第22回情報セキュリティ・シンポジウム

スマホマルウェアなどの脅威とその対策

KDDI株式会社　サービス統括本部　サービス開発1部
エキスパート　本間 輝彰
teruaki@kddi.com

2021年9月10日

au UQ mobile povo

自己紹介

氏　名　本間 輝彰

業　務　スマホやIoT機器のセキュリティ対策の推進およびセキュリティコンサルなど
セキュリティ関連記事監修やコラム投稿など

社外活動　一般社団法人 日本スマートフォンセキュリティ協会（JSSEC）副会長・理事・幹事

参考資料

TIME&SPACE by KDDI

iPhoneのウイルス対策は？ スマホの対策事情とすぐできる感染防止方法を解説
https://time-space.kddi.com/mobile/20200629/2930

スマホのフィッシング詐欺とは？あなたを守る対策と人間心理をついた手口を解説
https://time-space.kddi.com/it-technology/20200904/2968

スマホの偽警告（フェイクアラート）詐欺とは？カレンダーの悪用など最新事例と対策を解説
https://time-space.kddi.com/mobile/20210514/3109

不在通知を悪用するスマホのスミッシング詐欺とは？その対策と最新事例を解説
https://time-space.kddi.com/mobile/20210810/3156

コラム　スマートフォン・サイバー攻撃対策ガイド **一般社団法人 日本スマートフォンセキュリティ協会**

SMS認証の悪用、スミッシング(SMS+フィッシング)　https://www.jssec.org/column/20201130.html
マルウェア・bot対策　https://www.jssec.org/column/20210311.html
偽警告・偽契約詐欺対策　https://www.jssec.org/column/20210412.html

