**後悔先に立たず: 大手アプリ企業、欧州で蒔いた種の報いを受ける**

はてさて、よく使われる言い回しですが、これが自分の行いの結果でなければ…。欧州でデジタル市場法（DMA）への遵守計画が進む中、このDMAを意識的に推進してきた人々は、こんな後悔を抱いているに違いありません。ただ、公の場で皮肉なしにそう表明したいと思うことはないでしょう。主要アプリストアを通じてアプリを配信している世界有数の企業たちは、自分たちが過ちを犯したとは当然ながら認めていません。DMAの推進者たちは、Appleの遵守計画にしてやられ、Appleが配信料を徴収し続けることにショックを受けたふり（？）をしています。皮肉なのは、これも彼らがまさに求め続けていたこと―すなわち自分たちからアプリ経済の残りの部分へとコストを転嫁すべきとの主張―がもたらした結果の一部であるという点です。どの程度の転嫁が望ましいかは、その考えが誠実なものか不誠実なものかは別にして、コストが政府の命令で帳消しにされ、「フリーランチ」になるかもしれないと考える信念の度合いによります。このような大手アプリ企業はDMAの実験から学ぶことは何もないと考えているかもしれませんが、各国政府にとっては、今からでもいくつかの点を心に留め置くのに遅くはありませんし、そうすることが非常に重要です。「American Innovation and Choice Online Act(アメリカのイノベーションと選択のためのオンライン法)」(AICOA)や「Open App Markets Act(オープンアプリ市場法)」(OAMA)のような提案により、世界中の政策立案者がDMA型の介入を求められている中、今回の経験から、我々はすでにいくつかの教訓を得ることが出来ます。

*教訓1：DMA型の介入は必ずプライバシーとセキュリティの脆弱性をもたらします。*DMAの第6条第4項では、対象となるソフトウェア・プラットフォームに対し、サードパーティのアプリストアを許可するよう求めています。私たちがこれまで指摘したように、規制当局がこの義務を厳格に適用すれば、現在スマートデバイス上で消費者を保護している、サイバーセキュリティやプライバシー上の常識的で能動的な対策のほとんどが排除されることになります。この義務の例外は、わずかに「ハードウェアやオペレーティングシステム（OS）の完全性を危険にさらす」脅威に対処する場合にしか認められていません。Appleの遵守計画が、配信するアプリが偽物でないと確認するために、公証を用いる権利を留保していることを踏まえ、欧州の規制当局がこの一節を厳密に解釈することの難しさを理解してくれることを願います。この公証の仕組みは、消費者にとって、DMA遵守過程における極めて重要な勝利を意味します。しかしながら、公証はプライバシーやセキュリティ上の脅威に対する基本的な保証手段のひとつに過ぎません。例えば、公証だけでは後述するペアレンタルコントロールの実装を求めることはできず、許可取得審査にも必ずしも対応出来ません。以前説明したように、許可取得審査とは、アプリが要求するデータの種類が取得目的と合致しているかを確認するために行われる、アプリストアによる審査です。許可取得審査が、人々のデバイスを危険にさらしたり、情報やID、金銭を盗んだりする、驚くほど頻繁に起こっている試みを防いでいます。セキュリティに係るこのレイヤーを競争相手に開放することは望ましいことだと言う人もいるかもしれません。しかし、その競争そのものが、消費者が他の方法よりも垂直統合型ソリューションを明示的に好み、選択することを通じ、このソリューションを生み出したことを忘れてはなりません。様々な競争の中でも、このひとつの側面におけるDMAの下での競争は、規制当局主導によって各企業のプラットフォーム上で創られた、まやかしの競争であるということ、このことを忘れてしまっては意味がありません。

また、ここで注目すべきは、OS・ハードウェア・ソフトウェアへのアクセスを認めないことが違法であるとの前提に立つOAMAは公証を含む遵守計画については認めないと思われる点にあります。OAMAが認める「エンドユーザーに対する、サードパーティ製アプリやアプリストアの信頼性や出所を確認する技術的手段の提供」は積極的抗弁によってのみ可能となります。そして、この積極的抗弁は、プラットフォームが「第三者の排除、または不必要な条件や差別的な条件の適用」を行う口実として公証を用いていないと証明できる場合にのみ行うことができます。この文言は、ソフトウェア・プラットフォームにとって、何千万ドルもの訴訟費用を投じてそれを守ろうと考えるに至るまで、公証を手の届かないところへ遠ざけるもののように感じます。結局のところ、公証は、Appleが、彼らが製造したスマートデバイス上のセキュリティとプライバシーに対する、わずかな管理手段を維持するのみなのですが、AICOAとOAMAは、いずれも、これらの措置は競争を阻害する口実であるとの基本的な前提のもとに起草されているのです。

