LAC

セキュリティ診断レポート

2018 早春

特集

スマートフォンアプリケーション診断統計

金融系アプリケーションの課題

目次

1 セキュリティ診断結果からみる スマートフォンアプリケーションの現状とこれから

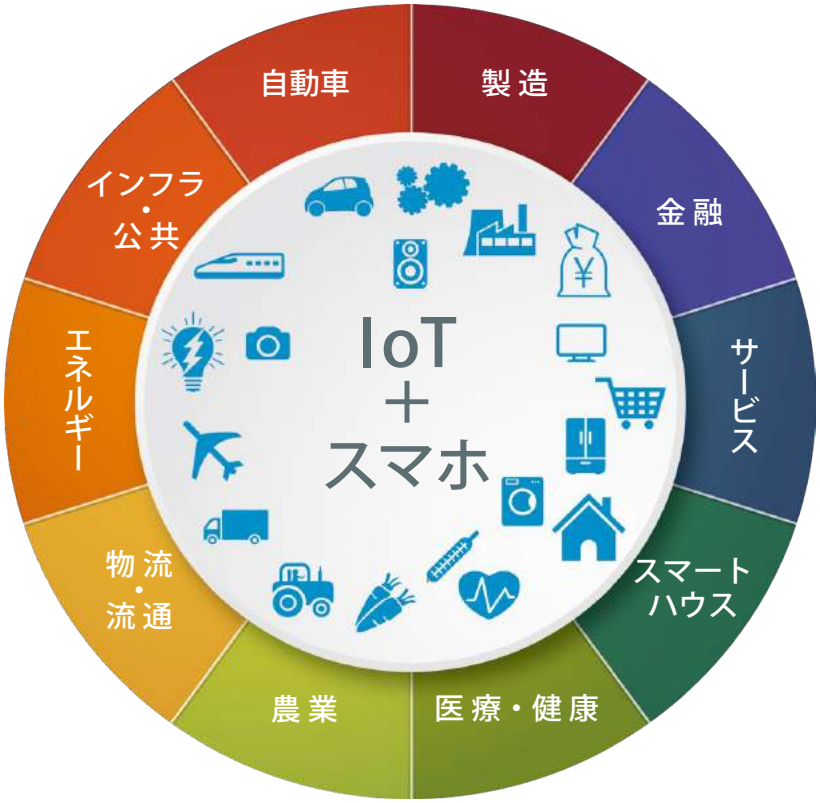
スマートフォン（以下、スマホという）の高機能化が進み、誰もがスマホを活用する現代。コンシューマ向けスマートフォンアプリケーション（以下、スマホアプリという）は多様化し、ビジネスでの利用もごく一般的になりました。総務省の平成29年版情報通信白書(※1a)によると、スマホの個人保有率は56.8%で、40代以下では平均8割以上が個人で所有しているように、年々、1人1台を所有する時代になっていることがわかります。また、スマホやスマホアプリが提供する多様な機能により、スマホが保有する情報はいまや電話帳だけでなく、プライバシー情報や電子マネー・モバイル決済の決済情報など多岐にわたっています。さらに近年では、スマホとスマホアプリはセンサーやデバイス（IoT）とも接続し、IoTシステムが扱う情報をクラウド側に伝送するIoTゲートウェイの役目を担います。以上から、スマホアプリ開発者は従来の携帯電話（フィーチャーフォン）用アプリを開発するときと同じセキュリティ意識のままでは不十分だということを理解する必要があります。特にスマホアプリは開発の歴史が浅い上に、スマホ自体の仕様が頻繁に変更されるため、意図せず脆弱性を作り込んだ状態で公開してしまうことがあり、スマホの特徴にあわせた対策が必要です図1-a。

ラックは、スマホアプリに関するセキュリティ上の問題を見つけ出すため、2011年に「スマートフォンアプリケーション診断」を開始しました。本レポートでは、2016年４月から2017年9月までの間に実施した「スマートフォンアプリケーション診断」の結果を分析し、開発時に作り込まれやすい問題の傾向や対策について解説します。

また、金融／FinTech(※1b)分野のスマホアプリ(※1c)（以下、金融系スマホアプリという）が登場し、交通系ICカードなどの電子マネーによる決済が浸透しつつあることから、こうした金融系スマホアプリに焦点を合わせ、問題の傾向と抱えるリスクについて考察します。

本レポートが、スマホアプリが直面する脅威への理解を深めるきっかけとなり、皆様の組織のセキュリティ向上の一助になりましたら幸いです。

図1-a スマホとIoTがさまざまな分野へ拡大



多様な分野へIoTが拡大している。あわせてIoTと接続するスマホやスマホアプリも拡大する見込み。

篠原崇宏

システムアセスメント部
スマートデバイスアプリケーション診断担当

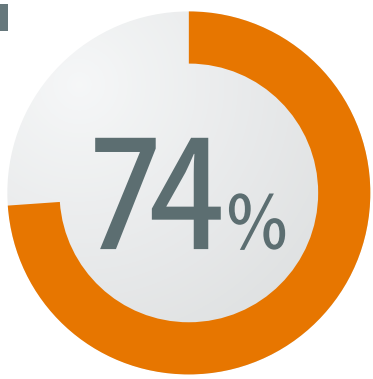
出向先の独立行政法人情報処理推進機構（IPA）にて脆弱性分析や標的型攻撃の啓発活動に従事した後、2016年にラックへ帰任。IPA、セキュリティキャンプにて講師として情報セキュリティの啓発活動に取り組んだ経験を活かし、現在は、スマートデバイスに対する診断業務や攻撃手法講座の教育業務に携わる。NPO日本ネットワークセキュリティ協会（JNSA）のIoTセキュリティWGにも参画。モットーは「あるべき論の後の現実的な対策検討」。

最近では、週末を使って自宅でIoT機器を調査するようになり、少しずつ機材が増えている。調査に使う専用の作業スペースを作り始めたため、妻から冷たい視線を送られる日々。

※1a 総務省 平成29年版情報通信白書：http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/index.html
※1b FinTech：FinTechとはFinance（金融）とTechnology（技術）を合成した造語。金融サービスと情報技術を結び付けたさまざまな革新的な動きを指す。
※1c 金融／FinTech分野のスマホアプリ：スクレイピング技術を導入したアプリケーションまたは金融事業者APIと電子決済等代行業者の連携したアプリケーション
http://www.fsa.go.jp/singi/singi_kinyu/financial_system/siryou/20161028/02.pdf

2 診断結果の傾向分析 7割超のスマホアプリで実害につながる問題点を検出

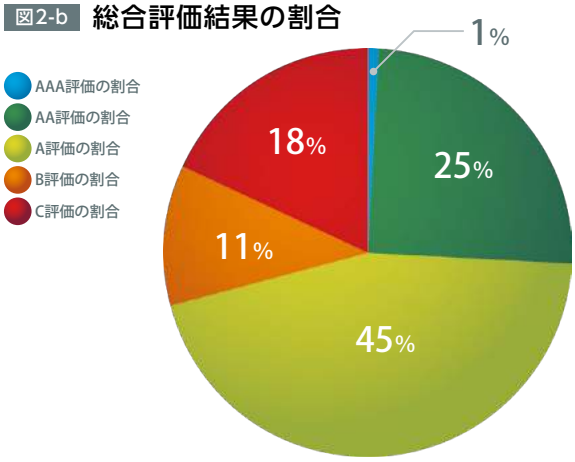
図2-a



Mediumリスク以上の問題点を検出したアプリケーションの割合

実害が発生する恐れのあるHighリスクと複数の条件により実害に結び付く恐れがあるMediumリスクの問題点を、診断対象としたスマホアプリの7割超で検出した。

図2-b 総合評価結果の割合



2016年4月から2017年9月までのスマートフォンアプリケーション診断の総合評価(※2a)(AAA、AA、A、B、Cの5段階)の割合を円グラフ化した。Mediumリスク以上を検出しているA～Cランクが74%であり、問題点を検出しなかったAAAが1%となっている。

スマホアプリの診断結果を分析すると、興味深いデータが得られました。図2-a 図2-bは2016年4月から2017年9月までの「スマートフォンアプリケーション診断」において、診断総合評価を集計したものです。集計データを見ると、74%のスマホアプリはMediumリスク以上の問題点(※2b)を抱えていることがわかります。

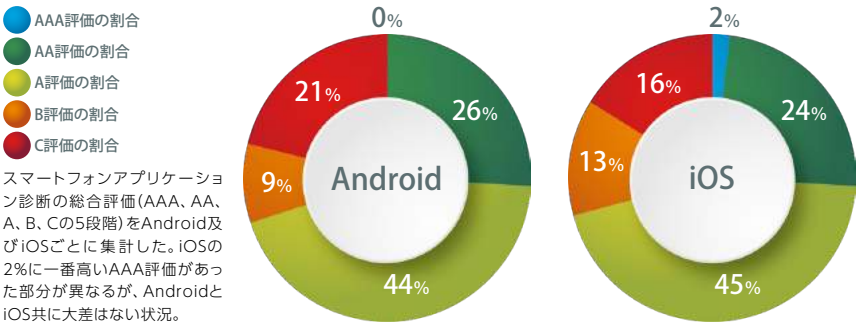
ラックでは検出した問題点のリスクレベルをHigh、Medium、Lowの3段階で評価しています(リスクレベルの詳細は13ページ、表7-b参照)。Highリスクに分類される問題点は、情報漏えいやアプリケーションの不正利用などの実害に結び付く恐れがあり、早急な対策が必要なものです。Mediumリスクは、複数の条件を組み合わせることで情報漏えいやアプリケーションの不正利用などの実害に結び付く恐れがあります。攻撃が成立するには端末のroot化(※2c)や、攻撃者が通信経路上で盗聴可能な状態などが必要とされるため、Highリスクの問題点より悪用される可能性は低いですが、これらMediumリスクについても攻撃に転用され得ることから、対策が必要です。

公開アプリケーションにも脆弱性が潜む!?

