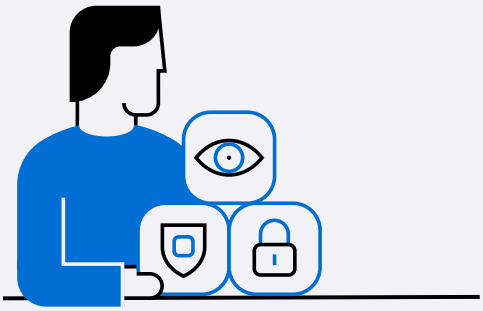


デジタル市場法（DMA）の遵守

欧州連合（EU）におけるユーザーのセキュリティと
プライバシーの保護に対する Apple の取り組み

2024 年 3 月

目次

Apple の目標はユーザーの保護

Apple が最も大切にしていることは、世界中のユーザーの生活を豊かにする優れた製品を作ることです。Apple では、私たち自身が使いたいと思う製品や、家族や親友に私たちと同じくらい気に入ってもらえる製品を作っています。 私たちは、 ハードウェア、 ソフトウェア、 サービスのシームレスな連係を通じて、 ユーザーに高品質で安全な体験を提供することに常に注力しています。 そして、 お客様が Apple と iPhone を選ぶ大きな理由は、 Apple がこのビジョンを実現していると、 お客様が信じているからだと理解しています[1]。

Apple が 2007 年に iPhone を発表した時、 モバイルコンピューティングの時代が到来しました。また、 これは、 人々の日々の生活になくてはならないものとなっているサードパーティデベロッパによる 200 万近いアプリを含め、 新しい製品を生み出すインスピレーションにもなりました。 こうして生み出されたまったく新しいアプリ経済は、 数百万人の雇用を支え、 世界全体で数兆ユーロの商取引を促進しています[2]。

残念なのは、 私たちが住む世界ではセキュリティとプライバシーに対する攻撃がますます巧妙なものに進化しており、あらゆる人の脅威となっていることです。悪意のある行為者は、データを改変したり、身代金目的のランサムウェアを作ったり、 ウェブ全体に情報を漏洩したりする悪意のあるアプリを作ります。 また、 不正行為や詐欺に関わっていたり、 相手が知らない間に情報を盗み見したり、 デバイスそのものを機能不全に陥れたりします。 偽のウェブサイトを作って機密データを提供するように欺したり、 危険なソフトウェアをダウンロードさせたり、 ユーザーのブラウザを攻撃したりもします。フィッシングメールを送信してパスワードを教えるように説得を試みることもあります。 また、サイバー犯罪者は、 Bluetooth アクセサリやオープンネットワーク接続を使って、 あるいは物理的にデバイスにアクセスして、ユーザーの同意なしに、知らない間にデバイスにアクセスして情報を盗もうとします。そのほかにも、 デバイスが送受信する情報やメッセージをデジタル回線上でハッキングして盗み見ようとします。 こうした悪意のある行為者は、 住む場所に関係なく、 すべての人の脅威となっており、これからも脅威であり続けます。

私たちは、個人情報を安全に保つという最終的な目標に向け、最大限のセキュリティと透明性のあるユーザー体験を提供できるよう設計されたハードウェア、ソフトウェア、およびサービスを一体化させ、このようなリスクからユーザーを保護するべく iPhone を作りました。これが、サードパーティアプリが iPhone 上で驚異的な成功を収めることができた大きな理由の一つです。先述したような、既知の、今後も存在し続けるリスクがある中で、ユーザーは、ユーザーを守るための Apple の取り組みを信頼しています。**Apple が最も重視している基準をいくつか紹介します。**

セキュリティ

ユーザーは、iPhone を信頼して最も機密性の高いデータを保存しています。Apple は業界をリードするセキュリティ保護対策を作り上げ、ユーザー以外の人が iPhone 上のデータにアクセスできないようにしています。また、マルウェアやサイバー犯罪、詐欺の心配なく、ソフトウェアを安全にダウンロードしたり発見したりできる信頼できる場所があることが、ユーザーにとって重要だと考えています。

プライバシー

Apple では、プライバシーを基本的人権と考えており、革新的なテクノロジーや技術を利用して、ユーザーのプライバシーを保護する製品とサービスを設計しています。ユーザーは、十分な情報にもとづく許可なしで、自分の情報を収集、利用、共有するソフトウェアやウェブサイトにさらされるべきではありません。私たちは、ユーザーが自分のデータをコントロールでき、許可のない情報の収集、利用、共有からユーザーを守る製品とサービスを作っています。また、どのデータが共有され、どのように使われているのかをユーザーが把握し、コントロールできるようにしています。

安全

ユーザーは、危害を助長したり、実際に危害を加えたりするアプリを含め、iOS を通して物理的な危害にさらされるべきではありません。

これらは、Apple にとって、また iPhone ユーザーが Apple に期待することや、プラットフォームの完全性にとって、最も基本的な理念です。

Apple は、世界中の 175 以上の国や地域のユーザーが iPhone を愛用していることに感謝しており、こうしたいずれの国や地域において、これらの中核となる理念を守っていくことに全力を尽くします。これは、Apple が事業を行うすべての国の法律を守りながら、ユーザーのセキュリティ、プライバシー、安全を守り、維持する方法を見つけていくことを意味します。

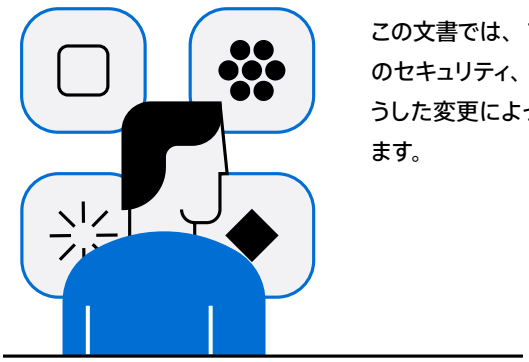
今年から、欧州連合（EU）の新しいデジタル市場法（DMA）により、EU のユーザーにサービスを提供する上で新しいアプローチを採用することが必要となりました。

DMA を遵守するために、Apple はデベロッパとユーザーに新しい選択肢を用意し、**これらの変更を可能にする 600 以上の新しい API とデベロッパツール**を開発しました。この新しい選択肢には、**サイドローディング**を可能にし、EU のユーザーが App Store 以外のアプリマーケットプレイスでアプリをダウンロードできるようするサイドローディングの有効化や、App Store で**代替決済手段**を利用できるようにすること、および**その他の様々な変更**が含まれます[3]。このために、私たちは、ユーザーのセキュリティとプライバシーを保護し、ユーザーの安全を確保するために Apple が採用し、成功を収めてきた独自のアプローチを変更する必要がありました。

2007 年の iPhone 発売以来、Apple は同じアプローチを採用し、無数の脅威に対する幅広い、業界をリードする保護機能を取り入れて、世界中のユーザーを保護してきました。特に App Store では、2008 年に運用を開始して以来、私たちはユーザーが安全にアプリを発見できる信頼性の高い場所、そしてデベロッパがアプリを開発・テストし、世界中のユーザーに配布できる安全でサポート体制の整った方法を作り出すことを目指してきました。そして、長年の間、40 以上のソフトウェア開発キット（SDK）、25,000 以上のアプリケーションプログラミングインターフェイス（API）、およびその他多数の高度なツールを提供することで、デベロッパをさらに支援してきました。

iPhone 上のすべてのアプリを、唯一の信頼できる提供元である App Store で配布することを必須にすることで、ユーザーの保護という Apple の目標をほかのどのプラットフォームよりも効果的に実現してきました。ユーザーとデベロッパを同様に保護するという Apple の取り組みは完璧ではありませんが、iOS では、ユーザーに対する商用マルウェアによる広範囲な攻撃を許したことは一度もありません。これは 17 年間も続いている現代のコンピューティングプラットフォームでは希有なことです。

DMA を遵守するために新しい選択肢を導入するということは、必然的にこれまでと同じようにはユーザーを保護できなくなることを意味します。Apple に対するユーザーの期待に沿いながら、最もセキュリティが強固で、最もプライバシーが保護された、最も安全なプラットフォームを提供し続けるために、Apple はユーザーを守り、ユーザーに十分な情報を提供するための新しいセーフガード措置を設計し、導入しました。DMA の要件に応じた変更により、EU 域外の Apple ユーザーが頼りにできる保護機能と、EU 域内の Apple ユーザーが今後利用できる保護機能の間に格差が生じることは避けられませんが、こうした変更で生じるリスクを完全になくすことはできないにしても、低減することで、私たちは iPhone が EU で利用できる最も安全な携帯電話端末であり続けることができるように努力を重ねていきます。



この文書では、アプリの流通と決済に関して DMA で要求される変更に対応するために、ユーザーのセキュリティ、プライバシー、安全という 3 つの分野で実施する重要なステップに焦点を当て、こうした変更によって EU のデベロッパとユーザーに対して何を実現しようとしているかについて説明します。

アプリの流通と代替決済手段に関する Apple のセーフガード措置は、ユーザーのセキュリティとプライバシーを保護し、ユーザーの安全を確保することを目的としている

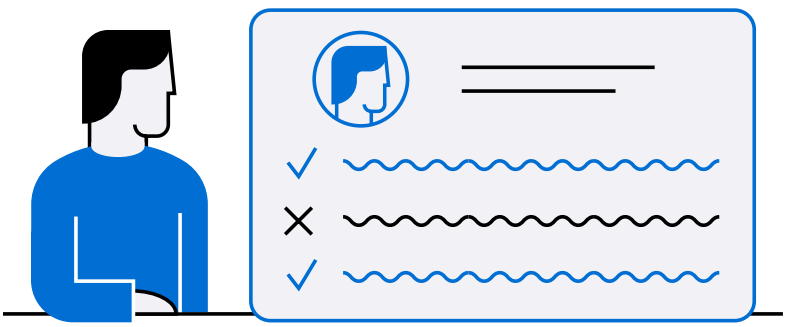
Apple は、EU の App Store でサイドローディング（アプリ代替流通経路）と代替決済手段を可能にしながら、ユーザーのセキュリティ、プライバシー、安全をサポートする数々の機能の導入と拡張を進めています。 Apple は、EU 域外のユーザーと同じセキュリティ、プライバシー保護、安全性は確保できないとしても、EU 域内のユーザーに、最も優れた、可能な限り最も安全な体験を提供し続けるために、セーフガード措置を開発し、実装しました。

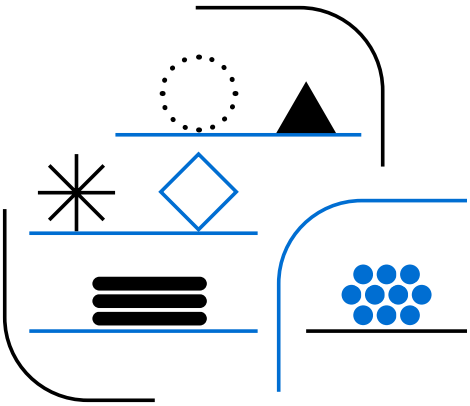
悪意のあるアプリの特定とブロック

Apple は、DMA によって生み出された新しい状況下に置かれている EU 域内のユーザーを保護するため、**iOS 向けの公証を開始します。公証は（App Store で配布されるか代替アプリマーケットプレイスで配布されるかに関わらず）すべてのアプリに適用される基本的審査で、新しいアプリ配布環境を反映し、プラットフォームの完全性とユーザーの保護に重点を置いています。**

