■セキュリティフォーラム 2023

アプリ開発時に気を付けたい JSSEC Mobile Top 10

2023年 3月1日（水）

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 マルウェア対策WG L 小笠原 徳彦 ((株)SHIFT SECURITY)

JAPAN SMARTPHONE SECURITY ASSOCIATION

スマートフォン開発における チェックポイントの存在意義

セキュリティ対策の重要性は誰もが知っているが

JAPAN SMARTPHONE SECURITY ASSOCIATION

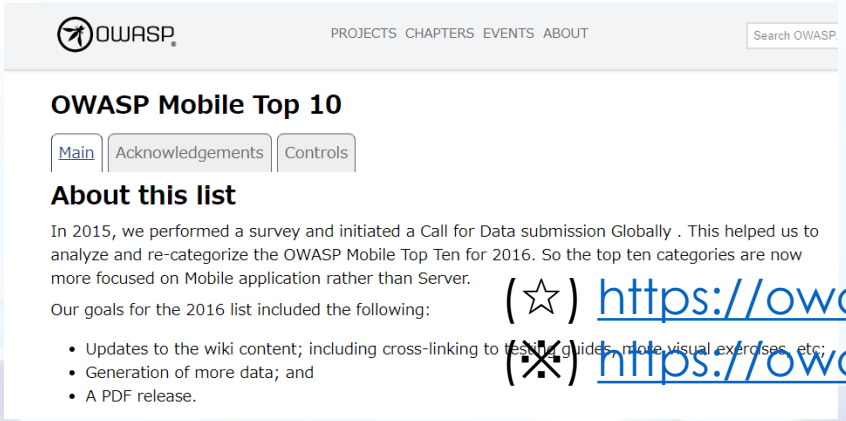
- アプリケーション開発者にとっては
  日々の開発でどこに気を付けたらいいかわからない
- **「最低限ここまで見ておけば」という指針**があればうれしい
- 数が多すぎるのも困るのでせいぜい10個ぐらい

OWASP Mobile Top 10

JAPAN SMARTPHONE SECURITY ASSOCIATION

OWASP - Open Web Application Security Project とは、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です。
(https://owasp.org/www-chapter-japan/ より)

- このOWASPが制定した「スマートフォンアプリケーション開発者がチェックすべき10個のチェックポイント」を示したものが「OWASP Mobile Top 10」（☆）
- OWASPが多数提供する（例：OWASP Top 10 ※）「Top 10」シリーズの一つ
- すべてのスマートホンアプリケーション開発者が知っておくべき啓発文書



(☆) https://owasp.org/www-project-mobile-top-10/
(※) https://owasp.org/Top10/ja/

OWASP Mobile Top 10

JAPAN SMARTPHONE SECURITY ASSOCIATION

OWASP - Open Web Application Security Project とは、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です。
(https://owasp.org/www-chapter-japan/ より)

- このOWASPが制定した「スマートフォンアプリケーション開発者がチェックすべき10個のチェックポイント」を示したものが「OWASP Mobile Top 10」（☆）
- OWASPが多数提供する（例：OWASP Top 10 ※）「Top 10」シリーズの一つ
- すべてのスマートホンアプリケーション開発者が知っておくべき啓発文書
- 最終リリースは2016年（7年前！）
- 2022年の時点では復活の兆しが見えなかった
- 現状の脅威やスマホアプリの開発状況とフィットしていない点も見えてきた
- ……

(☆) https://owasp.org/www-project-mobile-top-10/
(※) https://owasp.org/Top10/ja/

OWASP Mobile Top 10

JAPAN SMARTPHONE SECURITY ASSOCIATION

OWASP - Open Web Application Security Project とは、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です。
(https://owasp.org/www-chapter-japan/ より)

- このOWASPが制定した「スマートフォンアプリケーション開発者がチェックすべき10個のチェックポイント」を示したものが「OWASP Mobile Top 10」（☆）
- OWASPが多数提供する（例：OWASP Top 10 ※）「Top 10」シリーズの一つ
- すべてのスマ[illegible]
- 最終リリース[illegible]
- 2022年の時[illegible]
- 現状の脅威や[illegible]
- ……

