JSSEC技術部会活動報告

JSSEC技術部会長

仲上竜太

株式会社ラック サイバー・グリッド・ジャパン
CISSP

株式会社ラック

Agenda

1. JSSEC技術部会のご紹介
2. スマートフォン・サイバー攻撃対策ガイド
3. JSSECセキュアコーディングガイド
4. スマートフォンのセキュリティを高める技術イベントの開催

JSSEC技術部会のご紹介

■2021年度JSSEC技術部会のご紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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（株式会社ラック）
副部会長　佐藤導吉（東京システムハウス株式会社）
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 仲上竜太（兼務）

部会長　仲上竜太
株式会社ラック
デジタルペンテストサービス部 部長
兼サイバー・グリッド・ジャパン
情報処理安全確保支援士, CISSP
「デジタルペネトレーションとセキュリティ研究の立場からスマホの安全を考えます。」

副部会長　佐藤導吉
東京システムハウス株式会社
モバイルビジネス部
シニアスペシャリスト
「暗号、プライバシー保護等のソフトウェア開発に10年以上の実績があります。」

■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。

現在Android12に対応した第13版の編纂を進めています。編集に参加したい方は技術部会セキュアコーディングWGまでご参加ください。
また今年度は、ネットワークWG、マルウェア対策WGの活動を開始しました。

■JSSEC部会紹介/技術部会のご紹介

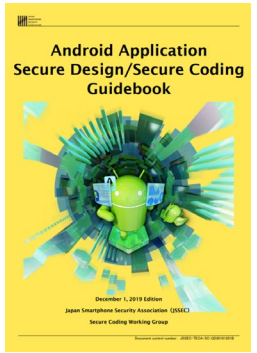
JAPAN SMARTPHONE SECURITY ASSOCIATION

■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■

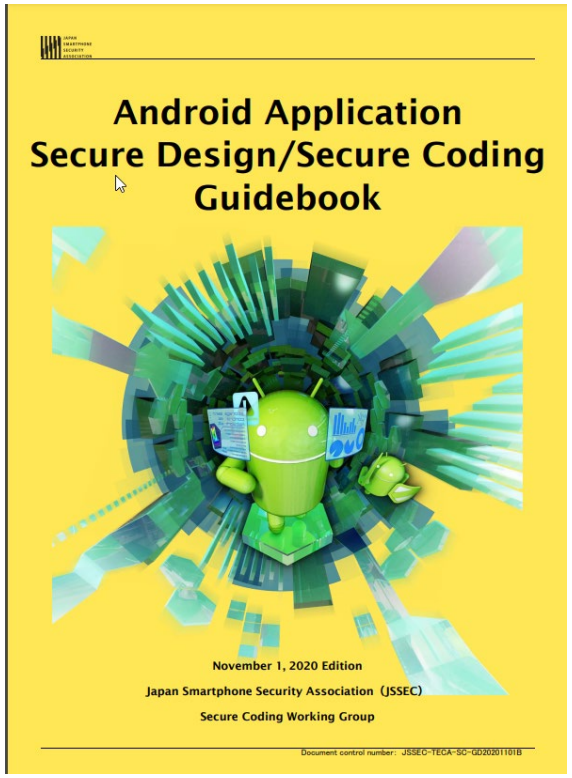
WGリーダー：仲上竜太（株式会社ラック）

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。

技術部会ではオンラインでの活動を推進しています。
オフラインでの定期会合は実施せず、Slackもしくは各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。また、不定期でスマホ技術に関連したセミナーも開催しています。お気軽にご参加ください。

JSSECセキュアコーディングガイド

JSSECセキュアコーディングガイド



https://www.jssec.org/report/securecoding.html

JSSECセキュアコーディングガイド

で検索

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 ガイドライン。
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。

