JAPAN SMARTPHONE SECURITY ASSOCIATION

「Android アプリのセキュア設計・セキュアコーディングガイド」7月１日版の追加ポイント

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
奥山　謙 <Ken.Okuyama@jp.sony.com>

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

http://www.jssec.org/

Androidセキュリティの教科書

Androidアプリセキュリティのノウハウ集

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_02000043.html

総務省 MIC Ministry of Internal Affairs and Communications

JAPAN SMARTPHONE SECURITY ASSOCIATION

セキュアコーディングガイド

2014/7/17(木) に

7月1日版が

公開されました

JAPAN SMARTPHONE SECURITY ASSOCIATION

７月１日版の特徴

2014年7月1日版　改定内容

下記の新しい記事を追加致しました

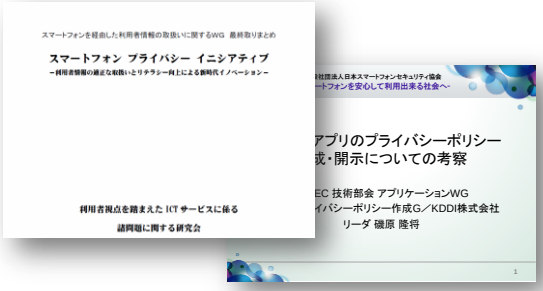
５．５　プライバシー情報を扱う

５．６　暗号技術を利用する

プライバシー情報を扱う

- 総務省SPI※１やJSSECアプリケーション・プライバシーポリシー作成G の成果※2をベースにプライバシーポリシーを組み込んだアプリケーションの実装方法を記事化しました

実装・コードに言及したドキュメントは本ガイドが初出



サンプルコード

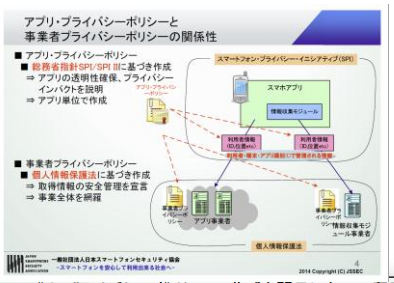
```
・・・（省略）・・・
public void onSendToServer(View view) {
        // ★ポイント3★ 慎重な取り扱いが求められる利用者情報を送信する場合は、個別にユーザーの同意を得る
        ConfirmFragment dialog = ConfirmFragment.newInstance(R.string.sendLocation, R.string.cofirmSendLocation, DIALOG_TYPE_PRE_CONFIRMATION);
        dialog.setDialogListener(this);
        FragmentManager fragmentManager = getSupportFragmentManager();
        dialog.show(fragmentManager, "dialog");
    }

    public void onPositiveButtonClick(int type) {
        if (type == DIALOG_TYPE_COMPREHENSIVE_AGREEMENT) {
            // ★ポイント1★ 初回起動時(アップデート時)に、アプリが扱う利用者情報の送信について包括同意を得る
            SharedPreferences.Editor pref = getSharedPreferences(PRIVACY_POLICY_PREF_NAME, MODE_PRIVATE).edit();
            pref.putInt(PRIVACY_POLICY_AGREED_KEY, getVersionCode());
            pref.apply();
        } else if (type == DIALOG_TYPE_PRE_CONFIRMATION) {
・・・（省略）・・・
```

※１　『スマートフォン プライバシー イニシアティブ』及び『スマートフォン プライバシー イニシアティブⅡ』
※２　「JSSEC スマホ・アプリのプライバシーポリシー作成・開示についての考察」http://www.jssec.org/event/20140206/03-1_app_policy.pdf

アプリ・プライバシーポリシーと プライバシー情報の扱い方

- プライバシーポリシーへの記載が望ましい8項目(SPIより)

①	情報を取得するアプリ提供者等の氏名又は名称	
②	取得される情報の項目	
③	取得方法	
④	利用目的の特定・明示	
⑤	通知・公表又は同意取得の方法、利用者関与の方法	
	1) 送信停止の方法	2) 送信された利用者情報の削除の方法
⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	
	1-1) 第三者提供先の事業者名	1-2) 提供先事業者の事業者プライバシーポリシー
	2-1) 情報収集モジュール名	2-2) モジュール提供者の事業者プライバシーポリシー
⑦	問い合わせ窓口	
⑧	プライバシーポリシーの変更を行う場合の手続	



