■セキュリティフォーラム 2024

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と OWASP Mobile Top 10

2024年 3月6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

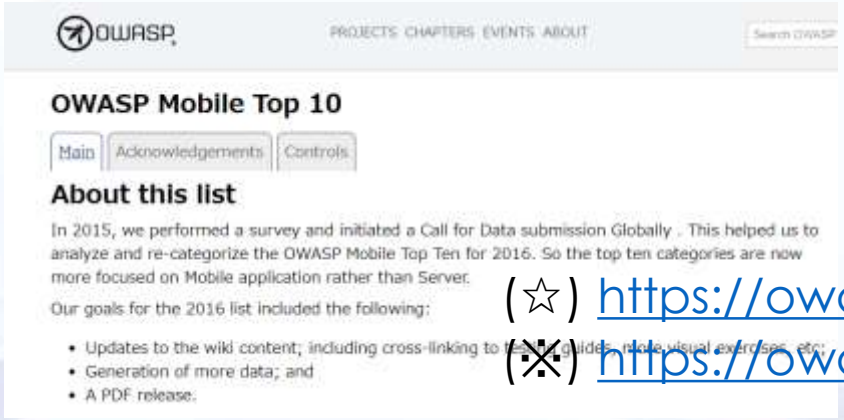
- アプリケーション開発者にとっては
  日々の開発でどこに気を付けたらいいかわからない
- **「最低限ここまで見ておけば」という指針**があればうれしい
- 数が多すぎるのも困るのでせいぜい10個ぐらい

OWASP Mobile Top 10

JAPAN SMARTPHONE SECURITY ASSOCIATION

OWASP - Open Worldwide 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
- すべてのスマートフォ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 Worldwide 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
- すべてのスマートフォ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 Worldwide 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
- 最終リリース
- 2022年の時
- 現状の脅威
- ……

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

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）

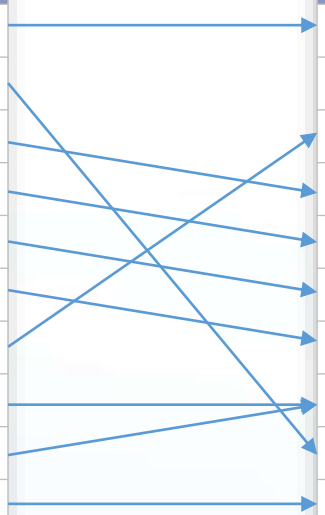
というわけで作りました！

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

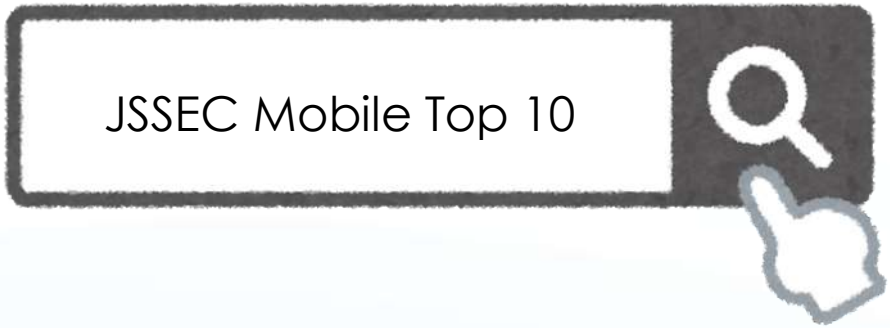
#	OWASP Mobile Top 10 2016
M1	プラットフォームの不適切な利用
M2	安全でないデータストレージ
M3	安全でない通信
M4	安全でない認証
M5	不十分な暗号化
M6	安全でない認可制御
M7	クライアントコードの品質
M8	コード改ざん
M9	リバースエンジニアリング
M10	余計な機能



#	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

こちらで公開

- https://www.jssec.org/mobile-apps-10checkpoint2023
- Top 10選定の裏話もこちらで公開
  - https://www.jssec.org/column/20230724.html



