公正取引委員会
Japan Fair Trade Commission

Draft Translation
For reference purposes only

Summary

Mobile Software Competition Act
Subordinate Legislations and Guidelines

May 2025
Office of The Counselor for Digital Affairs

The Importance of Promoting Competition for Specified Software

- With smartphones becoming the foundation of daily life and economic activity, it's crucial to ensure fair and open competition in the market for specified software (software particularly necessary for the use of smartphones), beginning with competition between third-party app providers.
- Fair competition allows new application stores to emerge and encourages the development of innovative software solutions that utilize advanced smartphone features. These innovations create diverse services for consumers, empowering smartphone users to make informed choices and enjoy a wider array of benefits.
- The seamless and appropriate application of this Act is essential to secure fairness and openness in these software markets. The Japan Fair Trade Commission (JFTC) will engage in ongoing dialogue with designated providers (companies designated to be subject to the Mobile Software Competition Act) to ensure their compliance, strictly addressing violations such as prohibited conducts, and promoting their compliance with necessary measures, making the regulations proportionate to the competition related problems at hand.

Regarding Future Guideline Revisions

- Rapid advances in technology and services mean new challenges in the realm of specified software for smartphones. Guidelines will be reviewed as necessary to address such challenges, reflecting changes in market conditions and business practices related to specified software.

Relationship Between This Act and the Antimonopoly Act

- Actions violating prohibited conducts under the Act are generally categorized as antitrust violations. Considering the intent behind the enactment of this Act, which is to swiftly eliminate practices restricting competition by making determinations of violations based on formal act requirements, cases (concerning designated providers and their conduct) that overlap between this Act and the Antimonopoly Act shall, as a general rule, prioritize the application of this Act.

  Restriction of technology due to the existence of intellectual property rights such as copyrights, patent rights, utility model rights, design rights, and trademark rights, shall be assessed in accordance with conventional practices under the Antimonopoly Act. If restriction of technology is recognized as an exercise of intellectual property rights, it will be determined that the conduct is not in violation of Articles 5 through 9 of this Act.

Article 5: Prohibited Conducts Related to Unjust Usage of Acquired Data ①

Basic Approach

- Article 5 of this Act prohibits designated providers designated for their basic operation software, application store, or browser from using data acquired through the utilization of such specified software to competitively benefit their own (or their subsidiaries') goods or services.
- The use of data collected by designated providers for their own goods or services may lead to competition issues by providing advantages in marketing, development, etc., compared to third-party app or website providers. The prohibition aims to promote competition among individual software.

Approach to the Scope of Covered Data

- It is challenging to comprehensively confirm what kind of data designated providers of basic operation software, application stores, or browsers acquire. Additionally, the technological advancements and market developments surrounding specified software for smartphones are significant.
- Thus, the types of data subject to Article 5 are comprehensively and abstractly defined in the Enforcement Rules established by the JFTC. Guidelines enumerate specific examples of what data is primarily anticipated to be in scope, ensuring foreseeability for designated providers and allowing flexible enforcement in response to technological progress and market changes.
- Specifically, the data in scope include data which designated providers are able to acquire regarding: smartphone users, individual software or website usage, operational status, and contents or specifications.

Enforcement Rules (relevant JFTC Rules)

The data prescribed in the Rules under each Item of Article 5 of the Act includes the following types of data (including processed data or aggregated generated data) concerning individual software or web pages displayed by third parties:

① Data concerning smartphone users utilizing individual software or viewing web pages (excluding those provided without the use of the software or viewing the webpage by the smartphone user).

② Data generated or provided while smartphone users are utilizing individual software or viewing web pages (excluding data considered as ① above).

③ Data related to the content and specifications of individual software or web pages.

Understanding the Concept of "Unjust Use of Acquired Data"

- "Competitive relationship" refers to goods or services of the same type from the perspective of smartphone users, including not only individual software or websites but also goods or services offered in practical conjunction with individual software.
- "Competitive relationship" also encompasses hypothetical competitive relationships.
- Whether acquired data has been "unjustly used" in a competition context is determined holistically based on factors such as the similarity and relevance of competing goods or services, the timing of development or update of designated providers' first party goods and services, and the data required for such development or update. No particular restrictions are imposed regarding the manner of "usage." Instead, the analysis focuses on the relevance to the purpose ("providing competing goods or services") and the manner of data usage to determine whether acquired data is deemed as being "used for providing competing goods or services."