図2-aで示されたMediumリスク以上の問題点を検出した74%のスマホアプリについて別の見方をすると、これらのアプリケーションは第三者に悪用される恐れがあるということができます。診断がスマホアプリの公開前に実施されたのであれば、明らかになった問題を修正してから公開すればよいのですが、これらMediumリスク以上の問題点を抱えるスマホアプリの中には、Google PlayやApp Storeといったスマホアプリの公式マーケットへの公開後に診断を実施したものもあります。ひとたび公開したスマホアプリは、攻撃者がそれを解析し悪用することも可能となるため、不備がある場合は早急な対策が必要となります。

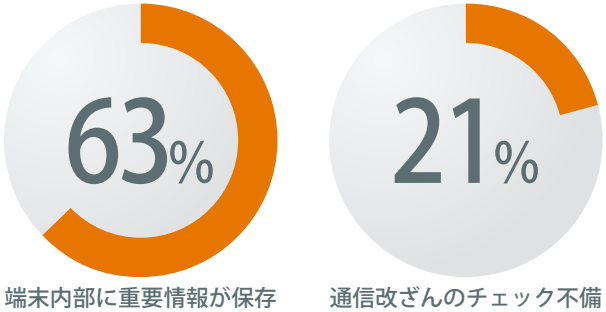
また、診断によって検出されたリスクをスマホのOS別に見ると、図2-cに示すように、Mediumリスク以上の問題点を抱えるスマホアプリの割合はAndroidとiOSとで大差ないことがわかりました。App Storeのアプリは Apple社による審査を受けているため、以前はスマホアプリを使うならiOSの方が安心だとされていましたが、分析結果からはそうとも言えない状況となっています。

図2-c スマホOS別検出リスク割合



スマートフォンアプリケーション診断の総合評価(AAA、AA、A、B、Cの5段階)をAndroid及びiOSごとに集計した。iOSの2%に一番高いAAA評価があった部分が異なるが、AndroidとiOS共に大差はない状況。

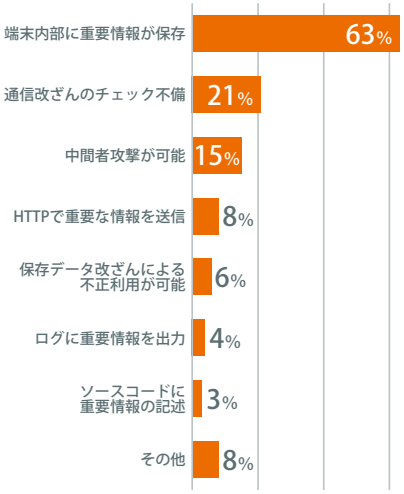
図2-d



2016年4月から2017年9月までの「スマートフォンアプリケーション診断」で検出されたリスクの高い問題点のうち、上位2つは「端末内部に重要情報が保存」と「通信改ざんのチェック不備」だった。

※2a 5段階の総合評価：総合評価の詳細については13ページ表7-aを参照
※2b 問題点：ラックでは、脆弱性とまではいえない軽微な問題も調査し、「問題点」として報告している。
※2c 端末のroot化：スマホ端末には通常、機能制限が施されており、いわゆる管理者権限を利用者は取得できないが、特殊な手法によってその管理者権限を取得する方法をroot化と呼ぶ。とりわけiOS(iPhone、iPad)で管理者権限を取得する手法は、Jailbreakと呼ばれることが多い。

図2-e Mediumリスク以上の問題点検出率



2016年4月から2017年9月までの「スマートフォンアプリケーション診断」で検出されたリスクの高い問題点を検出率が高い順に並べた。「端末内部に重要情報が保存」の多さがひと際目立つ。

スマホの重要情報が危ない

「スマートフォンアプリケーション診断」で検出された、リスクが高く、かつ多くのスマホアプリで見られた問題点を図2-eにまとめました。

検出率が高かった問題点の上位3つは、順に「端末内部に重要情報が保存」「通信改ざんのチェック不備」「中間者攻撃が可能」で、これらはいずれも、情報漏えいやスマホアプリの不正利用につながる恐れがあります。中でも注目したいのは、検出率が特に高く、半数以上のスマホアプリに見られた「端末内部に重要情報が保存」で、これはスマホアプリ特有の問題点です（上位3つの問題点は、4章 検出率の高い問題点の解説 にて説明）。

2016年4月から2017年9月の間にラックが診断したアプリケーションを、カテゴリごとに分類したのが図2-fです。診断で最も多く対象としたのは「金融／FinTech」系スマホアプリで、これらのアプリケーション提供者のセキュリティ意識の高さがうかがい知れます。次いで「教育・資格」、「エンターテインメント／ライフスタイル」の順に多く、一般コンシューマ向けで利用者の多いスマホアプリが上位を占めました。車載器や家庭用電気製品といった、IoTデバイスと連携するスマホアプリも登場しており、それに対する診断依頼の件数は2016年と2017年を比較すると2倍に増加しています。今後もこの増加傾向は続くと見込んでいます。

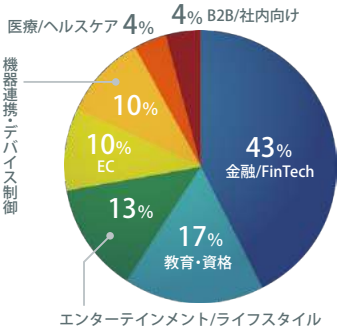
「スマートフォンアプリケーション診断」の実施を検討するに当たっては、開発ライフサイクルのどのタイミングで行うかがポイントになります。診断のタイミングは、大きく公開の前と後の２つに分かれます。公開前に実施するのは問題をあらかじめ解消するため、または、公開が可能かどうかを判定するためです。一方、公開後に実施する場合の多くはスマホアプリの現状把握を目的としています。診断実施のタイミングについてラックのお客様にアンケートした結果が図2-gです。それによると、全体の4分の3が「公開前」と回答（76%）、「公開後」としたのは4分の1（24%）でした。ラックにスマホアプリの診断を依頼する企業の多くが、セキュリティを念頭に置いて開発を実施していることがわかります。

スマホの進化と利用者保護のバランス

図2-hは、スマホアプリが対応するAndroid及びiOSのバージョンを示しています。気を付けておきたいのは、セキュリティパッチが提供されなくなった古い端末でも、スマホアプリを使い続ける利用者がいるということです。古くなったスマホを使い続けることは利用者にとってセキュリティ上のリスクを抱えることを意味します。開発者は、利用者保護の観点からスマホアプリが対応するOSのバージョンに一定の制限を設けることを検討する必要があります。

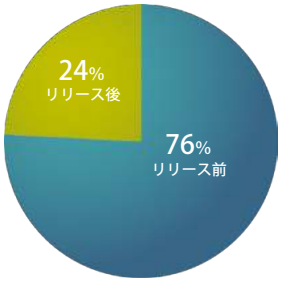
例えば、Android OS搭載端末では毎月セキュリティパッチが提供されていますが、発売してから一定の時間が経過した端末には、セキュリティパッチが提供されなくなります。そのため、2.X系、3.X系、4.4未満(※2d)といった古いAndroid OSを搭載した端末では、OSに脆弱性を抱えたままアプリケーションを利用することになります。2013年12月に公表されたWebViewの脆弱性(※2e)では、特定条件を満たすとAndroidアプリ経由で端末を攻撃することが可能になり、端末情報が読み取られたり、他のアプリケーションを起動させられたりする恐れがあります。フィーチャーフォンが主流だった時代は、対応する端末の種類が多いアプリケーションのほうが、利便性が高く有用でした。しかし、WebViewの事例から今、私たちが学ぶべきは、脆弱性を抱えたOSにアプリケーションが対応し続けると、利用者が攻撃の危険にさらされ続ける恐れがあるということです。対応OSのバージョンの制限は利用者の減少につながりますが、サービス事業者は、いかに利用者を増やすかだけでなく、利用者保護の観点からの考慮も必要な時代になっています。

