

スマートフォンにおいて利用される特定ソフトウェアに係る
競争の促進に関する検討会（第4回）議事録

- 1 日時 令和6年12月5日（木）9:00～12:00
- 2 場所 対面（中央合同庁舎第8号館特別大会議室）とオンラインの併用
- 3 出席者

【委員】

依田座長、石井委員、上沼委員、川濱委員、伊永委員、滝澤委員、仲上委員、日高委員、
増田委員、梶田委員、山田委員

【公正取引委員会事務総局】

岩成経済取引局長、佐久間官房審議官、稲葉デジタル市場企画調査室長

【オブザーバー】

内閣官房副長官補室、内閣官房デジタル市場競争本部事務局、内閣官房国家安全保障局、
内閣官房内閣サイバーセキュリティセンター、個人情報保護委員会事務局、消費者庁、
こども家庭庁、デジタル庁、総務省、文部科学省、経済産業省

4 議題

○ ヒアリング

Apple Inc. からのヒアリング

○依田座長 それでは、定刻になりましたので、ただいまから、第4回スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する検討会を開催いたします。

本日は、石井委員、川濱委員、伊永委員、仲上委員、増田悦子委員、山田委員はオンラインで御出席いただいております。

それでは、本日の議事や資料の取扱いについて、事務局から説明をお願いします。

○稲葉室長 本日の会議については、同時通訳を入れて実施をいたします。

本日は、Apple Inc. の皆様方にお越しいただきまして、スマホソフトウェア競争促進法の下位法令やこの運用に対する御意見などについて御説明いただき、委員の皆様と御議論いただきます。

配布資料につきましては、右上に「構成員限り」と赤字で書かれている資料については、非

公表とさせていただければと思います。

また、本日の議事については非公開で、Apple、それから本検討会の委員、公正取引委員会のほか、本検討会のオブザーバーである関係省庁のみが参加しています。

議事録については、いつもどおり発言者の御確認を経た上で公表いたします。

また、本日も検討会の終了後に記者ブリーフィングを予定しております。ここでの具体的なやり取りについて、特に言及するつもりはありませんが、特に記者に対して発言を控えるべき内容がありましたら、その旨おっしゃっていただければと思います。

以上になります。

○依田座長 それでは、本日の議事に進みます。

まずは、資料を基にAppleの皆様から30分ほどで御説明いただきます。その後、委員の皆様から御意見や御質問をいただき、Appleから回答をいただければと思います。御意見、御質問については、今回は名簿の下から順番にお願いします。お時間の都合上、委員からの御発言とAppleの回答を合わせて、お一人当たり最長10分程度でお願いできればと思います。御発言が一巡した後、お時間があれば、追加の質問などをしていただければと思います。時間内に全ての御質問が終わらなかった場合は、検討会後に書面で提出いただき、Appleから書面で回答いただきます。

それでは、Apple様から御説明をお願いします。

○Apple ありがとうございます。まず、最初にお礼を申し上げたいと思います。検討会の皆様、このような機会を弊社に提供していただきまして、ありがとうございます。本日お話しできる機会に感謝しております。短いプレゼンテーションを準備してまいりました。事前に頂いておりました質問事項にお答えできる内容になっているプレゼンテーションになっていることを願っておりますが、もちろんプレゼンテーションの後、質疑応答でも回答させていただきたいと思います。では、早速プレゼンテーションを始めたいと思います。

まず、非常に重要だと思いますのは、Appleにとって常に日本は非常に重要な市場であるということを明確にすることだと思います。40年以上、Appleは日本の市場にコミットしてまいりました。日本の消費者の皆様は、世界の中でもApple製品を最もよく御利用いただいているユーザでいらっしゃると思っています。Appleは、日本に多額の投資を行ってきました。iPhoneについて考えてみても、日本なしでは製造できません。すなわち、その部品の多くは、日本のサプライヤーの皆様から供給を受けています。また、横浜テクノロジーセンターを含む、

大規模な拠点を設けており、また、日本において約100万人の雇用を支えています。

App Storeに目を向けましても、やはり日本のデベロッパの皆様から多大な支持を頂いています。特に、日本のデベロッパの数は100万を超え、Appleとこうした日本のデベロッパの皆様が生み出した収益は【非公開】米ドルを超えています。すなわち、Appleから日本のデベロッパの皆様へ、【非公開】米ドルの支払いをしたということでもあります。この額は、デベロッパの皆様のアプリによって生み出されたものです。毎週約【非公開】人もの皆様が、App Storeの日本のストアフロントを訪れたと認識しています。App Storeに関して、日本のストアフロントは、世界の中でも最も成功し、高い人気を誇っているストアフロントの一つです。したがって、長きにわたって、Appleは、Appleが日本に対して行ってきた取組と、デベロッパの皆様がAppleに対して行ってきた取組を非常に誇りに思っております。

Appleの製品とiOSについて少し申し上げます。iOSは御存じのように、iPhoneのオペレーションシステムでありまして、iPhoneは統合された製品です。iOSは特にiPhone向けに設計されているOSで、iPhoneでは、ハードウェアとiOSがシームレスに統合されており、円滑で応答性に優れ、安全なユーザ体験を実現しています。AppleはまたiOSが極めて高い安全性を確保できるよう設計しています。iOSの初期段階で決定した重要な設計方針の1つは、Appleの審査を受けていないサードパーティ製のソフトウェアを一切組み込まないということです。競合他社とは全く違うアプローチをAppleは取っており、このアプローチは、競合他社に対する差別化要因であると考えています。

Appleは、セキュリティ、プライバシー、ユーザ体験において競争しており、その競争力を守りたいと考えています。そして、Appleは、規制によって、その競争力が妨げられることがないことを願っています。なぜなら、現在、消費者の方には、AndroidとiPhoneという選択肢があるところ、その選択肢が消費者から奪われることを望んでいないからです。

それでは、iPhoneの設計の話に戻ります。最初にiPhoneが発表された2007年と、2024年現在を比べますと、OSに非常に多くの機能が追加されています。しかしながら基本的な設計は同じです。iPhoneは、ハードウェア、ソフトウェア、そしてサービスをシームレスなエコシステムに統合した製品であり、Appleは、円滑なパフォーマンス、つまりエネルギー効率やユーザフレンドリーなインターフェース等といったものを確保すべく、このような設計を行っています。それだけでなく、デバイスに保護機能を組み込む設計を行っています。

このような保護機能の中には、いわゆる「サイドローディング」の禁止が含まれています。

Appleが事前に承認、審査していないソフトウェアをユーザがダウンロードすることを禁止しています。ですから、P Cのモデルとは大きく異なっています。2007年にiPhoneを設計した時やそれ以前には、P CのモデルやP Cの市場に目を向けると、たくさんのマルウェア、ウイルスがございました。Appleはそれを避けたいと考えたのです。なぜなら、iPhoneのようなスマートフォンは、P Cとは全く違うものになるだろうと分かっていたからです。スマートフォンは、皆様が常に身に付け、常にインターネットに接続し、最も個人情報保存するものになると考えていました。すなわち、スマートフォンには、写真や連絡先情報、健康情報、財務情報などの個人情報が含まれるため、Appleは高度な安全性を確保したいと考えました。Appleが、iPhoneを当時のP Cの一般的な設計とは異なるものにしたいと考えた理由はこの点にあります。

2008年、多くのデベロッパの皆様から、「App Storeでネイティブアプリケーションも提供したい」という御要望をいただきました。先ほど御説明しました理由により、Appleはこれを当初のiPhoneでは許可していませんでした。Appleは、サードパーティ製のソフトウェアがデバイスにダウンロードされることを非常に懸念しておりました。しかし、Appleはデベロッパの皆様の声に耳を傾け、デベロッパの皆様が本当に消費者の方にネイティブアプリケーションをお届けしたいと考えていることを理解しました。

そこで、Appleは、2008年にApp Storeをオープンいたしました。しかし、注意深く考えることなくこれを行ったわけではありません。AppleがApp Storeを開発した当時、スティーブ・ジョブズが述べていたように、Appleは同時に二つのことを成し遂げなければなりませんでした。それは、先進的でオープンなプラットフォームをアプリのデベロッパの皆様を提供すること、それと同時に、iPhoneユーザをウイルスやマルウェア、プライバシー侵害などから保護する方法を見つけることです。これは簡単なことではありません。そこで、これを実現するために開発したのが、一元的なアプリ配布モデルと呼ばれるものです。そしてこれは、全てのアプリがApp Storeから配布されることを意味します。

では、これがなぜ重要なのでしょうか。それは、ユーザの皆様提供される前に、全てのアプリをAppleが審査する機会を確保することができるためです。また、App Storeを一部として含む多層構造のセキュリティアプローチを提供できるという点でも重要です。この多層構造のセキュリティアプローチにより、iPhoneは世界で最も安全なコンピューティングプラットフォームとなっています。では、この多層構造のセキュリティアプローチは具体的にどのような要素で構成されているのでしょうか。まず、オンデバイスの保護機能があります。

どのような意味かと申しますと、例えば、サンドボックスによって、アプリを他のアプリからのアクセスから保護しています。また、後ほど御説明しますが、アプリ審査というものもあります。これは、基本的には、App Storeにリリースされる前に、Appleが実際に全てのアプリを審査するというプロセスです。また、デベロッパの皆様にはプライバシーポリシーとガイドラインを遵守いただくようにする機能もあります。そして、ポスト・エンフォースメント・レビューと呼ばれるものも行っており、アプリが配信された後でも、不正を検知した場合には、そのアプリを実際にApp Storeから削除することができます。これらは全て、2008年に導入した一元的なアプリ配布モデルにより可能になりました。

このアプリ審査のプロセスと、それがAppleの一元的な配布モデルにおいて重要な役割を果たしている理由について、少しお話させていただきたいと思います。別の者からお話しします。

○Apple おはようございます。アプリ審査について若干の説明をいたします。これは数年にわたってApp Storeの一部として開発されてきたものであり、Appleはこの分野で15年以上の経験を有しております。何よりもまずAppleは、アプリレビューアーからなる審査チームに支えられています。レビュー担当者はアプリをデバイスにロードし、そのアプリがデバイス上で正常に作動すること、全てのAppleのガイドラインに準拠していること、そして重要なことに、アプリがその表示どおりのものであることを確認します。例えば、計算機として申請されたアプリが実際には銀行アプリや暗号通貨アプリであった場合、Appleのレビュー担当者がこれを検知することができ、当該アプリを却下します。

