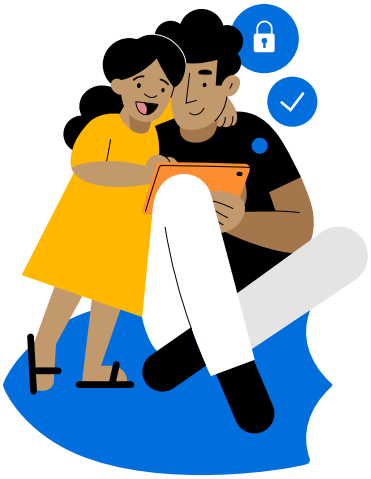


数百万のアプリのために信頼できるエコシステムを築く

App Storeの保護が果たす重要な役割

2021年6月

2007年

「私たちは2つの正反対のことを、同時にしようとしています。先進的でオープンなプラットフォームをデベロッパに提供しながら、iPhoneユーザーをウイルスやマルウェア、プライバシー攻撃などから守ろうとしているのです。これは簡単なことではありません」

Steve Jobs、2007年[1]

2016年

「公式のアプリケーションマーケットプレイスだけを使用するように。ユーザーは（中略）悪質なアプリケーションをインストールするリスクを最小限にするために、第三者提供元から（アプリケーションをダウンロード）するべきではない。正当で信頼できる提供元からのものでない場合には、ユーザーはアプリケーションをサイドローディングするべきではない」

欧州ネットワーク・情報セキュリティ機関（ENISA）、2016年[2]

2017年

「脆弱なアプリからの脅威を軽減するのに有効と認められたベストプラクティスには、悪質でプライバシーを侵害するアプリとの関連性がある。また、ユーザーはアプリのサイドローディングや無認可のアプリストアの使用を避けるべきである（さらに企業は自社デバイス上でのそのような行為を禁止するべきである）」

米国国土安全保障省報告書、2017年[3]

私たちが使う今日の携帯電話は、もはやただの電話機ではありません。私たちの私生活と仕事に関する最も機密性の高い情報を保管しているのです。私たちは携帯電話をどこに行く時も持ち歩きます。大切な人に電話やメッセージをする。子どもの写真を撮影して保存する。道に迷った時に経路を確認する。歩いた歩数を計測する。代金を支払う。あらゆることに携帯電話を使います。幸せな時にも、緊急の時にも、携帯電話は私たちとともにあります。

私たちはそのことを念頭に置いて、iPhoneを設計しました。さらに私たちは、App Storeという場所を作りました。App Storeは、世界中のデベロッパが革新的なアプリを作り、それらを10億人を超えるユーザーが集まり成長と繁栄を続けるグローバルコミュニティに届けることのできる場所です。App Storeにはユーザーがダウンロードできるアプリが約200万用意されており、毎週数千ものアプリが追加されています。そのようなプラットフォームの規模を考えると、iPhoneのセキュリティと安全性の確保は私たちにとって当初から極めて重要なことでした。iPhoneは最も安全なモバイルデバイスであり、ユーザーは極めて機密性の高いデータを安心して委ねられるという点でセキュリティ研究者たちの意見は一致しています。私たちは業界をリードするセキュリティ保護機能をiPhoneに組み込み、App Storeという、ユーザーがアプリを安全に見つけてダウンロードできる信頼のおける場所を構築したのです。App Storeにあるアプリは、Appleのガイドラインに沿うことに同意した既知のデベロッパが提供するものであり、第三者からの干渉を受けることなくユーザーに安全に配信されます。私たちはアプリとアプリのアップデートを一つひとつ審査し、それらがAppleの高い基準を満たしているかを評価しています。私たちが常に改善に努めているこのプロセスは、マルウェア、サイバー犯罪者、詐欺師をApp Storeから排除することでユーザーを守るよう設計されているものです。子ども向けのアプリの場合は、子どもたちを守るために作られたデータ収集とセキュリティに関する厳格なガイドラインに従い、iOSのペアレンタルコントロール機能と強固に統合されていなければなりません。

さらに私たちは、プライバシーは単に重要なだけでなく、基本的な人権であると信じています。この原則は、私たちが自社製品に組み込む高いプライバシー基準の指針となるものです。私たちは、製品やサービスを届けるために確実に必要な個人情報のみを収集し、アプリが機密性の高いデータにアクセスする前にユーザーに許可を求めることでユーザーが自身のデータを自分でコントロールできるようにし、アプリがマイク、カメラ、ユーザーの位置情報など機密性の高い特定の機能にアクセスする時にはそれを明確に通知します。さらに、ユーザーのプライバシーを保護するための継続的な取り組みの一環として、App Storeのプライバシーラベルと、アプリのトラッキングの透明性という2つの最新プライバシー保護機能を導入した結果、透明性がさらに高まったうえに情報にもとづいた選択ができるようになり、ユーザーはかつてないほど自分のプライバシーをコントロールできるようになりました。これらの機能により、ユーザーはApp Store上のどんなアプリも安心してダウンロードできます。また、このような安心感はデベロッパにもメリットをもたらします。自分たちのアプリを不安なくダウンロードしてくれる幅広いユーザーにリーチできるからです。

