サイバーセキュリティ政策・法務センター

２０２５年６月１３日

電子提出による

特定スマートフォンソフトウェアのための競争促進法の従位立法とガイドライン（モバイルソフトウェア競争促進法：MSCA）に関するパブリックコメントを要請

サイバーセキュリティ政策と法律センター（以下、センターとする）は日本フェアトレード委員会（JFTC）による特定スマートフォンソフトウェアのための競争促進法の従属立法とガイドライン（モバイルソフトウェア競争促進法：MSCA）（以下、ガイドラインとする）に関するパブリックコメントを要請への返事として以下のコメントを提出する機会に感謝いたします。

センターは政府、民間産業、市民団体にセキュリティの脅威により良い管理をするために実践と方針を提供しつつ世界中でサイバーセキュリティを強化することにひたむきに取り組む独立機関です。

日本政府によるモバイルソフトウェア産業の競争志向は、サイバーセキュリティの脅威の状況が急速に悪化しているときに始まった。日本政府自身が全ての政策は新たな国家安全保障の現実を考慮するべきであることを認識した。「政府は経済安全保障、国家安全保障に関連した技術力の向上に寄与するその他の政策との連携を向上させる。」2022年の国家安全保障戦略（NSS)で述べている。

この徐々に進化する脅威の状況とNSSで概説されている後続の国家安全保障政策の重点を考慮すると、JFTCの下位の法令は、それら（JFTC）が支持しようとするセキュリティの状況自体を不注意に損なわないことが重要である。消費者データやデバイスのセキュリティは今やより広範な日本の国家セキュリティ状況から切り離すことはできない。我々が推奨することは３つのハイレベルなポイントに纏められている。

１．屈強なサイバーセキュリティの特例を維持する

センターでは、MSCA全てにおいて準拠しない条項に対し、「正当化しうる理由」として、JFTCがサイバーセキュリティの例外を認めることを強く支持しており、これらは広義で、指定プロバイダーが積極的にユーザーやモバイルエコシステム、国家のセキュリティ権益を保護すると解釈される。

１．指定プロバイダーがサードパーティのアプリやアプリストアを制限し審査することを可能にする

センターは、指定プロバイダーが消費者のデバイスやデータのセキュリティを保証しつつ、屈強なサイバーセキュリティが実行されているか点検し、代替アプリストアや安全性が保証されていないサードパーティのアプリケーションの使用を抑制、または制限する柔軟性を常に持ち続けるよう推奨している。

１．外部サイトへの移行リンクを適正に制限できるようにする
センターでは、日本の国家的キャンペーンやセキュリティ政策に伴って、フィッシングや個人情報の盗難、不正取引など、高まるリスクを緩和するため、外部リンクへの移行に指定プロバイダーが適正な制限を課すことができるよう保証するようにJFTCに要請している。

センターはモバイルデバイスやオペレーシングシステム、アプリケーションやさらには信頼できるユーザーが所有するもののセキュリティが革新的かつ健全なモバイルマーケットプレイスの重要な要素であると確信している。
ほとんどのモバイルデバイスに備わっているセキュリティ保護は、－過去10年間で対話形式で開発されてきたのだが－多層的、包括的で、従来のコンピューティングデバイスのセキュリティ保護と比較してより効果的である。

当社の*モバイルの未来：モバイルセキュリティとプライバシーにおける絶え間ない向上への道筋*の報告書の中で、常に改良を続けながら、いかに適切にセキュリティを維持できるかのモデルをどのようにモバイルデバイスセキュリティが提供しているのかを説明している。

とりわけ、当社の*信頼できるアプリストア：セキュリティの保護と統合*の報告書の中で、アプリをインストールする選択肢が増えるとユーザーは圧倒され、彼らが悪意の行為者に搾取される多数の手段の道を開くことになる。これが今度は、サードパーティのアプリストアが実装している、していないのもあるが、信頼、安全性、セキュリティプロセスについて、またそれらが効果的なのかなど混乱を生じさせることになるだろう。

この混乱がユーザーエクスペリエンスや市民の安全性や、特に情報技術の知識が乏しいユーザーに重大な影響を及ぼし、モバイルエコシステムのセキュリティと競争の両方を弱体化させている。

