信頼できるアプリストア：セキュリティと完全性の保護

2024 年 2 月

作成者：
ヘザー・ウェスト|シニアディレクター
+1 202.344.4597
HEWest@Venable.com

ティム・マクジフ |プロジェクトマネージャー
+1 202.344.4365
TCMcGiff@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

目次

エグゼクティブ・サマリー **3**

はじめに **4**

DMA アプリストア規定 5

モバイル脅威エコシステム 6

主要なモバイル脅威 6

サードパーティアプリストア 8

サイドローディング 9

エンドユーザー責任の欠如 10

グーグルやアップルはいかにこれらの脅威と戦うのか 11

DMA 施行のロードマップ 12

結論 14

エグゼクティブ・サマリー

欧州連合（EU）は、デジタル市場に対して新しい政策と規制を導入する際には、アクセス、プライバシー、セキュリティと並行して経済学的に考慮すべき事項とのバランスを慎重に取る必要があります。 残念ながら、デジタル市場法（DMA）のモバイルアプリストアの規定によって、携帯電話のエコシステムを非常に信頼性が高く回復力のあるものにしてきた基本的なセキュリティコントロールが損なわれる可能性があります。 Center for Cybersecurity and Policy & Law は、アプリをインストールする方法が広がることはユーザーを圧倒するものであり、悪意のある者にそれらを悪用するための多く道を開いてしまうことを懸念しています。 これは、ユーザーを保護するためにできることが何もないことを示唆するものではありませんが、これまでには必要のなかった方法で、保護されることを確実にするために、企業とユーザー自身も行動を取ることが求められます。 本稿では、EU 市民、そのデバイスおよびデータに対する潜在的なリスク、ならびにそれらのリスクを軽減するためのアプローチを概説します。 最後に、規制当局と政策立案者が、ユーザーがモバイルエコシステムを信頼し続けられるようにするための推奨事項と、またユーザーと企業に対する潜在的なセキュリティ上の影響を軽減する方法について説明します。 本稿が、市民のセキュリティとプライバシーを保護しながら、自国のデジタル市場で競争を促進しようとしている他の国々にも見識を提供するものであることを願っています。

Center for Cybersecurity and Policy & Lawについて

Center for Cybersecurity and Policy & Law は、政府、民間産業、市民社会にセキュリティ脅威をより適切に管理するための実践とポリシーを提供することにより、世界中のサイバーセキュリティを強化することを目的とする独立した組織です。 Venable LLP（脆弱な顧客ケアポリシー）のサイバーセキュリティサービスグループ内の 501 (c)(6)非営利団体として 2017 年に設立された当センターは、政策の専門知識をグローバル、国家、および地域レベルにおける招集力と組み合わせて、業界のリーダーと政策立案者を結びつけ、実際に成果を生み出すための連携とイニシアチブの立ち上げを行っています。 センターでは、コンセンサス指向のリスク管理ベースのアプローチを適用し、デジタルインフラストラクチャと情報システムのセキュリティ保護において最前線にいる人々の視点と実践から引き出された実用的なソリューションと政策提言を促進することにより、サイバーセキュリティをめぐる複雑さを解明し、混乱を解消することを目指しています。

はじめに

ますます繋がりが進む世界では、携帯電話のアプリを使用して、サービス、情報、リソースの豊富なエコシステムとやり取りすることがよくあります。 携帯電話の利点は広く認識されてい[1]ます。携帯電話は、世界への窓口であり、私たちの健康を見守り、友人と共有し、商品を購入し、サービスを管理します。 そのため、私たちはモバイルアプリに多くの時間を費やしています。1 日に 4〜5 時間、またはそれ以上の時間です。[2] デバイスとアプリの安全性と信頼性を維持することが重要です。

調査によると、米国内では、18〜34 歳の消費者の 81 %が、所有している接続デバイスが安全であると感じていることが示唆されています。[3] これらのエコシステムを保護するためのオペレーティングシステム開発者とアプリストアの努力のおかげで、人々にはモバイルデバイスとアプリを信頼する正当な理由があります。

2021 年に発行したレポート「 *モバイルの未来：モバイルセキュリティとプライバシーの継続的改善への道筋* 」では[4]、業界、学界、市民社会の 23 名のサイバーセキュリティの専門家とモバイルセキュリティについて話し合い、「モバイルデバイスに対する新しい脅威が発生し続けている一方で、現在実装されている保護は一般的にサイバーセキュリティの他の分野よりも優れている」ことがわかりました。[5] フォーカスグループで得られたコンセンサスは、モバイル環境がオペレーティングシステム（OS）とアプリストアレベルで組み込まれたセキュリティとプライバシー保護の恩恵を受け、ユーザーが自分自身を保護する責任を大幅に軽減しているというものでした。