ご存知ですか？

AppleはApp Storeにあるアプリとアップデートをすべて審査し、ユーザーに害を与える可能性のあるものを阻止しています。その中には、不適切なコンテンツを含むアプリ、ユーザーのプライバシーを侵害するアプリ、既知のマルウェアが潜んだアプリが含まれます。マルウェアとは、悪質あるいは危険な目的のために使われるソフトウェアです。

ある調査では、Androidを搭載するデバイスはiPhoneより15倍も多く悪質なソフトウェアから感染していたことがわかりました。Androidアプリが「ほぼどこからでもダウンロードできる」のに対し、一般的なiPhoneユーザーはApp Storeという1つのソースからしかアプリをダウンロードできないことが主な理由です[4]。

セキュリティとプライバシーに対するこのようなアプローチは、高い効果を上げています。現在、iPhone上でユーザーがマルウェアに遭遇することは極めて稀だと言えます[5]。App Store以外のウェブサイトや第三者アプリストアを通じてアプリをダウンロードする「サイドローディング」というプロセスでデベロッパがアプリを配信できる方法を作るべきだという意見もありますが、サイドローディングを許せば、iOSプラットフォームのセキュリティが損なわれ、第三者アプリストア上のみならずApp Store上でもユーザーを深刻なセキュリティのリスクにさらすことになります。iPhoneのユーザー基盤の大きさと、写真、位置情報、健康や金銭に関する情報などのiPhoneに保存されるデータが持つ機密性の高さから、サイドローディングを許せばプラットフォームへの攻撃に新しい資金が大量に費やされるでしょう。悪意のある活動を行う人たちはそのようなチャンスを利用し、より多くのリソースを注ぎ込んでiOSユーザーを標的にした巧妙な攻撃を開発し、結果として武器化した一連の搾取や攻撃が増加します。そうした攻撃は「脅威モデル」とも呼ばれ、すべてのユーザーはそのような攻撃から保護されなければなりません。マルウェア攻撃のリスクがそのようにして高まれば、App Storeからしかアプリをダウンロードしない人も含め、あらゆるユーザーがより大きな危険にさらされます。さらに、アプリはApp Storeだけからダウンロードしたいと考えるユーザーでも、仕事や学校で必要なアプリがApp Storeで入手できない場合は、第三者アプリストアからダウンロードせざるを得なくなったり、App Storeを装った第三者アプリストアから騙されてアプリをダウンロードしてしまうかもしれません。

アプリが審査を受けることのないAndroid向けの第三者アプリストアは、公式アプリストアに比べてはるかにリスクが多く、マルウェアを含んでいる可能性が高いと言う研究があります[6]。その結果、安全ではないという理由から、セキュリティの専門家は第三者アプリストアを使わないよう消費者に勧告しています[3, 7]。サイドローディングを許可すれば、ユーザーがそのようなリスクを受け入れざるを得ない世界への扉を開くことになります。なぜなら、一部のアプリがApp Storeで入手できなくなったり、詐欺師がユーザーを騙してApp Storeから安全にアプリをダウンロードしていると思い込ませることができるようになるからです。サイドローディングは、アプリを悪用してユーザーを騙し、iPhoneのセキュリティ機能を攻撃し、プライバシーを侵害する詐欺師からの攻撃にユーザーをさらすことになります。また、子どもによるアプリのダウンロードやアプリ内での購入を保護者が管理できるペアレンタルコントロール機能の「承認と購入のリクエスト」や、自分と子どもたちがデバイスを使う時間を管理できる「スクリーンタイム」機能をユーザーが頼りにすることがより難しくなります。詐欺師がアプリの性質をわかりにくくして子どもや保護者を騙す機会を手にすれば、これら2つの機能の効果が低下するからです。

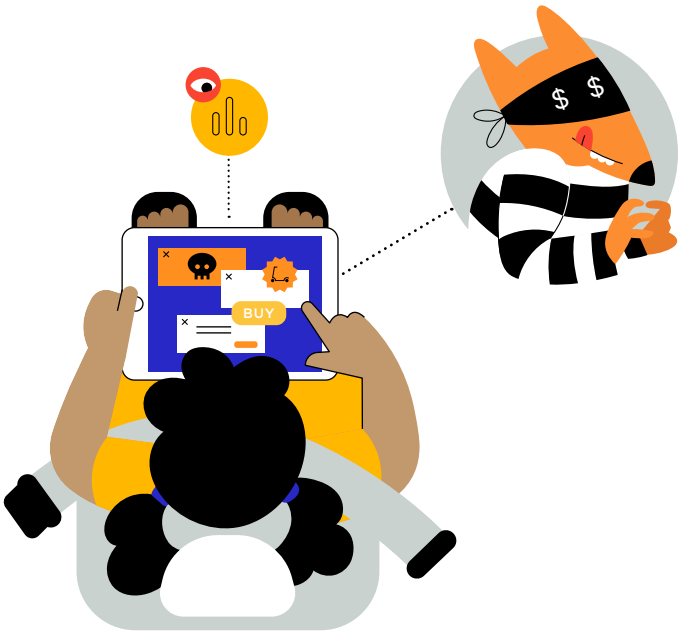
最終的には、ユーザーは誰や何を信頼して良いのか判断ができなくなり、常に詐欺を警戒しなければならなくなります。その結果として多くのユーザーは、より限られたデベロッパからより少ないアプリをダウンロードすることになるでしょう。デベロッパ自身も、マルウェアを含みそれを拡散してしまう感染したデベロッパツールを配布するような悪意のある人たちからの脅威に一段とさらされやすくなります。さらに、著作権侵害の被害も受けやすくなるため、自らの作品に対する報酬を得るデベロッパの能力が弱体化します。

