資料１－３

スマートフォン／モバイルにおけるセキュリティ課題とJSSECの取り組み

～モバイルセキュリティの現状～

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
（ニューリジェンセキュリティ株式会社・株式会社ラック）

自己紹介

仲上 竜太 ,CISSP
日本スマートフォンセキュリティ協会技術部会 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部長

奈良県出身。電気通信大学卒。ソフトウェアオフショアベンチャーにて2008年からスマートフォンアプリの開発に従事。その後、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にてスマートフォン・IoT向けセキュリティ診断サービスの運営を経て、現在は野村総合研究所とラックの合弁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)
・サイバーセキュリティイニシアチブジャパン
・日本バーチャルリアリティ学会

委員等：
・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(2022-2023)
・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(2022-)
・総務省「安全安心なメタバースの実現に向けた研究会」構成員(2023-)

連載：
・@IT「働き方改革時代のゼロトラストセキュリティ」

日本スマートフォンセキュリティ協会(JSSEC)のご紹介

■活動内容■

2011年に発足。スマートフォンやモバイルアプリケーション・IoTを安全に利用するための調査・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。

一般社団法人
日本スマートフォンセキュリティ協会

■目的■

- 企業・団体における利用者が安心して高度なサービスを受けられるようにする。
- 実装すべきセキュリティレベルの理解を社会に浸透させ、提供者が安心して事業推進を行えるようにする。
- 利用者のセキュリティリテラシー向上のための活動も行い、さらに高度なサービスを受けられるようにする。
- セキュリティを切り口とした「信頼できるニッポン！」を確立しグローバル市場へアピールする。

■体制■

会長

佐々木　良一	学校法人 東京電機大学

副会長

米田　章宏	ソフトバンク株式会社
富山　由希子	株式会社NTTドコモ
本間　輝彰	KDDI株式会社

理事

東　博暢	株式会社日本総合研究所
北村　裕司	サイバートラスト株式会社
佐々木　良一	学校法人 東京電機大学
下村　正洋	特定非営利活動法人日本ネットワークセキュリティ協会
末政　延浩	株式会社TwoFive
米田　章宏	ソフトバンク株式会社
デイビッド　チャン	株式会社 EMPRESS SOFTWARE JAPAN
西本　逸郎	株式会社ラック
本間　輝彰	KDDI株式会社

JSSEC技術部会のご紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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（ニューリジェンセキュリティ株式会社）

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。

総務省「Web3時代に向けたメタバース等の利活用に関する研究会」「安全安心なメタバースの実現に向けた研究会」委員

モバイルセキュリティの現状

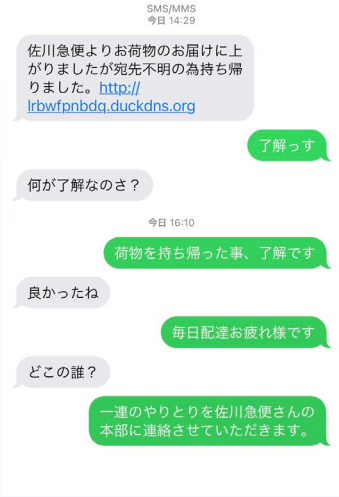
スマートフォン・モバイルにおけるサイバー脅威

■2024年現在もスマートフォンを始めとするモバイルデバイスに対する脅威は増加傾向にあり、組織や個人に被害が生じている状況

スマートフォン利用シーンに潜む脅威 Top 10 2023	
第１位	依然猛威を振るうスミッシング詐欺
第２位	なりすまし契約とアカウント詐取
第３位	ディープフェイク
第４位	メールを狙った様々な攻撃 ～フィッシングメール・ビジネスメール詐欺、ランサムウエアの脅威など～
第５位	提供元不明アプリによるマルウェア感染
第５位	誹謗・中傷
第７位	SNS フェイクニュース
第８位	アカウント乗っ取りと誤ったアカウント登録
第９位	検索エンジンの汚染
第１０位	不正通販サイト
ランク外	アプリストアのマルウェア感染
	不適切なパスワード管理
	スマホカメラの悪用
	短縮 URL 問題
	盗難・紛失

「スマートフォン利用シーンに潜む脅威Top10 2023」
日本スマートフォンセキュリティ協会会員および有識者による、スマートフォン利用シーンに潜む10大脅威を2023年に選定。