■ アプリ・プライバシーポリシーの作成と開示において留意すべき事項

◆ 概要版と詳細版を通じて、解りやすくかつ正確に、プライバシーインパクトを伝える。

◆ 送信される情報の重要度に応じて、ヘルプメニューからの参照、アプリ初回起動時の参照情報の送信直前の参照など、適切なタイミングで開示・承諾を経ること。

※『スマホ・アプリのプライバシーポリシー作成・開示についての考察』「アプリ・プライバシーポリシーの作成・掲示手順の一例」より抜粋

JAPAN SMARTPHONE SECURITY ASSOCIATION

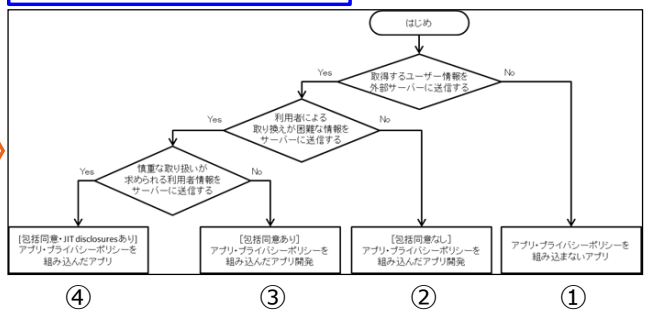
扱う情報の重要度に沿った実装方法

- プラポリ作成Gで提案された「アプリにおける対応方法」別にサンプルコードを用意

低・・・情報の重要度・・・高

該当情報(例)	作成の主旨	対応	アプリにおける対応
--- --- ブラウザエージェント OS名 バージョン情報など	不要	①	情報送信が無い旨、入力操作によって情報を送る旨などの説明をアプリの説明書や利用規約に記載する。
cookie UUIDなど +これらで管理される情報	必要	②	ヘルプメニューを入口とする、アプリ・プライバシーポリシーの参照機能を設ける。
IMEI IMSI ICCID MACアドレス OSが生成するIDなど +これらで管理される情報		③	対応②に加え、初回起動時のアプリ・プライバシーポリシーの提示による包括同意の取得を行う。
位置情報 アドレス帳 電話番号 メールアドレスなど		④	対応②と③に加え、情報送信の直前や解りやすい説明による個別同意の取得を行う。

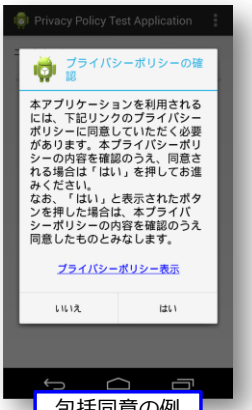
フローチャート（コード選択用）



利用者情報別の「アプリにおける対応」に１対１対応したソースコードを選択可

JAPAN SMARTPHONE SECURITY ASSOCIATION

サンプルコードを使ったアプリ（例）



包括同意の例

個別同意の例

概要版アプリ・
プライバシーポリシー

マーケット上
での説明例

JAPAN SMARTPHONE SECURITY ASSOCIATION

英語版　ー　近日公開予定

- ７月末～８月頭に ７月１日版の英語版を公開予定です


部会・WGからの報告 / 成果物

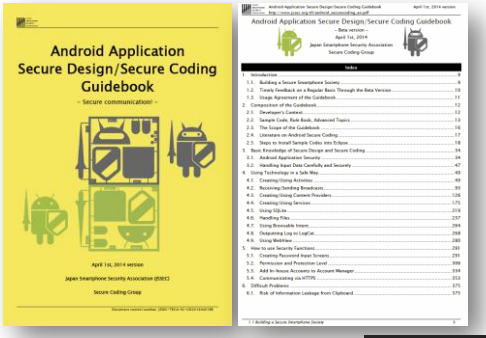
FOR IMMEDIATE RELEASE

JSSEC releases English version of
Android Application Secure Design/Secure Coding Guidebook
Sample Code

Japan Smartphone Security Association
Tokyo, Japan, 1 May 2014

Today, the Secure Coding Group (led by Masaru Matsunami) of the Japan Smartphone Security Association (JSSEC; Chairman: Hiroshi Yasuda) is releasing an English-language version of Android Application Secure Design/Secure Coding Guidebook, the industry-standard guide to ensuring application security when developing Android smartphone applications.

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



JAPAN SMARTPHONE SECURITY ASSOCIATION

プライバシー情報を扱う – 正しい利用手順

手順 1/3：プライバシー情報の利用方法を理解

総務省SPIの内容を確認し、プライバシー情報を扱う際の、利用者へのプライバシー情報利用に関する開示内容・方法を理解する

[参考資料]
総務省 “スマートフォン プライバシー イニシアティブ”
http://www.soumu.go.jp/main_content/000171225.pdf
総務省 “スマートフォン プライバシー イニシアティブⅡ”
http://www.soumu.go.jp/main_content/000236366.pdf

手順 2/3：プライバシーポリシーの作成

各種ガイドラインを元に、利用者が解りやすいプライバシー・ポリシーを作成する

[参考資料]
モバイルコンテンツフォーラム（MCF）“スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン”
http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf
JSSEC, “スマホ・アプリのプライバシーポリシー作成・開示についての考察”
http://www.jssec.org/event/20140206/03-1_app_policy.pdf

手順 3/3 ：プライバシー情報を利用したアプリの実装

セキュアコーディングガイドのサンプルコードを使い、プライバシー情報を適切に扱ったアプリを実装する

[参考資料]
JSSEC, “Androidアプリのセキュア設計・セキュアコーディングガイド”
http://www.jssec.org/dl/android_securecoding.pdf

利用者が安心して使えるアプリ