JSSECなりの解釈で「2022年のTop 10」を作ろう

そしてOWASP Mobile Top 10が活動を再開したら、この結果を持ち込んで積極的に議論に参加しよう

……という話をしたのが2022年の1月

[illegible]ile-top-10/

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC 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 （通称： JSSEC Mobile Top 10 2023）

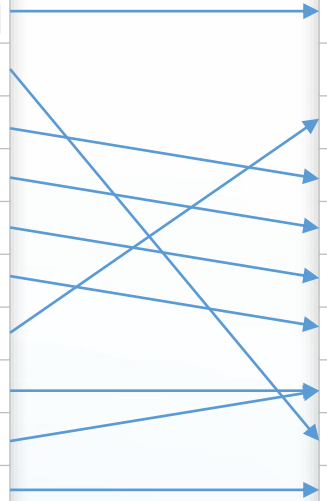
というわけで作りました！

JAPAN SMARTPHONE SECURITY ASSOCIATION

#	項目名
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

OWASP Mobile Top 10 2016 との比較

#	OWASP Mobile Top 10 2016
M1	プラットフォームの不適切な利用
M2	安全でないデータストレージ
M3	安全でない通信
M4	安全でない認証
M5	不十分な暗号化
M6	安全でない認可制御
M7	クライアントコードの品質
M8	コード改ざん
M9	リバースエンジニアリング
M10	余計な機能



#	JSSEC Mobile Top 10 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 NEW
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

M1:プラットフォームの不適切な利用

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリは、プラットフォーム機能の誤用や、プラットフォームセキュリティコントロールの不使用が対象です。Androidインテント、プラットフォームのアクセス許可、生体認証の誤用、キーチェーン、モバイルOSの一部である他のセキュリティコントロールが含まれます。モバイルアプリケーションには、本リスクを有してしまう幾つかの状況があります。
対応 セキュアコーディングガイド	4.1 Activityを作る・利用する / 4.2 Broadcastを受信する・送信する / 4.3 Content Providerを作る・利用する / 4.4 Serviceを作る・利用する / 4.7 Browsable Intentを利用する / 4.8 LogCatにログ出力する / 4.9 WebViewを使う / 4.10 Notificationを使用する / 4.11 共有メモリを利用する / 5.2 PermissionとProtection Level / 5.3 Account Managerに独自アカウントを追加する / 5.7 生体認証を利用する
OWASPとの差異	不動の一位。内容も「指紋認証」→「生体認証」に変えただけ

M2:不適切なクレデンシャルの利用

項目	詳細
概要	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。
対応セキュアコーディングガイド	
OWASPとの差異	新規。主にAndroidにおいては、アプリケーションバイナリの取り出し、リバースエンジニアリングが容易であり、これによってAPIキー、クレデンシャルが漏洩した脆弱性が報告されているため、M2に位置づけ

M3:クライアントコードの品質と安全性

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリは、モバイルクライアントのコードレベルの実装の問題が対象です。サーバサイドのコーディングミスとは異なるものです。本カテゴリは、バッファオーバーフローやフォーマットストリングの脆弱性や、他の様々なコードレベルのミスといったモバイルデバイス上で実行されるコードを書き換えることで解決できることが対象です。また、本カテゴリには同梱されるOSSなどのパッケージに対する脆弱性の不適切な管理を含みます。
対応セキュアコーディングガイド	
OWASPとの差異	OWASP Mobile Top 10 2016では外部由来の入力文字列の扱いといった狭い範囲を主に扱っていたが、クライアントコードの品質という意味ではより広い脅威が考えられるためこの限定を外した。 また、現代において関心が増しているOSSセキュリティ、サプライチェーンリスクもこの項目に含まれる。そのためOWASP Mobile Top 10 2016の7位から大きく順位を上げた

M4:安全でない通信

項目	詳細
概要	本カテゴリは、脆弱なハンドシェイク、不適切なSSLバージョン、脆弱なネゴシエーション、機密情報の平文通信などが対象です。
対応セキュアコーディングガイド	5.4 HTTPSで通信する
OWASPとの差異	OWASP Mobile Top 10 M3からスライド