また、技術的ツールや自動化されたプロセスも導入しています。これは本質的に、アプリのバイナリ（App Storeからのダウンロード中にデバイスに送信されるソフトウェアパッケージ）をスキャンするものです。このプロセスは、違法なソフトウェア、SDK、マルウェア、ユーザのプライバシーを侵害するAPI等を検出することを目的としています。これは、技術的審査と人による審査を組み合わせたアプローチです。Appleは、App Storeの安全性を確立し、デベロッパの皆様のビジネス環境を整備してきた素晴らしい実績を持っています。App Storeでは、悪質なアプリを公開したり、ユーザを欺いたり、プライバシーやセキュリティを侵害したりするデベロッパは認められていません。

Appleのレビューチームは、三つのタイムゾーンにまたがって活動しており、アプリは24時間年中無休で審査されています。また、多言語に対応した専門スタッフを配置しています。

○Apple 私が更に取り上げたい重要な保護機能として、iPhoneプラットフォームの安全性確

保に非常に有益なWebKitがあります。WebKitとは、基本的にはブラウザエンジンです。これはApple独自のブラウザエンジンであるSafariを動作させるだけでなく、i O S上の全てのブラウザにも使用されています。これは、ユーザの皆様がインターネットを閲覧する際のプラットフォームのセキュリティとプライバシーを確保するためのAppleの取組の一例です。モバイルでのウェブ体験が重要であることは言うまでもありませんが、ウェブブラウジングによって、デバイスは検証されていない未知のインターネット上の場所にさらされ、そこが攻撃の重要な経路となる可能性があります。ユーザがiPhoneに保存する情報の機密性の高さを考慮すると、Appleが最高水準のセキュリティとプライバシーを提供することが不可欠です。

そのため、AppleがiPhoneをウェブ用に当初設計した際、Safariだけがウェブを使用できるようにしていました。しかしその後、App Storeを開設し、他のブラウザでもWebKitが使えるようにしました。ここで重要なのは、なぜブラウザのエンジンが重要なのかについて御理解いただくことです。単一の安全なエンジンを持つことの利点は、App Store上の100万を超えるアプリが、そのアプリ内でウェブコンテンツを表示しているという点で重要です。つまり、「アプリ」であっても本質的にはインターネットにアクセスしているため、マルウェア等の懸念やリスクが生じます。

このため、AppleのブラウザやWebKitで脆弱性が発見された場合、容易に修正パッチを適用できます。そして、そのパッチは即座に100万ものアプリ全てに適用されます。一方、100万ものアプリで複数のブラウザエンジンが使用されている場合、非常に困難になります。WebKitは、全てのブラウザとアプリに統一したルールを適用できる優れた例であり、iPhoneでのマルウェアやその他の悪意ある行為の拡散防止に非常に効果を発揮してきました。

また、iPhoneで採用している一元的なアプリ配布モデルにより、青少年を保護できる点も重要です。「Ask to Buy」（承認と購入のリクエスト）機能では、子供がアプリ内で何かを購入しようとする際に、保護者の事前承認が必要となります。さらに、様々なコンテンツ制限も設けています。「スクリーンタイム」機能では、子供がアクセスできるコンテンツを保護者が管理できます。これらは全て、全てのトランザクションがApp Storeを通じて行われる必要があるからこそ実現可能なことです。保護者は子供がどのアプリにアクセスしているかを確認することができます。

もう一つの有用なデータとして、この仕組みが実際に効果を上げていることをお示したいと思います。2020年から2023年にかけて、Appleはユーザの皆様に対する非常に多くの悪質な

行為を防止してきました。具体的には、Appleは、2023年だけで18億米ドル以上を含む、総額70億米ドル超の不正取引を阻止しました。また、1,400万件以上の盗難クレジットカードと330万件以上のアカウントによる取引をブロックしました。安全性違反により却下したアプリや、プライバシー違反を理由に却下した37万5,000件のアプリ等、これら全てAppleが実施できていることです。なぜなら、AppleはこれらのアプリがApp Storeに公開される前に審査したり、既にApp Storeに公開されていても問題を特定した時点で削除したりすることができるためです。

もう一点重要なデータとして、第三者機関の調査ではiPhoneが一番安全なデバイスであり、これは議論の余地がない事実です。2020年時点でiPhone上のマルウェアは2%未満でしたが、最近のNokiaによる第三者機関レポートでは、iOSとiPhoneは掲載されていません。これはマルウェアがほとんどゼロであり、統計上表示されない水準だからです。このように、Appleはユーザの皆様の保護において非常に成功していると考えています。

しかも、ユーザの皆様はiPhoneを楽しんでいます。日本では、Appleはほぼ常に日本の消費者の皆様にとって最も人気のあるブランドの一つとなっています。顧客満足度調査においても、AppleとiPhoneはほぼ常に最上位に位置しています。つまり、Appleは安全でセキュリティとプライバシーが保護されたデバイスを開発しているだけでなく、とりわけ日本のユーザの皆様を楽しんでいただけるデバイスを提供しており、第三者機関のデータによれば、ユーザの皆様は非常に満足しています。

では、Appleが懸念していることは何でしょうか。スマホ新法が、Appleがこれまで行ってきた一連の取組を継続する能力に影響を与える可能性があることを心配しております。Appleは、日本政府がこの法律を導入された背景を理解しております。また、競争に関する懸念も理解しておりますが、バランスが必要だと考えています。競争を確保しながらも、同時にユーザの皆様を保護する能力や、意図したとおりに機能する、ユーザフレンドリーで消費者に望まれる製品を設計する能力を維持することは可能です。そのため、基本的な考え方として、この法律にもその点が考慮された規定が含まれていると思いますが、Appleはプライバシー、セキュリティ、青少年保護のための機能によって、ユーザの皆様を保護できるべきであり、同時にApple製品を他社製品と差別化し続けることができるべきであると考えております。

御説明したとおり、Appleの製品及びビジネスモデルは、ハードウェアを販売するビジネスです。そして今日、Appleは、自社のテクノロジーをサードパーティのデベロッパの皆様を提供し、御利用いただけるようにするあらゆるインセンティブを有しております。なぜなら、デ

ベロッパの皆様がAppleのテクノロジーを活用して素晴らしいアプリを開発することができれば、ユーザの皆様にとってAppleの製品はより魅力的なものになるからです。Appleには、既にこれを行うあらゆるインセンティブがあります。なぜなら、アプリを含め、消費者に気に入っていただける製品を作ることができれば、消費者により多くのApple製品を購入していただけるからです。そこで、Appleは実際にSDKとAPIを開発しました。これまでに25万を超えるAPIを作成しており、その数は増え続けております。デベロッパの皆様がそれらを活用して素晴らしいアプリを作成できるよう、これらを御利用いただけるようにしてきました。また、Appleがこれまで御利用いただけるようにした全てのテクノロジーについても、Appleが作成したハードウェアとソフトウェアのいずれについても、デベロッパの皆様がそれらを活用していただきたいと考えております。そのため、Appleは、あらゆる種類のテクノロジーをデベロッパの皆様が御活用いただけるようにしてきました。Appleがハードウェアやソフトウェアを開発しても自社だけで独占しているのではないかという見方がありますが、これは事実ではありません。繰り返しになりますが、Appleには、このテクノロジーを広く御活用いただくためのあらゆるインセンティブがあります。

ただし、Appleは、テクノロジーの共有について基準を設け、安全性、プライバシー、そしてセキュリティ上のリスクの可能性がある場合は、特定のテクノロジーをサードパーティに公開しません。さて、スマホ新法には、アクセスに関する規定があります。Appleの懸念は、このアクセスに関する規定が極めて広範に解釈され適用された場合、iPhone及びAppleが安全安心で意図されたとおりに機能する製品を設計する能力に深刻な悪影響をもたらすおそれがあるという点です。

したがって、Appleとしての結論は、特にガイドラインや下位法令を検討する際には、スマホ新法の下でのリスクを緩和する様々な方法を徹底的に検討する必要があるということです。また、ユーザの皆様の安全性、プライバシー、セキュリティに対する強力な保護を確保すべきだと考えております。これらの保護措置の一部は既にスマホ新法にもある程度織り込まれていると理解しておりますが、それらが十分に厳格であり、その厳格な要件が実際にガイドラインや規則において盛り込まれることを確認する必要があります。

また、Appleは、意図したとおりに機能するより優れた製品やサービスを提供することが許容されるべきだと考えています。Appleは製品を作り、その製品が意図したとおりに機能し、ユーザの皆様の御期待に応えることを望んでいます。Appleは、より質の低い製品につながる

と考えられる変更を強いられることがないようにしたいと考えています。

最後に、Appleは要件の緩和が指定事業者のイノベーション、競争、そして差別化された製品を提供するインセンティブを維持するものであるべきだと考えています。新しい機能を開発しても、そのテクノロジーを競合他社に明け渡さなければならないとなると、Appleにとって非常に困難です。Appleのイノベーションを生み出す能力を低下させてしまいます。また、先ほど申し上げたとおり、Appleは差別化された製品を作り続けたいと考えています。競合他社と異なるものを提供し続けたいと考えており、そのためにそれを続けられる能力が極めて重要であると考えております。以上が本日のプレゼンテーションです。御質問がありましたら喜んでお答えいたします。お時間を頂きありがとうございました。

○依田座長 どうもありがとうございました。

それでは、各委員から御質問を頂きます。1問ごとにAppleから御回答いただくやり方で進めます。質問と回答については、お一人10分程度を考えています。10分になったら私の方からリマインドいたします。時間も限られていますから、御質問並びに回答については、できるだけ簡潔にお願いいたします。

それでは、本日10人の委員がいます。まず、最初に山田委員からお願いします。

○山田委員 二つあるのですけれども、一つ目は、まず、この検討会の目的自体が新しい法律の下位法令とガイドラインを作成することになっているわけですが、どのようなガイドラインが望ましいのか。政府と企業側の両方にとってプラクティカルで意味のあるルールという意味で、予測可能性と、逆にフレキシブルさとのバランスについて伺えればと思います。

日本は欧州と違うラインを引くという理解ですが、逆に公取委がどこで線を引くのか、完全なブラックボックス、あるいはグレーだという状況にもかかわらず、突然調査だ、罰金だというのは、やはり問題があると思います。

