

情報の要請

質問1

ACT | App Association

ブライアン・スカルペリ

質問2

ACT | App Association

1401 K St NW

Ste 501

ワシントン州, DC 20005

質問3

ブライアン・スカルペリ

上級グローバル政策顧問

+1 517-507-1446

bscarpelli@actonline.org

質問4

非営利

質問6

ACT | App Associationは、日本国内および世界各地に拠点を置く、中小企業向けソフトウェアアプリケーションおよびコネクテッドデバイスの開発者コミュニティを代表しています。これらの企業は、224兆3,000億円規模以上のグローバルなアプリ経済を牽引しており、この経済は成長を続けています。App Associationのメンバーは、スマートデバイスの接続性を活用して、消費者と企業のユースケース全体に新たな効率性をもたらす革新的なソリューションを創造し、ビジネスを成長させ、新たな雇用を創出するために、プラットフォーム規制に対する予測可能で公正なアプローチに依存しています。

質問9

App Associationが代表する中小企業の技術開発者は、主要なアプリストアを通じてソフトウェア製品とサービスを提供しています。スマートフォンの台頭と並行して、アプリエコシステムは指数関数的に成長しました。ただし、アプリエコノミーの軌道はさまざまな要因によって決まります。アプリエコシステムのダイナミックな成長と圧倒的な成功において、最も重要な要素は、厳選されたプラットフォーム、つまりアプリストアの存在です。信頼性の高いアプリストアは、業界や企業全体でアプリの利用を促進するための重要な基盤となっています。ソフトウェア配布における革命を引き起こしたのは、次の3つの重要な特性です:

1. 諸経費を削減するサービスの提供
2. 即時かつ費用対効果の高い消費者信頼の仕組み、および

3. グローバル市場への費用対効果の高いアクセス。

現在、モバイル、デスクトップ、ゲーム、さらにはクラウドコンピューティングのあらゆる成功したプラットフォームは、これらの機能を提供しなければ、市場での失敗のリスクを冒します。プラットフォーム間の競争の増加は、起業家にとって前例のない機会を提供しました。

質問20

App Association の会員企業は日本を含む全世界で事業を展開しており、現在のデジタル市場エコシステムの利点と、欧州連合のデジタル市場法 (DMA) に触発された競争法の悪影響の両方を経験しています。次のセクションでは、これらの利点と悪影響についてさらに詳しく説明します。

小企業アプリケーション開発者に対する消費者の信頼を築き維持する面でプラットフォームが果たす役割

最初は、開発者たちはプラットフォームに参加することに消極的で、そのモデルが自分たちが迅速にアプリをリリースし、アプリを改良するというニーズに対応できないのではないかと心配していました。しかし、成功したプラットフォームは、アプリ開発者に広範な消費者へのアクセスを提供することで、アプリのエコシステムを変革しました。プラットフォームは、アプリ開発者に対して世界中の数十億のアプリユーザーとの関係構築と広がりを提供する中心的な枠組みを提供します。参入障壁とコストが低いいため、新興のアプリ開発者や確立された開発者の双方が成功を収めることができます。

開発者がプラットフォームに対して配信やマーケティングなどの様々なサービスの料金を支払う開発者サービス市場も重要な要素です。この市場も激しい競争が展開されています。前述の通り、市場ははるかに広範で、さまざまなプラットフォームを含んでいます。

サイバーセキュリティとプライバシー、著作権侵害、データの管理と移行面でプラットフォームが果たす役割

スマートフォンやソフトウェア配布プラットフォームが登場する前、ソフトウェア開発者は消費者の信頼を築くために時間と膨大な費用を費やしました。その信頼は、製品を市場に投入するためにソフトウェア開発者にとって不可欠であり、今もなお重要です。開発者の大半には、ソフトウェアを後押ししてくれる広く認知されたブランドがありませんでした。モバイルプラットフォームが普及する以前、ソフトウェア開発者はしばしば信頼の壁を乗り越えるために、製品を評判の高い企業に提供する必要がありました。デジタル配布が可能なシェアウェア製品でさえも、消費者の信頼を得るためには実績のあるブランドと提携することが一般的でした。現在、消費者はこれらのようなゲームをプラットフォーム上で無料でダウンロードすることができます。これらのプラットフォームは、製品の販売に伴う大きな経費を軽減するだけでなく、消費者に対してより簡単にアクセスすることができます。今日、消費者の信頼は継続的な維持と警戒が必要であり、そ

の信頼を失うことはプラットフォームと開発者の両方にとって損害をもたらします。

多くの消費者は、個人情報保護とセキュリティを重要な要素と考え、ソフトウェア配布プラットフォームとの関わり方や利用場所を選ぶ際に重視しています。互いに競争し、消費者と開発者の両方を引き寄せるために、主要なプラットフォームは悪意のあるアプリに対する高度な初期防御策を提供する必要があります。最後の防御ラインであるデバイスのオペレーティングシステムがアプリの活動をブロックすることを期待して、ユーザーに悪意のあるアプリをダウンロードさせるのとは異なり、最も競争力のあるプラットフォームは、アプリが消費者にアクセスする前にマルウェアをスクリーニングするアプリ審査プロセスを利用しています。また、このようなプラットフォームは、ユーザーのプライバシーを危険にさらす可能性のある不要なアクセス許可リクエストをアプリが防止することで、さらなる保護を提供しています。

