日本スマートフォンセキュリティ協会

技術部会活動報告

セキュアコーディングWG
技術部会・メタバースWG

2026年2月6日

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（株式会社ラック）
技術部会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）

Rev.20251212

JSSEC技術部会の活動成果(2025年度)

- アジェンダ
  - ①技術部会のご紹介
  - ②セキュアコーディングWG
    - 2025年8月27日版 改定ポイント解説
      Focus: Android 15 / 16に向けたプライバシーとセキュリティの強化
  - ③技術部会外部活動
    - 技術部会の参加する政府専門家委員会活動状況のご紹介
    - メディアへの注意喚起・技術解説への協力

JSSEC技術部会のご紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

設置趣旨

- 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・議論を行う。現在は3つのWGで構成し成果物を公開することで、日本におけるスマートフォン利用の安全性向上に寄与します。

セキュアコーディングWG　マルウェア対策WG　メタバースセキュリティWG

主な活動内容

- スマートフォン・モバイルデバイスを取り巻く新たな技術へのセキュアな対応の議論
- 技術者・開発者向けのセキュリティ情報の発信
- 変化するモバイルを対象とした脅威手法の分析

スマホ利用の安全性向上

技術的な調査や分析により、社会インフラとなったモバイル利用の信頼性を底上げ

実践的知識の提供

開発者コミュニティへ現場で使えるナレッジを提供。シフトレフト文化を醸成。

利用者保護と被害防止

脅威の実態を技術的に分析・公開することで「知る対策」による被害防止に貢献

JSSEC技術部会のご紹介

■活動内容■
JSSECでは、スマートフォンを安全に利用するための調査・研究・議論を行っています。技術部会では、セキュアコーディングWG、マルウェア対策WG、メタバースセキュリティWGが活動しています。

■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。

■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。

■メタバースセキュリティWG■
WGリーダー：仲上竜太（株式会社ラック）

スマートフォンが活用されるメタバースについてセキュリティ上の課題やプライバシーについて技術的な観点から議論を行うべく、技術部会にメタバースセキュリティWGを設置。

メタバース推進協議会、日本セキュアIoTプラットフォーム協議会とともに「メタバースセキュリティガイドライン」を策定中。

Android アプリのセキュア設計・セキュアコーディングガイド

2025年8月27日版 改定ポイント解説

Focus: Android 15 / 16に向けたプライバシーとセキュリティの強化

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WG

Android 16 (API Level 36) を見据えた改定

JAPAN SMARTPHONE SECURITY ASSOCIATION

今回の改定は、今後の「プライバシー保護の厳格化」と「コンポーネントの挙動変更」に焦点を当てています。

対象読者: Androidアプリ開発者、セキュリティ担当者

改定ポイント総覧 (1/2) - コンポーネントとNW

JAPAN SMARTPHONE SECURITY ASSOCIATION

Cat 1: インテント・コンポーネント

- Safer Intents: 明示的IntentでもFilter不一致時に受信拒否 (enforce IntentFilterフラグ)
- Intentリダイレクト対策: removeLaunchSecurityProtection() による例外解除とサブレベルIntentブロック
- 順序付きBroadcast: Android 16でのpriority指定の仕様変更

Cat 2: ネットワーク

- ローカルネットワークアクセス: LAN内デバイス (192.168.x.x等) への通信にNEARBY_WIFI_DEVICES 権限が必須化

改定ポイント総覧 (2/2) - ストレージと鍵管理

JAPAN SMARTPHONE SECURITY ASSOCIATION

Cat 3: ストレージとプライバシー

- MediaStoreバージョンのロックダウン: getVersion()の挙動変更による追跡防止 (Deep Dive対象)
- App-owned photos: Android 16での自アプリ保存メディアへのアクセス権限と「プリセレクト」挙動

Cat 4: 鍵管理 (Key Management)

- Key Sharing API: アプリ間鍵共有の仕組みとリスク
- Google Play App Signing: 鍵管理コラムの更新

そもそも「MediaStoreバージョン」とは?