Desirable Practices by Designated Providers to Avoid Violations

Since it is difficult to externally verify whether data subject to the prohibitions in Article 5 has been used, it is important that designated providers establish effective internal systems to ensure compliance. Designated providers are encouraged to create transparent decision-making processes and data management frameworks to prevent the use of data for goods and services in competitive relationships. When such internal systems are developed, it is expected that, within a scope that does not hinder the business activities of designated providers and related businesses, disclosure under Article 10 of the Act will be required. This disclosure is anticipated to allow verification that the regulations are being complied with.

Basic Approach

- ◆ Article 6 of this Act prohibits designated providers designated for their basic operation software or application stores from engaging in unfair or unjustly discriminatory treatment towards third-party app providers regarding the conditions for using such basic operation software or application stores by third-party app providers and the execution of transactions based on those conditions.
- ◆ This provision regulates various forms of unfair treatment toward individual app providers. A typical example of when Article 6 is applicable is when a designated provider conducts reviews or examinations (their framework to confirm whether certain individual software meets the conditions for using the basic operation software or application store) concerning individual software.

Approach to Reviews and Examinations of Individual Software by Designated Providers

- ➢ The act of conducting reviews or examinations of individual software by designated providers does not, in itself, violate Article 6. However, if the criteria used for such reviews or the way they are implemented involve “unjust discrimination or otherwise unfair treatment,” it would constitute a violation of Article 6.
- ➢ Conducting reviews or examinations based on the following criteria generally does not violate Article 6. However, this principle does not apply if the implementation of such reviews is discriminatory without reasonable grounds, or if the reviews are conducted in ways inconsistent with the established criteria:
  - ◆ Ensuring cybersecurity etc., maintaining public order and morals (e.g., preventing defamatory or discriminatory content such as hate speech, content promoting violence, pornographic content, false or inaccurate information, etc.), preventing so-called 'dark patterns' (deceptive or manipulative user interfaces), etc.

Understanding the Concept of "Unjust Discriminatory Treatment"

- ➢ “Unjust discriminatory treatment” refers to cases where third-party app providers are treated differently without reasonable grounds, either compared to the designated provider itself (its own goods or services) or where certain third-party app providers are treated differently from others.
- ➢ Whether there is a reasonable grounds for the treatment is determined comprehensively by considering factors such as the purpose of the treatment, its impact on smartphone users or the designated provider’s specified software business, the availability and nature of alternative measures to achieve the same purpose, and the content and degree of disadvantages incurred by third-party app providers.
- ➢ If a designated provider treats others differently from itself and such treatment lacks necessity or reasonableness, it will generally constitute "unjust discriminatory treatment" under Article 6.

Hypothetical Scenarios of "Unjust Discriminatory Treatment"

⑴ Actions by Designated Providers Regarding Basic Operation Software

A) Establishing additional review criteria only for specific third-party app providers when conducting reviews or examinations of individual software that uses alternative application stores.

B) For individual software reviewed for alternative application stores, operating in a manner that disadvantages the third-party app provider via refusing to allow distribution through the alternative application store or the designated provider's basic operation software despite the absence of factors such as the provision of inappropriate content that fails to meet the established review criteria, or, operating in a manner that disadvantages the third-party app provider by prolonging the review process etc. albeit lack of causes beyond the designated provider's control (such as delays resulting from other third-party app providers).

C) Failing to allow third-party app providers to utilize OS functions with equivalent performance that the designated provider or its subsidiaries have, despite the absence of technical constraints, cybersecurity concerns, or other issues related to ensuring such functionalities.

⑵ Actions by Designated Providers Regarding Application Stores

A) Introducing additional review criteria for individual software that uses alternative application stores without particular circumstances justifying the need for such criteria when reviewing individual software for the designated provider's own application store.

B) Through the review process of the designated provider's application store, operating in a manner that disadvantages third-party app providers or disadvantages specific third-party app providers via refusing to allow distribution on the designated provider's application store despite the absence of factors such as the provision of inappropriate content that does not meet the established review criteria, or prolonging the review process etc. albeit lack of causes beyond the designated provider's control (such as delays resulting from other businesses).