サイドローディングを許可するプラットフォームに対する攻撃の実例

子ども向けAndroidアプリが、子どものプライバシーを侵害するデータ収集を行っていたことが判明しました。これらのアプリはGoogle Playストアから削除されたにも関わらず、第三者アプリストア上ではいまだダウンロードすることができ、Androidユーザーを標的にし続けています[8]。

悪意のある人たちが、子ども向けのアプリ上に不適切な広告やわいせつな広告を掲載しました[9]。

iPhoneを使うある家族の日常が、サイドローディングによってどのように変化するかを見てみましょう。この一段と不確かな世界を生きる、ジョンと7歳の娘エマの一日を追います。



サイドローディングされたゲームがペアレンタルコントロールをすり抜ける

エマは、学校の友だちから聞いたゲームで遊んでもよいかジョンに尋ねます。ジョンはApp Storeを探しますが、デベロッパはそのゲームアプリを第三者アプリストアでのみ入手できるようにしていました。ジョンは不安を感じるものの、エマがどうしてもそのゲームを試したがるのと、そのアプリは子どもに適したものだと第三者アプリストアに記載されていたため、ダウンロードします。その後、公園に向かう車の後部座席でエマがそのゲームで遊んでいると、アプリが外部ウェブサイトへのリンクやターゲティング広告をエマに浴びせかけてきます。ゲームをダウンロードした時に、ジョンはエマにスターターパックを購入するためにクレジットカードの情報を追加しましたが、サイドローディングされたこのアプリでは「承認と購入のリクエスト」のペアレンタルコントロールが機能しないことにジョンは気づきませんでした。父親が購入を承認していないことを知らずに、エマはゲームで遊ぶ間に多くの追加ターンや特別アイテムを購入します。さらにそのアプリは子ども向けにも関わらず、エマのデータを収集、分析し、データブローカーに販売する第三者トラッカーも組み込まれていました。

サイドローディングを許可するプラットフォームに対する攻撃の実例

Androidでサイドローディングされたアプリは「ロッカー」と呼ばれるランサムウェア攻撃を実行することが知られています。これらの悪質なアプリをインストールすると、身代金の支払いに応じない限り、携帯電話がロックされてユーザーがアクセスできなくなったり、写真を標的にされます[10、11]。

Androidユーザーが騙され、Netflixやキャンディークラッシュなどのアプリの偽バージョンを安全でない方法でダウンロードしてしまうという状況も発生しています。これらの偽アプリは、アクセス権を与えられた場合やプラットフォームの脆弱性を悪用した場合、マイクを通じてAndroidユーザーの行動を探ったり、デバイスのスクリーンショットを撮ったり、位置情報やテキストメッセージ、連絡先をのぞき見たり、ユーザーのログイン用認証情報を盗んだり、ユーザーの携帯電話に変更を加えるといったことができます[12、13、14]。さらに、銀行口座の情報を盗んでユーザーの口座を乗っ取るために使われたアプリもあります[15、16、17、18]。

最近のランサムウェア詐欺では、新型コロナウイルス感染症の接触追跡アプリを装ったAndroidアプリの事例がありました。そのアプリをインストールするとあらゆる個人情報が暗号化されてしまい、ユーザーがデータを取り返したい場合に連絡するためのEメールアドレスが表示されるという仕組みです[19]。

第三者アプリストアで見つかった別のアプリは、システムアップデートを装ってユーザーを騙すもので、このアプリをインストールすると「アップデートを検出中」という通知が表示され、その間にアプリがメッセージ、連絡先、写真などの個人情報にアクセスして、それらを盗んでしまいます[20、21]。

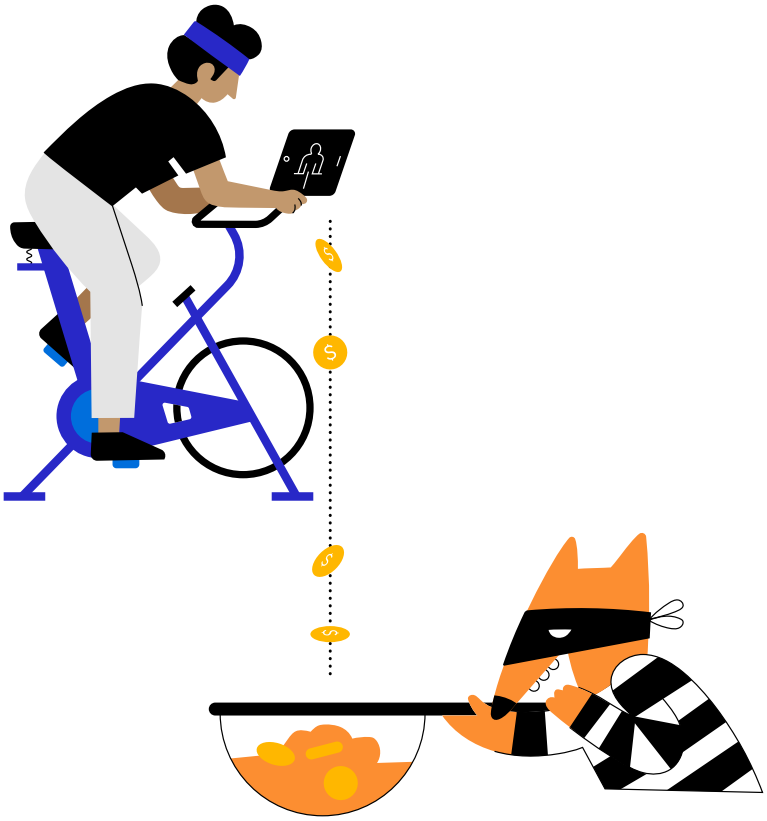
公園では、ジョンがサイドローディングした偽のフィルタアプリが、身代金を支払わない限り彼の写真をすべて削除するとジョンを脅迫

