスが充実したことで、アウトソーシングしたことが想定されるが、コストダウンによる要員減の影響を受けている可能性もある。
    - **運用・管理：** クラウド化によって減少が見込まれる職種であるが、今回は社外向け業務に関してのみ、その影響が観察される。
  - 職種間の業務の実態に関しては、職種による大きな相違は認められない。

http://www.itmedia.co.jp/enterprise/articles/1204/27/news083.html
http://www.ipa.go.jp/files/000024415.pdf

JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュリティ人材の育成がホット！

http://www.itmedia.co.jp/enterprise/articles/1202/22/news053.html
http://www.security-camp.org/

http://www.jnsa.org/seccon/
http://www.security-next.com/044157

今日は・・・

セキュリティ人材（専門職）育成の話ではありません

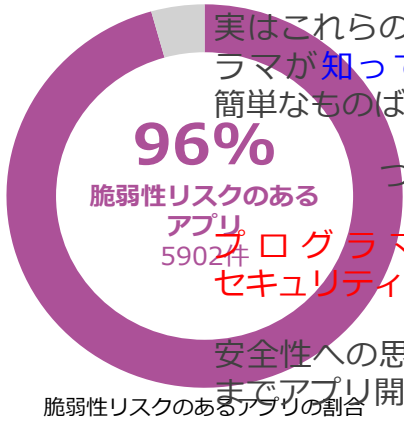
スマートフォンアプリの セキュリティ（脆弱性）の現状

調査報告書を公開しましたところ大きな反響がありました。

http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf
http://www.nikkei.com/article/DGXNASFK3002W_Q3A031C1000000/
http://www.atmarkit.co.jp/ait/articles/1311/01/news033.html

JAPAN SMARTPHONE SECURITY ASSOCIATION

ほとんどのアプリに 脆弱性（セキュリティホール）がある



脆弱性リスクのあるアプリの割合
人気アプリ6170件を検査

実はこれらの脆弱性はプログラマが知っていれば防げた簡単なものばかりでした。

つまり

プログラマがまったくセキュリティを知らない。

安全性への思慮が不足したままでアプリ開発している…

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

JAPAN SMARTPHONE SECURITY ASSOCIATION

会長のおっしゃるとおりです

ICT教育推進協議会のWebページより

会長ご挨拶

インターネット環境に代表される情報通信技術(ICT: Information and Communication Technologies)がグローバルスケールに普及し、すべての社会・産業活動の基盤としての役割を果たさなければならなくなりました。
私たちの日常生活において、多種多様な形態でICT基盤を活用することが一般化し、ICTの存在は私たちの意識の中で、そして、社会の中で透明化しつつあると言えるでしょう。すなわちICTは、もはや社会にとって、そして、産業にとって必要不可欠な社会インフラとなっています。

その一方で、社会に不可欠なICTの利用に対する体系的で実践的な教育カリキュラムが存在していないことから、ICTに対する関心度が薄れ、知識不足のまま、安全性への思慮が不足したままで、ICT基盤を利用している利用者は、増加しつづけています。我が国のICT基盤の整備と発展を支えるべき人材の供給は、その質と量の両面において需要を大きく下回っている状況であると言わざるを得ません。

