参考資料19－３

高まるプライバシー侵害のリスク

デジタル市場法（DMA）のOS機能へのアクセス規定の悪用によるプライベートな情報の漏洩の危険性

2024年12月

Appleはこれまでに

250,000

を超えるAPI（アプリケーションプログラミングインターフェイス）を開発してきました。APIは、Appleが開発した優れた機能をデベロッパが利用できるようにするためのツールです。

Appleは、ユーザーのためにすばらしいアプリを開発しているデベロッパの力になりたいと考えています。

新しい製品や機能に関して、Appleのアプローチは一貫しています。Appleはイノベーションを通じてユーザーを魅了する体験を生み出しており、その過程のあらゆる段階で、ユーザーのプライバシーとセキュリティの保護に取り組んでいます。Appleはまた、デベロッパのコミュニティに、Appleのデバイスですばらしいアプリを開発するための様々なツールやテクノロジー、リソースを提供しており、その数は着々と増え続けています。Appleは、デベロッパが特別なものを作り出し、それぞれのビジネスで非常に大きな成功を収めるために利用できる、優れた製品や機能の開発に何十億ドルもの投資を行ってきました。

デベロッパに対するこのコミットメントは、AppleのDNAの根幹をなすものです。私たちは、デベロッパとAppleの双方のために、Appleを含むあらゆる企業がユーザーの個人的なデータにアクセスすることなくすばらしいユーザー体験を可能にするアプローチを先導してきました。これはユーザーからの信頼の土台であり、ユーザー、デベロッパ、そしてAppleの成功の一因でもあります。

プライバシーを保護しながらOS機能へのアクセスを提供することで、デベロッパに成功をもたらすAppleのコミットメント

Appleのユーザーには、デベロッパが、自身のデバイスの重要な部分にどのような理由でアクセスし、それを何のために、いつ使用するのかを、完全に、かつ透明性のある方法で当然に理解する権利があります。

マイク

Appleは、デベロッパにiPhoneのマイクへのアクセスを許可し、それによってデベロッパがユーザーの発言や様子を知ることができる場合には、常にユーザー側がコントロールできるようにしています。デベロッパはユーザーにマイクへのアクセス許可を求める必要があり、そのアクセスによる音声の録音が行われる際にユーザーに知らせる必要があります。

Touch ID

2013年に導入されたTouch IDは、広く普及して使いやすい、初のスマートフォンへの生体認証によるアクセスのためのテクノロジーです。Touch IDが使用される場合、ユーザーの指紋データはiPhoneのSecure Enclaveに保存されるので、Appleでさえアクセスすることはできません。2014年には、デベロッパ向けにTouch IDのAPIがリリースされ、銀行アプリやゲームアプリなどのデベロッパは、ユーザーのセキュリティとプライバシーを保護しながら、このテクノロジーを利用できるようになりました。

しかし最近になって、**EUがOS機能へのアクセスに対する新しいアプローチを採用したことでユーザーが危険にさらされる**具体的な例が見られるようになっています。この新しいアプローチにより、ユーザーは自分のデバイス、そして最もセンシティブなデータを、ユーザーのプライバシーを侵害した実績がある企業に開示せざるを得なくなるのです。

人々に愛されているApple製品の魔法のような体験は、箱から出してすぐに使える製品を作り出すためにAppleが費やした時間、才能、資本によって実現しています。

こうしたプロセスはイノベーションを阻害することになるでしょう。本来、企業は、自社のアイデアを競合他社に提供させられることなく、自社製品が連携して機能することでユーザーに恩恵をもたらすよう、互いに競い合うことができなければならないからです。Apple はこのような方法で、自社のイノベーションをあらゆる他社に対して共有することを強いられる唯一の企業です。そして、これらの他社にはユーザーのプライバシーへコミットしていない企業も含まれています。

OS機能へのアクセスのリスク

2024年の前半、「OS機能へのアクセス」の概念を法律として規定したデジタル市場法が施行されました。その基本的な考えは、公平な競争の場を確保するため、デベロッパがAppleと同等にiOSおよびiPadOSのツールにアクセスできるようにするべきだというものです。Appleは常に、公平な競争の場の重要性を信じ、OS機能へのアクセスの機会を創出し続けていますが、それをユーザーにとって正しい方法で行うことが極めて重要であることに変わりはありません。**そのため、Appleはデベロッパに機能へのアクセスを提供する際には必ず、ユーザーを保護し続けながらこれを行うにはどうすればよいか、慎重に考慮しています。**私たちは誰もが、これに伴うリスクを知っています。適切な保護を行わないまま、ユーザーのデバイスの一部に第三者がアクセスできるようにすれば、悪意を持った攻撃者によってユーザーの個人情報が盗まれたり暴露されたりするおそれがあるのです。