ジョンとエマが公園にいると、ジョンはよく知られたデベロッパが提供するセルフィー用フィルタアプリの広告を目にし、エマと使ったら楽しそうだと考えます。その広告は、App Store上のアプリデベロッパページに似せたアプリダウンロード用のページにジョンを誘導します。そのためジョンは安全だと判断しますが、実際には第三者アプリストアからアプリの模倣版をダウンロードしていることに気づきません。ジョンはそのフィルタアプリが有名で信頼できるデベロッパのものだと考えているので、自分の写真へのアクセスを許可します。しかしアプリが起動すると、ジョンは間違いを犯したことに気づきます。クレジットカード情報を入力して身代金を支払わない限り、カメラロールにあるすべての写真を削除するとアプリが脅してきたのです。iPhoneのデバイス上の保護機能によってジョンはどのアプリが自分の写真にアクセスできるかをコントロールできますが、この場合はサイドローディングしたアプリがセルフィー用フィルタアプリを装い、ジョンを騙して写真へのアクセスを許可させたのです。

サイドローディングを許可するプラットフォームに対する攻撃の実例

第三者アプリストアで配信される海賊版アプリにより、デベロッパが受け取るはずの収益が年間数十億ドルも失われているという研究の結果が出ています[22]。

海賊版やそのほかの違法アプリはAndroid上に蔓延しています。それらには、位置情報を偽装できる「Pokémon GO」アプリの海賊版のように不正行為を可能にするゲームアプリや、プレミアムコンテンツや機能への不正アクセスができるよう改変されたアプリ、違法なギャンブルやアダルトコンテンツを含むアプリなどがあります[23, 24, 25]。

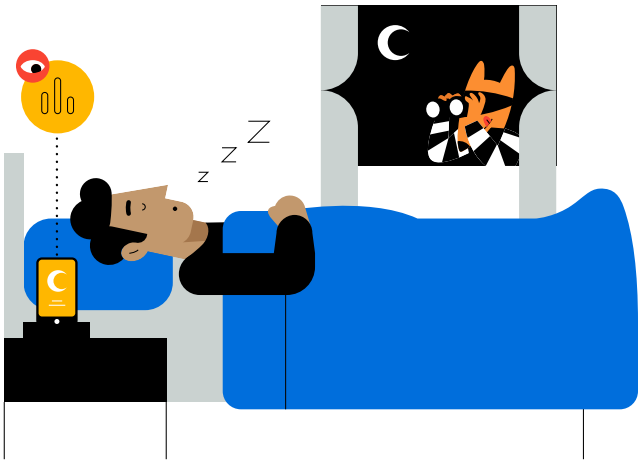


ジョンが第三者アプリストアから海賊版アプリと知らずにダウンロード

ジョンの友だちは、自分が使っているフィットネスアプリをとても気に入っているので、ジョンが試せるように彼をトライアルに招待します。ですがその招待を受けるには、App Storeではなく第三者アプリストアからアプリをダウンロードしなければなりません。ジョンはアプリをダウンロードし、1か月ごとのサブスクリプションに申し込みます。しかしジョンも友だちも、このアプリが海賊版であることに気づきませんでした。毎月ジョンが支払うお金は、アプリを設計、開発したデベロッパではなく、アプリを盗んだ詐欺師に支払われます。素晴らしいフィットネスアプリのデベロッパをサポートし、正しいことをしているとジョンは信じていましたが、実際にはデベロッパの収入を奪う不正行為を知らないうちにサポートし、詐欺師を儲けさせていたのです。

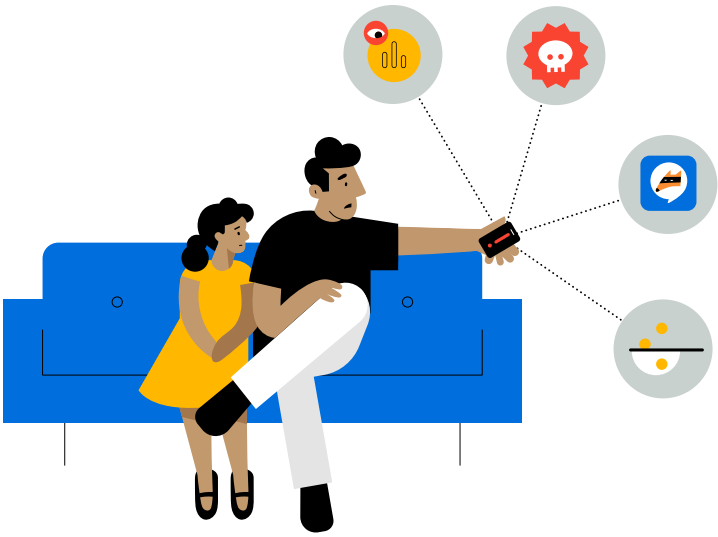
Appleのプライバシー保護についてさらに詳しく

アプリがどのようにデータを収集して使用するかについてのコントロールと透明性をユーザーに提供する「アプリのトラッキングの透明性」機能とApp Storeのプライバシーラベルについて、詳しくは「**あなたのデータの一日**」と **apple.com/jp/privacy/control** をご覧ください。