*教訓2：DMA型の介入は、米国議会がペアレンタルコントロールとオンラインの安全性を政策目的として優先しているにもかかわらず、それらの機能を損ないます。*公証が有するもうひとつの限界とDMAが認めるより幅広い自由のもとでは、サードパーティーストアで購入されたアプリにプラットフォームレベルでのペアレンタルコントロール機能は強制されません。むしろ、DMAは、代替アプリストアからダウンロードされたアプリへのペアレンタルコントロールをその購入元のアプリストアが行うことを要求しているように見受けられます。これでは、保護者が子どものアプリダウンロードを管理することははるかに困難となり、ともすればあれもダメこれもダメと加えていくことで崩壊する、昨今の新たな子育て問題において摩擦が増加します。米国の現行法は、保護者が子どものデバイスを設定し、[アプリのダウンロード・購入・使用状況を自分のスマートデバイスから確認できるとしています。](https://actonline.org/2024/01/31/developers-write-software-parents-parent-government-should-do-neither/)EUでは、この問題ははるかに複雑な状況となり、サードパーティーストア経由でダウンロードされたアプリには適用されません。これはとりわけ、最も認められた、最も力のある代替アプリストア推進者の一部が[常に子どもたちのプライバシーを侵害していること](https://actonline.org/wp-content/uploads/2023-02-15-ACT-FTC-Settlement-Letter-to-Senate-Commerce.pdf)が周知の事実であると考えると、特に懸念すべきことと言えます。結果、ペアレンタルコントロールや保護者の監視を逃れるための代替アプリストア作りに彼らのリソースが投入されることはもはや明らかです。突き詰めると、DMAがもたらすトレードオフは、保護者がオンライン上でも保護者であることを―偶然ではなく意図的に―今以上に難しくする代替ビジネスモデルを優先し、反対にオンライン上で子どもを守る強力な手段を保護者のもとからほぼ剥奪することになるでしょう。

*教訓3：DMA型の介入は、小規模デベロッパーにコストを転嫁します。*何年もの間、ACTはAICOAやOAMAのようなDMA型の法案は、[小規模デベロッパー](https://actonline.org/wp-content/uploads/Platforms-and-Competition_web.pdf)に[配信コストを転嫁させる](https://actonline.org/2021/11/12/antitrust-and-you-part-3-nondiscrimination-provides-a-platform-for-me-but-not-for-thee/)ことになると警告してきました。主として、これらのコストは、アプリメーカーがより多くのストア向けにアプリを開発する必要が生じたり、異なるアプリストアの利用規約をすべて遵守する必要が生じたりするなど、まだ見ぬ間接的な方法で顕在化することになるでしょう。この他にも、消費者がスマートデバイス上でより慎重な態度を取らざるを得なくなるなど、その間接的影響を数えればきりがありません。しかし、直接的なコストについては、私たちの警告が正しかったことが即座に判明しました。アプリストアに対するマストキャリー規制導入法案に関して行われた州議会の公聴会で、ACTは、最大手のアプリメーカーに課されるアプリ内課金手数料を廃止すれば、その手数料は必ずすべてのアプリメーカーに転嫁されることになり、結果的に小規模アプリメーカーのコストと参入障壁を不釣り合いに高めることになると指摘しました。ある議員の回答は、アプリストアが開発者登録料として数千ドルを徴収することで、すべての開発者にコストを分配すべきというものでした。それにより、アプリストアの維持とアプリの配信にかかるコストの多くを最大手のアプリ企業が一方的に負担しなくて済むようになるとの理由でした。もちろんこれは、公共政策が目指すべきところとは正反対の考え方です。なぜなら、提案された解決策は（むしろ不公平なほど）最小規模のアプリ企業のストア利用料を現在の100倍以上に引き上げ、最大手企業が負担しているアプリストアのコストを実質的にほぼゼロにするものだからです。この点、大手アプリ企業が切実に求めていたものの少なくとも一部は手に出来たことになり、彼らにとってはある程度ミッションが達成されたと言ってよいでしょう。

DMAが何を生み出すか、その多くはまだわかりません。ただ、今わかることは、直近の遵守計画の進展により、大手アプリ企業は求めていたものを手に入れつつあること、そして消費者や小規模アプリ企業は報われそうにないということです。今こそ、世界中の政府がこの試みの真の姿を見極める時です。政治リソース、プライバシーとセキュリティの保護手段、国民負担、消費者価値、そしてアプリ流通の価値の膨大な毀損・流出につながるこの試みの見返りは、目に見えるものがあるとしても、大手アプリ企業のコストをわずかに下げること以外にほとんどありません。