JSSEC　技術部会
アプリケーションWG

リーダ：竹森@KDDI

1. アプリの攻撃性検査TF（竹森@KDDI）
　　⇒「リスクウェアの分類」 2012/7頃JSSEC公開見込み

2. アプリ安全設計・セキュアコーディングTF（松並@ソニー）
　　⇒「アプリ安全設計・セキュアコーディングガイド」 近日JSSEC公開見込み

A.マーケットの運用TF（保留）
　　⇒「マーケットの安全運用」 公開や活動は調整中

B.情報収集モジュール対応TF（体制検討中）
　　⇒「安心・安全な情報収集に関する技術提言」 公開や活動は調整中

【活動報告】
JSSEC 技術部会 アプリケーションWG

セキュアコーディングTF


JSSEC成果発表会　2012年5月24日

TFリーダー：　松並　勝

<Masaru.Matsunami@jp.sony.com>

活動内容

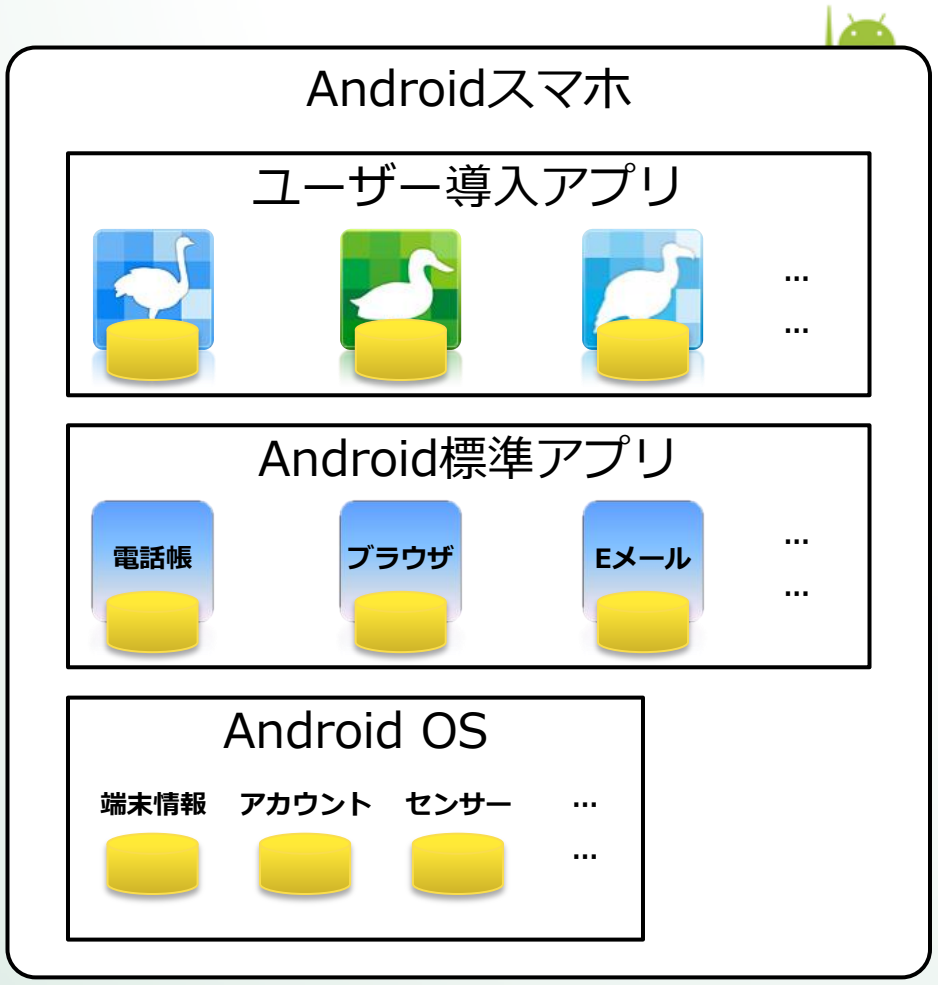
背景１

Androidスマホにはいろんな情報が入っている

情報	備考
電話番号	端末自身の電話番号
電話帳	
通話履歴	受発信の日時や番号
IMEI	携帯電話の端末ID
IMSI	回線契約者ID
各種センサー情報	GPS、地磁気、加速度…
Settings	各種設定情報…
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…
…	

情報	備考
Eメールアドレス	ユーザーのメールアドレス
Eメールのメールボックス	送受信メール本文、添付…
SMSのメールボックス	送受信SMSメッセージ本文…
Webブックマーク	
Web閲覧履歴	
カレンダー	予定、ToDo、イベント…
Facebook	アカウント、コンテンツ…
Twitter	アカウント、コンテンツ…
mixi	アカウント、コンテンツ…
…	