スマホマルウェア及びスマホへの攻撃手段

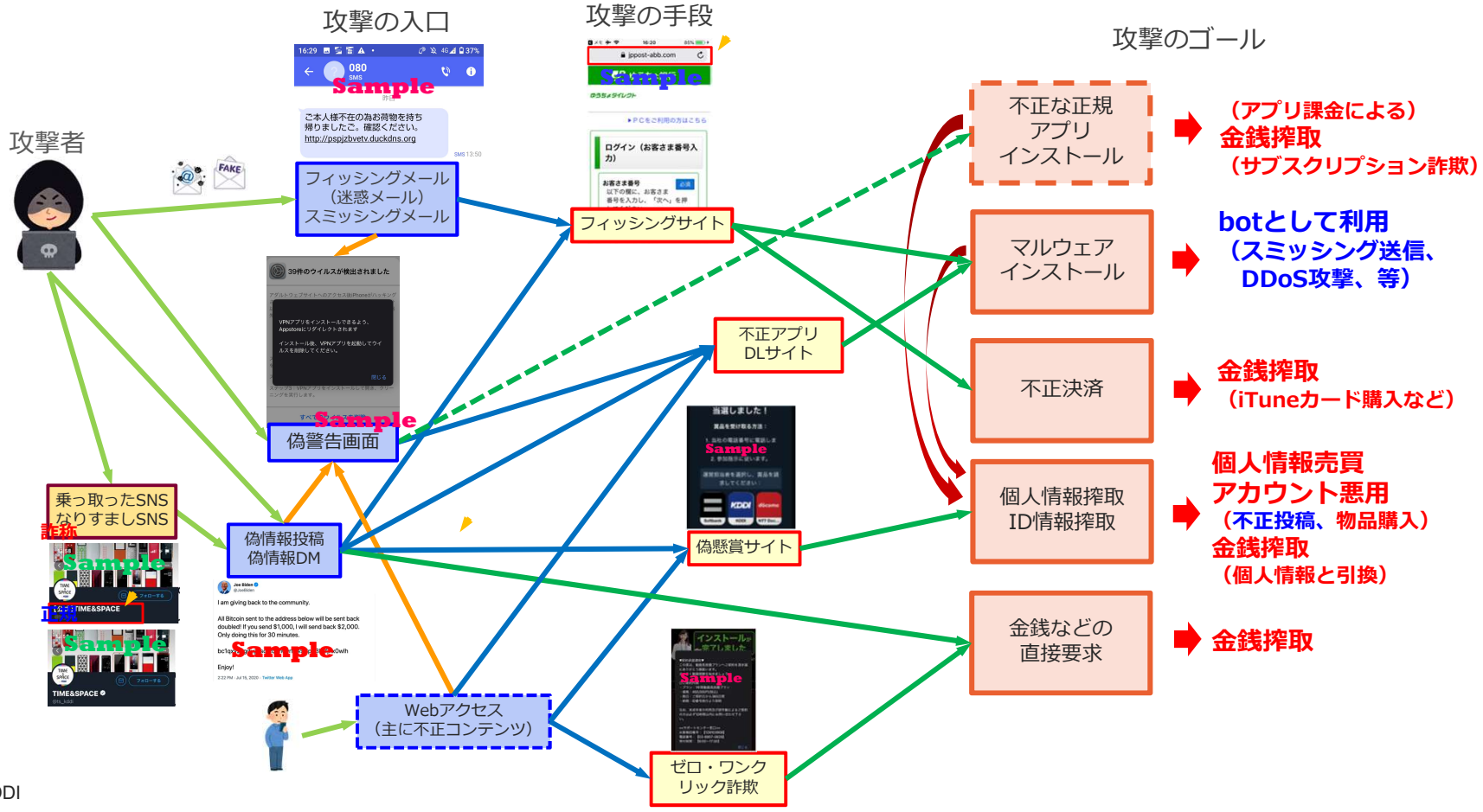
金融系サービスに対する脅威

OSのセキュリティ対策

対策一例

まとめ

主な攻撃の種類と主な攻撃の流れ



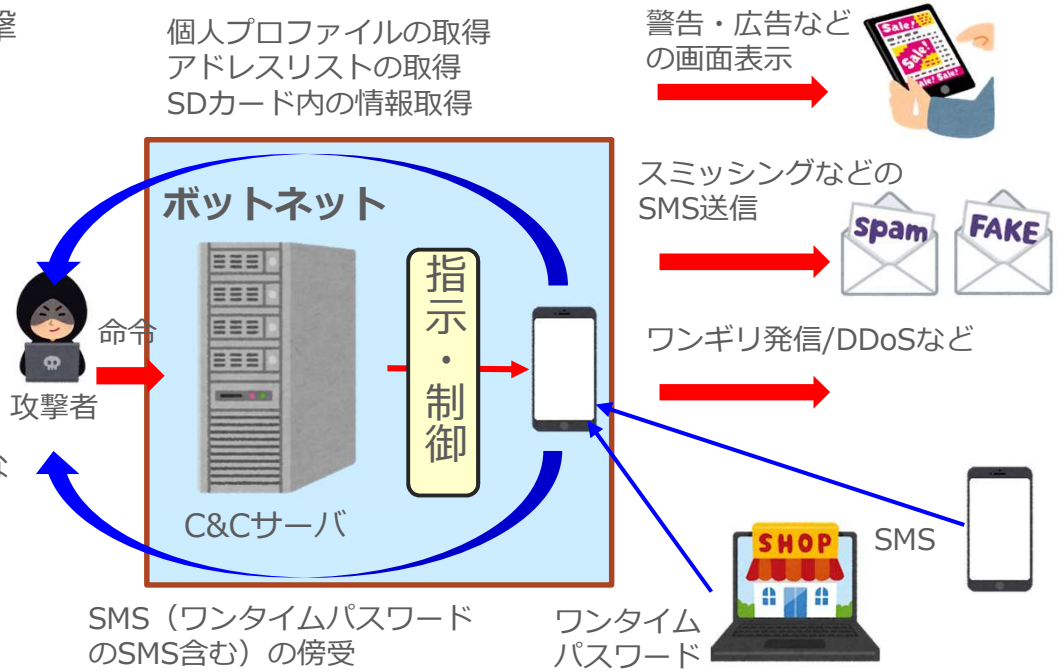
スマホマルウェアとは？

その名の通り、スマホを対象としたマルウェア。スマホは、OS側のセキュリティ対策が施されていることから、PCと比較してマルウェアに感染しにくいが、一方で利用者を巧みにだましてマルウェアに感染させているのが現状である

スマホのマルウェアは主に以下のような攻撃を行うことが一般的である

- 個人情報の搾取(アドレス帳、アカウント情報)
- SMSの送信
- SMSの盗聴（SMS認証のSMS搾取が目的）
- ワンギリ発信
- 位置情報の搾取
- （アフェリエイト収入目的）の広告表示
- DDoS攻撃

SMSや音声に関しては、スマホならではの特徴となる



マルウェア感染まで手順例

スミッシングから偽警告詐欺によるマルウェア感染まで手順例を下記に示します

送信者が電話番号となっていて、配達者がSMS送信しているようにみせかけている

①スミッシングSMS受信

偽警告を出してChromeのアップデートを要求

②Chromeのアップデート要求

Google PlayからのアプリDLではないため、OS機能で警告は表示

③apkフィルのダウンロード

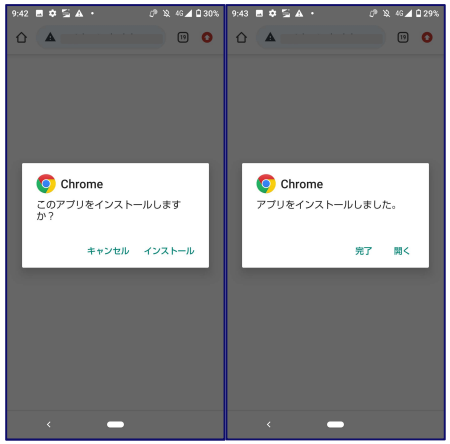
左記と同様にGoogle Playからのアプリではないので、インストール時に、OS機能で警告は表示