Apple は、アプリの配布方法に関係なく、EU 域内で配布されるすべての iOS アプリに電子署名を施します。この署名は iOS 上のすべてのアプリで必要となるものです。アプリに署名を施す前に、Apple は各アプリを（**自動ツール**と**人による審査**の組み合わせによって）分析し、既知のマルウェアやその他のセキュリティ上の脅威が存在しないこと、広告されている通りに機能すること、ユーザーが悪質な不正行為にさらされることがないことをチェックします。こうしたチェックを初期段階で実行することで、サイバー攻撃などの脅威がほかのユーザーに広がる**前**に防ぐことができます。このプロセスは macOS で実施されている公証を拡張したもので、Apple は何年もの間、macOS 上で配布されるソフトウェアに既知のマルウェアが含まれていないことを確認するためにスキャンを行い、署名を施してきました。この仕組みはうまく機能してきました。そのため、これを iOS でも採用し、世界で最も信頼されているモバイルコンピューティングプラットフォーム特有のニーズを満たすための新しい機能を含め、これを iOS に採用しました。

とはいえ、以下で論じるように、アプリのコンテンツ、ビジネス慣行、App Store のその他のユーザー保護機能など、公証だけではすべてに対応できないことは確かです。





保護対策は、アプリのデベロッパが EU 域内で iOS アプリを配布するために行う必要のある最初のステップから組み込まれています。

アプリの開発

デベロッパは、iPhone 上でのアプリの配布方法に関係なく、iOS アプリを開発する前に Apple Developer Program に登録する必要があります（これは EU でもほかの地域でも同じです）。Apple は、登録プロセスの一環として、デベロッパに正式名称、電話番号、住所（組織の場合はその他の ID も）の提示を求めて本人確認を行います。場合によっては、デベロッパは政府発行の ID 番号の提示を求められたり、本人であることの証明を求められたりすることもあります。この最初のセーフガード措置は重要な不正防止策で、デベロッパの本人確認を行い、配布するものに対する責任を取ることが求められます。Apple は 2022 年に、不正行為が疑われたという理由で、10 万 5 千近くの不正なデベロッパアカウントの作成を阻止しました[4]。

デベロッパがプログラムに登録すると、**Apple Developer Program 使用許諾契約に同意したことになります**。これにより、Apple は Apple 製デバイスにアプリを配布するためにデベロッパが従う必要のある基本ルールを定めることが可能になっています。デベロッパは、不正行為に従事しないこと、適用される法令に準拠すること、および迷惑行為、不正利用、スパミング、ストーカー行為、脅迫、または他者の法的権利を侵害する行為を目的としてアプリの設計またはマーケティングを行わないことに同意する必要があります。デベロッパが契約に違反した場合、Apple は契約を解除することができ、実際に解除します。2022 年に、Apple は不正行為のために 40 万以上のデベロッパアカウントを停止しました[5]。

提出

それに加えて、Apple はアプリ提出前の開発段階で発生する可能性のある特定のリスクから守るための**デベロッパ向けツール**を提供しています。たとえば、SDK パッケージの署名機能を実装して、デベロッパがサードパーティコードのソースを検証できるようにしました。これにより、アプリを構築中に悪意ある改変の行われたコードを意図せず使ってしまうことからデベロッパを守ることに役立っています。

公証は、デベロッパがアプリのバイナリを Apple に送信した時から始まります。この時に、デベロッパは（希望する場合には）App Store を含め、どのアプリマーケットプレイスでアプリを配布する予定かを申告します。

審査

公証中に、Apple は**自動審査**と**人による審査**の両方を実施し、ユーザーのセキュリティ、プライバシー、安全への脅威を含め、 アプリがプラットフォームの完全性を脅かすことがないようにします。

自動審査では、 機械学習とヒューリスティックス、 そして長年蓄積されたデータを使って、 アプリのバイナリをスキャンして既知のマルウェアなどのセキュリティ上の脅威がないか確認し、 問題のあるアプリを見つけ出します。

人による審査は、 悪意のある行為者からユーザーを守る上で決定的に重要な防衛線となります。 Apple の審査担当者はアプリを一つひとつ分析し、スペシャリストが公証ガイドラインに違反しているアプリを却下します。 また、 審査チームは各アプリを隔離されたプラットフォーム内で起動、 実行し、 説明通りに動作するかどうか、 ユーザーにとって安全そうかどうかをテストします。 自動審査は過去の脅威に依拠するため、 新たに発生しつつある脅威やまったく新しい脅威を検出するには、 人による審査で補完することが不可欠です。 サイバー犯罪者はますますクリエイティブに、 巧妙になってきており、 審査プロセスに人間を関与させることで、 Apple は進化し続ける脅威をコントロール下に置くことが可能になります。 また、 人による審査は、 悪質な詐欺など、 ソフトウェア以外の部分で脅威をもたらすアプリが iPhone に入ることを止めるための取り組みにも欠かせません。 人による審査は、ソーシャルエンジニアリングの手法を使って誰かになりすまし、 ユーザーからデバイスや情報へのアクセス権を取得しようとする悪意のある行為者を特定する上で特に重要になります。 人間の担当者は、 悪意のあるアプリが別のアプリのふりをするなどしてユーザーをだまそうとしていないか、 ユーザーを欺いて機密データへのアクセス権を取得しようとしていないかをチェックでき、 機械では見つけられないその他の悪意ある手法を調べることができます。

Apple は、 アプリを最初にダウンロードしたあとに、 悪意のある行為者がマルウェアやその他の危険な機能を各アプリに忍ばせることを阻止するために、 これと同じチェックを**すべてのアプリのアップデート**にも適用します。

ここで明確にすべきことは、公証は自動審査プロセスと人による審査プロセスの両方で成り立ちますが、これは App Review ではないということです。 公証では、 App Store Review ガイドラインの一部についてのみ、 提出されたアプリが準拠しているかどうかを分析し、 App Store Review ガイドラインの最も重要なガイドラインの多くは公証に**含まれていません**。公証に**含まれる**のは、ユーザーのセキュリティ、 プライバシー、 安全を守ることを特に目的としたものなど、 ユーザーの保護と**プラットフォームの完全性**に必要なチェックのみです。

- **セキュリティ：** 公証では、 アプリがデバイスにセキュリティ上の脅威をもたらすかどうかをチェックします。 例えば、 公証ではアプリに既知のマルウェアが含まれていないことを確認します。 また、 指定されたコンテナエリア外でアプリがデータの読み出し／書き込みをしようとすることは許可されません。 これを許可すると、 アプリが別のアプリを操作したり、 ユーザーのデバイスから不正なデータにアクセスしたりすることが可能になってしまいます。

審査

虚偽の説明でユーザーを欺いてアプリをダウンロードさせることは、ユーザーがそれを別の既存アプリだと思い込んだためか、ダウンロードされたアプリがアプリの**実際の内容**と異なっているためかに関係なく、悪意のある行為者がユーザーの知らない間にデバイスにマルウェアやウイルスに送り込んだり、その他の方法でデバイスのセキュリティを脅かす際に使う主な方法です。これを阻止するため、公証では、アプリがその特長や機能に関して虚偽の情報を含んでいるかどうか、別のアプリのふりをしているかどうか、隠れた機能や非アクティブな機能、明文化していない機能があるかどうかも調べます。また、アプリがダウンロードされた後に、機能を導入または変更するリソースをダウンロードする可能性があるかどうかも調査します。

- **プライバシー：**公証では、各アプリが、すべての Apple 製デバイスに組み込まれ、その完全性に欠かせないプライバシー機能に適切に対応し、これを迂回しようとしていないことを確認することで、ユーザーのプライバシーに対する脅威を阻止しようとします。ユーザーのプライバシーを保護し、データがどのように使用されるかに関する透明性をユーザーに提供するため、Apple は技術的な対策を講じてアプリがユーザーの機密情報にアクセスすることを阻止しています。iOS では、ユーザーの同意があって初めて、アプリはこの種のデータへのアクセスが許可されます。ユーザーは同意をいつでも取り消せます。これは以下のデータやサービスに適用されます。

  - マイク
  - カメラ
  - Face ID
  - 保存されたパスワード
  - 位置情報サービスで提供される位置情報データ
  - ヘルスケアのデータ
  - 広告主が使用する一意のデバイス識別子（IDFA）
  - Bluetooth
  - ウォレット
  - 連絡先
  - 写真
  - ホームアプリのデータ
  - カレンダー
  - Game Center の友達リスト
  - リマインダー
  - Apple Music のライブラリ

公証では、このような許可を求めているアプリが、アクセスを必要とする理由について明確かつ簡潔であるかどうかをチェックします。これにより、ユーザーは 何を許可するかについて情報にもとづいて判断でき、自分のデータを自分でコントロールし続けることができます。

位置情報サービスにより、アプリやウェブサイトは携帯電話、Wi-Fi、GPS、Bluetooth ネットワークからの情報を使って、ユーザーの位置を高い精度で特定できます。

Apple の**アプリのトラッキングの透明性**フレームワークでは、事前にユーザーが同意しない限り、デベロッパが広告主によって利用される一意のデバイス ID（IDFA）にアクセスして、広告やデータブローカーとの情報共有のためにウェブサイトやほかのアプリを横断してユーザーを追跡することはできません。

公証では、ユーザーが期待する方法でユーザーのデータを扱っているかどうかも評価します。例えば、公証では、アプリがデータの収集や共有を行う場合はユーザーの同意を得るようにし、ユーザーを操ったり、だましたり、強制したりしてアプリのユーザーデータへのアクセスに同意させないようにします。また、アプリがプライバシーポリシーを提供し、データがどのように収集、使用、販売されているかをユーザーが理解できるようにしているかどうかも調べます。また、個人の健康データは機密性が高いため、健康、フィットネス、医療に関する調査で収集されたデータを、広告、マーケティング、またはその他のユーザーベースのデータマイニングの目的で開示しないようにも義務付けています。

- **安全性：**公証に合格するには、ユーザーに危害を与えたり、デバイスに損傷を与えたりするリスクがアプリに含まれていない必要があります。たとえば、アプリが他の人に危害を加えるリスクがあるような活動に参加することをお客様に求めたり、そのようなリスクのある方法でデバイスを使用することを求めたりすることを禁止しています。また、公証では、iPhone のバッテリーを急速に消費する、過度な熱を発生させる、デバイスのリソースに不必要な負荷をかけるなどによって、デバイスを機能不全に陥れるアプリがないかも調べます。これらはすべて、緊急時に iPhone を使えなくする可能性があります。

公証に関する Review ガイドラインには、App Store Review ガイドラインで定められているコンテンツとコマースのポリシーは含まれていません。そのため、アプリがこれらのポリシーに違反することを禁じたり、違反しているかどうかをチェックすることはありません。これは、Apple が、App Store では許可されないポルノグラフィを配信するアプリや、たばこや電子たばこ（関連製品を含む）、違法薬物、過度のアルコールの摂取を助長するアプリ、海賊版のコンテンツが含まれる（あるいはほかのデベロッパからアイデアや知的財産を盗用する）アプリが代替アプリマーケットプレイスに出回ることを阻止できないことを意味します。App Store で配布することを選択したアプリのみが、公証に加えて標準の App Review プロセスを通過し、この場合は上記のような App Store のみに適用されるポリシーが実施されます。

アプリがこれらの審査に合格すると、Apple はアプリを公証し、iOS でアプリを配布するために必要な署名をデベロッパに提供します。Apple がアプリに署名してからユーザーが実際にアプリを iPhone にインストールするまでに何も変わっていないことを確かめるために、公証済みのアプリはインストール中に一連の基本チェックも受けます。これにより、公証されて以降に改変されてないことや、認証済みのソースからインストールが開始されたことを確認できます。