図2-f アプリケーション種別



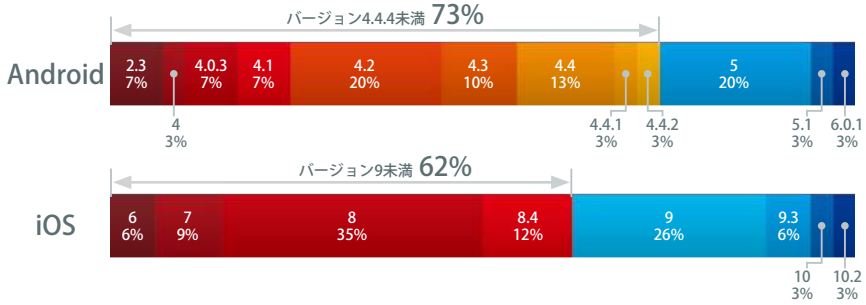
診断対象のスマホアプリをカテゴリ分けした。金融系スマホアプリの割合が多い。

図2-g 診断のタイミング



構築確認やリリース判定のために公開前（アップデートも含む）に診断するケース、公開後に現状把握として診断するケースの割合を円グラフにした。

図2-h スマホOS別バージョンの割合



上は、診断対象のAndroidアプリが動作をサポートする一番古いAndroid OSのバージョン（minSdkVersion）を一覧にしたもの。集計を開始した2016年時点でAndroidセキュリティチームからセキュリティパッチが配布されていないバージョン4.4.4未満に対応するアプリケーションが73%あった。
下は、診断対象のiOSアプリが動作をサポートする一番古いiOSのバージョン（MinimumOSVersion）を一覧にしたもの。集計を開始した2016年時点で2015年10月が最後のセキュリティパッチとなったiOS8.4及びそれ以前に対応するアプリケーションが62%あった。

※2d **2.X系、3.X系、4.4未満**：2017年12月時点で、Androidセキュリティチームが提供するセキュリティパッチはAndroid version4.4以上が対象。なお、Androidセキュリティチームが提供しないということであり、通信キャリアや端末ベンダが独自にセキュリティパッチを提供する可能性はある。
https://source.android.com/security/overview/updates-resources
※2e **WebViewの脆弱性**：JVN#53768697 Android OSにおいて任意のJavaのメソッドが実行される脆弱性
https://jvn.jp/jp/JVN53768697/

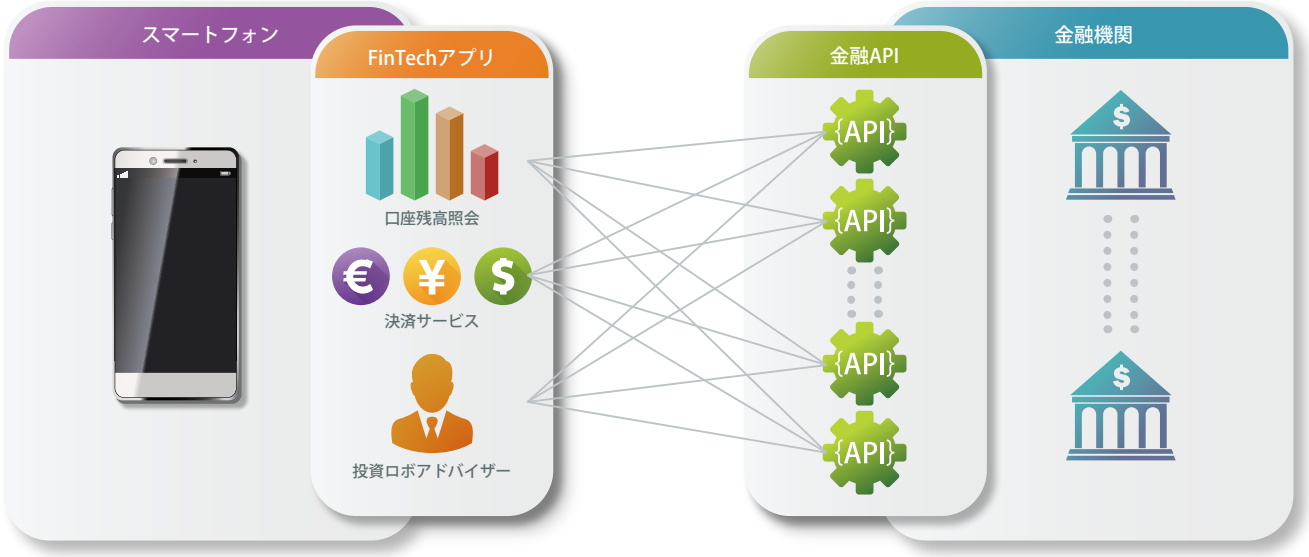
3 金融系スマホアプリのセキュリティ対策は一歩先行くが、見逃しがちな課題あり

スマホでは機能の拡充が頻繁に行われています。iOS（iPhone）やAndroid OSを搭載した端末には当初、電話やメール、ウェブブラウザといった最低限の機能しかありませんでしたが、後にGPSやBluetooth、指紋認証といったセンサーやモジュール類が搭載され、利便性が向上しました。2014年には、Apple Pay(※3a)、2015年にAndroid Pay(※3b)といったモバイル決済や電子マネーのための機能がグローバルスタンダードとして使用できるようになりました。それらの進歩とともに、金融機関においてもITを利活用する動きが活発になり、金融機関独自のスマホアプリや電子マネーが使えるスマホアプリ等が誕生しています。

金融APIが今後の主流へ

近年では、金融API(※3c)の公開による複数のサービス間連携が図られ、IT企業が金融事業に参入し始めています 図3-a。国からの金融サービスデジタル化推進の期待も高く、2017年５月には、金融機関に対してAPIを公開する努力義務を課す「銀行法等の一部を改正する法律」(※3d)が成立しました。APIの公開が進む前にもFinTechアプリケーションはありました。Webサイトから Webページのデータを収集し、情報を抽出するスクレイピング技術を用い、利用者の代わりに金融機関の口座情報を取得して利用者に提供していました。しかし、利用者の口座に認証するための機微情報をFinTech企業が預かるため、FinTech企業は漏えいリスクを抱えることになり、大きな問題となっていました。金融APIの具体的な仕組みについては割愛しますが、金融APIが公開されることでこうしたリスクが解消され、今後は、金融APIを利用したスマホアプリが増加していくことが見込まれます。

図3-a スマホアプリとつながる金融APIの例



複数の金融機関が提供するAPIをスマホアプリ経由で利用できる。金融機関を横断した口座の管理や決済など便利なサービスを享受できる。

金融系スマホアプリでは金銭・重要情報を取り扱うため、よりセキュリティを考慮する必要があります。ここでは、個人や法人の事業活動に影響を及ぼす恐れのある、金融系スマホアプリを取り巻くリスクを以下に見ていきます。

マルウェア感染のリスク

有名な、もしくは利用者の興味を引くスマホアプリを装ったマルウェアを利用者にインストールさせ、他のスマホアプリが端末内に保存した情報を狙う攻撃が以前から広く確認されています。近年では、金融機関のスマホアプリを狙うバンキングマルウェアが増加しています(※3e)。

被害事例：バンキングマルウェア

利用者の認証情報を窃取するバンキングマルウェアが発生しています(※3f)。あるAndroid向けのマルウェアは動画紹介アプリを装っていました。このアプリケーションをインストールした利用者がAndroid用バンキングアプリを起動させると、偽の認証画面が表示され、入力した認証情報を攻撃者に窃取されて不正送金などに悪用されます。すでに日本の銀行が標的にされているという情報もあります(※3g※3h)。

紛失した際のリスク

スマホには、「小型で持ち運びしやすいがゆえに紛失しやすい」という特有のリスクがあり、それによる脅威を考慮する必要があります。あるセキュリティ企業の調査によると、スマホを紛失した経験があるのは日本国内では全体の23%に上っていました(※3i)。紛失によるセキュリティ上の影響については、利用者だけでなくスマホアプリ開発者も理解しておく必要があります。特に、ID／パスワードやセッションといった重要な情報が暗号化されることなしに端末内部に保存されている場合は要注意です。紛失したスマホが悪意のある人物に拾われ、暗号化されていない重要情報が窃取されてしまうと、不正利用され被害にあう恐れがあります。