サイドローディングしたアプリが、ジョンのプライバシーを侵害

ジョンは新しい睡眠記録アプリの評判を聞き、試してみたいと思うのですが、App Storeではそのアプリを入手できません。そのため彼は第三者アプリストアからそのアプリをダウンロードして、自分のEメールアドレスを使って登録し、睡眠の質をチェックするために使い始めます。そのアプリは、ユーザーの健康と使用状況データに関するプライバシーを完全に守り、外部データと連動させたり他社と共有することはしないと主張しています。しかし、この主張は完全に嘘であることが判明します。アプリはサイドローディングされたため、アプリのデベロッパは制限なく何でもできたので、アプリはジョンに許可を求めることなく彼のEメールアドレスを使って彼をトラッキングしていました。このためデベロッパはユーザーの許可なく、阻止される心配もなく、ジョンのデータとそのほかのアプリから集めた情報を連動させ、彼の健康に関するデータをデータブローカーに売却しました。



iPhoneは毎日10億人を超える人たちによって、銀行取引や健康に関するデータの管理、家族の写真を撮る目的で使われています。このように大きなユーザー基盤は、サイバー犯罪者や詐欺師たちにとって魅力的で収益性の高い標的となります。サイドローディングを許可すれば、Macなどのほかのプラットフォームに対する攻撃の規模をはるかに超える大量の資金がiPhoneへの攻撃に新しく費やされ、詐欺師たちによるiPhoneのデバイスセキュリティを攻撃するためのツールとノウハウの開発に拍車がかかるでしょう。App Storeは現在行われている攻撃を検知、ブロックするように作られていますが、脅威モデルが変化すればこのような保護機能はすり抜けられてしまいます。そうなれば詐欺師たちは新たに開発したツールとノウハウを使って第三者ストアやApp Storeを標的にするため、App Storeだけでアプリをダウンロードする人も含めて、すべてのユーザーをより大きな危険にさらすことになります。サイドローディングによって配信のルートが増えることで、悪意のある人たちがシステムの脆弱性を悪用する機会は拡大します。それにより、マルウェアを開発して拡散するさらなる動機を攻撃者に与えることになるのです。

つまり、iPhoneとApp Storeの安全性や保護機能を当然のものと思うようになったジョンのようなユーザーは、誰や何を信頼できるのかまったくわからず、サイバー犯罪者や詐欺師たちが使う変化し続ける巧妙な手口を常に警戒しなければならなくなります。場合によっては、ジョンはApp Storeで入手できないアプリを第三者ストアでダウンロードするリスクを冒さざるを得ないかもしれず、あるいは騙されてダウンロードしてしまうかもしれません。最も深刻なケースでは、Appleのソフトウェアアップデートを偽装したり、ダウンロードのページをApp Storeに似せるなどのなりすましを行うサイドロードされたアプリがiPhoneのデバイス上の保護機能を破壊し、メッセージ、写真、位置情報などの保護されたデータにアクセスしようとするかもしれません。このようなリスクや詐欺を考えると、ジョンはどのアプリをダウンロードするかについて一段と警戒するようになり、最終的にはジョンがダウンロードするアプリの数は少なくなり、数少ない信頼できるデベロッパのアプリだけを使うようになります。そうなると、より小規模の新規デベロッパが革新的な新しいアプリをユーザーに届けることが一段と困難になります。自分のiPhone上のアプリが自分と娘にとって最も安全なオプションであるとわかっている場合に得られる安心を、ジョンが感じることもなくなるでしょう。

ご存知ですか？

セキュリティやプライバシーを心配するユーザーは、ダウンロードするアプリの数がより少なく、デバイスからアプリを削除しやすい傾向にあります[26, 27, 28]。ユーザーが安心してアプリをダウンロードできない安全性の低いエコシステムでは、ユーザーは革新的な新しいアプリや、新規のデベロッパやあまり知られていないデベロッパが作ったアプリを試す機会が少なくなる可能性があります。それによりアプリによる経済成長が鈍化し、ユーザーとデベロッパの両方に悪影響を与えることも考えられます。

Appleが構築している幾重ものセキュリティレイヤーと App Reviewが、ジョンとエマ、そして彼らのデバイスを守ります

iOSユーザーを悪質なアプリから守り、世界最高のプラットフォームセキュリティを提供するために、私たちは複数の保護レイヤーを伴う多方面からのアプローチを採用しています。iOSには独特なセキュリティ上の課題がありますが、それはユーザーが絶え間なくそして頻繁に新しいアプリをデバイスにダウンロードするためであるのと、iOSデバイスは保護者の監視なしで子どもが使えるほど安全性が高い必要があるためです。私たちはMacと比べてより強化されたアプローチをiPhone上でのセキュリティに採用しているということですが、それはユーザー人口の規模、行動、期待値が異なるからです。