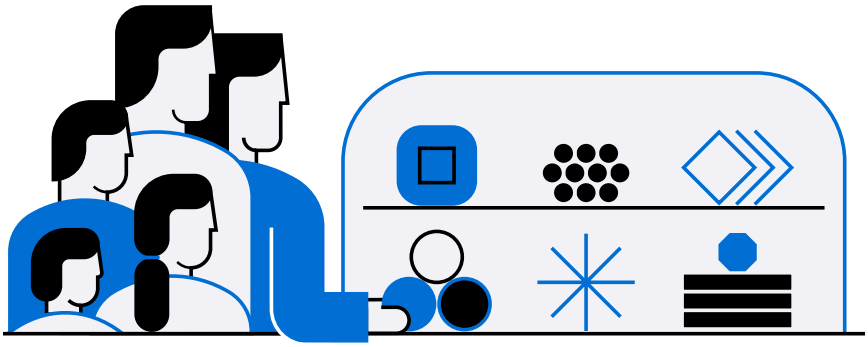
インストール

公証は、セキュリティ、プライバシー、安全に対する脅威からユーザーを守る取り組みにおいて重要なツールとなり、潜在的な脅威や有害な機能に対する早期防衛線になりますが、公証には限界があることも確かです。アプリがインストールされた後もユーザーを継続的に保護するためのセーフガード措置として、**代替アプリマーケットプレイス向けのベースライン基準を作成し、ユーザーを継続的に保護するという重要な責任を果たすために必要な最低限の機能が備わっていることを確認できるようにしました**。これには以下のようなものがあります。

- **継続的な監視を行い、悪意のあるアプリを検出して削除する。**この監視は、公証中にブロックされなかったアプリや、公証後に変更が加えられたアプリを見つけるために必要です。Appleの経験上、最初の審査後に新しい脅威が発生していないかどうかを継続的に監視することは、ユーザーの安全、セキュリティ、プライバシーを守るために欠かせません。また、このような監視を行うにはユーザーレビュー、お客様のフィードバック、マーケットプレイスデータの分析など、マーケットプレイス固有の情報が必要になりますが、Apple は App Store 以外でこれらの信号にアクセスすることはできません。それぞれの代替アプリマーケットプレイスが継続的な監視を行わないと、ユーザーのセキュリティ、プライバシー、安全が深刻な危険にさらされることになります。

- **代替アプリマーケットプレイスにユーザーを保護するための機能が備わっていることを保証する。**セキュリティ、安全、プライバシーを重大な危険にさらさずに、サードパーティアプリの配布を促進するアプリマーケットプレイスを運営するのは、簡単なことではありません[6]。悪意のあるアプリを継続的に監視するなど、アプリマーケットプレイスがこうした重要な責任を果たすにはリソースが必要となります。また、マーケットプレイスには、ユーザーとデベロッパに継続的なサポートを提供する能力を備えている必要があります。デベロッパがビジネスを行い、代替アプリマーケットプレイスを通してダウンロードしたアプリが期待通りに動作するとユーザーが信頼できるようにし、そうでない場合はサポートを受けることができるようにするためです。ユーザーを保護するために必要なリソースが欠如している、または必要が生じた時にユーザーとデベロッパにリソースを提供できないマーケットプレイスは、iPhone を危険にさらすことになります。

この要件は、アプリマーケットプレイスがユーザーのデータのセキュリティとプライバシーを守り、ユーザーの安全を確保するために最低限必要なものです。代替アプリマーケットプレイスには、App Store のセキュリティ、プライバシー、安全に関する高い基準を維持するために Apple が尽力してきた取り組みのすべてが取り入れられているわけではありません。

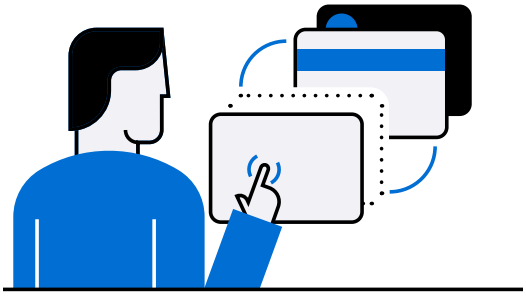


Apple は、アプリインストールシートを作成し、ユーザーがダウンロードしたアプリに関して十分な情報を得た上で選択ができるようにもしています。ユーザーが Apple 製品を選ぶ理由の一部として、私たちがユーザーに提供している透明性とコントロールがあります。これにより、ユーザーは自分のデバイスに何を入れたいかについて、十分な情報にもとづいて決定できるようになります。これらの新しいアプリインストールシートは、Apple がユーザーから期待される透明性への取り組みを継続していくために重要な手段です。

このシートでは、アプリ名、デベロッパ名、アプリの説明、スクリーンショット、システムの年齢制限などの公証中に審査された情報と、ユーザーがアプリをダウンロードしているマーケットプレイスの名称が、すべて見やすく標準化されたフォームに表示されます。デベロッパは、いったんアプリが公証されたら、再度公証プロセスを経ることなくこのシートの内容を変更することはできません。

DMA によって要求されるすべての変更を可能にするために、Apple は 600 以上の新しい API とデベロッパツールを作成しました。Apple は、これらの API に、データセキュリティ、プライバシー、ユーザーの安全を組み込んでいます。たとえば、iOS 上で代替アプリマーケットプレイスを運用できるようにするフレームワーク「MarketplaceKit」では、代替アプリマーケットプレイスから配布されるアプリの**安全な**インストールを可能にします。ユーザーが代替アプリマーケットプレイスを通じてアプリをダウンロードする際、この API によってマーケットプレイスのウェブサーバーが直接 iOS とやり取りできるようになり、認証サービス、アプリのライセンス、アプリのデータを提供し、安全な体験を生み出します。これらの API では、マーケットプレイスからのアプリのインストールが、ユーザーがマーケットプレイスとやり取りした結果として起きていることを確認するように設計されています。つまり、ユーザーが自分でアプリをダウンロードすることを選んだのであって、バグや自動ダウンロードの結果ではないことを確かめます。さらに、これらの API はアプリの簡単なアップデートを可能にし、デベロッパにアプリを最新に保つよう奨励しています。

また、Apple はほかにも「AdAttributionKit」など、ユーザーを保護する新しい API を開発しました。これはプライバシーを保護した広告を可能にするもので、広告主やデベロッパが、個別ユーザーやデバイスをトラッキングすることなく、他社が所有するアプリを横断して広告データの指標を取得できるようにするものです。これらの新しいツールにより、DMA を遵守するために Apple が行った変更が、ユーザーの安全を可能な限り保護しながら、可能な限りシームレスに機能するようになります。



この情報の要約をひと目でわかる形でユーザーに提供することで、ほかのマーケットプレイスではアプリ情報の開示について標準化された要件がなくても、また公証後にアプリが表示内容を変更したとしても、ユーザーは自分がどのようなアプリをダウンロードしているのか、またアプリが公証を受けた時はどのようなものだったのかを知ることができます。この開示により、ユーザーはどのアプリを使いたいかを選びやすくなります。ユーザーは、どのマーケットプレイスでも、シートの表示をオフにするよう選択することもできます。ユーザーがデフォルトに指定したマーケットプレイスでは、ほかのマーケットプレイスよりも優先する選択をしたということで、シートは自動的に非表示になります。

決済に関するリスクをユーザーに知らせる

DMA を遵守するために発表した変更に対応するため、Apple は App Store のデベロッパが代替決済手段を選択できる機能を導入し、EU では代替決済手段を使ってアプリ内のデジタル商品やサービスの取引を完了できるようにします。これにより、デベロッパには新しい選択肢が開かれますが、それと同時に、これらのアプリには、アプリ内課金（IAP）を含め、Apple のプライバシーとセキュリティが保護されたコマースシステムを通じてこれまで得ていたものと同じ保護とメリットはなくなることも意味します。例えば、サブスクリプションの簡単な解約や、一か所で確認できる購入履歴ページ、「承認と購入のリクエスト」などのペアレンタルコントロールのほか、ユーザーをだましてデジタル商品について広告されていた価格とは異なる金額を支払わせようとするといった詐欺的な手法からの保護なども利用できなくなります。この負担はユーザーにかかることになり、どのようなメリットや保護を受けられるか、取引がうまく行かない時はどこに連絡してサポートを求めればいいのかなど、ユーザー自身がアプリごとに判断する必要が生じます。こうした状況で、AppleCare エージェントがサポートできる範囲は（あっても）限られているためです。

ここでも、Apple はいつものように透明性とユーザーに必要な情報を提供するという価値観を重視します。そのため、**ユーザーに Apple の保護が提供されないことを知らせ、ユーザーが取引を完了するかどうかを決定するのに必要な情報を得ることができるようにします。**App Store では、ユーザーがアプリをダウンロードする前にアプリの製品ページに情報バナーを表示し、デベロッパが Apple の安全なコマースシステムではなく、代替決済手段を使用していることをユーザーに知らせます。また、ユーザーが Apple のコマースシステム外で取引を行う前に、Apple と取引しているのではないことを知らせるアプリ内情報開示シートを表示します。この情報により、ユーザーはデベロッパが誤解させるような支払い情報を表示したり、詐欺的な価格設定をしたり、サブスクリプションに必要な情報開示をしていないのではないかと警戒する必要があることを知ることができます。

設計に組み込まれたセキュリティ、プライバシー、安全

重要なことは、Apple のシステムアーキテクチャと設計により、ユーザーのセキュリティ、プライバシー、安全が引き続き保護されることです。 Apple は、パワフルな多層構造のセキュリティ保護機能を通じて、プラットフォームの中心にセキュリティを組み込んでいます。 この設計により、 私たちは、 EU 域内の iPhone が世界のそれ以外の地域の iPhone ほど安全でなくなっても、 EU 域内では最も安全な選択肢であり続けると確信しています。 基本レベルでは、 ハードウェアベースのデバイス暗号化のような主要なセキュリティ機能は無効化できません。 また、Apple は、アプリのための安定した、安全なプラットフォームを提供する何層もの保護機能も提供しています。 例えば、 すべてのアプリは**サンドボックス化**されているため、 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たりできないようになっています。 また、 システムファイルとリソースはユーザーのアプリから保護されています。 アプリが自身以外の情報にアクセスする必要がある場合は、 iOS によって明示的に提供されているサービスを通じてしかアクセスできないようになっています。 つまり、 アプリは通常、 ほかのアプリや iOS に影響を与えることはできず、 マルウェアによってプラットフォームのほかの部分に影響が及ぶリスクが低減されます。 また、 Apple は**コード署名**も取り入れています。 つまり、 サードパーティアプリのコードはすべてデベロッパにリンクされており、 デベロッパの本人確認は Developer Program の登録時に確認済みです。 起動時に、 iOS はアプリ内のコードが、 デベロッパがアプリを提出した時に署名されたものと同じであることを確認します。

Apple は、 **プライバシー**を中心にして iOS を設計しています。 例えば、 iOS では、 アプリに位置情報サービスデータへのアクセスを許可するかどうか、 許可する場合にはアプリがユーザーの正確な位置情報にアクセスできるか、 おおまかな位置情報にのみにアクセスできるかを、 ユーザーが選択できる必要があります。 アプリは、 ユーザーの許可なしに iPhone のマイクやカメラにアクセスすることはできません。 また、アプリがデバイスのマイクやカメラを使用している時は、デバイスに通知が表示され、ユーザーに知らせます。 同様の理由で、 Apple は、 アプリがバックグラウンドで実行している場合はカメラへのアクセスを禁止し、 ユーザーに気付かれない間にスパイ行為ができないようにしています。

もちろん、 Apple は、 Apple シリコン、 Secure Enclave、 Face ID、 Touch ID などのハードウェアによるセキュリティと生体認証や、 Apple オペレーティングシステムの安全な起動、 アップデート、 および継続的な稼働を提供する統合されたハードウェアとソフトウェア機能、 安全な認証と転送中のデータ暗号化を提供するネットワークプロトコルなど、 ほかにも数多くの保護機能を組み込んでいます。 Apple 製デバイスは、 データの保護と暗号化機能も備えており、 紛失・盗難にあったデバイスを保護したり、 権限のない人数がデバイスを使用または改変することを防止します。 さらに、Apple は、ユーザーの自宅と健康を安全かつプライベートに管理するためのフレームワークである「キット」を提供しています。 これは、 サードパーティアプリも API を通してアクセスできるため、 ユーザーの最も機密性の高い個人的なは安全かつプライベートに保たれます。

以上は、 Apple のシステムアーキテクチャとプライバシーバイデザインのほんの一例です。 これらの機能と今後導入される新しい変更によって、 この新しい環境で EU 域内のユーザーを引き続き保護していきます。

