

最新版セキュアコーディング ガイドのご紹介

一般社団法人 日本スマートフォンセキュリティ協会(JSSEC)
技術部会 部会長 仲上竜太
(ニューリジエンセキュリティ株式会社)

自己紹介

仲上 竜太 ,CISSP

JSSEC技術部会 部会長

ニューリジェンセキュリティ株式会社

CTO,クラウドセキュリティ事業部副部長

ソフトウェアオフショアベンチャーのち株式会社ラックに入社。サイバー・グリッド研究所長、ネットエージェント株式会社取締役、デジタルペンテストサービス部長を経て、現在は野村総合研究所とラックの合併企業であるニューリジェンセキュリティ株式会社にてCTOを務める。

研究分野：ゼロトラストセキュリティ・xR・メタバース

所属団体：

- ・日本スマートフォンセキュリティ協会(JSSEC) 技術部会 部会長
- ・日本ネットワークセキュリティ協会(JNSA)
- ・日本バーチャルリアリティ学会

委員会：

- ・総務省「Web3時代のメタバース等の利活用に向けた研究会」構成員
- ・内閣官房「デジタル市場競争会議ワーキンググループ」オブザーバー

連載：

- ・@IT「働き方改革時代のゼロトラストセキュリティ」



JSSEC技術部会のご紹介

■活動内容■

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。

「Androidアプリのセキュア設計・セキュアコーディングガイド」を毎年発行しています。

■体制■

部会長 仲上 竜太 (ニューリジェンセキュリティ株式会社)

副部会長 佐藤 導吉 (東京システムハウス株式会社)

副部会長 宮崎 力 (株式会社ラック)

ネットワークWGリーダー 佐藤 導吉 (兼務)

セキュアコーディングWGリーダー 宮崎 力 (株式会社ラック)

マルウェア対策WGリーダー 小笠原 徳彦 (Shift Security)

■活動内容■

JSSECの発行している「Androidアプリのセキュア設計・セキュアコーディングガイド」の編纂を中心に、スマートフォンに関するセキュリティ技術調査・研究を行っています。



JSSEC技術部会のご紹介

■各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3WGがメインに活動しています。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：小笠原徳彦（SHIFT SECURITY株式会社）