M5:安全でない認証

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリは、エンドユーザの認証やセッション管理の不備が対象です。 以下のようなものがあります。 - ユーザを特定できない - ユーザの同一性を維持できない - セッション管理の不備
対応 セキュアコーディングガイド	
OWASPとの差異	OWASP Mobile Top 10 M4からスライド

M6:不十分な暗号化

項目	詳細
概要	機密情報資産を暗号化するプログラムには、暗号処理が不十分な場合があります。TLSやSSLに関連するあらゆるものは、M4(安全でない通信)に含まれるという点に注意してください。また、暗号化すべき時にアプリが暗号を使用しない場合は、M9(安全でないデータストレージ)に含まれます。本カテゴリは、暗号化が実行されたにもかかわらず、正しく行われていないという問題が対象です。
対応 セキュアコーディングガイド	5.6 暗号技術を利用する
OWASPとの差異	OWASP Mobile Top 10 M5からスライド

M7:安全でない認可制御

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリは、認可制御の不備(例えば、クライアント側での認可決定や強制ブラウジングなど)が対象です。これは、認証の問題(例えば、デバイス登録やユーザ識別)とは異なるものです。もし、認証が必要な状況でアプリがユーザを全く認証していない場合は (例えば、認証され許可されたアクセスが必要であるにもかかわらず、一部のリソースやサービスに匿名アクセスが許可されているなど)、認証の不備(M5)であり、本カテゴリには含まれません。
対応 セキュアコーディングガイド	
OWASPとの差異	OWASP Mobile Top 10 M6からスライド

M8:コード改ざん

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリでは、バイナリ更新、ローカルリソースの改ざん、メソッドフッキング、メソッドスウィズリング、動的メモリ改ざんや、これを容易にするためのバイナリ解析によるリバースエンジニアリングについて記載します。アプリケーションがモバイルデバイスに一旦配信されると、コードとデータといったリソースは端末に常駐することになります。攻撃者は、そのコードを直接改ざんしたり、メモリ内容を動的に改ざんしたり、アプリケーションが使用するシステムAPIを変更や置換したり、アプリケーションのデータやリソースを改ざんしたりすることが可能です。これにより攻撃者は、個人的利益もしくは金銭的利益のために、ソフトウェアが本来意図している使用方法を直接覆すことができるようになります。
対応 セキュアコーディングガイド	
OWASPとの差異	主にゲームチート。OWASP Mobile Top10のM8とM9を統合

M9:安全でないデータストレージ

JAPAN SMARTPHONE SECURITY ASSOCIATION

項目	詳細
概要	本カテゴリはOWASP Mobile Top 10 2016のM2（安全でないデータストレージ）に対応するものです。スマートフォンの紛失・盗難に伴い悪意ある第三者からデータストレージの内容を抜き取られ、機密情報が奪われることを想定しています。現代ではOSによるデータストレージの暗号化が必須となったため、このカテゴリの順位は大幅に下がりました。
対応セキュアコーディングガイド	4.5 SQLiteを利用する / 4.6 ファイルを扱う / 5.1 パスワード入力画面を作る
OWASPとの差異	現代においてはOSによるデータストレージの暗号化が必須になったため、本カテゴリの危険度は下がったとみなしてM2→M9へ

M10:余計な機能

項目	詳細
概要	開発者は、本番環境にリリースするつもりではない隠されたバックドア機能や内部開発用のセキュリティコントロールを本番用に含めてしまうことがあります。例えば、開発者がうっかりハイブリッドアプリケーションのコメントにパスワードを記載してしまったり、テストで無効化した二要素認証をそのままにしてしまったりする恐れがあります。
対応セキュアコーディングガイド	
OWASPとの差異	M10のまま内容にも変更なし

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC　モバイルアプリケーション開発 10大チェックポイント /2022 の 今後

OWASP Mobile Top 10再始動

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **2023年1月18日のメールで再始動が宣言**
- 2023年2月9～10日に正式なリブートミーティング開催
- 貢献者リストに小笠原の名前を記名して反応待ち

- 我々の議論の**結果**を押し付けるのではなく
- 議論の**過程で出た意見**をOWASPの活動でも紹介して
- 2023年にふさわしいOWASP Mobile Top 10となるよう協力していく予定

ご清聴ありがとうございました。