④インストール警告

マルウェア感染まで手順例　～　つづき

インストールするために、不明なアプリのインストールを許容する

⑤不明なアプリのインストール許可



⑥マルウェアインストール

インストール後、初回起動時にマルウェアとして活動するためのパーミッションを取得する

- アドレス帳への搾取が可能
- ワンギリ発信等が可能
- ストレージ内のデータ搾取が可能
- (bot)スミッシング送信が可能
  SMSの盗聴が可能

⑦アプリ起動＆
パーミッション取得

この時点でマルウェアに感染
したがって、HPを閲覧しただけでマルウェアに感染するということはない

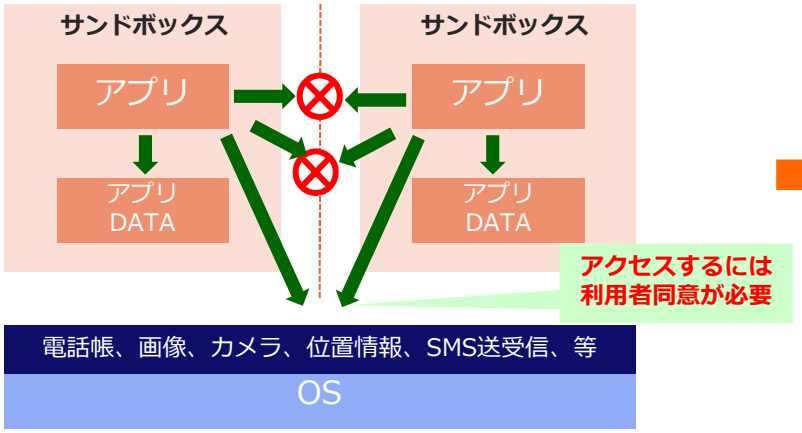
利用者が一覧の操作を実行してしまっていると推測される

マルウェアが完全に機能するのはパーミッションを取得後となる

マルウェアによる権限取得 ー サンドボックス機能の回避

iOS/Androidではサンドボックス機能により、各アプリは閉じた空間で動作し、共通データや共通機能を利用するにも承諾が必要となる

サンドボックス機能



各アプリの実行空間は分離されており、アプリ間の連携が難しい。システム間で共通して利用なデータや機能は利用者同意をする事で利用可能となる

マルウェアであっても、権限取得は必要

マルウェアと気づいていない利用者は、アプリ利用の為と同意してしまい、マルウェア感染となる

スマホマルウェアおよびスマホへの攻撃手段

金融系サービスに対する脅威

OSのセキュリティ対策

対策一例

まとめ

金融系サービスに対する攻撃

スマホのOSは各種セキュリティ対策が施されてとり、サンドボックス機能等によりマルウェアが直接金融系のアプリを乗っとるなどの攻撃を受ける可能性は限りなく低く、想定される攻撃としては以下が考えられる