C) Despite the absence of circumstances making implementation difficult, not allowing other third-party app providers to access application store functions (e.g., parental control features) or exclusively permitting access to such functions for specific third-party app providers.

Understanding the Concept of "Otherwise Unfair Treatment"

- "Otherwise unfair treatment" refers to actions that restrict the business activities of third-party app providers or cause them disadvantages without reasonable grounds.
- The method of determining whether reasonable grounds exist is consistent with the approach for assessing "unjust discriminatory treatment."
- When actions restrict the business activities of third-party app providers or cause them disadvantages, and the necessity or reasonableness of such treatment is absent, it will generally constitute "otherwise unfair treatment."

Hypothetical Scenarios of "Otherwise Unfair Treatment"

⑴ Actions by Designated Providers Regarding Basic Operation Software

A) When conducting reviews or examinations of individual software that uses alternative application stores, refusing to allow distribution through the alternative application store or withholding the review results for an extended period, without providing clear reasons, despite the absence of cybersecurity concerns or other legitimate needs.

B) When permitting third-party app providers to use OS functions, the designated provider imposes conditions that cause disadvantages exceeding the reasonable scope, as determined by considering the benefits obtained by the third-party app providers from such use. Alternatively, the designated provider unilaterally imposes conditions requiring the mandatory purchase or use of other goods or services provided by the designated provider.

⑵ Actions by Designated Providers Regarding Application Stores

A) Suspending the account of a third-party app provider or halting the distribution of their individual software through the designated provider's application store, despite the absence of circumstances such as violations of the application store's terms of use or factors beyond the designated provider's control (e.g., delays caused by other businesses).

B) When handling refund requests from users of individual software provided through the designated provider's application store, the designated provider, instead of the third-party app provider, determines whether to approve the refunds. Without implementing appropriate processes to verify the validity of each refund request (such as automated verification systems), the designated provider routinely accepts these requests. This creates a situation where third-party app providers are forced to handle fraudulent refund requests.

Basic Approach

- Article 7, Item 1 of this Act prohibits designated providers of basic operation software from limiting application stores provided through their basic operation software solely to those provided by the designated providers themselves or their subsidiaries (hereafter referred to as "designated providers, etc."). It also prohibits actions that interfere with other businesses providing alternative application stores through the basic operation software or smartphone users utilizing alternative application stores via the basic operation software.
- By prohibiting such actions that hinder the provision of alternative application stores by designated providers of basic operation software, this Item aims to promote new entries into the alternative application store market and foster competition in application stores.

Understanding the Concept of Actions that "Prevent" the Provision or Use of Alternative Application Stores

- Actions that "prevent" the provision or use of alternative application stores include those that create significant difficulties in continuing to provide alternative application stores or in initiating new ones, with a high probability of causing such difficulties.
- Such actions also include imposing unreasonable technical constraints, contractual terms, or excessive financial burdens on other businesses, which effectively create significant obstacles to the provision or use of alternative application stores, even while nominally permitting their existence.
- The degree of "likelihood of difficulty (to provide services)" caused by such actions is assessed comprehensively based on factors such as the nature of the designated provider's actions, the duration of those actions, the extent of impact on businesses providing alternative application stores, and the degree of impact on third-party app providers attempting to offer individual software through alternative application stores.

Understanding the Concept of Financial Burdens, Including Fees

- The level of financial burdens, such as fees, that are likely to prevent third-party app providers from using alternative application stores is evaluated based on specific circumstances.
- Considerations include, for example, the financial burdens applied by designated providers to third-party app providers for using their application stores, financial burdens applied by businesses for offering alternative application stores (taking into account whether efficient businesses providing alternative application stores can sustain their operations), and the financial burdens applied by designated providers when using alternative application stores. These factors are evaluated to ensure competitive conditions between designated providers' application stores and alternative application stores.

Hypothetical Scenarios of Actions that "Prevent" the Provision or Use of Alternative Application Stores

⑴ Actions limiting application stores to those provided by the designated provider, etc., through their basic operation software

A) Prohibiting smartphone users from utilizing alternative application stores through the licensing agreements or terms of use of the designated provider's basic operation software.