デバイスがかつてないほどパーソナルなものとなっている現在では、ユーザーの保護を私たちのあらゆる活動の中心に置くことが極めて重要です。Appleはユーザーのプライバシーとセキュリティを保護するソフトウェアの設計に多大な努力を払っています。私たちは、EUによって制定され、Appleが支持しているデータ保護法の高度な基準を満たさないデータ慣行を持つ一部の企業が、センシティブなユーザーデータにアクセスするために、デジタル市場法のOS機能へのアクセス規定を悪用しようとする可能性を懸念しています。

世界中のデータ取得に貪欲な企業が、OS機能へのアクセスを武器として使用するおそれがあります

Appleはデジタル市場法の遵守に努める一方で、OS機能へのアクセスに関して受け取った個々のリクエストについて慎重に精査しています。Appleの懸念の例を一つ挙げると、MetaはAppleの数々のテクノロジーに対して潜在的に非常に広範囲なアクセスにつながりうる15件以上のリクエストを行っており、もしもこれらを要求通りに認めれば、Appleのユーザーがデバイスに期待する個人データの保護が損なわれると考えられます。

Metaからアクセスのリクエストがあった機密性の高いテクノロジーの例

Appleに対してOS機能へのアクセスのリクエストをどこよりも多く行っている企業がMetaです。多くのケースで、Metaはユーザーのプライバシーとセキュリティに対する懸念が生じるような方法で機能を改変しようとしています。また、それらはMetaスマートグラスやMeta Questなど、Metaの外部デバイスの実際の使用にはまったく関係がないように思われるものです。

- AirPlay
- App Intent
- Apple通知センターサービス
- CarPlay
- ユーザーの全Appleデバイスとの接続性
- 連係カメラ
- Bluetooth接続デバイス
- iPhoneミラーリング
- メッセージ
- Wi-Fiネットワークとプロパティ

もしもAppleがこれらのリクエストにすべて応えなければならないとしたら、Metaは**Facebook**、**Instagram**、**WhatsApp**で、ユーザーのデバイス上のメッセージやEメールをすべて読んだり、通話の発信や受信をすべて確認したり、ユーザーが利用したすべてのアプリを追跡したり、写真、ファイル、カレンダーのすべてのイベントを閲覧したり、パスワードをすべて記録するなど、様々なことができるようになるでしょう。**これらは、ユーザーにできる限り強力な保護を提供するために、Appleであってもアクセスしないことを選択しているデータです。**

他社は、ユーザー自身が自分のデバイス上でデータをコントロールできるようにすることに関して、Appleと同じコミットメントを果たしていない可能性があります

Appleが個人データを収集するのは、製品またはサービスの提供にどうしても必要な場合に限られます。また、アプリがセンシティブな情報にアクセスする前にユーザーの許可を求め、ユーザーがコントロールできるようにしています。アプリがマイクやカメラ、ユーザーの位置情報など、慎重な取り扱いを必要とする特定の機能にアクセスする場合には、明確に通知を行います。Appleは、ユーザーのプライバシーを保護し、データの収集を最小限に抑えるため、できる限りデータをAppleのサーバに転送せず、デバイス上で処理しています。他社は、ユーザー自身が自分のデバイス上でこれらデータをコントロールできるようにすることに関して、Appleと同じレベルのコミットメントを果たしていない可能性があり、また、ユーザーの情報を自社のサーバに転送しようとする可能性があります。転送すれば、個人のプライベートなデータを組み合わせ、プロファイリングを行い、それを収益につなげることができるからです。

一般データ保護規則（GDPR）は、プライバシーに関してすべての企業が遵守すべき厳格なルールを定めており、Appleは常にこれを支持してきました。デジタル市場法はこのルールを回避できるようにすることを意図して作られたわけではありません。しかし、結果的に、プライバシーの侵害で再三にわたり罰金を科せられているMetaのような企業が、ユーザーのデバイスとユーザーの最もパーソナルなデータに自由にアクセスできるようになる可能性があります。もしもAppleが、その企業が保護する能力を持たないセンシティブなテクノロジーへのアクセスを許可するよう強制されれば、セキュリティリスクは甚大なものとなり、緩和することは事実上不可能となるでしょう。