Androidアプリの安全な開発を行うための設計・コーディングガイド

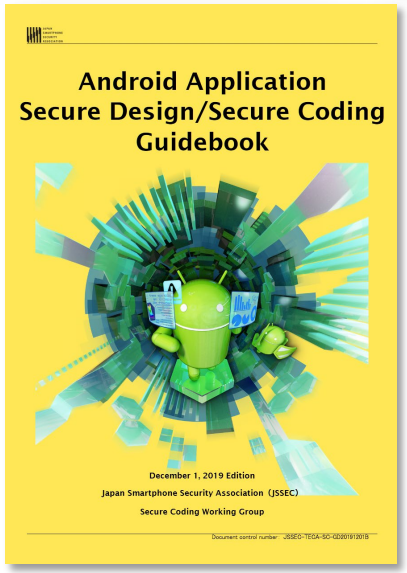
JSSECセキュアコーディングガイド

- 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でも活用。
受入基準にするアプリ発注会社もある。

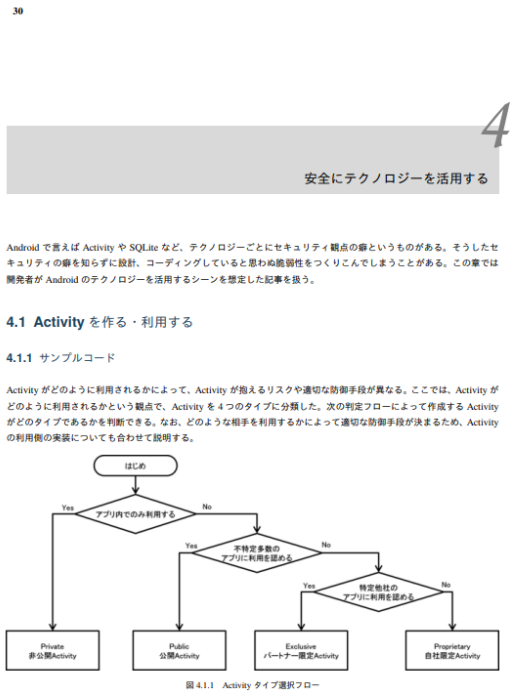
JSSECセキュアコーディングガイド

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



JSSECセキュアコーディングガイド

- 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



30

4

安全にテクノロジーを活用する

Android で言えば Activity や SQLite など、テクノロジーごとにセキュリティ観点の癖というものがある。そうしたセキュリティの癖を知らずに設計、コーディングしていると思わぬ脆弱性をつくりこんでしまうことがある。この章では開発者が Android のテクノロジーを活用するシーンを想定した記事を扱う。

4.1 Activity を作る・利用する

4.1.1 サンプルコード

Activity がどのように利用されるかによって、Activity が抱えるリスクや適切な防御手段が異なる。ここでは、Activity がどのように利用されるかという観点で、Activity を 4 つのタイプに分類した。次の判定フローによって作成する Activity がどのタイプであるかを判断できる。なお、どのような相手を利用するかによって適切な防御手段が決まるため、Activity の利用側の実装についても合わせて説明する。

図 4.1.1　Activity タイプ選択フロー

4.1.1.1 非公開 Activity を作る・利用する

非公開 Activity は、同一アプリ内でのみ利用される Activity であり、もっとも安全性の高い Activity 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　2022-01-17

同一アプリ内だけで利用される Activity（非公開 Activity）を利用する際は、クラスを指定する明示的 Intent を使えば誤って外部アプリに Intent を送信してしまうことがない。ただし、Activity を呼び出す際に使用する Intent は第三者によって読み取られる恐れがある。そのため、Activity に送信する Intent にセンシティブな情報を格納する場合には、その情報が悪意のある第三者に読み取られることのないように、適切な対応を実施する必要がある。

以下に非公開 Activity を作る側のサンプルコードを示す。

ポイント (Activity を作る) :

1. taskAffinity を指定しない
2. launchMode を指定しない
3. exported="false" により、明示的に非公開設定する
4. 同一アプリからの Intent であっても、受信 Intent の安全性を確認する
5. 利用元アプリは同一アプリであるから、センシティブな情報を返送してよい