被害事例：コンシューマ向け電子マネーアプリ

スマホを紛失したために多額の電子マネーを不正利用される被害も実際に起きています。不正利用を受けて、被害者が電子

※3a Apple Pay：https://www.apple.com/jp/apple-pay/
※3b Android Pay：https://www.android.com/intl/ja_jp/pay/
※3c 金融API：APIはソフトウェアコンポーネント同士がやり取りするのに使用する接続仕様等をいい、あるアプリケーションの機能、データ等を別のアプリケーションから呼び出すことが可能となる。身近なものでは、アプリケーション内で地図が表示されるGoogle Map APIが挙げられる。金融APIは金融サービスの残高参照や口座振り込み等の一部機能を金融機関がFinTech企業に公開するものを指す。
※3d 銀行法等の一部を改正する法律（銀行法の一部改正）：http://www.fsa.go.jp/common/diet/193/index.html
※3e Mobile Malware Evolution：2013：https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/
※3f Android Trojan Targeting Over 420 Banking Apps Worldwide Found On Google Play Store：http://thehackernews.com/2017/04/android-banking-malware.html
オンラインバンクを襲うトロイの木馬がAndroid機器に出現：https://eset-info.canon-its.jp/malware_info/news/detail/160329.html

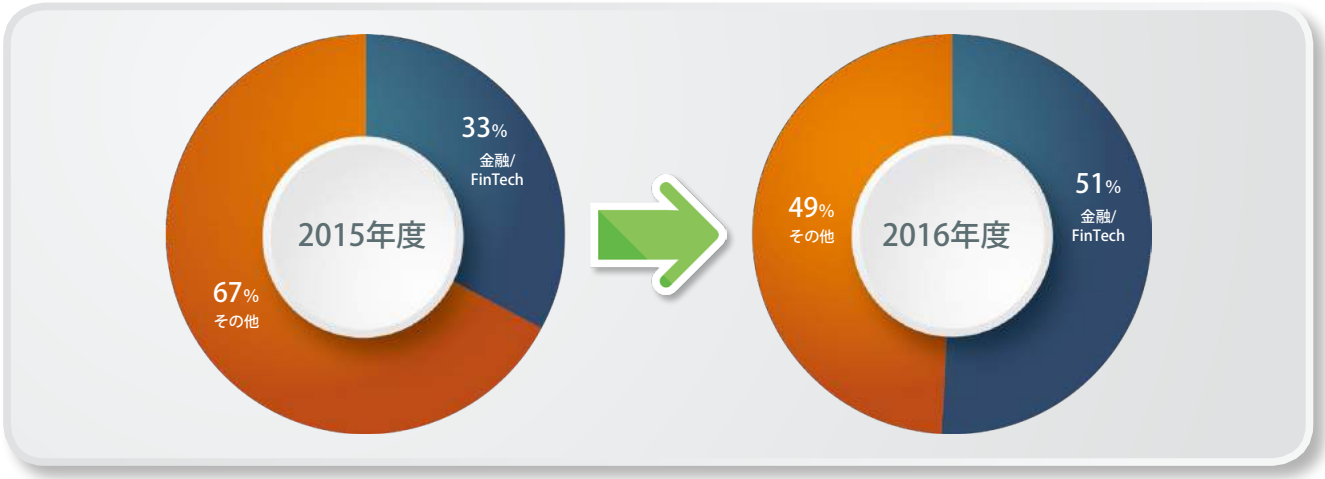
マネーのサービス提供会社を訴えたケース(※3j)では、携帯電話会社経由で、紛失した端末の専用データ通信を停止したものの、Wi-Fiを使っての通信は可能だったため、何者かにスマホアプリの設定を操作され、不正に電子マネーを利用されたとされています。

スマホには、パスコードを設定した画面ロック機能がありますが、絶対に安心だというわけではありません。スマホアプリで重要処理の操作前に認証情報入力を要求するよう実装することや、サービス運営側は、利用者がスマホ以外から利用停止を申請できる仕組みを備えるなどの策を講じることを推奨します。

スマホアプリを解析されたときのリスク

スマホアプリは公開されているプログラムであり、誰でもダウンロードして解析することができるため、スマホアプリそのものに重要な情報が含まれないかも確認しておく必要があります。米国セキュリティ会社Fallibleの2017年の報告によると、調査したスマホアプリにサードパーティのサービス(API)にアクセスするためのAPIキー(※3k)がハードコードされていることを確認したとされています(※3l)。金融系スマホアプリに、重要な機能を担うAPIキーがハードコードされ、APIキーを取得した悪意ある人物にそのAPIを悪用された場合、金銭被害が発生する恐れがあります。それだけではなく、信用を重視する顧客との間で信用問題に発展する恐れもあります。

図3-b 金融系スマホアプリとその他のアプリケーションにおける診断実施割合の推移

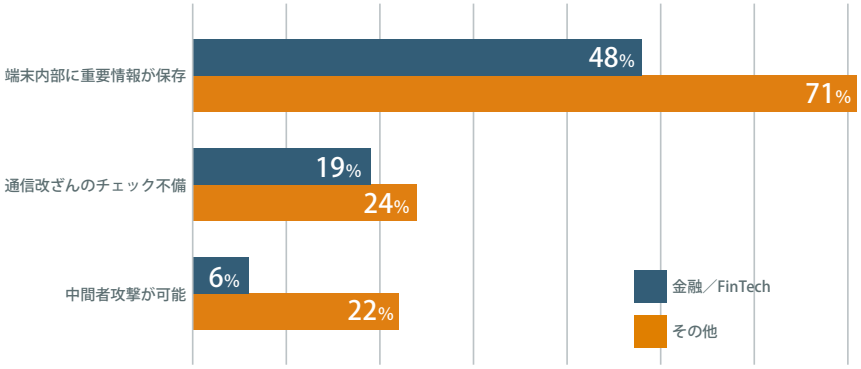


2015年度と2016年度のスマートフォンアプリケーション診断結果であり、2016年度は「金融／FinTech」が51%となっている

図3-bは、2015年度と2016年度のそれぞれ1年間に診断を実施した、スマホアプリの割合の推移を示したものです。2016年度の1年間では、「金融／FinTech」に分類されるスマホアプリが51%となっています。2015年度の33%と比較して診断に占める割合が増加している背景には、金融／FinTech企業がAI、IoTやブロックチェーンなどといった新しい技術を取り込んで積極的に新しいサービスを創出しており、その実現手段の一つにスマホアプリを採用していることが挙げられます。産業界全体で見ても、金融機関が他に先駆けてセキュリティへの取り組みを活発化させており、スマホアプリに対してもいち早く対応しました。スマートフォンアプリケーション診断がシステム運用の一部になっていることがわかります。

図3-cは、診断アプリケーションのカテゴリを「金融／FinTech」と「その他」に分け、問題点の検出率を抽出したもので、次の2点でとても興味深い結果となっています。1点目は、「通信改ざんのチェック不備」や「中間者攻撃が可能」の問題点が、金融系スマホアプリでは比較的検出率が低かったことです。これらは、Webアプリケーションにも共通する問題です。金融系スマホアプリやサービスに関して、金融機関はAPI公開へ向け、FinTech企業に対してセキュリティ要件の遵守を強く求める傾向にあります(※3m)。Webアプリケーションのセキュリティ対策にたけた金融機関自身は、開発ガイドラインやチェック体制をすでに整えており、問題点の検出率が低かったと考えられます。2点目は、「端末内部に重要情報が保存」の項目が「金融／FinTech」でも半数近くあり、「その他」では7割を超えて多いということです。これはWebアプリケーションにはないスマホアプリ特有の問題です。スマホアプリ特有の問題に関しては、セキュリティに積極的な金融系スマホアプリでさえも対策の必要性がまだ浸透していないことが推察されます。

図3-c 金融系とその他のアプリケーションにおける問題点検出率



2016年4月から2017年9月までのスマートフォンアプリケーション診断結果について、アプリケーションのカテゴリ「金融／FinTech」と「それ以外」に分けて問題点の検出率を出した。それぞれの診断数を母数として検出率を再計算している。「端末内部に重要情報が保存」は「金融／FinTech」アプリケーションでも半数近くで検出されており、対策が漏れがちな問題点といえる。

※3g Injections for Japanese Banks in High Demand on the Russian Underground：https://blog.sensecy.com/2017/07/04/injections-for-japanese-banks-in-high-demand-on-the-russian-underground/
※3h オンラインバンキングアプリを狙う「BankBot」を「Google Play」上で確認、国内銀行7行も対象：http://blog.trendmicro.co.jp/archives/15950
※3i Lookout、スマホ紛失に関する調査結果を発表：https://www.lookout.com/jp/news-mobile-security/phone-loss-in-japan1
※3j 楽天Edyに賠償命令 電子マネー不正利用被害で高裁：https://www.nikkei.com/article/DGXLASDG18HBG_S7A120C1000000/
※3k APIKey：Webサービスを利用するための認証キーのこと。
※3l We reverse engineered 16k apps, here's what we found：https://hackernoon.com/we-reverse-engineered-16k-apps-heres-what-we-found-51bdf3b456bb
※3m オープンAPIのあり方に関する検討会報告書－オープン・イノベーションの活性化に向けて－【中間的な整理(案)】：https://www.zenginkyo.or.jp/fileadmin/res/news/news290316_2.pdf

