



JAPAN  
SMARTPHONE  
SECURITY  
ASSOCIATION



# 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>

1 | 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


## 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、

事例以外の内容については、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。



2 | 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

# 一般社団法人 日本スマートフォンセキュリティ協会

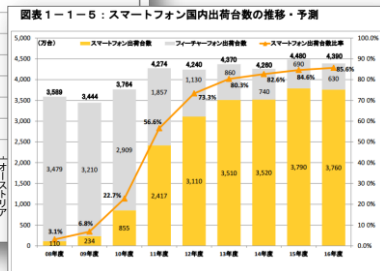
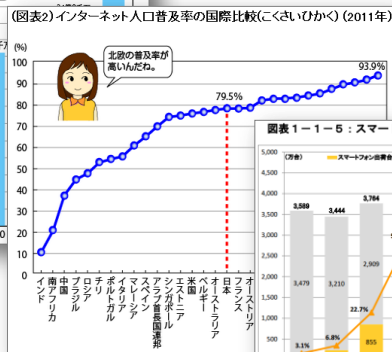
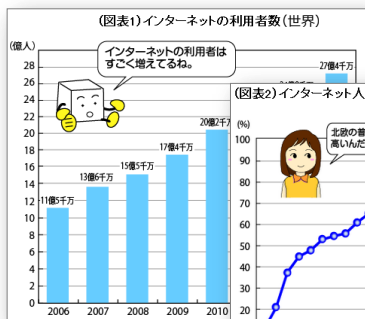


- 略称：JSSEC（ジェーセック）
- 目的：スマートフォンを安全・安心に利用できる社会をつくる
- キャリア、端末メーカー、アプリベンダー、SIer、セキュリティベンダー、ユーザー企業、等で構成
- ガイド文書などを作成して公開
- ボランティア活動
- 続きはWeb → <http://www.jssec.org/>

3 | 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



## 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/joho_tsusin/kids/Internet/statistics/internet_01.html)  
[http://www.soumu.go.jp/main\\_content/000219917.pdf](http://www.soumu.go.jp/main_content/000219917.pdf)

4 | 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



# 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

### 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

印刷/PDF ツイート (25)

あらためて解説Adobe Creative Cloud

情報新時代に求められるIT戦略-異業リーダーインタビュー

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

図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

グインのWebサイト管理者のパスワ

ード数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

情報セキュリティ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

撃が開始された。重要イン

フラストラクチャーが狙われた

ことがわかった。日本をターゲットしたの

は、水飲み型攻撃とは、水飲み場に

集まる人から名前を呼ばれる。多

数のプログラムを仕込み、特定のIP

アドレスからアクセスしてきたWeb

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

般に実施されている。調査は

今春頃から国内で不正ログイン

のWebサイト管理者のパスワード

数はそれぞれ3000件で、Web

サイトのセキュリティ対策は、

は勤務先の業務システム利用に

関する調査を実施するのが一

## 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]

印刷/PDF ツイート (147)

あらためて解説Adobe Creative Cloud

情報新時代に求められるIT戦略-異業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.nikkei.com/article/DGXNASFK1001P_Q3A011C1000000/)  
<http://www.itmedia.co.jp/enterprise/articles/1310/30/news044.html>

5 | 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



# 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。

印刷/PDF ツイート (47)

サーフェスが熱い！ビジネスに効く3つのポイント

情報新時代に求められるIT戦略-異業リーダーインタビュー

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

それによると、従業員数100人以上の企業23万人に上る。内訳は100人から300人未満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門者は約6割(約13.7万人)と推計した。

セキュリティ人材推計総数	スキルを満たしている人材推計	スキルの育成が必要とされている人材推計
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、事業に影響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。
  - **セキュリティ監視・検知**: アンケート調査結果において、担当者の増加が最も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**: アンケート調査結果において、人員を減らした企業が増えたり企業を上回る。これは社内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、カスタム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限ってのみ、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>