- **Mac上と同様に、私たちは自動ソフトウェアを使ってアプリをスキャンし、既知のマルウェアがないかを探します。これにより、マルウェアがApp Storeまでたどり着き、ユーザーに被害を与えることを防ぎます。**
- **さらにアプリのデベロッパは、アプリの概要と機能の説明を提出するように義務付けられています。**提出された情報の正確性はApp Reviewのプロセスにおいて専門家チームによって審査され、アプリをダウンロードするかどうかの判断時にユーザーに提示されます。このプロセスは、マルウェアを人気のアプリと偽ったり、魅力的ではあるが実際には提供されない機能を使えると主張するような、マルウェアを広めるために使われる最も一般的な詐欺に対抗する高い障壁となります。
- アプリの機能が説明通りであり、App Store上のアプリのページの内容が正確であるかを検証することに加えて、**専門家チームはアプリが不必要に機密性の高いデータへのアクセスを求めることがないか手作業で確認したり、子ども向けのアプリがデータ収集と安全性に関する厳格な規則に従っているかを評価します。**
- **アプリがApp Storeに登場した後にAppleのガイドラインに違反していることが判明した場合には、デベロッパと協力して迅速に問題を解決します。**詐欺や悪質な行為を伴う危険なケースでは、アプリはApp Storeから即座に削除され、アプリをダウンロードしたユーザーは、アプリの悪質な行為に関する通知を受け取ることができます。
- **App Storeからダウンロードしたアプリでユーザーがトラブルを抱えた場合には、AppleCareがサポートを提供し、返金も行います。**

App Reviewの目的は、App Store上のアプリが信頼できるものであることを保証し、App Store上のアプリのページに掲載されている情報がアプリの機能とアクセスするデータを正確に説明しているかを確認することです。私たちはツールや手法を継続的にアップデートし、向上させることでこのプロセスを常に改善し続けています。

App Storeを通じてアプリをダウンロードすると、そのアプリがどのように機能し、どのデータにアクセスできるのかをユーザーがコントロールできます。それを可能にするのが「アプリのトラッキングの透明性」と許可の機能です。さらに保護者は「承認と購入のリクエスト」機能で子どもが何を購入するか、スクリーンタイム機能で特定のカテゴリーのアプリを子どもがどれくらいの時間使えるか、どのようなデータを共有できるかを管理することができます。ユーザーはアプリ関連の支払いをすべて一括管理したり、「アプリケーション内での支払い」を通じて購入したサブスクリプションを簡単に確認、キャンセルできます。サイドローディングしたアプリには、このようなコントロールを完全に適用することができません。

また、App Reviewによる保護に加えて、有害なアプリがデバイスにダウンロードされた場合に備え、最後の防衛線となるような設計をAppleデバイスのハードウェアとソフトウェアの両方に適用しています。例えば、App StoreからiPhone上にダウンロードされたアプリは「サンドボックス化」されるので、ユーザーが明確に許可しない限り、ほかのアプリによって保存されたファイルにアクセスしたり、デバイスに変更を加えることはできません。

脅威に対する最高の防衛とは、悪質なアプリのインストールを防ぐ妥協のないApp Reviewや悪質なアプリが及ぼす被害を制限する強固なプラットフォームの保護など、あらゆるレイヤーの組み合わせを基盤とするものです。iOSに組み込まれたセキュリティは、消費者向けデバイスの中で最も優れたパワフルな保護機能をユーザーに提供しますが、それらはユーザーが騙されて選んでしまう選択肢から守るようには作られていません。ユーザーに害を与えようとするアプリや、機密性の高いデータにアクセスを許可するように騙そうとするアプリからユーザーを守るために作られたApp Storeのポリシーを強化するのがApp Reviewです。非常に深刻なケースとしてデバイス上の保護機能をすり抜けようとする悪質なアプリが挙げられますが、そのようなアプリがユーザーのデバイス上にたどり着くのをApp Reviewが最初から一段と困難にします。

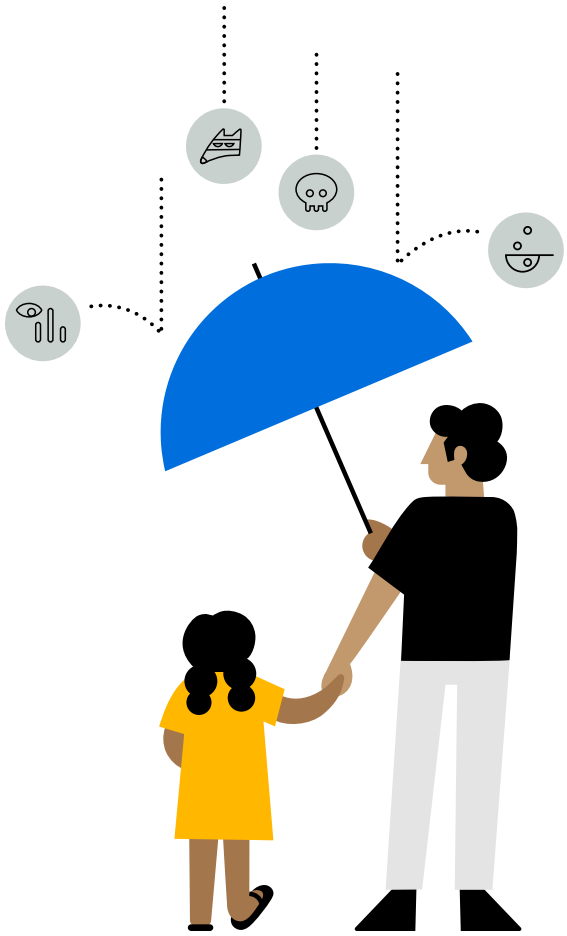
結果として、iPhoneは最も安全なモバイルデバイスであるという点でセキュリティの専門家たちの意見は一致しています。Appleの何層ものセキュリティレイヤーは、比類のないレベルでユーザーを悪質なソフトウェアから守り、安心をもたらします。