4 検出率の高い問題点の解説

4–1 スマホアプリならではの脅威

図4-a スマホアプリを取り巻く脅威

ここでは、スマホアプリ(もしくはそのサービス)を取り巻く脅威を改めて整理し、図4-aに示すような5つの脅威に分類しました。

① 通信の盗聴・改ざん（中間者攻撃）

中間者攻撃は、スマホアプリとサーバの通信経路上に攻撃者が介入して、通信の盗聴や改ざんが行われる脅威です。詳細は、「4-4 問題点：中間者攻撃が可能」を参照してください。

② 通信の改ざん

通信の改ざんは、スマホアプリからサーバへ送られる通信、もしくはその逆の通信内容を攻撃者に改ざんされ、意図しない処理を実行させられる脅威です。詳細は、「4-3 問題点：通信改ざんのチェック不備」を参照してください。

③ マルウェアによる脅威

スマホのマルウェアは、有名な、もしくは利用者の興味を引くアプリケーションに偽装したりすることで、不審に思われることなくインストールさせます。スマホアプリの機能を不正操作したり、保存している重要情報を窃取したりする恐れがあります。これらのマルウェアは、公式のアプリマーケットで公開されていることがあり、利用者がマルウェアか正規のアプリケーションかを見分けるのは困難です。

④ 解析による情報漏えい

スマホが攻撃者の手に渡ってしまうと、スマホアプリの内部にあるデータが攻撃者によって解析され、窃取されてしまう恐れがあります。詳細は、「4-2 問題点：端末内部に重要情報が保存」を参照してください。

⑤ 再コンパイルして既存のアプリケーションにマルウェアを注入（リパック）

攻撃者は、公開されているスマホアプリを解析して不正なコンテンツやマルウェアを仕込み、正規のスマホアプリに偽装して配布します。正規のスマホアプリを流用しているため、利用者には判別がつきません。リパックされたスマホアプリをインストールしてしまうと、保存している重要情報を窃取される恐れがあります。

技術の進歩によってスマホアプリが高機能になるにつれ、端末やアプリケーションが保有する情報資産は増加の一途です。そのため、スマホアプリ開発者は今まで以上にセキュリティへの配慮が求められます。十分な対策を施すことで、情報漏えいやなりすましといった被害の軽減につながります。

4–2 問題点：端末内部に重要情報が保存

スマホには、電話帳やメールなどのプライバシー情報に加え、スマホアプリの実装によっては認証情報、設定情報や暗号化／復号に用いられる秘密鍵など、端末の内部に重要な情報が保存されていることがあります。そのため、セキュリティを考慮せずに実装すると、これらの重要な情報が攻撃者に窃取される恐れがあります図4-b。

セキュリティ上の影響

端末の内部には、セッション情報が保存されていたり、ID／パスワードやカード情報といった、特に重要な情報が保存されていたりすることがあります。これらの情報が第三者に窃取されると、なりすましによる不正ログインやカード情報の不正利用などの被害にあう恐れがあります。問題を悪用するには端末のroot化が必要となるケースが多いものの、端末が攻撃者の手に渡った時点で端末のセキュリティ機構はいずれ破られる恐れがあるため、アプリケーション側でも対策をしておくほうがよいでしょう。

攻撃者像

悪意のある利用者、端末を拾った攻撃者、マルウェア。

被害例

端末内部に保存された重要情報の不正利用による被害例として、支払い機能を持つスマホアプリを使った不正な支払い処理のケースを説明します図4-c。被害者が紛失したスマホを攻撃者が拾い、スマホアプリを含めた端末内部を解析したと想定します。解析の結果、攻撃者が被害者の使用していたスマホアプリのID／パスワードを奪取すると、それを悪用して不正ログインし、支払機能を使用すると考えられます。

対策

端末の内部は解析される恐れがあるため、原則として重要情報はサーバに保存するようにしてください。やむを得ず端末内部に保存する場合は、重要情報を暗号化する必要があります。ただし、暗号化／復号用の鍵を管理する際は、解析に対してどこまで強度を保てるかの検討が必要です。ラックが実際に確認した対策が不十分な例では、暗号化／復号用の鍵がそれとわかる形で端末内部に保存されていたり、ソースコードそのものに記載（ハードコード）されていたりした事例がありました。また、Webサーバとの通信（リクエスト、レスポンス）がキャッシュとして保存されることがあります。通信には重要情報が含まれることがあるため、キャッシュしない、またはキャッシュを削除するといった対策を実施してください。

図4-b 端末内部に保存されていた重要情報

端末に残しがちな重要情報を例示した。いずれも「スマートフォンアプリケーション診断」で実際に指摘したものである。

図4-c 端末内部の情報を窃取される

青色の人物：利用者（被害者）、紫色の人物：攻撃者。被害者が紛失したスマホを攻撃者が拾い悪用する例。入手したスマホのアプリケーションを解析し、ID／パスワードを窃取。利用者になりすまして支払い処理を実行。

4−3 問題点：通信改ざんのチェック不備

通信改ざんのチェック不備は、サーバと通信するスマホアプリで注意が必要な問題点です。スマホアプリからサーバに送る通信（リクエスト）や、サーバからスマホアプリに送る通信（レスポンス）を改ざんすることで、本来とは異なる処理が行われます。

セキュリティ上の影響

リクエスト・レスポンスに含まれる利用者識別子や価格といったパラメータの値を改ざんし、そのまま処理されてしまうと、利用者のなりすまし、個人情報の漏えいやシステムの不正利用などが行われます。

攻撃者像

悪意のある利用者

被害例

ポイント不正取得の被害例として、ポイント交換機能を持つスマホアプリを悪用したケースを想定します図4-d。現金とポイントを交換する際、悪意のある利用者（攻撃者）に交換レートを改ざんされると、少ない金額で多くのポイントを取得されます。また、サーバレスポンスを改ざんされると、本来付与される以上のポイントを取得されます図4-e。スマホアプリとサーバ間のリクエスト通信、またはレスポンス通信のいずれかを改ざんでき、改ざんした値を重要な機能の処理に使われる場合は、悪用される恐れがあります。

対策

対策を実施するに当たって検討する必要があるのは、"どこで"重要な処理が行われているかです。

●サーバ側で処理している場合

重要な機能をサーバ側で処理している場合は、スマホアプリから渡される値が正しいか、改ざんされていないかのチェックを厳密に実施してください。

上で述べた被害例への具体的な対策は、スマホアプリからサーバに渡される値の取り扱いに注意することです。それには暗号化通信を徹底し、中間者攻撃を防ぐことが大前提です。サーバに渡される入力値に関しては、それぞれの入力項目の仕様に応じてチェックし、想定外の値はサーバ側で拒否するようにします。図4-dの例では、入力されたポイント数が数値以外や負の数値の場合、サーバ側で拒否します。また、スマホアプリから交換レートの値を送るという実装にはしないことも重要です。

●スマホアプリ側で処理している場合

スマホアプリ側に重要な処理を実装すると、解析され悪用される恐れがあります。一般的なWebアプリケーションと同様に、重要な処理はサーバ側で処理するように実装してください。

具体的には、保持ポイントやレートは原則としてスマホアプリ内に保存しないこととし、やむを得ずスマホアプリ側に持たせる場合は改ざん検知機能を実装するようにします。ただし、メモリ内が書き換えられて検知機能を回避される恐れがあるため、根本的な対策とはなり得ない点に注意が必要です。

図4-d レートの改ざん

スマホアプリからサーバへの通信（リクエスト）内で、「200円 1ポイント」という交換レートが定義されているアプリケーション。交換レートを改ざんできる脆弱性があり、攻撃者は「200円 1ポイント」を「100円 3ポイント」と改ざんし、ポイントを不正に多く入手した。

図4-e 付与されるポイントを改ざん

サーバからスマホアプリへ、送られてくる値を付与ポイントとして処理するアプリケーション。送られてくる値を改ざんできる脆弱性があり、攻撃者は1ポイント付与されるところを3ポイントと改ざんした。保持しているポイントの表示改ざんは容易だが、改ざんした所持ポイントを実際に使用できるかどうかは対象システムの実装に依存する。

4−4 問題点：中間者攻撃が可能

中間者攻撃が可能は、SSLサーバ証明書の検証方法に不備がある場合に検出される問題点です。HTTP通信は平文のため、通信経路から盗聴・データの改ざんが容易で、重要情報の送信には向きません。重要情報を送受信する際には、暗号化通信や接続先サーバが本物かどうかを検証するHTTPS通信を使います。しかし、スマホアプリとサーバ間でHTTPS通信する際にSSLサーバ証明書の検証方法に不備があると、通信先のサーバが偽物であっても通信が可能となるため、中間者攻撃が行われる恐れがあります。2014年に米国のCERT/CCは、数多くのAndroidアプリケーションにこの脆弱性が作り込まれていることを発表しました(※4a)。この発表により、作り込みが容易な脆弱性として話題になりましたが、依然として対策ができていないスマホアプリが国内にも数多く存在しているのが現状です。