センターは、JFTCがこれらのガイドラインで、セキュリティ上の考慮事項として明らかに説明していることを評価している。ガイドラインでは暗にサードパーティアプリのリスクプロファイルが、指定プロバイダーが開発したアプリとは異なっていて、ユーザーが自分のデバイスやオペレーティングシステムを使用するとき、また製造メーカーのアプリやサードパーティのアプリをその機器で使用するとき、指定プロバイダーは高レベルのサイバーセキュリティから消費者の利益を保証する重要な役割を演じていることを認めている。
それでもやはり、サイバーセキュリティを動機とするMSCA（モバイルソフトウェア競争促進法）が十分広範に適用されずに、要件が免除されると指定プロバイダーにもユーザーのセキュ

リティや彼らの機器を保護するのを妨げることになりうる。MSCAの７条と８条の指導に関連する我々の懸念にフォーカスしたコメント。

６条－　不当な差別化或いは不公平な扱い

MSCAの6条では、指定プロバイダーがそれらサードパーティのアプリプロバイダーに指定プロバイダーの基礎となるオペレーションソフトウェアやアプリストアの使用を許可するかどうか、どういった状況で許可されるのかを評価する際に、サードパーティアプリプロバイダーに対して不公平または不当な差別的扱いをすることを禁止している。しかしながらJFTCのガイダンスによると指定プロバイダーはーサイバーセキュリティを保証するために必要であればサードパーティのソフトウェアにレビューをすることが可能であり、ーそれによってサードパーティが基礎的なオペレーションソフトウェアやアプリを使用することができなくなる可能性がある。

センターはこのサイバーセキュリティーの例外をJFTCに含んでいることを強く支持している。しかし、例外はその他の管轄、欧州連合のデジタル市場法など、同様な法律には存在していない。この例外は指定プロバイダーにとって、サードパーティのアプリに（例：インストール前と後のレビュー）ルーティンとして多層セキュリティレビューを行うことで自社の製品に高レベルのサイバーセキュリティを維持することができるので重要である。指定プロバイダーは本質的に自社内部サイバーセキュリティ対策を信頼しており、検証することなしにサードパーティプロバイダーサードを信頼することができないため、パーティに対するこれらのレビューは、必須である。

消費者は自分の機器の安全を守りたいと要求し、彼らの要求が幾分サードパーティのセキュリティに影響を及ぼすが、これだけでは全てのアプリケーションにしっかりしたサイバーセキュリティを保証することは不十分である。更には消費者は常にこれらを自身でできるだけの判断を持ち合わせておらず、一般的には自分達を保護してくれる管理とポリシーを指定プロバイダーに頼っている。

実際、悪意のある行為者の場合、彼らのセキュリティを取り巻く技術的要求は消費者が効果的に評価できるようなものではありません。これらの事実からサードパーティのアプリのサイバーセキュリティを検証するための特定レビューを許可しない場合、ユーザーに重大な危害を及ぼす可能性がある。例えばユーザーが代替アプリストアから、危殆化サードパーティアプリをダウンロードすることができると想像しましょう。もしこれが危殆化されたアプリなら、指定プロバイダーが認証したアプリとして同じコアオペレーティングシステムの機能に、自動的にアクセスができ、ユーザーの個人情報へのアクセスを獲得できる可能性があります。

平均的な日本人ユーザーにとって、これにはユーザーの財務情報が含まれるかもしれません（例：クレジットカードナンバー）マイナンバー、国民IDカードやその他個人情報です。

もしアプリがデバイスのサイバーセキュリティを審査する重要な役割を担っていたら、センターはJFTCにサードパーティのアプリを別様に扱うためには、明確にはっきりと、広義で「合理的根拠」解釈することを要請します。これにより指定プロバイダーは、ユーザーと彼らのデバイスを保護するためにすべて必要な対策を行い、それによって競合モバイルエコシステムの成長をサポートすることができるのである。

9条、1号：代替アプリケーションの提供の妨げを禁止する

MSCA7条1号は基礎オペレーションソフトウェアの指定プロバイダーが、自分達が提供する製品のみに「アプリストアを限定」すること、その他のビジネスが基礎オペレーションソフトウェア上で代替アプリストアを提供することに干渉することを禁止してはならない。

しかしながら、JFTCのガイダンスには、「サイバーセキュリティを保証するために、、、
もしこれらの目的が競争力のないその他の会社にとって達成困難な場合、【7条1項に基づく要件に】準拠していない（ある）‘正当な理由’になる可能性があり、ー活動を制限するかもしれない。

センターは、代替アプリストアに関する要件に準拠しないための＂正当な理由”として、サイバーセキュリティを保証すること＂をJFTCが含むことを強く支持している。
*信頼できるアプリストア：セキュリティ保護と統合*の報告書で述べているように、
代替アプリストアは、メジャーな指定プロバイダーほどまじめにリストを取り締まっていないことはよくあります。そしそれが主要なモバイルOSがサードパーティアプリストアを歴史的に＂デフォルト＂として許容していない理由のようです。