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



# セキュリティ人材の育成がホット！

## セキュリティ人材を育成する「セキュリティ・キャンプ実施協議会」が設立

IPAや経済産業省が実施してきた「セキュリティ・キャンプ」を、官民連携による人材育成の場として、実施体制を強化する。



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

SECCON

セキュリティコンテスト (SECCON)

2013年10月～12月までの地方大会の  
オンライン申し込みを開始いたしました。  
<http://2013.seccon.jp/>

## 日本国内最大のセキュリティコンテスト 「SECCON 2013」 を実施

～8月を皮切りに、10月～12月までの地方大会を実施～

### 「SECCON 2013」四国大会、平均16歳のチーム が優勝

特定非営利活動法人日本スマートフォンセキュリティ協会主催の「SECCON 2013」の地方予選である「四国大会」が、10月20日に香川大学にて開催された。

実行委員会によれば、今回の四国大会は、高校から参加した地元チームと、翌日の「MWS Cup」に参戦する遠征組との混戦になったという。

2012年度の「SECCON全国大会」に出場した平均年齢約16歳のチーム「EpsilonDelta」が、最終リードする優勝となり優勝。決勝へ駒を進めた。残念ながら優勝は逃したものの、2名で参加したチーム「wasamsume」や、1名によるチーム「askn」なども人数的なハンデがありながら奮戦し、上位に食い込んだ。

競技では、競技ネットワークとは別のネットワークを使って解く問題や、プログラム実行時にキーボードのLEDが点灯し、目で確認しながら解く問題など、ハイレベルな難問が出題が行われたという。

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



7 | 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

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

8 | 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



# 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。

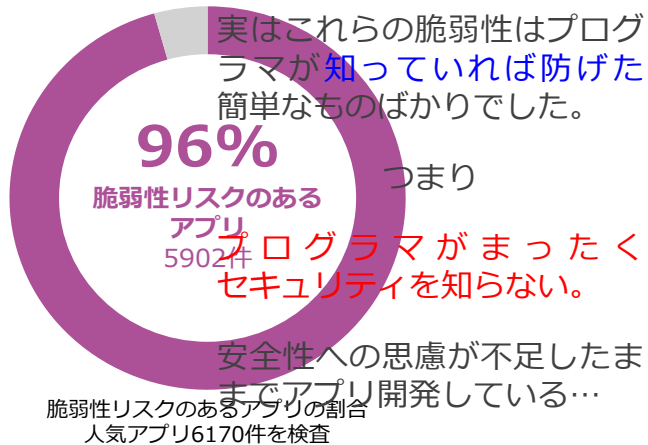


[http://www.sonydna.com/solution/android\\_vulnerability\\_report\\_201310.pdf](http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf)  
[http://www.nikkei.com/article/DGXNASFK3002W\\_Q3A031C1000000/](http://www.nikkei.com/article/DGXNASFK3002W_Q3A031C1000000/)  
<http://www.atmarkit.co.jp/ait/articles/1311/01/news033.html>

9 | 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



# ほとんどのアプリに 脆弱性（セキュリティホール）がある



[http://www.sonydna.com/solution/android\\_vulnerability\\_report\\_201310.pdf](http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf)

10 | 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



# 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、ICT基盤を利用している**利用者は、増加しつつあります。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>

11 | 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



## 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



12 | 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



## 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…

## Androidアプリ 脆弱性 事例



## 事例 1

# 勝手にツイートされてしまう Twitterアプリ

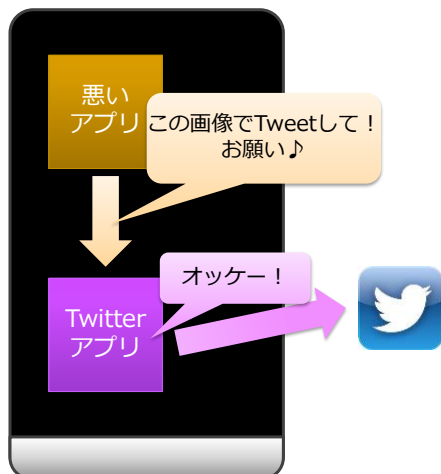
15 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会