知的財産権と著作権侵害への対応面でプラットフォームが果たす役割

プラットフォームが登場する以前、ソフトウェア開発者は知的財産 (IP) を著作権侵害や盗難から守るのに苦労していました。ソフトウェア企業は製品を小売店で保護する上で重大な課題に直面しました。なぜなら、ライセンスコードが有効である間は盗まれやすく、商品の保護が困難だったからです。開発者が市場に製品を出すために大きな障壁を乗り越えると、著作権侵害や盗難の脅威に直面し、ビジネスの規模を制限し、利益を減少させる結果になりました。

プラットフォームが提供する紛争解決手段を活用する前、ソフトウェア開発者は知的財産権侵害の訴訟による重大な負担を負っていました。訴訟による法的費用だけでなく、数か月または数年にわたって企業の問題から時間を奪われ、正当な知的財産権所有者は毎月数千ドルの費用を負担していました。さらに、侵害が海外で発生した場合、ソフトウェア開発者は外国の司法制度に頼るしかなく、中には法の支配や公平性の欠如している場合もありました。ソフトウェア開発者や著作権保持者は、プラットフォームが提供する紛争解決手段を活用することで、製品の配布と品質の保護を効果的かつ費用効果の高い方法で行えるようになっていきます。

これらのプラットフォームの利点にもかかわらず、一般のユーザーに届けたい開発者にとっては、ウェブを利用することも代替手段となります。特に、プラットフォームで利用できるものとは異なる種類の配信や検索サービスを求める企業にとっては、ウェブが選択肢となります。上述のように、開発者は異なるモデルを好む場合があるため、ソフトウェアプラットフォーム間の違いは、配布方法のマーケットにおける多様性を示しています。

ソフトウェアプラットフォームの安全性とセキュリティは、特にエンタープライズアプリ開発者にとっては、開発者サービスの重要な要素です。ソフトウェアプラットフォームのセキュリティ機能は、その存在の過程で大幅に向上してきましたが、新たな手法や脅威に対応するためには、継続的に適応する必要があります。かつてはデバイスを解除するために4桁のパスワードだけで十分でしたが、現在のデバイスは生体認証に対応し、ソフトウェアプラットフォームはこれらの認証手段を開発者にも提供しています。これにより、開発者は顧客に高度なセキュリティ対策を提供し、信頼を築き維持することができます。ただし、サイバーセキ

セキュリティの専門家とハッカーの間の攻防戦は終わりませんし、セキュリティは脅威に対抗するために常に進化し続ける必要があります。一部のプラットフォームはデバイスのセキュリティを制御していないものもありますが、開発者はプラットフォームのセキュリティ機能が関連するハードウェアとシームレスに連携し、全ての攻撃ベクトルに対応できることを求めています。ソフトウェアプラットフォームは、脅威が発生する場所に関係なく、プラットフォーム全体の開発者を確実に保護するために脅威情報の共有と収集能力を向上させるべきです。また、消費者だけでなく、開発者や彼らのクライアント、ユーザーを守るために重要なセキュリティ更新を迅速に承認し、展開する必要があります。

App Associationのメンバーシップ全体では、消費者のデータは関連する法律と規制に従って収集されます。これには、「アプリの機能のみ」や「機能とターゲット広告」といった目的が含まれます。繰り返しになりますが、私たちのメンバーが利用できるプラットフォームの幅広さにより、経験や実践方法はプラットフォームごとに異なる場合があります。App Associationは、企業が製品やサービスにプライバシーを早い段階から組み込むことを重要視し、責任ある透明なデータ管理に取り組んでいます。プラットフォームのオペレーティングシステムからのプライバシープロンプトは、消費者が自分のデータがどのように収集・利用されるのかを情報を得て明確に判断できるようにする必要があります。競争の視点だけで問題を考えることは、完全な視点ではありません。また、よりプライバシーを保護するアプローチを取るソフトウェアプラットフォームは、敏感なデータの収集を容易にする他のプラットフォームと競争上の差別化を図っています。こうした政策のもつれを解決するには、消費者にとって何が最も効果的であるかに焦点を当てる必要があります。したがって、もしプラットフォームが独立開発者の提供する製品よりも消費者が好む提供をしている場合、日本の政策立案者は、強力な競合他社の苦情がその選択肢を法律で制限する必要性を問うべきです。

App Associationのメンバーは、提供するサービスの機能に合わせたデータを収集し、法律や規制、および関連するプラットフォームに準拠しています。また、App Associationのメンバーは、収集した機密データを保護するために、エンドツーエンドの暗号化などの最新の技術的な保護メカニズムを使用するために努力しています。さまざまなプラットフォームには、消費者自身がプライバシーをより細かく制御できる機能が組み込まれており、App Associationの会員はこれをサポートし、消費者の信頼を高めることから恩恵を得ています。App Associationは、メンバーと協力して、消費者とのコミュニケーションに使用されるプライバシーポリシーが次の3つの重要な原則を反映していることを確認しています：(1) ポリシーは明確で透明であり、データ収集の実践だけでなくデータ保護の実践も明示されている必要があります。(2) ポリシーは提携している広告主、アナリティクスサービスなどの第三者について明確に説明し、彼らが消費者のデータにアクセスし、それをどのように処理するかを説明する必要があります。(3) 消費者は合理的な範囲で自分のデータにアクセスし、変更や削除を行うことができる権限を持つ必要があります。