メッセージ

Metaは、ユーザーのメッセージを送信したり読んだりすることができるよう、ユーザーのSMSやiMessageの機能へのアクセスを求めています。これとは別に、Metaはユーザーのメッセージ履歴へのアクセスも求めています。プライベートなコミュニケーションへのアクセスは、常に完全にユーザーがコントロールできるようにしておく必要があります。

AirPlay

Appleは長年、AirPlay経由でコンテンツを送信できるアプリに対応してきました。Metaはユーザーのテレビやスマートスピーカーへの直接アクセスを求めていますが、これにより新たなプライバシーやセキュリティに関する問題が生じるばかりか、ユーザーの自宅に関するデータも提供することになります。

App Intent

App Intentはユーザーが自分のデバイス上でアプリや機能の操作方法を管理するための新しいフレームワークです。Metaは、App Intentに対してほかのアプリから提供されるすべてのデータにアクセスすることを求めています。そのようなアクセスを認めれば、Metaがユーザーのデバイスを完全にコントロールできるようになる可能性があります。

例えば、ユーザーがSiriに、WhatsAppで受信した最新のメッセージを読み上げるように頼むと、Metaやその他の第三者企業はメッセージの内容に間接的にアクセスできることになります。それに伴うリスクの全容を理解できる人はいないのではないでしょうか。

CarPlay

Metaは、ユーザーのデバイスからiOSのアプリを起動し、別のコンテンツを表示できるようにするため、CarPlayの機能へのアクセスを要求しています。これによってユーザーによるコントロールができなくなると、ユーザーの選択が損なわれる可能性があります。

OS機能へのアクセスに対するAppleのコミットメント

Appleはすべてのリクエストの精査に取り組み、プラットフォーム上でプライバシーとセキュリティを保護する必要性を考慮した上で、可能な場合にはそれらのリクエストを実装します。それらのリクエストが、ここで示したような深刻なリスクを引き起こす場合でも、センシティブなユーザーデータの保護とデバイスのセキュリティ保持を継続しつつ一段と豊かな体験が可能となるよう、プラットフォームの強化を図ることを検討しています。Appleのコミットメントは、すべてのリクエストを速やかに評価しそれらに対応することによって、すべてのデベロッパに対してプラットフォームの完全性が保たれ、センシティブなユーザーデータが保護されるよう徹底することです。

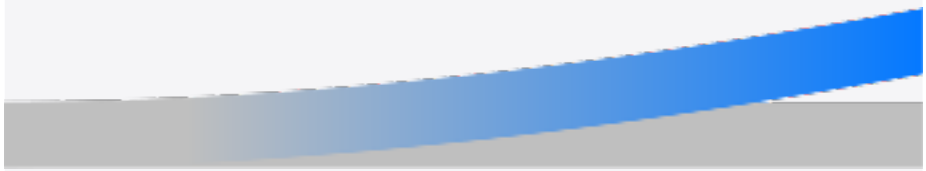
OS機能へのアクセスのリクエストに対するAppleの対応

リクエストの提出
EU域内のアプリのデベロッパは、iOS、iPadOS、iPhone、iPadに内蔵されているハードウェアやソフトウェアの機能とのOS機能へのアクセスをリクエストすることができます。

初期評価
Appleはリクエストの初期評価を行い、リクエストがデジタル市場法の第6条(7)の範囲に含まれるかどうか検討します。

暫定的なプロジェクト計画
Appleはリクエストされた機能に関する効果的な、OS機能へのアクセスのソリューションの設計を開始します。

開発とリリース
Appleは効果的なソリューションが実現可能で、デジタル市場法の下で適切である場合に限り、そのソリューションを開発します。



リクエストが提出されたら、Appleはそれぞれのリクエストの評価を行い、進捗状況を随時デベロッパに報告します。そのプロセスのいずれかの段階で、効果的なOS機能へのアクセスのソリューションの設計が実現不可能、またはデジタル市場法の下で不適切であると判断した場合には、その旨をデベロッパに伝達します。

プライバシーとセキュリティを高い水準で保護していることで、Appleは他社と一線を画しています。

Appleのユーザーはそれを信頼しています。Appleは、ユーザーとデベロッパのどちらにも、安全にiPhoneの優れた特長や機能を利用してほしいと願っています。

Appleはユーザーのプライバシーとセキュリティに対する根本的なコミットメントを決して捨て去りません。欧州委員会には、GDPRを尊重する形でOS機能へのアクセスの要件を実現しようと努めてもらえることを信じています。