## 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。

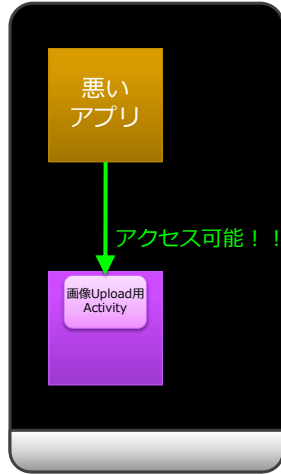


16 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会





## 勝手にツイートされてしまうTwitterアプリ



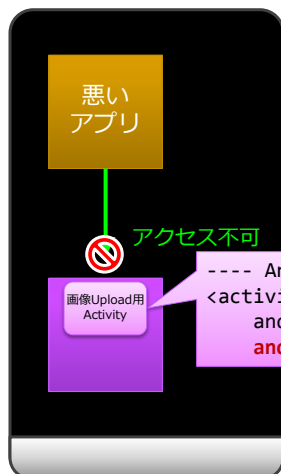
### 【原因】

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。

17 | 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



## 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

18 | 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



## 事例 2

# メッセージが盗み見られてしまうSNSアプリ

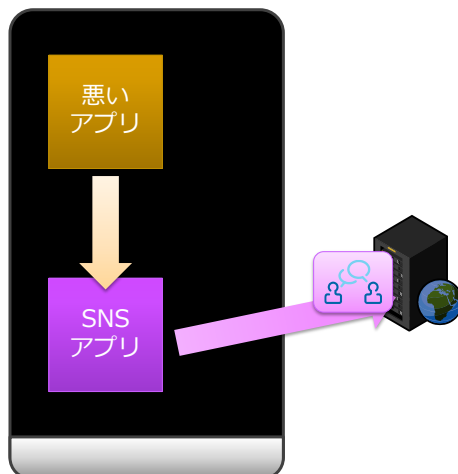
19 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会



## メッセージが盗み見られてしまうSNSアプリ

### 【問題】

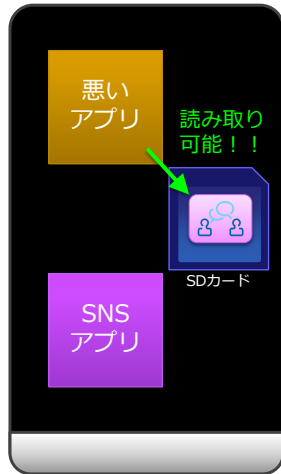
アプリが一時保存したファイルの内容を他のアプリに盗み見られてしまう問題があった。