Activity を非公開設定するには、AndroidManifest.xml の activity 要素の exported 属性を false と指定する。

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
          package="org.jssec.android.activity.privateactivity" >

  <application
      android:allowBackup="false"
      android:icon="@drawable/ic_launcher"
      android:label="@string/app_name" >

    <!-- 非公開 Activity -->
    <!-- ★ポイント 1★ taskAffinity を指定しない -->
    <!-- ★ポイント 2★ launchMode を指定しない -->
    <!-- ★ポイント 3★ exported="false"により、明示的に非公開設定する -->
    <activity
        android:name=".PrivateActivity"
        android:label="@string/app_name"
        android:exported="false" />

    <!-- ランチャーから起動する公開 Activity -->
    <activity
        android:name=".PrivateUserActivity"
        android:label="@string/app_name"
        android:exported="true" >
      <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
      </intent-filter>
    </activity>
  </application>
</manifest>
```

PrivateActivity.java

```
/*
 * Copyright (C) 2012-2021 Japan Smartphone Security Association
```

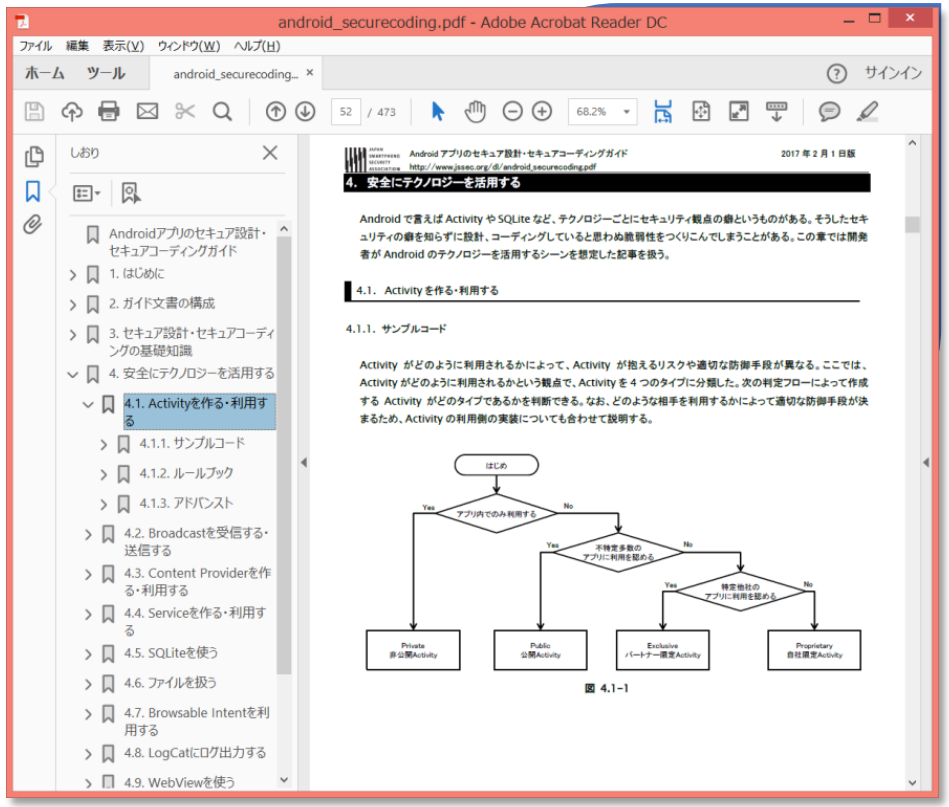
(continues on next page)

31

JSSECセキュアコーディングガイド

英語版も公開

PDF版ガイド



HTML版

JSSECセキュアコーディングガイド第12版（2020年）

Android 11では、許可のオートリセットや対象範囲別ストレージをはじめとするプライバシーに関する仕様の多くが追加・変更となった。