政府とユーザーから寄せられた懸念の声

Apple は、プラットフォームに加えようとしている変更について、現実的な懸念があることを承知しています。そのため、このような保護対策は多くの方に歓迎されると期待しています。2024 年 1 月 25 日に、Apple が EU 域内で iOS、Safari、App Store に DMA 関連の変更を加えることを発表して以降、様々な政府（EU 加盟国の政府機関を含む）とユーザーから、iOS で代替アプリストアと代替決済業者を許可することのリスクについて懸念する声が上がっており、こうしたリスクに対処するためにセーフガード措置をとるのか、またどのような措置をとるのかという質問を受けてきました。

EU 域内と EU 域外の両方の**政府機関**が、こうした新しい配布オプションによって生じるリスクと保護対策の必要性をすぐに指摘しました。これらの政府機関、特に国防、銀行、緊急サービスなどの国の基幹的な機能を担う機関は、こうした新しい変更について Apple に問い合わせ、政府職員が政府支給の iPhone にアプリをサイドローディングできないようにする手段を用意してほしいと求めてきました。

いくつかの機関は、管理しているすべてのデバイスでサイドローディングができないようにする予定だとも語っていました。EU のある政府機関は、デバイスに入れるアプリを確認して承認する予算も人員もないため、今後も Apple と App Store を頼りにしていると伝えてきました。Apple がアプリを総合的に調べているという点で私たちを信頼しているためです。

このような機関はみな、App Store 以外でアプリをダウンロードするサイドローディングがセキュリティを侵害し、政府のデータとデバイスをリスクにさらす可能性があると認識しています。

そして、これらの変更によって iPhone のユーザー体験がこれまでより安全でないものになるのではないかと恐れる**ユーザー**から、ティム・クック宛てに多数のメールが届いています。これらのお客様は、Apple と Apple 製品について気に入っている点や重視している点は、ユーザーのプライバシーとセキュリティの保護への取り組みであり、新たな変更によって自分や家族のデバイスがリスクにさらされるのではないかと恐れていると言いました。

私たちは、このような懸念を実際に聞き、また予想してきました。セーフガード措置を導入したのはそのためです。また、法律の下で可能な限りユーザーを保護するために、たゆむことなくイノベーションに取り組んでいる理由でもあります。

ティムへ

欧州連合（EU）で iPhone に実施される変更について、
ティム・クックが実際に受け取ったメール

宛先：**ティム・クック**
差出人：**EU 市民**
件名：**ありがとうございます**
日付：**2024 年 1 月 27 日**

プライバシーであれ、健康であれ、人権であれ、顧客を第一に考える会社をリードしてくださっていることに感謝します。

EU 市民として、...私のデバイス上でのサイドローディングを許可しません。

宛先：**ティム・クック**
差出人：**Apple ユーザー**
件名：**先日成立した EU 法に深く憂慮する**
日付：**2024 年 1 月 28 日**

私は 10 年以上も Apple 製品を愛用しており、とても満足しています。Apple は魔法のような製品を作ったと、心から思っています。私は、使いたいアプリのデベロッパが App Store の利用を回避して自社のサードパーティストアに登録するように仕向け、そこからダウンロードするように強制されたり、利用している銀行が Apple Pay への対応をやめて、サードパーティ製の決済アプリを使うことを強制されたりする日が来ることを望んでいません。現状で、すべてが魔法のように機能しているし、楽しく使用しています。

あなた自身と Apple がこれからも正しいことのために立ち上がり、最高の顧客体験を提供し続けてくれることを心から望みます。iPhone が Samsung や Google の携帯電話のようにサードパーティのアプリストアで溢れかえるのは見たくありません。

宛先：**ティム・クック**
差出人：**EU の iPhone ユーザー**
件名：**ヨーロッパのデジタル市場法に対する懸念**
日付：**2024 年 1 月 27 日**

最近、ヨーロッパのデジタル市場法の成立を受けて、iPhone に代替アプリストアが登場することについて盛んに議論されています。消費者として、私はこの展開に懸念を抱いています。**私が iPhone を選んだのは、プライバシーとセキュリティへの強いこだわりのためで、ここには Apple の哲学が反映されています。**

新しい規制の下で、App Store 以外でアプリをダウンロードするように強制されることはありません。とはいえ、外部ソースからのアプリに関するポップアップや通知を回避することを含め、外部ソースからのアプリに遭遇する可能性さえも回避できるような選択肢が与えられることを希望します。要するに、App Store がアプリを探す唯一の場所であるという、iPhone の現在のユーザー体験が保たれることを求めます。

私のようなユーザーが、Apple の App Store からしかアプリをダウンロードできないように iPhone に制限をかけられる機能の導入を検討してもらえませんか？この選択肢によって、すでに満足しているセキュリティとプライバシーのレベルを選ぶ顧客の権利が守られます。これは公正な競争の原則に沿ったものであると思います。

宛先：**ティム・クック**
差出人：**Apple ユーザー**
件名：**サイドローディング**
日付：**2024 年 1 月 16 日**

自分のデバイスでサイドローディングをしたくない人にセキュリティを保証してくれますか？

通常通りにアプリケーションを入手したい人は多いと思います。サイドローディングを認めず、インストールに関しては通常の Apple アプリケーションを使う方法があると素敵です。

サイドローディングを禁止するGoogleプログラム

Android では当初からサイドローディングが許可されてきましたが、Google は、この慣行によってセキュリティ条件の高いユーザーがリスクにさらされることを認識するようになりました。

Google は、「特に価値のあるファイルや機密情報を含むアカウント」を持つユーザー向けに高度な保護機能プログラムを設計し、「ジャーナリスト、活動家、企業の役員、選挙に関わる人」は、このプログラムに登録するように強く勧めています。このプログラムの中心的機能の一つは、「有害なダウンロード」を防ぐためにサイドローディングを許可しないことです。このプログラムに登録したユーザーは、「Google Play ストアやデバイスメーカーのアプリストアなど、確認済みのストア」からしかアプリをダウンロードできなくなります。

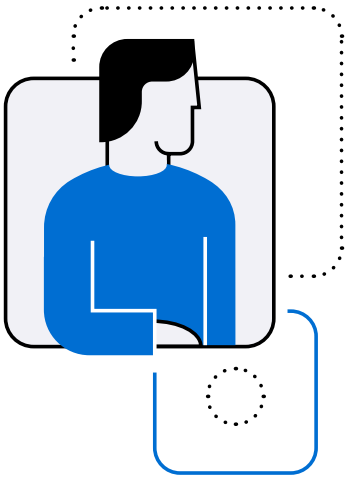
アプリの配布と代替決済システムに関する Apple のセーフガード措置によって（なくなるわけではないが）低減するリスク

以下のセーフガード措置は、世界のほかの地域と同等ではないとしても、EU 域内のユーザーの iPhone 体験を可能な限りセキュリティとプライバシーが保護された安全なものにするのに役立ちます。このセクションでは、これらのセーフガード措置によって対処しようとしているリスクのカテゴリをさらに詳しく説明します。

公証

公証は、ユーザーのセキュリティ、プライバシー、安全に対する深刻な脅威を見つけて、悪意のあるアプリを検出することを目的としています。例：

- 悪意のあるアプリがデバイスに侵入する一般的な方法の 1 つは、**ソーシャルエンジニアリング**です。これは人気のある正規アプリなど別のものになりすまし、ユーザーをだましてデバイスにアクセスする権限を取得する手法です。公証では、アプリがメタデータで申告しているとおりに実際に動作するかを審査時に確認することで、この脅威を低減することを目指しています。公証では、



そのような悪意のあるなりすましがデバイスに侵入するのを阻止することを目標として、アプリを分析します。これはほんの一例に過ぎませんが、Apple は人による審査と自動審査の組み合わせによって、正規の広告プラットフォームになりすましてログイン情報を盗もうとしていた一連のアプリを特定しました。公証では、そのような悪意のあるアプリがないかをチェックします。人による審査は、このようなスキームを見破るために欠かせません。自動審査では、ユーザーを巧みに操るように仕組まれた攻撃はチェックできません。

- また、悪意のある行為者は、位置情報サービスや（健康に関するデータを保存する）HealthKit、マイク、カメラ、連絡先、写真など、iPhone の保護された領域にアクセスする権限をユーザーに自発的に提供させるために、**本当の意図を偽る**ことがあります。悪意のある行為者は、不正に取得したアクセス権を使ってユーザーを**ランサムウェア**の標的にすることもあります。この場合、悪意のある行為者はユーザーのファイルにアクセスして暗号化し、身代金を支払わないと復号化しなかったり、金銭を支払わなければファイルを公の目にさらすと脅したりします。そのため、重要なファイルにアクセスできなくなったり、身代金を支払った場合は金銭的な被害を被ったり、ユーザーのプライベートなメモや写真、その他のファイルが公の目にさらされた場合は感情的、心理的な傷を負ったりする可能性があります。公証、特に人による審査では、iPhone のほかの部分へのアクセス許可を求める理由について、ユーザーをだまそうとするマルウェアを特定し、ブロックします。この許可がないと、悪意のあるアプリは厳格に管理されたサンドボックスの外にあるデータにアクセスできません。

- 悪意のある行為者は、不正に取得したアクセスを使って、**消費者向けスパイウェア**を導入する可能性もあります。この種のマルウェアは、エンドユーザーが知らないうちにデバイスにインストールされ、連絡先、写真、ビデオなどの機密情報を盗もうとするものです。商用スパイウェアを使うと、親密なパートナーのプライバシーを侵害したり、ハッカーが企業秘密などの金銭価値のあるデータを抜き取ったり、犯罪スキームの一環としてユーザーをゆするために利用できる情報を取得したりできます。悪意のある行為者は、そのような機密データをユーザーの許可なく販売することもできます。このような行為はユーザーの権利を侵害するもので、Apple のプライバシー保護ポリシーにも違反しています。公証および審査担当者は、本当の目的と機能を隠して商用スパイウェアを導入しようとしているアプリを見つけ出します。

- 故意に悪意があるか、感染したかを問わず、デベロッパツール自体に悪意あるソフトウェアが入り込んでいる可能性があり、ユーザーにとってもデベロッパにとっても脅威となります。知っていたか知らなかったかに関係なく、デベロッパがアプリの中に入れてしまった悪意のある SDK は、位置情報データを収集して悪徳業者に販売したり、アプリがユーザーの同意の下に取得した保護されたデータを勝手に収集したり、許可なくウェブサイトやアプリを横断してユーザーをひそかにトラッキングしようとしたりすることがあります。公証では、アプリを審査することで、**マルウェア**が含まれているとわかっている不正なデベロッパツール（SDK など）がアプリに埋め込まれていないかを確認し、マルウェアが含まれ、マルウェアを拡散するデベロッパツールを配布しようとする悪意のある行為者の脅威からデベロッパを守ります。

サイドローディングによる脅威についてもっと詳しく

悪意のある行為者がサイドローディングされたアプリを使ってユーザーのセキュリティ、プライバシー、安全を脅かす可能性については、2021 年の白書「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」をお読みください。特に、Apple の新しいセーフガード措置がない状態では問題になる点です。「サイドローディングの脅威分析」および「The Important Role of App Store Protections」

宛先：**ティム・クック**
差出人：**Apple ユーザー**
件名：**がっかりしました**
日付：**2024 年 1 月 15 日**

もうすぐ、Apple と他社を差別化する要因は何もなくなってしまいます。私の友人や家族の多くが iPhone の悪意のある行為者から守る機能に頼っているので、今回の決定から影響を受けます。私にとっては、今はもう iPhone にお金を使うべき理由はほとんどありません。このメールをご本人が読んでいるのかどうかわかりませんが、今回の決定が Apple の方針ならば、ユーザーの安全を守る方法を用意してほしいです。

