2023 年 8 月 18 日

デジタル市場競争会議の「モバイル・エコシステムに関する競争評価 最終報告」に対する Centre for Information Policy Leadership のコメント

Centre for Information Policy Leadership（以下「**CIPL**」）[1]は、デジタル市場競争会議（以下「**DMCH**」）の「モバイル・エコシステムに関する競争評価 最終報告」（以下「**最終報告**」）に対してコメントを提出する機会を歓迎します。CIPL は、DMCH が日本のデジタル経済において効果的なデータ保護を確保しつつデジタル市場における競争の促進を目指すことについて支持します。

CIPL は、日本のデータ関連の法規制の策定の動向を長年にわたり注視しており、データ関連の問題や規制を扱う日本の関連規制機関、特に個人情報保護委員会（以下「**PPC**」）、及び最近では DMCH と頻繁に連携しています。特に、CIPL は、2022 年 6 月 9 日に DMCH が公表した「モバイル・エコシステムに関する競争評価 中間報告」（以下「**中間報告**[2]」）に対し、欧州連合（以下「EU」）のデジタル市場法（以下「DMA」）提案に対する関与の過程で CIPL 会員企業およびその他のステークホルダーから収集した意見[3]を含め、コメントを提出しました。CIPL が最近日本に関与した例として、2023 年 6 月に東京で開催された G7 データ保護・プライバシー機関ラウンドテーブル会合に併せ開催されたマルチステークホルダー・ラウンドテーブルで、信頼性のある自由なデータ流通（Data Free Flow with Trust）推進におけるグローバル越境プライバシールール（Global CBPR）の潜在的役割を検討しました。また、CIPL のボヤナ・ベラミー代表は、日本の主要関係者や政策立案者、海外からのゲストを招いて PPC が主催した G7 DPA 公式サイドイベント「PETs（プライバシー強化技術）の可能性の検討／AI 利用における個人データ保護」のモデレーターを務めました。ラウンドテーブル会合、サイドイベントともに、PPC、経済産業省（METI）、民間企業の代表者が参加しました。さらに、CIPL のボヤナ・ベラミー代表は最近、PPC の代表も参加した IAPP のアジアプライバシーフォーラム 2022 で、「Cross-Border

[1]CIPL は、Hunton Andrews Kurth 法律事務所内にあるプライバシーおよびデータ政策に関するグローバルシンクタンクで、本法律事務所および世界経済の主要セクターにおけるリーダーである 85 社を超えるメンバー企業から財政的支援を受けています。CIPL のミッションは、情報化時代である現代において、効果的なプライバシー保護および個人情報の責任ある利活用双方の実現に向けたソートリーダーシップ(thought leadership)の発揮とベストプラクティス開発です。CIPL の活動は、世界中のビジネスリーダー、プライバシーおよびセキュリティ専門家、規制当局、政策立案者間の建設的な協働を促進します。詳細については、CIPL ウェブサイト http://www.informationpolicycentre.com/をご覧ください。本コメントの内容は、個々の CIPL 会員企業または Hunton Andrews Kurth 法律事務所の見解を表すものとして解釈されるべきではありません。

[2] 日本デジタル市場競争会議「モバイル・エコシステムに関する競走評価 中間評価」（2022 年 6 月 9 日）に対する CIPL の 回答。

[3]CIPL が DMA および GDPR との相互作用のコンテキストにおいて公開した 2 つのホワイトペーパーをご参照ください。CIPL ホワイトペーパー「Bridging the DMA and the GDOR - CIPL Comments on the Data Protection Implications of the Draft Digital Markets Act」および CIPL ホワイトペーパー「Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences」

Privacy Rules Are Going Global」というパネルディスカッションのモデレーターを務め、Global CBPR のような共同規制の認証メカニズムを通じて、信頼性があり説明責任を果たせるデータ流通を可能にすることの重要性について議論しました。本コメントにおいて、CIPL は、DMCH が提起した問題の本質と性質に関する議論の枠組みに有用となる、以下の見解を提示します。