セキュアコーディングガイド第12版の改訂内容は以下の通り

(Android 11対応)

・Android 11（API Level 30）における対象範囲別ストレージの適用について

・Android 11.0 以降での使用していないアプリの権限が自動リセットされる機能について

・Android 11 でのデータアクセスの監査について

・Android 11 での位置情報アクセスについて

・Conscryptモジュールについて

・Android 11における生体認証の変更点

（その他）

・Androidスマートフォンにおける機能資産について構成・内容を見直し拡充

・Android 6.0 以降の Permission モデルの仕様変更について構成・内容を見直し拡充

JSSECセキュアコーディングガイド第13版（2020年）

セキュアコーディングガイド第13版の改訂内容は以下の通り

(Android 12対応)
・ACTION_CLOSE_SYSTEM_DIALOGSについて
・特定のWindowをパススルーするタッチについて
・PendingIntentオブジェクトの可変性
・Android 12 における使用していないアプリの自動休止機能について
・パッケージアクセスの仕様変更にともなうAPIの戻り値の変化
・Android 12 におけるマイクとカメラ
・WebViewにおけるSameSite Cookieについて
・Clipboardへのアクセス通知について

（その他、構成・内容の見直しと拡充）
・exported 設定とintent-filter設定の組み合わせ
(Activityの場合)
・Intent経由など、他から受け取ったURLが想定されたURLか確認する （必須）
・データアクセスの監査について
・位置情報アクセスについて
・Conscryptモジュールについて
・Clipboardに格納されている情報の操作

最新版のAndroid 12における変更点を中心に改訂。
Android 12では、前バージョンでなされたプライバシーに関する仕様の拡張的な内容が変更点の中心となっており、あわせて記載内容を追加・変更した。

また、昨今問題となることの多い、フィッシングサイトへの誘導に悪用され得る、アプリ間におけるURLのやりとりについての注意点も追記しています。

サンプルコードのAndroid SDKバージョンをAndroid 12（API 31）に変更し、Android 12端末でそのまま動作させることが可能なようアップデートしております。

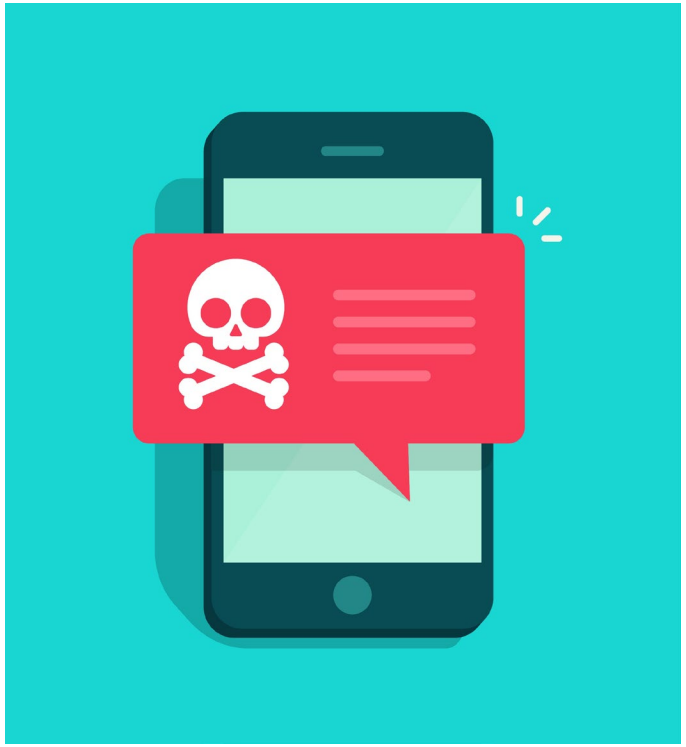
JSSECセキュアコーディングガイド更新プロセス

- 4月～5月