他方で、全てを細かくガイドラインに書き尽くしてしまうと、企業側にとってもフレキシビリティが失われるという懸念もあると思います。

ですから、このバランスについてコメントを頂ければと思います。これが一つ目です。

○Apple 御質問の内容を念のため確認させていただきたいと思います。どのように審査を行うことができるか、そしてもし可能であるとすれば、日本においてどのように異なる方法で審査を行うのかという御質問でしょうか。

○山田委員 政府がどのくらい詳細に指定すべきかということです。フレキシビリティとど

のくらい詳細までガイドラインに記載すべきかということです。

○Apple 【回答非公開】

○依田座長 山田委員、どうぞ。二つ目の質問がありましたらお願いします。

○山田委員 二つ目の質問は、アプリストアのノートライゼーション、公証審査に関して、日本政府との関係について伺いたいと思っています。

先週も携帯が乗っ取られて、インターネットバンキングのアプリから預金全て消えたというニュースが出ていましたが、また、安全保障関係の法令などでも、やはり携帯電話というのは、本当に基幹インフラの最も重要なものの一つだと言えます。

結局、今、戦後80年たって、私自身も含めて、一般国民が非常に平和慣れしていて、危機感を実感できていないかもしれないのですけれども、私自身も日常業務の中で日本のセキュリティというか、究極的には安全保障に関わるような、ある意味危ない試みの片りんに出くわすことが、実は確実に増えてきていると感じています。

ひょっとしたら、この危機感を持つべき必要性というのが、欧州の方が日本よりむしろ低いのかもしれないなというのは感じています。

今回の新法は、他社のアプリストアを受け入れる義務を運用する際に、Appleがノートライゼーションをする、言い換えれば、Apple社が日本国民の安全を守るために、非常に大きな一翼を担うということになるわけですが、正直なところ、このノートライゼーションを行う能力、やはり技術的にも経験という意味でもスピード感という意味でも、仮に政府がやろうとしても、今の日本政府には、残念ながら全くないというのが現実だと思います。

他方で、日本政府としても、この携帯電話周りの安全保障という分野について、Appleに大きく依存せざるを得ないという状況が生じます。それをApple社が実施をするに際して、大きな役割を果たすために、AppleとしてAppleが望む日本政府との関係性、どういう情報がもらえた方がいいのか、何か双方向で風通しがいい方がいいのか、その日本政府との関係性についてコメントを頂ければと思います。

○依田座長 ありがとうございます。Apple様から回答をお願いいたします。

○Apple セキュリティの観点から、Appleのデバイスは消費者にとって安全であるという意味で、おっしゃるとおりだと思います。日本だけでなく、世界中の多くの政府機関が、より安全でより保護されていることを認識しているため、iPhoneを利用するよう指示しています。そして明らかに、国家安全保障は現在大きな課題です。サイドローディングやこの種のものは、ス

スマートフォンを脆弱にし、Appleが安全なデバイスを作ることを妨げます。スマホ新法においてオープンなサイドローディングを義務付けていない日本政府の判断を高く評価しておりますが、代替アプリストア、アクセスの提供、iOSアクセスの要件等のいくつかの要件が依然として懸念材料です。これらは、デバイス上の多くの保護機能を損なう可能性があります。したがって、Appleが日本政府に対して希望することは、そのような問題に関して適切な決定を下していただくことです。そのような問題に関して、App Storeの外部にあるサードパーティのアプリストアに関しても、iOSテクノロジーへのアクセスを提供しなければならない状況に関しても、非常に大きなリスクがある場合や、安全でセキュアかつプライバシーが保護されたデバイスを作ることを妨げる場合には、スマホ新法の下でも特定の機能は対応しないと判断できる柔軟性をAppleが持つことができるようにすることが重要です。日本政府がAppleに対して消費者保護を継続するための柔軟性を確保いただくことは、非常に重要であると考えます。

○依田座長 ありがとうございます。

それでは、2番目になります。梶田佳江委員から御質問をお願いいたします。

○梶田委員 おはようございます。私は東京都の公立小学校で校長をしている梶田といいます。現場にいるという観点から安定性、青少年の安全性、特に小学生の安全性に興味があります。

今お話を頂いたとおり、やはりApple社は非常に安全であるという認識をしています。教員の中で、昨日ちょっとインタビューをしてきたのですが、親がAppleを使い、子供たちにも使わせていて、安全だよということでした。

例えばということで聞いたのですが、先ほど御説明があったように、何かアプリを買おうとすると、親のところに本当に買っていいですかという通知が来るというので、なるほどと理解したのですが、インタビューをしたのは教員ですので、ペアレンタルコントロールにも非常に興味、関心が高い保護者です。

しかし、一方では子供たちの様子を見ますと、ただスマホを与えるだけという保護者もまだまだいて、危険を伴うことが多くあります。

そのような中でも、今のAppleの環境であれば、安全だなと思うのですが、このスマートフォン新法になって、少しAndroid寄りになったときに、一番子供の安全性で懸念することとは何かというのを一つ教えていただきたいと思います。

○依田座長 では、まずこの質問について御回答をお願いします。

○Apple 最も懸念しているのは、例えば個々のアプリを審査することが可能な現在の一元的

な配布モデルを維持できなくなることです。他のアプリストアで配布されるアプリについても、Appleが何らかの審査を行うことができる仕組みを確保することは非常に重要であると考えています。これはAppleが現在ヨーロッパで試みていることであり、いくつかのルールを導入しています。もっとも、それらのルールでは十分でない可能性があり、このため、そうした審査を継続するための柔軟性について申し上げます。また、アクセス提供に関しても、アクセスの提供の義務化を通じて、企業が青少年を含む顧客のデバイス上での行動を把握できるアクセスを得ることになれば、それは非常に憂慮すべきことです。したがって、このような種類のアクセス要求に対処できる柔軟性をAppleが持ち、青少年を含めて、誰であっても、監視を目的としてAppleの技術へのアクセスを求めていると考えられる場合には、明確にこれを拒否できるようにすることが非常に重要です。

○Apple 私からも少し補足いたします。直近の御質問とこの御質問の両方において、公証について御説明しましたが、公証は、2008年から導入しているAppleのプラットフォームのユーザ保護システム、とりわけApple製品を使用する青少年を保護するためのシステムの一要素に過ぎません。Appleは、OSに組み込まれたセキュリティ、プライバシー機能、ペアレンタルコントロールに依拠しています。また、デベロッパの皆様との契約上の合意にも依拠しています。公証とアプリ審査にも依拠しており、さらには、審査後にApp Store上に掲載されたアプリを継続的に監視する能力にも依拠しています。

先ほど冒頭で述べたように、Appleは現在でも審査後に悪質な、あるいは悪意のある方法で変更が加えられたアプリを発見しており、そのようなアプリが問題を引き起こした場合に追跡して削除するための広範なメカニズムを備えています。App Store以外での配布経路が存在する環境においても、Appleが適切な保護措置を維持することが許容される限り、公証は有効に機能します。先ほど言及したアクセス提供に関する問題や懸念事項はありますが、私たちはOSレベルでの保護を維持するよう努めています。しかし、App Store以外で配布されるアプリについては、審査後のアプリの問題をAppleが監視、検出する能力は失われてしまいます。これらのアプリは新たな配布者、運営者、その他のアプリストアを通じて配布され、アプリの責任はそれらの事業者が負うことになります。それらの事業者は、Appleが現在導入している「Ask to Buy」（承認と購入のリクエスト）のような仕組みを持っているかもしれませんが、持っていないかもしれません。これまでAppleが行ってきたようにペアレンタルコントロールを重視するかもしれませんが、しないかもしれません。Appleは、そのことによる影響を非常

に懸念しています。これらの問題を真剣に受け止める善意のある運営者は適切に対応するかもしれない。青少年向けに非常に高度なスクリーニングを行うアプリストアが登場する可能性もありますが、全てのアプリストアの運営者が誠実に対応するとは考えにくいでしょう。これらの運営者がAppleが長年にわたって行ってきた、そして今後も継続する予定の徹底的な問題検出の取組と同レベルで実施することも期待できません。

○Apple ありがとうございます。一点だけ付言しますと、公証は、Appleの標準的なアプリ審査プロセスの一部であり、全てのルールを含んでいるものではありません。ネットいじめを助長するようなアプリについては、App Storeでは、そのようなアプリは許可されませんが、青少年が代替アプリストアでそれらを入手できる可能性があります。

○依田座長 梶田委員、御質問があればどうぞ。

○梶田委員 丁寧に御説明いただきありがとうございました。

実は私は、日本IBMで15年間働いておりましたので、大企業にいと、必ず独禁法の話が出てくると思うのですが、今回のこの新法に当たって、Apple社が絶対ここは譲れないというところを一つ政府にアプローチするとしたら、どこでしょうか。

○Apple イノベーションを志向する企業として重要なのは、Appleが創造することを望むデバイス、つまり、消費者にとって使いやすく、プライバシーが守られ、安全でセキュアなデバイスを作り続けるための柔軟性が与えられることだと思います。なぜなら、そのようなモデルは世界中で、特に日本で非常に良く機能しているためです。御存知のとおり、Apple製品はユーザの皆様から多大な支持を受けており、Appleは自らが望む方法によりそのような取組を継続できることを望んでおります。

○依田座長 ありがとうございました。

それでは、続いて3番目になります。増田悦子委員、御発言をお願いいたします。

○増田委員 私は消費生活センターで勤務する団体の理事長をしております増田と申します。よろしくお願いいたします。

まず、アプリ審査、今、梶田先生がおっしゃられたのと近い話ですが、アプリ審査についてです。欧州において代替アプリストアで配信するアプリや、代替アプリストアそのものについて、公証審査を行っているかと理解いたしました。その場合、代替アプリストアの公証審査においては、Appleはアプリストアと同等レベルのセキュリティ対策を求めるのかという点と、それから、審査後のアプリのスクリーニングができないというお話でしたけれども、Google

Playのプロテクトのようなスキャンができないというようなことなのではないかということが、まず1点です。

○Apple 再度申し上げますが、公証のプロセスは、Appleの完全なアプリ審査に適用されるガイドラインの一部分に過ぎません。そのため、App Storeでは承認されないものの、代替アプリストアでは入手可能となるアプリが存在し得ます。アプリが代替アプリストアで公開されてデバイスに配信可能になると、Appleの役割は非常に限定的なものとなります。アプリが公証プロセスを通過した場合、Appleは、そのアプリストアによるアプリ配布を許可しなければなりません。Appleはそのプロセスをコントロールすることはできません。Appleは、契約上の取決めにおいて、承認後のプロセスを持つこと、顧客の皆様からの苦情に対応すること、返金等の顧客満足に関する問題を解決すること等、一定の行為を義務付けていますが、それをリアルタイムで監視する方法はなく、代替アプリストアにAppleのビジネス慣行を押し付けることもできません。