B) Establishing technical specifications within the designated provider's basic operation software that make it impossible for smartphone users to utilize alternative application stores. (Excludes specifications related to settings that allow smartphone users to choose to restrict the use of alternative application stores for a duration they prefer.)

⑵ Actions that, while permitting the provision or use of alternative application stores, substantially create high likelihoods of difficulty in their provision or use

A) When another business attempts to provide an alternative application store through the designated provider’s basic operation software and undergoes reviews or examinations, the designated provider, without reasonable grounds, imposes additional review requirements exclusively on a specific alternative application store that are not applied to other alternative application stores. Alternatively, even if the review criteria are identical, the designated provider conducts the review process in a way that disadvantages a specific alternative application store.

B) Requiring financial burdens such as usage fees, including by expanding the criteria for determining the basic operation software usage fees imposed on individual software, to such an extent that there is a high likelihood of making the provision of alternative application stores difficult for other businesses attempting to provide or planning to provide alternative application stores through the designated provider’s basic operation software.

C) Between the installation of the alternative application store and the installation of individual software via the alternative application store, engaging in actions or placing displays that induce users to abandon installation. For example, presenting warnings that convey an exaggerated sense of risk associated with the installation, repeatedly showing screens requesting permissions for necessary access rights without reasonable grounds, or requiring users to change settings each time an installation is performed.

Justifiable Reasons

Basic Approach

- For Article 7 and Article 8, Items 1 to 3 of this Act (excluding cases where the specified software under Article 8, Item 3 is a browser), actions deemed necessary for ensuring cybersecurity, protecting information related to smartphone users, safeguarding minors, or achieving other objectives stipulated by the Cabinet Order (collectively defined as "Ensuring Cybersecurity, etc.") may qualify as "justifiable reasons" for noncompliance if these objectives are difficult to achieve through other less competition-restricting actions.
- Even if a designated provider's action appears to fall under Article 7 or Article 8, Items 1 to 3 of this Act, it will not constitute a violation of Articles 7 and 8 as long as there is an accepted justifiable reason.

Objectives Stipulated by Cabinet Order

- Under the "Cabinet Order stipulated objectives" in the proviso of Article 7 of this Act, the Enforcement Order specifies the following objectives as justifiable reasons in addition to ensuring cybersecurity, etc. :

Enforcement Order (Relevant Cabinet Order)

① Prevention of gambling and other criminal activities conducted using smartphones.
② Prevention of significant delays, freezes, or other abnormal operations of smartphones.

Basic Approach Regarding Applicability of Justifiable Reasons

- To allow smartphone users to safely utilize diverse alternative application stores and individual software distributed through them, it is vital to determine whether the actions of designated providers genuinely qualify as justifiable reasons. This requires carefully balancing the two imperatives of ensuring cybersecurity, etc., and promoting competition.
- Particularly, for the "prevention of criminal activities using smartphones," it is appropriate to consider the severity of such activities and the magnitude of risks when determining the extent of measures. It is essential to assess whether the objective of preventing criminal activities through smartphones is difficult to achieve through actions less restrictive to competition than by those of the designated provider for each individual case.

Hypothetical Scenarios of Justifiable Reasons for Actions that "Hinder" the Provision or Use of Alternative Application Stores

⑴ Hypothetical Scenarios Where Justifiable Reasons are Accepted and Not Considered Violations

A) When a designated provider conducts reviews or examinations based on necessary standards for ensuring cybersecurity, etc., regarding alternative application stores used with the basic operation software under its designation, and finds that the alternative application store does not meet such standards, the designated provider may prohibit the provision of such alternative application store on its basic operation software.

B) From the perspective of protecting minors in relation to smartphone usage—such as preventing the use of age-restricted individual software, unintended excessive charges, or erroneous charges—designated providers may enable settings (commonly referred to as parental control functions) to restrict the use of alternative application stores by minor smartphone users based on parental consent.

⑵ Hypothetical Scenarios Where Justifiable Reasons are Not Accepted and Constitute Violations

A) When designated providers, without conducting any reviews or examinations for any alternative application store, uniformly issue warning messages to smartphone users attempting to download and install alternative application stores, suggesting that such stores are unsafe from the perspective of ensuring cybersecurity or protecting user information.

B) When designated providers, citing the necessity for ensuring cybersecurity or protecting user information, require smartphone users to make complex configuration modifications each time they attempt to download and install individual software through an already installed alternative application store.

Desirable Practices by Designated Providers to Avoid Violations

◆In the case where a designated provider imposes financial burdens such as fees on alternative application stores and individual software provided by such alternative application stores within the basic operation software, the designated provider notifies the amount of such financial burdens by means such as posting it on the designated provider’s website. Additionally, the designated provider explains to providers of alternative application stores or third-party app providers how the level of financial burden imposed by the designated operator is reasonable in relation to the benefits derived by the providers of alternative app stores or third-party app providers from the basic operation software.

Basic Approach

◆ Article 7, Item 2 of this Act prohibits designated providers of basic operation software (OS) from preventing other businesses from using OS functions for the provision of individual software with equivalent performance. Specifically, it prevents designated providers from restricting access to OS functions that they themselves use for the provision of individual software.

◆ The Item aims to promote competition regarding individual software by prohibiting actions that prevent other businesses from using OS functions with equivalent performance to provide individual software, as utilized by designated providers.

Understanding the Concept of "Functions Used by the Designated Provider to Provide Individual Software"

➢ In addition to the OS functions currently used by designated providers to provide individual software in the market, OS functions whose specifications have been concretized to a degree that allows other business operators to develop or improve individual software using them—such as beta versions made available for testing with public disclosure—shall also be applicable, as long as they are targeted for development or improvement by designated providers for the provision of individual software within Japan.

➢ OS functions may be utilized not only in the individual software itself provided by designated providers but also in goods or services that are functionally integrated with such individual software are also applicable. In the latter case, OS functions serve both the provision of the goods or services and the provision of the individual software itself.

(Example) A companion app for a connected device, such as a wearable smartwatch, may be functionally integrated. If the companion app allows users to configure the connected device via a smartphone, the pairing function between the smartphone and the connected device is not only part of the connected device's service, but also a function utilized for the companion app itself.

Understanding the Concept of "Other Business Operators Using the Equivalent Performance to Provide Individual Software"

➢ The intent is to ensure that OS functions are accessible to other businesses in a manner that does not significantly disadvantage their performance compared to designated providers' use of the same functions for individual software provision.

➢ Achieving "equivalent performance" does not necessarily require identical methods of access or use between designated providers and other businesses. It is sufficient if the OS functions enable other businesses to use them at a comparable level for individual software provision.

Understanding Actions That “Prevent" the Use of OS Functions with Equivalent Performance

- Actions that “prevent" the use of OS functions refer to conduct that creates a high likelihood of making it difficult for other businesses to utilize OS functions with equivalent performance for the provision of individual software.
- The degree of difficulty is assessed comprehensively based on factors such as: the nature of the designated provider’s actions, the duration of such actions, the extent of impact on other businesses providing individual software using OS functions, the degree of impact on smartphone users who use such individual software, etc.
- For example, if access to OS functions with equivalent performance is permitted without charge or restrictions, such actions would not be considered as "hindering" conduct.

Hypothetical Scenarios of Actions That “Prevent" the Use of OS Functions with Equivalent Performance

⑴ Actions That Prevent Other Businesses from Utilizing OS Functions with Equivalent Performance for Individual Software Provision

A) Preventing other businesses from using OS functions via technical means, such as refusing to provide necessary APIs or other tools, including denying permissions for API use.

B) Contractually prohibiting other businesses from using OS functions for the provision of individual software through terms of use or agreements.

⑵ Actions That Allow Other Businesses to Use OS Functions for Individual Software Provision But Create a High Likelihood of Practical Difficulty

A) Imposing financial burdens, such as excessively high usage fees for OS functions, creating a significant practical obstacle for other businesses to utilize OS functions with equivalent performance.

B) When other businesses are required to submit prior applications to use OS functions, and despite having submitted a valid application, the designated provider excessively delays completing the necessary measures to enable the use of OS functions with equivalent performance over an extended period.