1. 総評

a. 「共同規制の枠組み」アプローチの支持

CIPL は、DMCH が「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」（以下「**透明化法**」）で採用された共同規制的枠組みアプローチ、すなわち、政府が原則的な枠組みを提示し、指定されたパラメータ内で枠組みの要件を運用することを規制対象事業者に委ねる枠組みについて言及していることを支持します。このアプローチは、組織の説明責任、行動規範、認証などの共同規制的かつ強制力のあるメカニズムによってさらに運用可能な、**技術中立的で、将来を見据えた、成果ベースのデジタル規制とルールを**可能にする必要性を求める CIPL の提唱に沿ったものです。しかしながら、最終報告における多くの規制の方向性が事前規制となっているため、透明化法のようなアプローチは最終報告では部分的にしか採用がされていません。これには DMCH による慎重な検討が必要であり、透明化法のようなアプローチが日本におけるモバイエコシステムにおける競争を規制するのにより適しているのか否かという観点から評価する必要があります。さらに、DMCH は、透明化法が 2021 年に施行されたばかりであり、モバイル・エコシステムの重要な部分であるアプリストアに適用されることを念頭に置く必要があります。DMCH は監督の重複を避ける必要があり、既存の透明化法を考慮して、新たな規制案が必要かつ正当かどうかを明確にしなければなりません。

また、デジタル規制や政策立案には、CIPL が 10 年以上にわたって開拓してきた**組織の説明責任の原則**を盛り込み、推進することが不可欠です。説明責任は、組織が独自のリスクやユースケースに合わせてコンプライアンス対策を調整できる柔軟性を提供すると同時に、規制当局から求められた場合には、その処理に関する意思決定を説明および検証できることを組織に求めます。説明責任によって、達成すべき目標と成果を設定する一方、これらの立法目標をどのように達成するかは組織に委ねられるため、法制度のアジャイルさを保持し、原則と成果にもとづく規制を実現できます。

CIPL は、効果的なデータ規制とそれに対応する企業内での実施において、組織の説明責任が重要な構成要素であると考えています。組織の説明責任は、企業が業種や規模に関係なく利用できるものです。その**リスクベースの枠組み**は、企業がコンプライアンスへの取り組みにおいてリスク評価を実施し、リスクの高い活動を特定し、優先づけていることを、政府の規制当局や執行機関に保証するものです。また、リスク評価およびコンプライアンスへの取り組みを示せ

るよう企業に求めることで、調査や執行の措置も簡素化されます。CIPL は、DMCH にクラス最高のデータプライバシーとデータガバナンスの実践、および組織のコンプライアンスプログラムを開発するための標準として認知されている CIPL の**説明責任の枠組み**を検討いただくことを推奨いたします。[4]この枠組みは法律にとらわれず、データ保護からコンテンツおよびプラットフォーム規制、競争や責任ある AI に至るまで、デジタル規制のあらゆる分野に適用できます。

b. 規制当局の継続的な対話と関与

十分に機能するデジタル市場を実現するために、CIPL は、様々な政策と規制の視点を結集し、デジタル規制へのバランスの取れたアプローチを確保することが重要だと考えています。競争法は、効果的なデータ保護への影響を考慮しなければなりません。同様に、データ保護法の解釈と実行においては、競争への影響を考慮すべきです。この点で、CIPL は、DMCH がモバイル・エコシステムに関する規制を検討するに際し、PPC、総務省（MIC）、消費者庁（CAA）、内閣サイバーセキュリティセンター（NISC）、その他ステークホルダー及び影響を受ける企業と協議を行う取り組みを評価します。この対話により、経験や見解の交換を可能にし、DMCH が市場の力学、技術的な意味合い、規制対象事業体やデータ主体の関心について包括的に理解することを支援します。これがひいては、より公平で効果的なルールと成果につながります。CIPL は、規制当局と影響を受ける企業とのこのような対話および協議をさらに正式に発展し、可能な限り制度化し、継続的に実施することが重要だと考えています。

DMCH と PPC、MIC、CAA、NISC が正式に協力することは、十分に機能する競争市場と効果的なデータ保護の双方を可能にするソリューションを構築する上で極めて重要です。双方の目的を完全に達成できない場合、規制当局は、必要なトレードオフを理解し合意するために協力しなければなりません。重要なことは、分野横断的な規制協力を執行の場面だけに限定せず、規制の協議、策定、解釈の全ての段階や、規制横断的なサンドボックスのような革新的な規制ツールの使用にも拡大することです。[5]

その意味で、英国の Digital Regulation Cooperation Forum（デジタル規制協力フォーラム、以下「**DRCF**」）[6]やオーストラリアの Digital Platform Regulators Forum（デジタルプラットフォーム規