■ スミッシング(SMS+Phishing：SMSを使った詐欺）



被害の形態
①スマートフォンのショートメッセージに左図のような「宅配」や「金融機関へのログイン」を装ったメッセージが届く
②URLにアクセスすると、実際のものとそっくりなログイン入力画面（偽の画面）にアクセスする
③入力したIDとパスワードが窃取される

メール送信者の実態
左図に見られるように一般ユーザの端末が**不正アプリに遠隔操作**されて送られている。返信されても無自覚なため覚えがない。

「迷惑メールに返信したら返事がきた、怖い→全く関係無い一般人が本人も気づかず送ってしまっている「知らずに煽っていました」」https://togetter.com/li/1727086
より引用

スマホアプリにおける脅威

■ **スマホアプリ（スマートフォンアプリケーション）におけるサイバー脅威は2つの観点で考える必要があります**

■ **スマホアプリ脆弱性（セキュリティホール）**

- スマホアプリやサービスに内在する悪用可能な不具合
- サイバー攻撃者が脆弱性を悪用してアプリの正規利用者に対して、不正行為や個人情報の窃取を行う
- アプリだけでなく、アプリから参照するウェブサービスの脆弱性が悪用されるケースも存在する
- アプリ開発者がセキュリティを意識した実装を行うなどの自主的な対策による防御が求められる
- どんなに気を付けても完全に脆弱性の発生を回避することは困難

■ **不正アプリ（マルウェア）**

- 攻撃者が悪意を持って作成し、リモート操作や個人情報の窃取、端末の破壊など、不正を目的としたスマホアプリ
- 不正アプリであることが発覚しないよう、別の目的をもったアプリのふりをして流通させる
- **セキュリティ制限の少ない提供元不明のアプリの許可を悪用**し、正規のアプリ流通手段以外でインストールさせる

スマホアプリ脆弱性（セキュリティホール）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■スマホでできることが増え、重要かつ機微なデータが蓄積される一方、開発者は脆弱性を作りこまないよう開発する必要があります

	モバイルアプリケーション開発 10 大チェックポイント 2023
M1	プラットフォームの不適切な利用
M2	不適切なクレデンシャルの利用
M3	クライアントコードの品質と安全性
M4	安全でない通信
M5	安全でない認証
M6	不十分な暗号化
M7	安全でない認可制御
M8	コード改ざん
M9	安全でないデータストレージ
M10	余計な機能

「モバイルアプリケーション開発10大チェックポイント2023」
2016年以降更新のなかったOWASP Mobile Top 10の派生として日本スマートフォンセキュリティ協会会員および有識者により2023年に選定。その後OWASP Mobile Top 10 2024に合流。

■ 不適切なクレデンシャルの利用

本カテゴリは、APIキーやクラウドサービスのクレデンシャルなどのハードコードなどが対象です。

ハードコードされたAPIキーやクレデンシャルは、リバースエンジニアリングによって漏洩する恐れがあり、これによってAPIやクラウドサービスが侵害される可能性があります。

例：
・アプリケーションバイナリへの書き込み
・暗号化されていない転送
・ソースコード管理サイトへの共有

OWASP Mobile Top10 2016→2024

- OWASP=Open Worldwide Application Security Project Webをはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティ

- OWASP Mobile Top 10
  開発時に注意すべき脆弱性をTop10を領域ごとにOWASPの有識者がオープンな議論のもと選定し発表。
  モバイルアプリケーション開発におけるTop10は2016年の発表以降活動が休止していました。

Comparison Between 2016-2024		
OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

https://owasp.org/www-project-mobile-top-10/

「クレデンシャルの平文埋め込み」に当たるものが候補には出たものの圏外になっていたので、「私たちは日本のJSSECというスマートフォンセキュリティの団体だよ。私たちのTop10ではこうなっていて、クレデンシャルの平文埋め込みは高いリスクがあると考えているんだ」と述べた

「モバイルアプリケーション開発 10大チェックポイント 2023」選定の裏話
https://www.jssec.org/column/20230724.html