スマートフォンマルウェ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。

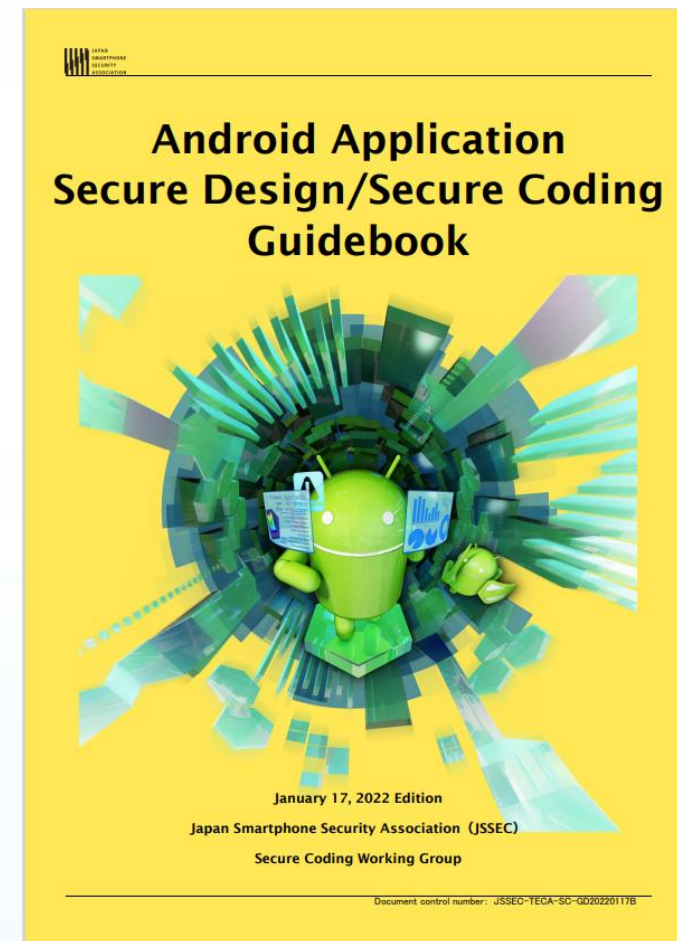
セキュアコーディングガイド のご紹介

JSSECセキュアコーディングガイド

JSSEC技術部会が発行している、Android アプリケーション開発者向けのセキュア設計、セキュアコーディングのノウハウをまとめた Tips 集。

日本語版をはじめ英語版も公開されている。

JSSECの公式サイトより無料で閲覧・ダウンロードすることができる。



改訂履歴

- 2012年に初版
- 以降年1~2回の改定を経て現在第14版
- 2018年以降はAndroid OSの更新にあわせて内容をアップデート

版数	版名	対象Android
第1版	2012年 6月版	
第2版	2012年11月版	
第3版	2013年 4月版	
第4版	2014年 7月版	
第5版	2015年 6月版	
第6版	2016年 2月版	
第7版	2016年 9月版	
第8版	2017年 2月版	
第9版	2018年 2月 1日版	Android 8
第10版	2018年 9月 1日版	Android 9
第11版	2019年 9月 1日版	Android 10
	2019年12月 1日版	Android 10
第12版	2020年11月 1日版	Android 11
第13版	2021年10月19日版	Android 12
	2022年 1月17日版	Android 12
第14版	2022年 8月29日版	Android 13