App Review（アプリケーションの評価）

App Reviewのプロセスを通じて、アプリが入念にチェックされた提供元からのものであり、既知の悪質な要素を含んでいないことを確認しています。さらに、アプリがユーザーに望まない購入をさせたり、個人情報へのアクセス権を与えるようユーザーを騙すことがないよう確認します。また、デベロッパとユーザーをスクリーニングし、問題行動を起こす人たちを追放する措置を取っています。App Reviewのプロセスで質の低いアプリの配信をすべて防ぐことはできません。ですが、私たちはテクノロジー、慣行、プロセスを革新、改善し続けます。

2020年にAppleが実践したアプリ保護

- **平均で毎週10万の新しいアプリとアップデート**が、様々な言語でアプリをチェックする500人を超える専任の専門家チームによって審査されました。
- **約100万の新しいアプリと同等数のアップデートに問題があり、却下または削除されました。**
  - 15万以上が、スパムや模倣あるいはユーザーに誤解を与えるため
  - 21万5,000以上が、プライバシーガイドラインを違反しているため
  - 4万8,000以上が、隠れた機能や記載されていない機能を含むため
  - 約9万5,000が、詐欺に関する違反が理由で、大部分が犯罪行為、あるいは禁止されているほかの行為のための「おとり」機能を含むため
- **Appleは、15億ドルを超える不正な可能性のある取引を防ぎました。**
- **Appleは不正関連の理由で、Apple Developer Programから47万のチームを除外しました。**不正にまつわる懸念を理由に、約20万5,000のデベロッパによる登録申請を却下しました。
- **Appleは、偽のレビューを含む不正行為や侮辱行為を理由に2億4,400万のカスタマーアカウントを停止しました。**不正あるいは侮辱的な行動パターンを理由に、4億2,400万のアカウント登録申請を却下しました。



App Reviewは、アプリをダウンロードするジョンに安心をもたらします

App Storeのセキュリティとプライバシー保護機能のおかげで、ジョンは安心して自分や娘のためにアプリをダウンロードできます。それは彼が、AppleがApp Store上のすべてのアプリをスクリーニングして既知のマルウェアをチェックしていること、ほかのデバイスに比べ、iPhone上で悪質なソフトウェアにユーザーが遭遇するのは極めて稀であることを知っているからです。

Appleが提供する保護機能についてさらに詳しく

AppleがApp Storeであなたのセキュリティとプライバシーをどのように保護しているかについては、**apple.com/jp/app-store** をご覧ください。

Appleがあなたの位置情報をどのように保護しているかについては、**位置情報サービスのホワイトペーパー（英語）** をご覧ください。

iOSのペアレンタルコントロールについては、**apple.com/jp/families** をご覧ください。

よくある質問

サイドローディングとは何ですか？

「サイドローディング」とは、ウェブサイトや第三者アプリストアなど、公式のApp Store以外の場所からモバイルデバイスにアプリをダウンロード、インストールするプロセスです。ユーザーのセキュリティとプライバシーを保護するために、私たちは一般的なユーザーがサイドローディングをはじめからできないようにiPhoneを設計しました。

脅威モデルとは何ですか？

脅威モデルとは、一連の攻撃や脆弱性を指し、ユーザーはそれらから保護される必要があります。デバイス、ユーザー、環境によって異なる脅威モデルが存在するため、それを考慮したセキュリティを構築する必要があります。App Storeは、iPhoneの脅威モデルから守るために欠かせない要素の1つです。ユーザーがアプリを安全にダウンロードできる信頼のおける場所がApp Storeです。App Storeにあるアプリは、Appleのガイドラインを遵守しなければならない既知のデベロッパから提供され、Appleによって評価されたものです。

ウェブサイトや第三者アプリストアからiPhone上にアプリのサイドローディングを許可することは、App Storeだけからアプリをダウンロードするユーザーにも危険を及ぼしますか？

はい。さらなる配信ルートを提供し、脅威モデルを変更し、潜在的攻撃を拡大することによって、iPhone上でのサイドローディングは、App Storeを通じてのみアプリをダウンロードすることによって自らを守ろうという慎重な取り組みをする人たちを含め、すべてのユーザーを危険にさらします。サイドローディングを許可することは、iPhoneへの攻撃に対する新たな資金を大量に呼び込み、悪意ある人たちに対し、これまでにない規模でiPhoneのデバイスセキュリティを攻撃するためのツールやノウハウを開発することを奨励します。ますます高度化する攻撃のノウハウを開発した悪意ある人たちは、それを使って第三者アプリストアとApp Storeを標的にし、あらゆるユーザーをさらに大きな危険にさらします。さらに、App Storeだけからアプリをダウンロードしたいユーザーさえも、仕事や学校で必要なアプリがApp Storeで手に入らない場合には、第三者アプリストアでダウンロードすることを強いられる可能性があります。もしくは、App Storeを装った第三者アプリストアから騙されてアプリをダウンロードしてしまう可能性もあります。