アプリ流通経路における脅威の低減

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **「アプリ脆弱性」「不正アプリ」ともに利用者に被害を生む可能性のあるスマホアプリの脅威ですが、流通経路の責任において一定のセキュリティ確保が可能です**
- **公式アプリストアでは「不正アプリ」の発見と排除を行うための審査が、厳格に行われている必要があります**
  - 利用者からすれば、サードパーティを含む公式ストアで配布されているアプリ＝信頼できるアプリの認識が生じている
  - ポリシーによる制約に加え、ストア運営者による審査によって不正アプリを排除されている
  - アップデート後に挙動が変化するアプリも存在するため、継続的に不正アプリを発見する取り組みが求められる

アプリの脆弱性は開発者による主体的な対策が可能ですが、不正アプリについてはサードパーティを含むアプリストア運営者が、ユーザに提供するアプリの品質と安全性について責任を持つ必要があります。
一方、現在Androidで許容ウェブからのアプリインストール（いわゆるサイドローディング）は**審査をなんら経由しないため**不正なアプリ配信の温床になっている実態があります。

ポリシー センター > モバイルの望ましくないソフトウェア > モバイルの望ましくないソフトウェア

モバイルの望ましくないソフトウェア

Mobile Unwanted Software

Google には、「成功の条件はユーザーを第一にすること」という理念があります。Google のソフトウェア原則と望ましくないソフトウェアのポリシーでは、優れたユーザー エクスペリエンスを提供するソフトウェアに関する一般的な推奨事項を紹介しています。このポリシーは、Google の望ましくないソフトウェアのポリシーを土台とし、と Google Play ストアの原則を概説するものです。原則に反するソフトウェアはユーザーの利便性に悪影響を与える可能性があるため、Google はそうしたソフトウェアからユーザーを守る措置を取ります。

望ましくないソフトウェアのポリシーに記載のとおり、望ましくないソフトウェアの大半にいくつかの共通点があります。

- 表示に虚偽がある。すなわちできていないことをできると約束している。
- ユーザーをだましてインストールさせようとする、または別のプログラムのインストールに便乗する。
- ユーザーにメインとなる重要な機能の一部を説明していない。
- ユーザーのシステムに予期しない方法で影響を与える。
- ユーザーが気付かないうちに個人情報を収集または送信する。
- 安全な処理（HTTPS による送信など）を行わずに個人情報を収集または送信する。
- 他のソフトウェアとバンドル（同梱）され、その存在が開示されていない。

Googleのモバイルアプリポリシー（抜粋）
https://support.google.com/googleplay/android-developer/answer/9970222?hl=ja

不正アプリの流通に対するストアの対策

Android エコシステムのセキュリティ(抜粋)
Google Play(公式ストア) での PHA のインストール率
https://transparencyreport.google.com/android-security/store-app-safety?hl=ja

- **Androidスマートフォンプラットフォームを提供するGoogle社は、OSの機能で不正アプリ(PHA: Potentially Harmful App)流通量をモニタリングしています**
- **本データでは2020年以降インストール率の上昇が確認できます**
- **Google社は不正対策としてアプリを特定して排除を行っています**

参考事例

- 2022/10
  クリッカーマルウェアが潜む16のアプリ、「Google Play」ストアから削除
  https://japan.zdnet.com/article/35195032/
- 2022/10
  「Facebookでログイン」を装うログイン情報盗用。悪質なアプリに注意
  https://www.watch.impress.co.jp/docs/news/1446185.html