Hypothetical Scenarios of Justifiable Reasons for Actions That "Prevent" the Use of OS Functions with Equivalent Performance

⑴ Hypothetical Scenarios Where Justifiable Reasons are Accepted and Not Considered Violations

A) When certain OS functions raise cybersecurity concerns, and it is difficult to resolve those concerns unless the ability to use such functions for individual software provision is limited to certain businesses. In such cases, the designated provider may conduct reviews or examinations based on necessary standards for cybersecurity, etc., and if a business fails to meet those standards, the designated provider may restrict use of those specific OS functions.

B) When the designated provider offers APIs or other tools necessary for utilizing specific OS functions with equivalent performance, but imposes restrictions in the terms of use to ensure compliance with existing laws—such as the Personal Information Protection Act— and prohibits the handling of smartphone user information in ways that violate the spirit of such legal provisions.

⑵ Hypothetical Scenarios Where Justifiable Reasons are Not Accepted and Constitute Violations

A) Conducting reviews or examinations based on necessary cybersecurity standards for multiple businesses, granting access to OS functions with equivalent performance to those who meet the criteria, but then denying access to specific businesses —without conducting a proper review, etc. — in the name of cybersecurity concerns.

B) Imposing a blanket prohibition on the use of specific OS functions by other businesses, without considering their initiatives or efforts, under the pretense of being necessary to achieve the purpose of protecting information related to smartphone users, even though it is not difficult to achieve the same purpose by limiting the eligible business operators to those who meet certain criteria, allowing them to use OS functions with equivalent performance to provide individual software.

Desirable Practices by Designated Providers to Avoid Violations

◆ During the design phase of basic operation software, designated providers ensure that OS functions are structured in a way that allows other businesses to use them with equivalent performance for the provision of individual software.

Basic Approach

◆Article 8, Item 1 of this Act prohibits designated providers of application stores from preventing individual app providers from using alternative payment management services.(i.e., payment management services other than those provided by the designated provider). It also forbids designated providers from obstructing individual app providers from enabling smartphone users to make payments using other methods without relying on payment management services.

◆By prohibiting actions that restrict the use of alternative payment management services, etc. (meaning either alternative payment management services or other payment methods that individual app providers can offer to smartphone users without utilizing payment management services), this Act aims to enhance competition in individual software by allowing app providers to offer diverse payment services.

Understanding Actions That “prevent" the Use of Alternative Payment Management Services, etc.

- Actions that "hinder" the use of alternative payment management services, etc., refer to conduct that creates a high likelihood of making it difficult for individual app providers to utilize such services while offering individual software through a designated provider’s application store.
- Such actions may include, among others: imposing unreasonable technical restrictions on individual app providers while allowing them to use alternative payment management services, placing excessive financial burdens on individual app providers for using alternative payment management services, etc., steering smartphone users away from utilizing alternative payment management services, etc.
- The degree of “difficulty” for use of alternative payment management services, etc. is assessed comprehensively based on factors such as: the nature of the designated provider’s actions, the duration of such actions, the impact on individual app providers attempting to provide individual software using alternative payment management services, etc., the extent of impact on smartphone users utilizing such individual software, etc.

Hypothetical Scenarios of Actions That “Prevent" the Use of Alternative Payment Management Services, etc.

⑴ Imposing Unreasonable Technical Restrictions on Individual App Providers Who Use or Seek to Use Alternative Payment Management Services, etc.

A designated provider manipulates the search algorithm within their application store to lower the search ranking of individual software that utilizes alternative payment management services or places such software in positions that make discovery by smartphone users more difficult, due to the individual software utilizing alternative payment management services, etc.

⑵ Imposing Excessive Financial Burdens on Individual App Providers Who Use or Seek to Use Alternative Payment Management Services, etc.

A designated provider, when individual app providers use alternative payment management services, demands fees or places financial burdens at a level that creates a high likelihood of making the use of such services practically difficult.

⑶ Steering Smartphone Users Away from Using Alternative Payment Management Services, etc.

A designated provider, as the provider of basic operation software and the application store, displays pop-ups promoting the convenience of its own payment management services whenever a smartphone user attempts to use alternative payment management services, thereby steering users toward its own payment management services.

Hypothetical Scenarios of Justifiable Reasons for Actions That “Prevent" the Use of Alternative Payment Management Services, etc.