ICT教育推進協議会
会長 **江崎 浩**

http://ictepc.jp/council/greetings.html

JAPAN SMARTPHONE SECURITY ASSOCIATION

お伝えしたいこと①

プログラマの人材育成にて、セキュアコーディング教育を必須にしてほしい

JAPAN SMARTPHONE SECURITY ASSOCIATION

お伝えしたいこと②

プログラマに効率よくセキュアコーディングを教育する方法を紹介します

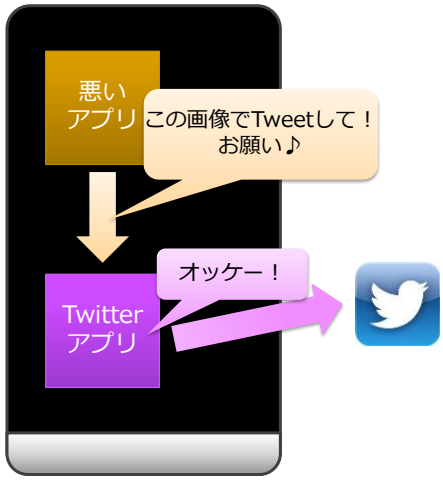
JAPAN SMARTPHONE SECURITY ASSOCIATION

事例 1

勝手にツイートされてしまうTwitterアプリ

JAPAN SMARTPHONE SECURITY ASSOCIATION

勝手にツイートされてしまうTwitterアプリ

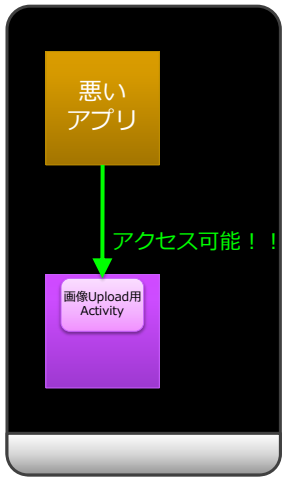


【問題】

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。

JAPAN SMARTPHONE SECURITY ASSOCIATION

勝手にツイートされてしまうTwitterアプリ

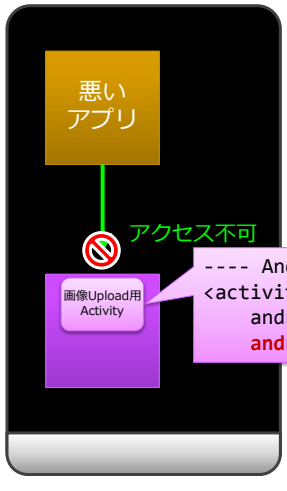


【原因】

画像アップロード機能（Activity）が他のアプリからアクセス可能であった。

JAPAN SMARTPHONE SECURITY ASSOCIATION

勝手にツイートされてしまうTwitterアプリ



⬅非公開

【対策】

Activityを非公開に設定する。

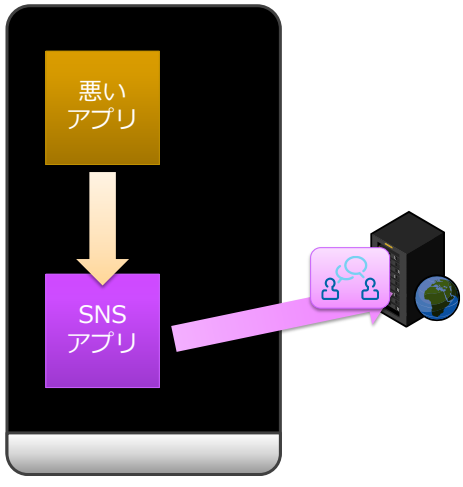
JAPAN SMARTPHONE SECURITY ASSOCIATION

事例２

メッセージが盗み見られてしまうSNSアプリ

JAPAN SMARTPHONE SECURITY ASSOCIATION

メッセージが盗み見られてしまうSNSアプリ

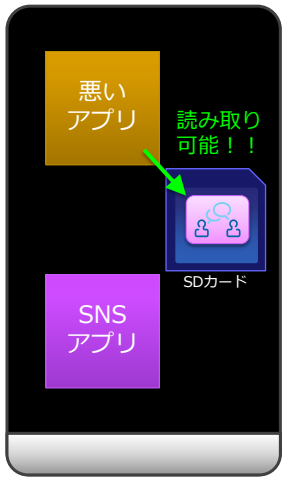


【問題】

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。

JAPAN SMARTPHONE SECURITY ASSOCIATION

メッセージが盗み見られてしまうSNSアプリ