- 悪意のあるアプリは、ユーザーに**物理的な危害**を与えることもあります。公証では、このようなリスクがないかアプリを審査します。例えば、公証では、アプリがユーザーやほかの人に危害を与えるように促していないかをチェックします。ユーザーに 50 日間にわたるタスクを与えて、自殺するように促すような危険なオンラインチャレンジなど、悪意のある行為者が作成した様々な「チャレンジアプリ」と呼ばれるアプリを見つけ出します。こうしたアプリは、自分を傷つける行為を少しずつ勧めていき、最後のチャレンジで「プレイヤー」に自殺することを求めます。Apple はこのようなアプリを見つけ出し、iOS から排除してきました。公証は、このような危険なアプリを引き続き iOS に入れないようにすることを目的としています。

代替アプリマーケットプレイスの要件

代替アプリマーケットプレイスを運営するための適格基準は、継続的な監視を義務付けることによって、iOS ユーザーがほかの悪意ある行為から被害を受けることを防ぐために役立ちます。Apple は世界で最も安全で最もセキュリティが保護されたモバイルコンピューティングプラットフォームを提供していますが、独立した専門家が繰り返し確認してきたように [7]、悪意のある行為者は常に Apple の安全策をくぐり抜けようとするものです。高度なツールや専門家による審査チームを用意しようとも、最初に公証で検知されることのない最先端の悪質な偽装アプリを見つけ出すには、粘り強く継続的に監視を行うことが不可欠です。

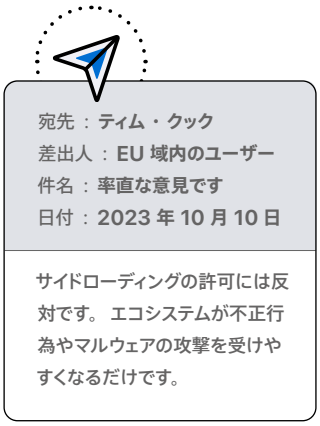
また、審査を通過した**あとで**、ごく平凡なアプリが悪意のあるアプリへと変わることもありました。問題がないように見え、公証を通過したアプリであっても、承認後に、外部の信号をきっかけに不正な機能が有効になり、暗号詐欺、模倣アプリ、マネーロンダリングツール、あるいはさらに悪質なものに変化する可能性があります。これは**ベイトアンドスイッチアプリ**と呼ばれます。このようなアプリには、デベロッパのサーバーから情報を取り込むコンポーネントが含まれている可能性があります。これにより、サイバー犯罪者は、ユーザーに提供されるユーザーインターフェイスを公証後に変更して、悪意のあるアプリにすることができます。

そのほか、難読化コードがアプリに含まれ、一見悪意のあるものには見えなくても、外部の条件がトリガーとなるものもあります。例えば、地理的位置情報、IP アドレス（つまり、Apple の従業員である可能性のある場所やデバイスで開かれていないこと）、提出後の経過時間（つまり、アプリの公証が完了した可能性が高いと悪意のある行為者が判断するのに十分な時間が経っていること）などがトリガーとなります。一例を挙げると、公証中は電卓のように見えたため、公証を通過したアプリに、Apple が把握していないコードが含まれ、それによって、公証の通過後に違法なギャンブルアプリに変わったということがあります。

このようなアプリを特定できる方法は、継続的な監視しかありません。実際、継続的な監視によって、Apple は App Store への公開後に悪意のあるものになった、以下のようなアプリを特定しました。

- 旅行情報・サービスを提供すると説明されていたアプリが、承認後に、未認可のサービス事業者による違法なローンアプリに切り替えられました。
- 人気のある成人向けチャットアプリに、ランサムウェアが密かに埋め込まれていました。このアプリは、まずユーザーの連絡先リストへのアクセスを要求し、その後、要求額を支払わなければ、成人向けチャットアプリの利用について連絡先リスト内の全員に知らせると脅しました。
- 動物に関する情報を提供すると説明されていたアプリが、承認後に、違法なギャンブルを促すアプリに切り替えられました。

Apple は、App Store を通じて配布されるアプリに対し、このような継続的な審査を行っており、特定した悪意のあるアプリはすべて迅速に削除することができます。こうした保護策の一部は、EU の新たな環境下でも導入される予定です。例えば、代替アプリマーケットプレイスを介してインストールされた場合と同様に定期的にアプリをインストールして起動するなどの方法で、公証後にアプリが変更されたかどうか検出を試みる自動ツールが導入されます。しかし、Apple は、App Store におけるユーザーレビューやダウンロード数に関するデータ分析など、マーケットプレイスに固有の信号を含むその他の信号も使用しています。代替アプリマーケットプレイスで配布されるアプリについては、そのようなマーケットプレイス固有の信号を使用して継続的な審査を行うことができず、アプリが悪意のあるものに変化した場合、それを把握するためのツールははるかに少なくなります。このため、代替アプリマーケットプレイスは、悪意のあるアプリという非常に現実的な脅威からユーザーを守るため、その監視に尽力する必要があります。



また、マーケットプレイスがデベロッパに代わってアプリを配布するのに必要なリソースを備えた合法的なビジネスであることを保証する基準がなければ、危険なマーケットプレイスがユーザーのデバイスに簡単に侵入できることにもなりかねません。こうした中に、短期間だけショップを開き、ユーザーをだまして偽アプリや偽造アプリを購入させた後、ユーザーが詐欺被害に気付く前にマーケットプレイスを閉鎖する（追跡が非常に難しくなる）という詐欺マーケットプレイスが紛れ込む可能性があります。また、提供するアプリについて、セキュリティ、プライバシー、安全性の問題を十分に監視する能力がないマーケットプレイスが含まれる可能性もあります。あるいは、確実な金銭的手段を持たずに運営するマーケットプレイスが、デベロッパとユーザーの間で取引を進めたあと、結局、資金不足により閉鎖するというケースも起こり得ます。このような場合、マーケットプレイスからダウンロードしたアプリに問題が見つかり、ユーザーが返金を求めたり、詐欺を報告したりする必要があっても、ユーザーには解決策が一切なくなります。Apple は、合法的なマーケットプレイスの選択肢を維持しながら、そのような危険なアプリマーケットプレイスのリスクを最小限に抑えるための基準を定めました。

宛先：**ティム・クック**
差出人：**Apple ユーザー**
件名：**iOS17 以降の iOS アップデートでサイドローディングやサードパーティのアプリストアを許可しないでください**
日付：**2023 年 1 月 11 日**

私自身をはじめ、世界中のほとんどのユーザーがサイドローディングを認めてほしくないと思っていることをお伝えしたく、このメールをお送りします。もし Apple がサイドローディングを許可すれば、私の思うとおり、多くのユーザーが iOS エコシステムから離れていくでしょう。私は 10 年以上 Apple 製デバイスを利用しており、App Store は iOS や iPad OS デバイスの中核だと信じています。
iOS でサイドローディングを認めれば、現在そして将来の iOS ユーザーにとって大打撃になるでしょう。
サイドローディングを許可することが iOS エコシステムにとってどれほど有害で危険であるか、Apple のみなさんは私以上によくご存知だと思います。

アプリインストールシート

アプリインストールシートも、ユーザーに情報を提供し、詐欺やソーシャルエンジニアリング攻撃の被害を防ぐのに役立ちます。多くの場合、悪意のある行為者はユーザーをだまして悪意のあるプログラムをダウンロードさせようとします。これには、模倣アプリ、ソーシャルメディアを利用した詐欺の拡散、偽のシステムアップデート、E メールによるフィッシング手法、正規に見せかけたウェブサイト上の広告など、多種多様な手口があります。例えば、悪意のある行為者がアプリに関する虚偽の説明をウェブサイトに掲載したあと、ユーザーを代替マーケットプレイスに誘導し、今度はそこで、デベロッパがアプリについて虚偽の説明をする可能性があります。アプリインストールシートは、ダウンロードしているアプリやダウンロード元に関する情報を各ユーザーに伝えるのに役立つため、悪意のある行為者がユーザーをだまして悪意のあるアプリをダウンロードさせるリスクがなくなるわけではないものの、大幅に低減します。
また、これらのシートは、代替アプリマーケットプレイスに虚偽の説明を載せるアプリを完全に防ぐことはできなくても、これに対する保護対策として役立ちます。アプリマーケットプレイスは、プラットフォーム上での宣伝方法についてルールを定めないという方針をとる可能性もあります。そのようなマーケットプレイスでは、アプリをまったく別のアプリとして宣伝できるだけでなく、実際の請求とは異なる料金体系やサブスクリプションを設定したり、様々な機能やサービスがあると偽って説明したりすることもできます。アプリインストールシートは、アプリに関してデベロッパが提出し、公証中に正確であることが確認されたデータを反映するものであり、審査のために Apple に提出された時点でのアプリの概要や説明された目的をユーザーが確かめられる最終手段となります。

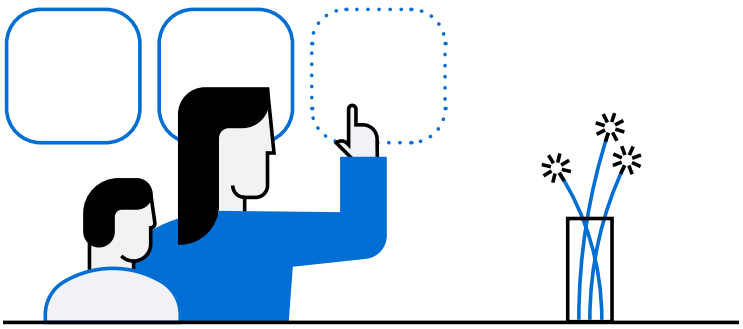
代替決済手段に関する情報

代替決済手段に関しては、Apple の安全なコマースシステムが阻止している特定の略奪的手法など、起こり得る不可避のリスクについて、Apple の情報バナーがユーザーに情報を伝えます。Apple のシステムは、悪意のある行為者が意図的に紛らわしいデザインやテキストを用いて、ユーザーが意図していない、あるいは理解していない条件で購入やサブスクリプションの登録をさせられたり、解約をほぼ不可能にしたりするような手口からユーザーを保護します。このほかに、以下のような保護策があります。

- アプリ内でデジタル商品やサービスを販売するすべての iOS アプリは、これまでは Apple の安全なコマースシステムを使用していたため、Apple はユーザーが登録したあらゆるサブスクリプションを 1 回タップするだけで簡単に解約できるようにしてきました。また、アプリ内課金をサポートするデベロッパ向けフレームワーク「StoreKit」を通じて、Apple は、アプリ内課金の料金体系や条件が、Apple Store Connect の SKU でデベロッパが設定したものと正確に一致するようにしています。アプリが販売時に料金体系や条件をどのように設定するかに関わらず、購入前に必ず、請求料金に関する確認がユーザーに表示されます。このようなシステムがなければ、アプリがサブスクリプションの解約方法をわかりにくくして、ユーザーに解約を躊躇させたり、

無料トライアル期間やサブスクリプションの支払いの頻度や金額を偽って伝えるなど、誤解を招くやり方で、ユーザーが理解すらしていない条件や料金でサブスクリプションに登録させることも起こり得ます[8]。