背景２



大雑把に言うと、情報はアプリによって管理されている

情報の保護はアプリの仕事

そのようにアプリを作るのは、アプリ開発者の仕事

活動内容

ミッション

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

趣旨

- ネット上にはセキュア設計・セキュアコーディングのTipsが分散している
- もちろん、みなさんの社内にもTips集や断片的なTipsが転がっているはず
- これらTipsを一か所に集めると、Androidアプリ開発者の助けとなる
- みんなでよってたかってTipsを集めよう

成果物

文書「Androidアプリのセキュア設計・セキュアコーディングガイド」

活動報告

活動状況

これまでの活動

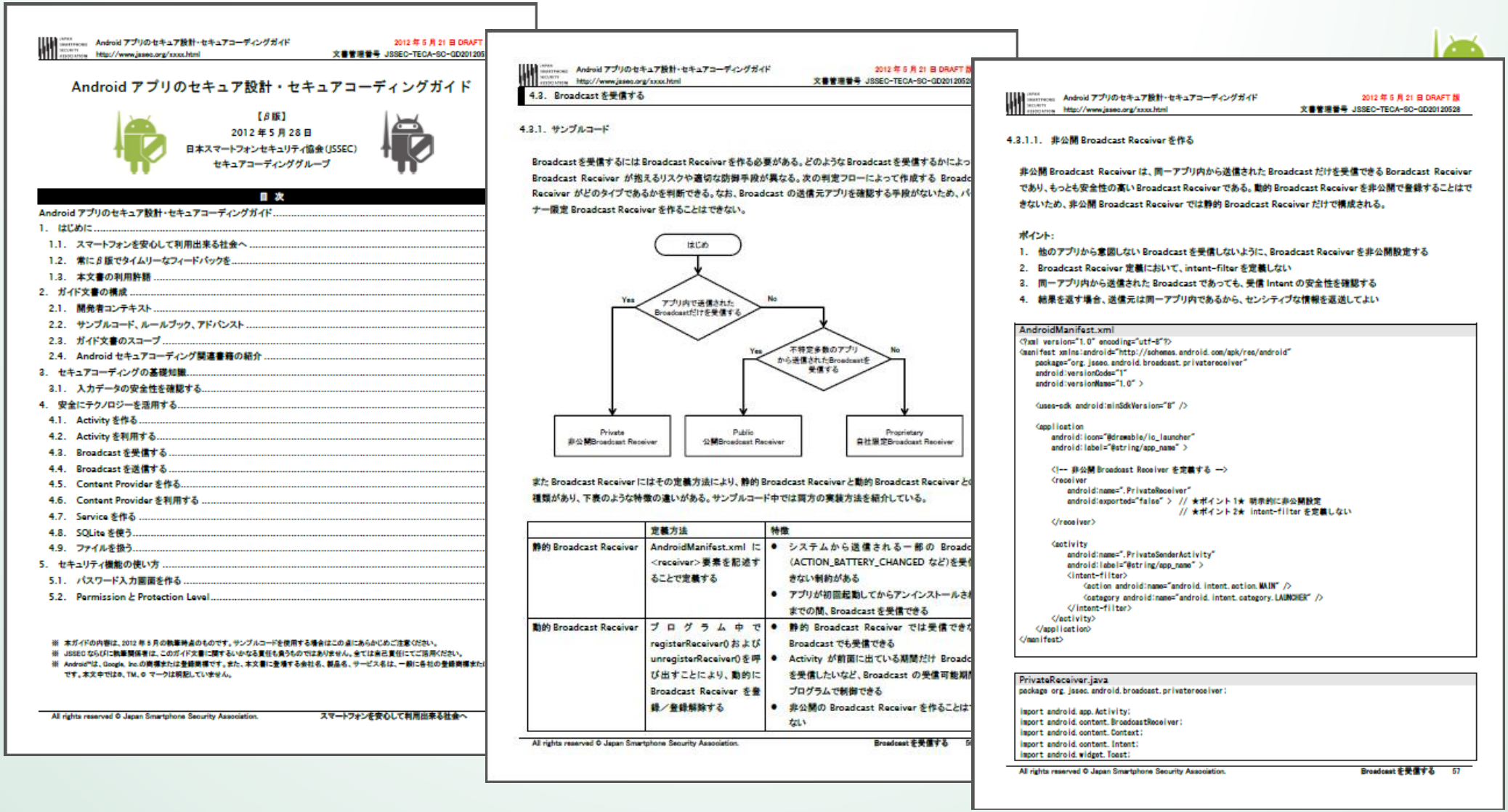
- 2011年11月末　　タスクフォースキックオフ
- 2011年12月　　タスクフォースメンバー募集
- 2012年1月～5月　　執筆活動
- 2012年5月　　JSSEC内会員パブコメ実施

現在の状況

- 約260ページのガイド文書がほぼ完成
- 公開用サンプルソースコード一式もほぼ完成
- 5月28日 初版公開に向けて文書内容調整中

ガイド文書　　http://www.jssec.org/dl/android_securecoding.pdf
サンプルコード一式　　http://www.jssec.org/dl/android_securecoding.zip