不正アプリ検証の方法と課題

■ 開発者が主体的に対策可能なアプリ脆弱性と比較して、不正アプリの検証は一般的に難易度の高い取り組みです

■ 不正アプリはサイバー攻撃者が隠ぺいするため、アプリの詳細な解析が必要となります

■ （参考）不正アプリ検証手法

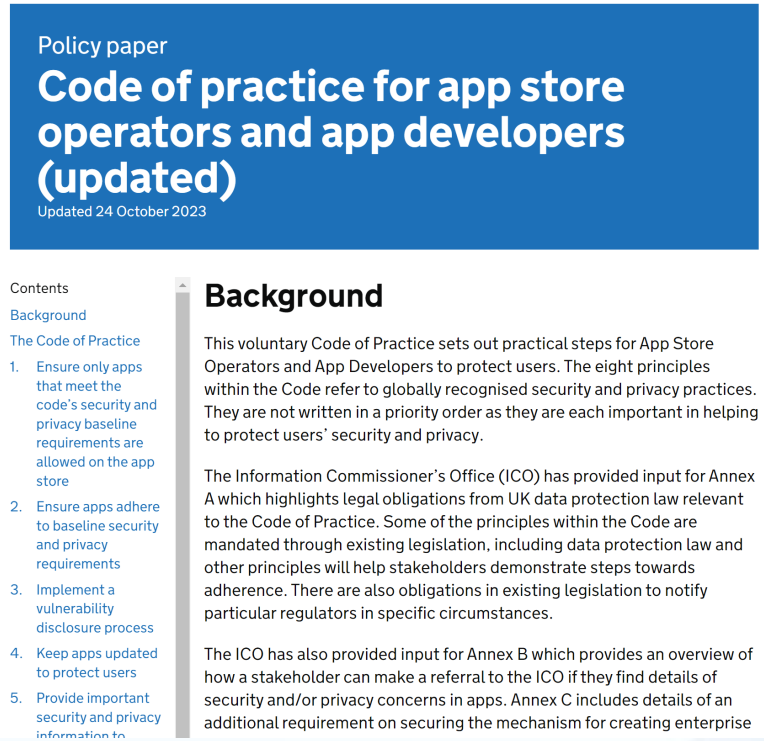
静的解析 動かさずに解析	アプリケーションをソースコードに戻せる範囲で戻し、行っている処理や設定方法を分析する方法。 大規模なアプリケーションではソースコードからの解析に時間がかかってしまう。
動的解析 動かして解析	利用者と同じ条件でアプリケーションを動作させ、不正な通信や個人情報の窃取、リモート操作などが行われないかを監視する検証方法。 動的解析中に不正動作が起こらない可能性がある。

一般的な不正アプリ調査では静的解析と動的解析を組み合わせて調査を行いますが、時間的・リソース的（費用的）制約の中で実施する必要があります。

■ 既存の公式アプリストア（Google PlayやAppStore）でも不正アプリの一定数の見逃しがあり、事後で排除する取り組みが行われています

モバイル開発者・ストア運営者に求められる実施規範

- **スマホ・モバイルアプリ開発者およびアプリストアは、アプリを提供する際のセキュリティ確保において大きな役割を担っています**
- アプリ開発者においてはセキュア設計・セキュア実装による安全なアプリケーション開発の実施や、サービスにおける個人情報保護の方針を定めたプライバシーポリシーの策定と遵守が求められます
- 各モバイルOS提供者による公式アプリストアでは、配布前のアプリケーション審査や配布後の追跡によるセキュリティ対策が実施されています
- 英国DSIT(科学・イノベーション・技術省)はモバイルエコシステムにおけるストア解放の議論に先立ち、アプリ開発者およびストア運営者に対して実施規範（Code of practice）を提示しています
- 日本国内においてもモバイルエコシステムの議論が進んでおり、日本スマートフォンセキュリティ協会では内閣官房「デジタル市場競争会議ワーキンググループ」にてセキュリティ面での意見発出のほか、これらの実施規範を含む先進事例をもとにガイドライン策定を推進しています。



Policy paper

Code of practice for app store operators and app developers (updated)

Updated 24 October 2023

Contents

Background

The Code of Practice

1. Ensure only apps that meet the code's security and privacy baseline requirements are allowed on the app store
2. Ensure apps adhere to baseline security and privacy requirements
3. Implement a vulnerability disclosure process
4. Keep apps updated to protect users
5. Provide important security and privacy information to

Background

This voluntary Code of Practice sets out practical steps for App Store Operators and App Developers to protect users. The eight principles within the Code refer to globally recognised security and privacy practices. They are not written in a priority order as they are each important in helping to protect users' security and privacy.

The Information Commissioner's Office (ICO) has provided input for Annex A which highlights legal obligations from UK data protection law relevant to the Code of Practice. Some of the principles within the Code are mandated through existing legislation, including data protection law and other principles will help stakeholders demonstrate steps towards adherence. There are also obligations in existing legislation to notify particular regulators in specific circumstances.