私たちは、日本の政策立案者に対して、違法なコンテンツや知的財産権の問題に取り組むための措置を講じているデジタル経済の関係者、およびそれらの取り組みに依存している関係者との綿密な協議を行うことを強く推奨します。これは、著作権侵害を管理し、違法コンテンツに対処する能力に重大な影響を及ぼす可能性のある提案を進める前の重要な手続きです。

消費者のアカウントを介して購入を可能にする取り組みや、ソフトウェア配信プラットフォーム間の切り替えコストの低さにより、プラットフォーム上での消費者はデータとサブスクリプションが管理しやすくなりました。これにより、新しいデバイスに移行したり、家族と共有したり、購入履歴を確認したり、親制限を設定したりすることが容易になりました。この集約化は、利便性を提供するだけでなく、不正な開発者と金融情報を共有することから生じるサブスクリプションやデータの詐欺、その他の違反から消費者を保護するのに役立ちます。そのため、消費者は異なる開発者によって作成された複数のプラットフォーム間でデータとサブスクリプションを管理する必要がある場合よりも、より多くのアプリをダウンロードし、アプリ内での購入にもっとお金を使う傾向があります。

厳格な基準やアプリレビュープロセス、アプリ内の支払いは、消費者の信頼を築き、小規模なアプリ開発者でもプラットフォームを通じて広くアプリを配信することができるようになります。実際に、ユーザーがプラットフォームを信頼すると、新しいソフトウェアアプリを試す意欲が高まり、小企業の開発者にとってもより多くの機会が生まれます。この組み込まれた消費者の信頼は開発者をプラットフォームに引き寄せ、利用可能なアプリの数と品質の持続的な成長をもたらしています。そして、日本の政策立案者が検討している両面プラットフォームの商業的な現実、独占化や反競争的な行動といった根拠のない独占化の主張とは矛盾しています。

関連して、プラットフォームのランキングや特集における透明性は、私たちのメンバーにとっては役立つものですが、プラットフォームでの成功にとって「重要」とまでは言えません。プリストアのランキングに関するさらなる洞察は有益ですが（例：技術仕様、ビジネスユーザー向けの利用可能なツールなど）、ソフトウェアプラットフォームは、ランキング固有のアルゴリズムなど、関連するすべてのビジネス運営の詳細を開示することを適切に避ける可能性があります。欧州委員会（EC）などの他の規制機関は、透明性のスコアカードなど、この分野でのさまざまな義務を提案しています。それには、説明内容、ランキング、およびデータの収集/使用状況などが含まれます。App Associationは、進化し、透明性が高まり、小企業の開発者に利益をもたらしているアプリストアランキングに過度な義務を押し付ける新しい仕組みに強く警告します。

データサポート面でのプラットフォームの果たす役割プライバシー

アプリメーカーは、プライバシーを最初から設計に組み込むよう努めるだけでなく、全ての能力を持つ人々が効果的にそれらを使用できるようにするという強い動機も持っています。たとえば、神経疾患を持つ患者のリモートスクリーニングやモニタリングを支援するアプリの開発者は、認知障害を持つ人々がそれを効果的に使用できるようにする必要があります。同様に、家の見学に利用される拡張現実アプリは、視覚障害を持つユーザーに対しては画面の内容を音声で説明する機能を搭載することができます。

小規模なアプリ会社にとって、これらの機能は過去には消費者自身が独自に追加するためのものであり、アプリ自体に統合される実用的なオプションとは言い難かったことがあります。一部のスクリーンリーダーの例では、視覚を必要とする場合があり、設定にはソフトウェアの操作にも十分な知識が必要です（ただし、一部のツールではモバイルオペレーティングシステム上での設定がデスクトップよりも容易かもしれません

）。障害のある人々に対して、これらの機能をアフターマーケットのツールとして他の人に頼ることを要求するのは、アクセシビリティを提供する上で費用がかかる方法であり、アプリ企業が製品を開封時にアクセス可能な状態にしたいという理想的な状況ではありません。

この点で、ソフトウェアマーケットプレイスは開発者と障害のある消費者に対して改善の余地を与えており、現代の開発者はこれらのプラットフォームイノベーションに大いに依存しています。例えば、現在のプラットフォームでは、消費者はデバイス上で声のコマンドを使ってプラットフォームをアクティベートすることができます。また、開発者が視覚障害のある人々のために自分で別の機能を作る代わりに、プラットフォームは広範なアプリケーションプログラミングインターフェース（API）に開発者が自由にアクセスできる環境を提供しています。例えば、視覚障害のある人々のためにアプリをアクセス可能にするために、開発者は独自に機能を作る代わりに、**VoiceOver API**を統合することができます。あるいは、過去の標準的な方法である顧客が別のアフターマーケットツールをダウンロードするという手法に頼ることもできます。

さらに、ソフトウェアプラットフォームが自社の製品をプラットフォーム上で優先することを禁止する提案は、現在の仕組みのままではこれらのアクセシビリティツールの提供を減らしてしまいます。この結果、それらのツールが人々が使用するオペレーティングシステムやデバイスとの統合によって実現可能で効果的かつ手頃な価格になるというメリットが失われてしまいます。その上、これらのツールが市場から姿を消すと、障害を持つスマートデバイスの所有者は再び主にアフターマーケットのオプションに頼らなければならなくなります。また、これらのオプションの統合にはより多くのリソースが必要となり、組み込み機能オプションに比べて高額かつ必要のないコストが発生することになります。