  - Googleから発表されるAndroid新バージョンのベータ版情報から、更新内容を特定し、セキュア設計・セキュアコーディングを行う上での内容を調査検討
- 6月～8月
  - 調査検討に基づき、修正部分の原稿を執筆
  - サンプルコードを新規作成
  - 最新版Androidにあわせたサンプルコードの修正
- 8月～10月
  - テクニカルレビューを行い内容を精査
- 10月～11月
  - Android正式版のリリースにあわせて最新版を公開
  - 英語版の翻訳を開始し、別途リリース

スマートフォン・サイバー攻撃対策ガイド

スマートフォンを狙った脅威

- 身近に使用するスマートフォンを狙ったサイバー攻撃が増加
- 手法も複雑なうえに頻度が高く、どのような手法かがわかりずらい
- 被害端末が悪用され、踏み台にされており被害が拡大している



サイバー攻撃の手法を理解できるコンテンツが必要

スマートフォン・サイバー攻撃対策ガイド

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

スマートフォン・サイバー攻撃対策ガイド

で検索

2020年11月より、JSSECサイトにて「スマートフォン・サイバー攻撃対策ガイド」を順次掲載

スマートフォン・サイバー攻撃対策ガイド

これまでに７本の記事を掲載

図 1. 郵便局を詐称した SMS

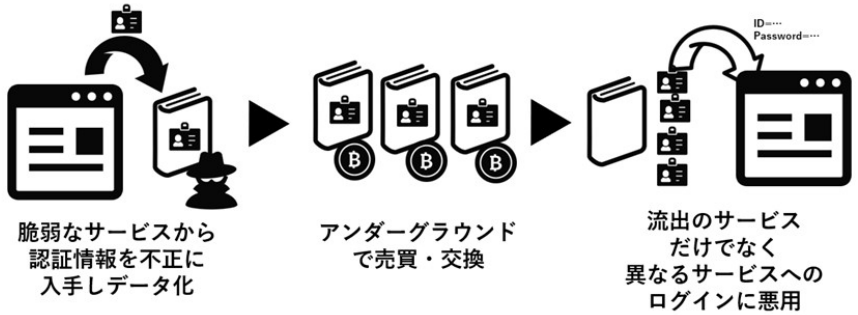
図 2. 郵便局を模倣した偽サイト

第1回 SMS認証の悪用、スミッシング(SMS+フィッシング)

執筆者：本間輝彰様（KDDI株式会社）

https://www.jssec.org/column/20201130.html

スマートフォンにおいては現在なお被害の広がるサイバー攻撃である、SMSの認証を悪用したフィッシング詐欺である、スミッシングについて説明。



第2回スマートフォン決済サービスにおける不正

執筆者：仲上竜太（株式会社ラック）

https://www.jssec.org/column/20201214.html

スマホ決済サービスの悪用がどのように行われたかを技術的に解説。クレデンシャルの不正取得から悪用までの経路や、脆弱なパスワードの危険性について解説。

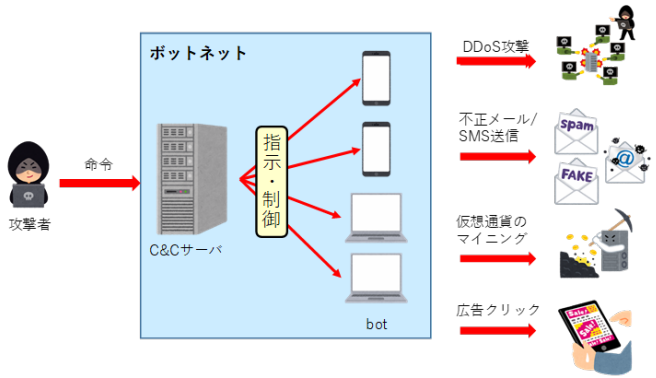
スマートフォン・サイバー攻撃対策ガイド

これまでに７本の記事を掲載

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
執筆者：仲上竜太（株式会社ラック）
https://www.jssec.org/column/20210202.html
広告ネットワークを通じて配信される詐欺広告・詐欺サイトの手口を紹介。