20 | 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



## メッセージが盗み見られてしまうSNSアプリ



### 【原因】

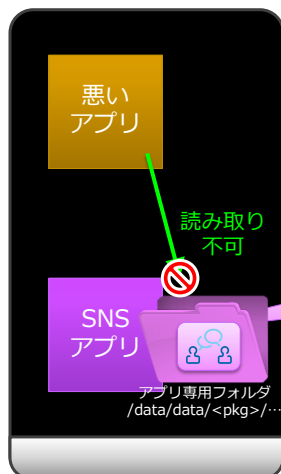
SDカード上にファイルを作成していた。

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。

21 | 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



## 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

22 | 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



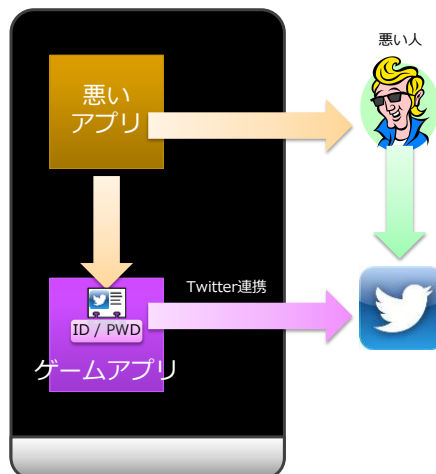
## 事例 3

# Twitterアカウントが乗っ取られてしまうゲームアプリ

23 | 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



## Twitterアカウントが乗っ取られてしまうゲームアプリ



### 【問題】

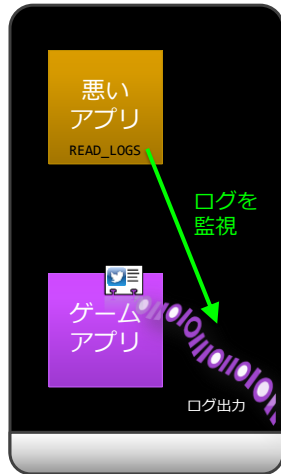
Twitter 連携用の ID/PWDが他のアプリに盗み見られてしまう問題があった。

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。

24 | 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



## 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。

25 | 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



## 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

26 | 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



## Androidアプリの脆弱性の傾向

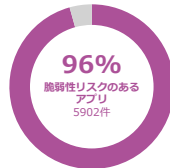
### 初歩的な問題ばかり

- exported
- ファイルの扱い
- ログ出力

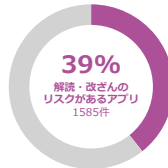
### 知っていれば防げた

JSSECセキュアコーディングガイドを読ん  
でいれば防げた

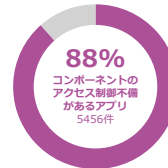
何らかの脆弱性があるアプリ  
の割合



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](http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf)

27 | 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



## 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

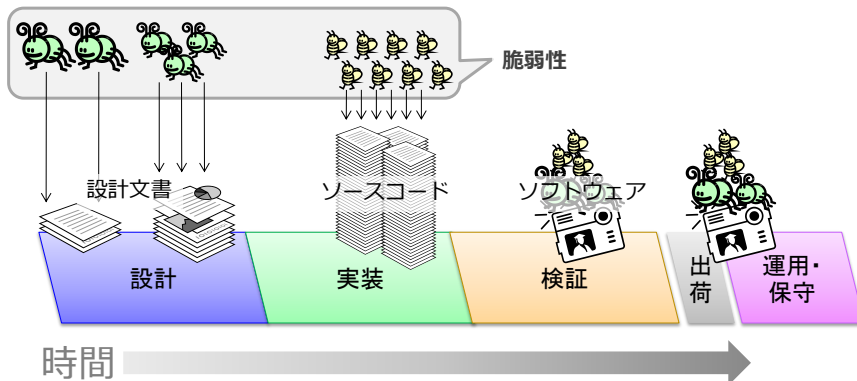
28 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会





## 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. セキュリティ人材の育成がホット！

**プログラマ**

セキュリティを考慮した

ひ込まないように注意してつくる

設計

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

実装

セキュリティ技術者

セキュリティコードレビュー

検証

セキュリティ技術者

疑似攻撃検査

出荷

運用・保守

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.