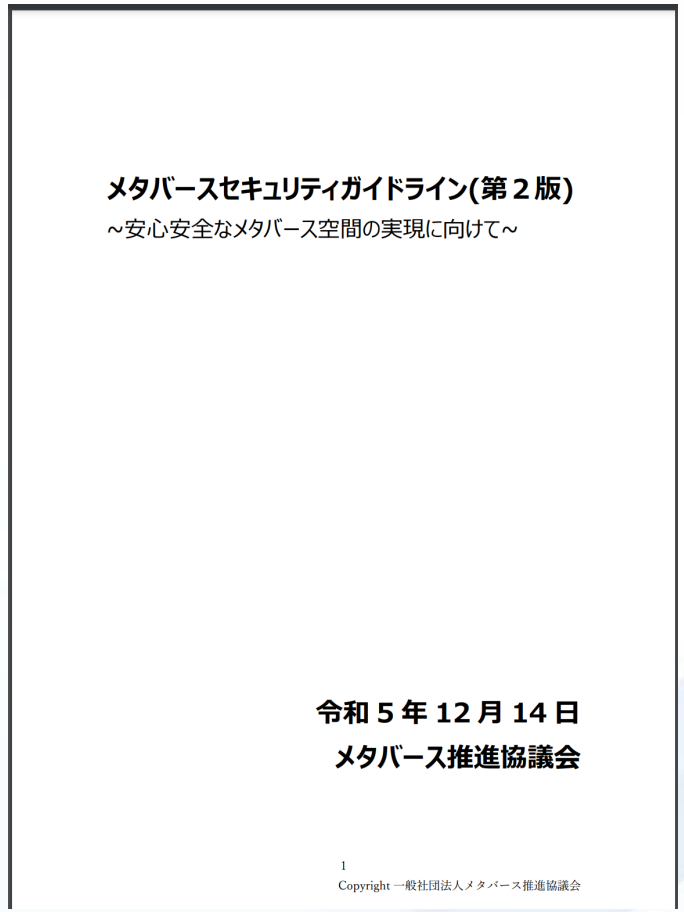
The ICO has also provided input for Annex B which provides an overview of how a stakeholder can make a referral to the ICO if they find details of security and/or privacy concerns in apps. Annex C includes details of an additional requirement on securing the mechanism for creating enterprise

Code of practice for app store operators and app developers
Department for Science, Innovation and Technology, Gov UK.
https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

新たな技術におけるセキュリティの考え方

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **IoT・Web3・メタバース・生成AIなど新たなテクノロジーにおいて、多くの場合スマホ／モバイルアプリケーションもユーザの入り口として活用されています**
- JSSECでは、スマホ／モバイルに関連する新たな技術におけるセキュリティ対策の考え方の整理、悪用による不正行為が行われるケースに対する調査および対策の検討を行っています
- **IoTデバイス・システムに対して**
  - **IoTセキュリティチェックシート第2.1版（JSSEC利用部会）**
  - 一般企業がIoTを利用・導入する際に検討すべきことを網羅的にまとめたもの
  - IT側（情報セキュリティ）とOT側（組込みや制御系）の認識を見える化
  - 一般企業がIoT導入時に考慮すべき項目を俯瞰的にA3両面60項目に集約
- **メタバースに対して**
  - **メタバースセキュリティガイドライン（第2版）**
  - メタバース推進協議会／IoTプラットフォーム協議会／日本スマートフォンセキュリティ協会の共同執筆
  - スマホ／モバイルを入口とする新たなデジタルコミュニケーション形態に対してプラットフォーム運営者や空間提供者が考慮すべきセキュリティ対策について取りまとめたもの



参考）組織・個人が行うべき不正アプリ対策

■スマートフォンでのアプリ利用に関しては、一見安全そうなアプリが「不正アプリ」に変化する場合もあります

■アプリの導入に関しては個々人が細心の注意を払うべき状況と言えます

業務利用におけるスマホの利用管理・許可リスト化

モバイル設定管理 MDMまたはEMMと呼ばれる	・企業や組織で利用するスマホアプリやアプリの機能を制限する ・貸与するスマホを所持する従業員の利用状況（アプリ操作時間・移動場所・連絡先など）を把握する ・紛失したスマホのデータ消去

※私的スマホの利用範囲の制限が課題

企業や組織が貸与するスマホはモバイル設定管理による利用制限・統制が可能ですが、個人所有のスマホについては利用ルールの設定などの人的な運用で縛る必要があります。しかし、人的運用による効果の有効性については課題があります。

ご清聴いただき、
ありがとうございました。