○依田座長 ありがとうございます。

増田委員、また質問がありましたらお願いします。

○増田委員 もう一点よろしいでしょうか。EUでDMAが実際に施行された3月以降、代替アプリストアやApple社の課金システム以外の決済手段の登場によって、リスクが現に生じているかどうか、それがどのくらいの割合かや、以前よりすごく増えているというようなことがあるのかを教えてください。

○Apple 3月にこれらの変更を実施しておりますが、まだプロセスは非常に初期段階にあります。御存知かもしれませんが、欧州委員会とは実装について複数回の協議を行ってきました。また、デベロッパの皆様向けに「オプショナリティ」と呼ばれるものも導入しています。つまり、デベロッパの皆様は、DMAの下で求められる新しいモデルを選択することができ、代替アプリストアに移行してサードパーティによる決済システムを利用することも可能です。あるいは、現在のモデル、つまりアプリ内課金（IAP）を利用してApp Storeに留まることもできます。時間の経過とともに状況は変化するかもしれませんが、このオプショナリティを撤廃する可能性もありますが、現時点では予測できません。

○Apple 先ほどの発言に全面的に同意します。付言しますと、私たちはあるアプリストアの運営者を欧州で承認しました。

別のアプリストア運営者も承認されましたが、そのアプリストアの対象ユーザ層については、

まだ正確に把握できていません。

○Apple 更に付言するとすれば、Appleは、不正行為、プライバシー、セキュリティ上の問題に対するリスク軽減策を、実際に導入しているということです。

もちろん、これらは他の地域で実施している対策よりもはるかに限定的ですが、公証のようなリスク軽減措置を導入しています。

これまで講じてきたリスク軽減措置は、現時点では役立っていると思います。私の懸念は、今後それらを実行できなくなる可能性があることです。

○依田座長 ありがとうございます。

それでは、続いて4番目、日高委員から御発言をお願いいたします。

○日高委員 私は日本のモバイルアプリ開発者の立場として参加しておりますので、その辺りが伺えればと思います。

サードパーティからのOSのインターオペラビリティに対するリクエストについて把握されている詳細があれば、お聞かせいただきたいと思っています。

大企業からの申請、リクエストが多いとお話を伺いましたけれども、施行以降、どれぐらいの事業者が興味を持ってアクセスしてきているのか、及びどの程度リジェクト、若しくはアクセプトしているのかというところ、また、その中で得た中小企業についての懸念の部分も何かありましたらお教えいただきたいと思います。

○Apple 承知しました。ポータルには多数のリクエストが寄せられましたが、正確な数字は今持ち合わせておりません。

その仕組みとしては、私たちはそれらのリクエストを受け取り、それらを検討します。承認された場合は、それらの開発・実装を行います。

これまでに承認したものとしていないものについては、現時点では詳細な数字を把握していません。しかし、繰り返しになりますが、このプロセスはまだ非常に初期段階です。また、何かを承認したとしても、その変更を開発・実装する必要がある、それには一定の時間がかかります。

○Apple 何点か追加させていただきます。

まず、いくつかのケース、実際には多くのケースにおいて、デベロッパの皆様提供済みの機能に対するリクエストを受けました。このようなリクエストは、デベロッパの皆様向けのドキュメントを更に改善する余地があるということであると受け止めており、私たちが常に真剣

に努力していることでもありますが、そのような場合には、それらのデベロッパの方々が意図としていることをどのようにすれば実現できるのかを明確に回答しています。

私たちがデベロッパの皆様簡単に提供できるものについては、既に25万以上のAPIの一部として提供済みであり、これらのAPIによってデベロッパの皆様が多岐にわたる機能を実装することが可能になっています。

私たちは、顧客の安全やデバイスの安全性を維持し続けるソリューションを構築するための良い方法がないか、多くの課題に取り組んでいます、解決するのは非常に難しい問題です。

○依田座長 日高委員、ほかに質問がありましたら、お願いします。

○日高委員 OSのインターオペラビリティについて、引き続き二つ目をお伺いできればと思います。

日本においても8月からデベロッパがNFCの非接触決済、いわゆるセキュアエレメントを使ったサービスを開発できるようにということで、新しくAPIを公開いただけるというアナウンスを見聞きしております。その際、利用に当たって関連する料金を支払う必要があるともアナウンスいただいていたかと思います。

NFC機能等のAPIの公開に関して、デベロッパが支払うべき料金について、どのような根拠を持ってお考えいただいているのか、また、OSのAPIをどのような根拠を持って開放する基準を定めているのか、お伺いできればと思います。

○Apple デベロッパの皆様が、NFCとセキュアエレメントにアクセスできる機能のリリースについてお話しいただいたかと思います。

まず、これを基本的にはAPIを利用できるようにすることだとお話しいただいたかと思いますが、実際はそうではありません。

私たちはデベロッパが利用可能なものを開発するに際して、文字どおり、iPhoneとiOSを再設計する必要がありました。これは、デベロッパの皆様からの要望によるものです。

このように、デベロッパの皆様がこの機能を利用できるようにするために行ったことはAPIの作成ではなく、私たちは多くの作業をする必要がありました。

これは、先ほど申し上げたポイントにつながると思います。繰り返しになりますが、私たちは、技術、とりわけデベロッパの皆様がすぐにアクセスしたいと望んでいる技術を利用可能にするあらゆるインセンティブを有しています。iPhoneのセキュアエレメントに保存されている種類の情報の機密性を考慮し、私たちは、安全で、プライベートで、セキュアに機能するもの

を作りたいと考えました。そのために、私たちは、この機能を今年リリースするまで、設計に何年も費やしてきました。

この技術への継続的な投資により、私たちは、セキュリティやパフォーマンスの観点からも改善を続けていきます。この機能へのアクセスについては、料金を設定させていただく場合がありますが、これは私たちが状況に応じて行っている施策の一つです。

しかし、これは、私たちがデベロッパの皆様に御利用いただけるようにしたものです。

○依田座長 ありがとうございます。

それでは、5番目になります。仲上委員、御意見、御質問がありましたらお願いいたします。

○仲上委員 本日は丁寧な御説明を頂きありがとうございます。私は日本スマートフォンセキュリティ協会の仲上と申します。

日本スマートフォンセキュリティ協会では日本のキャリア様ですとか、アプリケーションデベロッパの方、それからセキュリティベンダーが集まって、スマートフォンのセキュリティについて利用や技術的な観点から議論を行っております。

本日お話しいただきましたとおり、これまでiOSにおけるマルウェア排除の取組によって、多くの利用者が守られてきたという点については、我々も非常によく理解しているところでございます。

質問ですけれども、サードパーティアプリストアの今後行われるべき審査、公証がある際に、サードパーティアプリストアオペレーターがどのようなセキュリティ対策や審査プロセスが行われているかということについては、これは審査の対象になっておりますでしょうか、ということが質問の一つ目になります。

○Apple 御質問を確認させていただきます。代替アプリストアから提供されているアプリのセキュリティ対策に関して、Appleがレビューするかどうかという御質問だったと思います。その理解が正しければ、答えはイエスです。セキュリティも公証の範囲に含まれています。

これは私たちが望む水準ではなく、Appleの完全なアプリレビュープロセスと同等とは考えていませんが、セキュリティレビューは確かに公証の一部です。ガイドラインというのは、本来は全てが一連のレビュープロセスの一部として機能するものであると考えることができますが、公証プロセスによってレビュープロセスに制約が生じ、結果として、もはや適用できなくなったルールが存在します。

また、先ほど指摘させていただいた点ですが、アプリが代替アプリストアから配信されると、

Appleはそのアプリが何をしているかについての洞察の多くを失います。アプリがユーザやデベロッパの皆様、あるいはデバイスに危険をもたらす可能性のある活動を行っているかどうかを判断するために必要な情報や手がかりを失ってしまいます。

○仲上委員 公証プロセスについての理解が深まる回答を頂きありがとうございます。

聞きたかったところとしては、サードパーティアプリストアのオペレーターが、セキュリティ対策や審査を行う形になるかと思うのですが、そのプロセスの内容について、サードパーティアプリストアそのものの審査を行うのかというところをお聞きできればと思います。

○Apple いいえ、代替アプリストア自体のスクリーニングは行っていません。代替アプリストアに提出されるアプリはAppleの公証プロセスを経て、その後代替アプリストアでのリリースが承認されます。代替的アプリストアは契約上の要件があり、先ほど御説明をした一定の活動に従事する必要があります。彼らはセキュリティレビューを行うべきですが、実際にどの程度行われているのかは私たちには分かりません。ここで認識しておくべき重要な点は、AppleのApp Storeが15年以上運用されているということです。セキュリティ上の問題があるアプリを特定する経験において、世界中でApple以上の存在はいません。代替アプリストアは、これを一から始めることになります。彼らは私たちが持つ知見の蓄積を持ち合わせていません。このような知見を蓄積するには何年もかかり、この間ユーザの皆様はリスクにさらされることになります。

また、代替アプリストアがAppleと同じインセンティブを持っているかも不明確です。私たちのデバイスをセキュアでプライバシーが保護されたものとして皆様にお届けしています。これは顧客にとって素晴らしい価値提案であり、顧客がAppleに満足し、iPhoneを継続してお使いいただける理由だと考えています。

代替アプリストアはデバイスを販売せず、アプリレビュープロセスだけでなく、当社のソフトウェアやハードウェア、そしてその仕組みについての詳細な知識も持っていません。私たちは可能な限り最善のプロセスを導入するための対策を講じてきました。しかし、公証で認められているプロセスでは補えないリスクがあると考えています。

○仲上委員 御説明いただきありがとうございます。

もう一つだけ質問ですけれども、公証プロセスにおいてアプリケーションがリジェクトされた場合、これは開発者はその理由を明確に知ることはできますでしょうか。

○Apple はい、可能です。こうしたデベロッパの皆様は、App Storeに提出した場合と同様の

通知を受け取ります。AppleはApp Store Connectポータルを通じてデベロッパの皆様メッセージを送信します。アプリがガイドラインに準拠していないという理由で却下された場合、準拠していない具体的なガイドラインと却下に至った事実関係を明示します。