- App Store の安全なコマースシステムは、デジタル商品について、開示している以上の料金をアプリが請求することを防ぐのに役立ちます。App Store での公開のために Apple にアプリを提出する際は、必ずデジタル商品やサービスの料金を記載する必要があります。Apple は、そのアプリの実際の請求金額がユーザーへの宣伝通りかを検査し、提供されるデジタル商品やサービスに対して著しく過大な請求を行っていないかをチェックできます。昨年は、数百ものアプリについて、不正に操作された料金設定に対する措置を講じました。アプリ内課金を使用するデジタル商品やサービスのための一貫性のある標準の決済フローの一部として、Apple のコマースシステムの API も、ユーザーが購入を完了する前に、Apple に提出された料金（および、提出されたその他商品情報や重要な購入条件）が必ずアプリに表示されるようにしています。これにより、アプリが正しい金額を開示したかどうかに関係なく、ユーザーは請求内容を把握できます。これまでユーザーが頼ってきたこのようなシステムがなければ、ユーザーは、デベロッパが宣伝している価格がユーザーの最終的な支払い額を正確に表しているという確証を得られなくなる可能性があります。
- Apple はさらに、「**承認と購入のリクエスト**」のようなサービスを通じて子どもと家族を保護しています。このサービスでは、子どもが iPhone 上で商品を購入またはダウンロードしようとするたびに親の承認が必要となるため、親は、子どもが詐欺の標的になることを心配せずに済みます。
- Apple の不正対策は、不正なデベロッパからユーザーを守るだけでなく、不正なユーザー（盗難クレジットカードで取引するユーザーなど）からデベロッパも守っています。例えば、Apple の決済システムデータの分析から傾向や動向を特定することで、詐欺や悪質な個人を一掃できます。
- App Store のコマースシステムは、アプリが約束したとおりの内容を提供していることを確認するためにも役立ちます。ユーザーが Apple のシステムを通じて購入すると、その取引はユーザーの購入履歴に書き込まれます。ユーザーが料金を支払った後、アプリがデジタル商品やサービスを提供しない場合は、Apple は取引履歴を利用して、取引が行われたかどうかを検証し、取引を完了していないアプリに対して措置を講じることができます。この履歴がなければ、アプリが取引を反故にした場合に、Apple はユーザーを手助けすることができません。



ティムへ

欧州連合（EU）で iPhone に実施される変更について、ティム・クックが実際に受け取ったメール

宛先：**ティム・クック**
差出人：**Apple ユーザー**
件名：**Android はお断り**
日付：**2023 年 4 月 21 日**

私たちが iOS に満足しているのは、Android とは違って、iOS が高度なセキュリティとユーザフレンドリーなインターフェイスを備え、絶対に速度が低下しないからです。ところが、iOS 17 からはサイドローディングが可能になり、App Store 以外のストアからもダウンロードできるようになると聞きました。ダウンロードも可能になります。どうか、これはやめてください。私たちは App Store からだけダウンロードして、安全性を確保したいです。どうかサイドローディングを有効にしないでください。厳格なルールと最高のセキュリティがあった、これまでの iOS に戻してください。

宛先：**ティム・クック**
差出人：**EU 域内の Apple ユーザー**
件名：**心配している EU 在住の Apple ユーザーより**
日付：**2023 年 10 月 24 日**

EU でのデジタルプライバシーやオンラインの安全性について、ますます不安と恐怖を感じています。EU 在住の Apple ユーザーである私は、規制の保護（GDPR など）と Apple の安全性の機能（アプリのトラッキングの透明性や App Store など）との完璧なバランスに守られてきたといつも感じていました。しかし最近は、それが変わってしまいました。

私や私の家族、友人、同僚はみな、Apple 製品を使っていますが、仕事でもプライベートでもとりわけ Apple エコシステムを選んだのは、製品やソフトウェアがプライバシーとセキュリティを保護するように設計されているからです。もちろん、何年も前から導入されている安全機能も理由の一つです。考えるのも怖いことですが、EU 委員会の新しい規制によって、私が今、頼っている安全性とセキュリティの機能の多くが失われてしまうように感じています。

宛先：**ティム・クック**
差出人：**EU の iPhone ユーザー**
件名：**EU でのサイドローディング**
日付：**2024 年 1 月 25 日**

EU に住む一顧客として、サイドローダーを使わないという選択肢を提供してくれることを切に願います。得体の知れないものではなくて、実証済みの App Store を安心して使いたいのです。

宛先：**ティム・クック**
差出人：**EU の Apple ユーザー**
件名：**EU のサイドローディング指令に関する懸念と提案**
日付：**2024 年 1 月 26 日**

欧州連合（EU）が Apple に対して、iOS デバイスのサイドローディングを許可するよう要請したことについて、懸念を感じています。この決定が競争と消費者の選択を促進するために下されたということは理解していますが、これによってプライバシーとセキュリティに関する重要な問題が生じたと思います。

...App Store はこれまで、iOS アプリケーションの信頼できる入手元として、今日のデジタル時代に不可欠な信頼性と安全性を提供してきました。個人的に、App Store からダウンロードしたアプリは、厳格な審査プロセスを経ており、デバイスと個人情報を保護してくれるとわかっているので、いつも安心しています。

しかし、サイドローディングが導入されれば、悪意のあるアプリケーションや検証されていないアプリケーションをユーザーが知らず知らずのうちに外部ソースからインストールしてしまい、それによって iOS デバイスの全体的なセキュリティが損なわれる恐れがあります。この変更によって、ユーザーは様々なサイバーセキュリティの脅威にさらされる可能性があり、私はサイドローディングによって iOS に及ぶ可能性のある影響を危惧しています。

- また、Apple には数千に及ぶ AppleCare エージェントもおり、ユーザーは返金に関する支援やその他のカスタマーサポートを受けることができます。これらのエージェントは、代替決済システムを介した購入についてはサポートを提供できなくなります。

Apple の安全でプライバシーが保護されたコマースシステムは、これまで 20 年以上にわたりデジタル商品やサービスの購入に利用されており、ユーザーはそこで提供されるメリットと保護に信頼を寄せてきました。今後も情報バナーによって、これまで Apple が防いできた詐欺の手口に注意する必要があることを引き続きユーザーに伝えます。

宛先：**ティム・クック**
差出人：**EU 域内のユーザー**
件名：**近々導入行される EU におけるサイドローディングに関するアップデート - 個人的な見解**
日付：**2024 年 1 月 26 日**

私は、欧州連合で予定されている次回のアップデートに不安を覚えます。このアップデートがインストールされれば、iPhone や iPad をはじめとするすべてのデバイスのセキュリティが大きく損なわれると思います。

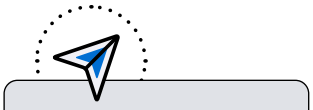
このアップデートはインストールしたくありません。怖いです。本当に怖いですし、このままでは iPhone のセキュリティが少し低下すると思います。

さらにリスクを低減する上で代替アプリマーケットプレイスと代替決済業者が果たす役割

今後数か月のうちに、EU 域内の多くのユーザーは、代替アプリマーケットプレイスから iOS にアプリをダウンロードし、代替決済業者を利用して料金を支払えるようになります。そのため、これまで iPhone で当たり前だったことが一変します。ユーザーは Apple を信頼し、自分のデバイスが保護されていると感じているため、これまでは、サードパーティアプリの提供元やアプリ内決済システムが脅威となるかどうかを心配する必要はありませんでした。今後、ユーザーはそのような保護を前提にすることはできなくなります。

DMA によって代替流通と代替の決済手段という新たな世界が開かれた中、Apple は EU 域内のユーザーを保護するために、有意義な対策を十分に講じていきます。しかし、その対策の範囲は、どうしても法律により制限されます。そのため、Apple は、私たち自身で実施することが認められなくなるユーザー保護機能に対する責任を、代替アプリマーケットプレイスや決済業者に委ねなければなりません。

つまり、代替アプリマーケットプレイスや代替決済業者は、ユーザーがその利用を望まないとしても、ユーザーの保護においておそらく避けて通れない役割を担います。DMA を遵守するための変更に関する Apple の発表を受けて、多数のユーザーから、その変更を単に拒否することは可能かという問い合わせが寄せられました。一部のコメンテーターは、Apple が EU で提供する予定の新たな選択肢を利用したくないユーザーは、それを利用する義務はないと主張しました。その代わり、これらのコメンテーターは、ユーザーは単に App Store からのみアプリのダウンロードを続けることができると言います。



宛先：**ティム・クック**
差出人：**EU の iPhone ユーザー**
件名：**欧州経済圏の顧客より**
日付：**2024 年 1 月 23 日**

Apple の iPhone を購入したのは私の自由な選択であり、Android を搭載したデバイスよりも iOS の方が安全だと感じたからです。そこで質問です。今後は、欧州市場向けの iOS バージョンをインストールするか、それ以外の地域で使用されている iOS バージョンをインストールするかを、顧客が自由に選べるようにできないでしょうか？

また、ユーザーは、利用するアプリマーケットプレイスや代替決済手段ごとに複数のアカウントを設定しなければならなくなります。これはユーザーにとって不便で、ユーザー体験が損なわれるだけでなく、データが盗まれるリスクも高まります。アカウントの数が増えれば、ユーザーの個人情報や財務情報の保存先も増え、データ漏洩によってデータが流出するリスクが高まります[9]。さらに、アプリの配布元が合法的な組織でなくても、ユーザーは個人情報を無分別に共有し、アプリの配布元を信頼するようになる可能性があります。悪意のある行為者は、iOS 以外のウェブサイトで正規のアプリマーケットプレイスを装い、ユーザーをだまして支払い情報や個人情報を入力させることができます。あとになって、ユーザーがそんなマーケットプレイスがないことに気付いても遅いのです。

しかし実際には、EU 域内のユーザーは、仮に望んだとしても、App Store だけを利用し続け、Apple の業界をリードする保護機能をすべて維持するという選択はできなくなります。デベロッパによっては、代替アプリマーケットプレイスでのみアプリを入手できるようにすることもあるでしょう。その中に、仕事や学校で必要なアプリや、家族や友人とつながりを保つために必要なアプリがあれば、代替アプリマーケットプレイスを利用したくなくても、ユーザーはそのアプリをダウンロードせざるを得ません。**EU 域内の膨大な数のユーザーが必要なアプリを入手するためにどこにアクセスする必要があるかは、最終的にデベロッパによりコントロールされます**。そのストアが提供する保護策にユーザーが満足しているかどうかは関係ありません。Apple が最善を尽くしても、多くのユーザーは、自分がそのマーケットプレイスとの取引を望んでいないにも関わらず、デベロッパに誘導されてその代替アプリマーケットプレイスからアプリをダウンロードしようとしていることに気付かない、あるいはそのことを理解していないかもしれません。

Android アプリは SMS フィッシングを使って人々をだまし、正規の郵便サービスアプリを装ったアプリをサイドローディングさせて、デバイスから機密情報を盗み出しました。この詐欺は、郵便サービスを装って複数の国で繰り返されました。実行されるアプリは手口によって微妙に異なるため、それぞれのマーケットプレイスがこのパターンを検知するのは難しかったでしょう[10]。

代替マーケットプレイスと決済業者に対する決定

EU では、すべてのユーザーのセキュリティ、プライバシー、安全性は、ある程度 2 つの質問に左右されることになります。第一に、代替マーケットプレイスや決済業者にユーザーを保護する能力があるか、そして第二に、代替マーケットプレイスや決済業者がユーザーの保護に関心を持っているか、ということです。 Apple が導入する対策は重要な基準となりますが、それだけで十分というわけではありません。ユーザー体験は、個々のマーケットプレイスや決済業者がどのような運営方法を選ぶかによって大きく変わります。これによって差別化のチャンスが生まれます。DMA が意図するとおり、Apple は積極的に競争し、App Store が消費者にとって最も安全で、セキュリティとプライバシーが保護された選択肢であり続けるよう努めていきます。しかし、これによって潜在的なギャップも生じます。