# 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

設計文書

設計

ソースコード

実装

ソフトウェア

検証

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

セキュリティ技術者

セキュリティコードレビュー

セキュリティ技術者

疑似攻撃検査

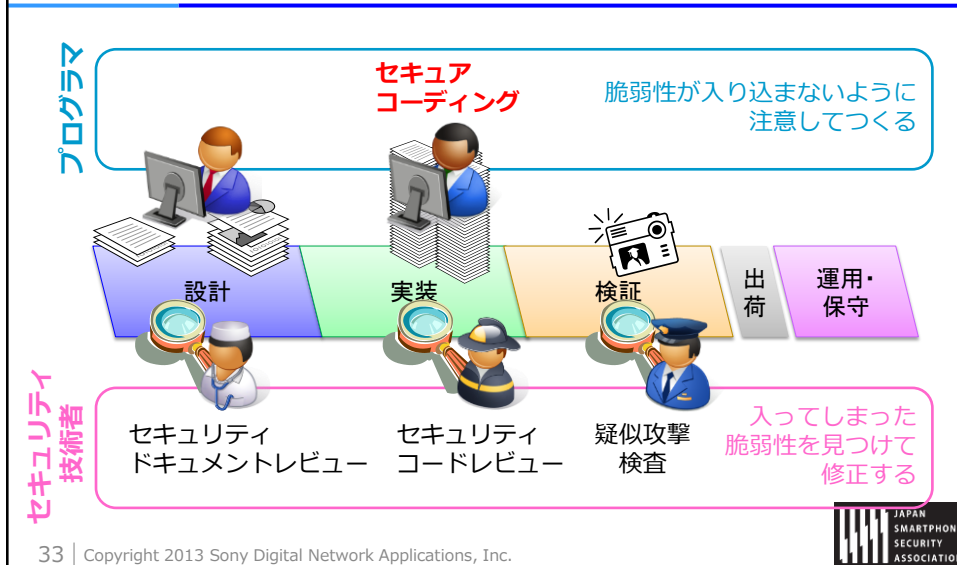
出荷

運用・保守

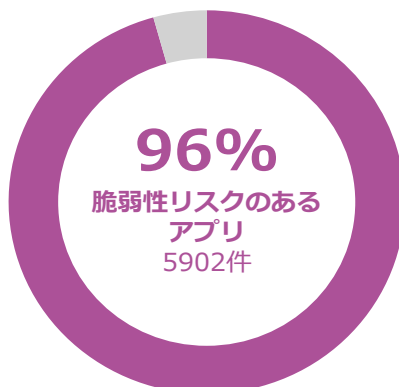
入ってしまった脆弱性を見つけて修正する

32 | Copyright 2013 Sony Digital Network Applications, Inc.

# 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

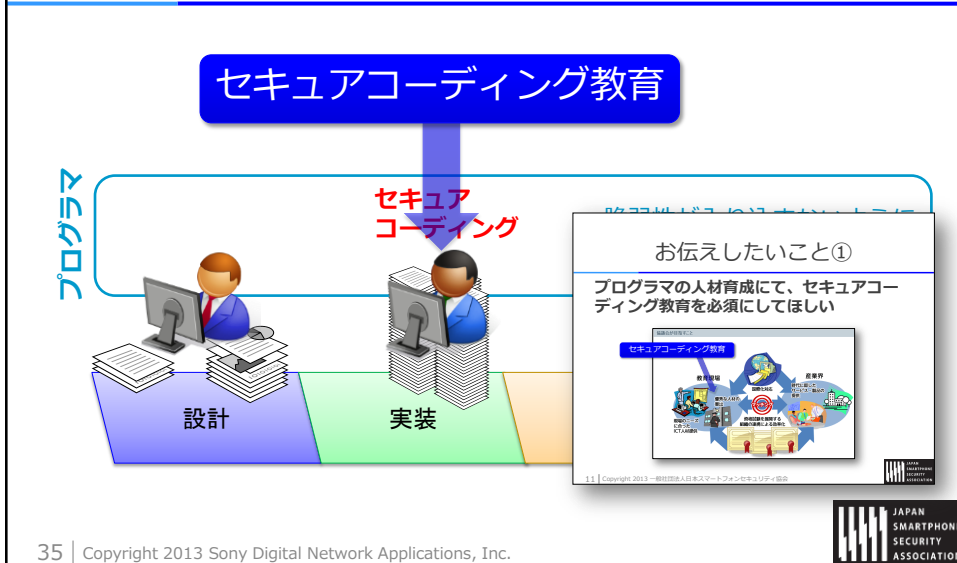
プログラマがまったく  
セキュアコーディングを  
知らない。

[http://www.sonydna.com/solution/android\\_vulnerability\\_report\\_201310.pdf](http://www.sonydna.com/solution/android_vulnerability_report_201310.pdf)

