JSSEC技術部会

進化するスマホの機能とその脅威を知る

～Android11に対応したセキュアコーディングガイド最新版と スマートフォン・サイバー攻撃対策ガイドの紹介～

JSSEC技術部会

部会長 仲上 竜太(株式会社ラック)

アジェンダ

JAPAN SMARTPHONE SECURITY ASSOCIATION

進化するスマホの機能とその脅威を知る

～Android11に対応したセキュアコーディングガイド最新版と
スマートフォン・サイバー攻撃対策ガイドの紹介～

- ▶JSSEC技術部会について
- ▶Android11の新機能とセキュアコーディングガイド最新版
- ▶スマートフォン・サイバー攻撃対策ガイドのご紹介

JSSEC技術部会の活動について

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC技術部会は、スマートフォンを安全に利用するための技術的な調査・研究・議論を行っています。

主な活動内容

- ▶Androidアプリ開発におけるセキュア設計・セキュアコーディングのガイドである「Androidアプリのセキュア設計セキュアコーディングガイド」の編纂
- ▶スマートフォンを対象としたサイバー攻撃の研究と対策
- ▶スマートフォン技術の利用におけるセキュリティガイドラインの策定
- ▶スマートフォンの技術にまつわるセミナー・イベントの開催

JSSEC技術部会の活動について

■WGの紹介■

現在技術部会では、セキュアコーディングWG、ネットワークWG、マルウェア対策WGの体制で活動しています。それぞれの領域で技術調査・ガイドライン策定を実施しスマートフォンの安全な利活用に貢献します。

■セキュアコーディングWG■

WGリーダー：宮崎力（株式会社ラック）

アプリケーションに関するセキュリティ側面の情報収集、対策検討、情報提供等を通じて、スマートフォン利用の安全・安心に寄与することを目的としたWGです。
主に「Androidアプリのセキュア設計・セキュアコーディングガイド」の編纂を中心に活動しています。

■ネットワークWG■

WGリーダー：佐藤導吉（東京システムハウス株式会社）

ネットワークに関するセキュリティ側面の情報収集、対策検討、情報提供等を通じて、スマートフォン利用の安全・安心に寄与することを目的として活動しております。
過去には、以下の成果物を作成し、公開しました。
・『スマートフォンネットワークセキュリティ実装ガイド』
・『スマートフォンの業務利用におけるクラウド活用ガイド』

現在は、『位置情報ガイドライン』の作成に取り組んでおります。

■マルウェア対策WG■

WGリーダー：仲上竜太（株式会社ラック）

スマートフォンマルウエアに関する時事問題等に関して情報発信の強化を検討することを目的に活動しています。

現在、最近の事例をもとにしたスマートフォンに関する各種攻撃手法の分類と整理、時事的なトピックの定期配信を行っています。

・スマートフォン・サイバー攻撃対策ガイド

セキュアコーディングガイドのご紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

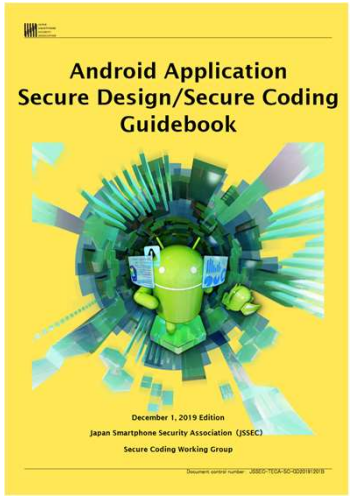
- 安全なAndroid™アプリの作り方のガイド
- 設計指針から実装まで
- 実装に便利なサンプルコードを添付
- 2012年から継続的に改訂
- 業界標準