わずか 3 年前のこの論文は、評判の良いオペレーティングシステム開発者と信頼できる公式アプリストアによる現在のモバイルアーキテクチャとセキュリティ機能に考慮し書かれました。 過去 10 年間でモバイルエコシステムは確実に安全になりましたが、欧州連合（EU）の競合に焦点を当てた DMA（デジタル市場法）におけるアプリのインストールに係る規定は、このセキュリティの進歩を継続させるのではなく、エコシステムを後退させる[6] 可能性があります。 私たちは、このセキュリティの進歩を確実に維持するために協力する必要があります。

オペレーティングシステムが追加のソースからのアプリのインストールを許可することを要求する DMA の規定は、ユーザーにとって圧倒させ負担となる可能性があり、モバイルデバイス管理を実装する企業管理者にとっても困難であり、悪意のある者に新たな道を開いてしまう可能性があります。 これらのリスクを軽減するには、よりオープンなエコシステムに伴うリスク

---

[1] https://www.pewresearch.org/internet/2019/03/07/majorities-say-mobile-phones-are-good-for-society-even-amid-concerns-about-their-impact-on-children/

[2] Data.ai 2 via Techcrunch は、モバイルユーザーがアプリに 1 日 4〜5 時間を費やしていると報告しています- リンク

[3] https://staysafeonline.org/wp-content/uploads/2022/07/Cybersecurity-Awareness-Month-2020-Results-Report.pdf

[4] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[5] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[6] デジタル市場法の6 テキストは、https://eur-lex.europa.eu/eli/reg/2022/1925 でご覧いただけます 。

を軽減するための合理的なアプローチをとりながら、DMA の目的とのバランスをとるためにモバイルオペレーティングシステムのゲートキーパーをサポートする必要があります。

本稿では、DMA におけるアプリストアの規定、これら規定によって悪化するモバイルエコシステムの脅威を簡単に概説し、ファーストパーティアプリストアとモバイル OS の所有者が過去にこれらの脅威とどのように戦ってきたかを簡単に検証します。 本稿では、準備ができていないエンドユーザーがモバイルエコシステムとそのデバイスのセキュリティのために、突然困難な立場に置かれないようにするために、EU 加盟国がサポートすべき様々な DMA 施行に際してのアプローチについて論証します。

DMA の文書は、技術的および契約上のメカニズムの両方を含む、ユーザーを保護するための潜在的な手段に言及しています。 さらに、立法者と規制当局は、アプリレビュー、強化されたマルウェア保護、透明性に係る要件、モバイルデバイスのオペレーティングシステムに組み込まれた権限とセキュリティモデルの調整を通じて、ユーザーを保護するため、オペレーティングシステム開発者の役割をサポートする必要があります。 活気に満ちた革新的なモバイルエコシステムを確保するために協力できるようにすることが重要です。 私たちは、政策立案者に、DMA の実施に際してセキュリティの重要性を強調するとともに、ゲートキーパーとしてコンプライアンスの確立に努めるよう求めます。

DMA アプリストア規定

2024 年 3 月までに、「コアプラットフォームサービス」を運営する「ゲートキーパー」の定義に該当する企業は、自社のアプリストアおよびモバイル OS とサードパーティのアプリストア及びアプリとのアクセスに関連する DMA の条項の対象になります。 ゲートキーパーとは、欧州委員会が指定したように、欧州市場に大きな影響を与え、ビジネス（アプリ開発者など）とエンドユーザー（アプリをインストールしている携帯電話のユーザーなど）の関係を仲介するサービスを提供する企業です。[7] DMA の目的は、小規模な欧州企業が、市場でより「固定した」地位を築いている可能性のある企業と競争しやすくすることです。

DMA の条項は、モバイルオペレーティングシステムがゲートキーパー以外のアプリストアからまたは他の方法を介してアプリをインストールすることを許可すること、またオペレーティングシステムがファーストパーティおよびサードパーティアプリそれぞれに同じシステムアクセスとツールを許可することを要求します。

これらの条項の主な内容は次のとおりです。

- *セクション 6.4 ：ゲートキーパーは、オペレーティングシステムを使用または相互運用するサードパーティソフトウェアアプリケーションまたはソフトウェアアプリケーションストアのインストールと効果的な使用を許可し、技術的*