[4]組織の説明責任に関する CIPL のリソースと論文はこちらでご参照ください。
[5]CIPL は、規制のサンドボックスのような革新的な規制ツールの開発も奨励しており、モバイル・エコシステムにおける競争とデータ保護の相互作用は、規制のサンドボックスの候補として最適だと考えます。例えば、シンガポールの情報通信メディア開発庁(IMDA)は、2022 年 7 月、プライバシー強化技術（PETs）の実験を希望する企業を対象に、シンガポール初の PET サンドボックスを立ち上げました。同庁は最近、PET サンドボックス構想を支援するため Google との新たなパートナーシップを発表しました。
[6]Digital Regulation Cooperation Forum（DRCF）は、英国の 4 つの規制当局、すなわち、情報コミッショナー事務局（ICO）、競争市場局（CMA）、情報通信庁（Ofcom）、金融行動監視機構（FCA）が集まり、オン

制フォーラム、以下「**DP-REG**」）[7]は、デジタルおよびオンラインサービス特有の課題に対処するための効果的かつアクション・ドリブンな規制協力の例となりえます。例えば、DRCF の 2023 年／2024 年作業計画は競争とデータ保護の促進を含むものであり、オンライン広告市場、オンライン選択アーキテクチャの実践、潜在的な規制上の救済措置に焦点が当てられています。最後に、これらのイニシアチブは、より協力的で成果にもとづく共同規制モデルにおいて、影響を受ける業界のステークホルダーとの効果的な関わり方を示すものでもあります。

c. プライバシーとセキュリティの正当化による個人の権利の保護

CIPL は、デジタル経済には、とりわけ競争、イノベーション、公共とオンラインの安全性、サイバーセキュリティから、消費者とデータの保護に至るまで、データに関連するあらゆる利害を考慮した規制アプローチが必要であることに言及したいと思います。「モバイル・エコシステムに関する競争評価 中間報告」に対するコメントで強調したように、バランスの取れたアプローチを行うためには、一方の規制分野が他方より体系的に優先されるべきであるとか、競争リスク分析がデータ保護リスク分析より優先されるべき（またはその逆）であるといった想定を行わないことが重要です。

この点で、CIPL は、プラットフォーム事業者の特定の行為は、プライバシーとセキュリティ対策を確保するために行われるものであり、したがって、許容され正当化されうるという DMCH の認識を支持します。[8]共同規制の枠組みのアプローチに沿って、組織は、DMCH やその他の関連規制当局の要求に応じて、プライバシーやセキュリティを含む、コンテキストに応じたリスクアセスメントやその他のコンプライアンス対策を実施することができます。したがって、実質的な正当性なくプライバシーやセキュリティ対策が講じられることが懸念される場合、規制当局や執行当局は、業界と協力し策定され合意された明確な基準に基づいて、その対策が過度なものであるか適切なものであるかを判断できる可能性があります。しかしながら、DMCH と関連機関は、プライバシーを侵害するインシデントやサイバー攻撃のリスクが高まる中、プライバシーとセキュリティのイノベーションを受け入れる必要があります。

ライン上の人々と企業に利益をもたらすデジタル規制への首尾一貫したアプローチを提供します。詳しくはこちらを参照してください。

[7] デジタルプラットフォームの規制に対する合理的で一貫性のあるアプローチを支援するため、オーストラリア通信メディア庁（ACMA）、オーストラリア競争・消費者委員会（ACCC）、オーストラリア情報コミッショナー事務局（OAIC）、および e セーフティー監督官事務所が共同で Digital Platform Regulators Forum を組成しました。当イニシアチブは、競争、消費者保護、プライバシー、オンラインの安全性、データ問題など、デジタルプラットフォームの規制が交差する分野横断的な問題や活動について、独立した規制当局間で情報を共有し、協力することを目的としています。詳しくはこちらを参照してください。

[8] DMCH の最終報告の I. 3-1 項。なお、モバイル・エコシステムに関する競争評価 最終報告は、「I. 総論」及び「II. 各論」という、2 つの主要な章から構成されています。