強制サイドローディングの可能性とモバイルアプリエコノミーへの害

上述のように、ソフトウェア配布プラットフォームのレビュー プロセスは、集団行動の問題を解決します。ユーザーの個人情報悪用して利益を得るいくつかの不正な開発者が存在するかもしれませんが、そのようなアプリをプラットフォームに許可することは、消費者のプラットフォームへの信頼を侵食し（そして使用する意欲を減退させる）可能性があります。小企業の開発者は、ユーザーのプライバシーとセキュリティを保護するためにプラットフォーム上のすべてのアプリを精査するなどの手段を通じて、プラットフォームの価値を維持するプラットフォームの取り組みに依存しています。実際、データの収集と保存に関連してデータのセキュリティとプライバシーを保護する措置を積極的に要求するこのようなプラットフォームの取り組みは、エンド ユーザーの信頼を獲得および維持する必要がある開発者に広く利益をもたらし、同じエンドユーザーのプライバシーを保護する主要な手段となります。この力関係は、開発者コミュニティの間で広く支持されています（プラットフォームの利点にアクセスするために料金を支払うことを逃れるために、今日のモバイルアプリエコノミーをひっくり返したい一部の外れ値の開発者にとっては非常に残念なことです）。

一般的に、日本のモバイルデバイスのユーザーは、デバイスのオペレーティングシステムに事前にインストールされているアプリストアを通じてアプリをダウンロードします。オペレーティングシステムとアプリストアがセットになって提供されることで、デバイスのオペレーティングシステムがアプリストアの利用規約

を遵守させ、非承認のアプリがデバイスの制御やユーザー情報にアクセスすることを防ぐことができます。残念ながら、アプリエコノミーの中でいくつかの最大手企業が、政策立案者を募って、ソフトウェアプラットフォームが消費者がメインのアプリストア以外からアプリをダウンロードする能力を管理することを禁止するよう求めるキャンペーンを開始しました。言い換えると、彼らは政府に対して、ソフトウェアプラットフォームにサイドローディングを許可するよう要求し、一部の提案では、プラットフォームがサイドローディングアプリの潜在的な危険性について消費者に警告することさえ禁止するよう求めています。

特に、2つの主要なソフトウェアプラットフォームは、消費者に損害を与える可能性のある未調査のソフトウェアのサイドローディングを防ぐために堅牢な対策を講じています。たとえば、iOSではサイドローディング（メインのアプリストア以外からソフトウェアをスマートデバイスにダウンロードすること）が禁止されているため、AppleのApp Storeの利用規約では著作権侵害が禁止されています。そのため、コンテンツを盗むようなサイドローディングされたアプリをiOSデバイスにインストールするのは困難です。同様に、Androidも著作権窃盗犯にとって問題となります。Google Playストアでは、著作権侵害に関与したり、著作権侵害を助長したりするアプリも一般に拒否されます。また、現在のAndroidのデフォルト設定では、サイドローディングは許可されていません。ただし、ユーザーは設定に入り、「不明なソース」からのサイドローディングを一つずつ許可することができます。

サイドローディングを防止するソフトウェアプラットフォームの機能は、サイドローディングされたアプリにインストールされたマルウェアを使用して個人情報にアクセスし、犯罪行為を行う悪意のある攻撃者から消費者を保護します。さらに、個人から大手エンターテインメント企業に至るまで、著作権所有者は現行の法律に基づいて利用可能なツールを使用して、偽造アプリや映画、音楽、テレビを違法にストリーミングするアプリを削除しています。それでも、サイドローディングされたアプリは、主に無料であり、最も人気のあるストリーミングやテレビ番組を含む、料金を支払わずにコンテンツにアクセスできるという点で消費者に魅力を持っています。ソフトウェアプラットフォームに対して、未検証のソフトウェアを許可するための法的な義務や裁判所の命令は、著作権所有者とその顧客にとってコストがかかることとなります。

サイドローディングを禁止するプラットフォームに対する政府の介入案は、通知と削除手続きの効果を弱めることとなります。（例えば、違法なアプリを削除するために特定の対策を実施するオンラインサービスプロバイダーに限定的な免責を提供する法律など、著作権所有者からの侵害物の削除要求に迅速に対応する措置を講じるオンラインサービスプロバイダーを支援する法律を含めます）。私たちは、日本の政策立案者（およびその他の政策立案者や関係者）に対して、ソフトウェアプラットフォームでモバイルデバイス上のアプリまたはアプリストアを許可する必要がある場合、日本の法律に基づく削除がいかにか非効果的であるかを検討することを強く求めます。たとえば、偽のDisney+を装った映像コンテンツの窃盗に特化した詐欺師が、消費者に対してサイドローディングを行わせ、可能な限り多くの個人デバイスにマルウェアをアップロードしようとする場合、サイドローディングを容認する提案では、Appleのようなプラットフォームがそのアプリを削除したり、デバイスの機能や個人情報へのアクセスを遮断したりすることができなくなります。なぜなら、そのアプリは名目上、Apple TV+と競合するからです。たとえDisneyが削除通知を提出したとしても、違法の推定は適用されます。このような状況では、プラットフォームは手を縛られ、削除要請に対する遵守による法的責任を負う可能性があります。これにより、プラットフォームが違法なコンテンツに対処する