[7] 公開時点で、Apple の iOS オペレーティングシステムと Google の Android オペレーティングシステムは、コアプラットフォームサービスと見なされています。 マイクロソフトの Windows デスクトップ PC オペレーティングシステムもコアプラットフォームサービスと見なされていますが、この文書の範囲外です。https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

- *セクション 6.7 ：ゲートキーパーは、サービスプロバイダーおよびハードウェアプロバイダーに対し、オペレーティングシステムまたはバーチャルアシスタントを介してアクセスまたは管理されるのと同じハードウェアやソフトウェア機能を、無料で、効果的な相互運用を許可し、相互運用性を目的としたアクセスを許可するものと**する**[...]。 さらに、ゲートキーパーは、[...]同じオペレーティングシステム、ハードウェアまたはソフトウェア機能との効果的な相互運用性、およびこれらの機能がオペレーティングシステムの一部であるかどうかにかかわらず、そのようなサービスを提供する際にそのゲートキーパーが利用可能または使用する相互運用性を目的としたアクセスを許可するものと**する**。*

これらの DMA 規定が、他の欧州連合の法律と組み合わされると、ゲートキーパーに対し、モバイルデバイスへのサードパーティアプリやアプリストアのインストールを容易にし、モバイルユーザーによるサードパーティアプリストアへのアクセスを容易にし、サードパーティデベロッパーとアプリに、ゲートキーパーが現在享受しているモバイル OS と同じアクセス、相互運用性、機能を付与することを効果的に義務づけます。

これらの規定に加えて、モバイルエコシステムの「開放」によってもたらされるセキュリティとプライバシーのリスク**も**認識**されていることが**強調**されて**いますが、あまり強調されていないセキュリティ上の注意事項があります。 DMA の法令前文 50 は、サードパーティアプリやアプリストアに提供された追加アクセスが、ユーザーとデバイスのセキュリティを損なう**ものであってはなら**ないと述べています。 ただし、DMA は、オペレーティングシステムがアプリへのアクセスを差別化または抑制する方法を**考慮し**、オペレーティングシステムがモバイルデバイスとユーザーを**どのように**保護すること**を**期待しているかについては説明していません。 慎重に検討せずに**施行**された場合、DMA の上記の**条項**は現在のモバイル脅威エコシステムを悪化させる可能性があります。

モバイル脅威エコシステム

モバイルマルウェアとの闘いは、世界中のモバイル OS 開発者や組織にとって**の**優先事項です。 その保護セキュリティアーキテクチャが成功しているにもかかわらず、モバイルデバイスは、その**どこでも使われるという性質**、一日を通して私たち**と行動を共にするという**事実、そしてそれらが私たちの生活の中核部分であり、多くのデジタル**なやり取りにおける中心的な役割を担っている**ため、魅力的な標的になります。

オペレーティングシステムがクローズド**な**エコシステムよりむしろ真のプラットフォームになるにつれて、モバイルの脅威も増加しており、モバイル OS 開発者と評判の良いアプリストア**運営者**は、**これまで** OS アーキテクチャ設計の選択を通じアプリとデータのサンドボックス化、アプリのモデレーション、アプリの機能性と品質チェック、そしてますます細分化された権限モデルなど、脅威を抑制するために取り組んできました。 CrowdStrike の 2019 年モバイル脅威状況レポートによると、モバイルプラットフォームはますます犯罪者の標的になっており、スキルの低い攻撃者**も今や**モバイルデバイスへのアクセスを簡単に試みることができる概念実証モバイルマルウェアにアクセスできるようになってい**ることがわかりました**。[8]

---

[8] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

悪意のある者もチャンスを狙う者も、これらの非常に人気のあるプラットフォームを活用する方法を模索しているため、モバイルエコシステムには無数の脅威が存在します。。 ゲートキーパーや政策立案者が DMA を実装する際に、これらの脅威を最小限に抑える方法を念頭に置く必要があります。

悪意のあるアプリは、機密性の高い保存データやモバイルデバイスのコア機能と直接やり取りを行う可能性があるため、、長年モバイルデバイスにとって最も重大な脅威となってきました。 Nokia[9] と Kaspersky の調査によると、[10] ほとんどのモバイルマルウェアはトロイの木馬化されたアプリを介してモバイルデバイスに侵入します。 これらのアプリは、懐中電灯アプリから高価なソフトウェアの無料版まで、人々が実際にインストールしたいもののふりをしていますが、トロイの木馬化されたアプリには、機密情報や資格情報を収集するなどの望まない動作が隠れています。[11] これは、アプリが携帯電話に保存されている位置データや連絡先を要求する懐中電灯アプリなど、表面レベルの機能に必要ではない権限を要求するためです。 [12]ユーザーは、通常は無料で、無害と思われるアプリやゲームをインストールしますが、デバイスやデータを悪意のある者に開放することになります。 Check Point は、これらのアプリ、特に無料トライアルや追加機能を提供することを目的としたアプリの増加を報告しています。[13] これらのアプリの多くが良く知られたブランドや製品名を利用していながらデータや認証情報を盗んだり、デバイスをボットネットに追加したりするため、良く知られたものであるからと信頼することにはリスクがあると指摘しています。[14]