AppleのApp Reviewプロセスとは何ですか？

私たちは高度なテクノロジーと専門家の知識を組み合わせて、あらゆるアプリとアップデートを慎重に審査し、プライバシー、セキュリティ、安全性に関するApp Storeの厳格なガイドラインを遵守しているかを評価します。プライバシー侵害や厳格なガイドラインを遵守しない子ども向けアプリなど、特定の問題を検知するのに自動審査だけでは十分でない場合に私たちが頼るのが、専門家の知識です。新たな脅威や課題に対応するためにガイドラインは時とともに変化しており、ユーザーを守り、App Store上で最高の体験をユーザーに提供することを目標としています。平均で毎週10万の新しいアプリとアップデートが、世界中の500人を超える専任の専門家チームによって審査されています。

何が審査されるのですか？

App Storeに提出されるアプリとアップデートすべてが、App Reviewプロセスの審査対象です。

Apple製デバイス上では、どのようなペアレンタルコントロール機能を利用できますか？

私たちは、子どもがどのようにデバイスを使うかを保護者が管理できる機能を設計しています。スクリーンタイムは、子どもがアプリを使ったりウェブサイトを見ている時間や、デバイスの利用時間について、保護者がより良く理解できるようにします。子どもが特定のカテゴリーのアプリやウェブサイト上で過ごす一日当たりの時間の長さを、保護者が設定することもできます。さらに、「承認と購入のリクエスト」機能を使うと、子どもによるアプリの購入やダウンロードを保護者のデバイス上で承認または却下することができます。「承認と購入のリクエスト」機能には、連続した購入を防ぐための15分間のタイムアウト機能も備わっています。

「アプリのトラッキングの透明性」機能とApp Storeのプライバシーラベルとは何ですか？

これらの新機能を使うと、ユーザーは自分のデータやプライバシーを自分で一段とコントロールできるようになります。「アプリのトラッキングの透明性」機能は、アプリが他社の所有するアプリやウェブサイトを横断してユーザーの行動を追跡する場合、事前にユーザーの許可を得ることを義務付けるものです。App Storeのプライバシーラベルは、プライバシーに関するデベロッパの方針概要をわかりやすく表示することをApp Store上のすべてのアプリに義務付け、アプリがユーザーのデータをどう使うかについての重要な情報を提供します。

Sources

1. Jobs, Steve, "Third Party Applications on the iPhone," October 17, 2007, accessed via tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, "Vulnerabilities - Separating Reality from Hype," *European Union Agency for Cybersecurity*, August 24, 2016.

3. Griffin, Robert Jr., "Study on Mobile Device Security," *U.S. Department of Homeland Security*, April 2017.

4. Nokia, "Threat Intelligence Report 2020," *Nokia*, 2020.

5. Johnson, Dave, "Can iPhones get viruses? Here's what you need to know," *Business Insider*, March 4, 2019.

6. Symantec, "Internet Security Threat Report, Volume 23," April 2018.

7. Golovin, Igor, "Malware in Minecraft mods: story continues," *Kaspersky*, June 9, 2021.

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations," *Tech Crunch*, October 23, 2020.

9. Henry, Josh, "Malicious Apps: For Play or Prey?" *United States Cybersecurity Magazine*, 2021.

10. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it," *Avira*, August 13, 2020.

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices," *ThreatPost*, June 24, 2020.

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, March 18, 2021.

13. Desai, Shivang, "SpyNote RAT posing as Netflix app," *Zscaler*, January 23, 2017.

14. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove," *The Washington Post*, November 6, 2015.

15. Palmer, Danny, "This Android trojan malware is using fake apps to infect smartphones, steal bank details," *ZDNet*, June 1, 2021.

16. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," *ThreatPost*, April 21, 2020.

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on," *WeLiveSecurity* by ESET, December 11, 2018.

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," *Cybereason*, July 1, 2020.

19. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, June 24, 2020.

20. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'," *Zimperium*, March 26, 2021.

21. Aamir, Humza, "Beware of this newly discovered Android spyware that pretends to be a system update," *TechSpot*, March 29, 2021.

22. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy," *Forbes*, February 2, 2018.

23. Koetsier, John, "App Developers Losing $3-4 Billion Annually Thanks To 14 Billion Pirated Apps," *Forbes*, July 24, 2017.

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit," *TorrentFreak*, January 8, 2021.

25. Campaign for a Commercial-Free Childhood, "Apps which Google rates as safe for kids violate their privacy and expose them to other harms," December 12, 2019.

26. J.P. Morgan, "2020 E-commerce Payments Trends Report: Japan," *J.P. Morgan*, 2020.

27. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019," 2019.

28. Gikas, Mike, "How to Protect Your Privacy on Your Smartphone," *Consumer Reports*, February 1, 2017.