つまり、私たちは、アプリが却下された理由、それが機能に関するものなのか、技術的な問題なのか、あるいはアプリ自体に起因するものなのかという点について説明します。これによりデベロッパの皆様は問題を修正して再提出することができます。

私たちの経験では、審査チームに一度却下されたアプリの大多数は、問題を修正した上で再提出することができており、その後、デベロッパの希望に応じてApp Storeまたは代替アプリストアでリリースされています。また、デベロッパの皆様には質問がある場合はAppleに相談することもできます。通知されたメッセージに関して不明な点があれば、そのメッセージから直接レビュアーに返信して追加情報を求めることも可能です。

デベロッパの皆様は不服を申し立てることもできます。その場合、私たちがアプリを誤解しているか、または判断を誤ったと考える理由を説明することができます。それにより、私たちはその不服申立てを検討し、追加の判断を下すことができます。デベロッパの皆様がアプリを公開できるようにするための様々なリソースやコミュニケーションチャネルが用意されています。

私たちの最終的な関心は、お客様により多くの、より良いアプリを提供することにあります。この点はApp Storeでも代替アプリストアでも同じです。私たちは、デベロッパの皆様が自らの申請のどこに問題があったのか、どのように修正すれば次回の提出で承認されるかを容易に理解できるようにしたいと考えています。

○仲上委員 分かりました。ありがとうございます。

○依田座長 ありがとうございます。

ちょうど10人の委員のうち半分の5人の御質問が済みましたので、ここで一旦休憩を取りたいと思います。

(休 憩)

○依田座長 それでは、お時間になりましたので、検討会を再開いたします。

6 番目、滝澤委員から御発言をお願いいたします。

○滝澤委員 滝澤と申します。東京大学で競争法を専門に研究しております。

今日は、充実した御報告を頂きまして、ありがとうございました。

御報告を伺いまして、新法7条2号に関する御懸念が強いのではないかという印象を受けましたので、私からはこの点について質問をさせていただきます。

デベロッパ向けのAPI群が25万あると伺いまして、どのように数えて25万になるのかにも関心はありますが、iOSでは依然として、例えばショートメッセージ機能や、近距離の無線通信など、まだサードパーティに開放されていないOS機能がいろいろあると認識しています。

そこで、このようにサードパーティにいまだ開放されていないOS機能のうち、特に法的に懸念の強いものについて、それから最初の山田先生の質問への応答で、そもそもサードパーティにアクセスを認められない部分があるというお話もされていたと思いますけれども、具体的に技術的観点からこういうところは開放できないとか、こういう懸念があるのでこの機能は開放できないといった点を、具体的にもう少し教えていただければ有り難いと思います。よろしく願いいたします。

○Apple 明確にするために申し上げますと、いくつか具体例を御紹介することは可能です。完全なリストを御用意することはできません。御承知のとおり、ソフトウェアは非常に技術的な側面があるためです。しかし、プライバシーや安全上の理由によりAppleがサードパーティに提供していないテクノロジーについて、いくつか具体例を御説明できると思います。

○Apple まず、御質問にあった「Appleのユーザ情報へのサードパーティアクセス」という点と、それに関するAppleの懸念点について明確にさせていただきます。ユーザの皆様は当然、iPhoneを様々な目的で利用しており、最も機密性の高い健康情報、位置情報、パスワード、プライベートな写真、メッセージ等、多岐にわたる情報を扱っています。Appleはこれらを自社の情報だとは一切考えておらず、あくまでユーザ御自身の情報だと捉えています。iPhoneの最も重要な特徴の一つは、ユーザの皆様には帰属する情報はあくまでユーザのもとに留まり、その取扱いについてはユーザ御自身が完全に管理できること、そして多くの場合、Appleが当該情報に一切アクセスできないことを確保するためにAppleが構築してきたテクノロジーです。

現在の技術環境においては、OSがAppleによるユーザ情報の特定部分への閲覧しないことを徹底していますが、サードパーティにその情報を提供することになれば、同様の保証ができなくなります。プライベートなメッセージや全ての通知がサードパーティにアクセス可能になってしまうと、もはやユーザの皆様に対してメッセージのプライバシーや機密性が確実に保護されていると保証できなくなります。さらに、そのようなデータへのアクセスを求める企業は、私たちとは非常に異なる動機を持っており、その真の目的を明確に開示しない可能性が高いの

です。対照的に、Appleはユーザ情報の使用目的について常に明確かつ率直に説明しています。したがって、私たちは上記の問題について深く懸念しており、特に単純に開放できない機能と開放可能な機能を区別するという観点から検討しています。先ほど申し上げましたように、具体的なリストを挙げることはできますが、そのリストは、テクノロジー、ハードウェア、ソフトウェアの進化、そして時間の経過とともに変化していきます。ただ、大まかに申し上げますと、Appleが懸念している事項には、デバイスが適切に機能するために必要な特徴や機能が含まれます。具体的には、OSの安定性に影響を与えるものや、携帯電話ネットワーク、Wi-Fiネットワーク、Bluetooth、衛星接続等のネットワークアクセスに影響を与えるものです。これらの領域へのアクセスを開放することにより、公共の携帯電話ネットワークに重大な危険が及ぶ可能性があります。また、デバイスの性能に影響を与え得る領域へのアクセス提供についても懸念しています。この懸念から、私たちは長年にわたり、デバイスの性能に影響を与えることなくバックグラウンドで特定のタスクを実行するアプリケーションのサポートに多大な努力を重ねてきました。例えば、オーディオを再生するアプリやファイルをアップロードするアプリ等です。しかしながら、それらの機能に対して無制限かつ無制約のアクセスを提供しなければならないとすると、アプリが私たちの保護機能を回避してしまう可能性が非常に高くなります。過去にも多くの事例を見てきました。このようなアプリはユーザの皆様の端末速度を著しく低下させたり、使用中のソフトウェアを妨害したり、あるいはそのアクセスを悪用して位置情報を常時追跡する等、バックグラウンドでユーザ情報を監視したりする可能性があります。当然ながら、バッテリーの寿命についても懸念があります。ユーザの皆様は端末が一日中持つことを期待しています。Appleはそのような期待に応え、またサードパーティによる端末の悪用を防止するためのソフトウェア開発に膨大な労力を費やしてきました。そのため、私たちが機能を管理できなくなるような領域へのアクセスの開放には強い懸念を抱いています。製品の安全性、ユーザの安全性、規制遵守に関しても多くの懸念があります。青少年の安全保護についても議論してきました。OS機能へのアクセス要求により、Appleが現在システムに実装しているペアレンタルコントロールの仕組みや青少年の安全対策が回避されることが想定されます。これらは、Appleにとって非常に深刻な懸念事項です。また、緊急通報機能を妨げるような要求や、デバイスの発熱対策や電気系統の安全保護を妨害するような要求も想定されます。セキュリティやプライバシーの懸念事項は他にも多数あります。OSの中核に近い階層で実行できるソフトウェアは、例え安定性の問題を引き起こさない場合にも、通常は保護されているシス

テム内部の機密データである特権的情報にアクセスできることが多く、それが様々な目的に使用される可能性があります。

2008年のサードパーティアプリの導入以来、iPhoneが世界で最も安全なモバイルプラットフォームであり続けている理由の一つは、システム上の全てのコードに署名があり、デベロッパとの紐付けが可能で、コードの出所を正確に把握できる点です。コード署名メカニズムや実装を妨げるようなOS機能へのアクセス要求は深刻な懸念事項です。また、先ほどのNFCに関する御質問について、Appleのセキュア・エンクレープについて言及しましたが、OS機能へのアクセスの要求により、Appleが実装しているFace IDやTouch ID等のセキュリティ認証機能をはじめ、ユーザの機密情報を保護するために構築した機能が毀損されてしまうことも想定されます。プライバシーについても詳しく御説明できます。データアクセスに加え、ハードウェアへのアクセスも重要な懸念事項です。他のプラットフォームでも見られる問題ですが、ユーザが認識あるいは予期していない形でカメラ、マイク、位置情報を密かに利用しようとするアプリが存在します。すなわち、元のお話に戻りますが、Appleはこれらについてユーザを保護することが極めて重要だと考えています。結論として、アクセス開放に強い懸念を持つ領域の確定的なリストを提供することは極めて困難ですが、Appleが深く懸念している分野や、アクセス要求に対して適切な解決策を見いだせない可能性がある領域について御理解いただけたと思います。

○依田座長 それでは、7番目、伊永委員から御発言をお願いいたします。

○伊永委員 私も競争法を専門としている学者です。

日本のスマホ新法は、Appleの優れたエコシステムの良さを活かしながら、ユーザ選択をオープンな状態に戻すということを考えています。

クローズドな中央集権型のシステムをオープンな分散型、ディセントラライズドされた形に変えるということになりますので、規制を受ける事業者がプライバシーやマルウェア、それから違法行為などからユーザを守るためには、これまで以上の高い技術力というのが必要となってきます。

ユーザのオープンチョイスを確保するという基本的価値をApple社と我々とは共有していると考えておりますが、そのために御社の高い技術力で果敢に挑戦していただき、更なるブランドとしての地位を築いていただきたいと考えています。

私からの質問ですけれども、スマホ新法の7条2号では、OSオペレーターと同等の性能で

OSの各種機能にアクセスさせることを義務付けています。この義務について、先ほど様々な例を挙げていただきましたが、ウェアラブルデバイスに絞って御質問したいと思います。

ウェアラブルデバイスをBluetoothやペアリング機能でiPhoneに接続する場合、サードパーティ製品は、Apple製品よりも接続性能が劣る状態になっていると聞いています。

他社が同等の性能でiPhoneに接続できなければ、ユーザにとっては実質的な選択肢とすることができません。これでは、Apple製品が本来的に持っている、もともとの優れた性能や機能とは全く別の事情から、ユーザにApple製品の選択を強いているという側面を持つことになりまますので、Apple社としても本意でないのではないかと思います。

ネットワーキング、トラッキング、バッテリーといったような事情を挙げられましたが、このBluetoothやペアリングを通じたウェアラブルデバイスとの接続ということについて、なぜ接続性能に差を設ける必要があるのか。その理由を具体的に教えていただければと思います。