競争市場ではプライバシーの利点が得られる可能性がありますが、個人の権利を保護するプライバシーとセキュリティのイノベーションは、競争の目標とは別のものであり、区別されるものです。 プライバシー領域に独占禁止法の原則を適用すると、個人の権利が損なわれ、競争市場の目標が弱まる可能性があります。 したがって、プライバシーとセキュリティの正当化は、個人情報保護法などの関連する法的要件の遵守だけに限定されるべきではありません。 その代わりに、組織は法的要件を超えた高度なプライバシーとセキュリティ対策を提供し、プライバシーとセキュリティ対策の堅牢性によって市場で差別化を図る機会を持つべきです。

d. 競争が消費者のプライバシー保護と選択肢の改善につながることについて

今日、プライバシーは単なるコンプライアンス上の問題ではなく、企業間の差別化を図るための重要な機会となっています。「シスコ 2022 年 消費者プライバシー調査（Cisco 2022 Consumer Privacy Survey）」によると、消費者の 76%が、データの扱いについて信頼できない組織からは購入しないと回答し、81%が、データの取り扱いは組織が顧客をどのように見ているか、また尊重しているかを示すものであるという意見に同意しました。[9]同様に、Cisco との共同で発表したレポート「Business Benefits of Investing in Data Privacy Management Programs」では、組織がプライバシープログラムに投資する際は、歴史的にコンプライアンスとリスクのために行われてきましたが、プライバシープログラムが、ビジネスの実現、持続可能なビジネス、ブランドの評判、競争力、そして顧客と消費者の信頼など、従来の法的コンプライアンスを超えた複数のメリットと投資対効果を提供するという認識が高まっていることが示されています。[10]
そのため、規制は消費者のために一定レベルのプライバシーとセキュリティの保護措置を確立するよう組織に求める一方で、組織は、特にデータプライバシーを差別化要因とする新技術の出現により、基本的なプライバシーとセキュリティの対策を成長させ、競合他社と差別化する機会を得ています。実際に CIPL は、堅牢なデータ保護と消費者の選択は競争力のある消費者プライバシー市場の先駆けであることを指摘したいと思います。個人のプライバシー保護を向上させるこのような競争と差別化は、業種や規模に関係なく、どのような組織でも利用できるようにする必要があります。したがって DMCH は、反競争的とみなされる可能性のある行為を正当化する可能性があるとして、プライバシーとセキュリティを考慮するだけでなく、エンドユーザーのためにより良いプライバシーとセキュリティを提供することに対する産業界と消費者の要求が高まっていることも認識する必要があります。いかなる規制も、こうした取り組みを阻害することなく、むしろ促進するものでなければなりません。

[9]「シスコ 2022 年 消費者プライバシー調査」（Cisco 2022 Consumer Privacy Survey）はこちら。
[10]CIPL と Cisco の共同レポート「Business Benefits of Investing in Data Privacy Management Program」はこちら。

さらに CIPL は、最終報告は主に市場関係者に焦点を当てており、消費者の視点には十分な重点が置かれていない点を指摘したいと思います。この点に関して PPC、METI、裁判所等の他の関係規制当局は、需要側、すなわちより優れたプライバシーとセキュリティ保護を求める消費者の選好を調査する上で、より適切な立場にある可能性があります。

e. EU の DMA モデルには、日本のモバイルシステムには当てはまらない特定の目的が存在

CIPL は DMCH に対し、規制への期待値と目標を明確にすること、および現行の競争体制が期待と目標に対応できるのか、あるいは新たな規制が必要なのか評価することを推奨します。例えば、CIPL の最新の論文「*Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences*」でも強調しているように、[11]EU DMA は、競争の調和を達成し、また各国が独自の競争規制当局と独立した司法機関を持つ EU 域内市場における断片的で一貫性のないルールを回避するため、という特定の理由により導入されました。[12]一方、英国[13]、韓国[14]、オーストラリア[15]、米国[16]など、ほかの管轄区域の執行メカニズムは、既存の執行体制が、

[11]CIPL 論文「Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences」2023 年 5 月 30 日

[12]CIPL は、欧州の立法府がデジタル市場法に関して拠り所とした法的根拠、すなわち「Treaty on the Functioning of the European Union」（欧州連合の機能に関する条約、以下「TFEU」）の第 114 条を検討しました。特に TFEU の 114 条は、国内規則を近似させ、域内市場における規制の分断を防ぐことを目的とした措置を採択する権限を立法府に与えています（調和条項）。「DMA Impact Assessment Report」（DMA 影響評価報告）およびその「Explanatory Memorandum」（説明資料）によると、TFEU 114 条は、（i）ゲートキーパーが提供するサービスの本質的な国境を越える性質、（ii）デジタルサービスの単一市場の機能に関するさらなる分断の危険性から、関連する法的根拠と考えられます。

