
信頼できるアプリストア：セキュリティと 整合性の保護

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
サイバーセキュリティと法律センターについて	Error! Bookmark not defined.
はじめに	4
DMA アプリストア規定	Error! Bookmark not defined.
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	Error! Bookmark not defined.
グーグルやアップルはいかにこれらの脅威と戦うのか	Error! Bookmark not defined.
モバイルアプリストアへのセキュリティは投資です	Error! Bookmark not defined.
DMA 実施のロードマップ	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実施しているため、アクセス、プライバシー、セキュリティと経済学的思考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は、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を損なう可能性があります。サイバーセキュリティポリシー&法律センターは、アプリをインストールする方法が急増しユーザーは圧倒的されそうになり、悪意の行為者がそれらを悪用するための多くのを開く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、過去にははしなくて良かった方法で、本当に保護されているかを確認するために、企業とユーザー自身から行動を取るようになります。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への推奨事項として、ユーザーがモバイルエコシステムを引き続き信頼できるよう確認するため、および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。この論文が、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力を育成しようとしている他の国々にも見識を提供することを願っています。

サイバーセキュリティと法律センターについて

サイバーセキュリティ法センターは、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方針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した独立した組織です。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 年に設立されたこのセンターは、政策の専門知識をグローバルな、国家の、および地方レベルでの召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、実際の成果を生み出す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を保護する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、複雑さを解明し、サイバーセキュリティに関する混乱を解消することを目指しています。

はじめに

ますます接続された世界では、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ます¹。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。したがって、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年のレポート「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人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、設置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のコンセンサスは、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することでした。

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という状況下で書かれました。過去10年間でモバイルエコシステムは徐々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）のアプリのインストール規定は、このセキュリティの進歩を続けるのではなく、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必要とするDMAの規定によって、ユーザーが圧倒される可能性があり、モバイルデバイス管理を実装する企業管理者にとっての課題であり、悪意のある行為者に新しい道を開く可能性があります。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を軽減する

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。

ための合理的なアプローチをとりながら、DMA の意図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。

この論文では、DMA 内のアプリストアの規定、これらの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討します。本稿では、準備不足の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 実施アプローチについて論証します。

DMA の文書では、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可能性のある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、透明性要件、認可の調整およびモバイルデバイスオペレーティングシステムに組み込まれたセキュリティモデルを通じて、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 の実装におけるセキュリティの重要性を強調し、ゲートキーパーとしてコンプライアンスを確立するよう促します。

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」の定義の対象となる企業は、それらのアプリストアおよびサードパーティのアプリストアやアプリとのモバイル OS の相互作用に関連する DMA 条項のに従うことになります。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、小規模なヨーロッパ企業が、市場でより「定着した」地位を持っているかもしれない企業と競争しやすくすることです。

DMA 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を持たない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し、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のそれぞれのアプリ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。

これらの規定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、技術的に有効にし、それらの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に、そのゲートキーパーの関連するコアプラットフォームサービス以外の手段でアクセスできるようにするものとします。

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します[...]。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します。

これらの DMA 規定が、他の欧州連合の法律と組み合わせられると、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を認識することを強調していますが、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べきでは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規制した場合、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保護することにどのような期待しているかについては説明していません。慎重に検討せずに実施された場合、DMA の上記の規定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、その普遍性、一日を通して私たちに同行するという事実、そしてそれらが私たちの生活の中核部分であり、多くのデジタルインタラクションの真ただ中にあるため、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オペレーターは、それ以来、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の OS アーキテクチャ設計の選択を通じて、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は現在、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ます。⁸

⁸ <https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/>

モバイルエコシステムには無数の脅威があり、悪意のある人もチャンスを狙った行為者も、これらの信じられないほど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ます。ゲートキーパーや政策立案者が DMA を実施する際に、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インターフェースで接続する可能性を考えると、モバイルデバイスにとって最も重大な脅威となっています。Nokia⁹ 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は、機密情報や資格情報を収集するなどの望まない動作を隠しています。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な権限を要求するためです。¹² ユーザーは、通常は無料で、良性のアプリやゲームと思われるもの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行為者に開放します。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 彼らは、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活用しているため、良く知られたものを信頼することにはリスクがあり、その後、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、その本質を隠すことに成功しています。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、いくつかのインスタントローンアプリ詐欺は、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、アプリは当然ローンを提供