セキュアコーディングガイド更新プロセス

2月ごろ

Android
Developer
Preview

Android developer previewに搭載された機能をもとに掲載内容の方針を検討する。

4月ごろ

Android β1

新規搭載機能の検証、更新記事の執筆、サンプルプログラムの作成・確認。コラムの執筆。

6月ごろ

Android RC1

新規搭載機能の検証、更新記事の執筆、サンプルプログラムの作成・確認。コラムの執筆。

8月ごろ

Android リ
リース

執筆内容のレビューを経てリリースへ。



<https://developer.android.com/about/versions/14>

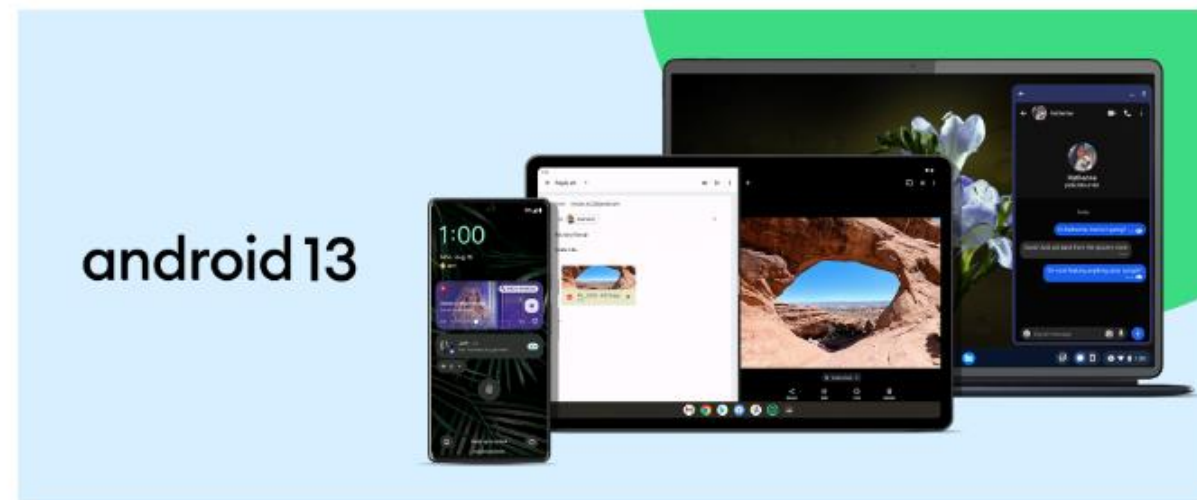
最新版 セキュアコーディングガイド 第14版更新ポイントのご紹介

Android13について

- Android OS最新バージョン13は8月16日公開
- Android13の更新をふまえたセキュアコーディングガイド第14版は8月29日に公開

Android 13 を本日より公開

2022年8月16日火曜日



Android OS の最新バージョン Android 13 は、スマートフォンなどのデバイスをあなた好みにパーソナライズできます。例えば、アプリのカラーテーマの拡張やアプリごとに異なる言語設定、より改良されたプライバシー コントロール、他にも Android デバイスでテキストや素材などをコピーして、別の Android デバイスにワンクリックで貼り付けることができます。

更新ポイント

第14版は、Android 13のアップデート内容に追従した改訂版

Android 13では、動的Broadcast ReceiverやNotificationなど、それまであった機能のうち、安全性の問題について指摘されることがあった機能のセキュリティ強化が変更点の中心となっている。

改訂内容

【下記の新しい記事を追加しました】

- 4.1.3.8. マッチしない Intent のブロックについて
- 4.2.3.8. 動的 Broadcast Receiver の安全性の強化
- 4.6.3.8. Android 13 (API Level 33) におけるメディアコレクション権限について
- 4.10.3.4. 通知に関する実行時の権限
- 5.2.3.10. 実行時の権限の取り消し
- 5.2.3.11. 新規インストールアプリでの sharedUserId の無効化

【下記の構成・内容を見直し拡充しました】

- 5.1.3.4. スクリーンキャプチャの無効化
- 5.5.3.6. 位置情報アクセスについて
- 6.1.3.2. Clipboard に格納されている情報の操作

動的 Broadcast Receiver の安全性の強化

Android 13から動的Broadcast Receiverであっても公開・非公開を明示的に設定することができるようになった。

設定手順は以下の通り。

1. DYNAMIC_RECEIVER_EXPLICIT_EXPORT_REQUIREDを有効にする
adbから設定 または 開発者オプションから指定
2. 動的Broadcast Receiver登録時、registerReceiverの引数に
RECEIVER_EXPORTEDあるいはRECEIVER_NOT_EXPORTEDを指定する

1で有効に設定した場合、2で公開・非公開をしてしなかった場合にSecurity Exceptionが発生します。

メディアコレクション権限

- メディアコレクションの権限が変更になりました
- 従来
READ_EXTERNAL_STORAGEで
動画・写真・音声にアクセス可
- Android13
READ_MEDIA_VIDEO
READ_MEDIA_IMAGES
READ_MEDIA_AUDIO
でそれぞれを要求する

きめ細かいメディア権限

Android 13 をターゲットとするアプリの場合、`READ_EXTERNAL_STORAGE` 権限や `WRITE_EXTERNAL_STORAGE` 権限ではなく、新しい権限を 1 つ以上 リクエストする必要があります。

リクエストする権限のセットは、アプリがアクセスする必要があるメディアの種類によって異なります。

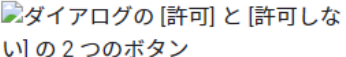
 ダイアログの [許可] と [許可しない] の 2 つのボタン

図 1. `READ_MEDIA_AUDIO` 権限をリクエストするとユーザーに表示されるシステム権限ダイアログ。

メディアの種類	リクエストする権限
画像や写真	<code>READ_MEDIA_IMAGES</code>
動画	<code>READ_MEDIA_VIDEO</code>
音声ファイル	<code>READ_MEDIA_AUDIO</code>

ユーザーが以前にアプリに `READ_EXTERNAL_STORAGE` 権限を付与していた場合は、それぞれの新しい権限がアプリに自動的に付与されます。

それ以外の場合は、アプリが前の表に示すいずれかの権限をリクエストすると、ユーザー向けダイアログが表示されます。図 1 では、アプリが `READ_MEDIA_AUDIO` 権限をリクエストしています。 `READ_MEDIA_IMAGES` 権限と `READ_MEDIA_VIDEO` 権限の 2 つを同時にリクエストした場合、システム権限ダイアログは 1 つだけ表示されます。