セキュリティ上の影響

中間者攻撃が可能な場合、スマホアプリとサーバ間の通信経路上に攻撃者が介入し、盗聴や改ざんが行われる恐れがあります。また、通信先のサーバが偽物であってもSSL通信が確立するため、利用者からは偽物と判別できず、重要情報の漏えいにつながる恐れがあります。

攻撃者像

スマホアプリとサーバ間の通信経路に入ることができる攻撃者

被害例

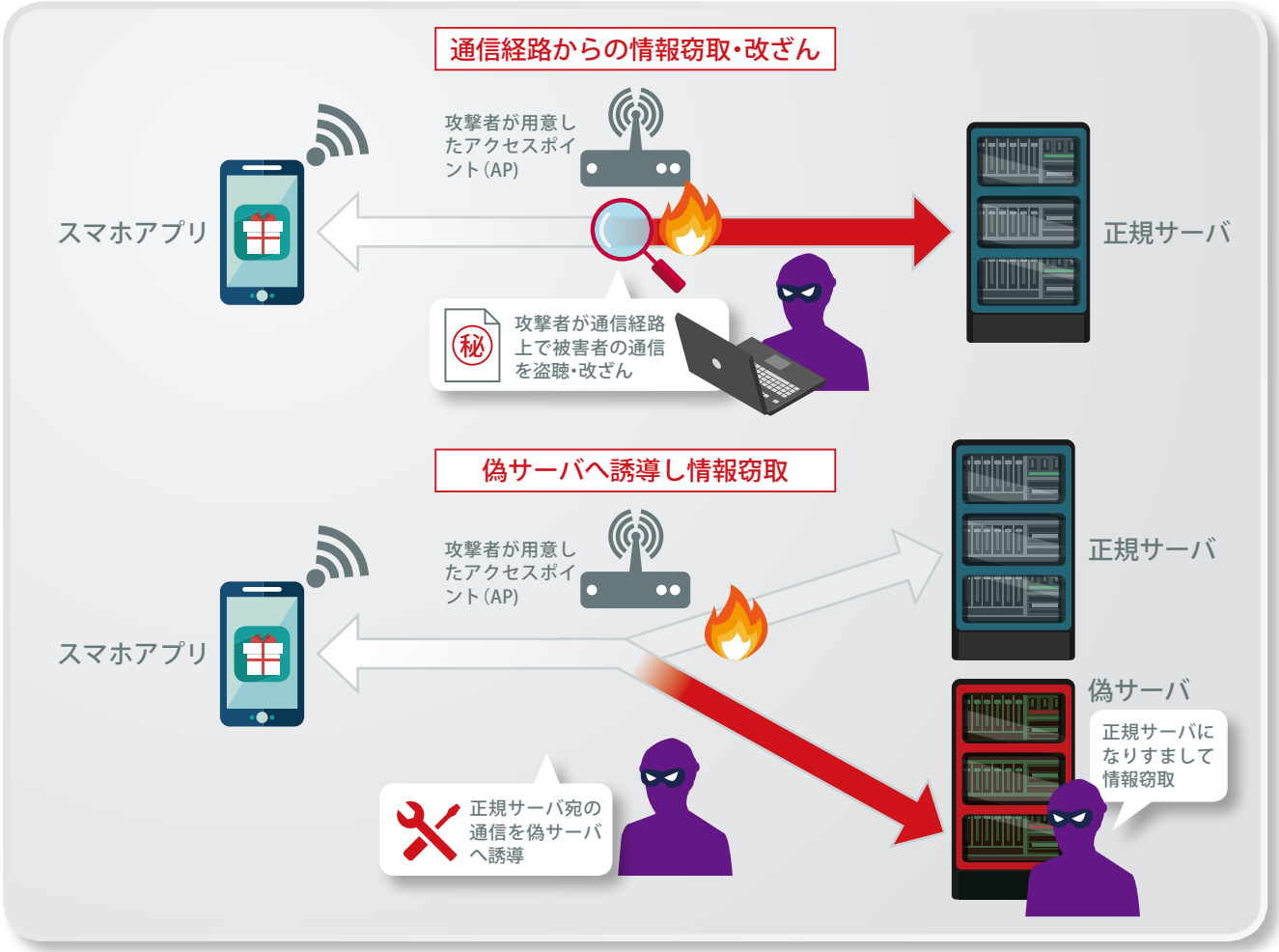
ここでは、送金機能を持つスマホアプリへの攻撃例を説明します図4-f。被害者が送金機能を持つアプリケーションで送金をしようとしたとき、攻撃者の用意したAP(アクセスポイント)にそれと知らずWi-Fi接続してしまうと、攻撃者に通信を盗聴され、送金先を攻撃者が用意した口座に改ざんされて金銭を詐取されます。

対策

対策として、接続するサーバから送付されるSSLサーバ証明書が適切であるかを検証する仕組みをスマホアプリ側に実装し、SSLエラーが発生した場合は通信を切断してください。昨今は公衆無線LANが急速に普及していますが、利用する公衆無線LANが安全なものかを利用者自身が把握することは難しいためです。

また、HTTP通信で重要情報を送信することは避けてください。HTTP通信には中間者攻撃を防ぐ仕組みがありません。重要情報はHTTPS通信で送受信するようにしてください(※4b)。

図4-f 中間者攻撃で情報窃取・改ざんされる例



攻撃者は、カフェや駅などが無料で提供している公衆無線LANのSSIDに似せたSSIDを持つアクセスポイント(AP)を用意する。被害者はそれと知らず偽物のAPに接続し、サービスを利用する。中間者攻撃対策の取られていないスマホアプリを利用すると、通信内容の盗聴や通信内容の改ざん等が生じる。また、攻撃者により正規のサーバへの通信を、攻撃者が用意した偽サーバへ強制的に接続させられる恐れがある。

※4a **Multiple Android applications fail to properly validate SSL certificates**：https://www.kb.cert.org/vuls/id/582497
※4b **【iOS】**
ネットワーク通信のセキュリティ機能
https://developer.apple.com/jp/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/SecureNetworking/SecureNetworking.html#//apple_ref/doc/uid/TP40010220-CH1-SW1
【Android】
HTTPSおよびSSLによるセキュリティ
https://developer.android.com/training/articles/security-ssl.html?hl=ja

5 スマホアプリユーザを守るために 無償ガイドラインを活用して上流工程からセキュリティ対策を

本レポートで説明したさまざまな問題は、入念なセキュリティ対策を実施しているお客様のスマホアプリからも検出しています。大規模なシステム開発とは異なり、スマホアプリは技術や端末、開発環境の進化が著しく開発期間も短いことから、セキュリティ対策に十分な時間を割きにくいのが実情です。しかし、だからこそ開発工程に合わせてセキュリティ対策を実施することが有効となります図5-a。特に、仕様や設計に関わるところでセキュリティ上の問題を抱えてしまった場合、公開後の修正は影響する範囲が広くなり、改修コストもかさみます。開発工程ごとにセキュアな設計やセキュアコーディングを心がけ、必要に応じて第三者によるセキュリティ診断・監査を受けることをお勧めします。

設計にガイドライン活用

スマホアプリの開発において、日本スマートフォンセキュリティ協会(JSSEC)が提供する『Androidアプリのセキュア設計・セキュアコーディングガイド』(※5a、図5-b)は開発者必携の手引きです。これはAndroid向けのガイドラインですが、特に設計工程の考え方はiOSにおいても参考になります。

設計工程で検討する点は、守るべき情報資産及び機能資産を明確にすることです。JSSECのガイドラインでは、電話番号やプライバシー情報などを情報資産とし、カメラやGPS、通話機能など、漏れた場合にプライバシーを損ないかねない機能を機能資産として定義しています。スマホアプリの設計では、スマホが持っている情報や機能を守るために、スマホアプリからスマホへの機能へのアクセスを必要最小限にするなどの考慮が必要です。

実装時の具体的な事例も紹介

JSSECのガイドラインは実装工程でも活用できます。ガイドラインの中にはサンプルコードの紹介があります。アプリケーション機能の仕様のフローが用意されており、開発中のアプリケーションに合わせたサンプルコードを選択してセキュリティ上のポイントを確認しながら実装できます。例えばHTTPS通信の場合、証明書で注意する点や、HTTPS接続したサーバからのデータでも安全性を確認するといったポイントが紹介されています。実装に当たっては、アプリケーションの性質や機能に合わせて次の2点のようなセキュリティ対策を心がける必要があります。

●root化した端末で解析されて情報を窃取されないように、認証情報・口座番号・金額といった情報はアプリケーション内に保存しない。同時に、重要な処理もアプリケーション側で行わない。トークンを保存する場合は期限を設ける

●限定的に公開されているAPIキーは、攻撃者に入手されないように暗号化などの措置を講じる

公開前の最後の砦

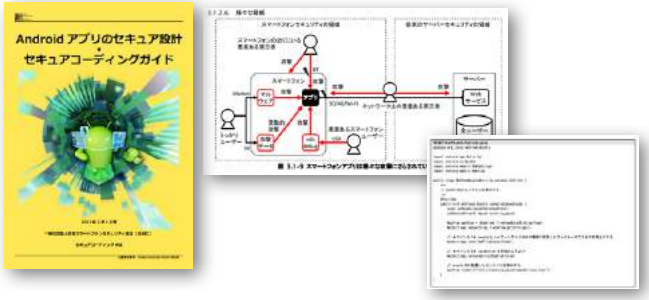
テスト工程には、アプリケーションが正常に動作するかを確認する機能テストと、パフォーマンスや障害時の影響や復旧手順を確認する非機能テストがありますが、セキュリティ診断は非機能テストに大別されます。昨今では、多くの企業がセキュリティを重視するようになり、セキュリティ診断を自社で実施するだけでなく、第三者に依頼する場合もあります。ラックの診断では、スマホアプリを実際に動作させた際の通信内容や、端末に残る重要情報など、スマホアプリそのものも解析しています。これに加えて、スマホアプリの通信先のサーバ側となるWebアプリケーションやそのAPIの診断を同時に実施することも推奨しています。ラックの主なセキュリティ診断対象は、7章のセキュリティ診断ラインアップで示しています。

公開時や診断終了時には十分なセキュリティが担保されていたとしても、その状態は永続的に保証されるものではありません。度重なるアップデート中に脆弱性を作り込んでしまったり、サードパーティのモジュールに新たな脆弱性が発見されたりすることがあり、年を経るごとにセキュリティ上の問題が露見する事態が起きます。例えば、Bluetoothによって機器連携を試みる機能を新たに実装した場合、Bluetoothが新たな攻撃経路となり得ます。そのため、定期的またはアプリケーションの改修タイミングに合わせて継続的なセキュリティ診断を実施するという観点も必要となります。

図5-a 開発工程に合わせた主なセキュリティ対策

開発工程に合わせて必要なセキュリティ対策を行うことで、コストパフォーマンスの高い対策ができる

図5-b Androidアプリのセキュア設計・セキュアコーディングガイド



スマートフォンの安全な利活用を促進しているJSSECが提供する「Androidアプリのセキュア設計・セキュアコーディングガイド」。セキュアな設計から具体的なソースにまで落とし込んだ実装例があり、スマホアプリの開発では必携の手引き。

※5a Androidアプリのセキュア設計・セキュアコーディングガイド：https://www.jssec.org/dl/android_securecoding.pdf

6 スマートフォンアプリケーション診断／IoTセキュリティ診断の紹介

6-1 スマートフォンアプリケーション診断

ラックの「スマートフォンアプリケーション診断」は、2011年に開始し、これまでさまざまな業種やカテゴリのスマホのアプリケーションの診断実績を積み重ねてきました。最大の特徴は、業界最多水準を誇る診断項目数です。多角的な観点からスマホアプリの問題を洗い出し、利用者が安全・安心にスマホを利用できる社会を目指しています図6-a。

診断方法は、お客様のスマホアプリを実機(iOS/Android)にインストールし、攻撃者の視点からさまざまな疑似攻撃を試みて、スマホアプリの安全性を徹底的に調査します。

診断項目は、JSSECやOWASP Mobileプロジェクトなどの各ガイドラインから診断実施項目を厳選した上で、ラック独自の項目を拡充しています。これは、アプリケーションの設定だけでなく、仕様や設計上のミス、スマホアプリがマルウェアに乗っ取られた場合のリスクや、最新の攻撃事例から想定されるリスクに対応するためです。

診断対象となるアプリケーションは、スマホだけでなく、Apple WatchやWindows Phone向けのものにも対応しています。

図6-a 3つの特徴

1 最新の脆弱性に対応

2 業界最多水準の診断項目数

3 国内最大級の豊富な診断実績

ラックが提供する「スマートフォンアプリケーション診断」の特徴は、最新情報を収集・研究し、診断項目や手法に随時反映していること。業界最多水準の診断項目数を誇る。金融系やヘルスケア、ゲームなど、さまざまなアプリケーションの診断実績あり。

6-2 IoTセキュリティ診断

爆発的な勢いで生活に広がりつつあるIoTを活かしたサービスやデバイス。生活が豊かになる一方で、IoTのセキュリティへの不安が高まってきています。ラックでは、社内に設立したIoT技術研究所の知見を活かし、2017年9月から個別に「IoTセキュリティ診断」を提供しています。

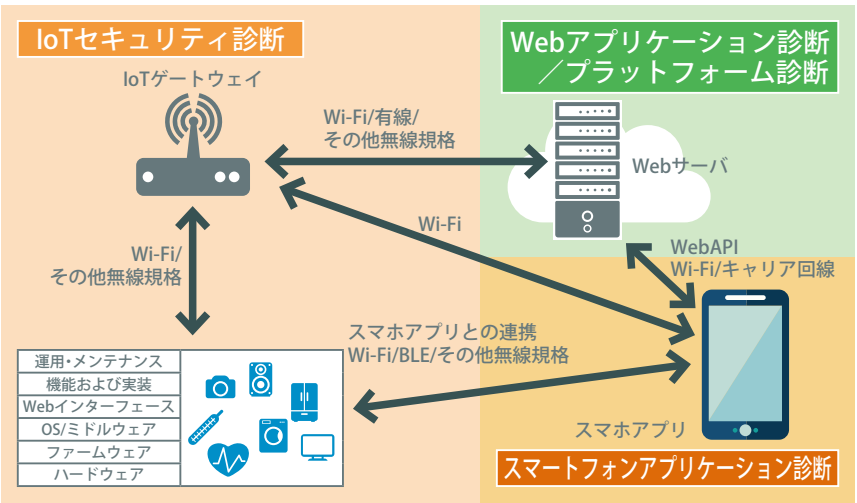
「IoTセキュリティ診断」では、各種センサー、通信装置、スマート家電、スマートホーム、スマート工場、医療機器など多種多様なIoT機器を診断対象としています図6-b。

IoTで利用するWi-Fi/Buletooth Low Energy(※6a)やその他の規格の無線通信、IoT機器上で動作するOS・ミドルウェアやWebインターフェース、IoT機器のファームウェアやハードウェアへの「IoTセキュリティ診断」。これらに加え、ラックが従来から提供しているWebアプリケーション、プラットフォーム、スマートフォンアプリケーション診断サービスを組み合わせることで、IoTシステム全体の診断サービスが提供可能です図6-c。