[13] 英国の「Digital Markets, Competition and Consumers Bill」（デジタル市場・競争・消費者法）案は、英国の競争・市場庁（CMA）に、（i）ある組織が特定のデジタル活動に関連して「戦略的市場地位」を有するかどうかを判断するため、および（ii）相互運用性やデータポータビリティを強制するなどの目的で、対象を絞った競争促進的介入を設計し実施するための、広範な裁量権を与えています。執行に関して、CMA は、軽度かつ非公式な関与を重視し、必要な場合にのみ正式な執行措置に移行する段階的なアプローチを取ると予想されます。

[14] 韓国の公正取引委員会は 2023 年初め、市場参入を阻止して力を強めるプラットフォームをめぐる競争上の懸念が高まる中、デジタル経済における支配力の乱用に関する指針を発表しました。

[15] オーストラリアの競争・消費者委員会は、「Competition and Consumer Act 2010」（2010 年競争・消費者法、Cth）にもとづき、デジタル市場における競争を規定する現行法を執行しており、過去 6 年間にデジタルプラットフォームに関連し、以下 3 件の調査を行いました：DPI（Digital Platforms Inquiry）、DPSI（Digital Platform Services Inquiry）、AdTech Inquiry。

[16] 米国では、オープン・アプリ・マーケッツ法案（OAMA）、イノベーション・選択法案（AICOA）などの同様の法案が議論されているものの法制化されておらず、広く支持される可能性は低いです。業界団体、専門家、シンクタンクを含む多様な個人や組織が、国家安全保障、ユーザーのセキュリティ、プライバシー、米国の経済競争力などの問題に影響を与えるとの懸念を示しています。

ゲートキーパーが反競争的に行動しているかどうかをケースバイケースで検討できると考えています。

したがって、DMCH は、全面的な規範的規制を導入することなく、代わりに市場における特定の反競争的行為について個別的かつケースバイケースの分析を追求することで、同じ規制目的を達成することができる可能性があります。先ほど指摘した通り、事前規制の場合、規制当局は、介入の有無によって、監督する将来の市場がどのようになるかを予測するために、その市場に関する事実を想定することになります。このような想定と予測の対象となる日本市場は、EU 市場とは実質的に異なっています。また日本のグローバル、地域的パートナーシップも実質的に異なります。アジア太平洋地域においては、欧州のような調和ではなく、収斂に重点が置かれており、また複数政党、複数国のシステム内における分断化を回避することにも重点が置かれています。規制の収斂においては、各国の規制枠組みの異なる特性を考慮し、各管轄区域の法制度に組み込まれている特定の文化の異なる価値観と優先順位を尊重します。収斂の考え方には、収斂のプロセスが動的でかつ柔軟である、つまりはテクノロジーの変化、市場の力学、国民の期待などに適応可能であるという考えが内在しています。しかし日本は厳格な事前規制を課すことで、このような柔軟性と将来性を備えた規制アプローチを失ってしまう可能性があります。したがって日本は、正当性のある競争促進的な行為を禁止することによって、日本の消費者に不利益をもたらすという予期せぬ結果をもたらすかもしれない、厳格な事前規制を回避するべきです。

2. 具体的なコメント

a. 決済・課金システムの利用義務付け（最終報告 II. 2-1 項）

- **競争上の懸念：**決済・課金システムの利用義務付けにより、代替的な決済・課金方法を提供する事業者の参入が妨げられ、事業者が多様な料金プランやサービスを提供することが妨げられ、イノベーションが低下する。ユーザーは選択肢を奪われ、様々なサービスを受けることができない。
- **DMCH による対応の方向性：**一定規模以上のアプリストアを提供する事業者に対し、アプリストアを利用する開発者に自社の決済・課金システムの利用を義務付けることを禁止する。当該事業者は、アプリストアのビジネスユーザー向けに、手数料を含め、公正、合理的かつ非差別的な利用条件を適用することが求められる。

CIPL は、ユーザーがさらに自由に代替サービスを選択できるように決済・課金サービスにおいて業界の競争を促進させるという DMCH のイニシアチブを支持します。しかし、DMCH は、代替手段を提供することでプライバシーやセキュリティを守る手段が損なわれたり、ユーザー側に混乱が生じたりすることがないようにしなければなりません。一般的にユーザーは、アプリストアが提供するようなプライバシーに配慮した安全な決済・課金ソリューションを利用すると考えられます。特に、十分に確立された枠組みが存在しない場合、悪意ある行為者が、返金やカスタマーサポートポリシーに対し様々なレベルの組織慣行、様々なレベルのプライバシーとセキュリティ保護を備えた複数のサービスに直面するユーザーを誤解させようとする可能性があります。さらに、代替の決済・課金システムを許可する場合、アプリストアは、特定の取引情報や個人に関するその他の個人データを代替サービスプロバイダと共有する必要があります。特にデータ共有に関する安全な規制の枠組みがない場合、個人データの拡散を招き、悪意ある行為者によるデータ搾取のリスクも高まる可能性があります。