34 | 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

JAPAN  
SMARTPHONE  
SECURITY  
ASSOCIATION

# 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！



## セキュアコーディング教育

# まず効率の前に 教科書は？

37 | 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



## 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

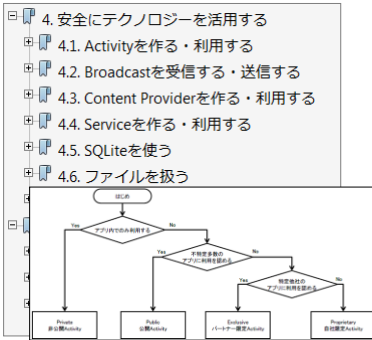
38 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会



# 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

```

AndroidManifest.xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="org.jssec.android.activity.privacyactivity"
    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 には launchMode を指定せず、値をデフォルトのまま "standard" とする -->
        <activity
            android:name=".PrivacyActivity"
            android:label="@string/app_name">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <!-- ★ポイント3★ Activity には launchMode を指定せず、値をデフォルトのまま "standard" とする -->
        <!-- ★ポイント4★ taskAffinity を用いてアフィニティを指定しない -->
        <activity
            android:name=".SupportActivity"
            android:label="@string/app_name">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </manifest>
    
```



# デファクトスタンダードな Androidセキュリティ教科書

総務省  
MIC  
Ministry of Internal Affairs and Communications

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

平成25年3月20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 株式会社が発行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。



## 課題



365頁もある！

読むのが大変！



どうするの？

41 | 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

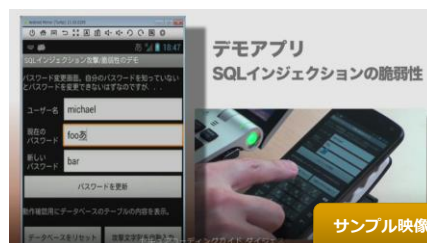


ガイドの基礎知識を手早く  
習得できるDVDを用意しました！



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！

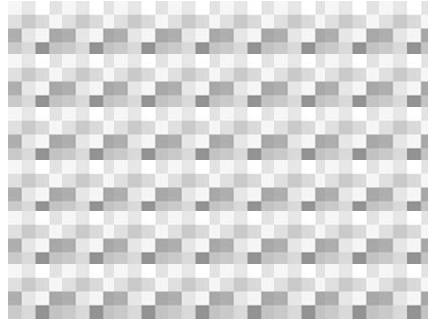


42 | Copyright 2013 一般社団法人日本スマートフォンセキュリティ協会



## 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



43 | 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



ソニーの現場でみつけた

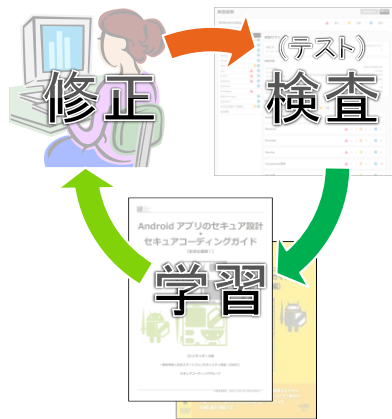
**効率よく  
セキュアコーディングを  
学習する方法**

44 | 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





## (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

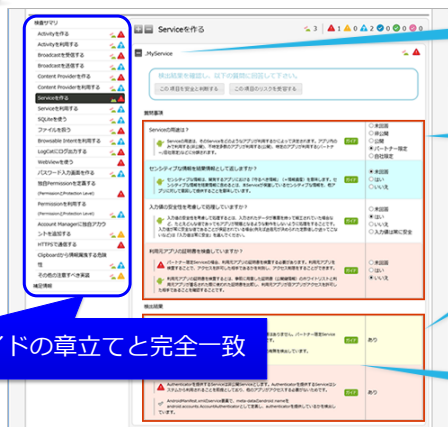
脆弱性検査ツールとプログラムの自作アプリを組み合わせることで、**理解度、学習意欲、学習効率**をすべて高められる学習方法