能力が事実上なくなってしまう。

アプリストアに対する政府の命令によって未審査のサードパーティ製アプリがスマートデバイスに許可されるようになると、消費者のマルウェアのリスクが増し、ハッカーがユーザーの個人情報にアクセスする可能性が高まります。サードパーティ製アプリをサイドロードしたい消費者の大半は、デバイスを「ジェイルブレイク」するか、デバイスの設定を使用して信頼されたアプリのダウンロードを許可する必要があります。この制限は、悪意のある攻撃者が無知な消費者にアクセスするのを防ぐための簡単で効果的な障壁を提供します。偽造ソフトウェア アプリは、消費者データの損失、サービスの中断、デバイスの誤作動、コンテンツへのアクセスの喪失、デバイス保証の無効化、個人情報の盗難、詐欺、さらには著作権侵害による民事および刑事訴追につながる可能性があります、実際に引き起こされます。

消費者にとってのコストは明らかに大きいですが、企業の評判や収益への損害も同様です。コンテンツやサービスを提供する企業は、顧客の保護に強い関心を持っています。著作権侵害や偽造ソフトウェア アプリはエンドユーザーの信頼を脅かし、評判悪化につながる可能性があります。これらのコストを定量化するのは難しいかもしれませんが、それでも否定することはできません。日本の政策立案者を含む規制当局が、モバイルエコシステムにおいて偽造アプリを正規のアプリと同等の立場に置かないことが重要であり、消費者が間違ったアプリをダウンロードした場合に危険にさらされることとなります。ソフトウェア プラットフォームは、コンテンツ プロバイダーとその顧客の両方に利益をもたらす安全なオンライン マーケットを提供する上で必要かつ重要な役割を果たします。スマート デバイスを管理するための複数のオプションと柔軟性があることも優れた点です。しかし、サイバー犯罪者がアプリ マーケットプレイス内にショップを開設できるようにすると、著作権侵害が増加し、収益が失われ、顧客の不満が増大することとなります。これらおよび上記の理由により、私たちは日本の政策立案者に対し、ソフトウェアプラットフォームが偽造アプリやその他の盗まれたコンテンツを削除することを妨げるような政策変更を追求しないよう強く警告します。

プラットフォームの指令が国際貿易に与える悪影響

政策立案者は、DMA（および同様の競争プラットフォームの介入）が、デジタル経済における外国の競争相手、特に日本のデジタルイノベーターとみなされる企業を差別することを目的とした貿易障壁であることを認識すべきです。DMA は、モバイル エコノミーの成功と成長を可能にしてきた自由で公正な貿易の原則と条件に反するものであり、他の重要な市場で DMA が複製される可能性は、イノベーションと雇用創出に対する脅威となります。この結論は、DMA をいくつかの角度から分析することで明らかになります：

- DMA の「ゲートキーパー」の範囲
- 非関税貿易障壁 (NTB) としての DMA 禁止事項
- 世界貿易機関協定に基づく差別禁止
- 世界的な文脈における DMA の貿易上の懸念

DMA の「ゲートキーパー」の範囲。

DMA の範囲は、一見しても差別の懸念を引き起こします。DMA は、欧州委員会 (EC) が「ゲートキーパー」とみなした団体にのみ適用されます。このような決定を行う際、EC は、特定の企業が次の 3 つの定性的基準をそれぞれ満たしているかどうかを分析します。(1) 「内部市場に重大な影響を与えている」。(2) 「ビジネス ユーザーがエンド ユーザーに到達するための重要なゲートウェイとなるコア プラットフォーム サービスを提供する」。(3) 「事業運営において確固たる永続的な地位を享受している、または近い将来そのような地位を享受することが予見可能である。」¹⁾しかし、一連の定量的要因により、企業が定性的テストを満たしているという EC の推定が成立します。(1) 過去 3 会計年度の EU での年間売上高が少なくとも 75 億ユーロであった、または前会計年度の平均時価総額または同等の公正市場価値が少なくとも 750 億ユーロであり、および少なくとも 3 つの加盟国で同じコア プラットフォーム サービスを提供する。(2) 昨年会計年度において、EU 内で月間アクティブ エンド ユーザーが少なくとも 4,500 万人、年間アクティブビジネス ユーザーが少なくとも 10,000 人いるコア プラットフォーム サービスを提供している。および(3) 過去 3 会計年度のそれぞれで、(2) の基準を満たした。²⁾

定量的要因により、EC は大企業を「ゲートキーパー」とみなし、DMA の対象とする広範な裁量権が与えられていますが、議論の多くは定量的要因に焦点を当てています。定量的要因は定性的要因が満たされているという前提を生み出すからです。この推定は、競合する欧州の同業者を除外しながら、大規模なプラットフォーム企業に適用するように調整されているようです。Spotify などのオンライン マーケットプレイスを運営する欧州最大の企業でさえ、基準を満たしていない可能性があります。Spotify の価値は最近変動していますが、企業価値の基準である 750 億ユーロを依然として大幅に下回っています。ヨーロッパの他の最大手企業は現時点で定性的基準を満たしていないようであるため、DMA がヨーロッパのすべてのプラットフォームを取り上げることを断るか、それともほぼすべてのプラットフォームを取り上げることを断るかという文脈で Spotify が最も引用される傾向があります。興味深いことに、ブッキング・ドットコムはこの規則の対象となる可能性のある欧州企業としてEUの政策立案者によって頻繁に引用されていますが、同社はコネチカット州に本社を置くブッキング・ホールディングスの完全子会社であり、規則が適用されるのは非EU企業であるという事実がさらに強調されています。数字が何を示すかに関係なく、欧州の政策立案者が欧州企業を支援する目的で外国企業を取り上げる意図を持っていたという証拠になります。欧州議会の議員らも同様のことを公的に認めています。³⁾