規制対象となる組織は、プライバシーおよびセキュリティのリスク、新たな競争要件に従ってデータへのアクセスを提供することによる悪影響を事前に評価できる必要があり、データ受領者は、関連するリスク軽減措置を実施することが求められるべきです。

最後に、データの管理にもとづく責任の分担については、慎重に検討する必要があります。DMCH の指示に従った後のデータ受領者の行為について、規制対象の組織が責任を問われるべきではありません。

b. 信頼あるアプリストア間の競争環境整備（最終報告 II. 2.3.項）

- **競争上の懸念：**アプリの代替流通経路の制限は、次のように様々な競争上の問題を引き起こしている：（i）企業がアプリストア事業に参入する機会を失う、（ii）アプリストアの手数料に競争圧力がかからない、（iii）アプリのレビューが必ずしも透明で公正でないため、イノベーションとユーザーの選択が妨げられる。
- **DMCH による対応の方向性：**一定規模以上のオペレーティングシステムを提供する事業者は、セキュリティとプライバシーを確保しつつ、アプリの代替流通経路の実効的な利用を認めるべきである。

CIPL は、個人の選択の最適化と市場アクセスの改善は重要な政策優先事項と考えていますが、プライバシーとセキュリティを犠牲にしてそれらを実現すべきではないと考えます。実に、プライバシーとセキュリティに対する消費者の懸念は、アプリ代替流通経路の選択を常に上回るものです。消費者の選択と市場アクセスに対する措置を急ぐのではなく、意思決定者はこの慣行に関わる競合する正当な権利について、より広く深い分析を行うべきだと考えています。（中間報告へのコメントでも強調いたしましたが）CIPL は、DMCH に考慮いただきたい点をここで再度挙げたいと思います。

- アプリストアの所有者とアプリ開発者の双方に必要な法的確実性を提供する方法で、プライバシーとセキュリティを含む競合する正当な権利の両立や費用対効果の評価をどのように運用するか
- アプリストアの所有者、デバイスメーカー、ユーザーが、例えば合意されたセキュリティプロトコルを介して、悪意のあるアプリ（国家主導のサイバー攻撃やなりすまし詐欺など）からユーザーをどのように保護するか
- データプライバシーおよびセキュリティの侵害が発生した場合、ほかのどのような法律（消費者保護など）が関係する可能性があるのか、そしてサイドローディングによる侵害が発生した場合、オペレーティングシステム、アプリストアおよびデバイスメーカーがそのような法律にもとづく責任を負う可能性を検討するために、ほかの所轄当局とどのように連携するか
- サイドローディングに代わる、消費者の選択と競争の問題により効果的に対処できる、よりリスクの低い代替手段があるか
- サイドローディングがデジタルエコシステム全体と消費者に与える、プラスとマイナスの両面における長期的な潜在的影響

また、DMCH には、EU の DMA 制定過程における最新の規制の進展にも注視していただきたいと考えています。具体的には、DMA の提案では、代替流通経路からのサードパーティ製アプリケーションのインストールと効果的な使用を可能にする義務をゲートキーパーに課していますが、現在、最終文の規定は、対抗的利益に服することになっています。つまり、ゲートキーパ

ーは、ハードウェアやオペレーティングシステムの完全性を確保するための措置や、エンドユーザーのセキュリティを効果的に保護するための措置を講じることを妨げられません。[17]

さらに CIPL は、DMCH が業界と市場関係者に法的な明確性をもたらすアプリストアの行動規範やガイドラインの採用を検討していることを支持します。この点に関して、CIPL は DMCH に対し、最終報告で言及された行動規範、すなわち日本スマートフォンセキュリティ協会が作成している「セキュアコーディングガイドライン」、および英国の科学・イノベーション・技術省（以下「**DSIT**」）が公表した「Code of Practice for App Store Operators and App Developers」をさらに調査することを推奨します。DMCH は、このような行動規範を策定する際、開示と透明性の要件を慎重に検討し、アプリ開発者だけでなくサイバー犯罪者もデータにアクセスできる可能性があることを念頭に置く必要があります。例えば、英国の DSIT は、アプリストア事業者に対し、アプリやアップデート対して実施したセキュリティチェックの概要を一般にアクセス可能な形で提供することを求めています。[18]