## 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



違反項目を指摘

用途や使い方を質問形式で確認  
⊕ 拡大表示する

違反内容に関する解説  
⊕ 拡大表示する


個々の違反について修正方法を記した  
ページヘリンク  
※修正に必要なソースも公開されています

ガイドの章立てと完全一致

<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

 Secure Coding Checker

違反内容に関する解説

intent-filterの有無

パートナー固定Serviceの場合、intent-filterを定義する必要はありません。パートナー固定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を提供するシステムから利用されることを

AndroidManifest.xmlのService要素のandroid:accounts.AccountType属性の有無を検出しています。

検査結果から教科書への導線

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。

これは 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=".PrivateStartService" android:exported="false"/>

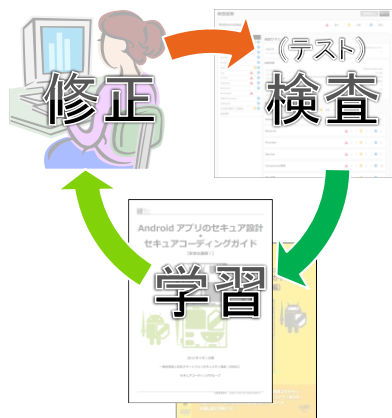
```

詳しい解説と修正方法

47 | 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

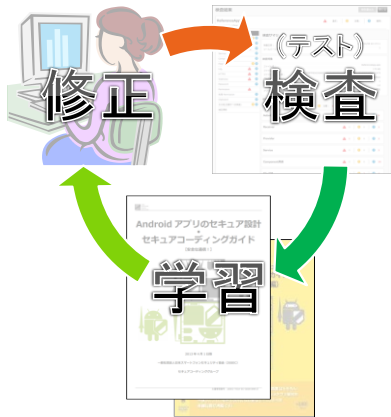
JAPAN SMARTPHONE SECURITY ASSOCIATION

## 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



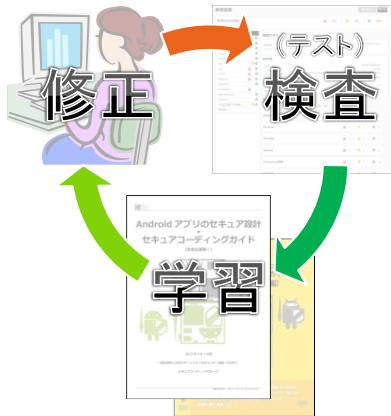
**【メリット1 理解度】**  
 自作アプリの脆弱性という具体事例を題材に学習できるので、脆弱性とセキュアコーディングの理解が深まる

**【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られるため、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】**  
 自作アプリの脆弱性を修正するために必要な学習だけに絞られるため、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

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**

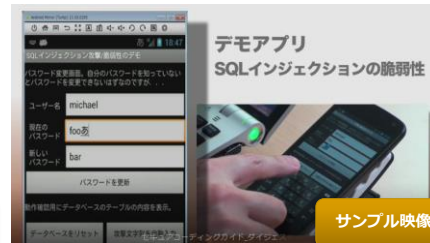
**わたしはこのガイド執筆のリーダー**

## 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！



53 | 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



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

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

Secure Coding Checker お試し版

お試しい版では、Androidアプリの脆弱性を検査するSecure Coding Checkerについて理解していただくために、機能の一部を試すことができます。

今すぐ試用してみる

**新規登録者様限定 2週間無料キャンペーン実施中!**

本サイトのお試し版でSecure Coding Checkerの機能を確認したら、ぜひ登録してフル機能をお試しください。

自分自身でAndroidアプリを開発

「問題箇所と原因、対処法をセットに指摘してくれるので、効率よく思われます。それに自分分ったapkファイルで脆弱点かわかるので、セキュリティに関する自分自身のスキルアップに繋がっています。」

自社ブランドのアプリの開発をプログラマーに発注

「以前、すべての検査を納品前の最終チェック時にやっていました。でもそこで見つかったすべての不具合に対応するのは開発時に無理でした。今は開発段階で脆弱性は解決しているので、検査結果一覧を確認するだけ、とても安心です。」