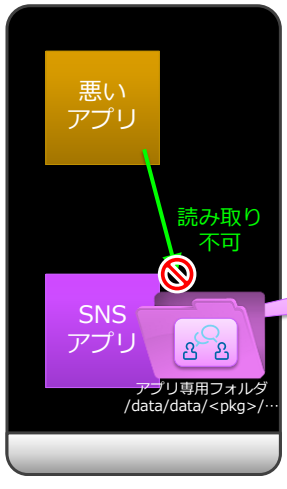
【原因】

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。

JAPAN SMARTPHONE SECURITY ASSOCIATION

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

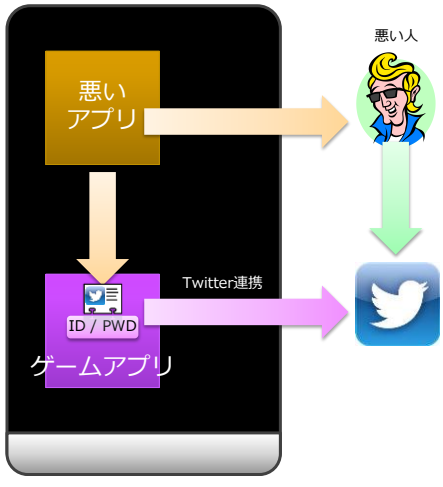
JAPAN SMARTPHONE SECURITY ASSOCIATION

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

JAPAN SMARTPHONE SECURITY ASSOCIATION

Twitterアカウントが乗っ取られてしまうゲームアプリ



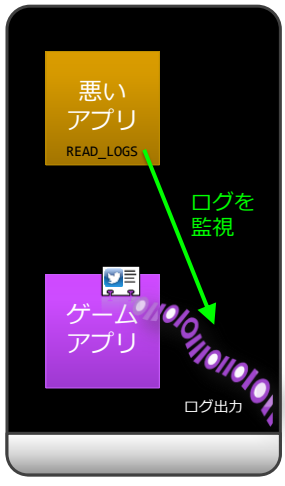
【問題】

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。

JAPAN SMARTPHONE SECURITY ASSOCIATION

Twitterアカウントが乗っ取られてしまうゲームアプリ



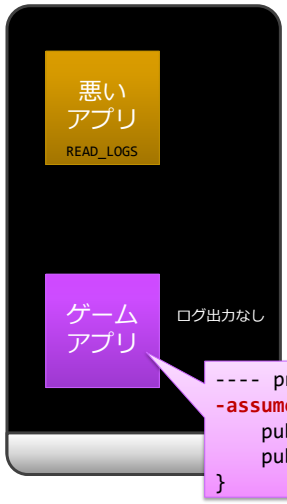
【原因】

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。

JAPAN SMARTPHONE SECURITY ASSOCIATION

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

JAPAN SMARTPHONE SECURITY ASSOCIATION

Androidアプリの脆弱性の傾向

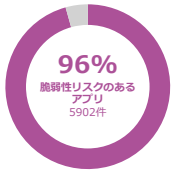
初歩的な問題ばかり

- exported
- ファイルの扱い
- ログ出力

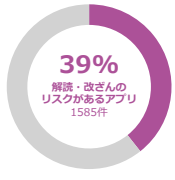
知っていれば防げた

JSSEC セキュアコーディングガイドを読んでいれば防げた

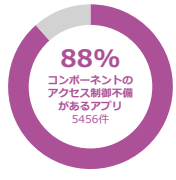
何らかの脆弱性があるアプリの割合



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