まずは、1問、お願いします。

○Apple ペアリングにつきましては、私たちが長期にわたって検討してきたことです。私たちは、自社製品でこの分野において成し遂げたイノベーションを大変誇りに思っております。そして、それらの改良を可能な方法でサードパーティにも徐々に提供できるよう継続的に取り組んできました。例えば、iOS 18では「Accessory Setup Kit」という新しいフレームワークを導入し、デベロッパの皆様にご利用いただいていることを大変嬉しく思っております。ここでの課題は、冒頭で申し上げたイノベーションの種類と差別化に関する点に遡ります。すなわち、AppleがAirPodsやApple Watchのようなアクセサリと、iPhone及びそのソフトウェアの両方を開発する場合は、アクセサリ側とiPhone側からなる通信における両側面のセキュリティプロトコルと、どのデータが共有されるかについて完全に管理することが可能になります。

Appleが両方のデバイスを開発することで、アクセサリが仕様どおりに正しく動作していることを確保できます。また、アクセサリがスマートフォンのBluetoothチップに不必要に頻繁にアクセスせず、端末のバッテリーを過度に消費しないよう管理することが可能です。さらに、ファームウェアアップデートが安全かつ確実な方法で配信される仕組みも構築することが可能になります。アクセサリメーカーの中には、この状況に変化を求めている企業があることは理解しております。それは私たちとしても気にかけております。OS設計における大きな課題の一つは、自社製品向けのソリューションを開発し、ソフトウェアとハードウェアの両方を自社で管理する場合、自社と自社のユースケースに特化したソリューションを構築できる

一方で、A P I を開発する際は、Appleが保有する25万のA P I 全てについて取り組んできたことですが、全てのユーザに対して実際に機能するものを構築する必要があるということです。

これは様々な異なるデバイス上で動作するものを開発することを意味します。また、Appleのアクセサリーと同じように動作しない可能性のあるデバイスでも機能するものを開発する必要があります。また、動作の悪いソフトウェアやバグ等、私たちが管理できない問題を抱えるデバイスでも作動するものを構築しなければなりません。アクセサリーのセットアップ等に関して、過去には興味深い課題がありました。セットアップ通知が悪用され、ユーザが実質的に端末を使用できなくなるような状況もありました。A P I を公開する際、そのような悪用が簡単でなくとも可能になることは大きな懸念事項です。

つまり、安全なペアリングやデバイスの通信機能を提供することは、単に私たちが持つインターフェースを取り出して文書化し、サードパーティに公開すれば全てが上手く機能するというものではありません。そのようなアプローチでは非常に不完全な結果になると考えます。ユーザのニーズを満たさず、ユーザの皆様を多くのリスクにさらすことになります。これらは複雑な問題ですので、私たちはこうした機能の向上に懸命に取り組んでいます。Appleのプラットフォーム上で優れたサードパーティ製アクセサリーを利用いただきたいと考えており、今後もこの体験を向上させるために可能な限りの努力を続けてまいります。

○Apple 補足しますと、先ほども申し上げましたとおり、私たちにはサードパーティのアクセサリーが私たちの製品で動くようにすることに大きなインセンティブがあります。そうでなければサードパーティ製品が使える他社製の携帯が購入されることになるためです。先ほどの御説明に関連して、Appleはあらゆるユーザとデバイスに対応するソリューションを考案する必要があります。私たちは、全てのアクセサリーメーカーと個別に協力して当該メーカーの製品体験を最適化するためのリソースや時間はありませんが、幅広い互換性を持つソリューションを生み出すために最善の努力を行っています。

○伊永委員 ありがとうございます。

Marketplace Kitのように、若しくはWebKitのように、新しいキット、A P I 接続用のキットを開発されることなどによって、高い技術力が求められるとは思いますが、より安全な形で外部接続ができるようにしていただければと思います。

それから、もう1点、【質問非公開】

○Apple 【回答非公開】

○依田座長 ありがとうございます。

それでは、8番目の委員、川濱先生から、御発言をお願いします。

○川濱委員 川濱と申します。私も先ほどの2人と同じく競争法の研究者でございます。

本日は貴重な御報告をありがとうございます。

既に御指摘があったとおり、日本のスマホ新法はDMAと異なって、消費者の選択肢や競争環境の整備とともに、プライバシーの保護及び青少年の保護、それからセキュリティとの間のバランスを取るということを念頭に置いていることはそのとおりでございます。

その上で、お聞きしたいがございます。

このバランスというものはすごく難しい問題でもあり、バランスを取る価値として何を入れるかということが課題となるわけですが、スマートフォン新法下でのリスクの緩和策というところについて、バランスの取り方に関する御指摘をしたいと思います。

ユーザの安全性、プライバシー、セキュリティの強力な保護の確保の部分というのは、新法に明示的に書かれているもので、我々にとっては非常に分かりやすいものです。もちろんどのように均衡を取るかに関しては争いがあるところではございますけれども、製品、サービスが本来の予想通りに動作できることの確保というのは、日本の新法では明示的には捉えておりません。

この問題というのは、通常はこのような意図しない形で動作することというのは、不正なアプリに起因するものであって、不正なアプリによるリスクとしてセキュリティの中に含めて捉えております。

しかし、ここでセキュリティの強力な保護以外に今おっしゃったような内容が入っているというのは、セキュリティとは異なった側面でそのような問題があるという御理解でしょうか。だとしたら、具体的にはどのようなシステムなのかということを教えていただければと思います。

○Apple ユーザプライバシーやユーザセキュリティ以外にも懸念事項がいくつかあると考えています。安全性も重要な点であり、更にデバイスが当初意図されたとおりに動作すべきであるという点も重要です。本日何度も述べてまいりましたが、場合によってはAppleが実装を余儀なくされる変更によって、実質的にデバイスが機能しなくなったり、動作が遅くなったり、バッテリーが急速に消耗したりする可能性があります。ユーザ体験やデバイスが意図したとおりに動作すること等、これらすべての要素について、Appleは法律による保護ないしは適用除

外を確保したいと考えています。つまり、「デバイスの性能を実質的に阻害し、機能に悪影響を与え、消費者体験を損なうような場合は、Appleはスマホ新法の特定条項に従う必要はない」という法律上の保護、すなわち適用除外が確保されることが必要なのです。

○川濱委員 今のお話ですけれども、スマホ新法で要求している内容で、要求内容に従うことで直ちに問題が起きる場合というのはどのような場合なのでしょう。またそれらの防止に関しては強固な拒絶以外で、例えばそのようなある種のアプリに関しては機能を低下させること、あるいは機能を低下させるということの警告などで対応できるということはないのでしょうか。

○Apple 代替手段を申し上げることは困難です。まず、Appleが問題としているのは、「アプリを禁止すること」ではありません。それが問題の本質ではないと考えています。問題は、例えば先ほど申し上げたように、ユーザ体験を損なう可能性のある方法でアクセスを提供することです。スマホ新法はサイバーセキュリティのための適用除外を認めています。また、プライバシーと青少年の保護についても適用除外を認めています。安全性については明示的に言及していません。Appleとしては、ユーザの安全を阻害したり危険にさらすような方法でアクセスを提供することがないようにしたいと考えています。

例えば、バッテリー温度を管理するデバイス機能へのアクセスが可能になると、iPhoneが爆発させられる可能性があります。Appleはそのような事態を望みません。しかし、安全性はスマホ新法に明記されていないため、法令そのものに明記する必要があるというのが私たちの見解です。なぜなら、ユーザへの警告だけでは不十分だからです。「このアプリはあなたの端末の温度を上昇させる可能性があります」と単に表示するだけでは効果がありません。ユーザは警告を理解せずにクリックするかもしれませんが、その結果デバイスが爆発する恐れがあります。したがって、Appleはこのような問題に対処する柔軟性が失われることを強く懸念しています。このような問題はケースバイケースで検討する必要がありますが、多くの場合、単にユーザ警告を表示するだけでは問題解決にはならないと考えています。

○川濱委員 今おっしゃったワーニングの問題というのは、基本的には我々はセキュリティの問題と考えており、スマホ新法の中の明示の項目の中に該当すると考えています。

それから、もう1点、別の観点ですけれども、DMAと日本法は違うとはいっても、もちろん共通の基盤があるわけですから、先ほど御指摘があったとおり、DMAの対応のために様々な努力をされていると思います。

その点で、デベロッパ向けのAPI群というのはこれはかなり努力されているし、これは恐

らくDMA施行後、新たにデベロッパ向けのA P I が開放されているかと想像しているのですが、仮にそのような形でE Uで新たに開放されたA P I というのは、日本で導入することは可能なのでしょうか。

○Apple Appleはi O S 18.2において、DMAに準拠し、O S 内にデフォルト設定を一元管理できる専用セクションを設置しました。このi O S 18.2はまだ正式リリースされていませんが、間もなくリリースされる予定であり、現在ベータテスト版として利用可能です。これらのデフォルト設定の多くはすでに利用可能または適用されています。例外となるのは、現在欧州でのみ利用可能な代替配信に関する設定と、特定のマーケットではまだ利用できないN F C アクセスに関する設定のみです。なお、N F C アクセス設定は日本では利用可能であり、今後対応するマーケットが拡大する可能性もあります。

一般的に、Appleがデベロッパの皆様に対して提供するA P I や新機能に関しては、新しいA P I や新機能を開発する際、それらを世界中でお使いいただけるようにするというのがAppleの基本方針です。現在Appleが提供しているA P I のリストを御覧いただければ分かるように、そのほぼすべて、99%もの割合のA P I が世界中のデベロッパの皆様提供されています。

○依田座長 ありがとうございます。

それでは、9番目の上沼委員、御質問をお願いいたします。

○上沼委員 弁護士の上沼と申します。ネットと青少年に関する活動を行っています。

その関係で、青少年に関する点を主に質問したいのですが、まず最初に簡単な確認です。公証で行っているものがセキュリティとプライバシーと安全性に関するものとなっていて、青少年と明確に書いてないと思うのですが、これは実際に今はされていないという理解でよろしいでしょうか。

○Apple おっしゃるとおりです。欧州委員会はAppleに対して特定の事項について審査を行うことを許可し、Appleはそれを公証に組み込みました。

○上沼委員 そうすると、サードパーティアプリストアのアプリのレーティングというのは、iPhoneのレーティングシステムとの関係でどのようになっていますか。

○Apple まず第一に、アプリがApp Storeでも提供されている場合には、代替アプリストアも同じレーティングを踏襲すべきだと考えます。デベロッパの皆様には当然、App Storeで提供するか、代替アプリストアで提供するか、あるいはその両方で提供するかという選択肢があり