最後に、DMCH は、プロバイダーがセキュリティとプライバシーを確保するための措置を講じる際に、オペレーティングシステムの比例性と必要性を精査するとしていますが、この比例性についてはさらに検討する必要があります。セキュリティリスクは増大し、テクノロジーは高度化しているため、「比例的」が何を意味するかは重要な議論になります。一般的に、規制対象の組織は、可能な限り高いセキュリティとプライバシー保護を目指すことができなければなりません。DMCH は、この急速に変化するデジタル空間では、プライバシー規制への法的遵守は最小限必要なものではあるものの、決して十分ではないことを念頭に置く必要があります。さらに、DMCH（およびその他の関係規制当局）は、プライバシーとセキュリティに関する技術的知識を持つ必要な専門スタッフを確保し、この業務に十分なリソースを割く必要があります。

[17]DMA 第 6 条 4 項。DMA の最終テキストはこちらをご覧ください。
[18] 2022 年 12 月 9 日に英国科学・イノベーション・技術省が公表した「Code of Practice for App Store Operators and App Developers」の 1.3.項は、こちらからご覧ください。

c. デフォルト設定、プリインストール（最終報告 II. 4-1.項）

- **競争上の懸念：**現状維持バイアスによってユーザーはデフォルトのサービスを利用する傾向があり、デフォルト設定のサービスには競争優位性があるため、ユーザーの自律的な意思決定や選択の機会を妨げている。ユーザーにアプリをインストールする選択肢を明確に示すことなく、自社のアプリを自動的にインストールすることは、サードパーティを競争上不利な立場に追いやり、ユーザーの自律的な意思決定や選択の機会を妨げる。
- **DMCH による対応の方向性：**一定規模以上のオペレーティングシステム提供事業者は、（i）オペレーティングシステムまたはブラウザのデフォルト設定をユーザーが容易に変更できるようにし、かつ技術的に可能にすること、（ii）オペレーティングシステムがデフォルトでユーザーに案内または誘導するブラウザ、検索エンジン、音声アシスタントの選択画面を表示すること、（iii）プリインストールされたアプリをユーザーが容易にアンインストールできるようにし、かつ技術的に可能にすること。しかし、場合によっては、アンインストールの制限を認める必要がある。

CIPL は、DMCH の方向性が、EU の DMA と同様のアプローチに従っていることに注目しています。[19]重要な点として、DMA は、サードパーティが技術的にスタンドアローンベースで提供することができないオペレーティングシステムやデバイスの機能に不可欠なソフトウェアアプリケーションに関して、アンインストールの制限を許容しています。実際、カメラ、メッセージ、メールアプリといった特定の機能は、オペレーティングシステムにとって不可欠な部分です。したがって、CIPL は、ある機能がオペレーティングシステムの中核機能を構成している場合、特にプライバシーやセキュリティに配慮した機能というコンテキストにおいては、アンインストールに制限を課す柔軟性をオペレーティングサービスに提供する DMCH の方向性を支持します。

CIPL は DMCH に対し、ユーザーが代替サービスのリストからインストールするかどうかを選択できるようにするため、ブラウザ、検索エンジン、音声アシスタントの選択画面を表示することをオペレーティングサービスに求めるという方向性について再検討することを推奨します。選択画面の表示が競争の促進につながる可能性はありますが、複数の選択肢に直面した時、個人が情報にもとづかない意思決定をするようになる可能性もあります。これは、ひいては効果的なプライバシーとセキュリティの保護に影響を及ぼし、選択メカニズムの価値を大きく損なってしまいます。したがって、選択画面に関する DMCH の対応の方向性は、非常に特殊な目的のみのために、また絶対に必要な場合にのみ、慎重に使用される必要があります。

[19]DMA 第 6 条 3 項。

d. 自社サービスの優遇（最終報告 II. 4-2.項）

- **競争上の懸念：**クエリで検索した場合、様々な自社サービス（地図、ビデオ、金融、航空券など）の検索結果がオーガニック検索枠の上部またはその近辺に表示されるため、ユーザーが代替市場プレイヤーを犠牲にしてそれらのサービスに移行することが可能になる。
- **DMCH による対応の方向性：**一定規模以上の検索エンジンを提供する事業者は、検索順位の表示において、類似のサードパーティサービスよりも自社のサービスを優位に扱うべきではない。

