セキュリティフォーラム2025
JSSEC技術部会成果発表②

モバイルを取り巻く脅威のトレンド変化とセキュリティの考え方

2025年 2月18日（火）

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

概要

日々激化するスマートフォンやモバイルデバイスを取り巻く脅威のトレンドは、生成AIの登場によって新たなパラダイムを迎えています。

JSSEC技術部会では、モバイルを狙ったサイバー攻撃技術の分析をもとに、ICTの利活用やプライバシーガイドライン、メタバースのセキュリティなどの提言を行っています。

本講演では、技術部会の様々な取り組みを通じて、これからのモバイルの新たなセキュリティの在り方を解説します。

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。
2011年より「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。

JSSEC技術部会の紹介(1/3)

■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　宮崎力（株式会社ラック）

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）
メタバースセキュリティWGリーダー 仲上竜太（兼務）

■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技術部会の紹介(2/3)

■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。

■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。
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』

■メタバース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）

現在新たなネットの利用形態として注目されているメタバースにおいては、スマートフォンやスマートフォンOSを使用したデバイスがその接続に際して中心的なデバイスになりつつある。
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を運営している。

技術部会ではオンラインでの活動を推進しています。
JSSECのKintoneやTeamsにて各WGの持つコミュニケーションシステムで成果物の生成や議論を進めています。お気軽にご参加ください。

スマートフォン・モバイルにおけるサイバー脅威

スマートフォン・モバイルにおけるサイバー脅威

JAPAN SMARTPHONE SECURITY ASSOCIATION

■スマートフォンはデジタル空間＝実社会における情報空間と密接したインターフェースでありデバイスであり、多くのサイバー犯罪被害の「入り口」となっている現状です。

◢ 情報セキュリティ10大脅威 2025 [個人]

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	6年連続9回目
インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
クレジットカード情報の不正利用	2016年	10年連続10回目
スマホ決済の不正利用	2020年	6年連続6回目
偽警告によるインターネット詐欺	2020年	6年連続6回目
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
フィッシングによる個人情報等の詐取	2019年	7年連続7回目
不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続7回目
ワンクリック請求等の不当請求による金銭被害	2016年	3年連続5回目

「情報セキュリティ10大脅威」
情報処理推進機構が発表する年度ごとのセキュリティ脅威。個人編・組織編に分かれる。セキュリティ有識者が選定。

■ 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「金融機関への口グイン」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

スマホアプリ脆弱性（セキュリティホール）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■スマホの多機能化にともない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。

OWASP-2016	OWASP-2024リリース	2016-2024年の比較
M1: 不適切なプラットフォームの使用	M1: 不適切な認証情報の使用	新規
M2: 不適切なデータ保存	M2: 不十分なサプライチェーンセキュリティ	新規
M3: 不適切な通信	M3: 不適切な認証/認可	M4とM6がM3に統合
M4: 不適切な認証	M4: 不十分な入力/出力検証	新規
M5: 不十分な暗号化	M5: 不適切な通信	M3からM5に移動
M6: 不適切な認可	M6: 不十分なプライバシーコントロール	新規
M7: クライアントコード品質	M7: 不十分なバイナリ保護	M8とM9がM7に統合
M8: コード改ざん	M8: セキュリティ設定ミス	再定義 [M10]
M9: 逆アセンブル	M9: 不適切なデータ保存	M2からM9に移動
M10: 不要な機能	M10: 不十分な暗号化	M5からM10に移動

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

OWASP Mobile Top 10 2024
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年に選定した「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」 の活動をOWASP Mobile Top 10 2024に提言

■ 注目：不適切な認証情報の使用

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

スマホアプリの脆弱性の悪用ケース

■ **OWASP Mobile Top 10に掲載されるようなスマホアプリに作りこまれる脆弱性は、以下のようなケースにより悪用される可能性があります**

不適切な認証・セッション管理

アプリケーションが適切な認証メカニズムを実装していない場合、攻撃者はセッションハイジャックや不正アクセスを行うことができます。

悪用ケース:
ユーザーがログイン後にセッションIDが適切に管理されず、攻撃者がセッションIDを盗むことで、ユーザーアカウントに不正アクセスが可能になります。
特に、セッションIDがURLに含まれている場合や、認証トークンが暗号化されていない場合に悪用されます。

不適切なデータ保存

モバイルアプリケーションが機密データ（パスワード、個人情報、クレジットカード情報など）を安全でない方法で保存する場合、攻撃者がデバイスを物理的にアクセスした際にデータが流出する危険があります。

悪用ケース:
アプリケーションが平文でパスワードやその他の機密情報をデバイスに保存していると、デバイスが盗まれたり、悪意のあるアプリによってアクセスされたりすることで、保存されたデータが不正に抽出されます。