ます。Appleとしては、両方において提供されるアプリに対して矛盾する対象年齢区分に関するレーティングが存在することは適切でないと考えます。もっとも、代替アプリストア上のアプリであっても、本来はAppleのレーティングの対象年齢区分に関する評価システムを使用して適切な年齢レーティングをユーザに表示することが望まれるものの、これはアプリストアが独自のレーティングを設けることを妨げるものではありません。

○Apple また、App Store で配信されておらず、レーティングを付与されないアプリであっても、（代替ストア経由で）配信されるものについても、公証の制約の中で、サポートを追加せざるを得ませんでした。Apple は、保護者が非表示とさせることができるペアレンタルコントロールを設けました。

○上沼委員 今、ペアレンタルコントロールのシステムの方では、サードパーティアプリのマーケットのアプリを許さないという設定ができるとおっしゃっていましたが、これはDMAの下でもそうして、今後日本でもそのような設定をされる予定だと理解していいでしょうか。

○Apple はい、保護者が子供のiPhoneに代替アプリストアをインストールできないよう設定することが可能です。保護者がこのような制御を行えることは非常に重要だと考えています。もっとも、これまでAppleはペアレンタルコントロールにおいて、AppStore特有の機能とプラットフォーム上でアプリを実行する機能とを区別する必要はありませんでした。DMA以前は、そのような区別が存在しなかったためです。

現在、プラットフォームレベルで適用される管理機能も一部あります。しかしながら、Appleができないこともあります。先ほど申し上げた「Ask To Buy」（承認と購入のリクエスト）機能はその一例です。「Ask To Buy」はApp Storeとそのコマーシステムに本質的に紐づいた優れた機能ですが、それ故に、ユーザが代替アプリストアからインストールするアプリに対しては、この機能を提供することができません。

○上沼委員 あと1点だけ。WebKitのお話をされていたと思いますが、例えばブラウザフィルタリングみたいなものが、WebKitを使うことでほかのブラウザでも提供されるというような性能が入っていたりしますでしょうか。

○Apple 代替ブラウザエンジンを使用して動作しているブラウザがフィルタリングの機能を使えるかという御質問でしたでしょうか。

○上沼委員 WebKitを使うと、例えば御社で提供している、御社で設定しているフィルタリン

グがほかのブラウザでも使えたりしますか、という質問です。

○Apple 残念ながら、Appleが現在提供可能なフィルタリングの機能について、それほど私は熟知しているわけではありませんので、後ほど改めて回答させていただく必要があるかもしれません。WebKitを使っているブラウザについては、現在、Safariの他は、i O SのすべてのブラウザがWebKitを使用しています。

○依田座長 ありがとうございます。

それでは、10番目の石井委員、お願いいたします。

○石井委員 中央大学の石井と申します。よろしくお願いいたします。

私からは総務省の研究会の報告書との関係で御意見をまず伺えればと思います。

先月末に、総務省においてスマートフォン・プライバシー・セキュリティ・イニシアティブという報告書の改訂版が取りまとめられたと承知しています。この総務省の取組というのは10年以上前から行われてきたものでして、具体的にはアプリ提供者に対して、透明性や利用者情報の適正な取得、そして、プライバシーバイデザインやセキュリティバイデザインなどの取組を求めており、アプリストア運営事業者がアプリ提供者において取り組むべき事項がきちんと実施されているか確認することが望ましいとされています。

今回のスマホ新法によって、そのような取組の確認が代替アプリストアによって行われるということになりますが、それに対する懸念があるのではないかと思います。

総務省の検討会の報告書における、これまでのプライバシーの取組には御社も深く関わっておられると思います。総務省の情報プライバシー法の取組が損なわれないようにする必要がありますので、今回のスマホ新法に対して、改めて御社として考えられているセキュリティやプライバシーの懸念についてお話しいただければと思います。

○Apple 本日は、プライバシーとセキュリティに関するAppleの懸念について多くの議論をさせていただきました。Appleとしては、総務省とも議論するだけでなく、スマホ新法の下でも継続してユーザの皆様を保護できるような働きかけを続ける必要があると考えております。なぜなら、デバイスをオープンにすることは、あらゆる種類のセキュリティ及びプライバシーに関する問題を引き起こすからです。サードパーティのアプリストアについてお話がありましたが、理解すべき重要な点は、サードパーティのアプリストアがAppleと同じユーザプライバシーの保護へのインセンティブを持っておらず、今後も持つことはないということです。サードパーティは当然ながら自社のアプリストアに関心を持っています。彼らの関心は自社の利益に

あります。Appleは、サードパーティのアプリストアが接続するデバイスを提供するという意味で、より広範な利害関係を有しています。Appleはデバイスを提供しており、そのデバイスをプライバシーや機密性が保護された安全な製品としてお客様にお届けしています。そのため、AppleはApp Storeを安全なものにしたいと考えていますが、サードパーティのアプリストアには同様の義務はなく、ユーザのプライバシーやセキュリティを保護するためにAppleと同じインセンティブを持っているわけではありません。

したがって、サードパーティのアプリストアに要件を課すことができないとしても、少なくとも（代替アプリストアを含む）アプリストアで入手可能なアプリについては、プライバシーの観点からAppleが審査を行うことが可能となるようにしたいと考えています。Appleは総務省の取組とユーザプライバシーに関する姿勢を高く評価しています。他方で、Appleとしては常に、政府の法令上の要求事項はあくまで最低ラインであるという立場をとってきました。Appleは常に、政府の最低限の法令上の要求を上回る対策を講じたいと考えています。これは、ユーザの皆様には最高のセキュリティやプライバシー保護を提供させていただくためです。Appleは、ユーザの皆様には自身のデータをコントロールいただけるようにしたいと考えており、単に法令を遵守するだけでなく、法令が要求する以上のことを実現したいと考えています。

○石井委員 ありがとうございます。ほかの観点からも御質問させていただければと思います。

スマホ新法の正当化事由のところ、既にOS、ハードウェアのインテグリティの保護の必要性については十分お話ししていただいたと思っておりますが、セキュリティ、プライバシー、青少年保護のほかに、正当化事由として含めるべきか。今、OSのインテグリティの観点から御質問をさせていただいておりますが、正当化事由に取り入れるべき観点が3つのもの以外にもあるのではないかと私は考えておりますので、正当化事由に含めるべき観点として、御主張されたいことがあればお聞きできればと思います。

○Apple 承知しました。本日は多くのことを議論してきましたが、スマホ新法にはプライバシー、セキュリティ、及び青少年保護に関する正当化事由が含まれていると理解しています。Appleの観点では、完全性（インテグリティ）の概念はデバイスが意図したとおりに動作しない問題をカバーしています。つまり、デバイスが単に遅くなるのではなく、機能が損なわれるという問題です。また、安全性についても申し上げました。ここで言う安全性とは、犯罪関連の安全性ではなく、デバイス自体の安全性、例えばデバイスが発火するようなことがないという意味での安全性です。したがって、これらの概念はすべて、指定事業者のためのその他の正

当化事由として含められるべきだと考えています。Appleというまでもなく、貴委員会と協力してこれらの概念の意義を明確にする取組を行ってきました。しかしながら、完全性や安全性等の追加すべき概念は単にセキュリティ、プライバシー、そしてAppleがこれまで実施してきた保護策だけにとどまらず、それらを超えたものを含む必要があります。

○石井委員 ありがとうございます。1点だけ、個別のソフトウェアとOSの関係についてお聞きしたいと思います。

一つ一つのソフトウェア、個別のソフトとして評価できるものと、OSに深く組み込まれているソフトウェアがあると思いますが、それらの切り分けについて、すなわち、個別のソフトだと言えるものとそうでないものの考え方についてお聞きできればと思います。個別ソフトの捉え方についての質問です。

○Apple 複雑な御質問ではありますが、非常に良い御質問です。OSとアプリケーションの区分においては、明確に分類できる両極端の事例と、判断が難しい中間的な事例が存在します。例えば、サードパーティアプリはOSの一部ではないことは明らかなです。これらは明確に独立したソフトウェアです。セカンドパーティアプリ、つまりAppleがApp Storeで提供し、ユーザの方が御自身の端末にダウンロードしてインストールするアプリもあります。これらもサードパーティアプリと同様の方法で動作・機能するアプリです。さらに、OSにプリインストールされているものもあります。現在、プリインストールされたものの大半は、ユーザが削除できます。これらはシステムから削除することができ、それらがなくてもシステムは想定されたとおりに動作し続けます。iPhoneから計算機アプリを削除しても、通常の電話機能には影響しません。

したがって、OSとともにインストールされ更新されとしても、あるアプリがこれはアプリであり、OSとは別個のものであると言う場合は比較的明確です。他方で、分類のもう一方の極端な例として、システムファームウェア等のシステムの最下層コンポーネントや、アプリの実行方法を管理するシステム部分は、明らかにアプリではなくOSの一部です。

OSのコンポーネントを検討し、iOSにおけるアプリの定義を考えると、iOSのアプリケーションは特定の方法でパッケージ化され、ユーザはホーム画面のアイコンをタップして操作します。ユーザはアプリスイッチャーでこれらを個別の項目として確認できます。ユーザは、ごく一部の例外、特に一部のプリインストールアプリを除いて、これらを削除でき、データも個別に保存されます。Appleの見解では、これらの定義に該当しないものはアプリではありません。

せん。

例えば、Siriはアプリではありません。Siriは個別のアイコンとして表示されず、ユーザがタップできるものでもありません。ユーザはその機能をオフにしたり、利用しないことを選択したりできますが、起動できるアイコンはありません。アプリスイッチャーにも表示されません。実際、システム内のどのアプリからでもSiriと対話することができます。同様の方法で機能する他のシステムコンポーネントも多数あります。そのため、Appleはこれらを技術的な差異の観点から考えています。残念ながら、時にはこのような定義や法的用語を文書化することは難しい場合もありますが、少なくともAppleの考え方の概要を御理解いただければ幸いです。

○依田座長 ありがとうございます。

10人の委員の御質問は全て終わりました。時間的には若干余裕がありますので、もしよろしかったらもう少しだけ質問をお願いします。

○滝澤委員 ありがとうございます。そうしましたら、1点質問させていただきたいのですが、Nokia社による脅威に関するインテリジェンス・レポートに関してお伺いしたいと思います。