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSECセキュアコーディングガイド

Androidアプリのセキュア設計・セキュアコーディングTipsを集めて文書化して公開する

Androidアプリセキュリティのノウハウ集

下記URLからダウンロード可能（無料）

ガイド文書とサンプルコード一式

http://www.jssec.org/report/securecoding.html

2013年4月23日、最新版（第3版）が公開

今後も継続的に更新を続けていく

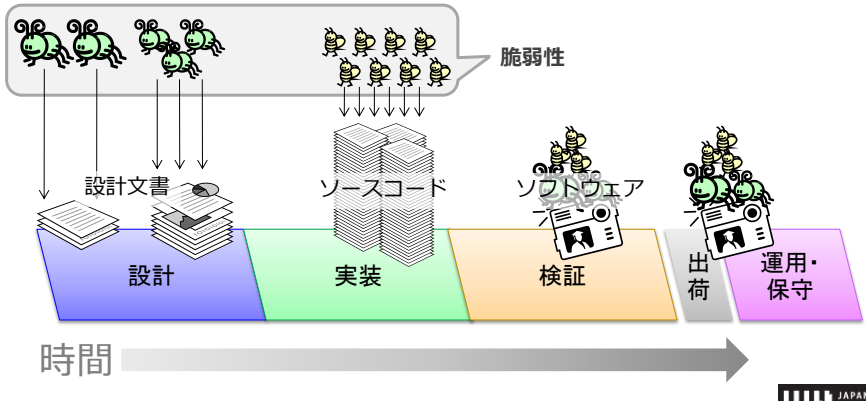
20万件超もダウンロードされている人気コンテンツ

わたしはこのガイド執筆のリーダー

JAPAN SMARTPHONE SECURITY ASSOCIATION

脆弱性がソフトウェアに入っていく様子

何もしないと脆弱性が設計文書やソースコードの中に入り込んでそのまま出荷されてしまう



安全なソフトウェアをつくる
5[redacted]策

セキュリティ人材の育成がホット！

6 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会

プログラマ

セキュリ[redacted]
考慮した[redacted]

[redacted]り込まないように
注意してつくる

セキュリティ技術者

セキュリティ
ドキュメントレビュー

セキュリティ
コードレビュー

疑似攻撃
検査

入ってしまった
脆弱性を見つけて
修正する

31 | Copyright 2013 Sony Digital Network Applications, Inc.

JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュリティ技術者の処理能力

なんとかすべて
レビューできる
分量

もはや、すべてを
レビューするのは
不可能な分量

検査できる分量

セキュリティ技術者

セキュリティ
ドキュメントレビュー

セキュリティ
コードレビュー

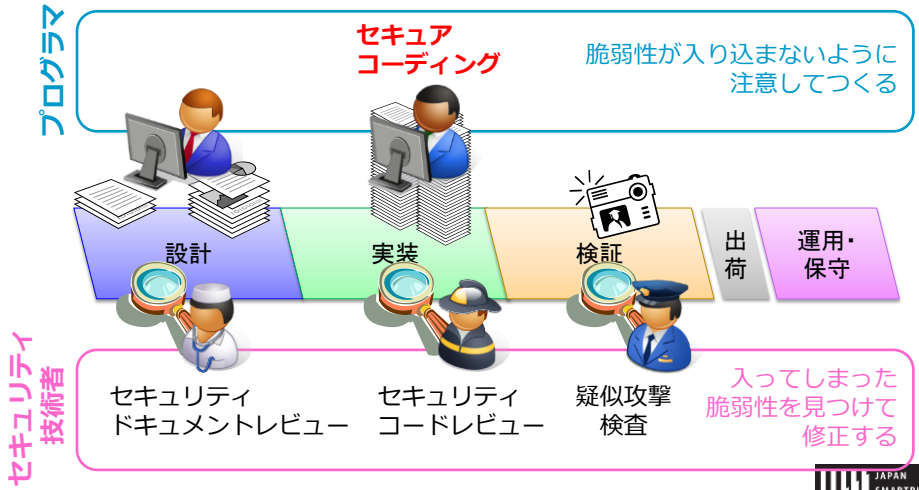
疑似攻撃
検査

入ってしまった
脆弱性を見つけて
修正する

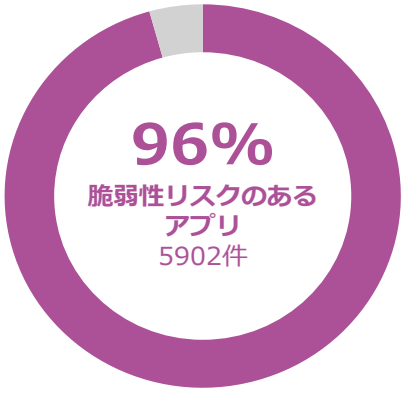
32 | Copyright 2013 Sony Digital Network Applications, Inc.

JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュアコーディングは超必須！



だけど

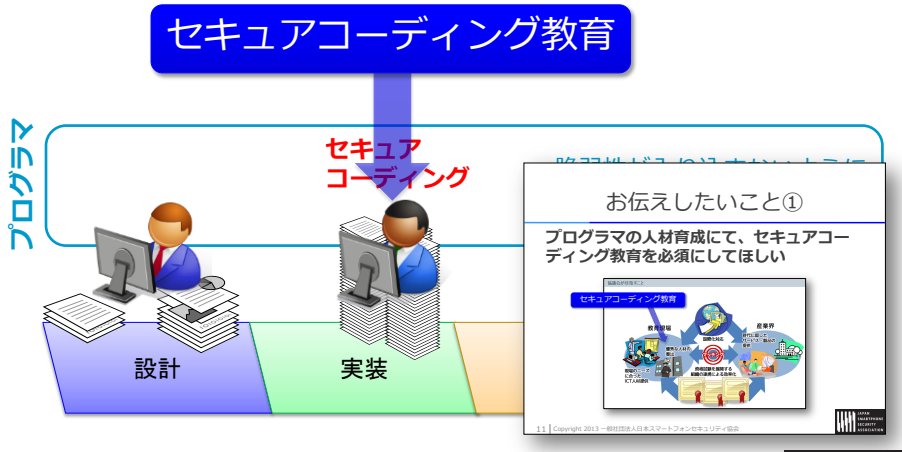


脆弱性リスクのあるアプリの割合
人気アプリ6170件を検査

プログラマがまったく
セキュアコーディングを
知らない。

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

だからすべてのプログラマに
セキュアコーディング教育を必須に！



JAPAN SMARTPHONE SECURITY ASSOCIATION

伝えたいこと②
プログラマに効率よくセキュアコーディングを教育する方法

セキュアコーディング教育

まず効率の前に
教科書は？

JAPAN SMARTPHONE SECURITY ASSOCIATION

無料の良書がございます！

Androidアプリのセキュア設計・セキュアコーディングTipsを集めて文書化して公開する

Androidアプリセキュリティのノウハウ集

下記URLからダウンロード可能（無料）

ガイド文書とサンプルコード一式

http://www.jssec.org/report/securecoding.html

2013年4月23日、最新版（第3版）が公開

今後も継続的に更新を続けていく

20万件超もダウンロードされている人気コンテンツ

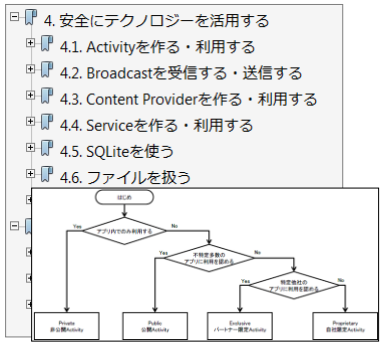
わたしはこのガイド執筆のリーダー

JAPAN SMARTPHONE SECURITY ASSOCIATION

プログラマがセキュアコーディングを学ぶことに最適化した構成

プログラマのやりたいこと視点でまとめた記事構成

- セキュリティ書籍によくある、NG例を解説するのではなく、**OKな方法を前面に押し出して解説**



セキュアなサンプルコード

- **セキュアなコードをコピーペーストして使ってください**
- コードがセキュアなだけでなく、セキュリティのポイントがコメント中に記載

JAPAN SMARTPHONE SECURITY ASSOCIATION

デファクトスタンダードなAndroidセキュリティ教科書

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

JAPAN SMARTPHONE SECURITY ASSOCIATION

課題

365頁もある！

読むのが大変！

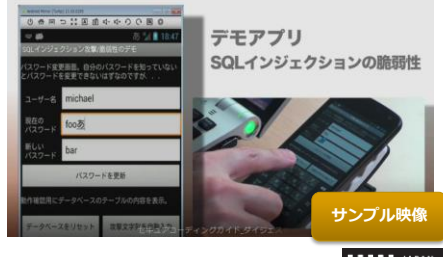
↓

どうするの？

ガイドの基礎知識を手早く習得できるDVDを用意しました！

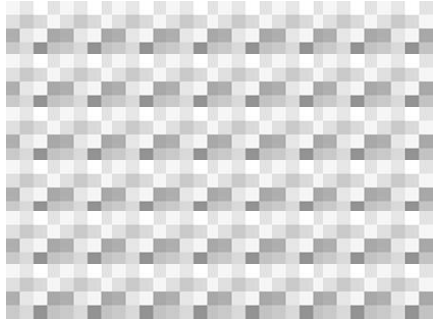
計90分の映像をご覧いただくと、ガイドのどこを読んでもすぐに理解できるようになります。

