資料５－３

アプリ診断の取組紹介

安田 良明（yoshiaki.yasuda@owasp.org）

OWASP Mobile Application Security Design Guide
Project Lead

アジェンダ

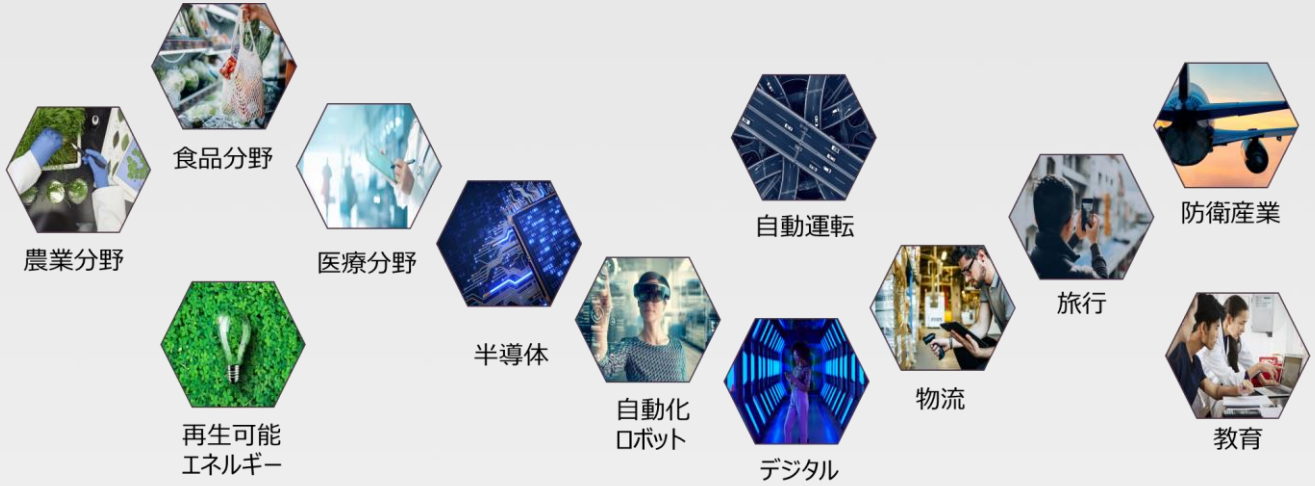
- アプリ診断の現状（対象分野・課題）
- アプリ診断の取組
- アプリ診断の品質向上の取組
- 日本におけるセキュア設計・開発ガイドの取組
- まとめ

アプリ診断の現状

- スマートフォンやタブレットなどのモバイルデバイスは、私たちの日常生活に欠かせない存在となっている。
- しかし、それらのデバイスにインストールされるアプリケーションは、さまざまセキュリティやプライバシーのリスクにさらされている。
- アプリのセキュリティやプライバシーを確保するためには、アプリ診断というプロセスが必要。
- そのため、アプリ開発やリリース時前後にアプリ診断を行い、アプリの設計、ソースコード、バイナリや動作環境などを検査し、脆弱性や不正な動作を発見し、改善を行っている。

アプリ診断の対象分野

- ICT技術革新（5Gやエッジデバイスの技術向上）により、アプリが利用者環境で実行される傾向が増加している。



アプリを取り巻く課題

- モバイルアプリの安全性確保が必要な分野
  - プライバシー（個人識別情報/マイナンバー等）
  - 経済安全保障（サイバーサプライチェーンリスク/サードパーティーライブラリリスク）
  - 金融業（電子決済/銀行口座）
  - 製造業（モビリティ関連（自動運転）/スマートホーム/スマート家電等）
  - ヘルスケア（医療DX/デジタルカルテ）

- サイドローディングにおける不正なアプリの流通
  - Apple の App Store や Google の Google Play は、アプリ流通のストアであると同時にアプリの品質を1つ1つ手作業でチェックし、利用者の安心安全を守る審査機関としての側面がある
  - 悪性のアプリの混入を防ぐ審査を誰（新規参入するアプリストア）かが実施する必要がある
  - 自動車検査、医薬品の審査、建築基準のような審査がアプリには不要なのか

アプリ診断の取組

- アプリ提供者は、アプリの開発段階、リリース前やリリース後など、さまざまなタイミングでアプリ診断を実施している。

- アプリ診断は、手動、自動またはハイブリッドで実施される。
  - 手動で行うアプリ診断は、高度なセキュリティ技術者がアプリ設計からソースコード、動作までを検査・分析し、脆弱性や欠陥を検出する。 多くの場合、アプリ診断サービスを提供するセキュリティ専門業者に委託して実施する為、深い検査・分析結果を期待できるが、検査・分析結果の揺れ等の人的制約、高価な費用等による経済的制約を併せ持つ。
  - 自動で行うアプリ診断は、専門ツール・ソフトウェアを用いて、アプリ設計からソースコード、動作までを自動検査し、脆弱性や欠陥を検出する。専門ツール・ソフトウェアの購入又はサービスを利用する為、利用者が利用したいタイミングにアプリ診断が出来、効率的（自動化、強制化、低コスト、診断レベルの均一化、等）に検査することが出来るが、検査内容が専門ツール・ソフトウェアの対応範囲内に制限される制約がある。