¹⁾ デジタル分野における競争可能かつ公正な市場に関する、2022 年 9 月 14 日の欧州議会および理事会の規則 (EU) 2022/1925 および指令 (EU) 2019/1937 および (EU) 2020/1828 の修正、第3条(1)は、<https://eur-lex.europa.eu/eli/reg/2022/1925/oj>【デジタル市場法 (DMA)】に掲載

²⁾ ヴァネッサ・アンマリー・ターナー「EUデジタル市場法 – デジタル市場の新たな夜明け?」AMER. BAR ASSOC. Vol. 37、第 1 号 (2022 年秋)、https://www.americanbar.org/groups/antitrust_law/resources/magazine/2022-fall/eu-digital-markets-act/?login (DMA、第 3 条第 2 項を引用)。

³⁾ 「EUはトップ5のハイテク企業に焦点を当てるべきだと主要議員は語る」フィナンシャル。タイムズ、<https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b> (ペイウォール)を参照。

このような立法の歴史に加えて、DMA は、共通点がほとんどなく、まったく異なる市場で競合するビジネス モデルを持つ複数のオンライン マーケットプレイスとプラットフォームを対象としています。同じ DMA 規定が、行動広告から収益の相当額を得ているソーシャル メディア プラットフォームと、販売者と購読者から収益を得ている小売プラットフォームの両方に適用されるという事実は、この範囲の目的が次のとおりであることを明確に示しています。対象事業体が競合する市場の種類や、顧客、競争、または EU 域内市場に損害が発生したかどうかには関係ありません。企業の行為から生じる潜在的な危害が共通のルールの対象となるのに十分な類似の属性を有するように、少なくとも同じ種類の市場で競争する企業に対して、競合と消費者への損害を軽減するための規制をもっと調整することを、政策立案者は期待されるでしょう。たとえば、高インフレの時期には、DMA で規制されている小売業者とそうでない小売業者間の競争圧力を減らすことは逆効果になる可能性があります。

DMA の立法意図とその定量的要因の両方からの証拠は、DMA の範囲自体が WTO 協定分析の下で差別の問題を引き起こす可能性があることを示唆しています。貿易およびサービスに関する一般協定 (GATS) に基づき、加盟国政府は、他の加盟国の管轄区域に拠点を置く競合他社に対し、国内に拠点を置く「同様のサービスおよびサービス提供者」よりも「不利な」扱いに同意する場合、差別的行為を示す可能性があります。皮肉なことに、DMA の柱の 1 つは、プラットフォームを介して提供される独自のサービスについて、対象となるプラットフォームによる優遇措置の禁止です。したがって、EC も、DMA が軽減と防止を目指しているのと同じ種類の差別行為の責任を負っている可能性があります。しかし、注目すべき違いは、DMA の対象範囲が、市場規律によって罰せられない価格引き上げや生産制限を可能にする可能性がある実証可能な市場支配力を持つ企業に限定されていないことです。一方、EC は、EU 競争法の分析や日本の独占禁止法の原則に基づいて想定されるあらゆる形態の市場支配力を大幅に超える政治権力を行使する可能性があります。つまり、新しい法律の採用により、市場または市場主体の業績や価格に一方的に影響を与える可能性があります。したがって、国籍に基づいて特定の企業を差別するために政府権力を行使することを精査することには、オンライン市場における同様の差別を防止する法律の制定と同様に、少なくとも同等に強い貿易関連の公共の利害があります。

非関税貿易障壁 (NTB) としての DMA 禁止。

DMA の範囲が差別的であるかどうかという問題と切り離せないのは、その要件の内容がその範囲内の市場やプラットフォームに不当な負担を課すかどうかという問題にあります。加盟国はまだ NTB に関連した競争政策に特化した WTO 協定を採択していませんが、この問題に関して参考となる関連する分析的および外交的枠組みは存在します。例えば、加盟国は、「WTO の枠組みにおいてさらなる検討に値する分野を特定するために、反競争的慣行を含む、貿易と競争政策との相互作用に関する加盟国が提起した問題を研究するための作業部会」を設立することに同意しました。同様に、最近設立された米国・EU 貿易技術評議会 (TTC) は、交渉当事者が潜在的な NTB に対処し、さまざまな技術関連問題について政策アプローチを調整するため

⁴ シンガポール閣僚宣言、世界貿易機関、(1996 年 12 月 13 日に採択)、https://www.wto.org/english/thewto_e/mission_e/min96_e/wtodec_e.htm。