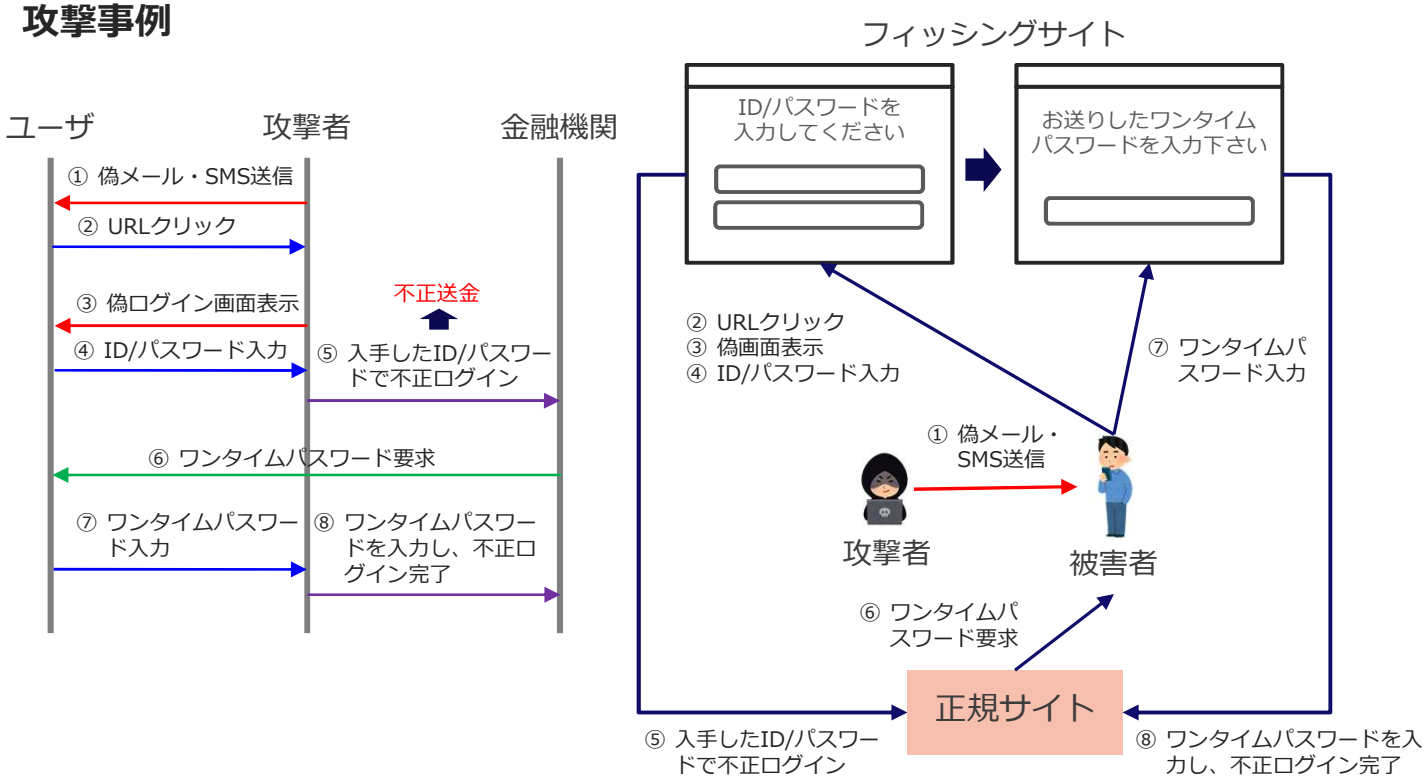
- IDを取得する、クレジットカード情報を取得する
- サービスの脆弱性を突いて攻撃する
- 悪意のある3rd Party SDKによる攻撃