これによって代替アプリストアのユーザーは不必要なサイバーセキュリティリスクに晒されるかもしれません。例えば、多くの代替アプリストアではうわべは良性アプリ、または人気有料アプリの海賊版を装って、要配慮個人情報などを取得するなど、望まない、有害な行動を隠すトロイの木馬化されたアプリをリストに載せている。

代替アプリストアの中にはこれらの悪意のあるアプリをユーザーにインストールさせる目的のみのために存在しているものもあります。同様に多くの代替アプリストアで、悪いユーザー体験をするばかりでなく、最新のセキュリティ修正プログラムや脆弱性対策を欠くようなアプリの古いバージョンや海賊版をリストに載せています。これらの問題を悪化させるように、指定プロバイダーの基礎オペレーティングシステムは、信頼できないソースを元にするアプリの責任を取るように設計されていないでしょう。
JFTCの7条1号のガイドラインには、代替アプリストアに関して指定プロバイダーが取ることができない措置の仮説シナリオが幾つか示されています。

- **レビューなしの均一警告**

”指定プロバイダーは、いかなる代替アプリストアにもレビューや検査をすることなしに、代替アプリストアからダウロードやインストールをしようとするユーザーに対してサイバーセキュリティを保証し、ユーザー情報を保護する観点から、それらのストアは安全でではないことを示唆し、均一の警告メッセージをを発します。

- **インストールをやめるようユーザーに警告**

代替アプリストアのインストールと代替アプリストアと経由したインストールの間にユーザーにインストールをやめるように促す行為を行ったり、表示させたりする。例えば、インストールに関連する誇張されたリスク感を誘導する警告を表示する。、正当な理由なく必要なアクセス権の許可をリクエストするスクリーンを繰り返し表示する、またはユーザーにインストールを行う度に毎回設定を変更させたりなど。

センターはJFTCに、代替アプリストアに関して、ガイダンスからこれらの仮説を削除し＂サイバーセキュリティを保証する”ために必要なより広い視点での実践を採用するように奨励しています。センターは指定プロバイダーがアプリストアを不公平に不利な立場においやることがないようにするJFTCの意図を理解している一方で、私達はこれらの仮説が正確にそのリスクプロファイルを反映していないと思います。実際、全ての代替アプリストアに関連するリスクは動的であり、指定プロバイダーが直接実態を把握することができないかもしれない様々な要素によります。

これらにはサードパーティアプリストアの内部方針や、サードパーティアプリケーションストアのセキュリティ努力を支える財政能力、悪意の行為者が使用する進化する地政学的な緊張、戦術、技術、手順（TTP)などが含まれます。例えば、今日は安全にアプリをリストに載せている代替アプリストアが明日は管理をやめるかもしれません。これはつまり、指定プロバイダーが内在する不確実さを認識することが唯一正確にリスクを説明する方法です。その結果、保証する唯一の方法は、ユーザーは指定プロバイダーが均一の警告を発し、ユーザーに特定の環境でのインストールをやめるよう推奨するのを許可することです。

7条2号：スマートフォン操作に関する機能の使用を妨害の禁止

MSCA7条2号は、基礎オペレーティングソフトウェア指定プロバイダーが、＂その他ビジネスがOS機能【（例：APISその他ツール）】を個々のソフトウェアに同様のパフォーマンスを提供するために使用することを妨げることを禁止する。＂しかし、JFTCのガイドラインには”サイバーセキュリティに必要な規格に基づき、指定プロバイダーがレビューを行うまたは検査する可能性があり、もしビジネスがこれら規格を満たさない場合、、、それら特定のOS機能の使用を制限するかもしれない。＂と説明している。

センターはJFTCがこのサイバーセキュリティの例外を含めることを強く支持しているが、サードパーティが重要なOS機能へのアクセスすることの制限を明確に認めるより広範なアプローチを推奨するだろう。サイバーセキュリティという状況下で、ユーザー認証、アクセス管理、

メモリー保護、ファイル保護、暗号化など、重要なOS機能はデバイスを脅威から保護するのに重要な役割を担い、サードパーティからの使用や干渉から保護されます。しかしMSCAの元に、悪意の行為者を含む、いかなるサードパーティはOS機能や機密情報を保護する技術や機能にアクセスを要求することができるがそれらは広範な使用を意図されていない。

これは悪意の行為者があるOSの脆弱性を見つけ、ユーザーデータにアクセスし、またはその他アプリの機能に干渉するために重要な機能にアクセスすることができることを意味する。JFTCのガイドラインでは、指定プロバイダーに特定の要求を拒否できることで、これに責任を負わないように思われるが、これでは規模として十分ではないかもしれない。特に指定プロバイダーは詳細な規準に従って個々のリクエストをレビューしなければならない。

同様にサードパーティは、それらが設計された使用事例のために使用する意図だったり、意図されない目的のためだったり、悪意目的であったりすることに関わらず、OS機能へのアクセスを要求することができる。例えば、指定プロバイダーは以前、Covid-19を追跡するためにオペレーティングシステムに組み込まれている契約追跡機能性を使用し、接触通知を提供した。MSCAの元では、サードパーティはこの機能性を全く別の目的のためにアクセスを要求することができる（例：五感で捉えられる物理的な社会でのデートアプリや親密なやりとりの追跡）。

これはサイバーセキュリティだけでなく、プライバシーでもサードパーティがこれらの機能を悪用するだろうということを暗示している。その結果、センターはJFTCにデバイスの機能性を使用するリスクに関連して厳格に考慮するよう、ガイドラインに比例制限を設けるように要請した。

8条、2号：関連するウェブページ等から物やサービスの提供の妨害の禁止

MSAC、8条、2号は、指定プロバイダーは「個々のアプリプロバイダーがウェブページや指定プロバイダーのソフトトウェア以外で、その他個々のソフトウェア（以下、”ウェブページ等に関連する”とする）の操作中に、物やサービスについて価格やその他情報を提示することに条件を課したり、妨害したりすることを禁止している。それはまた、指定プロバイダーに個々のアプリプロバイダーが個々のソフトウェアの外部リンク（リンクアウト）のウェブページにユーザーをダイレクトする外部リンクを含むことを禁じることを禁止している。

センターはユーザーがリンクアウトすることで特にリスクが高まると信じており、その結果、リンクアウトへの妥当な制限を許可するという方法でこの要求を実行するようJFTCに要請している。指定プロバイダーにはウェブ上で行われた支払取引が見ることができず、アプリがユーザーが支払った製品や機能が本当に届けられたか確かめることができず、外部のウェブサイトでの取引に対して詐欺防止モニタリングができません。

このリスクは真実で重大です。2022年4月の報告によると、それは顧客を20億ドル以上の詐欺の疑いのある取引から保護し、詐欺の疑いのあるユーザーからの約1700万個のリスクのある脆弱アプリやアップデートを阻止しました。またリンクアウトは個人情報やデータ盗難、アカウントの乗っ取り、児童のポルノに晒し、マルウェアの拡散などののリスクを高めます。

日本政府自体はこれを認識しており、最近「知らないリンクを開かないで」というキャンペーンを行っています。センターは特にフィッシングは歴史的にもサイバー犯罪への主要な最初のアクセスベクトルだったことを考慮し、日本人ユーザーの興味を引きつつこの警告を支持しています。これらリスクを考慮し、知らないリンクを開かないという日本独自の公共周知キャンペーンをしたなら、フィッシング攻撃や関連するサイバー脅威のターゲットになる日本人ユーザの増加につながるアプリのリンクアウトを制限を要求することは明白である。

まとめ

センターは、モバイルエコシステムの競争促進とサイバーセキュリティの推奨との間でガイドラインがぶつかったMSCAとJFTCとのバランスを評価しています。しかしながら2022年の国家安全保証戦略で強調され、現在のますます高度化する脅威の環境により過小評価されたように消費者のデバイスとデータが日本の国家安全とが深く絡み合っていることを認識するのが重要です。

私達はJFTCが指定プロバイダーのために提供された免除の範囲が広範に保たれ、新たに出現するサイバーセキュリティのリスクに積極的に対処し、彼らの最も影響をうけやすいユーザーのセキュリティの保護を保証してくれるよう要望します。これらの免除がなければ、善意の政策が日本の広範なセキュリティに対する姿勢を不注意で弱め、消費者と国家の両方をこれらの出現する脅威により脆弱になってしまうでしょう。

私達はこれらの問題をあなたのチームと話し合う機会を歓迎し、重要な会話に参加したいと思ってくれることに感謝します。もし何でも質問があればお知らせください。

心より

ヘザー・ウェスト
HEWest@Venable.com

アダム・ドベル
ARDobell@Venable.com

ルークオグラディ
LJOGrady@Venable.com