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ガイド

【β版】
2012 年 5 月 28 日
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グループ

目 次

※ 本ガイドの内容は、2012 年 5 月の執筆時点のものです。サンプルコードを使用する場合はこの点にあらかじめご注意ください。
※ JSSEC ならびに執筆関係者は、このガイド文書に関するいかなる責任も負うものではありません。全ては自己責任にてご活用ください。
※ Android™は、Google, Inc.の商標または登録商標です。また、本文書に登場する会社名、製品名、サービス名は、一般に各社の登録商標または商標です。本文中では、TM、© マークは明記していません。

スマートフォンを安心して利用出来る社会へ

4.3. Broadcast を受信する

4.3.1. サンプルコード

Broadcast を受信するには Broadcast Receiver を作る必要がある。どのような Broadcast を受信するかによっ
Broadcast Receiver が抱えるリスクや適切な防御手段が異なる。次の判定フローによって作成する Broadc
Receiver がどのタイプであるかを判断できる。なお、Broadcast の送信元アプリを確認する手段がないため、パ
ナー限定 Broadcast Receiver を作ることはできない。

また Broadcast Receiver にはその定義方法により、静的 Broadcast Receiver と動的 Broadcast Receiver と
種類があり、下表のような特徴の違いがある。サンプルコード中では両方の実装方法を紹介している。

	定義方法	特徴
静的 Broadcast Receiver	AndroidManifest.xml に <receiver> 要素を記述することで定義する	● システムから送信される一部の Broadc (ACTION_BATTERY_CHANGED など)を受 きない制約がある ● アプリが初回起動してからアンインストールさ までの間、Broadcast を受信できる
動的 Broadcast Receiver	プログラム中で registerReceiver() および unregisterReceiver() を呼び出すことにより、動的に Broadcast Receiver を登録／登録解除する	● 静的 Broadcast Receiver では受信でき Broadcast でも受信できる ● Activity が前面に出ている期間だけ Broadc を受信したいなど、Broadcast の受信可能期 プログラムで制御できる ● 非公開の Broadcast Receiver を作ることは ない

Broadcast を受信する 56

4.3.1.1. 非公開 Broadcast Receiver を作る

非公開 Broadcast Receiver は、同一アプリ内から送信された Broadcast だけを受信できる Boradcast Receiver であり、もっとも安全性の高い Broadcast Receiver である。動的 Broadcast Receiver を非公開で登録することはできないため、非公開 Broadcast Receiver では静的 Broadcast Receiver だけで構成される。

ポイント:
1. 他のアプリから意図しない Broadcast を受信しないように、Broadcast Receiver を非公開設定する
2. Broadcast Receiver 定義において、intent-filter を定義しない
3. 同一アプリ内から送信された Broadcast であっても、受信 Intent の安全性を確認する
4. 結果を返す場合、送信元は同一アプリ内であるから、センシティブな情報を返送してよい

AndroidManifest.xml

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

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

    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name" >

        <!-- 非公開 Broadcast Receiver を定義する -->
        <receiver
            android:name=".PrivateReceiver"
            android:exported="false" >  // ★ポイント1★ 明示的に非公開設定
                                        // ★ポイント2★ intent-filter を定義しない
        </receiver>

        <activity
            android:name=".PrivateSenderActivity"
            android:label="@string/app_name" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

PrivateReceiver.java

```
package org.jssec.android.broadcast.privatereceiver;

import android.app.Activity;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.widget.Toast;
```


Broadcast を受信する 57

制作関係者

総勢28名の人たちがガイド文書作成に協力

（執筆関係者、社名五十音順）

佐藤　勝彦	Androidセキュリティ部
大内　智美、比嘉　陽一、星本　英史	株式会社SRA
武井　滋紀	エヌ・ティ・ティ・ソフトウェア株式会社
久保　正樹、熊谷　裕志、戸田　洋三	一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）
大園　通、谷田部 茂	シスコシステムズ合同会社
田口　陽一	株式会社システムハウス．アイエヌジー
坂本　昌彦	株式会社セキュアスカイ・テクノロジー
安藤　彰、市川　茂、奥山　謙、佐藤　郁恵、西村　宗晃、松並　勝、山岡　一夫	ソニーデジタルネットワークアプリケーションズ株式会社
倉永　英久	株式会社大和総研ビジネス・イノベーション
谷口　岳、島野　英司、北村　久雄	タオソフトウェア株式会社
佐藤　導吉	東京システムハウス株式会社
服部　正和	トレンドマイクロ株式会社
八津川　直伸	日本ユニシス株式会社
千田　雅明	ネットエージェント株式会社
藤井　茂樹	ユニアデックス株式会社

今後の活動

今後の活動

常にβ版で継続的に更新・公開していく

- βでどんどん公開し、こまめにFeedbackしていく
- 新しいネタを継続的に追記していく

みなさまへのお願い

ガイド文書の制作にご協力いただける方を募集します。
ご連絡は下記にお願いいたします。

To: JSSEC**事務局** <sec@jssec.org>
Subject: JSSEC**セキュアコーディング参加**