- ここまではセキュリティフォーラム2023で発表した通りです

JAPAN SMARTPHONE SECURITY ASSOCIATION

OWASP Mobile Top10 2023

OWASP Mobile Top 10再始動

- **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

- というのがセキュリティフォーラム2023でのステータス

2023年6月1日、BETA2リリース

Alaeddine Mesbahi 18:09

M1: Insecure Authentication/Authorization and Access Control
M2: Insecure Communication
M3: Inadequate Supply Chain Security
M4: Inadequate Privacy Controls
M5: Insufficient Input/Output Validation
M6: Security Misconfiguration
M7: Insufficient Cryptography
M8: Insecure Data Storage
M9: Insufficient Binary Protections
M10: Data Leakage

2

5 件の返信 最終返信: 7ヶ月前

Alaeddine Mesbahi 18:09

The 5 that didn't make the list:
Hardcoded Secrets
Insecure Access Control
Path overwrite and Path Traversal
Unprotected Endpoints (Deeplink, Activitity, Service ...)
Unsafe sharing

2023年6月1日、BETA2リリース

サプライチェーンリスクを脅威ととらえて
「クライアントコードの品質と安全性」をM3に
入れた我々とは目線が合致している

一方でシークレットのハードコードは
CVEも採番されている大きなリスクであり
これが圏外なのはちょっと納得いかない

以下のようにSlackに意見を投下

naruhiko 12:37

Hello, I'm from JSSEC, Japanese smartphone security community.

We discussed how we would update the Mobile Top 10 in 2022. I would like to share that with you.

- M1: Improper Platform Usage
- M2: Improper Credential Usage
- M3: Client Code Quality
- M4: Insecure Communication
- M5: Insecure Authentication
- M6: Insufficient Cryptography
- M7: Insecure Authorization
- M8: Code Tampering
- M9: Insecure Data Storage
- M10: Extraneous Functionality

3

以下のようにSlackに意見を投下

naruhiko 7ヶ月前

皆さんがBeta2で落とした「シークレットのハードコード」に対して我々は懸念を持っている。なのでM2: Improper Credential Usage として配置した。
Hackernewsなんかでも話題になっていたし

naruhiko 7ヶ月前

それから我々のTop10のM3: Client Code Quarityにはサプライチェーンリスクも含んでいる。（のでそこは認識が一致しているね）

週次ビデオ会議で主張

- シークレットのハードコードはCVEとしてもしばしば報告されている現象でありぜひ入れたい
- 我々の議論の根拠としては日本語になるがリンクがあるので参照してほしい
  - といってJSSEC Mobile Top 10のリンクを共有

最終版のOWASP Mobile Top 10

JAPAN SMARTPHONE SECURITY ASSOCIATION

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

  - M1: Improper Credential Usage
  - M2: Inadequate Supply Chain Security
  - M3: Insecure Authentication/Authorization
  - M4: Insufficient Input/Output Validation
  - M5: Insecure Communication
  - M6: Inadequate Privacy Controls
  - M7: Insufficient Binary Protections
  - M8: Security Misconfiguration
  - M9: Insecure Data Storage
  - M10: Insufficient Cryptography

Improper Credential Usageとして
クレデンシャルのハードコー
ドがTop1の位置を獲得

Comparison between 2016 and 2024

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

OWASP Mobile Top 10 2023の特徴

JAPAN SMARTPHONE SECURITY ASSOCIATION

Comparison between 2016 and 2024

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

- 全体として新たなリスクを取り入れ、2016年でのTop10は統廃合されランクが下がる傾向に
- シークレットのハードコードを主な脅威とするImproper Credential Usageが一位に（新規）
- Mobile以外でも注目を集めるサプライチェーンセキュリティが二位（新規）
- 2016のM7 Client Code Qualityがより具体的なInsufficient Input/Output ValidationになりM4に
- OSの堅牢性向上を理由にInsecure Data StorageがM2からM9に、Insufficient CryptographyがM5からM10に

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

基本的にはOWASPの活動の叩き台に

- 今回、JSSECの提案がOWASPに受け入れられたのは、JSSEC内での議論をきちんと形にできていたことがポイント
- JSSEC 技術部会 マルウェア対策WGとしては、OWASP Mobile Top 10の今後の改定をにらみ、日本国内で議論する場として活動していく
- また、セキュアコーディングガイドラインとの紐づけも、独自に行っていく（これを2024年の活動の柱に）

- 今後ともグローバルと協調して開発者にとってより良いガイドラインをタイムリーに示せればと思います
- 応援よろしくお願いします

ご清聴ありがとうございました。

JAPAN
SMARTPHONE
SECURITY
ASSOCIATION