不十分なサプライチェーンセキュリティ

サードパーティのライブラリやソフトウェアコンポーネントにマルウェアやバックドアが含まれている場合、攻撃者はそのライブラリを悪用してアプリケーションやそのユーザーを攻撃することができます。

悪用ケース:
アプリケーション内で利用しているオープンソースが悪意ある開発者によって不正なコードが埋め込まれ、アップデートによって知らずに組み込まれることがあります。

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

アプリ流通経路における脅威の低減

- **「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

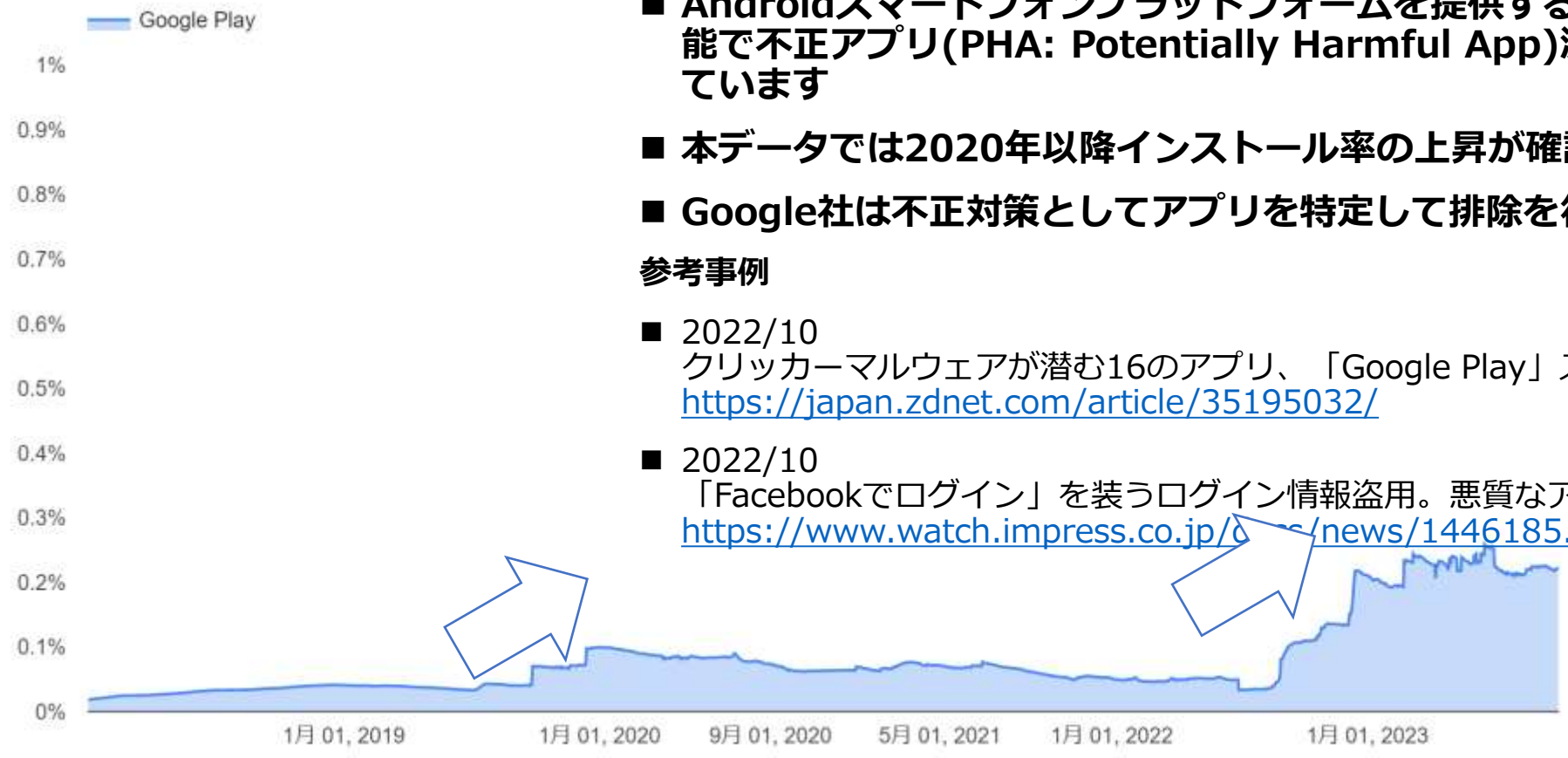
Google には、「成功の条件はユーザーを第一にすること」という理念があります。Google のソフトウェア原則と望ましくないソフトウェアのポリシーでは、優れたユーザー エクスペリエンスを提供するソフトウェアに関する一般的な推奨事項を紹介しています。このポリシーは、Google の望ましくないソフトウェアのポリシーを土台とし、と Google Play ストアの原則を概説するものです。原則に反するソフトウェアはユーザーの利便性に悪影響を与える可能性があるため、Google はそうしたソフトウェアからユーザーを守る措置を取ります。