通知に関する実行時の権限

- Android 13から、Notificationの通知機能を利用するにはユーザーの事前許可が必要になった。
- この動作変更は、targetSdkVersionに関係なくAndroid 13プラットフォームで動作する全てのアプリに適用される。

プライバシー

通知に関する実行時の権限

Android 13（API レベル 33）では、実行時の通知権限 `POST_NOTIFICATIONS` が導入されました。この変更は、ユーザーが重要な通知に集中するのに役立ちます。

★ 注: [メディアセッション](#)に関連する通知と、通話を自己管理するアプリは、この動作変更から除外されます。

この機能による制御の強化と柔軟性の向上の効果を得るため、できるだけ早く Android 13 以上をターゲットに設定することを強くおすすめします。

詳しくは、[アプリの権限に関するおすすめの設定](#)をご覧ください。

更新執筆者の紹介

- 最新版第14版は以下のメンバーに執筆いただきました。

制作

一般社団法人 日本スマートフォンセキュリティ協会 技術部会 セキュアコーディングWG

リーダー	宮崎 力	株式会社ラック
メンバー	Pantuhong Sorasiri	株式会社ラック
	塩田 明弘	株式会社エヌ・ティ・ティ・データ
	本間 輝彰	KDDI 株式会社
	上松 晴信	KDDI 株式会社

(執筆関係者、社名五十音順)

**セキュアコーディングガイド
更新にご興味のある方へ。**

セキュアコーディングガイド更新プロセス

2月ごろ

Android
Developer
Preview

Android developer previewに搭載された機能をもとに掲載内容の方針を検討する。

Android14
のPreviewが
スタートし
ました。

4月ごろ

Android β1

新規搭載機能の検証、更新記事の執筆、サンプルプログラムの作成・確認。コラムの執筆。

6月ごろ

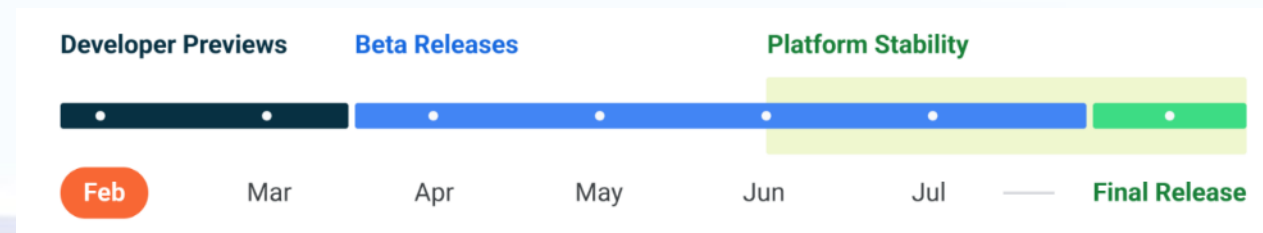
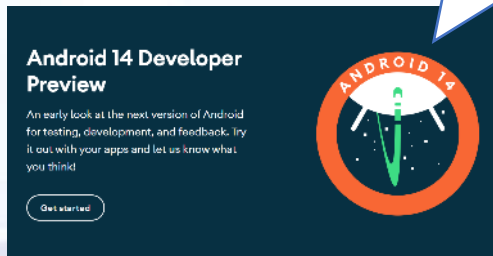
Android RC1

新規搭載機能の検証、更新記事の執筆、サンプルプログラムの作成・確認。コラムの執筆。

8月ごろ

Android リ
リース

執筆内容のレビューを経てリリースへ。



<https://developer.android.com/about/versions/14>

執筆者募集

- JSSEC技術部会セキュアコーディングWGでは、セキュアコーディングガイド本編の改定やコラム執筆に参加いただける方、興味のある方を募集しています
- 執筆参加要件は **JSSEC 会員**となります
- 問い合わせ窓口はJSSEC公式サイト問い合わせから

ありがとうございました