



Arxan アプリケーションセキュリティレポート第 5 弾

モバイルアプリケーションセキュリティの認識と現実との乖離を暴く

医療および金融モバイルアプリのユーザーや開発企業経営層の 84%が自分のモバイルアプリは安全だと思っているにもかかわらず、評価した医療および金融アプリの 90%が 2 つの重大なセキュリティリスクを抱えていた。

米国メリーランド州 Bethesda 市- 2016 年 1 月 12 日- アプリケーション保護ソリューションの主要ベンダーであるアークサン・テクノロジー(Arxan Technologies)は本日、アプリケーションセキュリティレポート第 5 弾の 2016 年アニュアルレポートを公表しました。今回は、米国、英国、ドイツと日本で評価の高い医療および金融分野の 126 アプリケーションをリサーチ対象とし、さらにアプリユーザーである消費者、およびアプリ開発側のセキュリティ専門家のアプリケーションセキュリティに関するインタビュー結果をまとめたものです。

アークサン (Arxan) は、医療及び金融モバイルアプリに取り込まれている安全対策レベルに関する消費者の理解と、組織が既知のアプリケーション脆弱性を周知するレベルとの大きな乖離を発見しました。大多数のアプリユーザーとアプリ開発企業の経営層が、彼らのアプリが安全であると思っているにもかかわらず、広く使われている銀行のアプリや決済アプリ、FDA 認可の医療アプリを含む Arxan が評価したほとんど全てのアプリで、OWASP が提唱するセキュリティリスクトップ 10 のうち少なくとも 2 つの脆弱性が認められました。

リサーチ結果の例:

- **消費者とアプリ開発企業の経営層は、医療や金融のモバイルアプリが安全であると信じています。**
モバイルアプリユーザーとモバイルアプリ開発企業の経営層あわせて 84%が、彼らの医療アプリと金融アプリは「十分に安全である」と確信し、63%がアプリプロバイダーはモバイル医療アプリと金融アプリを保護するために、できる限りのすべてのことをしていると思っています。
- **医療および金融のモバイルアプリの大多数が重大なセキュリティ脆弱性を含んでいます。**
今回評価したモバイル医療アプリおよびモバイル金融アプリの 90 パーセントで、OWASP (Open Web Application Security Project) が定義するモバイルアプリトップ 10 リスクのうち少なくとも 2 つのリスクを抱えていることがわかりました。
評価対象の医療アプリの 80%が米国の FDA (Food and Drug Administration) または英国の NHS(National Health Service)という公共機関で承認されたものでしたが、それらのアプリにおいても OWASP が提唱するトップ 10 リスクのうち 2 つのリスクを抱えていました。
- **セキュリティと安全性リスクは現実であり、大変重要です。**



テストしたアプリの 98%がバイナリ保護をしておらず、それが今回確認された最も一般的な脆弱性でした。モバイルアプリの 83%がデータ転送レイヤーの保護が不十分でした。それらの脆弱性はアプリケーションコードの改ざんやリバースエンジニアリングを容易にし、機密情報や個人情報流出の危険性を増すものです。機密データ盗難に加えて、悪意のあるハッカーが医療アプリを改ざんすることで薬物の致死量を操作したり、金融アプリを改変して送金先を変更したりすることも可能になります。

- **アプリが安全でないとわかったら、ほとんどのユーザーがプロバイダーを変えると回答しています。**
80%のモバイルアプリユーザーが、自分が使っているアプリが安全でないと分かった場合プロバイダーを変えていると回答しています。82%のユーザーが同様のアプリがより安全なアプリを提供していたら、安全なほうに乗り換えると言っています。

「ビジネスでは、モバイルアプリはお客様を保持し続けるために使われます。それでも、市場に新しいアプリを出すことを急ぐあまり、企業はユーザー維持のために必須であるとわかっているはずの重要なセキュリティ対策を蔑ろにする傾向があります。」と、Arxan の CMO である Patrick Kehoe は述べています。「今回の Arxan アプリケーションセキュリティレポートにおけるリサーチ結果は、モバイルアプリのセキュリティが顧客保持の重要な要素であることを証明しています。強力で有効なモバイルアプリのセキュリティを施すことは、悪意のあるハッカーから身を守るための賢明なテクノロジー投資であるばかりでなく、組織が競合との差別化として、お客様から信頼に基づくロイヤリティを獲得するための聡明な設備投資でもあります。」

医療アプリと金融アプリに特化したリサーチからけられた結果は以下の通りです。

医療アプリのリサーチ結果骨子

- **政府機関の認可を受け公的規制に準拠したモバイル医療アプリであっても、他のモバイルアプリと同様の脆弱性を持っている。** 米国 FDA で認可されたアプリの 84%、UK の NHS が承認したアプリの 80%が、少なくとも OWASP トップ 10 モバイルアプリリスクのうち 2 つのリスクを持ち合わせていた。
- **モバイル医療アプリのほとんどがアプリケーションコード改ざんやリバースエンジニアリングをされやすい状態にある。** 95 percFDA 認可アプリのうち 95%、NHS 承認アプリの 100% においてバイナリ保護が欠如しており、個人の医療データやプライバシーにかかわる情報が不正操作されるリスクに曝されています。

金融アプリのリサーチ結果骨子

- **評価した主要なモバイルバンキングやモバイル決済アプリのすべてが OWASP モバイルトップ 10 リスクのうち 2 つのリスクを抱えていた。** 評価対象のモバイル金融アプリ（一般的にモバイルバンキ



ングや電子決済に使用されているアプリケーション) のすべてが、コード改ざんやリバースエンジニアリングによる不正操作の危機に曝されていました。

- **今回の評価で比較すると、Android アプリは iOS アプリよりもまだ安全性が多少は上回っているという結果が出ました。** Android モバイル金融アプリの 59%が OWASP モバイルトップ 10 リスクのうち少なくとも 3 つのリスクを抱えていましたが、iOS アプリでは、調査対象のすべて 100%にあたるアプリが同様のリスクに曝されていました。

今回のリサーチで Arxan は、モバイルアプリセキュリティにおいて米国、英国、ドイツ、日本での地理的な相違はほとんどないという結果を得ました。さらに、iOS アプリは Android アプリとほぼ同様に脆弱であるということもわかりました。

Arxan について

Arxan は世界で最も強固なアプリケーション保護ソリューションを提供しています。Arxan のユニークな保護技術は次にあげる機能を有しています。1)サイバー攻撃からアプリケーションを保護する 2) 攻撃が試みられていることを探知する 3) 検出された攻撃に反応し、警告を発したりアプリを停止、修復したりする。Arxan は、モバイルデバイス、デスクトップ、サーバー、組込型プラットフォーム (IoT による接続デバイスを含む) 等で稼働するソフトウェアソリューションです。自動車、ゲーム、ハイテク、ISV、医療機器、ヘルスケア、デジタルメディア等幅広い業種にわたって 5 億台を超えるデバイスで稼働しています。本社ならびに開発拠点は米国国内で、販売・サポート網を、日本をはじめとするアジア太平洋地域ならびに EMEA 地域に置いています。

アプリケーションセキュリティレポート 2016 をご希望の方は、infojapan@arxan.com までお問い合わせください。