App Storeでの信号

1 日あたり
1 億 5,000 万件
の取引（すべての無料／有料アプリのダウンロードとアプリ内課金を含む）

1 日あたり
312 万件の
評価とレビュー

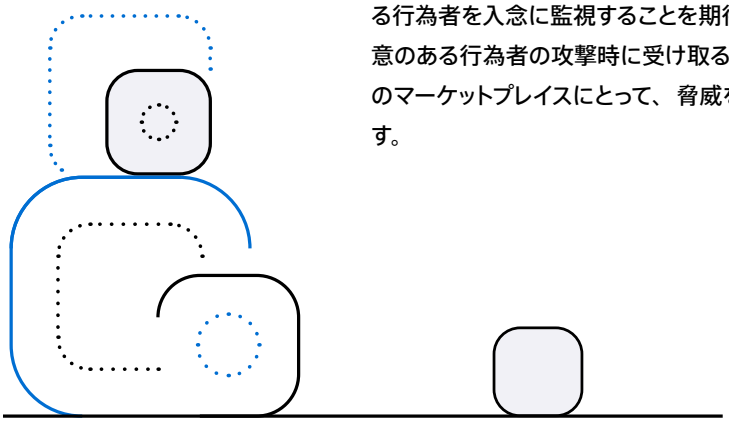
20 年間の大半にわたる App Store の運営は大変な仕事でした。 Apple は、悪意のある行為者、そして進化し続ける悪意のあるアプリを見つけ、阻止しようと常に努めています。 数千人のエンジニアが悪意のある行為者による危害からユーザーを守るためのハードウェアやソフトウェアを作っていることに加え、数百人の Apple のフルタイム従業員が App Review に関与し、3 つのタイムゾーンに及ぶ 80 以上の言語のアプリを審査しています。 毎年、 Apple は 600 万本以上の提出されたアプリを審査しています。 データを参照できる最近の 1 年間で、 Apple は約 450 万本のアプリを承認し、 160 万本以上のアプリを却下しました。 その多くは、デバイス上で正しく動作しなかったためであり、 Apple のセキュリティとプライバシーのルールに違反していたため却下されたものもありました。 このような根気強い取り組みは、iOS が公開以来、世界で最も安全なモバイルコンピューティングプラットフォームであり続けていること、また、 ほとんどの悪意のある行為者が iOS をマルウェアに感染させようとすることは、 時間、 労力、 リソースを費やすだけの価値がないと結論付けていることの主な理由です。

私たちの経験や 24 時間体制での人による審査をもってしても、 のちに Apple のガイドラインに違反していることが判明したという理由で、 年間 18 万 5,000 本以上のアプリを App Store から削除しました。 そのようなアプリを見つけ、削除するために、 Apple は Apple Store 自体も注意深く監視ししています。 **毎日** 1 億 5,000 万件以上の取引が行われ、 310 万件以上の評価とレビューが投稿される中から、 問題のあるアプリを特定しています。 Apple は監視において様々な指標を検討しています。 例えば、 ユーザーのレビュー、「問題を報告する」 ツールからの報告、 ユーザーをサポートする数千の AppleCare エージェントへのフィードバック、データ内の疑わしいパターン（通常と異なるレビュー状況、 ダウンロード数の急増、 通常と異なる購買行動など）といった指標があります。 Apple のチームが悪意のある行為者を一掃できる方法は、 そのような信号を注視することだけです。

今後は、代替アプリマーケットプレイスを運営する事業者が、App Store 以外でベイトアンドスイッチやその他の悪意のあるアプリから EU 域内のユーザーを保護するために必要な、継続的な監視を行わなければなりません。

代替アプリマーケットプレイスがこのような監視に多大なリソースを投じても、これらの悪意のあるアプリを特定することは、 DMA の施行前よりも難しくなるでしょう。 これまでは、このようなアプリやデベロッパの信頼性を測る信号はすべて App Store 一か所で見つけて分析できたため、悪意のある行為者を特定するための豊富なデータセットが確立されていました。 しかし今後は、 アプリの配布が**細分化**されるため、そのような信号は多数のマーケットプレイスに分散されることになります。 個々のアプリマーケットプレイスの事業者がどれほど責任を持っても（Apple は各事業者が悪意のある行為者を入念に監視することを期待しています）、**すべての当事者**（Apple を含む）にとって、悪意のある行為者の攻撃時に受け取る信号が少なくなるという事実は変わりません。 つまり、 すべてのマーケットプレイスにとって、 脅威を一掃するにあたっての効率が低下するのは避けられないことです。

これらには、 20 ページで紹介したアプリ（Apple が検出した、未検証のローンアプリに変貌したアプリ、ランサムウェア攻撃が埋め込まれていた成人向けチャットアプリ、違法なギャンブルアプリ）も含まれています。



宛先：**ティム・クック**
差出人：**iPhone ユーザー**
件名：**どうか Apple の iOS を閉じたままにしてください**
日付：**2024 年 1 月 27 日**

もし私が Google や Samsung のようなオープンソースのオペレーティングシステムが欲しかったのなら、最初からそちらを購入していました。どれほど強調しても足りないくらいですが、私が Apple のスマートフォンを購入し、所有している主な理由は、それが閉じられた iOS であり、iOS が Android よりも安全だからです。でも、門戸が開放されて安全でなくなるのなら、いっそのこと乗り換えた方がいいのかもしれません。どうかお願いです。Apple の iOS をこのまま閉じておいてください。

Apple は長年、非倫理的で悪質な海賊版アプリからデベロッパとアプリのエコシステムを保護することを重視してきました。このような「クラックされた」（不正に改ざんされた）アプリの中には、有料アプリを無料で利用できるように改ざんされたものや、コードを書き換えて作成者が意図していない改変が加えられているものもあり、苦労して作り上げたデベロッパから盗んで彼らの権利を侵害するだけではなく、ユーザーにも深刻なリスクをもたらします。こうした海賊版アプリは、マルウェアの媒介となることが多いのです。

Apple が DMA の要件に応じた変更を発表してから数週間経ちますが、その間も私たちは、代替アプリマーケットプレイスの構築に関心を持つ多くのデベロッパと協力してきました。彼らがどのようなものを構築するのか、私たちは非常に楽しみにしています。**しかし、中には、ほかのデベロッパの知的財産を盗んで海賊版アプリを配布するマーケットプレイスを構築するためだけに、これらの変更に関心を持っているように見える悪意のあるデベロッパがいるということもわかりました。**実際、あるデベロッパは、Apple との会議を予定し、DMA に対する Apple の変更について質問してきました。私たちは誠実に答えましたが、あとになってそのデベロッパが海賊版ソフトウェアの悪名高い配布元と関係があり、会話を違法に録音してオンラインに投稿していたことがわかりました。残念ながら、彼らの質問の目的は、iOS 上で海賊版アプリの公式マーケットプレイスを構築するために、EU で導入される Apple の今後の変更をどのように利用するのが最善の方法なのか探ることだったようです。

この 15 年間、私たちはこのような悪意のある行為者との戦いに多大な時間と技術を費やしてきました。彼らは、あらゆる機会を利用して Apple のデベロッパの知的財産を盗み、配布しようとしてきました。しかし、公証では、代替アプリマーケットプレイス上のアプリが他人の知的財産を侵害しているかどうかはチェックされません。つまり、海賊版の配布元が、名目上だけ知的財産侵害をチェックするマーケットプレイスを作るのを阻止し、捕まえるのはずっと難しくなります。**代替配布経路を声高に求め続けている人々の中には、この目的のためだけに代替経路を求める、このような悪質な配布元も混ざっています。**実際、Apple との会話を違法に録音したデベロッパに問い合わせたところ、彼らの言い分は、Apple が彼らに対して何らかの措置を講じて iOS 上での海賊版アプリの配布を防ごうとすることは DMA によって禁止されている、というものでした。

コンテンツおよびビジネスモデルのルールに関する決定

代替アプリマーケットプレイスは、コンテンツやビジネスモデルなどについてそれぞれ独自の市場基準を設けます。そして、Apple が常にユーザーを保護するために規制対象としてきた一部のコンテンツやビジネスモデルも、iPhone で利用可能になります。これが DMA の意図するものです。マーケットプレイスは、Apple が App Store で認めなかったようなアプリを提供できるようになります。例えば、Apple の新しいユーザー保護策では、アプリに成人向けコンテンツが含まれていないか、ギャンブルや暗号通貨取引に関するアプリが必要なライセンスを所持しているか、ユーザーが生成するコンテンツを含むアプリにコンテンツモデレーションポリシーがあるかといった点は評価しません。アプリが軽率な武器の使用を促していないかや、伝染病の流行などの国家的、世界的な危機から暴利を得ようとしていないかも検討しません。このような種類のコンテンツやビジネスを自社のマーケットプレイスで許可するかどうか、そしてそれに違反するアプリを自社のプラットフォームから排除するためのルールの実施にどれだけ投資するかは、各アプリマーケットプレイスが決定しなければなりません。

ユーザーとその子どもの保護に関する決定

代替アプリマーケットプレイスは、プラットフォームのユーザー、特に親と子どもに対して、どのような保護機能を提供するかも決定する必要があります。例えば、「**承認と購入のリクエスト**」では、子どもが親の承認を得ずに iPhone で商品を購入したり、iPhone にダウンロードしたりすることを防ぐことができます。また、Apple は、App Store のダウンロードページにアプリの年齢制限を目立つように表示しています。App Store では、アプリのリストに Privacy Nutrition Labels

[redacted]

Android デバイスでは、成人向けコンテンツ専用のアプリマーケットプレイスを含め、様々なポルノアプリやゲームをサイドローディングできます。

[redacted]

Apple は、主に匿名でのネット上のいじめを助長するために使用されているとして、App Store から複数のアプリを削除しました。そのようなアプリの 1 つは、中高生の子どもたちに「死ねばいいのに」という匿名のメッセージを送るために使われていました[11]。

[redacted]

Apple はこれまでにも App Review の際に、一見無害に見えても、メタデータに不正な意図を示す信号が含まれているアプリを特定してきました。例えば、あるアプリは最初は語学プログラムを装っていましたが、App Store に公開されたあと、無許可の賭場に変わることを示す信号が隠されていました。Apple はこれを見つけ、このアプリを却下しました。

[redacted]

Apple は、App Store 上の暗号通貨による取引に対し、ビジネスを行うすべての国と地域で適切なライセンスを取得することを義務付けており、暗号通貨取引所であるかのように見せかけてユーザーに詐欺行為を働くアプリや、合法的なアプリを装ってアプリを提出し、ライセンスを取得していない取引所として運営しようとするアプリを定期的に却下しています。

[redacted]

子ども向けの人気ゲームアプリの多くは、ゲーム内通貨、パワーアップアイテム、戦利品ボックスなどを含むアプリ内課金を取り入れています。「承認と購入のリクエスト」のような機能がなければ、子どもたちは親に気づかれることなく、こうした買い物に何百ドルも使ってしまう可能性があります。例えば、昨年、米連邦取引委員会は、あるゲームデベロッパに対し、「同社がダークパターンを使ってプレイヤーをだまして不要な買い物をさせ、保護者の関与なしに子どもたちに不正な課金をさせたという申し立てに対し、消費者への 2 億 4,500 万ドルの罰金の支払い」を命じたばかりです[12]。

[redacted]

Apple は、新型コロナウイルス感染症の世界的流行のような国家的危機から利益を得ようとするアプリを App Store で許可していません。世界的流行の最中、自宅待機命令にも関わらず内輪のパーティの開催を奨励したアプリを削除し、接触者追跡アプリによる公衆衛生機能を利用した広告販売を止めさせました。代替アプリマーケットプレイスでは、このようなアプリが許可されるかもしれません[13]。

を提示することもデベロッパに義務付けています。 このラベルは、 ユーザーがアプリをデバイスにダウンロードする**前**に、 アプリがどのようにユーザーのデータを収集および追跡するかをユーザーに説明するものです。 このような機能はいずれも、代替アプリマーケットプレイスでは必須ではありません。 マーケットプレイスは、 類似する保護機能を提供することも、 提供しないことも選択できます。

ユーザーのプライバシー保護に関する Apple の取り組みは、 アプリがどのようなデータをユーザーから集め、 どのようなデータをユーザーに紐づけているかを、 その Privacy Nutrition Labels で宣言することを義務付けていることにも表れています。 ほかのプラットフォーム上にある既存のアプリマーケットプレイスでは、 これほどまで明確にトラッキングについて開示することは義務付けられていません。

Apple は、 代替アプリマーケットプレイスがユーザーのセキュリティ、 プライバシー、 安全性の保護に多大な投資を行うことを期待していますが、 それを保証することはできません。 それぞれのビジネスモデルに応じて、 ユーザーの保護機能の開発に対する動機は異なる可能性があります。 例えば、 ユーザーデータの収集と販売にもとづくビジネスモデルを持つ代替アプリマーケットプレイスであれば、データの収集と利用についてユーザーに必要な事項を伝え、 承諾を得ることを促す Privacy Nutrition Labels のような機能を提供する商業的動機はないでしょう。 その結果、そのマーケットプレイスのユーザーは、 自分のデータのプライバシーを保護するための選択肢について詳しく知らないままになります。 そのようなアプリマーケットプレイスは、 Apple が App Store でユーザーのために続けているような、 ユーザーのプライバシーを保護する革新的な新しい方法に投資し続ける動機もないはずです。