これらの悪意のあるアプリは、多くの場合、その本質をうまく隠しています。 ハッキングツール、アクセスウェア、スパイウェア、アドウェア、ダイヤラー、ジョークプログラムなど、トロイの木馬化されたアプリが急増しており、ユーザーが望まない迷惑行為や有害な行為が行われています。[15] アカウントを乗っ取り、モバイルデバイスをボットネットに接続するアプリを作成するサービスとしてのマルウェアプロバイダー（マルウェア・アズ・ア・サービスプロバイダー）もあります。[16]

これらのアプリの中には、高度にターゲットを絞ったものもあります。 たとえば、いくつかの即時貸付（ローン）アプリによる詐欺は、インドやアジア、アフリカ、ラテンアメリカの他の国々で流行しています。 インストール後、アプリは当然貸付を

---

[9] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[10] https://securelist.com/mobile-malware-evolution-2020/101029/

[11] https://www.mcafee.com/blogs/mobile-security/mobile-spyware/、 https://www.appdome.com/dev-sec-blog/mobile-payment-security/

[12] https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

[13] チェックポイント、2023 年サイバーセキュリティレポート、2023 年

[14] https://www.verizon.com/business/resources/T9bc/reports/mobile-security-index-report.pdf

[15] https://docs.broadcom.com/doc/istr-23-03-2018-en

[16] https://www.androidpolice.com/android-botnet-trojan-steal-banking-data/

提供する可能性がありますが、電話からユーザーに関する情報とヌード写真を含む携帯電話上のその他のデータの両方を収集し、嫌がらせ、脅迫、恐喝に使用することになります。[17]

主要なモバイル脅威が特定された場合、当然の疑問は「しかし、これらの悪意のあるアプリはどのようにインストールされるのですか？」ということです。 Google Play ストアや Apple App Store などのファーストパーティアプリストアは、悪質なアプリを防ぐのに完璧であるものではありませんが、ストアを安全に保つための努力により、ストア上のほとんどのアプリは無害です。 マルウェアの最も危険なベクトルは、サードパーティのアプリストアとサイドローディングから発生します。 各方法によってもたらされるリスクの度合いを正確に定量化することは非常に困難ですが、一部の研究では、ユーザーに重大なリスクがあることが示唆されています。

サードパーティアプリストア

一部の研究では、Google Play ストアのようなファーストパーティアプリストアと比較して、主要なサードパーティアプリストアが安全である可能 性が示唆されている一方、サードパーティストアがモバイルユーザーのセキュリティとプライバシーのリスクを増加させることを示す証拠もあります。しかしそれはオペレーティングシステムに関連付けられていないからではありません。 それよりもむしろ、彼らは一般的にアプリの取り締まりにおいて同様の熱心な取り組みをしない、またはすることができません。これはおそらく、主要なモバイル OS が過去にサードパーティのアプリストアをデフォルトで許可してこなかった理由の 1 つです。[18] また、アプリストア自体が悪意のあるアプリをインストールすることを意図している例もあります。[19] 2021 年のフォーカスグループ、CrowdStrike は、モバイルマルウェアの大部分は、提供するアプリケーションの包括的なチェックを実行しないサードパーティのソースから配布されていると指摘しました。[20]

正確なリスクを定量化することは困難ですが、2020 年のある調査によると、Android で「その他の主要な代替市場」のユーザーは、Google Play ストアを使用したユーザーよりも、平均して 5 倍リスクが高く、マルウェアや悪意のあるアプリに遭遇する可能性が [20]19 倍以上高かったことが示されています。[21] さらに、サイバーセキュリティ企業のシマンテックは、2018 年に発見したモバイルマルウェアの 99.9 %がサードパーティアプリストアでウイルスにホストされていたと報告しています。[22]

これにより、セキュリティの専門家や規制当局の間で、ほとんどのサードパーティのアプリストアからアプリをダウンロードすることは、信頼できるファーストパーティからダウンロードするよりもはるかにリスクが高いというコンセンサスが得られました。 主要な政府および民間組織は、非公式 および 信頼できないソースからのアプリのダウンロードを控えるようアドバ

---

[17] https://www.bbc.co.uk/news/world-asia-india-66964510

[18] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[19] https://www.makeuseof.com/what-are-the-dangers-of-third-party-app-stores/#:~:text=Many%20malicious%20actors%20have%20created,hidden%20trackers%20and%20malicious%20code.

[20] 2021 年センターペーパー

[21] https://arxiv.org/pdf/2010.10088.pdf

[22] https://docs.broadcom.com/doc/istr-23-03-2018-en

イスしています。これには ENISA[23] 、ユーロポール、米国[24] NSA、消費者保護を**責務とする**米国 FTC、英国国家サイバーセキュリティセンター、[25] インド の CERT - In 、[26] 米国 DHS の CISA、商務省の[27] NIST、[28] ニュージーランドの CERT NZ などからのさまざまな時期の警告**が**[29] 含まれます。それにもかかわらず、調査によると、アプリが無料である場合、またはよく知られているゲームやアプリの修正版である場合、消費者はサードパーティのアプリストアを使用することが示されています。[30] ユーザーはセキュリティを念頭に置いていません。**ユーザーは**ただ、**迅速に**、できれば無料で**手に入れるには現実的に考えれば良すぎる**アプリを手に入れたいだけです。

サイドローディング

比較すると、サイドロー**ディング**は従来のアプリストアフロントのようなものを**一切**必要とせず、サイドロー**ディング**されたアプリは、バックグラウンドコンテキストが少なく、審査**も行われず**、セキュリティと信頼性に関して虚偽または誤解を招くような主張**が行われた状態**で配布または宣伝される可能性があります。 ウェブサイト、メッセージの添付ファイル、または不明瞭なリンクなど、どこからでもサイドロー**ディングは**発生する可能性があるため、この**ような熱心な取り組み**を実行する仲介者はいません。

サイドロー**ディング**は、アプリが改ざんされていないことを確認するための評判、経験、または手段を持たないかもしれないサードパーティを**個人が**信頼**し行う**必要がありますが、ユーザーは試してみたい新しいゲームを見つけたときに**そのようなこと**について考えません。 多くのサードパーティのウェブサイトやストアは安全であるかもしれませんが、ユーザーはアプリがどのように審査され、どのような権限を求めているのかについて、同じレベルの透明性**でわかる**可能性は低く、評判の良いアプリストアのインフラストラクチャが**なければ、自分で**ない**ものになりすますのは**はるかに簡単です。

サイドローディングは、ユーザーがモバイルアプリを取得するための最も危険な方法です。 そのリスクは、サイドローディングが多くのエンドユーザーが持っていないレベルの技術的専門知識を必要とすることが多いという事実によって従来相殺されてきましたが、モバイルオペレーティングシステムがデフォルトでサイドローディングを許可すると、**こうした葛藤は無くなってしまいます。**サイドロー**ディング**をしている、情報に通じたエンドユーザーでさえ、最終的には未知のまたは疑わしい開

---

[23] ユーロポール: https://www.europol.europa.eu/sites/default/files/documents/infographic_-_apps.pdf

[24] 米国 NSA モバイルデバイスベストプラクティス V 3 ： https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3% 20 -% 20COPY.PDF

[25] 英国 NCSC ： https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf

[26] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013

[27] 米国 CISA ： https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf

[28] 米国 NIST ： https://www.nccoe.nist.gov/sites/default/files/legacy-files/mtc-nistir-8144-draft.pdf

[29] N.Z. CERT ： https://www.cert.govt.nz/individuals/guides/keep-mobile-phone-safe-secure/

[30] https://www.jamf.com/blog/what-are-third-party-app-stores-and-are-they-safe/

発者やアプリストアを信頼していることが多く、確立された企業から直接ダウンロードしない限り、技術的な知識**がいくらあったとしても**リスクを確実に下げることはできません。

エンドユーザー責任の欠如

調査によると、ユーザーのセキュリティ上の意思決定は、セキュリティ上の脅威に関する知識と必ずしも相関していないことが示されています。[31] 悪意のあるアプリが引き起こす可能性のある非常に現実的な害にもかかわらず、モバイルユーザーはアプリが要求する権限を批判的に見るためにかなりの時間を費やすことはめったになく、**そうしようとしても**その意味を理解していないことがよくあります。[32] ユーザーはセキュリティ警告で中断されると、圧倒的にそれを無視します。[33]