いわゆるアプリの脆弱性をついた攻撃ではなく、**人の脆弱性**や**サービス仕様の脆弱性**をついた攻撃が主流となると推測される

ID情報の取得例（2段階認証の無効化）

フィッシングメール・スミッシングSMSを送信し、フィッシングサイトに誘導し、被害者が入力した情報をバックグランドで正規サイトに情報を送り、攻撃を成立させる

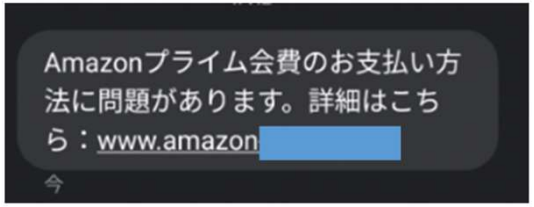
攻撃事例



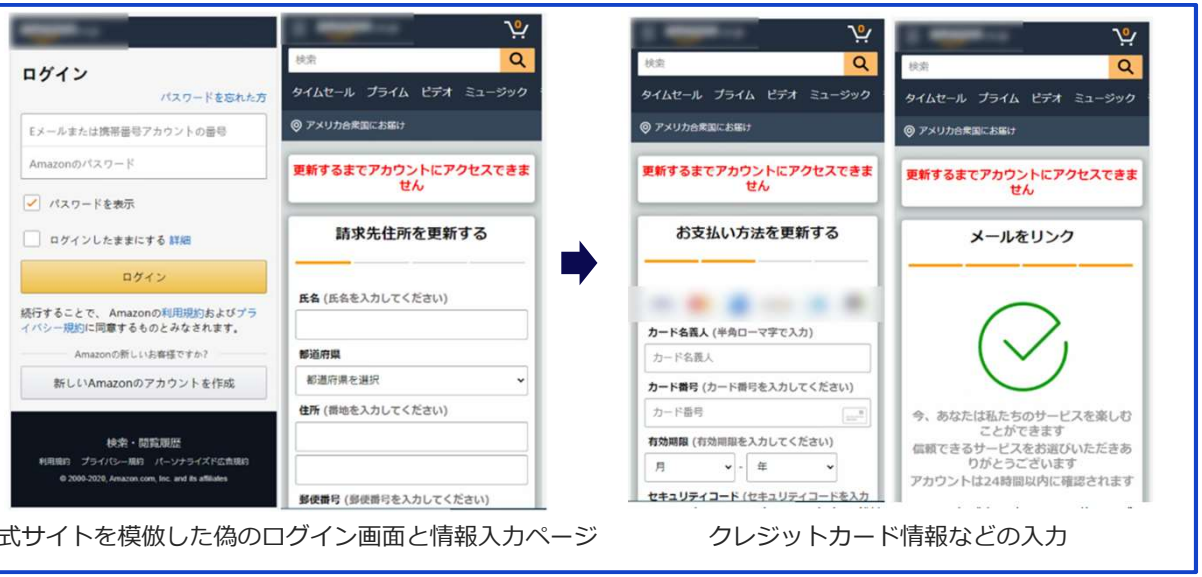
クレジットカード情報取得例

偽SMSでフィッシングサイトに誘導し、クレカ情報を含む個人情報を取得。取得したクレカ情報を悪用し、金品価値のある製品を購入

メールアドレスを攻撃者のアドレスに変更してサービスに登録することで、被害者はカード請求などを見るまで被害にあっていることに気づかない



偽装したSMSを送信



公式サイトを模倣した偽のログイン画面と情報入力ページ　　クレジットカード情報などの入力

正規サイト

一部情報を書換えて悪用
（メールアドレス、住所など）

他サービス

入手した個人情報をもとにサービス登録し悪用

https://is702.jp/news/3804/

サービスの脆弱性を突いた攻撃

サービスのデジタル化に伴い、セキュリティ設計は機密性・完全性・可用性の概念だけでなく、プライバシー・安全性・ユーザ信頼性等の観点の考慮が必要となっている

これらの考慮をおこたる、技術的には問題がなくても、サービス仕様として欠陥を抱えた状態でサービスを提供する可能性がある

攻撃者は、サービスの脆弱性を虎視眈々と狙っており、実際にサービス仕様の脆弱性を突かれた攻撃により社会的問題となった例も存在している

サービス仕様の脆弱性、特にID管理や金融連携に不備があると攻撃の的になる可能性が高くなる

3rd Party SDK での問題事例

もし、3rd Party SDKによる悪意のあるコードが埋め込まれていた場合、該当のSDKを組込んだアプリはデータ等を悪用される可能性がある

百度（Baidu）のアプリに組み込まれていた、百度のSDKが各種個人情報の収集を行ってたことを、Unit 42が発見。結果、Google Playは、アプリの削除を一旦実施

Google Play ストアの**Android**アプリに個人を特定可能なデータの漏えいが発覚 米国で**600**万回のダウンロード実績のある**Baidu**アプリも

By Stefan Achleitner and Chengcheng Xu
11月 24, 2020 at 3:00 午前
Category: Unit 42
Tags: Android, Cybercrime, privacy

Unit 42のリサーチャーは、機械学習（ML）ベースのスパイウェア検出システムの助けを借りて、データを漏えいする複数のAndroidアプリが米国Google Playストアにあることを特定しました。そのなかには、600万回のダウンロード実績をもつBaidu（バイドゥ）のBaidu Search BoxやBaidu Mapsも含まれていました。漏えいしたデータにより、場合によってはユーザーは一生涯、追跡をされてしまう可能性があります。米国のGoogle Playストアで利用可能なAndroidアプリの調査から確認した証拠によれば、Baidu Search BoxとBaidu Mapsのすべてのユーザー（推定14億ユーザー）が影響を受ける可能性があります。こうしたデータがいったん漏えいした場合、どのように攻撃者に使用されうるかについては、以前のUnit42の調査で概説しています。

https://unit42.paloaltonetworks.jp/android-apps-data-leakage/

2020年8月1日の朝日新聞記事で、一部アプリにてWi-Fiの接続状況から位置情報を取得しているが、その旨の記述がないアプリが多数あることが指摘されている

朝日新聞デジタル ＞ 記事

人気アプリが取得する位置情報　業者と共有明らかにせず

有料会員記事
牛尾梓 、渡辺淳基　2020年8月1日 19時13分

スマートフォン で使われる人気アプリの約9割で、利用者の位置情報が業者側に共有されていることが、朝日新聞の調査でわかった。その半分以上は、共有していることを明らかにしていなかった。日常的に持ち歩く スマホ を通じて、個人のデータが自覚のないまま多くの業者に共有されていたことになる。