通信キャリアや多くのアプリベンダーが活用。
アプリ外注時の受入基準となるケースも。

セキュアコーディングガイドの歴史

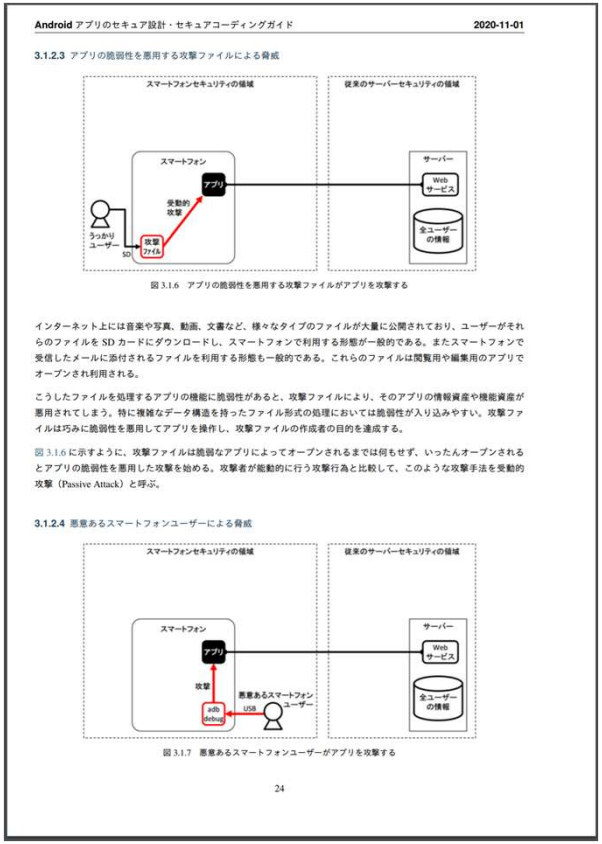
JAPAN SMARTPHONE SECURITY ASSOCIATION

- **2012年～発行**
  - 年１～２回のペースで更改
  - 最新版は2020年11月に第12版（2020年11月1日版）を発行
- **2014年～**
  - 英語版リリース
- **2019年～**
  - 中国語版リリース



セキュアコーディングガイドの使い方

- Androidアプリケーションの設計時、実装時にセキュリティを考慮することができる
- サンプルコードをコピー・ペーストすることで、セキュリティを考慮した安全なアプリケーションが開発可能
  （ApacheLicense2）
- Androidのバージョンアップに対応し、将来的な変更への対応も可能



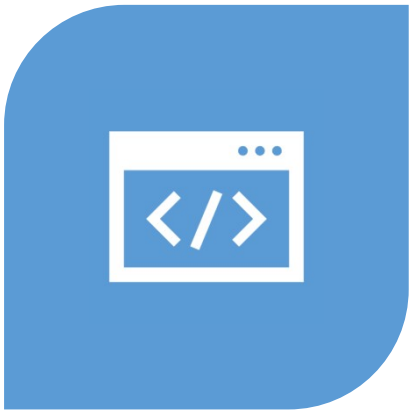
セキュアコーディングガイドの構成

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **セキュア設計・セキュアコーディングの基礎知識**
  - Androidアプリケーション開発時に必要なセキュリティの考え方を解説
- **Androidテクノロジーの安全な使用方法**
  - 開発者が実装する場面に合わせたセキュアな設計・コーディング方法を機能ごとに解説
- **Androidセキュリティ機能の使い方**
  - Androidに用意されているセキュリティ機能を使用した、アプリケーションのセキュリティ確保のための設計・コーディング方法を解説
- **サンプルコード**
  - 各機能を実装する際に使用可能なサンプルコードを掲載
  - ビルド可能なコードセットを提供

お好きな形式で読めます

JAPAN SMARTPHONE SECURITY ASSOCIATION



HTML版

PDF版

HTML版について

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **URL**
  - https://www.jssec.org/dl/android_securecoding/
  - 「セキュアコーディングガイド」で検索
- **特徴**
  - 見出しの階層構造
  - 各見出しへの直接リンク
  - ソースコードの可読性向上

セキュアコーディングWG

JSSECセキュアコーディングガイド最新版(第12版)更新ポイント

2020年度セキュアコーディングガイド最新版 更新ポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **Android11(APIレベル30)の変更に対応**
  - 機能資産におけるアプリ間の連携機能のポリシー厳密化
  - 対象範囲別ストレージの適用
  - Permissionモデルの仕様変更
  - 位置情報アクセス
  - 権限の自動リセット
  - 生態認証の変更点
  - データアクセスの監査
  - Conscryptモジュールについて

アプリ間の連携機能のポリシー厳密化

JAPAN SMARTPHONE SECURITY ASSOCIATION

ターゲットSDKをAndroid11(API Level30)以降に指定した場合、アプリ間連携機能のポリシー厳密化により、連携機能によりアクセスする可能性のある他のアプリを定義する必要がある

- **アプリの提供する機能を他のアプリから悪用されないための最小権限を定義**
  - たとえば端末の全機能にアクセス可能なセキュリティアプリの機能が悪用されるとプライバシーの侵害の恐れがある
  - 操作する他アプリのパッケージを事前に宣言
- **アプリが他のアプリを操作する場合に<queries>要素で事前にアクセス定義**
  - <queries> 要素内では、対象となるアプリのパッケージ名、インテント シグネチャ、またはプロバイダ オーソリティによってパッケージを指定できる