```
$ hashcat -m 17210 -a 3 -w 4 --session helloworld -o result.txt greet.txt.zip.hash
:
Started: Fri Feb 19 16:58:06 2021
Stopped: Fri Feb 19 16:58:22 2021
$ cat result.txt
$pkzip2$1*2*2*0*19*d*40f63a90*0*43*0*19*40f6*5a8f*08508e9b6131d777eaa0d6f31b
07927f4662a6cd435deddcab*$/pkzip2$:0219
```

第4回　インターネットバンキング情報窃取
執筆者　：宮崎力（株式会社ラック）
https://www.jssec.org/column/20210301.html
インターネットバンキングの情報窃取についてクレデンシャルの窃取や番号の解読の観点から解説

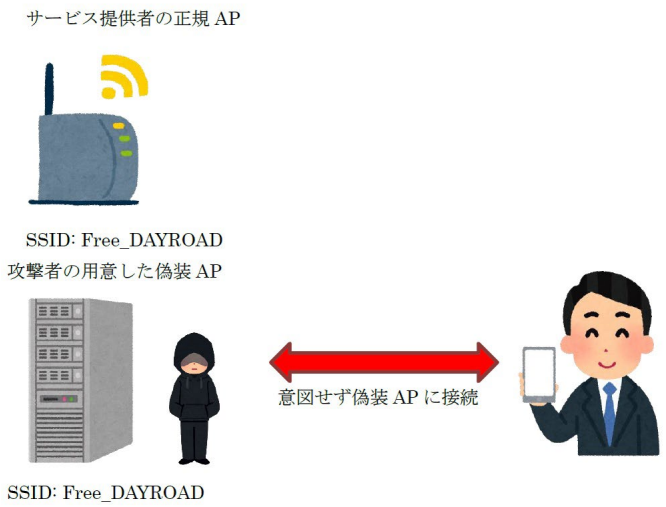


第5回 マルウェア・bot対策
執筆者　：本間輝彰様（KDDI株式会社）
https://www.jssec.org/column/20210311.html
スマートフォンも対象となるマルウェアやボットネットなどのサイバー攻撃の基本的な攻撃手法と対策について解説。

スマートフォン・サイバー攻撃対策ガイド

これまでに７本の記事を掲載

第6回 偽警告・偽契約詐欺対策
執筆者：本間輝彰様（KDDI株式会社）
https://www.jssec.org/column/20210412.html
サイト閲覧時に時折表示される「あなたのスマートフォンのセキュリティが危険です」などの偽警告詐欺の解説。



第7回偽装AP
執筆者：宮崎力様（株式会社ラック）
https://www.jssec.org/column/20210521.html
街中などに設置された偽アクセスポイントを用いた情報窃取や不正侵入を解説。見分けるのが困難な偽APへの対処方法について紹介。

スマートフォン・サイバー攻撃対策ガイド

対策ガイドの記事構成

攻撃の概要

- サイバー攻撃の種類と被害を簡潔に説明

技術解説

- 攻撃に悪用される技術や方法を説明

対策

- 利用者が普段注意すべき対策を紹介

スマートフォンのセキュリティを高める技術イベントの開催

スマートフォンにおけるプライバシー・セキュリティ啓発

個人情報保護に対する取り組みとスマホセキュリティの実態・対策として
セキュアコーディングを紹介

スマートフォンに関連した技術や取り組みの紹介

JSSEC加盟企業向けのクローズドイベントとして開催。
技術的に「濃い」内容をショートプレゼンで紹介。

JSSEC技術部会今後の取り組み

- **JSSECセキュアコーディングガイドの更新 2022年度**
  - JSSECセキュアコーディングガイドは2022年も引き続きAndroidのバージョン更新にあわせてアップデートを行ってまいります。
  - コラム等、スマートフォンアプリのセキュリティ実装に役立つコンテンツも募集中です
- **スマートフォン・サイバー攻撃対策ガイド 2022年度**
  - スマートフォンを対象としたサイバー攻撃の「大辞典」となるべく、内容の充実を進めています。
  - 執筆者を募集しています

- このほかイベント等様々な企画を進行中ですので、ご興味のある方は是非JSSEC技術部会までお問合せください

※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。
※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。