JAPAN SMARTPHONE SECURITY ASSOCIATION

バージョン管理の仕組み

スマートフォンは、写真や音楽などのメディア情報を
「MediaStore」というデータベースで管理しています。

本来の用途:
DBが更新されるたびにバージョン番号を発行し、アプリ側で「キャッシュ更新が必要か」を判定するために使用します。

従来の問題点: バージョン番号が「名札」に

Fingerprinting (ユーザー追跡) のリスク

これまでの挙動では、getVersion() が返す文字列は端末ごとにユニークであり、すべてのアプリに対して「同じ値」を返していました。

- App A: 「このユーザーIDは 1506...」
- App B: 「このユーザーIDは 1506...」
- 結果: アプリ間でユーザーを名寄せ・追跡が可能に

Android 16の変更点: ロックダウン

アプリごとに「異なる顔」を見せる

Android 16以降、OSはアプリごとに「異なるランダムな値」を生成して返します。

> Lockdown効果:
> App AとApp Bで取得できる値が異なるため、名寄せや追跡が不可能になります。特定可能な情報を含まない短い文字列となります。

この変更がもたらすメリットと注意点

JAPAN SMARTPHONE SECURITY ASSOCIATION

一般ユーザーの方へ

特別な設定をしなくても、OSが自動的にアプリ間の追跡（フィンガープリント）を防止します。行動履歴が不透明に共有されるリスクが大幅に低減します。

開発者の方へ

getVersion() の値をデバイスIDやユーザーIDの代わりに使用してはいけません。あくまで「キャッシュの再構築判定」のみに使用してください。

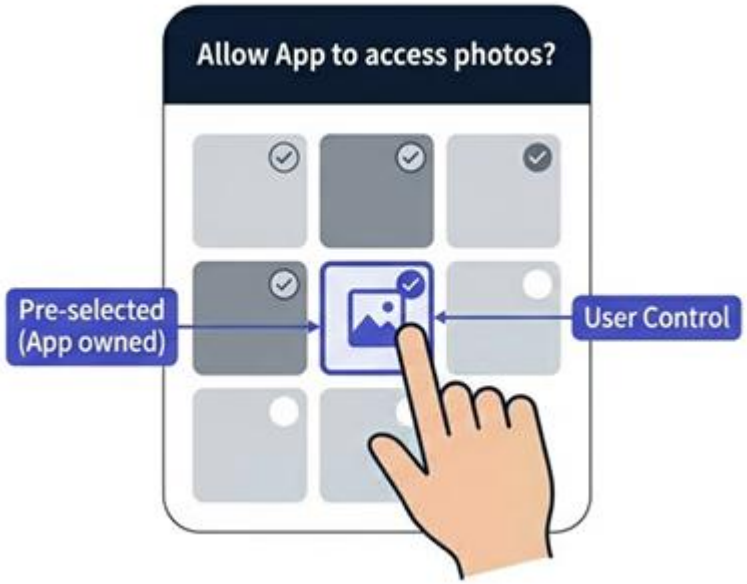
注目ポイント: 自アプリ写真へのアクセス権

JAPAN SMARTPHONE SECURITY ASSOCIATION

ユーザー主権の強化 (App-owned photos)

Android 16では、アプリ自身が保存した写真へのアクセス権限がより直感的になります。

- プリセレクト機能: 権限リクエスト時、自アプリが保存した写真は「最初からチェックが入った状態」で表示されます
- ユーザーの拒否権: ユーザーはこのチェックを外すことで、アプリ自身のデータであってもアクセスを拒否可能です。



注目ポイント: ローカルNWの保護

家庭内のデバイスを守る

従来、アプリはLAN内のIPアドレス（192.168.x.x等）を自由にスキャンできましたが、これが制限されます。

変更点:
ローカルネットワークへの通信には、新たに
NEARBY_WIFI_DEVICES
権限が必要になります。

Impact:
ユーザーの許可なく、勝手に自宅ネットワーク内のデバイスを探索する行為が防がれます。

まとめ: セキュリティからプライバシーへ

JAPAN SMARTPHONE SECURITY ASSOCIATION

1. 追跡の防止

MediaStore IDの分離により、アプリ間追跡が不可能に。

2. 境界の強化

自宅LANやIntent連携の境界線がより厳格に。

3. ユーザー主権

自アプリ生成データでもユーザーが制御可能に。

Action: targetSdkVersion 36 の挙動変化を早期に確認してください。

Reference / 参照元

Android アプリのセキュア設計・セキュアコーディングガイド
2025年8月27日版

一般社団法人日本スマートフォンセキュリティ協会 (JSSEC)

- https://www.jssec.org/dl/android_securecoding/ガイド文書
- https://www.jssec.org/dl/android_securecoding.zip (サンプルコード)