まず各アプリが、スマホ のどのデータにアクセスする「権限」を与えられているか、その説明を調べた。全地球測位システム（GPS）などの「正確な位置」や、WiFi（ワイファイ）の接続状況などから分かる「おおよその位置」の取得を挙げていたものが41アプリあった。

そこで残りの59アプリについて、アプリをダウンロードして初めて利用した直後に接続された通信先を、専門会社の指導のもとで専用ソフト「Charles（チャールズ）」を使って調べた。位置情報を収集すると表明している外部業者と通信していたアプリは47あった。計88アプリで、何らかの位置情報が把握できていたことになる。

https://www.asahi.com/articles/ASN815TD1N6ZUUPI005.html

スマホマルウェアおよびスマホへの攻撃手段

金融系サービスに対する脅威

OSのセキュリティ対策

対策一例

まとめ

マーケットの対策

Google Play、App Storeともに年々マーケットのポリシーを強化し、不正なアプリが審査を通過しないように取組をおこなっている。また掲載されたアプリのパトロールを強化し、不審なアプリは排除するように努めている

※　ただし、それを掻い潜ってくるケースはある

Google Playのポリシーの一例
マーケット登録時に、ポリシーに違反していないかの審査を行い、問題がある場合は拒否を行う

※ App Storeも同様の取組をおこなっている

セーフブラウジング

安全ではないWebサイトを特定し、ユーザーやWeb管理者にその有害性を知らせる機能。
Webアクセス時に該当のURLの問題有無を確認し、問題がある場合にはブラウザ上に警告を表示し利用者に危険なサイトへのアクセスを抑止させるための機能

警告メッセージ	警告内容
アクセス先のサイトで不正なソフトウェアを検出しました	アクセス先で不正なソフトをインストールさせる可能性がある際に表示
偽のサイトにアクセスしようとしています	フィッシングサイト等、偽サイトにアクセスした際に表示
不審なサイト	（理由は問わず）安全ではないと判断されたサイトにアクセスした際に表示
この先のサイトには有害なプログラムがあります	ユーザーをだまして、問題を引き起こすプログラムをインストールさせようとする可能性がある際に表示
このページは承認されていないソースからのスクリプトを読み込もうとしています	安全と判断出来ないスクリプトを実行している際に表示
もしかして: [サイト名] またはこのサイトは正しいですか？	意図したサイトと異なる紛らわしいサイトの可能性がある際に表示

Chrome警告一覧

Android

iPhone

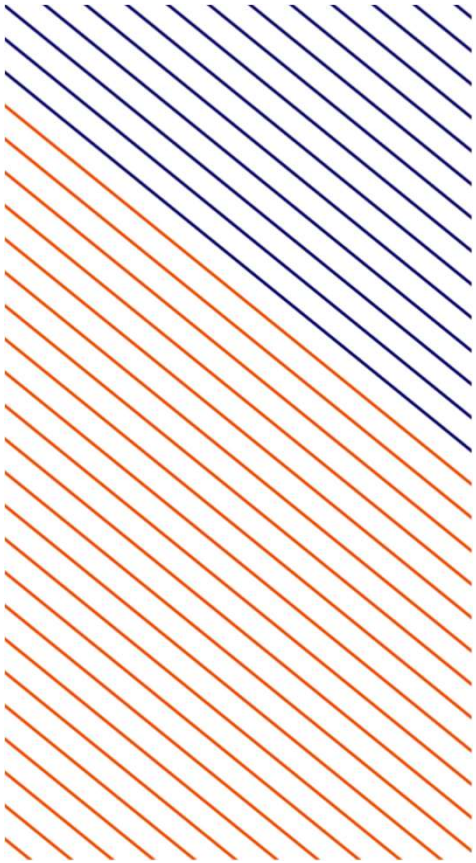
Google Play Protect

2017年7月よりAndroid OSがデフォルトで提供しているセキュリティ機能（Windows 10のMicrosoft Defenderに近い機能）。なお、本機能はデフォルトオンで提供されている

- Google Play プロテクトの仕組み
  ユーザーがアプリをインストールする際に、そのアプリをチェックする。また、デバイスを定期的にスキャンする。有害な可能性のあるアプリが検出された場合は、次のような処理を行う
  - ユーザーに通知を送信する　ー　ユーザーは通知をタップして [**アンインストール**] をタップするとアプリを削除可能
  - アプリがアンインストールされるまで無効にする
  - アプリを自動的に削除する

Google Play ストア以外の不明な提供元からアプリをインストールする場合、[有害なアプリの検出精度を改善] をオンにすると、Google Play プロテクトから不明なアプリが Google に送信され、有害なアプリを回避しやすくなる

https://support.google.com/googleplay/answer/2812853?hl=ja

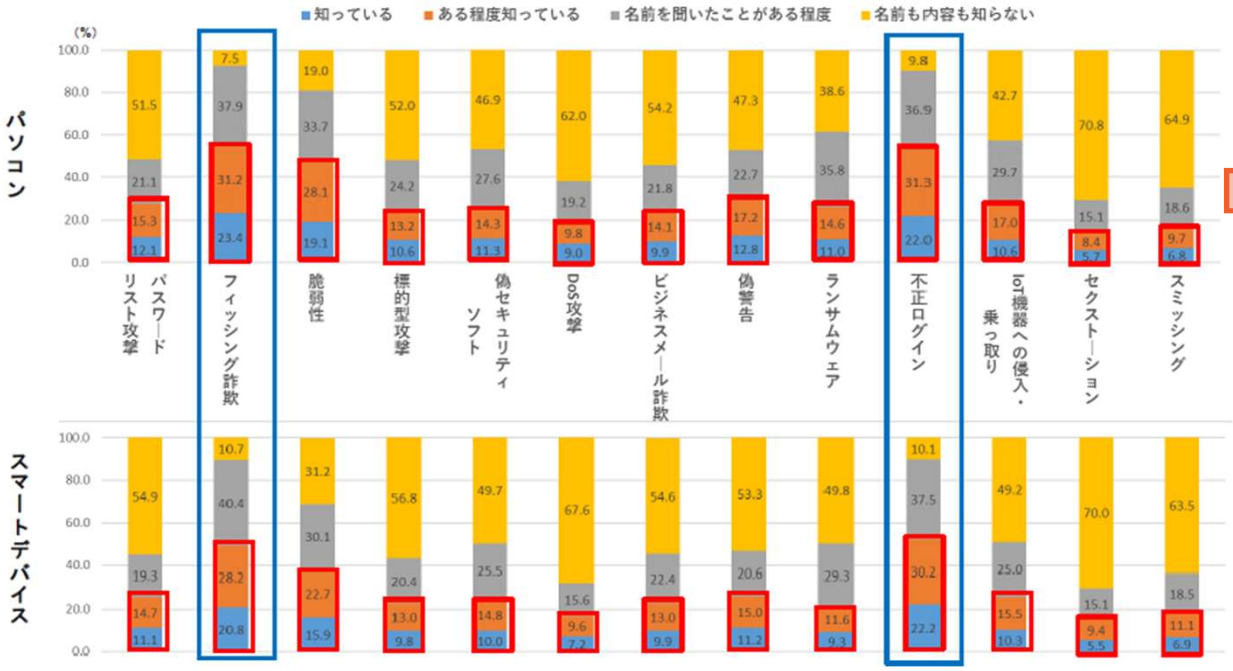


- スマホマルウェアおよびスマホへの攻撃手段
- 金融系サービスに対する脅威
- OSのセキュリティ対策
- **対策一例**
- まとめ

Tomorrow, Together KDDI

利用者への継続的な啓発

IPAが実施した、2020年度情報セキュリティの脅威に対する意識調査の結果では、ある程度認知されている脅威もあるが、全体的には高い認知度とは言い難い結果となっている



攻撃のメインは、“**人の脆弱性**”を突いた攻撃と推測される

各サービス提供者が利用者に、 **わかり易く効果的**、且つ、**継続的に啓発**し続けることが重要

「2020年度情報セキュリティの脅威に対する意識調査」報告書
https://www.ipa.go.jp/files/000088916.pdf

サービスセキュリティ対策の推進

サービスを安全かつ継続的に提供するため、Security / Privacy by Designの考えに則り、企画・開発段階で、リスクを定義し、守るものを定め、リスクの分析を行い、必要な対策を実施することで、**サービス仕様や技術的対策の不備を防ぐ**可能性が高くなる

顧客が利用するデジタルサービス等 において発生するセキュリティインシ デントを対象としにセキュリティ対策を検討するSSIRT（DSIRT)※を構築し、 安全なサービス企画・設計、サービスの悪用/炎上を想定した対応計画の策定、大規模なサービス悪用/炎上発生時の対応を行う組織を構築し、サービスの仕様を含め問題がないか判断をする組織の設置が推奨される

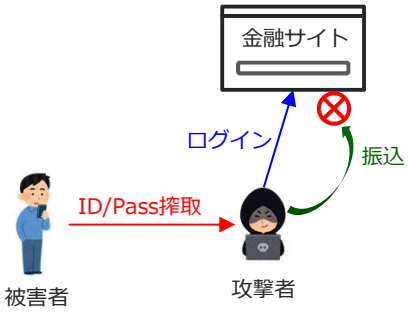
サイバーセキュリティ体制構築・人材確保の手引き
経済産業省 商務情報政策局サイバーセキュリティ課 ／　独立行政法人 情報処理推進機構（ＩＰＡ）
https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf

※　SSIRT（DSIRT）: Service（Digital) Security Incident Response Teamの略

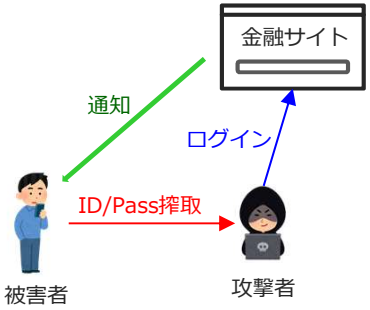
ID等が漏洩する前提でのサービス仕様の策定

フィッシング・スミッシング詐欺、偽警告詐欺など、人の脆弱性をついて攻撃が多く、技術だけで完全に防ぐことは不可能に近い
したがって、考えうるリスクを想定し、ID等が漏洩することを前提に、利用シーンや扱う情報の重要性を踏まえて対策を行うことが重要となる

- 多要素認証・多段階認証の導入
- デバイス制限機能の導入（事前に登録したデバイス以外のアクセス拒否）
- （複数手段での）取引通知機能の提供



ID/Passが搾取されて、サイトには接続可能となるが、振込のような重要手続きは、別の手段での確認を行うことで、被害を最小化する



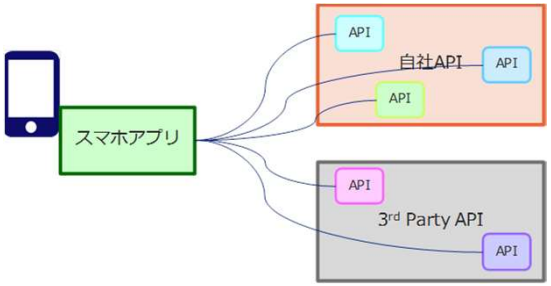
サイトにログイン、取引実施した際に、登録済みのメアドなどに通知メールなどを送信することで利用者が不正な接続に気づかせる

多層防御の採用、さらには利用者が被害を検知出きる仕組みも重要

利用者がID/Passwordを意識しない仕組みも考える必要

アプリが利用するSDKの確認

スマホアプリでは、3rd Party SDKを利用して開発するケースが多い。これらSDKは仕様がブラックボックスなケースもあり、開発者が意図しない動作となる可能性があり、外部的脅威の観点に加え、設定不備等がないかチェックする必要がある



シャドーSDKの確認

予期せぬ宛先に対して、通信が発生していないか？
意識していない（個人）情報を外部に送信していないか？

SDK設定不備の確認

APIの設定（利用方法）が誤っていないか？
（特に、API Ver. UP時に仕様変更されていないか？）

SDKの動作の確認

仕様通りの動作になっているか？
安全な通信（TLS通信）を行っているか？
不要なアクセスを許容していないか？
予期せぬコードが含まれていないか？

信頼できるSDKかの確認

古いバージョン（脆弱性があるバージョン）を利用していないか？
継続してメンテナンス行われている体制になっているか？

セキュアコーディングの実践

悪意のある攻撃者やマルウェア等による攻撃に耐え得る、堅牢なプログラミングとして、セキュアコーディングの実践が推奨されている

日本スマートフォンセキュリティ協会では、Android開発者向けに、セキュアコーディングのノウハウをまとめたセキュアコーディングガイドを公開している

https://www.jssec.org/activities#cn02

さらには、アプリの脆弱な実装を見つけるために、セキュアコーディング診断を行うことが推奨される

スマホマルウェアおよびスマホへの攻撃手段

金融系サービスに対する脅威

OSのセキュリティ対策

対策一例

まとめ

まとめ

マルウェアなどからの攻撃リスク

- スマホ（OSなど)のセキュリティ強化によりマルウェアからアプリが攻撃を受ける可能性は限りなく低い
- 狙いはマルウェアのインストールに加え、ID/Passwordを含む個人情報の搾取が主と推測される

スマホへの攻撃方法

- フィッシング・スミッシング詐欺、偽警告詐欺など、人の脆弱性をついた攻撃が主流である
- サービスの脆弱性を狙われるケースもある
- 信頼できない3rd Party SDKの利用は危険性を含んでいる

安全なスマホ利用環境を目指すには

- 人の脆弱性を突かれるため、利用者へのセキュリティ啓発が何よりも重要
- 企画・開発段階からサービスや設計仕様のリスク評価が必要
- ID情報等が漏洩することを前提とした実装も重要である
- セキュアコーディングやセキュアテストなどによる対策も必要となる


au
UQ
mobile
povo