ここで脅威というとき、脅威の中身として、何を意味しているのかというのをまず確認させてください。2020年版のレポートで見ますと、Androidの脅威がiPhoneよりもとても高いように見えるのですが、ここでいう脅威というのはウイルスだけを指すのでしょうか、それともほかのものも含むのでしょうか。

また、ここに表れた数字が世界全体の数字ということになると、そもそも端末数はAndroidの方がかなり多いと思いますので、その点を考慮した場合に数字をどのように理解すればよいのでしょうか。

それから、他社さんについて聞くことになるのですが、先ほどの御説明の中で、Appleはダークパターンとか詐欺的なものなどもチェックしているのだというお話がありましたが、それは例えばAndroid端末ではウイルスのスキャンだけ行っていてそうしたタイプの脅威についてはチェックしていないと御社は理解されているのかという、その辺りの脅威の定義やチェック体制の違いなどがございましたら、御説明いただければと思います。

○Apple 重要なのは、これは第三者機関による報告であるということです。手法やマルウェアインシデントの件数を御確認いただけるよう、Appleは、報告書全体へのアクセスを提供することが可能です。私の理解では、これはマルウェアに関するデータであり、詐欺行為やぎま

ん、その他の重大なセキュリティ脅威等は含まれていません。マルウェアはより広範な、又は他のタイプの脅威と関連している可能性もありますが、この統計はマルウェアに特化したものです。他の情報源を調査いただければ、更に多くの詐欺行為やウイルスが存在することが御理解いただけるかと思います。

iOSのアプリに関して、Appleはより厳格な要件を設定しています。これにより、アプリはルールに従い、また、同意等を取得する必要があります。そのため、Appleのプラットフォームではユーザの皆様から過剰な情報を収集することができません。写真や連絡先へのアクセスを希望する場合には、許可を得なければならないためです。

○依田座長 どうもありがとうございました。

恐らく、日本は世界の中で最もApple製品を信頼し、シェアも非常に高い国だと思います。

幾つか理由があります。一つは、スティーブ・ジョブズが日本の文化、特に禅の文化に深い関心と理解を持っており、マッキントッシュの開発初期段階からその文化を製品に取り入れてきたことです。その結果、日本のユーザにとってApple製品は、ユーザエクスペリエンスの面で非常に魅力的なものとなっています。

さらに、日本の消費者が好むApple製品のユーザエクスペリエンスの中には、プライバシー、セキュリティ、セーフティといった要素も含まれていると考えます。そのため、私どもとしてもAppleのエコシステムにおいて重視されているこれらの要素に大きな敬意を払っています。また、今後、世界、特にヨーロッパやアメリカで議論されているように、プライバシー、セキュリティ、セーフティと競争上のオープンアクセスのバランスを、日本としても最適化していくことを目指したいと考えています。そのため、政府とApple社との間で建設的な対話を引き続き行えることを期待しています。

また、幾つか具体的な点についてもお尋ねしたいと思います。先ほどの滝澤委員の質問にも関連しますが、Nokiaのレポートは、iOSに比べてAndroidの方がマルウェアの感染リスクが15倍から47倍高いと述べています。これに対し、他社からは、Appleがサードパーティによるマルウェアの感染リスクやアクセス状況の調査を認めていないため、この数字がAppleに有利に、他社には不利に出ているのではないかという指摘があります。

この点について、Appleとしてどのようにお考えでしょうか。また、サードパーティによるマルウェア感染リスクの調査を外部に認めていない理由についてもお聞かせいただければと思います。

○Apple アンチウイルスやパワースキャンといった分野における企業の従前の課題の一つは、サードパーティがOS上でそのような機能を実行するには、システム上で発生するあらゆる事象を実質的に把握できる極めて深いレベルのアクセス権が必要だということです。Appleがサードパーティにそのようなアクセスを認めないという事実は、iOSのセキュリティアーキテクチャ全体の根幹を成しています。

したがって、Appleがそういったアクセスを提供すべきだと示唆している企業は、実質的に、当該アクセスを提供する代わりにAppleが自身のシステムの安全性を低下させることを提案していると考えられます。同時に、Appleはその種のアクセスを提供せず、サードパーティアプリとそれらがシステム上で実行できることに非常に強固なセキュリティアーキテクチャを提供しているため、マルウェアがiOS上で実際に動作することは極めて困難です。そのため、これらの報告書を御覧いただくと、その多くでiOSにおけるマルウェアインシデントの件数がほとんどゼロに近いことがわかります。セキュリティ研究者やセキュリティアーキテクチャの専門家に聞いても、一様にiOSがこの種の脅威に対して非常に強力な保護機能を備えていると言うでしょう。

○依田座長 分かりました。

既に、他社、特にAndroidは、サードパーティのアプリストア、いわゆるサイドローディングを認めています。しかし、そのサードパーティアプリストアに対する審査については、他社はデベロッパプログラムポリシー（DPP）に基づく審査を行っておらず、Google Playプロテクト（GPP）による審査・チェックのみを実施している状況です。

これに対し、本日さまざまな説明を伺った限りでは、Appleとしては、サードパーティが提供するアプリストアについても、自社のデベロッパプログラムポリシーに基づく審査が必要であるとの考えであると理解しました。

私たちも、Appleのビジネスにおける差別化（ディファレンシエーション）は正当なものであり、必要であると認識しています。ただし、日本の消費者やエンドユーザに対して、なぜサードパーティアプリストアに対する事前審査やレビューが必要なのか、その理由を丁寧に説明していただくことが重要であると考えています。この点については、ぜひ一層の配慮をお願いしたいと思います。

また、課金システムに関しても、サードパーティが提供する場合やアプリストアを運営する場合、セーフティ（安全性）やプライバシー、セキュリティのチェックが引き続き必要となる

ことに伴い、Appleに一定のコストがかかり続ける点については理解しています。

しかしながら、これまでの垂直統合型ビジネスモデルとは異なり、Appleの審査に関連するコストや、サードパーティがアプリストアや課金システムを提供する際のコストが合算され、最終的にはエンドユーザがこれを負担する形になる可能性があります。この点について、Apple社としては、サードパーティに課すコミッションの合理的な根拠について、透明性を持って説明責任を果たしていただくことが望ましいと考えます。

これは異なる産業の例ですが、1982年にAT&Tが分割された際、長距離電話会社が市内電話会社にアクセスチャージを課された際にも、市内電話会社がその根拠を説明する責任を負ったことがあります。このケースは、競争上の課題として参考になるのではないのでしょうか。

以上を踏まえ、Apple社のビジネスモデルについては、差別化に基づく独自性が認められるべきであると思います。ただし、スマホ新法の施行においては、Apple社がサードパーティデベロッパやエンドユーザに対して説明責任を果たすことを強く期待しております。

私からの意見は以上です。何かコメントがございましたら、よろしくお願いいたします。

○Apple 御意見をいただき感謝いたします。おっしゃられたことの多くは私の観点からも理にかなっていると思います。特に、Apple、日本、そして私たちの利害が多く点で一致しているという御指摘は重要です。スマホ新法が、様々な認識されている競争上の課題に対応することを目的としていると理解しており、Appleはその取組の意義を認識しております。Appleは常に健全な競争を支持してきました。この種の取組や立法の必要性については異なる御意見をお持ちかもしれませんが、これは現実のものとして受け止めています。貴委員会がAppleと協力して取り組んでいただいていることを高く評価しております。また、貴委員会のこれまでの透明性のある対応にも感謝申し上げます。この法律自体は妥当なものであるように思われます。改めてその点に感謝し、そのプロセスが今後も続くことを期待しています。そのために本日参加をいたしました。Appleとしましては、皆様と緊密に協力していきたいと考えております。

また、Appleのテクノロジーに対する課金の正当性について説明する必要があるとの御意見をいただきました。確かに消費者やデベロッパの皆様に対し、Appleが何に対して課金しているのかをより良く理解いただけるようにすることが重要かもしれません。しかし、「Appleはプラットフォームを提供している」という基本的な根拠はあると考えています。Appleはデベロッパの皆様テクノロジーを提供しており、その一環として他の企業やアプリストアと同様に、その対価をいただく資格があります。

したがって、デベロッパの皆様が何に対して対価を支払っているのかを御理解いただけるよう、いかにその点をお伝えするかという論点かもしれません。それはAppleが取り組むことができることだろうと思います。また、Appleは、引き続きデベロッパの皆様のためにイノベーションを起こし新機能を開発し続けるインセンティブを維持したいと考えております。本日の議論でも、そうしたインセンティブを維持することの重要性を強調させていただきました。本日このような機会をいただいたことに改めて感謝申し上げるとともに、皆様、特に貴委員会の検討会構成員の皆様と今後も協力していきたいと考えております。ありがとうございました。

○依田座長 委員の皆様から追加の御質問がありましたら、一つか二つ、受けられる時間もございますが、どなたかございませんか。全体、最後を通じて。

また、委員の皆様でもう少しだけ細かなことを聞きたい場合がありますら、あるいはAppleの方からもう少し追加の御説明をしたい資料等がございましたら、書面で受け付けたいと思いますので、後ほどまた御提出して下さい。

いずれにしても、日本としては競争上のオープンアクセスとユーザのプライバシー、セキュリティ、セーフティはいずれも両方大事なものと考えておりまして、そのバランスに対して最も適切なベストバランスを追求していきたいと考えています。

また、それについては例えばGoogleにはGoogleのバランスがあるだろうし、AppleにはAppleのバランスがあるとは考えておりますので、それぞれに対して事業者様、プラットフォーマー様の丁寧な御説明、納得できる根拠というのを示していただくことが、一番重要かと考えております。

事務局の方から何か確認したいことがありますか。まだ時間が若干ありますので、どうぞ。

○稲葉室長 事務局としても特段、確認したい点等はございません。お時間が若干ありますので、せっかくの機会ですので、委員の皆様方からもし1問、2問あればと思いますが、いかがでしょうか。

○依田座長 そちらは大丈夫そうですね。丁寧に質問しまして、回答もいただきました。何かあれば書面でお願いします。

事務的な連絡をお願いします。

○稲葉室長 1点、事務連絡だけですが、次回の検討会は、12月16日月曜日に予定しております。詳細についてはまた追って委員の皆様方に御連絡を差し上げますので、よろしくお願いいたします。

以上になります。

○依田座長 それでは、本日長い時間になりましたが、Appleの皆様におかれましては、ヒアリングに対応していただきまして、どうもありがとうございました。

以上をもちまして、本日の検討会を終了いたします。