図6-b 多種多様な機器を診断対象に

IoTセキュリティ診断の対象は、各種センサーや通信装置、スマート家電など多種多様である。

図6-c IoTシステム全体の診断が可能に



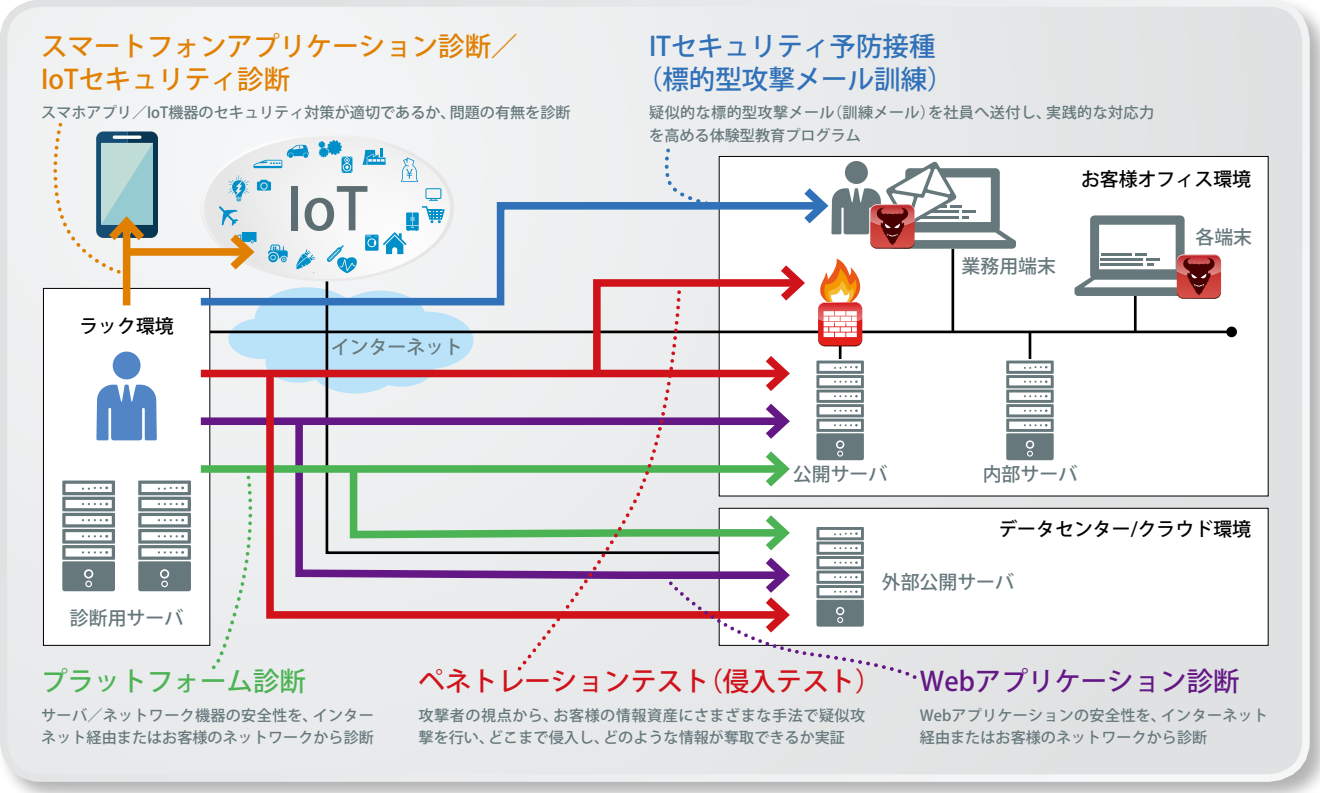
※6a Buletooth Low Energy：Bluetooth 4.0で追加された仕様のひとつで、BLEと表現されることが多い。通信可能距離は短く、通信速度は低いが、低消費電力で動作するため、IoT機器で利用されるケースが多い。

7 ラックのセキュリティ診断ラインナップ

ラックでは「スマートフォンアプリケーション診断」の他にも、豊富なセキュリティ診断サービスを提供しています図7-a。Webアプリケーション診断、プラットフォーム診断などのラインナップを取り揃えています。1995年に日本で初めてセキュリティ診断サービスを開始し、そこから培った長年の経験と多数の実績を基に、セキュリティ診断のエキスパートがお客様のシステムの安全性を徹底的に調査します。

2017年12月からは「ペネトレーションテストサービス」もスタートしました。これは、侵入を中心とした総合的セキュリティサービスで、これまでは問い合わせがある度に個別に対応していましたが、最近の診断ニーズの拡大に合わせて正式にメニュー化したものです。多様化・高度化するサイバー攻撃に対抗するため、そしてお客様のIT資産を安全に守るために、ラックは今後も先手を打ち、診断対象範囲をより一層拡大していきます。

図7-a ラックが提供するセキュリティ診断一覧



参考 総合評価基準および問題点のリスクレベル

ラックでは、「スマートフォンアプリケーション診断」の総合評価基準と問題点のリスクレベルを独自に定義しています。

総合評価は、AAAからCまでの５段階です。評価基準は、スマホアプリごとに検出した問題点のリスクレベルとその検出数から導いています表7-a。

問題点のリスクレベルは、検出された個々の問題点（脆弱性）に対してHigh、Medium、Lowと３段階に分かれます表7-b。各リスクレベルは、セキュリティ上の影響や再現性を考慮して分類しています。

Highリスク、及びMediumリスクの問題点（脆弱性）は「対策が必要」、Lowリスクの問題点（脆弱性）は「対策を推奨」としています。

表7-a 総合評価基準

総合評価結果	説明
AAA	脆弱性なし
AA	Lowが1種類以上
A	Mediumが1種類
B	Mediumが2種類
C	Highが1種類以上またはMediumが3種類以上

表7-b 問題点のリスクレベル

リスクレベル	説明
High	攻撃者の積極的なアプローチによって直接的に情報漏えいやアプリケーションの不正利用などの実害に結びつく可能性のある問題であり、早急に対策が必要
Medium	攻撃手法が複雑、または複数の条件を組み合わせることで情報漏えいやアプリケーションの不正利用などの実害に結びつく可能性のある問題であり、対策が必要
Low	実害に結びつく可能性は低いものの、セキュリティ上好ましくないと考えられる問題であり、対策を推奨

8 スマートフォンアプリケーション診断の7つのギモン!!

スマートフォンアプリケーション診断をより身近に感じていただくため、これまでお客様からいただいたさまざまな質問・ご意見の一部を紹介します。

<診断全般>

Q1：スマホアプリにセキュリティ診断は必要？
A1： 根本的な質問ですが、特にWebAPIを多用するスマホアプリをお持ちのお客様からよくこのような問い合わせを受けます。スマホアプリを取り巻く脅威は多種多様なため、第三者によるセキュリティ診断を推奨しています。ただ、予算との兼ね合いや、仕様上、通信をしない場合、また重要情報を取り扱わないアプリケーションについては優先度を下げてよいと思います。

Q2：セキュリティ対策する上でわかりやすいガイドラインはないか？
A2： 共通で使えるものとしては、本文でも触れた『OWASP Mobile Top 10(※8a)』がオススメ。他にもAndroidでは、5章で紹介したJSSECの『Androidアプリのセキュア設計・セキュアコーディングガイド』が役に立ちます。iOSでは、Appleの公式ドキュメント(※8b)を参照するか、JSSECのAndroid向け資料も設計という点で参考になります。

Q3：どんな環境で診断しているの？
A3： スマホアプリ用の診断ツールやエミュレータも使いますが、攻撃者の目線に立ち、スマホの実機を使ったリアルな環境で診断します。Android、iOSはさまざまなバージョンのOSをroot化して診断に活用しています。

Q4：リバースエンジニアリングはしているの？
A4： iOSアプリ、Androidアプリ両方とも技術的には可能です。開発元からの依頼であればリバースエンジニアリングします。一般的に困難とされるiOSアプリも実施しています！

Q5：アプリケーションの仕様や環境に合わせたカスタマイズ診断は実施している？
A5： カスタマイズ診断にも対応します！　対象となるスマホアプリの仕様や環境に合わせ、メモリ解析、機器連携の通信等の診断項目をカスタマイズして実施します。費用は別途見積もりとなります。

<診断結果について>

Q6：スマホの画面ロック機能があるから、端末内に重要情報が保存されていても問題ないのでは？
A6： 多くの場合はその通りです。しかし、マルウェア感染により窃取されるケースや、紛失した端末を拾われ、解析されてしまうリスクがあります。最悪の場合を想定して重要情報はそもそも保存しない、保存するなら暗号化するといった対策が重要です。

Q7：重要情報を暗号化した際に使った鍵はどこに保持すればよい？
A7： 核心に迫る質問ですね！　Keystore(Android)やKeychain(iOS)といったOSの機能を使うのが一番です。独自に暗号化しようとする際は、暗号化に使った鍵をどうするかが大きな課題です。鍵を鍵とわからないように工夫するのが一つの答えです。とはいえ、Androidは鍵が発覚しやすいという問題があります。これには、Android NDKを使用することで解析難易度を高めることができます。

若いスペシャリストが集結しています。スマホとIoTのセキュリティ診断はお任せください！

ラックのセキュリティ診断チームの中では、一番新しいスマートデバイスアプリケーション診断チームです。2011年にスマホアプリの診断を開始しましたが、IoTの普及をうけて2017年よりチーム名に「スマートデバイス」を冠しました。

スマートデバイスは目まぐるしく進化しているため、チームとしてアジャイルに動くことをモットーとしています。各種ガイドラインの項目はもとより、スマホを含め持ち運びが可能なデバイスのため、悪意を持った攻撃者の手に渡ることを視野に入れてハードウェアを調査したり、メモリ解析や通信の中間者攻撃の調査を実施したりするなど、サポートする技術範囲が広いのが特徴です。

チームメンバーは、暗号研究者、ツール開発者のほか、IPAにて脆弱性分析をしていた者、スマホアプリの元開発者、外資系企業出身のSEなどで、多様なスキルを持っています。システムや機器の弱点はないかを想像しながら、日々勉強を積み重ねて診断手法を習得し、診断範囲を順次拡大中！

国内外のカンファレンスに積極的に参加し、診断技術の研究や発表をしていますので、どこかで皆さんにお目にかかることを楽しみにしています。

チームメンバー(写真上)と診断風景(写真下)

※8a OWASP Mobile Top 10：https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
※8b Appleの公式ドキュメント：https://developer.apple.com/jp/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html

株式会社ラック システムアセスメント部

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113（営業） E-MAIL：sales@lac.co.jp https://www.lac.co.jp