DMCH は、自社優遇や検索結果の表示全般の規制を検討するにあたり、それに伴う潜在的なプライバシーとセキュリティのリスクを慎重に検討する必要があります。最終報告の当テーマに関して、DMCH から損失となる実質的な証拠が提示されていないことを考えると、このような禁止による潜在的な損失及び意図しない結果についてより明確に検討していくことが特に重要です。多くの機能を実行するために、一般的な検索エンジン事業者は、地図、航空券、ビデオなどを提供する代替的なサードパーティ サービスと特定の種類のデータを交換する必要があります。このようなサードパーティ サービス プロバイダーの例は数百件ありますが、その多くは外国にあり、人権、プライバシー、セキュリティに同等の重点を置いていない可能性のある国の政府関連機関も含まれています。共有されるデータの種類には、少なくとも、クエリを行っているユーザーに関する情報と、ユーザーの選好に応じて位置データが含まれる可能性があります。共有されたデータは、プライバシー規則に遵守していない組織によって処理されたり、一部の国では国家安全保障や諜報目的で政府によるデータへの過剰なアクセスの対象となったり、あるいは最近採択された OECD「Principles for Trusted Government Access to Data」の対象にならない可能性があることから、データ共有にはリスクが伴わないわけではありません。[20]したがって、DMCH の対応の方向性として、代替サービスプロバイダが十分なプライバシーとセキュリティの保護措置を講じていない懸念がある場合、検索エンジン事業者の正当な理由を認める必要があります。

[20] OECD「Declaration on Government Access to Personal Data Held by Private Sector Entities」（民間部門が保有する個人データに対するガバメントアクセスに関する宣言、2022 年 12 月 13 日採択）はこちら。

e. エンドユーザーによるデータポータビリティの確保（最終報告 II. 5-3.項）

- **競争上の懸念：**オペレーティングシステムの乗り換えを容易にし、オペレーティングシステム間の競争を促進するうえで、データポータビリティの現状は簡便さに欠け、不十分である。
- **DMCH による対応の方向性：**一定規模以上のオペレーティングシステム、アプリストア、およびブラウザを提供する事業者は、エンドユーザーの活動を通じて発生したデータの効果的なポータビリティを可能にするため、エンドユーザーおよび当該エンドユーザーが認めたサードパーティからの求めに応じ、データポータビリティの実施を促進するツール、およびデータへの継続的かつリアルタイムでのアクセスを促進するツールを無償で提供しなければな

CIPL の調査と経験から、標準的な技術的枠組みが利用可能であること、共有側と受領側それぞれの義務と責任が明確であることが効果的なデータポータビリティの前提条件であることが示されています。データポータビリティを可能にする安全な技術的枠組みがない場合、悪意ある行為者によってデータが侵害されるリスクを高めることなく、データへの継続的かつリアルタイムなアクセスを実現できるフレームワークの導入を組織に委ねる必要があります。さらに、組織は、データ受領者が正規の事業体であることを保証するために、当局から明確なガイダンスを受ける必要があります。そうしない場合、組織がデータポータビリティ義務を遵守することで、適用されるデータ保護規則に違反することになりかねません。

最後に、データが正しい受領者に安全に送信された後は、規制対象となる事業者の責任は受領者に移る必要があり、受領者は受領したデータをデータ保護規則に従って処理し、付随するすべての責任を負わなければなりません。

f. ソーシャル・ログイン（最終報告 II. 5-4.項）

- **競争上の懸念：**アプリ開発者にアプリストアのソーシャルログインオプションの表示を義務付ける行為によって、アプリストアの立場を利用し、自社サービスを優遇することを可能にしている。
- **DMCH による対応の方向性：**一定規模以上のアプリストアを提供する事業者は、アプリ ストアを利用する開発者に対し、自社の本人確認サービスの利用、提供、相互運用を義務付けてはならない。

CIPL は、ユーザーに利便性、プライバシー、セキュリティなどを考慮した上で選択可能な、真の選択肢のリストを提供する必要があると考えています。

そうすることで、ユーザーはアプリストアの付帯サービスを利用するか、代替サービスが提供する付帯サービスを利用するかを自由に選択できるようになります。そうしなければ、個人は、プライバシーやセキュリティへの期待を含め、必ずしも期待に沿うわけではない、限られた選択肢に直面することになります。CIPL はまた、政策の対応の方向性は開発者へのアンケート調

査にもとづいて決定されるだけでなく、適切なバランスを探るために消費者へのアンケート調査を実施すべきであることを強調したいと思います。