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/>

しますが、電話からユーザーに関する情報とスード写真を含む電話上のその他のデータの両方を収集し、嫌がらせ、脅迫、ゆすり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、自然な疑問として「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ドです。各方法によってもたらされるリスクの量を正確に数値化することは非常に困難ですが、一部の研究では、ユーザーに実質的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

いくつかの研究では、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あると示唆されている一方で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証拠を示していますが、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。代わりに、彼らは一般的にアプリを監視する際に同じ努力をしない、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いない理由の 1 つです。¹⁸ また、悪意のあるアプリをインストールすることを意図したアプリストアの例もあります。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

正確なリスクを数値化することは困難ですが、2020 年のある調査によると、「他のトップの代替市場」の Android 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 倍以上高かった。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ると報告しています。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 ENISA²³、ユーロポール、米国²⁴ NSA、消費者保護を担当する米国 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 ニューージーランドの CERT NZ などからのさまざまな時期の警告を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。彼らはただ、すごく速く、できれば無料であり、信じられないほど良い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、サイドロードは従来のアプリストアフロントのようなものを必要とせず、サイドロードされたアプリは、バックグラウンドコンテキストが少なく、審査がなく、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ドが発生する可能性があるため、このデリジェンスを実行する仲介者はいません。

サイドロードでは、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信頼する必要がありますが、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れ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を見つける可能性は低く、評判の良いアプリストアのインフラストラクチャがないというわけではないふりをする方がはるかに簡単です。

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、不和が消えるでしょう。サイドロードをしている、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、技術的な知識でリスクを確実に下げることができません。

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/>

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、多くの場合、試してもその意味を理解していません。³² ユーザーが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、それが便利な場合を除いて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%が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。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差別化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、ベストプラクティスは彼らからできるだけ多くの負担をだんだん取り除くことです。国のサイバー戦略と政府のベストプラクティスは、ますますバランスをシフトしてユーザーから離そうとしており、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 [CSIRT Americas 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のバランスをシフトするための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決定できる可能性があります。

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、受け入れられたリスクに最適な設定の組み合わせを構成する方法、他の方法は、単に規模的に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持つように期待するのは不合理です。エンドユーザーは、普

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>

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、長年にわたる投資とユーザーを保護するためのアプローチの情報を提供することを学び、消費者の信頼と安全性で評判を得ています。

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施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、アプリで宣伝されていることを実行し、適切な権限のみを求め、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、アプリストアのリストに透明性が必要です。^{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するため分析します。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見直しさせたりすることができます。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再調査します。最後に、ファーストパーティアプリストアは、消費者やセ

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>

セキュリティ研究者の苦情や、アプリが歓迎されない行動を取っているとの通知に基づいて、見直すきっかけにする傾向があります。

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提出を拒否し、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る。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、悪意のある行為者にデバイスを感染させる他のより有益な手段を探す刺激となります。

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、かなりの投資になります。

モバイルアプリストアへのセキュリティは投資です

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安全に保護されるようにポリシーとプロセスをさらに促進する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、他のほとんどの企業は同じことを言うことができません。

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じ程度に実装されることはめったにありませんが、それは悪意のある、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思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。その一方で、ファーストパーティアプリストアは、マーケットプレイス上のアプリのセキュリティを向上させるためにかなりの資金を費やしています。

DMA 実施のロードマップ

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>

ードパーティアプリ開発者に OS レベルの機能へもっとアクセスを許可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たように、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前向きにサポートする必要があります。

- ゲートキーパーは、流通チャンネルに関係なく、ベースラインアプリの見直し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整合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互いから保護し、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、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、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、DMA に準拠するよう仕事をしてユーザーを保護するために使用されます。
- 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を必要で、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ています。
- 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整合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を持って行動すること、そしてそうでない場合に責任を負うことができることを査定、保証するために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取り組む方策は、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アプリに最初から組み込まれていることを確認する必要があります。これまでの進歩を脅かす提案は見直す必要があります。

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、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別な練習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練習をサポートする必要があります。

結論

DMA が法律に制定され、ゲートキーパーがコンプライアンスを守るために取り組んでいるため、モバイルエコシステムにとって重要な移行期に入っています。サイバーセキュリティポリシーと法律センターは、政策立案者とゲートキーパー、そしてモバイルエコシステムの残りの部分が、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ために協力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の、これらの要素の多くの影響を数値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、ユーザーは気づいてい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。