顧客への決済サポートに関する決定

2021 年、 米国連邦取引委員会は、 ある会員制オンライン学習ツールに対し、 最初の無料トライアル期間が終了したあと、 無期限に課金されることを消費者に適切に開示せず、 時間のかかるわかりにくい手続きを経ないと解約できないようにしていたとして、 1,000 万ドルの罰金を科しました。 現在、 Apple のサブスクリプションツールでは、 ユーザーがワンクリックでこのようなサブスクリプションを解約できるようになっていますが、 ほかのマーケットプレイスではこのようなサービスは提供されていないかもしれません[14]。

ユーザーに決済サポートを提供するかどうかは、 個々のマーケットプレイス、 アプリデベロッパ、 代替決済業者に委ねられます。 素晴らしい消費者保護策を提供する事業者もいれば、 そうでないものもいます。 しかし、 いずれの場合でも、 Apple は、 サブスクリプションの罠にはまるユーザーや、 だまされて意図しない購入をしてしまうユーザーを助けることができなくなります。 また、 Apple の多数の AppleCare エージェントは、 Apple が管理していない決済システムのサポートは提供できなくなります。 このような選択肢は、 ユーザーにとって非常に複雑なものになります。 App Store で入手できるアプリからデジタル商品やサービスを購入したユーザーは、 当然ながら、 引き続き Apple に問い合わせてサポートを受けられると考えますが、 デベロッパが別の決済ソリューションを選択していれば、 Apple はユーザーをサポートできないのです。 このため、 ユーザーはこうした取引に関与する前に、 できる限り多くの情報を入手しておくことが重要です。 Apple は、 情報提供を含め、 代替決済手段を利用したユーザーの取引をサポートする役割を果たしますが、 そのソリューションを導入しているサードパーティも同様にその役割を果たします。 そうでない場合は、 ユーザーはより厳しい状況に陥ります。

サイバー犯罪の新たな動機

今回の変更によって、 新たな競争の機会がもたらされますが、 悪意のある行為者にとって利益となる新たな市場が生まれることも避けられません。 iPhone はクラス最高のセキュリティとプライバシー保護機能を備えているため、 悪意のある行為者は長らく iPhone へのアクセスを手に入れるのに苦戦してきました。 プラットフォームセキュリティに対する Apple の総合的な取り組みにより、 iOS エ

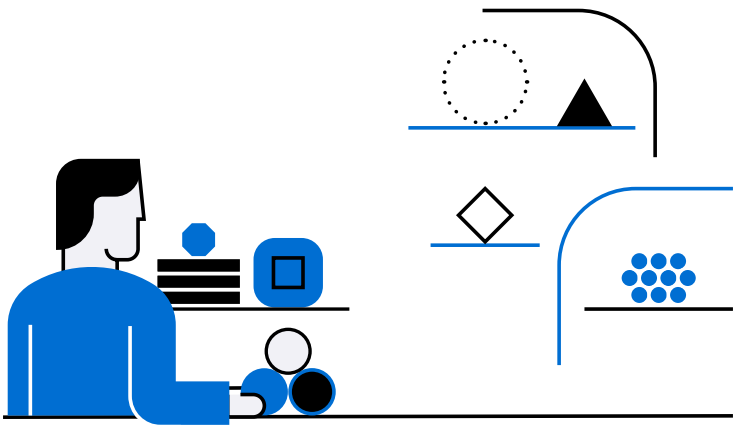
コシステムは商用マルウェアの被害を免れてきました。 実際、 サイバー犯罪者は、 iOS で消費者向けの広範なマルウェア攻撃に成功したことが一度もありません。 プラットフォームセキュリティに対する Apple の総合的な取り組みのもとでは、 大半のマルウェア感染の試みが徒労に終わることを、 犯罪者は学んでいます。 悪意のあるソフトウェアの作成と配布には、 多大なリソースが必要です。 iPhone には強力な防御策があり、 こうした試みは投資に見合う利益が得られないため、 デバイスはさらに攻撃対象として狙われにくくなります。

同様に、 Apple が予防的な監視を続けていることも、 継続的な詐欺が iOS で足がかりを得ることをより困難にしています。 例えば、 Apple では、 正規の投資アプリ上でユーザーをだまして詐欺の証券口座に投資資金を入金させる「豚の屠殺」 詐欺など、正規アプリが詐欺行為に悪用されるケースを防ぐための措置を講じています。 そのような詐欺が判明したら、Apple は正規アプリのデベロッパに連絡し、 そのアプリでの詐欺の拡大を食い止めます。 こうした措置を講じることでも、 iOS アプリは、 そのような詐欺の標的として狙われにくくなっています。

EU での iPhone への新たな変更により、 これまでは得られる利益が比較的少ないとして、 iOS やそのユーザーを狙おうとしていなかった悪意のある行為者にとって収支の計算が変わることになります。 今回の変更に伴い、 デベロッパにとって新たな選択肢が増えると同時に、 詐欺師やサイバー犯罪者が新たに入り込みやすくなり、 潜在的な脆弱性が生じることにもなります。 悪意のある行為者がますます工夫をこらすほど、 脅威は高度になります。 多くはソーシャルエンジニアリングを利用してユーザーをだまし、 最も機密性が高い個人的な情報を盗み出します。 その手口は、 どれほど知識があるユーザーでも引っかかる可能性があります。 代替アプリのダウンロードチャネルを介して iPhone ユーザーにアクセスしやすくなることで、 投資に対する利益が大きくなり、 iPhone を標的にすることは、 全体として比較的儲かることになります。 Apple が自社のコマースシステム外での不正な過大請求をテストできなくなったことや、 マーケットプレイスの信号が細分化されたことなど、 上述したすべての理由により、 詐欺やその他の悪意のある行為者を見つけ出すには、 より時間がかかるようになります。 また、 代替アプリマーケットプレイスが Apple と同様に迅速な対応をとることは保証できません。 その結果、 ユーザーが潜在的な悪意のある行為者にさらされる時間は長くなり、 そのような悪意のある行為者がユーザーをだます巧みな方法を見つける余地も与えてしまう可能性があります。

宛先 : **ティム・クック**
差出人 : **iPhone ユーザー**
件名 : **サードパーティアプリ**
日付 : **2023 年 2 月 20 日**

iPhone の iOS は Android よりもはるかに安全なので、とても気に入っています。 選択肢が提供されても、サードパーティアプリをダウンロードできないようにしてほしいです。 設定に「許可しない」というチェックボックスを作ったらどうでしょう？



このため、悪意のある行為者が新しい手口を編み出し、iOS ユーザーを狙う新たなマルウェアを開発する動機が生まれます。悪意のある行為者は、アプリを配布する代替アプリマーケットプレイスを次々と変えながら、複数のマーケットプレイスで同じ詐欺を何度も繰り返し使う機会を手にします。あるいは、軽微な変更を加えれば同じマーケットプレイスでも、その可能性があるかもしれません。こうしたすべての要因が相まって、悪意のある行為者が iOS で投資から利益を得られる可能性が高まり、さらに悪意のある開発が進みます。おそらく最大の懸念材料は、iOS ユーザーを標的とするツール、サービス、インフラの構築への犯罪目的の投資にこの新たな動機が加わることで、App Store だけを利用するユーザーにまで攻撃が波及し、そのコストが低下するリスクがあるということです。

ここで明確にしたいのは、Apple は、自社のデバイスとシステムに何重ものセキュリティを組み込んでいるということです。Apple は、このようなリスクを低減するために今後も最善を尽くします。しかしそれでも、ここで述べたような理由でリスクは高まります。

Apple は、iPhone でセキュリティ、プライバシー保護、安全なユーザー体験を提供できるよう取り組んでいます。この取り組みは、DMA を遵守するための変更をすでに実施した今も続いており、EU 域内のユーザーを保護するためにあらゆる対策を講じています。EU 域内での体験は、Apple がその他の地域で提供できるものと同じにはならないとしても、これらの新しいツールやプロセスが、今回の変更で生じるリスクへの対抗手段となります。

公証は、ランサムウェアや消費者向けスパイウェアといったマルウェアを含む悪意のあるアプリにユーザーがさらされ、意図する以上の個人情報が漏えいしたり、自身の安全性が危険にさらされたりすることを防ぎます。アプリインストールシートは、ユーザーがダウンロードするアプリについて正確な情報を受け取れるようにします。これにより、ユーザーがだまされて、偽のアプリや条件を理解していないアプリをインストールしてしまう可能性が低くなります。代替アプリマーケットプレイスに継続的な監視を義務付けることで、悪意のあるアプリが野放しになることを阻止できます。代替決済システムに関する情報シートは、過大な請求金額を支払わせることを目的とする不正や詐欺に注意しなければならないことをユーザーに伝えます。

このような保護策によって、ユーザーは引き続き充実した、安全で透明性の高い iPhone 体験を得ることができ、自分のデータをコントロールすることができます。また、これによって iPhone は、今後も EU で現在入手できる中で最もセキュリティとプライバシーが保護された、安全なスマートフォンであり続け、ユーザーが Apple に期待している通りの素晴らしい製品を提供します。

参考文献

1. *Survey: Nearly half of Android users consider switching to iPhone over security and privacy concerns,* 9to5Mac (Aug. 16, 2022), https://9to5mac.com/2022/08/16/android-users-consider-switching-iphone/.

2. *App Store developers generated $1.1 trillion in total billings and sales in the App Store ecosystem in 2022,* Apple (May 31, 2023), https://www.apple.com/newsroom/2023/05/developers-generated-one-point-one-trillion-in-the-app-store-ecosystem-in-2022/.

3. For more information, *see Apple announces changes to iOS, Safari, and the App Store in the European Union,* Apple (Jan. 25, 2023), apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/.

4. *App Store stopped more than $2 billion in fraudulent transactions in 2022,* Apple (May 2023), https://www.apple.com/newsroom/2023/05/app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/.

5. *2022 App Store Transparency Report,* Apple (2023), https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf.

6. Steve Jobs recognized this very issue in 2007. *See* Steve Jobs, *iPhone SDK Letter (Oct. 17, 2007), available at* https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter.

7. *Threat Intelligence Report 2023,* Nokia, https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/.

8. *See* European Consumer Centre Germany, *Tips against subscription traps on the internet,* https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html.

9. Stuart Madnick, *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase* (Dec. 2023), https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

10. *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading,* Apple (Oct. 2021), at 14.

11. Elizabeth Cassin, *Sarahah: Anonymous app dropped from Apple and Google stores after bullying accusations,* BBC (Feb. 25, 2018), https://www.bbc.com/news/blogs-trending-43174619.

12. *FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges,* FTC (Mar. 4, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making; *Kids Mobile Gaming Report: More Than Two-Thirds of Parents Worry Kids Overspending on In-App Purchases,* Sell Cell (June 5, 2020), https://www.sellcell.com/blog/more-than-two-thirds-of-parents-worry-kids-overspending-on-in-app-purchases/.

13. *App promoting private parties amid COVID-19 removed from Apple App Store,* Bus. Insider (Dec. 30, 2020), https://www.businessinsider.in/tech/apps/news/app-promoting-private-parties-amid-covid-19-removed-from-apple-app-store/articleshow/80020920.cms; Khadeeja Safdar & Kevin Poulsen, *Google, Apple Struggle to Regulate Covid-19 Tracing Apps,* Wall St. Journal (June 5, 2020), https://www.wsj.com/articles/why-google-and-apple-stores-had-a-covid-19-app-with-ads-11591365499.

14. *Children's Online Learning Program ABCmouse to Pay $10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices,* FTC (Sept. 2, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing.