

## 提出用フォーマット

意見 提出者名	所属(会社名・団体名等) または職業(個人の場合) 氏名(※) 住所(※)	Apple Inc.  [Redacted] [Redacted]
	連絡先	連絡担当者氏名: [Redacted] 電話: [Redacted] e-mail: [Redacted]

※ 法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地をご記入ください。

「モバイル・エコシステムに関する競争評価 中間報告」及び「新たな顧客接点(ボイスアシスタント及びウェアラブル)に関する競争評価 中間報告」に関する意見

1. 記載された内容に対する意見

<中間報告の該当箇所: ページ>

添付資料をご確認ください。

2. 記載された内容の他に、考慮すべき視点とそれに対する意見

添付資料をご確認ください。

内閣官房デジタル市場競争本部の  
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  
Apple のコメント

A. はじめに

1. スマートフォンのユーザーに対してできるだけ最高のユーザー体験を提供する製品を開発するという Apple のビジョンは、Apple が統合型アプローチをとっていることと、最高のソリューションにはハードウェアとソフトウェアの深い統合が必要であるという信念に当初から根ざしています。iPhone は、最先端の設計と、ハードウェアの構成要素（市場をリードする Apple のマイクロプロセッサ技術やカメラ等、Apple によって設計された構成要素を含みます）が緊密に統合されたパッケージと、iPhone の特徴に合わせて設計された独自のオペレーティング・システムとを組み合わせたものです。これによって当該システムの各コンポーネントが信頼できるものとなることで、当該システム全体が有効に機能し、競合他社のエコシステムとは異なる Apple 製品に特有の見た目や雰囲気（“look and feel”）を実現しています。このモデルにおいて、Apple の端末とサービスはそれぞれ補完的なものであり、それらが「全体」として顧客に満足をもたらし、Apple が質的に異なるスマートフォン体験を消費者に提供することを可能としています。
2. 質とセキュリティの水準を維持しつつ、サードパーティ App 内での使用のために自社の専有技術を開放するということから、消費者が自らのデータの取扱いについて説明を受けた上で選択することを可能とするプライバシー保護にかかるイノベーションを率先することに至るまで、Apple が行う各選択は、消費者の利益を向上させることを明示的に意図したものです。
3. さらに、デベロッパも Apple の取り組みによって多大な利益を得ています。Apple は、デベロッパが Apple の専有技術と知的財産を使用して、App をより容易に作成できるようにしてきました。そして Apple は、デベロッパが世界中の顧客に容易にアクセスできるようにしてきました。Apple は、世界中で一貫した規則、価格設定、ガイダンスと併せて、世界 175 ヶ国の顧客へのアクセスをデベロッパに提供しています。これにより、デベロッパが国境を越えて成功したり、新たな市場に参入したりするためのコストを下げ、それらの実現をより容易なものとしています。
4. さらに、デベロッパが低コストで参加できる App Store を提供・維持することによって、Apple は、それがなければ実現不可能であったかもしれない新たなビジネスを前に進めることを可能としています。また、Apple の安定した、安全で、信頼できるプラットフォームは、デベロッパによる将来の技術革新に向けた投資を奨励する環境を作ることに役立っています。Apple の App Store は、独立した小規模なデベロッパが、世界中のユーザーに追加投資無しで接触できるという膨大なビジネス・チャンスを作り出しており、より大規模で資金豊富な競合他社と同等に競争できるようにしています。これは、デベロッパが App Store から受けている利益について、高い割合のデベロッパが大いに満足しているとの結果を示している最近の調査によって裏付けられています<sup>1</sup>。これらのすべては、Apple のビジネスモデルによって可能となったものです。
5. 2022 年 4 月 26 日に内閣官房デジタル市場競争本部によって公表された「モバイル・エコシステムに関する競争評価 中間報告」（以下、「DMCH 中間報告」または「中間報告」といいます

---

<sup>1</sup> 経済産業省が実施したウェブ調査によれば、Apple の App Store ユーザーの 78.9%が、デジタル・プラットフォーム運営事業者が説明する不正決済の防止やエクスペリエンスの向上等のメリットを享受していると回答しています。

[https://www.meti.go.jp/shingikai/mono\\_info\\_service/digital\\_platform\\_monitoring/pdf/002\\_01\\_00.pdf](https://www.meti.go.jp/shingikai/mono_info_service/digital_platform_monitoring/pdf/002_01_00.pdf) をご参照下さい。

す。)は、これらの全体的な利益を認識し、Appleの「モバイル・エコシステムは、アプリやウェブ・サービスを提供するデベロッパにとっては、それまでには出来なかったような形で幅広いユーザー群にアクセスする機会を得られる場として、極めて大きな貢献を果たしてきている。特に、モバイル端末は、ユーザーが常時携帯し、利用しているという意味で、極めて強い顧客接点としての機能を有することから、これらデベロッパにとっての顧客接点も、時間やオケーションなどの広がりも含め、これまでにはないレベルでの機会がもたらされてきたと言える」と指摘しています<sup>2</sup>。

6. ユーザーにとっても、「サーチ、ショッピング、エンタテインメント、コミュニケーション、金融サービス、スマートホーム等の様々なサービスにとってのユーザー・インターフェイスがモバイル端末に集約する形で提供されており、常時保有し、いつでもどこでもデジタル空間に入って多様なサービスを利用することのできるゲートウェイとして、人々の生活をより豊かなものに変えることに大きな貢献を果たしてきている」と DMCH 中間報告は指摘しています<sup>3</sup>。
7. 全体的に、DMCH 中間報告は、「モバイル・エコシステムは、これらのサービスを利用する消費者の日常生活、そして、当該サービスを提供するビジネスユーザーの経済活動の基盤（インフラストラクチャー）としての機能を果たしている」とらえることができる」と考えています<sup>4</sup>。
8. それにも拘わらず、DMCH 中間報告は、合理的な根拠なく、これらの利益を完全に無視するか、あるいは単なる憶測に基づき退けています。その結果、DMCH 中間報告は、裏付けのない主張と憶測的な懸念から導き出された、技術、製品設計、および競争上の影響に関する結論に至っています。これらの裏付けのない主張や憶測的な懸念の多くは、消費者データへのアクセスの拡大を求めている苦情申立者らによって主張されたものです。そのため、DMCH 中間報告における調査結果（findings）は、事実上、Appleのエコシステムが「潜在的に」どのように競争を阻害する「可能性がある」かについての仮説に過ぎません。
9. Apple は、内閣官房デジタル市場競争本部が裏付けのない仮説的な問題に対する解決策を提案しており、その結果、ユーザーのプライバシーやデータ・セキュリティーを犠牲にして、ひと握りの有力なデベロッパを利するために現実に市場介入が行われ、iPhone の再設計を余儀なくされることを強く懸念しています。これは iPhone が 15 年間存在しており、Apple の投資と知的財産によって絶えず改良され続けており、何百万という消費者によって高く評価され信頼されている製品であるという事実を無視したものです。これらの変更は、消費者および最も幅広いデベロッパ群の双方に対して、選択肢を制限し、コストを大幅に上昇させる可能性があり、顧客との繋がりを Apple のエコシステムに頼っている小規模で新興のデベロッパを不利にし得るものです。
10. Apple は、内閣官房デジタル市場競争本部に対して、Apple のエコシステムが消費者とデベロッパの両方にもたらす利益についてより詳細な分析を行うこと、および、提案された各介入案について、その影響を受けることとなる様々な市場における消費者と競争に与える影響を客観的に検討することを強く要請します。また、Apple は、競争上の評価は単独で評価するべきではなく、(プライバシーやデータ・セキュリティーへの影響を含む) 消費者保護において意味することも等しく考慮し、比較考量するべきであると考えます。消費者への影響は、DMCH 中間報告で示唆されているような「例外的」な場合に限って関連性があるとされるべきでは

---

<sup>2</sup> DMCH 中間報告 14 頁。

<sup>3</sup> DMCH 中間報告 14 頁。

<sup>4</sup> DMCH 中間報告 35 頁。

ありません。この観点から、Apple は、内閣官房デジタル市場競争本部に対し、このプロセスに消費者やより幅広い利害関係者を含めることを強く要請します<sup>5</sup>。

11. この目的のため、以下の DMCH 中間報告に対する Apple のコメントにおいて、次のトピックを取り上げています。

- セクション B では、Apple のエコシステムの主要な構成要素とその開発について述べています。
- セクション C では、iOS 端末の安全性と性能を確実とするための手段の重要性について述べています。
- セクション D では、Apple のプライバシー・イニシアティブについて述べています。
- セクション E では、音声アシスタントとウェアラブルに関して提起された別個の懸念について述べています。
- セクション F では、内閣官房デジタル市場競争本部が検討中の対応オプションについて検討しています。

---

<sup>5</sup> 公正取引委員会の競争政策研究センターの「データ市場に係る競争政策に関する検討会」報告書は、「競争」、「データ保護」及び「消費者保護」の3つについて別個に議論するのではなく、三位一体での議論を行い、3つのバランスを欠かないようにすることが重要である」と明示的に結論付けています。  
[https://www.jftc.go.jp/houdou/pressrelease/2021/jun/210625\\_data.html](https://www.jftc.go.jp/houdou/pressrelease/2021/jun/210625_data.html)

## B. Apple のエコシステムの主要な構成要素とその開発

12. DMCH 中間報告で認識されているように、Apple のエコシステムは緊密に統合されており、その主要な構成要素によって、相互に補強し合う顧客向けのサービスが生み出されています。それは、消費者に選択肢がないからではなく、消費者が、提供されている価値を認識しているために機能しています。Apple のコマースエンジン (IAP) と Apple が課す手数料は、かかる構成要素の一つです。DMCH 中間報告は、IAP が顧客サービスや代替的な決済手段の発展に及ぼす影響について根拠のない仮説的な懸念を提起しており、IAP が消費者とデベロッパの双方に提供している利益を適切に考慮に入れていません。

13. また、内閣官房デジタル市場競争本部は、Apple がそのエコシステムを支えるルールを設定、更新、運用する際のデベロッパとのやり取りに関して、裏付けのない不正確な懸念も提起しています。以下のセクションでは、Apple はこれらの不備について述べます。

### (i) App Store の App 内課金が提供する利益が十分に理解・評価されていないこと

14. Apple の App Store における IAP 要件に関する中間報告の評価は、IAP の性質を十分に理解していません。IAP は決済処理ではありません。IAP は、Apple が手数料を徴収できるようにするコマースエンジンであり、取引を一覧化することで、Apple が App Store を運営し、デベロッパに対してツール、技術、ビジネスを行う機会、その他のサービスを提供することに対する対価を受け取ることができるようにします。IAP は、デベロッパに自身の App をマネタイズする手段を提供するとともに、App 内課金に至るために Apple が初めから用意した多くの機能（技術、顧客との繋がり、顧客の信頼など）に対する手数料を Apple が徴収することを可能にするものです。したがって、IAP が提供する利益と、決済処理業者が提供する利益とを比較することは、不適當かつ不十分な評価です。

15. また、IAP は、App Store におけるプレミアムな消費者体験の基本となる多くの機能を可能にするものです。このことは、IAP が、広範囲に亘る便益を提供していることから明らかであり、決済処理業者が提供するものとは実質的に異なるものです。IAP がもたらす便益は、以下のものを含みます。

- 子供が行うすべての App のダウンロード、App の購入、および App 内課金について親の承認を可能とする「ファミリー共有」と「承認と購入のリクエスト」。これらが金銭上および安全上の便益を提供していることは明らかです。
- 明確で分かりやすい価格設定。十分な価格情報がユーザーに提示されるまで購入が完了しないようになっています。
- Touch ID 対応端末では指紋、Face ID 対応端末では顔による生体認証。
- 領収書と購入履歴のメール送信。これにより、顧客は支出を把握・管理することができます。
- 「問題を報告」および「返金」。これにより、個々のデベロッパを探し出すことを必要とせず、Apple という評判を有する会社が単一の窓口として対応するという、大きな便益をユーザーに提供しています。
- 「購入の復元」。ユーザーが App 内課金のために「購入」ボタンを押したにもかかわらずデベロッパが何らかの技術的な理由で当該コンテンツを配信しなかった場合や、ユーザーが新しい Apple 端末に App や App 内課金したコンテンツを移行したい場合に、購入の完了や復元を可能にします。
- サブスクリプション管理。これにより、ユーザーは端末上で一回タップするだけで、複数の App のサブスクリプションを 1 つの便利な場所で簡単にキャンセルできます。

- 不正行為の防止。トレンドや全体的な動向を特定することによって、Apple が詐欺および悪意のあるデベロッパを根絶することを可能としています。
16. これらの便益は、ユーザー体験の向上にとどまらず、極めて重要な消費者保護機能を提供しており、悪意のある行為者が App Store 上の消費者に付け込むことができないようにすることで、ユーザーが安心して App Store を通じた購入をすることを可能にしています。例えば、「承認と購入のリクエスト」は、親が、子供によるデジタル商品やコンテンツの購入をコントロールすることを可能にします。重要なことは、デベロッパが、第三者の決済サービス提供者を利用することによってこれらのコントロールを回避しようとした場合は、Apple は直ちにその問題に対処することができるということです<sup>6</sup>。同様に、Apple のサブスクリプション管理は、サブスクリプションのための明確で分かりやすい情報開示と顧客の同意を要求することに加え、ユーザーがサブスクリプションをキャンセルすることを極めて容易にすることによって、オンライン・サブスクリプションに登録するように騙されたり陥れられたりする可能性のあるユーザーに対して、真の保護を提供しています。
  17. 最後に、IAP は、デベロッパに対して、価格設定について相当な柔軟性を与えています。Apple の価格設定方式は、デベロッパが App やデジタル・コンテンツの価格を自国の通貨で設定すれば、同等の価格が、世界 175 ヶ国の App Store の店頭で自動的に現地通貨に変換されることを可能としています<sup>7</sup>。これは、特に、価格設定、サブスクリプション、プロモーション等に関する現地市場の慣習をほとんど知らず、世界規模のサービスを提供することができないデベロッパにとって重要なものです。
  18. Apple は、自社のシステム上、安全かつ効果的な方法でサポートできる場合、より多くの柔軟性を導入し続けています。Apple は、デベロッパからのフィードバックに基づき、お試しオフター（新規ユーザー向け）、プロモーションオフター（失効した / 既存ユーザー向け）、そして最近ではサブスクリプションオフターコード（App 外配信向け）と、長期にわたって様々なタイプのサブスクリプション・オフターをリリースし続けています。
  19. 限られた数のデベロッパにより提起された主張と比較して、Apple の IAP がもたらす便益を適切に認識・検討しない限り、IAP が競争上の懸念を引き起こし、および／または、消費者に損害を与える可能性があるとして適切に認定することはできません。  
  
(ii) Apple の手数料は合理的であり、競争を制限するものではないこと
  20. Apple の App Store 手数料は、App のデベロッパが Apple の iOS プラットフォームの利用に対して支払うことに同意した料金です。Apple はデベロッパに対して、重要な技術およびマーケティングのノウハウを提供しています。Apple の提供する便益は、App・ソフトウェアの構成ブロック、Apple の知的財産のライセンス、iOS ユーザーの獲得、IAP およびその他の統合された iOS 機能から得られる便益、そして、技術支援、顧客サービス、マーケティングを含む Apple のサービスを受けられることを含みます。（内閣官房デジタル市場競争本部による）市場調査にかかる情報提供への要請に対する Apple の回答の中で記したように、Apple は App Store を

---

<sup>6</sup> このようなコントロールは、子供たち、特にゲーム・アプリを使用している子供たちが、意図するところなく大金を使ってしまう可能性を考えると、極めて重要です。例えば次のリンクをご参照下さい。  
<https://www.businessinsider.com/fortnite-addictive-epic-games-parliament-prince-harry-2019-6?r=US&IR=T#fortnite-sells-digital-currency-in-packs-for-between-10-and-100-parents-can-restrict-purchases-for-kids-but-it-requires-changing-account-control-settings-outside-of-the-game-4>。Epic Games の「Fortnite」に対する議会による質問をカバーするものであり、プレーヤー、より具体的には子供たちが、ゲームに時間または金銭を使い過ぎないようにするための適切な制限が設けられているか、という質問が含まれています。

<sup>7</sup> この価格設定の柔軟性は、デベロッパに対するマーケティング及び編集サポート、並びに請求及び税金に関するサービスに加えて提供されるものです。

含む iOS プラットフォームを開発、運営するために何十億ドルも支出しています。当該手数料は、デベロッパが Apple から享受し得る、そして現に享受する価値に基づくものであり、その価値と整合するものです。実際に、最近の調査<sup>8</sup>によれば、大多数のデベロッパが、当該手数料に相当するサービスを受けていること、および/または、Apple による説明を受け入れていることに同意しています。

21. 第二に、Apple はその手数料を 2008 年に初めて導入して以来、一度も引き上げたことがありません。実際には、Apple の手数料は時の経過と共に下がってきています。これは、Apple が一定の取引について手数料の支払いを免除しており、また、サブスクリプションおよび小規模なデベロッパが作成した App に対する手数料率を（30%から 15%に）下げたためです。実際、デジタル・コンテンツを販売している日本のデベロッパの圧倒的多数は、15%の手数料しか支払わなくてよい資格を有しています。さらに、App Store 内の全 App のうち、何らかの手数料を支払う必要があるのは約 15%に過ぎません。ほとんどの App は、Apple に何の手数料も支払いません。
22. 第三に、Apple の手数料は一度も業界の標準的な料率を超えたことがありません<sup>9</sup>。App 内課金に対する Apple の 30%または 15%の手数料は、Google Play Store（30%または 15%<sup>10</sup>）、Amazon App Store（30%または 20%<sup>11</sup>）および Samsung Galaxy Store（30%<sup>12</sup>）が課している料率を含む市場の料率と完全に整合しています。Microsoft Store は、ゲーム、ビジネスおよび教育ストアでの販売、そして Windows8 端末上での販売に対して、30%の手数料を課しています。Steam は、売上高 1 千万ドル以下に対しては 30%、1 千万ドルから 5 千万ドルの間に対しては 25%、そして 5 千万ドル以上に対しては 20%の手数料を課しています。中国内の App Store は一般的に 50%あるいはそれ以上の手数料を App 内課金に対して課しています。他のセクター内のプラットフォームも同様の手数料率を適用しています。YouTube は広告収入の 45%を徴収していると報告されており、Amazon は自社のプラットフォームを通じてビデオ・コンテンツが配信された場合、購入またはレンタル収入の 50%を徴収しています。電子書籍に対する一般的な手数料は 30~35%であり、オーディオブックは Amazon で 60%超、Kobo で 55~68%の手数料率を得ています。CDiscount は 39.99 ユーロの月額課金と共に最高 22%の手数料を課しています<sup>13</sup>。Spartoo は 39 ユーロの月額手数料に加えて 15%から 20%<sup>14</sup>の製品別手数料を課しています。これらの事例から、App 内課金に対する手数料率のうち最も高い 30%ですら、業界の標準的な料率であることが確認できます。

---

<sup>8</sup> 経済産業省が実施した Web 調査によれば、Apple App Store ユーザーの 75.2%が、自らの支払う対価に見合ったサービスを受けている、またはプラットフォーム運営事業者からの説明に納得していると回答しています。以下をご参照下さい。

[https://www.meti.go.jp/shingikai/mono\\_info\\_service/digital\\_platform\\_monitoring/pdf/002\\_01\\_00.pdf](https://www.meti.go.jp/shingikai/mono_info_service/digital_platform_monitoring/pdf/002_01_00.pdf)

<sup>9</sup> 他社との比較における Apple の手数料の詳細な分析については、以下をご参照下さい。

[https://www.analysisgroup.com/globalassets/insights/publishing/apples\\_app\\_store\\_and\\_other\\_digital\\_marketplaces\\_a\\_comparison\\_of\\_commission\\_rates.pdf](https://www.analysisgroup.com/globalassets/insights/publishing/apples_app_store_and_other_digital_marketplaces_a_comparison_of_commission_rates.pdf)

<sup>10</sup> 「Google Play デベロッパー販売/配布契約」、<https://play.google.com/about/developer-distribution-agreement.html>、Play Console ヘルプ、「お支払い」、

<https://support.google.com/googleplay/androiddeveloper/answer/9858738>; Play Console ヘルプ、「サービス手数料」、<https://support.google.com/googleplay/android-developer/answer/112622>。

<sup>11</sup> 「Amazon Developer Services Agreement」、<https://developer.amazon.com/support/legal/da>。

<sup>12</sup> Samsung Galaxy Store Seller Portal Terms and Conditions、<https://seller.samsungapps.com/help/termsAndConditions.as>

<sup>13</sup> CDiscount、General Conditions for Making Available the CDiscount Marketplace via the Hosting Site <https://seller.cdiscount.com/DocumentCgmad/20210501/ff8398f0-2afb-4e4a-8d3f-844497c2c5e9> (最終更新日 2021 年 5 月 1 日)。

<sup>14</sup> Spartoo、U.K. Department for International Trade: Selling Online Overseas, <https://www.great.gov.uk> Apple's response to Annex C of the Market Study information request, paragraph 6.7./selling-online-overseas/markets/details/spartoo/ (<https://cedcommerce.com/blog/sell-inspartoo-france/> も参照ください)。

23. Apple デベロッパ・プログラム (ADP) の年間料金は 99 米ドルで、Apple デベロッパ・エンタープライズ・プログラム (ADEP) の年間料金は 299 米ドル (いずれも適用可能な場合は現地通貨) であり、メンバーシップのある年ごとの料金です。これらは App Store の収入源とは考えられていません。これらの料金は、基本的に、Apple のツール・技術にアクセスするデベロッパが App Store で App を配信することに誠実になることを確保するために利用されます。App の配信後にデベロッパを特定することを可能にして詐欺を防止するために、クレジットカードの利用も求めています。日本には、500,000 以上の ADP メンバーと 35,000 以上の ADEP メンバーが存在しています。
24. この料金は、App ごとではなくデベロッパ・アカウントごとにかかります<sup>15</sup>。そのため、1 つのデベロッパ・アカウントにより複数の App を提出することもできますし、アカウントが個人ではなく法人である場合は、そのチームの複数のデベロッパが利用することができ、その場合も年間費用は 99 米ドルのみです。例えば、Google や Microsoft も、チーム内に多くのデベロッパがおり App Store で複数の App を提供しているものの、年間 99 米ドルのみの会費を支払っています。
25. デベロッパが、対象地域に所在する NPO、認証された教育機関、または行政機関であり、App Store で無料の App のみを配信する場合、App Developer Program の会員年間費用の免除を申請することができます。費用免除の資格要件は以下に記載されています。  
<https://developer.apple.com/support/membership-fee-waiver/>
26. また、DMCH 中間報告は、デベロッパが IAP の利用を完全に回避する方法で自身の App をマネタイズすることを選択できる程度を正しく認識していません。これらの方法のうち最も重要なものは、リーダールールやマルチプラットフォームルールなどのルールを使用するものです。これらのルールは、デベロッパが IAP を利用せずとも、そして手数料を Apple に支払わなくとも、デジタル・コンテンツを iOS 消費者に販売することを可能とするために、Apple が時間と共に発展させてきたものです。
- リーダールールは、デジタル音楽、電子書籍、ビデオ、オーディオ、新聞、雑誌 (漫画を含みます) を販売しているデベロッパに対して、IAP の利用をオプションとするものです。Apple は、サブスクリプションおよび購入を管理するために、最近、リーダー App からリンクアウトすることを可能とする変更を実施しました。
  - マルチプラットフォームルールは、IAP を実装するデベロッパに対して更なる柔軟性を提供するものであり、デベロッパが App の外 (ウェブサイト、Microsoft Xbox のようなゲーミング・プラットフォーム、その他の流通経路) でデジタル商品やコンテンツを販売し、ユーザーに iOS App 内で当該コンテンツにアクセスできるようにするためのものです。デベロッパは、他のプラットフォーム上で行われるそれらの取引に対しては、それらが iOS 内で消費されるとしても、Apple に何の手数料も支払いません。
27. このような変更により、すべてのデベロッパが支払いの選択肢を持つようになりました。App Store 上のデベロッパの 85% を含むほとんどのデベロッパは、IAP を全く利用しないことを選択しています。そしてマルチプラットフォームルールやリーダールールのようなルールの存在は、自身の App 内に IAP を導入しているデベロッパにとっては、それがユーザーに対してデジタル・コンテンツと商品を販売するための 1 つの選択肢に過ぎないことを意味しています。
- (iii) Apple のアンチステアリングルールは合理的かつ相応のものであること

---

<sup>15</sup> <https://developer.apple.com/programs/whats-included/>.

28. また、DMCH 中間報告は、Apple のアンチステアリングルールに対しても問題視し、「情報提供の制限は、手数料を確実に徴収することを目的とし、そのためのツールである自社 IAP を利用させるための手段であると言える」という理由で、同じ懸念が適用されるとしています<sup>16</sup>。IAP の利用義務自体に関する懸念と同様、この懸念には根拠がありません。
29. Apple は、デベロッパが一般的なマーケティング活動に従事すること、あるいは iOS App の外で個別のユーザーと支払い方法についてターゲット化した方法でコミュニケーションを行うことさえ、何ら制限を課していません。これは、デベロッパが、App 内のコールトゥアクションによって生成された電子メールを用いて、自身の IAP 以外のサブスクリプションを個別の iOS ユーザーに売り込むことができることを意味しており、このことから、Apple が、App のデベロッパが利用できるマーケティングの機会を拡大することにコミットしていることは明らかです。
30. アンチステアリングルールは、競争を妨げたり、消費者の認識を妨げたりするものではなく、単に、App のデベロッパが、IAP を利用し、Apple に合法的な手数料を支払う義務を回避することを防ぐものです。
31. Apple は 2009 年に IAP と共に導入されたガイドラインの 3.1.1 と 3.1.3 における「反迂回」(“Anti-Circumvention”) ルールを限定的に適用しています。それは全世界的に導入され、適用されています。Apple は、デベロッパが App Store を通じて App やコンテンツを無料で配信することを許容しています。また、デベロッパは、App Store を通じて、消費者が App の外で購入したデジタル・コンテンツにアクセスできる App を、Apple に手数料を支払うことなく配信することができます。この手法は、デベロッパが App Store を利用し、App Store を通じて無料で App を配信しながら、顧客がその App 内で有料コンテンツを楽しむことができる可能性をデベロッパに提供するものです。
32. この「無料」のアプローチの当然の帰結として、デベロッパは、その App を通じて顧客に IAP を回避するよう意図的に促すことによって Apple の投資にただ乗り (フリーライド) するべきではない、ということになります。ガイドラインの 3.1.3 項には、長い間、デベロッパが App Store を経由して顧客を獲得しながら、Apple への手数料の支払いを回避するために当該顧客に他の場所でデジタル・コンテンツを購入するよう促すことを禁止する文言が含まれています。3.1.3 項は、デベロッパが、実際のユーザーや潜在的なユーザーに対して、(i) App Store を通じて App をダウンロードし、(ii) そのコンテンツを他の場所で購入し、(iii) 購入された有料コンテンツを App Store で取得した App に移転することを奨励しないようにすることを意図したものです。このようなスキームの唯一の目的は、IAP を回避することによって Apple の投資にただ乗りすることであり、それは不適切なことです。
33. ガイドラインにおいて、iOS のユーザーに対して、App Store の外でコンテンツやサービスを購入するよう誘導するコミュニケーションを禁止することは、実店舗とオンライン店舗の両方を含む他のあらゆる小売業者の方針と事実上何ら異なりません。例えば、eBay や Yahoo!Japan は、手数料の支払いを回避する目的で、売主と買主が自社のプラットフォームの外で商品を購入するためにやり取りすることを禁止しています。Amazon は、自社のマーケットプレイスで商品を販売している売主が販促メッセージや広告を含む「Call to Action」(行動喚起)を行い、顧客が他のウェブサイトの商品を購入するように仕向けることを禁止しています。同様に、Apple は、自社の店舗の中でその顧客に対して他の場所で製品を購入することを促すコミュニケーションを許している実店舗の小売業者を知りません。

(iv) Apple のデベロッパとのコミュニケーションは、適時、公正、かつ非差別的であること

---

<sup>16</sup> DMCH 中間報告、150 頁。

34. DMCH 中間報告は、「デベロッパ側がアップデートに際して必要な対応を行う上で、情報開示の内容、周知の期間や方法、頻度、問い合わせ対応が十分ないし適切なものとはなっていない」という「懸念」を指摘しています<sup>17</sup>。
35. Apple は、Apple の情報が「常に変更される」、またはデベロッパに困難をもたらす、という考えに強く反論します。iOS 端末とそれらの端末で利用可能なサービスの、安全で、機密で、高性能な運用を確実にするために、Apple は自社のルールが技術の進化および消費者の期待に沿ったものであり続けるように見直し、発展させる必要があります。Apple のガイドラインは、「この文書は今後変更される可能性があります。新しい App の開発により新しい疑問が生じることもあり、その場合は随時新しいルールが追加される可能性があります。」と明確に述べています<sup>18</sup>。
36. Apple は、ガイドラインの改正や重要な変更を行う場合、デベロッパに十分な予告を与え、変更が発効する前に対処するための合理的な期間を提供しています。例えば、Apple が、WWDC 2020 において、サードパーティ App がどのようにユーザーのデータを追跡し利用するかについてユーザーがよりコントロールできるようにするために設計された「App のトラッキングの透明性」機能 (ATT) を発表した際には、Apple は ATT の導入を直ちに進めることはしませんでした。その代わりに、デベロッパに対して、当該機能を評価し、フィードバックを提供するための時間をより長く与え、リリース予定日を 6 ヶ月遅らせました。これは、DMCH 中間報告で指摘されているような「懸念」とはほど遠く、変更の実施前に潜在的な問題に対処するために Apple がデベロッパと効果的に取り組んでいることを示しています。
37. より一般的には、Apple は App 審査手続きの外でデベロッパと頻繁にやり取りを行い、そこで App Store の機能に関する質問に回答しています。デベロッパは、App Store チームとデベロッパ・リレーションズに、それらの通常の連絡手段を通してコンタクトすることができます。また、デベロッパは、App Store 上の自身の App を管理するための専用インターフェース (App Store Connect) や、専用のデベロッパ・フォーラムを通じて、Apple と対話することもできます。
38. iOS の大きな変更は 6 月の世界開発者会議 (WWDC) で発表され、デベロッパには 9 月まで、時にはそれより長い期間、自社の App を変更するための時間があります。Apple は WWDC で変更が発表されたのと同じ日に OS のベータ版をデベロッパに提供し、すべてのデベロッパがソフトウェアのベータプログラムに参加することができます。このことは、デベロッパが、新しい OS について学び、一般リリースに向けて自社の App を準備するために、数カ月間の猶予があることを意味します。WWDC では、1 対 1 のラボ、Developer Forums での Apple エンジニアとのディスカッション、個別のテキストでのチャットなど、デベロッパが Apple と関わり、質問に対する答えを得るための機会が複数用意されています。また、Apple は、過去にも今年も、Extended Tokyo や MOSA WWDC ミーティングなど、東京に本拠地を置くデベロッパ向けに特定のイベントを開催しています。
39. さらに一般的には、Apple は、次のような様々な公表されたリソースを通じて、次期 OS やブラウザのアップデートに関する追加の通知、資料および情報をデベロッパに提供しています。(i) リリースノート - <https://developer.apple.com/documentation/ios-ipados-release-notes/>、(ii) デベロッパフォーラム - <http://developer.apple.com/forums/>、(iii) WebKit ブログ - <https://webkit.org/blog/>。Apple は、特に日本のデベロッパのために、多くの公表されたリソースを維持しています<sup>19</sup>。デベロッパとの直接的な関わりは、日本のローカルチームが担当し、

<sup>17</sup> DMCH 中間報告、70 頁。

<sup>18</sup> <https://developer.apple.com/app-store/review/guidelines/> (「はじめに」)。

<sup>19</sup> ニュースとアップデート - [developer.apple.com/jp/news/](https://developer.apple.com/jp/news/) (デベロッパに対するアップデートはここで日本語によって提供されています); 日本語字幕付きデベロッパ動画 - <https://developer.apple.com/videos/> (2018 年以降リリースされたデベロッパ・カンファレンス動画のほと

1対1の会話、バグレポート、ソフトウェアのトラブルシューティングなど、現地のデベロッパ向けの活動を行っています。また、現地のデベロッパ・リレーションズのチームは、日本のデベロッパで会議に参加できなかった方やフォローアップの質問がある方向けに、WWDC Recap セッションを実施しています。

40. 2021年に、Appleは、デベロッパがAppleのスペシャリストから追加情報を得るためのTech Talksプログラムを導入しました。デベロッパは、「セッション」や、1対1の会議のための「オフィスアワー」に登録することができました。オフィスアワーは、日本在住のデベロッパにとって都合の良い時間帯に、日本語で利用できました。Tech Talksのプログラムの詳細については、<https://developer.apple.com/tech-talks/>をご覧ください。
41. Appleは、新しい機能を開発する際、日本のデベロッパと連絡を取り、そのフィードバックを慎重に検討しています。昨年、Appleは、KLab株式会社と協働してStoreKit 2プロジェクトに関するフィードバックを得て、ゲームデベロッパに有益な新機能を提供しました。Appleは、iOSで1,500万回以上ダウンロードされた接触確認App・COCOAのリリースに先立ち、日本政府と緊密に連携しました。昨年、株式会社カカオピッコマは、プロダクトページバリエーション機能のパイロットプログラムに参加しました。株式会社カカオピッコマは、Appleがすべてのデベロッパに向けてリリースする前に、この機能を改善するために有益なフィードバックを提供しました。
42. 政府との連携で成功した他の例には、デベロッパがNFCタグやカードを読み取ることができるCore NFC APIがあります。この機能により、日本政府はマイナンバーカードを読み取るAppを開発することができ、他の日本のデベロッパはEdyやSuicaなどの電子マネーの物理カードを読み取るAppを開発できるようになりました。また、Appleは、Suica Appの開発のためにJR東日本と緊密に連携しました。
43. また、Appleは、新しいハードウェアがリリースされる前に、デベロッパを招待して自社のAppをテストしていただき、デベロッパのフィードバックを得るとともに、Appをアップデートする必要があるかどうかデベロッパが理解するための支援をしています。このような招待は、使用可能なデバイスの数が限られているため、通常、より少数のデベロッパに限られます。しかし、Appleにとって、日本のデベロッパコミュニティから参加者を得ることは重要なことです。
- (v) Appleは、アップデートをリリースする際に、自社に不公平な優位性を与えていないこと
44. DMCH中間報告はまた、「サードパーティにおいては、アップデートや仕様変更に必要な対応期間が確保されない場合があり、また、アプリの品質向上に割く時間が十分に確保できなくなる一方、OS事業者の自社内でアプリやブラウザ、ウェブ・サービスの開発が行われ、即対応が可能となる」という懸念を提起しています<sup>20</sup>。Appleは、これに強く反論します。
45. AppleのAppは、WWDC期間中にリリースされるiOSの初期ベータ版と連携して更新されることはありません。Appleの各Appの開発チームは、サードパーティ・デベロッパと同様に、9月のiOSの一般リリースに向けて、AppleのAppの更新に取り組んでいます。明確化のために申し上げますと、Appleには「App開発部門」はありません。AppleのApp開発は、独立した個々のビジネスユニットが行っています。

---

んどには日本語の字幕が付されています); App Review ガイドライン - <https://developer.apple.com/jp/app-store/review/guidelines/> (最優先のローカル化プロジェクト); および 1. フィーチャー・ページ - [developer.apple.com/jp](https://developer.apple.com/jp) (2019年以降、ベータ・ソフトウェア・フィーチャー・ページのローカル版を提供しています)。

<sup>20</sup> DMCH 中間報告、76 頁。

46. Apple の App とサードパーティ App は、新しい iOS のアップデート版がリリースされるのと同様に、ユーザーに提供されます。サードパーティ App には、Apple の App と同様に、新しい iOS のアップデート版のリリースの前に、App を更新するための時間が与えられます。上記のとおり、それらの App のデベロッパに対してソフトウェアアップデートのベータ版へのアクセスを与えることによって、ソフトウェアのアップデート版がリリースされる前に App のアップデートを行うことを可能とします。このように、Apple 自身の App には何の有利な点もありません。このことは、人気が高い多くの App は、人気においても利用率においても、Apple 自身の App を凌ぐと結論づけた最近の独立の調査<sup>21</sup>によっても裏付けられています。
47. Apple はまた、iOS 内の新しい機能および技術（「機能」）をそれらがリリースされる前にテストするために、デベロッパと共に頻繁に作業します。当該機能をテストするために、Apple は、エンタイトルメントを通じて、限られたデベロッパのグループに対してハードウェアあるいはソフトウェアへの早い段階でのアクセスを提供します。これは、それらが意図されたとおりに作動し、デベロッパと顧客にとって安全であることを確実にするために必要とされます。このプロセスを通して、デベロッパは Apple にパフォーマンスに関するフィードバックを提供し、それが当該機能の分析および改善のために使われます。テスト期間の終了後に、多くのエンタイトルメントが、適格性を有するデベロッパに対して申請手続きを通じてパブリック・エンタイトルメントの形で開放されるか、あるいは、すべてのデベロッパに対してパブリック API の形で開放されます。

---

<sup>21</sup> 「The Success of Third-Party Apps on the App Store」と題する調査が Analysis Group によって実施されました。以下をご参照下さい。 <https://www.apple.com/newsroom/pdfs/the-success-of-third-party-apps-on-the-app-store.pdf>。

### C. iOS 端末のセキュリティとパフォーマンスを確保する手段の重要性

48. DMCH 中間報告は、iOS 端末のセキュリティとパフォーマンスを確保することを目的とした Apple の多くの方針および実務に関して懸念を示しており、それらには、サイドローディング、WebKit の要件、およびサードパーティ App とブラウザによる機能へのアクセスに対する Apple のアプローチが含まれています。DMCH 中間報告は、このような実務は、モバイル・エコシステムの様々な層に渡り、Apple 製品を優遇する意図または効果を有しており、他のプロバイダとの競争を制限する効果を有している、という見方をしています<sup>22</sup>。Apple が以下で示すように、内閣官房デジタル市場競争本部の評価には根本的な誤りがあり、Apple のアプローチの根底にある正当性と、異なるアプローチが採用された場合に生じる結果を、適切に考慮していません。

#### (i) Apple のセキュリティに向けたアプローチは極めて効果的であること

49. マルウェア、ウイルス、セキュリティおよび互換性が継続的な課題であったパーソナル・コンピュータで被った経験を防ぐために、Apple は、iPhone が可能な限り安全であることを確保することに常に精力を傾けています。その根本的な理由は、Apple が 2007 年 10 月に、サードパーティ App を iPhone 上で流通させることを可能とするためにソフトウェア・デベロッパ・キット (SDK)<sup>23</sup> を作成してライセンスする予定であることを発表した際に、明確に示されました。

「我々は、デベロッパに高度で開放されたプラットフォームを提供すると同時に、iPhone ユーザーをウイルス、マルウェア、プライバシー攻撃等から保護するという、二つの完全に相対することを実行しようとしているため、SDK をリリースするには 2 月までかかるでしょう。これは容易なタスクではありません。一部では、ウイルスとマルウェアは携帯電話にとって問題ではないと主張されていますが、これまったく誤っています。すでに他の携帯電話上には深刻なウイルスが存在しており、その中には、セル・ネットワークを介して電話から電話へと静かに拡散されているものもあります。我々の電話の能力が高まるほど、これらの悪意のあるプログラムはいっそう危険になるでしょう。そして iPhone は今までで最も先進的な電話であるため、とても目立つ標的となるでしょう。…我々は、数カ月の辛抱強さが、その後長年に亘り優れたサードパーティ・アプリケーションが安全で信頼性の高い iPhone 上で稼働するということによって報われるであろうと考えます。」

50. カスタムメイドのセキュリティ・ハードウェアは、決定的に重要な iPhone のセキュリティ機能を作動させます。ソフトウェア・プロテクションは、オペレーティング・システムとサードパーティ App を安全に保つために機能します。サービスは、安全で適時のソフトウェア更新の仕組みを提供し、より安全な App エコシステムを推進し、安全な通信と支払いを届け、そしてインターネット上のより安全な体験を提供します。iOS 内に構築された技術的なプロテクションに加え、更に決定的に重要な保護層が App 審査の仕組みであり、すべての App および App 更新の包括的な審査が、それらがダウンロード用に提供される前に実施されます。

<sup>22</sup> 例えば、DMCH 中間報告 268 頁の「仮に、一律に禁止されていないファーストパーティによる MiniApp へのアクセスに対する許諾の判断が不透明、不公平であるとすれば、それによって、アプリ事業者間の公平な競争が阻害されるおそれがあるほか、Apple 自身の場合は、MiniApp を利用せず(※)とも、MiniApp を使う場合と同等の価値提供が可能な場合であって、他の事業者に対して MiniApp へのアクセスを正当な理由なく拒んで、ビジネス展開を阻害しているとすれば、Apple による不当な自社優遇の観点からの懸念もあり得る」という記載を参照ください。

<sup>23</sup> 2007 年 10 月 17 日付のスティーブ・ジョブズからのオープン・レターを参照ください。

(<https://bits.blogs.nytimes.com/2007/10/17/programmers-welcome-for-the-iphonenext-year/>;  
<https://web.archive.org/web/20071018221832/http://www.apple.com/hotnews/>)

51. この重層的なアプローチは効果的であり、iOS を世界で最も安全な消費者コンピューティング・プラットフォームにしています。サードパーティ・セキュリティ・プロバイダのデータによれば、稼働している消費者用および商業用プラットフォームの中で、iOS は最も安全なものに位置付けられています。例えば、2020 年の Nokia Threat Intelligence Report によると、iPhone は、プラットフォームによるマルウェア感染のおよそ 1% ですが、Android はすべての感染の 4 分の 1 以上を占めています。同報告書は、iOS 端末のマルウェア感染数が Android 端末のそれと比べて 15 から 47 倍少ないことを確認しています。別の調査では、モバイルマルウェアの 98 パーセントが、iOS 端末ではなく Android 端末を標的としていることが分かりました。iOS のより優れた安全性は、iOS を購入することを判断する際の主要因の一つであり、iOS を Android と同様のプラットフォームに転換させようとする、安全性に関する iOS のシステム・レベルの競争優位性を低下させる恐れがあり、実証されているユーザーの選好に相反することとなります。

(ii) 代替的なアプリケーションのストアとサイドローディングを認めることは、重大な被害を引き起こし得ること

52. Apple は一度も iPhone へのサイドローディングを許可したことがありません。Apple の iOS エンドユーザーソフトウェア・ライセンス契約は、「お客様は、お客様の本デバイスおよび暗証番号の安全性の保持に対して、全責任を負うものとします。お客様は、お客様がお客様の本デバイスの紛失またはアクセス共有をされた場合、Apple は一切責任を負わないことに同意するものとします。お客様は、お客様が Apple ソフトウェアに無許可の変更を加えた場合（例えば、「脱獄/ジェイルブレイク」のような方法により）、Apple は一切の責任を負わないことに同意するものとします。」と記しています<sup>24</sup>。さらに、Apple のウェブサイトは、消費者に対して次のことを明確に強調しています。「Apple では、iOS にハッキングソフトウェアをインストールしないよう強く警告しています。iOS の不正改造は iOS のソフトウェア使用許諾契約に違反しています。このため、不正なソフトウェアがインストールされている iPhone/iPad/iPod touch に対しては修理サービスを拒否する場合があります。」<sup>25</sup>

53. Apple はまた、今までに、Apple の専有技術にアクセスする App、または、デベロッパ・プログラムを通してデベロッパに提供されるツール、ソフトウェア、リソースを利用する App をサードパーティが流通させることを許可したことはありません。iPhone はクローズドなエコシステムとして設計されており、その OS である iOS は、サードパーティ App またはソフトウェアが端末にダウンロードされるのを阻止するように設定されています。

54. サイドローディングを阻止するという判断は、App Store のローンチ以前に、iPhone を安全かつセキュアで信頼でき、使い易いものとするという Apple の目標に基づきなされました。上述のとおり、Apple の際立った見た目や雰囲気（“look and feel”）は、消費者にとってその端末を可能な限り魅力的なものとするという戦略の中核をなします。（もし App Store と App が端末にサイドローディングされてしまうと、その効果が完全に損なわれてしまうであろう）厳しい App 審査プロセスを作り出している、App デベロッパのための設計ガイドラインを提示することによって、Apple は Apple 端末上のユーザー体験が何ものにも劣らないことを確実にすることが可能となります。

55. 仮に、Apple が、代替的なアプリケーションのストアまたはサイドローディングを許容することを強いられたなら、それによって増大したマルウェアの攻撃を受けるリスクは、すべてのユーザーをより大きなリスクに曝すこととなります。App Store は、今日の攻撃を検出しブロックするよう設計されていますが、脅威モデルを変更すると、より洗練された攻撃からのこれらの保護が無視されてしまうことになり得ます。そして詐欺師が新たに開発した自身のツールと専門知識を、サードパーティ・ストアと App Store を標的とすることに使い、それは App

<sup>24</sup> [https://www.apple.com/legal/sla/docs/iOS14\\_iPadOS14.pdf](https://www.apple.com/legal/sla/docs/iOS14_iPadOS14.pdf) を参照ください。

<sup>25</sup> <https://support.apple.com/en-us/HT201954> を参照ください。

Store のみから App をダウンロードしているユーザーを含むすべてのユーザーを、より大きいリスクに曝すこととなります。さらに、マルウェアは、エントリーポイント App にのみ影響を与えるわけではありません。例えば、電池の過度な使用あるいは侵害的なデータ収集のような影響は既にダウンロードされている App を妨害するため、他の App の機能に重大な悪影響を及ぼす可能性があります。潜在的にさらに一層深刻な問題として、端末に導入されたマルウェアは、当該端末が接続している他の端末やシステムへのアクセスを得るための手段として使用される可能性があります。個々の携帯端末は、企業環境におけるネットワーク全体に対する攻撃を配置するための共通のエントリーポイントとして認識されています<sup>26</sup>。さらに、ユーザーの端末から個人情報へのアクセスを得た攻撃者は、ユーザーの友人や家族に対する攻撃を開始するために好都合な立ち位置にいることとなります。

56. また、詐欺的 App によるリスクの増加は、ユーザーのみならずデベロッパまでもより大きい危険に曝すこととなります。日本の情報処理推進機構 (IPA)<sup>27</sup>によると、IPA が消費者から受けた相談事案の中では、iOS 上におけるマルウェア感染が非常にまれであるだけでなく、違法または詐欺的 App に関する事案も比較的少数に留まっています。もし Apple が代替的なアプリケーションのストアまたはサイドローディングを許容することを強いられたなら、入手可能な著作権侵害 App や違法または詐欺的 App の数が劇的に増加する可能性が極めて高いといえます。子供たちに有害となる可能性があるコンテンツまたは機能を含む App の数も増加し得ます。実際に、Apple が提供する親によるコントロール手法である ScreenTime はサイドローディングされた App に対しては機能せず、親と子供の支援のために進めている試みを損なうこととなり得ます。

57. さらに、万一、Apple がサイドローディングを許容することとなると、iPhone の抜本的な再設計が必要となります。Apple はこのようなかたちで自社製品を再設計することを検討評価したことは今までに一度もないため、何らかの正確性をもって申し述べる立場にありませんが、相当なエンジニアリング作業と時間が要求され、そして莫大なコストがかかることになるといえることは言えます。iPhone にサイドローディングを導入することは、Apple に iPhone を完全に別の製品に変えることを要求することとなるため、軽く受けとめることのできない問題です。

(iii) WebKit 要件は、iOS 端末のセキュリティとパフォーマンスにとって中核となる要件であること

58. すべてのブラウザは WebKit エンジン上で稼働する必要があるという Apple の要件は、Safari 以外のブラウザとの競争を制限する手段であるという DMCH 中間報告の憶測に反して、Apple の全体的なセキュリティ保護と iOS 端末のパフォーマンスにとって中核的な要素を成すものです。

59. Apple は、端末上で App が実行するコードが、確実に既知の調査されたソースから提供されるように iPhone を設計しました。Developer Program と App Store によって、Apple は、App が Apple のガイドラインに従うこと、および App を App 審査の対象とすることに同意した既知のデベロッパから提供されることを確保しています。iOS 上のユーザー体験にとってウェブは極めて重要ではあるものの、ウェブはまた、端末を未知で未調査のソースに曝すことにもなります。これは、次のような内在的な葛藤を生じさせるものです。すなわち、ユーザーはウェブを閲覧することができる必要がある一方で、ウェブはまた、未知で悪意のある行為者が iOS 端末に対する攻撃を仕掛けるための危険な媒体でもある、ということです。iOS 端末の保護の

<sup>26</sup> <https://www.perle.com/articles/why-byod-culture-poses-a-major-risk-to-enterprises-40188803.shtml> を参照下さい。

<sup>27</sup> Apple は、この事実を 2022 年 5 月 31 日に IPA に確認しました。

ために、多くの重要なセキュリティ上の機能と便益をもたらすよう、Apple は以下のとおり WebKit を iOS に緊密に統合しました。

- iOS 上の WebKit は、10 年間分のセキュリティ向上を体現し、他の iOS プロセスおよび macOS 上の Webkit とさえ本質的に異なる、カスタマイズされたサンドボックス・プロファイルをサポートします。iOS 上の WebKit のサンドボックス・プロファイルは、ネイティブの iOS App のためのサンドボックスよりも桁違いに一層厳しいものです。これが、悪意を有する行為者が iOS プロセスを攻撃できる攻撃対象領域を劇的に制限することになります。WebKit と iOS のセキュリティ・エンジニア間の緊密な共同作業によって、WebKit サンドボックスは定期的に更新され、そして、進化し新たに出現する脅威に応じてそれを強化するために、新規のサンドボックス技術が開発されます。
- 今日、およそ百万の App が iOS 上でウェブ・コンテンツを提供しており、それらのすべては共通の WebKit インストールを使用しています。これによって Apple は、これらのすべての App に対する重要なセキュリティの更新を単一の更新によって配信することができます。他のプラットフォームは、ブラウザ・エンジンのセキュリティに対して断片的な手法を実施しており、各 App が異なるブラウザ・エンジン（実質的には、当該ブラウザ・エンジンの異なるバージョン）を組み込むことを許しています。例えば、Android 上では、Chrome、Edge、およびサムソンのブラウザはそれぞれ、異なるバージョンの Blink ブラウザ・エンジンを組み込んでおり、それらは、Google が Android に対してセキュリティ更新を送り出した際に、必ずしも整合性をもって更新されるわけではありません。結果、Android は、Blink が組み込まれた App が何時重大な脆弱性を修正するかについて管理できず、それはつまり、更新が整合性をもって大規模に適用されることが決してないということです。結果として、修正がブラウザ・エンジン・ベンダーによってリリースされた後でも、App が旧式バージョンの組み込みブラウザ・エンジンを何カ月も、またはそれ以上の間、使い続けることが許されてしまう可能性があります。
- WebKit は、ジャスト・イン・タイム・コンパイラ、あるいは「JIT」にアクセスすることができる唯一の iOS プロセスです。JIT は、ウェブ内を閲覧している App が迅速且つ効率的に JavaScript コンテンツを提供することを可能とするものであり、それはユーザーにとって価値のあることですが、同時に、悪意を有する行為者が利用できる脆弱性を露出することにもなります。JIT によってもたらされた危険を軽減するために、WebKit は iOS ハードウェアとの緊密な統合を強化します。攻撃者が JIT へのアクセスを得ることを阻止するために極めて効果的なハードウェア・セキュリティ・エクステンション（APRR）を Apple は採用しています。Apple はまた、攻撃者が JIT の外でのコード実行を獲得することを阻止するために、Pointer Authentication Code（PAC）を導入しています。PAC は、メモリ破損バグの悪用から保護するために、暗号署名と認証を関数ポインターと戻りアドレスに提供します。

60. WebKit は iOS 端末での使用のために慎重に設計され最適化されています。これによって、iOS 端末が、ウェブに基づくブラウジング・ベンチマークにおいて競争相手を凌ぐ<sup>28</sup>と同時に、業界の先頭を行く電力効率と電池性能を達成することが可能となっています<sup>29</sup>。もしサードパーティ・ブラウザ・エンジンを許容することが義務化されると、Apple はすべての iOS 端末上での高いパフォーマンスと安全なブラウジング体験を保証することができなくなります。

---

<sup>28</sup> <https://www.pcmag.com/news/iphone-13-benchmarks-apples-a15-chip-crushes-qualcomm> (「ウェブ・ブラウジング・ベンチマークである Basemark Web において、iPhone 13 Pro 上の Safari は、Galaxy S21 Ultra 上の Chrome のほぼ 2 倍のスコアを上げた (On Basemark Web, a web browsing benchmark, Safari on the iPhone 13 Pro gets nearly double the score Chrome on the Galaxy S21 Ultra does)」); <https://www.anandtech.com/show/16192/the-iphone-12-review/3>

<sup>29</sup> <https://www.anandtech.com/show/17004/apples-iphone-13-series-screen-power-battery-life-report-long-lasting-devices>; <https://www.anandtech.com/show/16983/the-apple-a15-soc-performance-review-faster-more-efficient/2>

(iv) Apple の Safari に対するアプローチは、iOS 端末上で利用可能な競合するブラウザを制限することを目的とするものではないこと

61. DMCH 中間報告は、iOS 端末への Safari のプリインストールが、Apple の Safari ブラウザを優遇すること、あるいは App Store との関係における Apple の立場を「保護」することを目的としていると懸念しています。これらの懸念は、Apple が有しているインセンティブと Apple の実際の行為の両方を無視したものです。
62. Apple のインセンティブはその全体的なビジネスモデルによって推進されており、それは未だ変わらず、モバイル端末を販売するというものです。すなわち、端末がより魅力的であるほど、Apple の売上高は大きくなります。ユーザーが望むより多くの特徴と機能性を備えていることが、Apple 端末の魅力を確認するために重要です。プリインストールとデフォルト設定に伴う利便性は、モバイル端末のユーザーが高く評価する真の利益をもたらすものであり、テクノロジーに精通しておらず、自身のモバイル端末のポテンシャルを最大限発揮させるための App を見つけてインストールすることに苦勞するようなユーザーにとって最も役に立つものです。これは、可能な限り最良の総合的な iPhone 体験をユーザーに提供するという Apple の目的を反映したものです。
63. 2007 年のリリース以来、iPhone の特徴は、その使い易さにあります。ユーザーは、iPhone を開いて、容易に理解できる少数の手順を経てそれを設定すれば、動作する端末を直ちに手にすることができるのであり、多数の設定画面や選択を経る必要はありません。この端末取得直後の体験を可能にするために、iPhone は電話 App、ブラウザ、カメラ等、多くのプリインストールされた App を包含しています。例えば、Apple は、ユーザーがブラウザ App を開いて URL ボックス内に当該ウェブ・リンクを入力または貼り付けなくとも、Apple Maps あるいは Messages 内で選択されたウェブページが、プリインストールされていれば直ちに立ち上がることとなるウェブ・ブラウザを構築するために、相当なリソースを投資しました<sup>30</sup>。
64. ユーザーにシームレスな端末取得直後の体験を提供するために、Safari は iOS 端末にプリインストールされていますが、Apple は、ユーザーが、代替的なブラウザ App をダウンロードして使用することを制限していません。iOS 端末上でユーザーは、Firefox、Firefox Focus、DuckDuckGo、Google Chrome、Microsoft Edge、Brave、Aloha、Cake、Opera Touch、DuckDuckGo Privacy Browser、そして Dolphin を含む、App Store で取得可能な他の様々なモバイル・ブラウザの中から選択することができます。さらに、Bing Search、Yahoo Search、Ecosia、Quant、Start Page、そして Google Search はすべて、ユーザーによるウェブ閲覧を可能とする検索機能を備えた App です。
65. 第三に、Apple は、他のブラウザが Safari と差別化することを可能としており、ユーザーに対して真の選択肢を提供しています。WebKit は、異なるブラウザ間の実質的な差別化を可能とし、デベロッパが、Apple による厳しいプライバシーおよびセキュリティ保護を守りつつ、WebKit の上に機能やインターフェースを構築することを可能とします。他のデベロッパは、サードパーティ・ブラウザを管理しており（例えば、Google は Chrome を管理し、Mozilla は Firefox を管理しています。）、iOS エコシステムの制約内において Safari にはない機能を自身のブラウザ内に自由に構築することができます。
66. 実際に、サードパーティ・ブラウザは、Safari との差別化を実現するために、WebKit ブラウザ・エンジンの上にウェブ・プラットフォーム機能を導入しました。WebKit はオープン・ソース・プロジェクトであり、それは、いかなる貢献者でもコードを提供することができることを意味します。また、デベロッパは WebKit の上で機能を有効化することができます。例えば、サードパーティ・ブラウザである Brave は、自身が WebKit の上に構築した Web Authentication サポートを、それが WebKit によって広く提供される前に送り出しました。Web Authentication は、

<sup>30</sup> もちろん、ユーザーが望む場合は、「設定」においてデフォルト・ブラウザを Safari から別のブラウザに変更することができます。

特定のウェブサイト上でしっかりとユーザーを認証する目的のため、ウェブ・アプリケーションによる優れた暗号の身分証明の作成および使用を可能とします。同様に、Brave は 2020 年に Global Privacy Control (GPC) を導入しましたが、その iOS ブラウザ内には、WebKit 内では未だ提供されていない機能が含まれています。GPC は、オンラインでプライバシーの要請を行い、または処理するために、ウェブ・ブラウザとウェブサイトが使用することができるウェブ標準です。(ウェブページの特定の部分へのリンクを可能とする) Google の Scroll to Text Fragment 機能は、現時点では Safari、WebKit のいずれによってもサポートされていませんが、Google の Chrome iOS App は当該機能をサポートしています。

(v) ウェブ App について、Apple は競争を促進していること

67. Apple は iPhone の最も初期の頃からウェブ App をサポートしています。Apple は 2007 年に iPhone をローンチした時にウェブ App の概念を受け入れました。Apple は、ウェブ App が、iPhone に大きな機会を提供すると考えました。Apple は、自社専有の技術プラットフォームをネイティブ App に開放することを決めた時に、ウェブ App へのサポートを続けました。Apple は近年、ウェブ App のためにより多くの特徴や機能を使用できるようにするために、WebKit に新しい機能を加えました。それらは例えば次のようなものです。

- iOS 11 の導入と共に Apple は、プログレッシブウェブ App の開発にとって重要な要素となった Service Workers 向けのサポートを導入しました。それはブラウザがバックグラウンドで走らせることができるスクリプトであり、開いている App の特定のページに依存しないため、当該ウェブ App はユーザーの活動と無関係に、そして、最も重要なことに、ネットワーク接続と無関係に稼働します。Service Workers はアプリケーションからのネットワーク要求を阻み、コンテンツのダウンロードとキャッシングを制御し、バックグラウンド同期を行い、そして標準的なウェブページではできない他の様々なタスクを行うことができます。
- Apple は Web Authentication API をリリースしましたが、これによってウェブ App が、確実なユーザー認証のために、Touch ID や Face ID にアクセスすること、および、外部のセキュリティキーを使用することが可能となりました。
- WebRTC は、ビデオ・コミュニケーションを含むピア・ツー・ピア・コミュニケーションを可能とし、これによって、ウェブに基づくビデオ会議やストリーミング・ゲーム・サービスのウェブ App が中央サーバーに依存する必要がなくなり、ピア・ツー・ピア・コネクションに頼ることができるようになりました。

68. WebKit はイノベーションが行われ、ウェブ App を改善する特徴や機能に対する需要に応え続けています。例えば、WebKit は、現在、次の機能を開発しています。

- 小さい、大きい、動的な、そして論理的な、新しいビューポート・ユニットに対するサポート。WebKit は、ウェブ App の、自身の App が表示され得る外形寸法を正確に測定する能力を向上させるために、この機能を開拓しています。
- HTML ダイアログ要素に対するサポート。このツールは、コンテンツと情報のユーザーに対する表示の質を高めるために、ウェブ App ・デベロッパがプロンプト等のオーバーレイを作成することを支援します。この機能をリリースする前に WebKit は、それが一般的なアクセシビリティ基準に対応することを確保するための作業を行いました。
- Web App Manifest アイコンおよびマニフェスト・ファイル・フェッチング改良に対するサポート。これらの機能は、ウェブ App ・インターフェースのテーマとアイコンの能力をサポートします。
- Apple は、近年、iOS 16 の更新に伴い、ウェブ App のためにプッシュ通知をサポートすることを発表しました。プッシュ通知は、ウェブ App がそのユーザーに対して、急を要す

る、あるいは高優先順位のイベントを、ユーザーが現在当該サイトを開いていなくとも通知できるようにします<sup>31</sup>。

(vi) 機能に対する制限は、セキュリティを保護しパフォーマンスを確保する必要性によって正当化されること

69. 上述のとおり、Apple は競合するブラウザとウェブ App の開発をサポートしてきました。しかしながら、このことは、新しい機能を導入する際にユーザー・プライバシーとデータ・セキュリティを犠牲にしないという保証と両立する必要があります。
70. ウェブ App が使用できない機能について、Apple デベロッパ・プログラムは、ネイティブ App 作成のために、広範囲に渡る Framework、API、および、その他の技術へのアクセスをデベロッパに付与しています。これらの技術のリストは次のサイトで取得できます。<https://developer.apple.com/documentation/technologies>。これらの技術にアクセスするためには、ネイティブ App のデベロッパはデベロッパ・プログラムに登録し、デベロッパ料を支払い、そして DPLA の要件を遵守しなくてはなりません。ウェブ App のデベロッパは、自身のウェブ App を作成し、試し、流通させるために、デベロッパ・プログラムのツールおよび技術へアクセスすることに対する対価を支払わず、また、同デベロッパは適正使用に関する DPLA の要件によって拘束されないため、同デベロッパにこれらの技術へのアクセスを付与することは不適當であり、さらに、潜在的に危険です。
71. 他のブラウザに与えられる API へのアクセスについて、Apple は、最新のソフトウェアの機能および特徴へのアクセスをデベロッパに提供し、それらが素晴らしい App を作成できるようにし、Apple の App エコシステムの質と堅牢さを高める、あらゆるインセンティブを有しています。Apple が新しい特徴、新しい機能、そして新しい製品を導入すると同時に、それらの技術をサードパーティ・デベロッパが利用できるように Apple は懸命に努力します。実際に、Apple は毎年 iOS 内および iPadOS 内の多数の新しい Application Program Interfaces (API)、技術、そして機能をリリースしており、それらは、iOS と iPadOS が提供する内蔵された機能をデベロッパが活用し、デベロッパ自身の素晴らしい App を設計し作成することを可能とします。Apple は 2008 年に初めて iOS をサードパーティの開発に開放した時に、10,000 の API をデベロッパが利用できるようにしました。今日では、デベロッパは、250,000 以上の API を利用可能であり、その数は増加し続けています。
72. 同時に、Apple は、ソフトウェア技術および API へのアクセスを提供する際には、セキュリティ、安全性、品質、端末パフォーマンス、およびユーザー体験の一貫性が損なわれず、そして、コードと API がデベロッパの App および専有技術とうまく機能するように、注意しなければなりません。API を開発し、改善し、テストし、そして最終的に使用のためにサードパーティ・デベロッパに提示するためには時間がかかります。API が一度リリースされると、サードパーティ・デベロッパは、自身の App を作動するために当該 API の基礎を成す機能が常に利用可能であることに依存するようになるため、API はリリースされる前に安定しており、十分に試験され、長期性が担保されていなければなりません。したがって、Apple が、自社の統合された App に与えるアクセスと同レベルのアクセスを同じタイムフレームでサードパーティに与える義務を課さなければならないとはいえません。そして、Apple のユーザーのセキュリティ、安全性、またはプライバシーを損ない得る場合に、サードパーティによる利用を可能にしていない技術は存在しています。
73. 問題は、背景事情を考慮せずに、理論上より制限的でないアプローチが存在するかどうかではなく、Apple がサードパーティ・アクセスに対して課している制約が、客観的であるか否か、そしてそれらが実際に競争を制限しているか否かです。内閣官房デジタル市場競争本部の懸

<sup>31</sup> <https://webkit.org/blog/12945/meet-web-push/>

念の対象となっている API に関して、そのような結論を支持する証拠が存在しないことは明らかです。

- NFC に関して、サードパーティの非接触式支払い App による使用のために Apple が NFC カード・エミュレーション・モードをアンロックすると、Apple 端末ユーザーのデジタル世界での行動痕跡に対する新しい攻撃に当該ユーザーを曝すこととなり、Apple ユーザー・エコシステム内で、高価値の新しい攻撃対象領域を作り出すこととなります。技術系プロバイダと銀行によって開発された HCE ソリューションのような、代替となる可能性があるものは、保護がより弱いと広く認識されているセキュリティスタンスを取っており、それが提供する保護も一貫して展開されておらず、(当該デベロッパ自身のデータ保護とセキュリティ・プログラムが不十分である可能性がある) 各デベロッパの選択および能力に左右される App の中に含まれています。しかしながら、安全な Apple Pay 技術アーキテクチャを通して Apple 端末上の NFC 機能にアクセスする会社は世界中で [REDACTED] [REDACTED] 存在しており、そのうち日本には約 [REDACTED] [REDACTED] が存在しています。
- 超広帯域 (UWB) チップに関して、中間報告が認識しているように、Apple はすでにチップへのアクセスをサードパーティに提供し始めています。昨春にチップセット製造業者のために仕様をリリースし、昨秋に製品認証を始めました<sup>32</sup>。サードパーティは既に、iPhone 内の UWB を利用する製品を発表しています<sup>33</sup>。
- MiniApp は、ネイティブ App 内でアクセス可能とされている、実質的なウェブ App です。これは、App Review を通じた Apple による審査を経た後であっても、デベロッパは、当該 App をサーバーサイドで容易に (例えば、ネイティブ機能にアクセスできるようにするために) 修正できることを意味します。したがって、Apple による規制 (すなわち、自身の App 内で HTML5 に基づく MiniApp を提供するデベロッパは、App Store ガイドラインの 4.7 の規定の適用を受けること<sup>34</sup>) が必要です。仮に、デベロッパがその負担を過大であると考えるのであれば、当該デベロッパは、自身の MiniApp を、ウェブ App としてウェブ・ブラウザを通して App Store の外で提供することが可能です。
- Apple は、現在、iOS 上のサードパーティ・ブラウザのためのウェブ拡張機能をサポートしていません。我々のユーザーに高水準のセキュリティとプライバシーを提供するために、Safari ウェブ拡張機能を App Store を通じて流通させており、それらは徹底的な App Store 審査手続きを活用しています。しかしながら、Apple は将来サードパーティにこの能力を付加する可能性を否定しません。仮に、Apple が、現時点でサードパーティ・ブラウザのための拡張機能を提供するのであれば、必要となるテストの時間的・技術的な限界のために、Apple は同様のプロセスを提供することはできません。

74. サードパーティ App と Apple のサービスとの間に Apple の専有技術へのアクセスに関して差異が存在する場合、かかる差異は、Apple 端末の安全性とパフォーマンス、そしてユーザーのプライバシーとセキュリティを確保する必要性によって、客観的に正当化されます。

<sup>32</sup> <https://developer.apple.com/nearby-interaction/>

<sup>33</sup> <https://www.engadget.com/tile-pro-ultra-wideband-tracker-new-devices-100025451.html> を参照下さい。

<sup>34</sup> 本ガイドラインに基づき提供されるソフトウェアは次の条件に従わなければなりません。(i) 無料、または App 内課金を使用して購入されること、(ii) 標準的な WebKit ビュー内で使用可能な機能のみを使用すること (例えば、当該ソフトウェアは、変更または追加ソフトウェアなしで、Safari 内でネイティブとして開き作動しなければならない)、また、サードパーティ・ソフトウェアを作動させるために WebKit および JavaScript Core を使用し、ネイティブ・プラットフォーム API をサードパーティ・ソフトウェアに対して拡張または曝さないこと、(iii) Apple デベロッパ・プログラムに参加し、Apple デベロッパ・プログラム・ライセンス契約書に署名したデベロッパによって提供されること、(iv) 実価貨幣ゲーム、富くじ、または慈善寄付へのアクセスを提供しないこと、(v) App Store Review ガイドラインの条件 (例えば、不快なコンテンツを含有しないこと) を遵守すること、(vi) 販売の対象としてデジタル商品あるいはサービスを提供しないこと。

## D. Apple のプライバシー・イニシアチブ

75. DMCH 中間報告は、Apple のプライバシー・イニシアチブ、特にアプリのトラッキングの透明性（App Tracking Transparency (ATT)）とインテリジェントトラッキング防止機能（Intelligent Tracking Prevention (ITP)）に関して、懸念を示しています。DMCH 中間報告はまた、Apple のデータ取得方針が問題である可能性があり、Apple はサードパーティとより多くのデータを共有することを義務付けられる必要があり得ることを示唆しています。それらは、大量の個人データを編集して販売することに関心を持っているデータ・アグリゲータや企業による、自己の利益のみを追求しようとする申し立てによって推進されていることが考えられるため、内閣官房デジタル市場競争本部がそのようなアプローチを採っていることは残念です。

76. Apple のプライバシーに関するアプローチは長年に亘り一貫しており、「プライバシーは基本的人権である」という考えに基づいています<sup>35</sup>。このプライバシーに対する権利を保護するために、Apple のアプローチは、いずれも 4 つの主要原則を念頭に置いて構築されています。それらは次のものを含みます。

- データの最小化 — Apple または第三者がアクセスする個人情報を最小とするために、Apple は革新的な技術と技法を使用します。
- デバイス上の知能 — Apple は、ユーザーのデータを収集してサーバーに送信するのではなく、できる限りユーザーの端末上で処理します。
- 透明性とコントロール — Apple は、データがどのように利用されるのかをユーザー自身が選べるようになるために、収集されているデータについてユーザーがよりよく理解できるように支援します。
- セキュリティ — セキュリティ保護は上記すべての基礎を成すものです。

Apple はまた、ユーザーのデータがどのように利用されるかについてユーザーを啓蒙すること、そしてその利用をコントロールする権限をユーザーに与えるよう努めることにおいて、一貫して業界をリードしています。例えば、Apple は、最近、「あなたのデータの 1 日」と題する報告書を発行しましたが、そこでは、企業がトラッキングを通じてどのようにしてユーザーの大規模なデータプロフィールを構築して収集するかを説明しています<sup>36</sup>。Apple がユーザーに対するプライバシー・コミットメントの中で記しているとおりに、「あなたの端末は、あなたの生活のとても多くの部分にとって重要なものです。あなたが体験することのうち、何を共有するか、そして誰と共有するかは、あなたが決められるべきです。我々は、Apple 製品を、あなたのプライバシーを保護し、あなたの情報に対するコントロール手段をあなた自身に与えるように設計しています。」<sup>37</sup>

77. DMCH 中間報告において示された懸念について、Apple のアプローチの意味するところは次のとおりです。

(i) ATT の導入は自社優遇としないこと

78. 内閣官房デジタル市場競争本部は次のように述べています。「[ATT の実施に関するこれらの方策は] プライバシーへの配慮の側面はあるものの、広告ビジネスモデル間の競争環境という視点で見ると、広告をパーソナライズする能力を制限することで、他社の広告のビジネスモ

<sup>35</sup> <https://www.apple.com/jp/privacy/>

<sup>36</sup> 次のサイトで取得可能です。

<https://www.apple.com/privacy/docs/A Day in the Life of Your Data.pdf>

<https://www.apple.com/jp/privacy/docs/A Day in the Life of Your Data J.pdf>（日本語）

<sup>37</sup> 同上。

デルの展開に制約が加わり、結果的に、自社の広告のビジネスモデルが有利に展開されることにつながっていると評価される。」<sup>38</sup>しかし、この懸念には根拠がありません。

79. Apple は、一部の企業が膨大な量の個人情報を収集するために用いている迷路のように複雑な隠れた慣行について、消費者は知らず、また知ることを期待できないと理解しています。これらのデータ収集行為について消費者を教育する努力をするとともに、Apple は、消費者に権限を与え、個人情報の利用をコントロールする能力を消費者自身に提供するための具体的な手段を導入しました。ATT は、この目的で導入された最新の施策にすぎません。

- 個人の永続的識別子の不正な漏洩に対する消費者からの苦情を受けて、Apple は 2012 年にランダムな端末識別子である IDFA を導入しました。「設定」におけるオプトアウトの仕組みに従い、「広告トラッキングの制限」ボタンをクリックすることによって、消費者はデベロッパに対して、IDFA の使用を通して追跡されることを望まないことを示すことができます。IDFA の改良は 2013 年と 2016 年に行われました。
- 2017 年、Apple は ITP を導入しました。これは端末上の機械学習を利用して、広告主がユーザーに知られることなくウェブサイト全体に渡りユーザーを追跡するために使用する手法を確定し、サードパーティ広告主が許可なくユーザーの端末内に保存させようと試みる追跡クッキーを隔離し削除するものです。ウェブサイトが使用できる隠れた追跡手法の例は、「いいね！」ボタンや「共有」ボタンのようなソーシャル・ウィジェット、および、ユーザーがそれをクリックまたは使用せずともユーザーを追跡することができるコメント欄を含みます。Safari は、ITP を用いて、デフォルト設定によってこの追跡を阻止し、透明性とコントロール手段を提供し、ユーザーにソーシャル・ウィジェットがユーザーの個人情報にアクセスすることを認めるか否かを問い合わせることによって、ユーザーにコントロール手段を与えています。
- 2020 年、Apple は、デベロッパ間および App 間の追跡について、ユーザーから明示的な同意を得ることをデベロッパに求める ATT ユーザー・プロンプトを発表しました。かかる ATT プロンプトは各デベロッパに、ターゲティング広告の目的のため、広告測定目的のため、または、データ・ブローカーと共有するために、ユーザーを追跡することに対して、そして、ユーザーの端末の IDFA にアクセスすることに対して、ユーザーの許可を求めることを要求しています。

80. 上述のとおり、これらの手段の目的は、競合他社のビジネスモデルを不利にして Apple のビジネスモデルを有利にすることではありません。その目的は、消費者に対して、その個人情報の利用に対して必要な保護とコントロール手段を提供することにあります。実際、これらの措置により、Apple は、消費者のプライバシーのために、追跡が必要となる形態で広告をパーソナライズしない<sup>39</sup>ことによって、Apple のデジタル広告ビジネスモデルを競争上不利な立場に置くことを意識的に決断したのです。特に、Apple は、限られた数のファーストパーティ App における Apple 自身の限定的なデータ収集行為に関して、プライバシーに関する追加の選択肢をユーザーに提供していますが、この選択肢はサードパーティがユーザーに提供していないものです。Apple は、その配信する広告に関して、パーソナライズされた広告

<sup>38</sup> DMCH 中間報告、82 頁。

<sup>39</sup> 「サードパーティ・データを全く利用しないことを選択したことによって、Apple はユーザーを追跡することによって得られたであろう追加の広告収入のすべてを放棄していることは注目に値するものです。したがって、Apple は、ATT が Apple の広告事業に課し得る収入ペナルティを 100%自発的に引き受けたこととなります。」と論じられています。Kinshuk Jerath、「Mobile Advertising and the Impact of Apple's App Tracking Transparency Policy」(2022 年 4 月)、コロンビア・ビジネス・スクール、<https://www.apple.com/privacy/docs/Mobile Advertising and the Impact of Apples App Tracking Transparency Policy April 2022.pdf> を参照下さい。

のオンまたはオフのいずれかを選択するための、より顕著で不回避的な選択肢を積極的にユーザーに提示しています。この選択画面では、パーソナライズされた広告の目的とそのプライバシー慣行についてユーザーに通知し、ユーザーがパーソナライズされた広告を有効化するか無効化するかを判断することができるようにしています。

81. 対照的に、Meta および Google を含むほとんどの大手広告プラットフォーム会社は、ターゲティング広告のためのファーストパーティ・データの利用を無効とする選択肢をユーザーに提供していません。そして、そのような選択肢を提供している企業は、多数の設定画面を含む煩雑な手続きの下にそれを埋没させています。Apple は、パーソナライズされた広告を配信するためにファーストパーティ・データを利用する許可を明示的かつ不回避的にユーザーに促すことで、またしても最前線に立っています。
82. 透明性を低下させて、消費者が握る権限は小さい方が望ましいと考える利害関係者は、パーソナライズされた広告プロンプトと ATT プロンプトとを比較しようとしています。彼らは、プロンプトの差異によって、ユーザーが追跡を許可するよりもパーソナライズされた広告を許可する選択をする可能性を高くしている可能性があり、結果として Apple を優遇していると主張しています。これらの懸念には根拠がありません。これらの二つの性質は根本的に異なっているため、選択の構造およびプロンプトの文言が同一であるべきであると結論付ける理由は存在しません。
- 第一に、上述したとおり、ATT は、複数のデベロッパをまたいでユーザー・データを「追跡する」こと（言い換えれば、広告の目的でサードパーティ・データを利用すること）に関係しているのに対して、パーソナライズされた広告は、Apple が自身のサービスによって収集したファーストパーティ・データを利用することにのみ関係しています。これらの二つの間には、業界で広く認識されている本質的かつ実質的な差異があり、前者は後者よりも相当干渉的です<sup>40</sup>。
  - 第二に、ATT 自体に関して、Apple とサードパーティは同じルール of 適用を受けています。サードパーティ ATT プロンプトと比較するのに適切なプロンプトとなるであろう ATT プロンプトを Apple が表示しない唯一の理由は、Apple が追跡を行わないからです。
  - 最後に、ATT プロンプトとパーソナライズされた広告プロンプトとの間の形式上の差異が、ユーザーの選択率に不公平な差異を生じさせるという仮定には根拠がありません。この結論は、ユーザーは会社間の追跡とファーストパーティ・データの使用を同一視するはずであり、したがって選択の違いは実質ではなく、プレゼンテーションの様式に起因するという脆弱な憶測に基づくものです。より一般的には、ATT の影響を完全に測定するには時期尚早ですが、ATT の実施が Apple 自身の広告サービスのパフォーマンスを大きく向上させたことを示唆する証拠はありません。
83. したがって、DMCH 中間報告の懸念は、原則論として、Apple がユーザーに権限拡大のために導入した重要なユーザー・プライバシー対策を問題視しており、Apple がプライバシー保護対策を通して自社優遇を行っているという認定を裏付けるものではなく、相当誇張されたものといえます。

---

<sup>40</sup> 例えば、<https://clearcode.cc/blog/difference-between-first-party-third-partycookies> を参照下さい。  
<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>、44 頁；  
<https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc-cross-device-tracking-report-1-23-17.pdf>、6-9 頁；pdf；  
<https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc-cross-device-tracking-report-1-23-17.pdf>、46-49 頁； および [Comment to the FTC from the Center for Digital Democracy \(Nov. 16, 2015\)](#) も参照ください。

- (ii) ATT がいかなる危害からユーザーを保護しているのかを適切に考慮する必要があること

84. Apple は、DMCH 中間報告の焦点が、ATT の消費者に対する影響ではなく、他社のビジネスモデルに当てられていることを強く懸念しています。Apple は、ATT がデータ収集活動に悪影響を与える可能性があることを認識しています。しかし、このような隠れたデータ収集および追跡活動こそが危害を与えるものであり、ATT によって対処されることが意図されているのです<sup>41</sup>。実際に、消費者保護団体とプライバシー擁護団体は、ATT を広く歓迎しています。例えば、

- アムネスティ・インターナショナル、ヒューマンライツ・ウォッチ、電子フロンティア財団などは、これらの変更を公然と支持し、擁護しています。The Center for Democracy and Technology はこの機能を称賛し、それが「データ収集と共有がより透明化され、追跡がもはや標準ではなくなるように、エコシステムがバランスを取り戻すのに役立つだろう」と指摘しました。<sup>42</sup>
- Mozilla Foundation は、ATT プロンプトの導入を支援するためのオンライン請願を立ち上げました。「Apple が計画している反追跡機能の実装は、その多くが自分の携帯電話の App を通して追跡が行われることを知らない可能性がある消費者にとって大きな勝利です。実際に、2019 年の Mozilla-Ipsos 調査によって、iPhone 所有者の大半は、IDFA や App によるデータ収集の存在を知らなかったことが判明しました。さらに、それらの存在を知っていた所有者も、それらのリセットの方法を知りませんでした。現在では、使用時に直接追跡を拒否することができるようになったため、消費者は、これからは自分のプライバシーを保護するために自分の電話設定内を捜し回る必要がなくなりました。しかし、先ず始めに、Apple がこの変更を実施しなくてはなりません。私たちは、この会社がこの施策から離れることがないようにする必要があります。」<sup>43</sup>
- フランスのプライバシー規制当局である CNIL は次の立場を採っています。「Apple が提案する変更は、ユーザーとアプリケーション・デベロッパの両方にとって真の利益をもたらすことができます。第一に、そのデバイスは、一方では、(上記で想定される要素に従うことを条件に)ユーザーが自分の選択をシンプルかつ十分な情報に基づいた方法で表明することを可能にし、他方では、ユーザーの同意無しにデベロッパがユーザーを追跡することを技術的および/または、契約上阻止することによって、ユーザーに自分の個人情報に対するより良いコントロールを提供することになります。さらに、同意を得るためのプロンプト自体を標準化し、広告目的の追跡を実施するすべてのアプリケーション・デベロッパがそれを使用することにより、ユーザーの選択の行使を大幅に促進することを可能にします。第二に、当委員会は、問題の「ポップアップ」は、多くの小規模デベロッパに、広告追跡業務に対する有効な同意を得ることを可能とするシンプルなツールを提供することによって、「データ保護法」の第 82 条の規定によって課せられた義務を遵守するのに役立つことを指摘します。」<sup>44</sup>

<sup>41</sup> 最近の Washington Post-Schar 世論調査によれば、回答者の 79%が、ハイテク企業は、自分の情報がどのように追跡され、利用されるのかについて十分なコントロールを提供していないと考えていることが分かりました。この同じ世論調査によれば、Facebook が個人情報とインターネット上の行動に関するデータを責任を持って取り扱っていると信頼している回答者は 20%しかいないことが分かりました。以下を参照下さい。 [https://www.washingtonpost.com/context/nov-4-22-2021-washington-post-scharschool-tech-poll/1f827037-688f-4030-a3e4-67464014a846/?itid=ik\\_inline\\_manual\\_6](https://www.washingtonpost.com/context/nov-4-22-2021-washington-post-scharschool-tech-poll/1f827037-688f-4030-a3e4-67464014a846/?itid=ik_inline_manual_6)。

<sup>42</sup> 以下を参照下さい。 <https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-andempowering-users>。

<sup>43</sup> [https://foundation.mozilla.org/fr/campaigns/apples-anti-trackingplansiphone/?subscribed=1&utm\\_source=email&utm\\_medium=email&utm\\_campaign=2020advocacyfr&utm\\_content=appleidfathanks&utm\\_term=5383151](https://foundation.mozilla.org/fr/campaigns/apples-anti-trackingplansiphone/?subscribed=1&utm_source=email&utm_medium=email&utm_campaign=2020advocacyfr&utm_content=appleidfathanks&utm_term=5383151)。

<sup>44</sup> [https://www.autoritedelaconurrence.fr/sites/default/files/integral\\_texts/2021-03/21d07.pdf](https://www.autoritedelaconurrence.fr/sites/default/files/integral_texts/2021-03/21d07.pdf)、第 62-64 項。

85. プライバシー保護組織や規制当局のみならず、デベロッパも ATT を支持しており、その消費者への利益を認めています。例えば、Snap は、「我々は Apple を称賛しており、彼らが顧客のために正しいことをしようとしていると信じています」、「我々は、(ATT は) 短期的には広告主に多少の混乱を招くとしても、消費者にとって全体的によいものであると考えています」と述べ、ATT を称賛しています<sup>45</sup>。

86. ATT が具体的に対処している危害を考えると、内閣官房デジタル市場競争本部によるデベロッパへの影響の評価は、単に財務的影響と広告活動に対する悪影響のみを検討し、そこで終わってはなりません。そうではなく、その評価は、ATT が消費者にもたらす重要な対立利益も十分に考慮しなければなりません。Apple は、ユーザーに対するこれらの利益を、(パラグラフ 78 で指摘したコメントのように) 単に表面的に認めるのではなく、(ATT が、隠された追跡およびデータ収集活動によって生じる危害にどのように対処しているかについて、) 適切な分析をすることを勧めます。

(iii) ITP が、Apple の広告ビジネスモデルに利益をもたらし、他者を不利にすることはないこと

87. ATT と同様、内閣官房デジタル市場競争本部は、ITP について次のように異論を唱えています。「Apple 自身はトラッキング・クッキーの使用を求めているため、ITP は適用されない。すなわち、サードパーティが広告をパーソナライズする能力を制限される一方、Apple 自身には ITP は適用されないことから、そうしたルール変更の影響を受けることなく、引き続き、ファーストパーティとしてユーザーに関するデータを取得することができる状況となっており、総合的にみれば、Apple が有利になっているといえる。」<sup>46</sup>前述の ATT に対する懸念と同様に、これには根拠がありません。

88. 第一に、前述したように、ファーストパーティとサードパーティ・データの収集の間には、広く認識されている正当な違いがあります。第二に、ITP は、活発な競争の結果であり、競争を阻害するものではありません。ITP は、サードパーティ・クッキーに対するプライバシー優先のアプローチを開拓し、それによってユーザーの選択肢を広げ、競合他社の対応を促しました。2017 年に Apple が WebKit に ITP を導入した時に、デフォルト設定によってサードパーティ・クッキーを遮断し、プライバシーを侵害する、サイトをまたぐ追跡に対抗する最初のエンジンとなり、2018 年に初めて発表され 2019 年にデフォルト設定として実装された Mozilla の Enhanced Tracking Prevention (ETP) がそれ続けました<sup>47</sup>。Gecko も同様に、追跡防止手段を実装しています。これは競争の結果であり、そして ITP の価値を実証するものです。

(iv) Apple は自社製品を優遇するような方法でデータを取得・使用していないこと

89. DMCH 中間報告は次のように懸念を示しています。「Apple、Google は、OS、ブラウザ、アプリストアなどモバイル・エコシステムの主要サービスを提供しているため、そのような立場にないプレイヤーが得ることができない非公表データを入手し、それを自己の製品開発やサービス向上などに活用することができる。」<sup>48</sup>少なくとも Apple について、この懸念に根拠はありません。

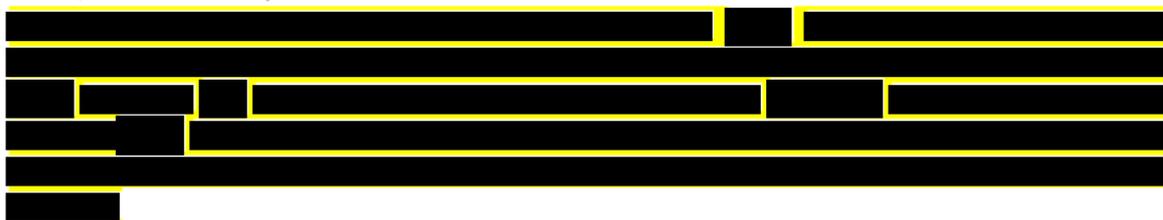
<sup>45</sup> <https://www.cnbc.com/2021/02/05/snap-ceo-spiegel-says-apples-iphone-privacy-change-is-good-forconsumers.html>。

<sup>46</sup> DMCH 中間報告、86-87 頁。

<sup>47</sup> <https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-bydefault/>; <https://blog.mozilla.org/futurereleases/2018/08/30/changing-our-approach-to-anti-tracking/>

<sup>48</sup> DMCH 中間報告、243 頁。

90. 第一に、事実の問題として、Apple が取得する情報は、内閣官房デジタル市場競争本部が考えているよりも、かなり限定的です。Apple は、ユーザーの「属性」やユーザーが App で使用する機能に関する情報を保持・使用することはありません。同様に、App Store 内の広告は、Apple Pay、Maps、Siri、iMessage や iCloud 等他の Apple サービスから消費者データにアクセスすることはありません。また、Health app、HomeKit、電子メール、連絡先、通話履歴等のサービスや機能を通してデバイスからデータを使用することはありません。Apple は、個々の消費者がどのような広告を受け取っているかを知ることはありません。同様に、Apple は、ユーザーの閲覧履歴のデータを収集・保持することはありません。Safari は、ユーザーのプライバシーを保護するために一から設計されています。ITP やフィンガープリントの保護などの重要なプライバシー保護機能は、デフォルト設定で有効になっています。Safari は、Apple が収集し、サードパーティと共有するデータ量を最小限におさえます<sup>49</sup>。
91. App Store の運営者として、Apple は、他のあらゆる店舗（デジタルまたは実店舗）運営者と同様、エンドユーザーと製品サプライヤーの両者による店舗の利用によって生じる情報へのアクセスを有しています。スーパーマーケットが、どの商品が販売されているか、どれだけ販売されているか、そしていくらかそれらが販売されているかに関する情報を持っているのとまったく同じように、App Store も、販売されている App およびデジタル・コンテンツに関する情報を持っています。これは何も珍しいことではありません。しかしながら、他の多くの企業と異なり、Apple はデータの最小化（ある特定のサービスのために、ユーザーが必要とするものを提供するために必要最低限のデータのみを収集すること）やデバイス上での処理（ユーザーのプライバシーを保護しデータ収集を最小化するために、データを Apple に送信するのではなく、可能な限り端末上で処理すること）等の手法を採用し、Apple がユーザーから収集するデータを制限するために多大な努力をしています。
92. Apple は、適用法令に基づき正当な法的根拠がある場合にのみ、ユーザーの個人情報を使用します。状況に応じて、Apple は、次のことに依拠することがあります。(i) ユーザーの同意、(ii) ユーザーとの契約を履行するために処理が必要であること、(iii) 正当な利益の目的、または(iv) Apple ユーザーその他の者の重要な利益を保護すること、若しくは法律を遵守すること。Apple は、設計上、プライバシー保護を組み入れており、ユーザーに対して、ユーザー・データについての透明性とコントロールを提供しています。
93. 第二に、(ユーザーエンゲージメント、財務業績、課金データを含む) App Store データは、App の開発に関する意思決定や検索順位に影響を与えるために、Apple のサービス事業と共有されることはありません。Apple のデータ解析チームは、App Store データへのアクセスを一元的に管理しており、事前に必要な許可を得ることなくデータが拡散されることを防止する手続きを確立しています。



94. App Store から取得可能なデータは、主にデベロッパと消費者の双方にとっての App Store のエクスペリエンスを改善するために使用されます。例えば、App の使用情報は、特定の App ま

<sup>49</sup> 例えば、ITP は、機械学習を用いてトラッキングデータをローカルに分類し、閲覧履歴が Apple に送信されないようにしています。Apple は、Safari ウェブ・ブラウザのプライバシーに関する Apple のコミットメントについての詳細な情報を含むホワイトペーパー「Safari Privacy Overview」を公表しました。Safari Privacy Overview (2019 年 11 月) は次のサイトで取得できます。

[https://www.apple.com/safari/docs/Safari\\_White\\_Paper\\_Nov\\_2019.pdf](https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf)

たは App が使用する技術（例えば API）が、デバイスのパフォーマンス（例えば電池寿命）に悪影響を与えているかどうかを判断するために役立つ可能性があります。

95. 第三に、Apple は自社製品を有利にするためにデータを保持しているわけではありません。Apple は、デベロッパが自身の App がどのような成績を上げているかを理解できるように、App Store Connect ポータルを通じて販売その他のデータをデベロッパと共有します。例えば、Apple は、デベロッパが、ユーザーがデベロッパの App にどのように関わっているのかをより良く理解し、売上を伸ばすことを助けるために、売上高、App・ユニット・インストール、削除、クラッシュ、返金、サブスクリプションの更新等の、個人を特定できない集積された豊富な App 解析データ一式をデベロッパに提供しています。
96. 同様に、Apple は、最もダウンロードされている App に関する情報を取得しますが、Apple はこの情報を、上位ダウンロード・チャートの中で公開しています。この情報は、App Annie のようなサードパーティ・サービスからも取得可能です。

(v) ソーシャル・ログイン（「Sign in with Apple」）は Apple に競争上の優位性をもたらさないこと

97. DMCH 中間報告は、「SIWA のこのような効果によって、それが無い場合と比べて、Apple が容易に様々な取引等のデータを入手することが可能となり、その結果、Apple 自身は当該データを利用でき、サービスの改良等がなされることによりユーザーの利便性を向上させることが比較的容易となる。そのような観点からも、この SIWA によって、Apple は競争上有利となるおそれもある。」と考えています<sup>50</sup>。この懸念も同様に根拠がないものです。
98. App 内の活動追跡を減らすためにデベロッパからユーザーの電子メールアドレスを隠す Sign in with Apple (SIWA)は、Apple が長年にわたって導入してきたプライバシー保護機能の一つです。そのほかにも、Touch ID、Face ID、キーチェーンとパスワード等のイノベーションがあります。これらの機能はすべて、端末とその中に保持される情報のセキュリティを向上させるという同じ目的を有しています。
99. Apple は今までに、ソーシャル・ログインの最初のオプションとして SIWA を表示することを要求したことはなく、それを理由に App を拒否したことは一度もありません。2019 年に導入されたガイドライン 4.8 では、自身の App 内でサードパーティのソーシャル・ログイン・サービス（例えば、Facebook Login、Google Sign-In、Sign in with Twitter、Sign In with LinkedIn、Login with Amazon、WeChat Login）を提供することを選択したデベロッパは、SIWA も選択肢の一つとして提示しなくてはならないという義務を課しています。しかし、SIWA を優先的に表示することはガイドラインで求めていません。また、デベロッパが自身のサインイン機能のみを使用している場合は、App 内で SIWA を選択肢として提供する義務を負いません。例えば、自身のログインオプションのみを使用する WeChat は、SIWA を提供する義務を負っていません。
100. このガイドラインは、ユーザーがデベロッパの App にログインする際に、ユーザーが個人情報をデベロッパまたは Google や Facebook のような大規模広告主に提供することを要求しないことから、プライバシーにより配慮した選択肢を与えるために導入されました。Apple は SIWA の使用に対して課金することはなく、いかなる方法によっても収益化することはありません。単に、広告主やデータ・アグリゲータによる追跡を避けたい Apple 製品ユーザーのための選択肢として提供されています。
101. さらに、たとえユーザーが「Sign in with Apple」を選択することによって、ユーザーの個人情報を追跡し共有するサードパーティ・サインイン・サービスの能力を弱めても、これは他のデベロッパとの競争において Apple に優位性を与えるものではありません。Apple は、App 内あ

<sup>50</sup> DMCH 中間報告、249-250 頁。

るいはウェブサイトにおけるユーザーの活動をまったく追跡しないため、SIWA から「優位性」を得ることはありません。Apple は、ユーザーが Sign-in with Apple を経由して接続することを選択した App およびウェブサイトの記録を有するのみであり、それは単にユーザーが選択した場合には接続を断つことを可能とするためのものです。

## E. 音声アシスタントとウェアラブル

102.別の報告書の中で、内閣官房デジタル市場競争本部は、音声アシスタントやウェアラブルに関して多くの懸念を提起しています。同報告書で指摘されているように、市場では多くの音声アシスタント、ホーム・デバイス、およびウェアラブルが出回っており、それらの市場は日本で発展し続けています。Apple は、自身が厳しい競争に直面していると考えており、自身の行為が競争を妨げる、または、消費者を害する効果を有しているとは考えておりません。例えば、ユーザーは、Amazon、Google、Sonos、その他多くの企業が提供する人気が高いオプションを含むスマート・スピーカーを経由して、音声アシスタントにアクセスすることができます。実際、Amazon と Google が世界のスマート・スピーカー市場を支配しています。Apple のスマート・スピーカーである HomePod と HomePod Mini の市場シェアは、比較的小さいものです。

103.以下では、音声アシスタントおよびウェアラブルに関して提起された主な懸念について述べます。

### (i) Siri のプリインストールとデフォルト設定は競争上の懸念を惹起しないこと

104.内閣官房デジタル市場競争本部の報告書は、スマートフォンのスクリーンが小さいために、プリインストールされた、またはデフォルト設定の音声アシスタントを使用する傾向がユーザーの間にあるように思われ、音声アシスタントのそのようなプリインストールやデフォルト設定は、他社の音声アシスタントを競争上不利にする、という懸念を提起しています。Apple は、Siri に関してはこの懸念に根拠はないと考えます。

105.Siri は、Apple の端末と緊密に統合されているシステムの中核的機能であり、ユーザーにコントロールを与えている厳格なプライバシー保護を備えて設計されています。上記で詳細に論じたように、Apple は、ハードウェアとソフトウェアの統合が、ユーザーが期待している最上級のユーザーエクスペリエンスおよび強化されたプライバシーとセキュリティを提供する最良の手法であると考えています。一般に、ハードウェア、ソフトウェア、およびサービスの統合は、ユーザーの利益となる相乗効果を達成することに役立ちます。Apple は、Siri がデータをユーザーの身元と結び付けることを防ぐために、これらのデータがユーザーの端末を離れる前にエンドツーエンドの暗号化やローターとする識別子を含む厳格なプライバシー保護を適用しています。サードパーティの音声アシスタントが、Apple のユーザーが期待するような、同等のプライバシーとセキュリティの保護を提供するとは限りません。しかし、いずれにせよ、Apple は、消費者が Amazon Alexa や Google Assistant を含む他の音声アシスタントを選択することを可能としています。

106.機能性をサポートするために他の音声アシスタントにアクセスすることに関しては、Apple は、ユーザーが App Store を通じて音声アシスタントにアクセスすることを容易にしており、これらの音声アシスタントは、様々な特徴や機能を提供しています。例えば、iPhone 上の Amazon Alexa App では、ユーザーは、Alexa を使用できる端末の管理、音楽再生の操作、外出先での買物リストの表示、今後のリマインダーの記録、稼働中のタイマーの確認などができます。ユーザーが Alexa でハンズフリー機能を有効にすると、当 App がユーザーの画面上にある時に単に「アレクサ」と呼びかけることで話をするすることができます。同様に、iPhone 上の Google Assistant App では、ユーザーは、即時の電話、テキストメッセージの送信、電子メールの送信、リマインダーの設定、カレンダー・イベントの設定、音楽の再生、ナビゲーション、そして天気情報の取得が可能です。

107.しかし、音声アシスタントの同時操作は、ユーザーにとって重大なプライバシーのリスクを伴います。ユーザーが、自分の発言を Siri に向けることを明確に選択したことを確認することが重要です。もしサードパーティ音声アシスタントが、ユーザーが Siri に向けた発言を聞くことができると、Apple はユーザー・データに対する高水準の保護やユーザーエクスペリ

エンスの質を保証することができなくなります。そのため、Siri は、使用のトリガーとなる言葉である「Hey Siri」の発言、または HomePod 若しくは HomePod Mini 上の Siri ボタンのプッシュのみに反応します。HomePod と HomePod Mini 上では利用できませんが、他のスマート・スピーカーに搭載されているその他の音声アシスタントは、異なるトリガーまたは「ウェイク」ワードを選択することができます。

(ii) Apple は、サードパーティによる音声アシスタントの開発を制限しないこと

- 108.内閣官房デジタル市場競争本部の懸念に反して、サードパーティが自身のサービスを以前と変わらず提供することを継続するために必要な機能を提供することは不可能ではなく、音声アシスタントの柔軟な開発が制限されることはありません。
- 109.Apple は、デベロッパに対して、デベロッパが既存の App の「拡張機能」を通じて App と Siri を統合することを可能とするフレームワークである SiriKit を通じて、App を Siri と統合する選択肢を提供しています。SiriKit は次の 2 つのタイプの App 拡張をサポートしています。(1) SiriKit からユーザーのリクエストを受領し、それを App 独自のアクションに変える Intents app extension、および、(2) Intents app extension がユーザーのリクエストを満たした後に、Siri インターフェース内で、ブランディングその他のカスタマイズコンテンツを表示する、Intents UI app extension。Siri が developers Intents app extension と連携するためには、ユーザーの許可が必要です。Intents UI extension は任意のものです。デベロッパ・プログラムに参加し、Apple Developer Program 使用許諾契約に同意しているデベロッパは、SiriKit によって Siri と統合させることができます。Apple は、デベロッパが、その App を Siri と連携させることを容易にし Siri 経由で利用できるようにするために、SiriKit の開発に投資しています。
- 110.さらに、HomeKit は、ユーザーが、そのスマートホーム内のサードパーティ接続アクセサリと通信し、それらをコントロールすることを可能にします。HomeKit は、HomePod、Apple TV、モバイル端末等の Apple 端末に統合されており、Home app、tvOS および Siri 等のスマートホーム・ユーザーインターフェースでコントロールすることができます。Apple は、デベロッパに対して、MFi プログラムを通じて、HomeKit を広く提供しています。世界中で 100 を超えるブランドが HomeKit のフレームワークに対応するアクセサリを提供しており、利用可能なアクセサリ数は、日々増加しています。その一覧は、<https://www.apple.com/ios/home/accessories/>で確認できます。
- 111.Apple は、HomeKit や Siri などの機能や技術を導入する際に、サードパーティデベロッパがそれらを利用可能にするために尽力しています。同時に、Apple は、プライバシーが基本的人権であると考えており、これらの新しい技術へのアクセスを提供する際には、ユーザーのプライバシーとセキュリティを確実に保護するために細心の注意を払い続けています。
- 112.Apple は、Siri のプライバシー保護を徹底し、ユーザーがコントロールできるように設計しました。Siri の音声入力が入力されている場合、発言内容や音声入力された内容が Apple に送信され、リクエストが処理されます。位置情報サービスが入力されている場合は、リクエストに対する Siri の応答精度が向上するよう、リクエストされた時点の端末の位置情報も Apple に送信されます。Siri にリクエストしたときに位置情報サービスが入力されているかどうかにかかわらず、リクエストは特定の Apple ID ではなくランダム識別子に紐付けられます。このランダム識別子は、Apple ID や E メールアドレス、その他のユーザーデータとは紐付けられません。すなわち、Siri を使用する際に、位置情報と Apple ID が結び付けられることはないため、ユーザーのプライバシーは保護されます。音声入力はいつでも無効にでき、ランダム識別子に紐付けられている音声入力の履歴は、「設定」>「Siri と検索」>「Siri と音声入力の履歴」と選択して「Siri と音声入力の履歴を削除」をタップすると削除できます。ユーザーによって削除されることがないリクエストの大半は、2 年後に Apple サーバから削除されます。2 年以上保持されるごく一部のデータは、Siri の今後の改善目的でのみ使用されます。Siri は、収集するデータを最小限にするために、端末上のローカル処理によって、ユーザーによるトリガ

ーコマンドをモニタリングします。ユーザーは、その利用するサービスをコントロールし、選択することができます。ユーザーが Apple のサービスにアクセスする際のプラットフォームに関わらず、Apple の厳格なデータ管理の慣行は一律に適用されます。サードパーティのサービスを利用する場合、ユーザーはサードパーティのデータの慣行に従うことになります。

113. サードパーティ音声アシスタントに関して、内閣官房デジタル市場競争本部の報告書で言及された特定のデバイス機能へのアクセスを可能にすることは、相当のプライバシーリスクを伴います。例えば、サードパーティ App が iOS 端末のマイクに常時アクセスすることやメッセージ App 内のユーザー・テキストを読むことを許可すると、端末のマイクやメッセージ App に露出したユーザーの発言やデータ（機密性が高い健康情報や財務情報を含む）が、Apple の厳格なプライバシー基準に従って収集、処理、保護されることを保証できなくなり、Apple のデータ・プライバシー・ポリシーが直ちに無効化されます。実際に、Google や Amazon のようなデータ収集会社は、ユーザー・データに関して完全に異なるビジネスモデルで事業を展開しています。

(iii) Apple Watch はデベロッパの競争力を制限しないこと

114. 内閣官房デジタル市場競争本部は、Apple Watch、特にヘルスケアデータに関して多くの懸念を示しています。これらの懸念は、ヘルスケアデータにリンクするサードパーティ事業者に対する制限と、Apple が自らの利益のために使用するためにデータを取得することに関するものです。これらの懸念には根拠がありません。

115. HealthKit は、iPhone および Apple Watch 上のヘルスケアやフィットネスに関するデータの一元管理を可能にします。ユーザーの許可があれば、App は HealthKit の記憶装置と通信し、このようなデータへのアクセスや共有を行うことができます。また、HealthKit は複数のソースからのデータも管理、統合できるように設計されています。たとえば、ユーザーはすべてのデータをヘルスケア App で閲覧・管理でき、データの追加、削除、App の許可の変更などを行うことができます。

116. デベロッパは、Apple の HealthKit を利用することで、ヘルスケア App その他の App とデータの共有ができる、ヘルスケアとフィットネスのための App を作成することができます。ユーザーは、HealthKit の情報のうち、どの要素を、どの App と共有するか、管理することができます。HealthKit と連携する App は、ユーザーが許可した場合に、ユーザーの健康やフィットネスの増進、健康に関する調査などの目的でのみ、データを共有できます。信頼できる App とデータを共有することをユーザーが選択した場合、データは Apple のネットワークを経由することなく、HealthKit からサードパーティの App に直接送られます。研究者は App 開発用のオープンソースのフレームワークである ResearchKit を使用することで、参加者の登録や研究の実施を容易にすることができます。ResearchKit はプライバシー重視の設計になっており、どのような情報を提供するかは、ユーザーが管理できます。

117. ヘルスケアデータには機密性の高い個人情報が含まれている可能性があるため、App が HealthKit の記憶装置からデータを読み取ることや、HealthKit の記憶装置にデータを書き込むには、ユーザーから許可を得る必要があります。また、そのようなデータを常時保護するための措置を講じることが義務付けられています。詳細については、[https://developer.apple.com/documentation/healthkit/protecting\\_user\\_privacy](https://developer.apple.com/documentation/healthkit/protecting_user_privacy) を参照してください。

118. Apple は、ユーザーの許可なくユーザーのヘルスケアデータにアクセスできません。また、ユーザーが信頼できる App とデータを共有することを選択した場合、そのデータは HealthKit からサードパーティの App に直接送られ、Apple のネットワークを経由しないため、HealthKit が Apple の App 開発に有利に作用することはありません。同様に、ユーザーがサードパーティに

データの閲覧を許可している場合、Apple は、サードパーティが同社の App からヘルスケアデータにアクセスすることを妨げていません。

119. 上述した理由により、HealthKit は、Apple サービスに有利なものではありません。Apple は、データに関して最恵国待遇や排他性を求めています（ユーザーからアクセスを認められたサードパーティは、適切なプライバシー保護が行われていることを確実にしなければならぬという要件を除きます）。

## F. 対応策

120. DMCH 中間報告を通じて、エコシステムに対する広範囲に渡る対応策や変更の可能性が提案されています。以下に述べるとおり、これらの対応策には合理的な根拠がなく、対応策自体も実行可能でなく十分に検討もされていません。

- (i) 内閣官房デジタル市場競争本部の対応策の基礎となる結論は、根拠がなく、推測の域を出ないこと

121. 内閣官房デジタル市場競争本部は、根拠のない憶測、根拠のない主張、および仮説的な懸念から、技術、製品設計、および競争上の影響について結論を出しています。このような熟慮を欠くアプローチの例は、次の「認定 (findings)」に見られるとおりです。

122. 104 頁：「Apple はプライバシーやセキュリティを理由にあげることがよくあるが、こういってしまえば、プライバシーやセキュリティを保護する必要性については否定できず、どういう点に問題があり得るかは技術的専門性や Apple のデバイスの詳細等も分からないと何とも言えず、それ以上突っ込めなくなるので、便利な口実になっているという印象を受ける。」内閣官房デジタル市場競争本部による Apple のプライバシーとセキュリティに関する考察は全く不十分であり、Apple が提出した証拠を考慮せずに不当な推論に至っていることは、上記から明らかです。

123. 他の例では、内閣官房デジタル市場競争本部は、純粋な仮定と憶測に基づいて回答しています。例えば、110 頁において、内閣官房デジタル市場競争本部は、「App Store 以外のアプリストアを認めれば、ユーザーはセキュリティも考慮した上で複数のアプリストアの中から選択することができるようになる。Apple を含むアプリストアを運営する事業者は、アプリストアのセキュリティの面で競争することになり、その結果、セキュリティというサービスの質が向上することが考えられる」と述べています。

124. 同様に、内閣官房デジタル市場競争本部は、110 頁で、「Apple は、サイドローディングを認めると iPhone 及び iOS のセキュリティが脆弱化する旨を主張する。しかしながら、仮にそのような面があるとしても、将来の技術の進展・革新によって、サイドローディングに伴うセキュリティ・リスクに対処できるようになる可能性は否定できず、セキュリティ上のリスクを理由に App Store 以外の配信手段を禁止することが将来に亘って正当化されるものではないと考えられる」と認定 (finds) しています。

125. DMCH 中間報告は、159 頁において「Apple は、ブラウザ・エンジンを改良せず、ウェブ・アプリのインストール機能の実装に消極的」と結論付けています。この大まかな認定 (finding) には、一つの商業ウェブサイトによる極度に単純化された比較以外、何の裏付けも与えられていません。この認定は、証拠による裏付けを全く欠くものです。

126. 最後に、197 頁に記された「現在の iPhone には、約 40 の自社製アプリが内蔵されており、ブラウザである Safari、アプリストアである App Store はそれらの内蔵アプリである。このよう

に、Apple が iPhone のデフォルト・アプリを決定しているところ、Safari は iOS のデフォルト・ブラウザとして設定されている」という認定は、プリインストールやデフォルト設定の利便性がモバイル端末のユーザーに高く評価される実益をもたらすこと、また、ユーザーが望めば「設定」でデフォルトのブラウザを Safari から他のブラウザに変更できるという事実性を完全に見落としています。

127.結果として、DMCH 中間報告による認定 (findings) は、事実上、未検証かつ一方的な証拠に基づくものであり、Apple のエコシステムがいかに競争を阻害する「可能性がある」かについての仮説に過ぎないものとなっています。このような仮説は、現段階において、抜本的なものになり得る対応策を議論することを正当化するには不十分です。競争阻害に関する理論を根拠付け、競争と消費者に対する実際の影響を検討するために必要な、重要な調査作業が残っています。

(ii) 内閣官房デジタル市場競争本部が提案する対応策は、曖昧、不明確であり、実行不可能であること

128.内閣官房デジタル市場競争本部による根拠のない懸念と認定の結果、それらの懸念に対処するための対応策も同様に、証拠または適切な検討の裏付けがないものです。その例は次のとおりです。

129.DMCH 中間報告は、163 頁で「ウェブ・アプリには OS やそれをベースとしたアプリストアに非依存で、アプリストアを介さず顧客にリーチできるという特性がある。この特性に鑑みれば、ウェブ・アプリとネイティブ・アプリが競争する環境を整えることによって、モバイル・エコシステム全体における競争環境の改善が図られるべきと考えられる」と提案しています。このまったく漠然とした提案は、明らかに、改善がいかなるものであるべきか、および/または、その「改善」を行うために現行システムの変更をすることの影響について、ほとんど検討していません。上記のセクション C およびセクション D で述べたように、現行の仕組みは、ユーザーとデベロッパが同様に、安全でプライバシー保護が強化された高性能のシステムの便益を得るために必要なものです。内閣官房デジタル市場競争本部がこのことを考慮せずに結論を出したことは明らかです。

130.内閣官房デジタル市場競争本部は、33 頁で「レイヤーの特性や影響力に応じた形で対応策を組み合わせることにより、エコシステム全体のあるべき姿の実現を目指していく」とつもりであると述べています。しかし、同頁で示されている「あるべき姿」とは、単純化された完全競争のモデルであり、高い消費者満足度、利用の増加、高いイノベーション率を特徴とする現在の状況と比較して、「競争圧力」が増加するだけで、ユーザーとデベロッパにとって何らかのより良い結果をもたらされるという大前提に立っています。サードパーティの参入によって競争圧力を高めようとする試みは、緊密に統合された現在の設計と根本的に対立し、現在 Apple の製品の主要な差別化要因となっているエコシステム内のセキュリティおよびプライバシーの悪化につながるのみです。

131.内閣官房デジタル市場競争本部は、38-39 頁において、Apple のモバイル・エコシステムが「一人勝ちの状態」となる可能性があるという全く根拠のない前提を採用しています。これは近視眼的であり、エコシステムがユーザーと開発者の双方にとって常に良い結果をもたらしていることを示す高い満足度などの明確な指標を、完全に無視しています。そして、この曖昧な前提は、「[Apple による] 競争に悪影響を及ぼす危険性の高い行為類型」を禁止対象として特定する唯一の根拠として依拠されており、特定の行為が禁止されるのを回避するためには、Apple が、セキュリティとプライバシーに対する考慮が「例外的理由」を構成することを示す必要があると異常に指摘されています。これも、セキュリティとプライバシーが、「ウォールド・ガーデン」としての Apple のエコシステムの設計のあらゆる部分の根底にある基本的な支柱であることを完全に無視するものです。

132.内閣官房デジタル市場競争本部は、51 頁において「他の事業者によるクエリ・データ及びインデックス・データへの合理的条件によるアクセス確保」を提案しています。制限を課す原則がまったく存在しないこのような対応策は、Apple の明示的な取り組みである「プライバシーバイデザイン」を根本的に否定するものです。Apple の信念は、ユーザーが知らないうちに、または同意なしに、侵害的なデータ収集行為の対象とされるべきではないというものです。さらに、このような極めて広範かつ包括的な要件は、ユーザーの利便性とセキュリティの両方を最大化する緊密に統合されたシステムを確保するという Apple の現在のアプローチを完全に損なうものであり、モバイルエコシステム内での当該データのアクセスおよび保存方法を根本的に再設計することを Apple に要求することになります。このような対応策により、App は端末やユーザー・データにアクセスしてユーザーの許可なくこれを収集または共有できることとなるため、ATT などの Apple の内蔵プライバシー保護手法は効力を失うこととなります。また、この対応策により、Apple の厳しいプライバシー基準に従ってユーザーデータが収集、処理、保護されることを保証できなくなるため、Apple のデータプライバシーポリシーを無効化することになります。

133.内閣官房デジタル市場競争本部は、84 頁および 211 頁において、「ユーザーへの通知の表示において、非中立的な方法でエンドユーザーに選択肢を提供したり、自律的な意思決定や選択を阻害する行為」を禁止することを提案しています。しかし、内閣官房デジタル市場競争本部は、Apple が「非中立的な」行為をし、または、ユーザーの「自律的な意思決定」を何らかの形で阻害しているという考えを裏付ける基本的な仮説、フレームワーク、分析すら提示していません。Apple は、ユーザーが希望すればブラウザ等のデフォルト設定を自由に変更することができること、また、一定のユーザーはプリインストールされたデフォルトオプションの利便性を高く評価していることを示す明確な証拠を提供しています。この提案は、このような曖昧で不明確な根拠に基づく対応策は、効果がないばかりか全く不相応なものとなり得るという重大な懸念を抱かせるものです。

134.最後に、内閣官房デジタル市場競争本部は、234 頁において、「事業者が提供する OS、ブラウザ、アプリストアをエンドユーザーが利用した際に得られたデータについて、当該エンドユーザー又は当該エンドユーザーが承認したサードパーティからの求めに応じて、当該データのポータビリティの有効な行使を容易にするツールを無償、継続的かつリアルタイムで提供することを義務付ける規律」を Apple が導入することが考えられる、と認定しています。この対応策は全く実行不可能かつ非現実的であり、セキュリティの目的のために、可能な限りユーザー・データを端末上で処理することに対する Apple のコミットメントを完全に無視するものです。

(iii) 内閣官房デジタル市場競争本部の提案する対応策は、消費者の選択と競争に対してより大きな弊害をもたらすリスクがあること

135.上述の懸念は、代替的なアプリケーションのストア、サイドローディング、代替決済処理方法、および代替ブラウザ・エンジンを iOS で許容することを義務付ける対応策のように、エコシステム全体の中核的な要素に対して重大な変更を求める可能性のある対応策に関して特に関係するものです。

136.Apple の製品は、品質、(特徴と機能性を含む)性能、セキュリティ、およびプライバシー保護の点で差別化されています。これらは消費者による選択の主な要因であり、多くのユーザーが Android ではなく Apple の端末を選ぶ理由として広く認識されています。キュレーションされた App Store、IAP 機能、WebKit 等のエコシステムの構成要素は、Apple の端末が最高水準のパフォーマンス、セキュリティ、およびプライバシー保護を提供することを保証するための Apple の全体的な取り組みの中心を成しています。

137.しかし、内閣官房デジタル市場競争本部の対応策は、問題に対して断片的なアプローチを採っており、Apple の緊密に統合されたエコシステムの現実を無視したものとなっています。あ

る分野のセキュリティまたはプライバシー保護を低下させる措置は、エコシステム全体に波及します。例えば、審査が不十分なストアからダウンロードされた App によるセキュリティ侵害は、当該 App だけでなく、他の App や端末全体のパフォーマンス、さらには感染した端末に接続する他の端末にも大きな影響を与える可能性があります。サードパーティ・ブラウザ・エンジンを通して端末にマルウェアが侵入した場合も同様です。このように、ある分野のセキュリティやプライバシー保護に悪影響を及ぼす対策は、Apple が提供するパフォーマンスや保護の水準を、システムに導入された最も安全性の低い代替手段が提供する水準まで低下させることとなります。

138. すなわち、端末の性能、セキュリティ、およびプライバシー保護の観点から、Apple が Android と同じ立場になるということです。2つのエコシステム間の競争上の差別化は、本質的に排除されることとなります。したがって、この対応策は、一方では、Apple のエコシステム内の特定の分野における選択肢を増やそうとするものですが、他方では、Apple のエコシステムと Android のエコシステムとの間に現在存在する競争を破壊することとなります。エコシステム間に存在する重要な競争は減少し、より広い消費者の選択肢も減少します。エコシステムの中での選択を望む消費者の要求は既に満たされている（そして今後も満たされる）のに対し、エコシステムの全体的なパフォーマンスと質を基準として選択することを望む消費者はその選択肢を失うこととなるため、これによる弊害は明らかです。

\*\*\*\*