アプリ診断の市場製品や企業（例示）

- テクマトリックス株式会社
  - モバイルアプリケーション脆弱性診断サービス
- バルテス株式会社
  - 脆弱性診断（Web/モバイル/IoT）
- KPMGジャパン
  - モバイルアプリケーション診断
- 株式会社アイ・エフ・ティ
  - スマートフォンアプリケーション脆弱性診断
- 株式会社sMedio
  - RiskFinder
- 三和コムテック株式会社
  - SCT SECURE モバイルアプリ診断サービス
- 大日本印刷株式会社
  - NowSecure Platform
- 株式会社ラック
  - Secure Coding Checker

例示したアプリ診断の企業およびサービスを「OWASP」としてエンドースする意図はありません。

アプリ診断の品質向上の取組

- アプリ診断は、アプリのセキュリティやプライバシーを確保するための重要なプロセスだが、それだけでは十分ではない。
- アプリ診断は、アプリのセキュリティやプライバシーの状態を評価するものであり、それを改善するためには、セキュア設計・開発ガイドのサポートが必要。
- セキュア設計・開発ガイドとは、アプリのセキュリティ要件やリスク分析、セキュアコーディングの指針、セキュリティテストの方法などをまとめたもの。
- セキュア設計・開発ガイドには、国際的なものだけでなく、日本が発信するものも存在する。

日本におけるセキュア設計・開発ガイドの取組

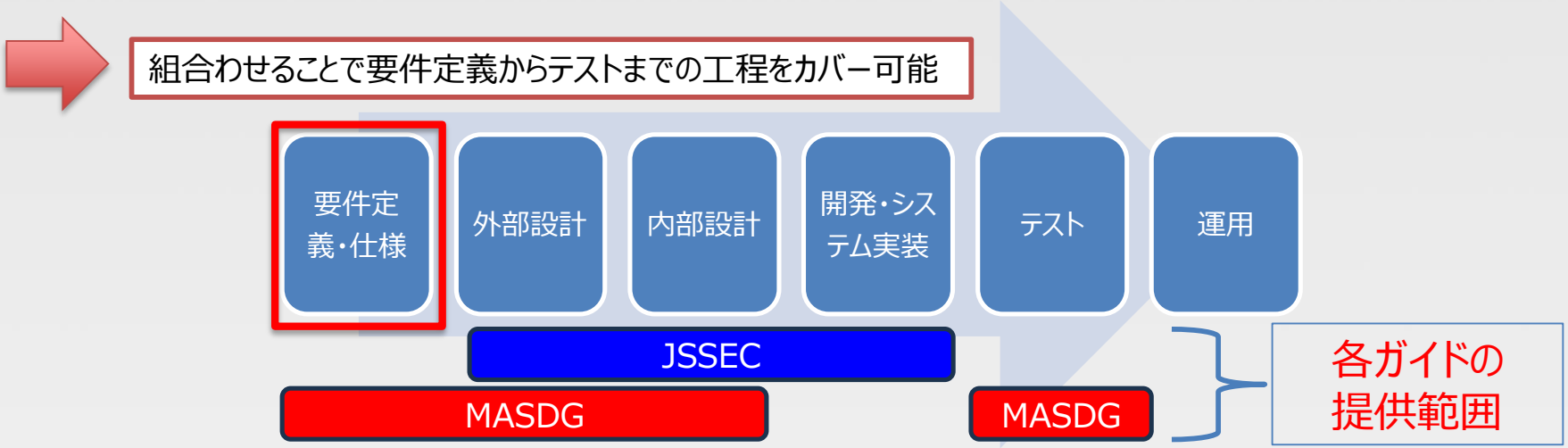
- 日本スマートフォンセキュリティ協会（JSSEC）
  - JSSEC は、アプリ開発者や企業が参考にできる「モバイルアプリ開発セキュリティガイドライン」を公開している。このガイドラインでは、アプリのライフサイクルに従って、セキュリティ活動やチェックポイントが示されている。

    https://www.jssec.org/report/20240229_securecoding.html
- OWASP MASDG
  - OWASP（The Open Worldwide Application Security Project）とは、世界中のセキュリティ専門家が参加するオープンソースのセキュリティコミュニティ。OWASP は、Web やモバイルアプリのセキュリティに関する様々な資料やツールを提供している。
  - 2011年より OWASP Japanチャプターを中心に翻訳や国際的コラボレーションが推進されている。
  - OWASP MASDG（OWASP Mobile Application Security Development Guide）とは、MSTG や MASVS などの OWASPプロジェクトと連携したモバイルアプリのセキュア設計・開発に必要な知識や技術を網羅したガイド。

    https://owasp.org/www-project-mobile-application-security-design-guide/

セキュア設計・開発ガイドを組み合わせたアプリ開発の例

JSSEC：サンプルが多く目的に応じた具体的な実装パターンを提示　⇒　内部設計、開発・システム実装に強い
MASDG：要件定義や設計で考慮する必要のある幅広いルールを提示　⇒　要件定義、外部設計、内部設計に強い
　　MASTGを基にしているのでガイドではテストについても記載 ⇒　テストにも強い



まとめ

- アプリ開発時にセキュリティやプライバシーへの取組が必要な分野が拡大している。
- アプリ診断は手動または自動で利用可能。
- アプリ診断をサポートするセキュアコーディングガイドが日本からも発信されている。
- セキュリティやプライバシーを「バイ・デザイン」とした取組が、ITを利用することで実現可能。