多くのユーザーは、モバイルデバイスに対して基本的なセキュリティ対策を講じてすらいません。たとえば、ある調査では、ユーザーの 40 %が、**都合がつかない限り**オペレーティングシステムやアプリを更新しないと回答し、28 %は画面ロックを使用していないことがわかりました。[34] 別の調査によると、スマートフォンユーザーの 4 分の 3 が、アプリストアからダウンロードするアプリは本質的に安全であると考えている[35] ため、懐疑的になる可能性は低いという**ことがわかりました**。 その調査では、アプリユーザーがさまざまなアプリストアによって提供されるセキュリティレベルを**区別**することができなかった、またはする気がないことさえわかりました。 最近の追加の調査では、ユーザーはセキュリティリスクを気にかけていますが、効果的に自分自身を保護するための知識とスキルが不足しており、しばしばそうしようとさえしていないことが確認されています。[36]

ユーザーがオンラインで自分自身を保護するためにより積極的な役割を果たすことを願っていますが、**最善の方策**は**ユーザー**からできるだけ多くの負担を**徐々に**取り除くことです。 国のサイバー戦略と**政府による最善の方策は、バランスを転換し**、デバイス、データ、および人々を保護する責任をそれらを配布している企業に負わせています。 2023 年、米国（CISA）、チェコ共和国 、 イスラエル 、 シンガポール 、 **韓国** 、 ノルウェー 、OAS/CICTE CSIRTAmericas Network 、日本（JPCERT/CC 、NISC）のサイバーセキュリティ機関は、エンドユーザーから リスクバランス**の転換に関する**ガイダンスを共同で発表しました。[37] 公共部門と民間部門の両方の多くの組織は、承認されたアプリのみが機密データやアプリにアクセスできるデバイスにインストールされることを保証するために、モバイルデバイス管理（MDM）を使用することを選択しています。これらのツールにより、管理者は将来、どのアプリストアが許可されるか**判断**できる可能性があります。

---

[31] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

[32] https://link.springer.com/chapter/10.1007/978-3-031-35822-7_36

[33] https://news.sophos.com/en-us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/

[34] https://www.pewresearch.org/short-reads/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

[35] https://www.sciencedirect.com/science/article/pii/S0167404812001733#fn6

[36] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[37] https://www.cisa.gov/resources-tools/resources/secure-by-design

上記のリスクの程度と複雑さを考えると、エンドユーザーが突然、階層化されたセキュリティを介して自分自身を保護する方法、許容されたリスクに応じた最適な設定の組み合わせを構成する方法、他の方法では大規模には実行可能ではないなど、モバイルセキュリティとプライバシーに関する必要な認識と理解を突然得ることを期待するのは不合理です。エンドユーザーは、普遍的に利用可能なアプリストアが安全であると想定する可能性があります。 他のアプローチもありますが、ゲートキーパーがすでに独自のアプリストアに導入しているような保護が必要になります。

グーグルやアップルはいかにこれらの脅威と戦うのか

Apple App Store や Google Play Store、DMA の下でその他ゲートキーパーであると判断されていない多くのファーストパーティアプリストアは、新しいアプリや更新されたアプリをスクリーニングしてマルウェアや元のアプリ機能への重大な変更がないかを確認するように設計されたポリシーとプロセスを通じて、上記で特定されたリスクを軽減するための広範な措置を講じています。 Apple と Google の両方が、開発者から公式アプリストアを経由して消費者にまで及ぶポリシーとプロセスを作成しました。 完全に安全なアプリストアはありませんが、これらの取り組みにより、Google Play ストアと Apple App Store は、ユーザーを保護するためのアプローチについて情報を提供するため、長年にわたる投資と学習を通じ消費者の信頼と安全性において評判を得ています。

Apple App Store や Google Play Store などの主要なファーストパーティアプリストアは、ベースライン要件やガイドラインの設定、自己認証の要求、アプリのレビューなどによるプロセスの実装を通じてセキュリティを実現します。[38] アプリ開発者は、これらのアプリストアのいずれかに掲載されるために、自分達のアプリのさまざまなセキュリティ、プライバシー、透明性の要件を満たす必要があります。 これには、アプリで通知されていることを実行し、適切な許可のみを求め、機能的なプライバシーポリシーを設定していることの確認が含まれる場合があります。 Apple と Google のアプリストアでは、アプリが使用する権限やデータ収集に関する情報などを含めて、アプリストアでの掲載において透明性が求められます。[39] [40]

ファーストパーティアプリストアには、アプリ自体のレビュー以外にも、デベロッパーアカウントの審査など、追加の保護が備わっているかもしれません。 たとえば、Google Play ストアは「開発者の Google アカウント、アクション、履歴、請求明細、デバイス情報など」を分析して、潜在的な危険信号を特定します。[41]

アプリの提出内容を確認する場合、ファーストパーティアプリストアは、アプリの機能を安全にするためにさまざまなアクションを実行できます。ストアは、アプリ開発者の認証を確認したり、さまざまな自動レビューを適用したり、人間のレビュアーにアプリを手動でレビューさせることができます。 これらのレビューは、マルウェアやその他の潜在的に有害または望ましくない側面を検索する静的および動的レビューを実行するために、さまざまなツールと技術を使用する場合があります。 さら

[38] https://developer.apple.com/app-store/review/guidelines/, https://play.google.com/about/developer-content-policy/

[39] https://support.google.com/googleplay/android-developer/answer/10144311?hl=en

[40] https://developer.apple.com/app-store/user-privacy-and-data-use/#:~:text=In%20order%20to%20submit%20new,websites%20owned%20by%20other%20companies.

[41] https://developers.google.com/android/play-protect/cloud-based-protections

に、新しく提出されたアプリの定期的な検査以上に、Apple のようなファーストパーティアプリストアは、新しい機能が全て安全であることを確認するためアプリの更新をレビューします。 最後に、ファーストパーティアプリストアは、アプリが望ましくない挙動をしていると消費者やセキュリティ研究者の苦情や問い合わせが契機となり、レビューを開始する傾向にあります。

アプリがアプリストアに掲載されるための必要な要件とガイドラインを満たしたり、維持したりできない場合、アプリは通常、削除されます。 これらの問題の規模は注目に値します。Apple は、2022 年に 150 万件以上のアプリの申請をを却下し、アプリストアから 186,000 以上のアプリを削除したと詳述しています。[42] これらの削除により、安全で信頼できるアプリストア環境を促進し、エンドユーザーを害から守りますが、悪意のある者にデバイスを感染させる他のより有益な手段を探させる契機となります。

消費者レベルでは、Apple と Google は、セキュリティとポリシーの保護と要件をアプリストアのユーザーが簡単にアクセスし、理解できるようにするために多大な努力を払ってきました。 さらに、両社とも、審査されたアプリが求める権限に関して、より透明性を高めることを目指しており、消費者は公式のアプリストアベースライン以上に求められるプライバシーとセキュリティのレベルについて情報に基づいた決定を下すことができます。 Google Play ストアは、独立したセキュリティレビューを完了したアプリにバッジを表示し始めています。[43] これらのプロセスとポリシーは効果的であることが証明されていますが、多額の投資になります。

モバイルアプリストアへのセキュリティは投資である

上記のように、エンドユーザーにセキュリティの責任を負わせることは効果的ではなく、ユーザーがデフォルトで確実に保護されるようにポリシーとプロセスをさらに促進させるというサイバーセキュリティのベストプラクティスに反します。 Google や Apple のようなリソースが豊富な大企業は、効果的にそうするための専門知識、リソース、そして意欲を持っていますが、同様のことが当てはまる企業はほとんどありません。

上記の種類の保護は、サードパーティのアプリストアによって同程度に実装されることはめったにありませんが、悪意のある、低品質の、欺瞞的なアプリの大部分を排除します。 サードパーティアプリストアには、ファーストパーティアプリストアのように、アプリストアを保護したり、ホストされているアプリを、審査したりするためのリソース、経験、プラットフォームと OS の知識、インセンティブがありません。 さらに、サードパーティアプリストアは、その他の点で歓迎されないと見なされるアプリに対しより寛容になることで、大規模な確立されたストアとの差別化を図る可能性があります。 その対岸にマー

[42] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

[43] https://security.googleblog.com/2022/12/app-defense-alliance-expansion.html

モバイルオペレーティングシステムを必要とすることは、モバイルエコシステムのプライバシーとセキュリティに必然的にマイナスの影響を与えますが、サードパーティアプリやアプリストアへユーザーが安全に、よりアクセスできるようにするのと同時に、サードパーティアプリ開発者が OS レベルの機能へもっとアクセスできるようにする方法もあります。 上記で示したように、そして Apple のようなファーストパーティが証明しているように、DMA の遵守は、「マルウェア、不正と詐欺、違法で有害なコンテンツ、およびその他のプライバシーとセキュリティの脅威」の蔓延を増加させることはほぼ確実です。[44] しかし、議員や政策立案者は、ゲートキーパーが消費者を保護できるようにする建設的な実施ガイダンスによって、これらの問題を軽減することができます。

EU 加盟国は、以下をサポートすることにより、ファーストパーティアプリストア、モバイル OS 所有者、およびモバイルデバイスユーザーを積極的にサポートする必要があります。

- ゲートキーパーは、流通チャネルに関係なく、アプリのベースラインレビューを行う必要があります。 これには、オペレーティングシステムに組み込まれた新しいメカニズム、またはアプリストアとの契約が必要になる場合があります。 また、認証と第三者評価を使用して、アプリが安全であることを証明する方法もあります。
- 政策立案者は、基本的な機能と重要な情報に関するアプリの説明通知を検討して、ユーザーや他の人がアプリの仕組みと目的を理解できるようにする必要があります。
- オペレーティングシステムは、マルウェアがモバイルデバイスのセキュリティ及び完全性を損なうのを防ぐために強化されたモバイル保護を実装することができ、これには、サンドボックス化してアプリを相互に保護し、オペレーティングシステム、ユーザーデータ、及びデバイスハードウェアを悪意のあるアプリから保護するための追加のツールが含まれます。これらのツールには、エンタープライズ管理者向けの MDM ツールが含まれる場合があります。
- ゲートキーパーは、サードパーティアプリストアが信頼できることを保証するために、サードパーティアプリストアの技術的および契約上の管理を導入する必要があります。 各ゲートキーパーは、DMA に準拠するよう取り組むため異なる緩和策の間で異なるバランスを選択する可能性があり、他方でデバイスとユーザーを保護するための幅広いオプションを用意する必要があります。
- ゲートキーパーのモバイル企業は、ユーザーを保護できるという明確なガイダンスが必要で、ユーザーを保護するための新しいシステムを概念化、構築、テスト、および実証するのに十分な時間が与えられる必要があります
- 規制当局は、アプリとアプリストアの両方でセキュリティと完全性の懸念事項に注意を払い、すべてのアプリとストアが同じように作られているわけではないことを認識する必要があります。 彼らは、アプリやアプリストアの開発者が責任ある行動をしているかどうかを評価し、そしてそうでない場合に責任を負うことができるメカニズムの開発を支援する必要があります。
- モバイルオペレーティングシステムを開発するゲートキーパーは、開発者が変化するエコシステムを悪用できないようにするために、権限とセキュリティモデル、およびそれらがどのように動作するかを調整する柔軟性を持つ必要があります。 政策立案者は、アプリストアとデバイスオペレーティングシステムが、エコシステムと一体化するために利用可能なさまざまなセキュリティメカニズムと制限を進化させる能力を保護する必要があります。
- モバイルエコシステムに対応するポリシーは、それらのエコシステムのセキュリティを弱めてはなりません。 政策立案者は、モバイルプラットフォームのセキュリティとプライバシーが継続的に改善され、両方がプラットフォームと

[44] https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

- 政策立案者は、ユーザーがどのようなセキュリティ責任と負担を引き受ける意思があり、準備が整っているかについて現実を認識しなければいけません。 研究によって、セキュリティに対する意識と適切にセキュリティ上の意思決定を行うことは相関しないことが示されています。[45]
- 政策立案者は、モバイルデバイスの操作方法やインストール可能なアプリに関する特定のプラクティスを義務付けるのではなく、モバイルデバイスのリスクに基づいたプラクティスをサポートする必要があります。

結論

DMA が法制化され、ゲートキーパーがその遵守を徹底するために取り組んでおり、私たちはモバイルエコシステムにとって重要な移行期に入りつつあります。Center for Cybersecurity Policy and Law は、政策立案者とゲートキーパー、その他のモバイルエコシステムが協力し、ユーザーとそのモバイルデバイスを安全かつ確実に保つことができることを望んでいます。 政策立案者は、企業、エコシステム、消費者へのセキュリティの影響を考慮する必要があります。 現在のアプリストアのレビューと監視についてこれらの要素の多くの影響を定量化することは困難ですが、アプリストア開発者がユーザーを保護するために行った投資は認識され、報われるべきです。 アプリストアの所有者と開発者がセキュリティとプライバシーを強化するアクションを取ると、ユーザーは気づかない方法で恩恵を受けています。

すべてのモバイルマルウェアからユーザーを保護する完璧なシステムはありませんが、私達はユーザーが考慮しなければならない、望まないまたは悪意のある行為の数を大幅に減らす方法を知っています。

[45] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/