好評発売中 3,000円 Amazonでも買えます！



お伝えしたいこと②

プログラマに効率よくセキュアコーディングを教育する方法を紹介します



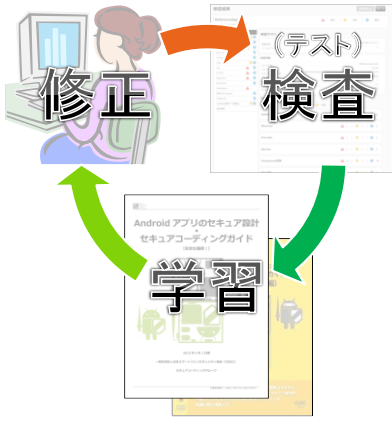
JAPAN SMARTPHONE SECURITY ASSOCIATION

ソニーの現場でみつけた

効率よく セキュアコーディングを 学習する方法

JAPAN SMARTPHONE SECURITY ASSOCIATION

（テスト駆動型学習）
検査駆動型学習

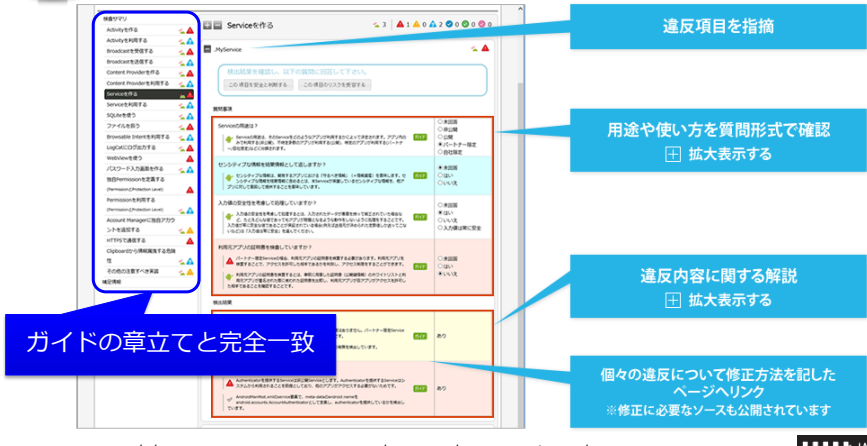


テスト駆動型開発のアイデアを学習に転用

脆弱性検査ツールとプログラマの自作アプリを組み合わせることで、理解度、学習意欲、学習効率をすべて高められる学習方法

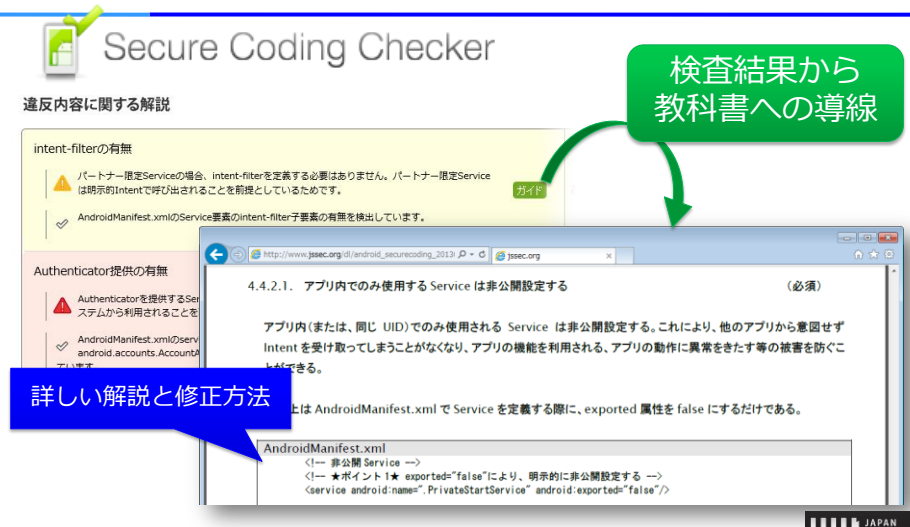
JSSECセキュアコーディングガイドを基準にした脆弱性検査ツール

Secure Coding Checker

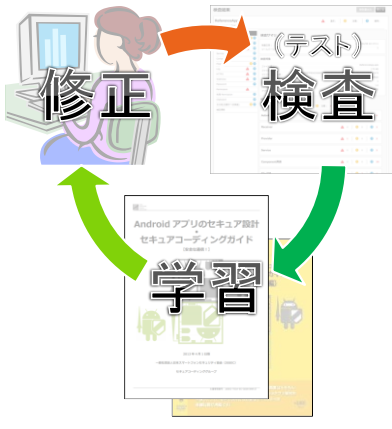