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/[illegible]/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

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。

■個人の不正アプリ対策は…

- 入れない：意図しないアプリのダウンロード画面が表示された場合「キャンセル・拒否」してください
- 見ない：操作していないのにSMSなどで認証や確認メッセージが来ても、そのURLを見ないでください
- 騙されない：まっとうな企業を装ってあの手この手で騙しにくることを知っておいてください

JSSEC技術部会の活動とスマホセキュリティ対策

モバイル開発者に求められる実施規範を公表

■ **2024年3月 JSSEC技術部会 公表**

「スマートフォンアプリケーション開発者の実施規範 第1版」
～スマートフォンのアプリ開発および提供時に求められる対策について～

■ スマートフォン（以下、スマホ）の普及から 10 年以上が経過し、Google Play や App Store などのアプリケーションマーケット（以下、アプリマーケット）では、多数のスマホ向けアプリケーション（以下、アプリ）が提供されています。アプリマーケットは、利用者の安全を確保するために、様々な条件や規制を定めています。しかし、アプリ提供者がアプリのセキュリティに取り組む方法は、明確な手順書やドキュメントが存在していないため、提供者によって異なるのが現状です。

■ 本実施規範では、アプリ開発者がアプリ提供に際して利用者を保護するための具体的な手順を定めています。

【スマートフォンアプリケーション開発者の実施規範 作成タスクフォース】

リーダー　本間輝彰（KDDI株式会社）


スマートフォンアプリケーション開発者の実施規範

～スマートフォンのアプリ開発および提供時に求められる対策について～

【第一版】

2024 年 03 月 08 日

日本スマートフォンセキュリティ協会（JSSEC）
技術部会

Androidモバイルアプリケーションのセキュア開発ガイドライン

■ **2025年1月 JSSEC技術部会 最新版公表**

「Androidアプリのセキュア設計・セキュアコーディングガイド」

■ Androidアプリケーションのセキュリティを考慮した設計・開発のノウハウを集めた文書です。

■ アプリケーション開発現場で「使う」ことを想定した文書構成が特徴

■ 各テーマの文書は、忙しい開発者向けにお手本となるサンプルコードを紹介したサンプルコードセクション、サンプルコードの背景にあるセキュリティ観点の留意事項をまとめたルールブックセクション、さらにセキュリティの理解を深めるための話題をまとめたアドバンストセクションで構成されています。

→最新版ポイントをセキュリティフォーラム成果発表についてご説明

【JSSECセキュアコーディングガイド】

リーダー　宮崎力（株式会社ラック）

各省庁・団体でのスマホセキュリティに関する議論への参加

■ **JSSECは、スマートフォンを取り巻くテクノロジーや不正利用への対策への各省庁・団体での検討に参加しています**

■ **ICTの不正利用について**
総務省「ICT不適正利用対策に関するワーキンググループ」構成員

■ **スマホサービスにおける利用者情報の取り扱いについて**
総務省「利用者情報ワーキンググループ」構成員

■ **メタバースの利活用について**
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」構成員
総務省「安心・安全なメタバースの実現に関する研究会」構成員

■ **メタバースセキュリティについて**
メタバース推進協議会メタバースセキュリティ分科会

■ **スマホアプリストア等競争の促進について**
公正取引委員会「ス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」委員
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

メディアへのスマートフォンセキュリティの啓発

■ニュース／報道番組やウェブメディア、新聞等にスマートフォンセキュリティに関する情報発信や啓発活動を行っています

週刊BCN「拡大するモバイルへの脅威、対策製品は進化を遂げる」

https://www.weeklybcn.com/journal/feature/detail/20240729_205297.html

東洋経済オンライン「盗撮される？「スマート家電」が乗っ取られる恐怖～家族の安全のために取るべき「ハッキング対策」

https://toyokeizai.net/articles/-/831550

TBS NEWSDIG
効果はある？スマホ「週1回 再起動」…米NSAも推奨　「Cookie受け入れ」リスクは？【Nスタ解説】

https://newsdig.tbs.co.jp/articles/-/1219138?display=1&mwplay=1

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


メタバースセキュリティガイドライン(第２版)
~安心安全なメタバース空間の実現に向けて~
令和５年12月14日
メタバース推進協議会

ご清聴ありがとうございました。
部会へのご参加お待ちしております。

https://www.jssec.org