の二国間会議の場を提供しています。⁵実際、TTC のサブグループの 1 つであるワーキング グループ 5 では、特に「データ ガバナンスとテクノロジー プラットフォーム」を取り上げています。⁶ TTC を設立する米国と EU の共同声明の中で、署名国は「オンライン プラットフォーム サービスのグローバルな性質を認識し、安全、公正、オープンなオンライン環境を確保するためのそれぞれのポリシーの施行に協力することを目指す」と述べています。⁷オンライン プラットフォームのグローバルな性質を認識することは、オンライン プラットフォームに関連する署名国のポリシーが、当事者が採用することを選択した協定の下で NTB または同様の障壁となるかどうか、またどの程度の障壁となるかを判断するのに役立つかもしれません。

2 つの DMA の義務は、プラットフォームのグローバルな性質や、プラットフォームが安全、公正、オープンなオンライン環境を促進する程度を干渉する可能性があります。まずはDMAの第6条(4)では、対象となるゲートキーパーに対し、「そのオペレーティング 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 ストアのインストールと効果的な使用を許可および技術的に可能にすることを求めています。⁸この義務によって生じる明らかなセキュリティとプライバシーの問題を改善するために、2 つの差し止め請求があります。1つ目は、サードパーティのアプリやアプリストアが「ハードウェアやオペレーティングシステムの完全性を危険にさらさない」ことを保証するための措置を講じることをゲートキーパーが「妨げられない」ということですが、それは「厳密に必要であり、かつ必要な範囲に限り」、「ゲートキーパーによって正当に正当化されている場合」というものです。2 つ目は、ゲートキーパーが、エンドユーザーがサードパーティから効果的にセキュリティを保護できるようにするデフォルト以外の対策や設定を適用することを「妨げられない」ということですが、これも「厳密に必要かつ適切な範囲」にあり、「ゲートキーパーによって正しく正当化された場合」に限られます。

たとえ「厳密に必要かつ適切」かつ「正しく正当化される」ことによって暗示される証拠提出義務を満たすことが比較的容易だったとしても（そしておそらくそうではないでしょう）、例外を「ハードウェアまたはオペレーティングシステムの完全性を危険にさらす」脅威に限定することはむしろ範囲が狭く、広範なサイバー脅威や消費者被害が含まれなくなります。したがって、第6条(4)の推定は、いかなるセキュリティ対策にも重くのしかかり、少なくとも推定上、現在小規模なアプリ会社とユーザーを保護している積極的なセキュリティ構造を確実に不可能にします。たとえば、世界的な大手アプリ ストアは現在、販売を承認する前にアプリを精査し、データ収集活動や、カメラや正確な地理的位置などの機密デバイス機能へのアクセスを、アプリの目的を果たすために必要な機能のみに制限していることを確認しています。ストアは、そもそも審査プロセスに合格したことに基づいてのみ許可されていたアクセスを取り消すことで、消費者をだまして、よ

⁵米国とEUの貿易と技術。米国貿易代表部執行委員会。OFFICE OF THE PRES. (2021年6月発表)、<https://ustr.gov/ustr/seuttcc>。に掲載

⁶ユーロ。共通、EU・米国の貿易と技術。評議会、ワーキング グループ 5 – データ ガバナンスと技術。プラットフォーム、<https://futurium.ec.europa.eu/en/EU-US-TTC/wg5>。に掲載

⁷米国・EU 貿易と技術に関する共同声明。評議会、2022 年 5 月 16 日、フランス、パリ・サクレ。12段落、<https://www.commerce.gov/sites/default/files/2022-05/US-EU-Joint-Statement-Trade-Technology-Council.pdf>。

⁸ DMA第5条(4)。

り機密性の高いデータを不正な目的で収集できるようにするアプリの削除を実行します。今回、DMAがその構造を違法化した場合、アプリストアは、消費者に意図的に害を及ぼすアプリを正規の開発者のソフトウェアと並んでストアに掲載することを許可すると同時に、アプリプラットフォームが現在アクセスを取り消すために使用している技術的メカニズムを廃止することが求められる可能性があります。これらの問題が実装時に対処されない限り、その結果、プラットフォーム上の安全性と公平性、そして最終的にはオンラインプラットフォーム自体のグローバルな性質に対する脅威が大幅に増大することになります。これらの結果は、潜在的なデジタル貿易 NTB に焦点を当てた TTC 交渉担当者やその他の貿易会場の焦点となる可能性があります。

DMA の 2 番目の要件である第 6 条(7) および第 6 条(10) は、連携して中国を拠点とする競合他社や悪質な行為者に意図せず有利になるように作用します。具体的には、第 6 条 (7) は、ゲートキーパーが、オペレーティング システムやその他のソフトウェア、デバイス機能と、ゲートキーパー自身の製品に提供されているのと同じレベルの相互運用性を提供することを要求しています。⁹第 6 条(10)は、ゲートキーパー事業体に「個人データを含む。非集約データへの高品質、継続的、リアルタイムのアクセス」を提供することを要求します。¹⁰ DMA は、この要件の適用対象を、「関連するビジネス ユーザーが提供する製品またはサービスに関してエンド ユーザーが実行する使用」に直接関係する個人データにのみ制限しています。。、およびエンドユーザーが同意することでそのような共有をオプトインする場合。¹¹残念ながら、この制限は、外国の敵対者が管理する組織が所有するプラットフォームやオンライン マーケットプレイスと個人情報を共有するというゲートキーパーの義務を取り消すほど狭いものではない可能性があります。同様に、第 6 条 (7) は、ヨーロッパの消費者のデバイス、オペレーティング システム、およびデバイス上のその他のソフトウェアへの可能な限り最良のアクセスを、外国の敵対者によって管理されている事業体に提供することをゲートキーパーに要求する可能性があります。同様に問題があるのは、このような必須の義務は、ダークパターンやプライバシー侵害による消費者保護法違反の繰り返しかつ永続的な実績を持つビジネスユーザーを排除する取り組みを複雑にしたり妨害したりすることです。¹²機密情報への継続的アクセスを提供するという第 6 条 (10)の要件と組み合わせると、この義務は、イノベーションのリーダーから基本的人権と民主主義を保護しない政府への強制的な技術移転の一形態になる可能性もあります。この観点から見ると、DMA は日本企業にとって貿易に対する非常にコストのかかる障壁となる可能性があると同時に、EU の外交的および経済的利益を世界的に損なう可能性があります。