http://www.sonydna.com/sdna/solution/scc.html

検査結果には簡潔な解説に加え、ガイドPDFの該当箇所を表示

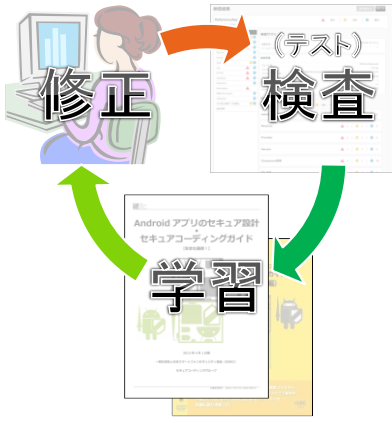


学習プロセス



1. プログラマが自作アプリを検査ツールにかけると、自作アプリの脆弱性が見つかる
2. 検査結果からガイドの参照先が分かるのでガイドの該当箇所を学習し、セキュアコーディングを学ぶ
3. 自作アプリのソースコードを修正する
4. 再度、自作アプリを検査ツールにかけると修正した問題が検出されなくなる

検査駆動型学習のすごい効果

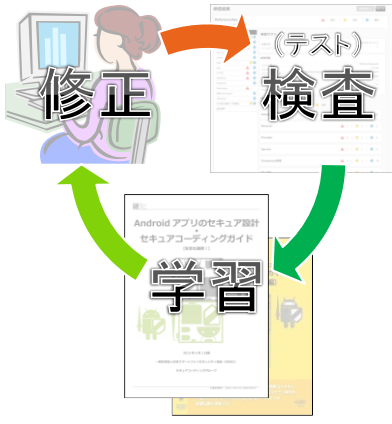


【メリット１ 理解度】
自作アプリの脆弱性という具体事例を題材に学習できるので、脆弱性とセキュアコーディングの理解が深まる

【メリット２ 学習意欲】
自作アプリの脆弱性を修正するために必要な学習だけに絞り込まれるため、自作アプリを効率よく安全にすることができ、学習効果を実感し学習意欲が高まる