※ 詳しい実装コードや例外処理については、ガイドの「4.6.3.11」および「更新履歴」を参照してください。

技術部会対外活動のご紹介

- 技術部会では省庁主催の専門家委員会にて構成員・オブザーバーとしてご下命いただき、各種行政諸課題への対応についてプライバシーおよびサイバーセキュリティの観点で議論に参加しています。

総務省様

ICTサービスの利用環境の整備に関する研究会
不適正利用対策に関するワーキンググループ

ICTサービスの利用環境の整備に関する研究会
利用者情報に関するワーキンググループ

総務省　情報流通行政局
没入型技術の利活用促進に向けたマルチステークホルダー連携会合

情報通信政策研究所　調査研究部
Web3時代に向けたメタバース等の利活用に関する研究会（安心･安全なメタバースの実現に関する研究会）

公正取引委員会様

マートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する検討会

技術部会対外活動のご紹介①

ICTサービスの利用環境の整備に関する研究会
不適正利用対策に関するワーキンググループ

- **活動趣旨**:
  - 電気通信の不適正利用対策について新たな対策を検討
  - いわゆる「闇バイト」犯罪や特殊詐欺への対策
  - 携帯電話契約時の本人確認ルールの見直し
  - SMS等による不適正利用対策

主な検討事項:

•SIMの不正転売対策

•法人の代理権確認（在籍確認）

•他社の本人確認結果への依拠

•追加回線の本人確認

•上限契約台数の見直し

•データSIMの本人確認

•固定・携帯電話、SMS・メール対策

•スプーフィング対策

•海外電話番号による詐欺電話対策

日本における犯罪の実態に照らし合わせた、電気通信サービスの改善による犯罪対策の推進

技術部会対外活動のご紹介①

総務省　情報流通行政局
没入型技術の利活用促進に向けたマルチステークホルダー連携会合

- **活動趣旨**:
  - VR/AR/MR等の没入型技術の利活用促進に関する課題の議論
  - 「メタバースの原則」のさらなる改定の検討
  - 国民への啓発の在り方の検討
  - マルチステークホルダー(仮想空間提供者、デバイスメーカー、ビジネスユーザー等)の知見共有と連携促進

- **主な検討事項**:
- 没入型技術の利活用促進に関する事項
  - 医療・教育・製造・建設・行政等での社会課題解決への適用
  - ビジネスユーザーのユースケース共有
  - 技術の安全性と実用性の両立
- 「メタバースの原則」に関する事項
  - 原則の継続的な改定・更新
  - 国際標準との整合性確保
  - 実務への適用可能性の検討
  - その他関連事項
- 国民への啓発方法
  - 国際動向への対応(OECD GFTech、IGF、DPC、EC等との連携)
  - ステークホルダー間の共通言語形成

VR/AR/MR等の没入型技術の社会実装を安全かつ効果的に促進するため、官民学の多様なステークホルダーが参画する日本初の本格的な連携プラットフォーム

技術部会対外活動のご紹介①

マートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する検討会

- **活動趣旨**:
  - 「スマホソフトウェア競争促進法」の運用における検討
  - セキュリティの確保や青少年保護等を図りつつ、特定ソフトウェアに係る競争を促進
  - 政令や公正取引委員会規則、ガイドラインの内容を検討

- **主な検討事項**:
- スマートフォンにおける特定ソフトウェア（os、アプリストア、ブラウザ等）の競争環境整備
- セキュリティと競争促進のバランス
- 青少年保護の確保
- 多様なイノベーションの活性化
- 消費者の選択肢拡大

ビッグテックが独占的に提供するスマートフォンにおいて、利用者の安全や利便性を確保しつつも競争的環境を醸成するための具体策を法律・技術の観点から議論

JSSEC技術部会の活動成果(2025年度)

- アジェンダ
  - ①技術部会のご紹介
  - ②セキュアコーディングWG
    - 2025年8月27日版 改定ポイント解説
      Focus: Android 15 / 16に向けたプライバシーとセキュリティの強化
  - ③技術部会外部活動
    - 技術部会の参加する政府専門家委員会活動状況のご紹介
    - メディアへの注意喚起・技術解説への協力

技術部会メンバーの募集

- 各種ガイドラインの策定、政策への提言やコメント提出、モバイル脅威の解説記事執筆、メディア対応など、技術部会に依頼いただく案件の対応メンバーを募集しています。

- JSSEC事務局までお問合せください

JSSEC で検索ください。