対象範囲別ストレージの適用

ターゲットSDKをAndroid11(API Level30)以降に指定した場合、対象範囲別ストレージ(scopedstrorage)が適用される

※API Level30以降はマニフェスト属性requestLegacyExternalStorageの設定によるバイパスは不可

- **アプリコレクション（アプリ専用のファイル）**
  - getExternalFilesDir() またはgetExternalCacheDir()を使用してアクセス
  - アプリ固有であり、アプリケーションが削除されると同時に削除される
- **メディアコレクション**
  - MediaStoreAPIでアクセス。他アプリから参照可能
  - アプリケーションが削除されても残る
- **ダウンロードファイル**
  - Storage Access Frameworkでアクセス
  - アプリケーションが削除されても残る

Permissionモデルの仕様変更

Android11より、位置情報、マイク、カメラに関連する一部のパーミッションについて、実行時に権限の付与を行う際に、「**今回のみ**」という選択肢を選べる (1回だけのアクセス許可)

- **位置情報・マイク・カメラが対象**
  - android.permission.ACCESS_FINE_LOCATION
  - android.permission.ACCESS_BACKGROUND_LOCATION
  - android.permission.RECORD_AUDIO
  - android.permission.CAMERA
- **アプリが終了したり、バックグラウンドへ移動して一定時間後に権限取り消し**

権限の自動リセット

Android11より、一部のパーミッションに対するアプリ権限が
一定期間使用されていない場合にリセットされる。

- **ターゲットSDKをAndroid11(API Level30)以降に指定した場合にデフォルトで有効**
- **Protection levelがDangerous Permissionのものが対象**
- **バックグラウンドで動作するアプリは、権限が取り消しされていないかに注意する**
  ※isAutoRevokeWhitelisted()で自動リセットの状態を確認し、ユーザに無効化設定を促す必要がある

マルウェア対策WG

スマートフォン・
サイバー攻撃対策ガイド

スマートフォン・サイバー攻撃対策ガイド

JAPAN SMARTPHONE SECURITY ASSOCIATION

スマートフォンを標的としたサイバー攻撃について、
技術的解説と対策を紹介しています

https://www.jssec.org/smartphone-malware

第1回　SMS認証の悪用、スミッシング(SMS+フィッシング)
第2回　スマホ決済の不正利用
第3回　マルバタイジング：広告ネットワークを悪用した攻撃
第4回　インターネットバンキング情報窃取
第5回　マルウェア・bot対策
第6回　偽警告・偽契約詐欺対策
第7回　偽装AP

第1回　SMS認証の悪用、スミッシング(SMS+フィッシング)

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 正規な会社を装ったSMSを送信し、メッセージに記載のURLから、実在する正規サイトとそっくりなフィッシングサイト（偽サイト）に誘導し、マルウェアのダウンロードやID情報やクレジットカード情報などを搾取する詐欺
- SMSを使ったフィッシング（Phishing）詐欺から、スミッシング（Smishing）と呼ばれる
- 攻撃者は以下の方法でSMSを送信
  - ①海外SMSアグリゲータを利用した送信
  - ②国内SMSアグリゲータを利用した送信
  - ③海外のスマホから直接送信
  - ④国内のスマホから直接送信
  - ⑤マルウェア感染したスマホからの直接送信
- 最近も⑤のパターンを観測。Androidの場合「提供元不明のアプリインストール許可」に注意する。

図 1. 郵便局を詐称した SMS

図 2. 郵便局を模倣した偽サイト

まとめ

JAPAN SMARTPHONE SECURITY ASSOCIATION

進化するスマホの機能とその脅威を知る

～Android11に対応したセキュアコーディングガイド最新版と
スマートフォン・サイバー攻撃対策ガイドの紹介～

- ▶JSSEC技術部会について
- ▶Android11の新機能とセキュアコーディングガイド最新版
- ▶スマートフォン・サイバー攻撃対策ガイドのご紹介

技術部会では参加メンバーを募集しています

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC技術部会では、以下の活動に参加していただける方を常時募集しています

- ▶セキュアコーディングガイドの執筆・レビュー
- ▶スマートフォン・サイバー攻撃対策ガイドの執筆・レビュー
- ▶技術部会主催イベントの支援・登壇

参加希望の方は、JSSEC事務局までご一報ください。

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC技術部会

進化するスマホの機能とその脅威を知る

～Android11に対応したセキュアコーディングガイド最新版と スマートフォン・サイバー攻撃対策ガイドの紹介～