【メリット３ 学習効率】
検出される脆弱性には必ず解決方法がセットで提示されるため、プログラマが効率よく自力で学習でき、効率よく脆弱性を修正できる

検査駆動型学習のすごい効果



【メリット１ 理解度】
自作アプリの脆弱性という具体事例を題材に学習できるので、脆弱性とセキュアコーディングの理解が深まる

【メリット２ 学習意欲】
自作ア
要な学
アプリ
学習効

検出さ
セット
効率よ
性を修

お伝えしたいこと②

プログラマに効率よくセキュアコーディングを教育する方法を紹介します

のちほど詳しく…

ガイドをぜひご活用ください

Androidアプリのセキュア設計・セキュアコーディングTipsを集めて文書化して公開する

Androidアプリセキュリティのノウハウ集

下記URLからダウンロード可能（無料）

ガイド文書とサンプルコード一式
http://www.jssec.org/report/securecoding.html

2013年4月23日、最新版（第3版）が公開

今後も継続的に更新を続けていく

20万件超もダウンロードされている人気コンテンツ

わたしはこのガイド執筆のリーダー

JAPAN SMARTPHONE SECURITY ASSOCIATION

DVDもぜひご活用ください

計90分の映像をご覧いただくと、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。

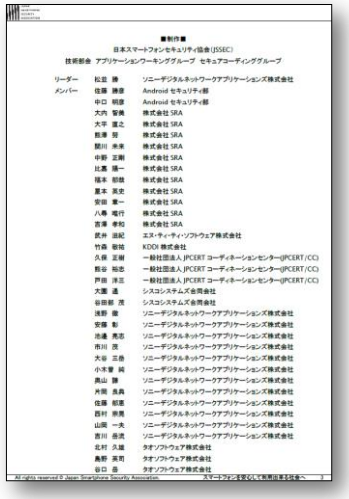
好評発売中 3,000円 Amazonでも買えます！

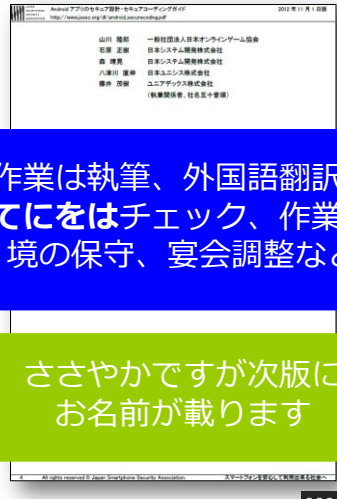
検査ツール Secure Coding Checker もぜひお試しください

https://scc-mini.sonydna.com/

今だけ！

ガイド作成にボランティア協力してくださる方を探しています





作業は執筆、外国語翻訳、**てにをは**チェック、作業環境の保守、宴会調整など

ささやかですが次版にお名前が載ります

ご協力いただける方は下記の要領でご連絡ください

1. JSSEC会員でない方はAndroidセキュリティ部へご参加ください

会員かどうかは下記URLで確認
http://www.jssec.org/members/

Androidセキュリティ部への参加は下記URLからできます
https://groups.google.com/group/android-security-japan
右の(4)では「Androidセキュリティ部」と記載してください

あとでお読みください

2. 次の書式でメール送信してください

```
To: Masaru.Matsunami@jp.sony.com
Subject: JSSECセキュアコーディングG参加
本文:
(1) Google account: (メアドを記載)
(2) First name: (名前を記載)
(3) Last name: (名字を記載)
(4) Organization: (組織名を記載)
(5) Git access: (必要 or 不要)
```

各種アカウント発行後、メール返信にてご連絡いたします
(1)はGmailメアドまたはご自身のメアドをGoogleアカウント化したもの
(4)は下記URLページ内から選択
http://www.jssec.org/members/

みなさまのご参加を

JAPAN SMARTPHONE SECURITY ASSOCIATION

まとめ

高度なセキュリティ人材育成とは別に、プログラマにもセキュアコーディング教育が必要です。

プログラマの人材育成にて、セキュアコーディング教育を必須にしてほしい旨、お願いしました。

プログラマに効率よくセキュアコーディングを教育する、検査駆動型学習法を紹介しました。

JAPAN SMARTPHONE SECURITY ASSOCIATION