世界貿易機関協定に基づく差別禁止。

⁹ DMA、第6条(7)。

¹⁰ DMA、第6条(10)。

¹¹同上。

¹²ACT | App Associationの会長であるモーガン・リードから上院商業・交通・科学委員会のリーダーシップに宛てた連邦政府に関する手紙。連邦貿易委員会とエピック ゲームズとの和解、<https://actonline.org/wp-content/uploads/2023-02-15-ACT-FTC-Settlement-Letter-to-Senate-Commerce.pdf>。

主要な 3 つの世界貿易機関 (WTO) 協定のそれぞれにおいて、署名国政府は通常、協定の対象となる国内外の商品およびサービスを平等に扱わなければなりません。具体的には、関税及び貿易に関する一般協定 (GATT) の第3条、^[13]貿易およびサービスに関する一般協定 (GATS) 第 17 条、^[14]および知的財産権の貿易関連の側面 (TRIPS) の第 3 条^[15]にそれぞれ、この差別禁止義務の概要を示しています。各条項は差別禁止の扱いが若干異なりますが、DMA の目的に最も関連する協定である GATS は、オンライン市場の規制上の扱いにどのように適用される可能性が高いかという点で非常に単刀直入です。第 17 条では、各会員は「他の会員のサービスおよびサービス サプライヤーに従うものとする。。。。自社の同様のサービスやサービス サプライヤーと同等の待遇を提供する」と規定しています。^[16]この義務は、サービスが EU 市場に参入した場合にのみ適用され、ヨーロッパでの使用がどれほど広く普及しているかを考えると、主要なオンライン マーケットプレイスやプラットフォームはその基準を満たす可能性が高くなります。

DMA のグローバルな文脈における貿易の懸念。

政策立案者らがハイテク関連政策の貿易への影響について議論を続ける中、オンライン市場に対する DMA の潜在的な差別的影響が焦点となるのは間違いありません。EC が自らの利益を積極的に主張する姿勢を考慮すると、政策立案者は、支援を求めるイノベーターや消費者の国家的重要な利益をしっかりと明確に表明することを躊躇すべきではありません。政策立案者らの異議は、DMA の範囲が特定のプラットフォームのみを対象とすることを意図しており、これに準拠するにはコストがかかるという事実よりも、もっと深いところまで踏み込むべきでした。DMA の制限の内容は、これらの貴重なプラットフォームの世界的な性質や、公正かつ安全なオンライン取引や商取引を促進する機能を保護するという条約に基づく約束にも違反する可能性があります。これには、環太平洋パートナーシップのための包括的かつ先進的な協定 (CPTPP) などの枠組みが含まれます。また、交渉担当者にとって、特に市場にコストを課すことは、最先端技術の研究開発への多額の投資能力を妨げることになるということを見逃すことは難しいでしょう。業界リーダーの投資インセンティブが大幅に減少すれば、我が国の経済と国家安全保障が弱体化することになります。通商政策当局者にとって、この結果から身を守ることは最優先事項でなければなりません。

これらの問題は、いくつかの国がオンライン市場を対象とした同様の規制の枠組みを真剣に検討している重要な時期に発生しています。これらの提案は、方法は若干異なりますが、DMA の基本要素の一部をそのフレームワークに暫定的に組み込むことを試みています。それだけでなく、EU はさらなる立法作業において基本的な DMA 枠組みを構築してきました。たとえば、EU の立法者は、EU データ法のような新しい立法

^[13]関税および貿易に関する一般協定 (GATT)、第 3 条。1994 年 4 月 15 日、https://www.wto.org/english/docs_e/legal_e/legal_e.htm#GATT94。

^[14]サービス貿易に関する一般協定 (GATS)、第 XVII 条、https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXVII[GATS]に掲載

^[15]知的財産権の貿易関連側面に関する協定 (TRIPS)、第 3 条、1994 年 4 月 15 日、https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm。

^[16]GATS 第 17 条、1段落。

提案に「ゲートキーパー」の概念を取り入れ始めています。この新しい法律の下では、DMA のゲートキーパーは、競争力の強弱に関係なく、他の企業に与えられた権利を行使することができなくなり、競争圧力がさらに軽減されます。したがって、DMA の貿易への影響については、政策立案者が世界の他の地域への DMA の卸売輸入に抵抗すべき理由をよりよく理解し、EC によるその実施について情報を提供するために、さらなる研究と分析が必要です。政策立案者は、DMA やそれに類似する提案を支える主要な前提に注目し、反対すべきであり、世界中の政府関係者がそのような介入がもたらす大きなコストを公然と評価するのを助けるために行動すべきです。