Secure Coding Checkerの特徴

Secure Coding Checkerは、あなたのアプリの脆弱性を発見、修正するためのWebベースの検査ツールです

Secure Coding Checkerは、Androidアプリの脆弱性を検査するWebベースのツールです。apkファイルをスキャンすると、脆弱性の有無を確認し、問題点があれば該当箇所と原因となる要素、修正方法を提示します。

← 今だけ！

54 | 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



# 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

■制作委員		
日本スマートフォンセキュリティ協会(JSSEC)		
技術顧問 アプリケーションワーキンググループ セキュアコーディンググループ		
リーダー	松田 勝	ユニバーサルネットワークスアプリケーションズ株式会社
メンバー	佐藤 謙吾	Android セキュリティチーム
	中川 朝暉	Android セキュリティチーム
	大内 智典	株式会社 SRA
	大平 寛之	株式会社 SRA
	藤原 智	株式会社 SRA
	藤川 未来	株式会社 SRA
	中野 正樹	株式会社 SRA
	北原 謙一	株式会社 SRA
	橋本 朝暉	株式会社 SRA
	藤本 寛史	株式会社 SRA
	安部 謙一	株式会社 SRA
	八尋 竜行	株式会社 SRA
	宮澤 孝和	株式会社 SRA
	長岡 誠記	エヌ・ティ・エス・システムズ株式会社
	竹内 朝暉	KDDI 株式会社
	八尋 正樹	一般社団法人 JPCERT コーディネーションセンター@PCERT(CO)
	藤原 朝暉	一般社団法人 JPCERT コーディネーションセンター@PCERT(CO)
	伊藤 洋生	一般社団法人 JPCERT コーディネーションセンター@PCERT(CO)
	大塚 謙	システムシステムズ株式会社
技術顧問	大塚 謙	システムシステムズ株式会社
	安部 謙一	ユニバーサルネットワークスアプリケーションズ株式会社
	藤本 寛史	ユニバーサルネットワークスアプリケーションズ株式会社
	高田 洋	ユニバーサルネットワークスアプリケーションズ株式会社
	大内 正樹	ユニバーサルネットワークスアプリケーションズ株式会社
	小室 謙	ユニバーサルネットワークスアプリケーションズ株式会社
	藤本 寛史	ユニバーサルネットワークスアプリケーションズ株式会社
	佐藤 謙吾	ユニバーサルネットワークスアプリケーションズ株式会社
	藤原 朝暉	ユニバーサルネットワークスアプリケーションズ株式会社
	山崎 一史	ユニバーサルネットワークスアプリケーションズ株式会社
	藤川 未来	ユニバーサルネットワークスアプリケーションズ株式会社
	北村 久哉	オゾンウェア株式会社
	藤原 朝暉	オゾンウェア株式会社
	松田 勝	オゾンウェア株式会社

Android アプリのセキュリティに関するセキュリティガイド		2013 年 11 月 1 日版
http://www.jssec.org/~android-security-guide		
山崎 朝暉	一般社団法人日本オンラインゲーム協会	
佐藤 正樹	日本システム開発株式会社	
藤 謙吾	日本システム開発株式会社	
大塚 謙	日本システム開発株式会社	
藤川 未来	ユニファックス株式会社	
藤原 朝暉	(執筆陣: 社名及十音順)	

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

55 | 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



## 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@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/>

56 | 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





## みなさまのご参加を



57 | 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



## 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。

58 | 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