⑴ Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

A designated provider, in order to prevent criminal activities using smartphones and to protect smartphone user information to the necessary extent, establishes requirements that limit the use of alternative payment management services to those that properly handle payment information (such as credit card details) and ensure appropriate refund and cancellation procedures.

⑵ Hypothetical Scenario Where Justifiable Reasons are Not Accepted and Constitute Violations

A designated provider, citing cybersecurity concerns such as an increased risk of credit card information leaks due to cyberattacks, and concerns over criminal activities using smartphones, imposes a blanket prohibition on individual app providers using alternative payment management services without conducting proper reviews or examinations.

Desirable Practices by Designated Providers to Avoid Violations

◆ When imposing fees or other financial burdens on individual app providers using alternative payment management services, designated providers disclose the amount by posting it on their website or through other notifications. Additionally, they explain to such providers that the level of imposed financial burden is reasonable in light of the benefits individual app providers gain from the application store.

Basic Approach

◆Article 8, Item 2 of this Act prohibits designated providers of application stores from imposing conditions that prevent individual app providers from displaying pricing or other information about goods or services offered through web pages or other individual software outside their own software (hereafter, "related web pages, etc.") during the operation of their individual software. It also forbids designated providers from prohibiting individual app providers from including external links ("link-outs") that direct users to web pages outside the individual software. Additionally, designated providers may not prevent smartphone users utilizing individual software from accessing goods or services provided through related web pages, etc.

◆By prohibiting actions that prevent transactions or payments conducted through related web pages, etc., this Act aims to enhance competition in individual software by allowing individual app providers to offer diverse services through such external platforms.

Hypothetical Scenarios Where Article 8, Item 2 May Be Applied

- Article 8, Item 2 would typically apply to cases where an individual app provider sells the same digital content both within their individual software and outside their software through related web pages, etc.
- Furthermore, the provision in the Act states: "(including cases specified by Cabinet Order as equivalent thereto)." The enforcement order specifies the following conditions:

Enforcement Order (relevant Cabinet Order)

Under Article 8, Item 2, the enforcement order defines applicable cases as instances where an individual app provider offers goods or services through related web pages, etc., that are utilized within the individual software but are not provided through the individual software itself. The Enforcement Order allows for the following scenarios to also be in scope of Article 8, Item 2:

- Typical scenarios include: ① "Reader apps" and similar services – where the individual software does not sell any digital content, but smartphone users purchase digital content via related web pages, etc., and then access it through the individual software; ② Non-identical goods or services – where the individual software sells digital content, but the individual app provider offers additional goods or services through related web pages, etc., that are not the same as the digital content sold within the software.

Display of External Promotional Information and Link-Outs

- The display of external promotional information includes not only the pricing of goods or services sold on related web pages, etc., but also announcements regarding their availability, sales promotions, special offers, and other marketing content related to such goods or services.
- Regarding the provision of link-out capabilities — where individual software allows users to access related web pages, etc. — the Enforcement Rules define the conditions as follows:

Enforcement Rules (relevant JFTC Rules)

The Rules under Article 8, Item 2 specify that link-out capabilities refer to the ability for users to obtain domain names or other location-related information of related web pages, etc., by selecting displayed text, graphics, or other perceptible information on a smartphone screen, allowing them to access those web pages, etc.

Understanding Actions That Prevent the Provision of Goods or Services Through Related Web Pages, etc.

- Actions that prevent the provision of goods or services through related web pages, etc., refer to conduct that creates a high likelihood of making it difficult for individual app providers to display external promotional information, offer link-out capabilities, or facilitate transactions through related web pages, etc., when providing individual software via a designated provider’s application store.
- Such actions include ① imposing unreasonable technical restrictions on individual app providers, ② placing excessive financial burdens on them, or ③ steering smartphone users away from obtaining goods or services through related web pages, etc. These actions constitute "preventing" the provision of goods or services through related web pages, etc., if they create a high likelihood of making such provision practically difficult.
- The impact of such actions on the likelihood of making provisions difficult is assessed comprehensively based on various factors, including the nature of the designated provider's conduct, the duration of the conduct, the degree to which the conduct affects individual app providers offering goods or services through related web pages, etc., and the extent of impact on smartphone users utilizing the individual software.

Hypothetical Scenarios of Actions That Prevent the Provision of Goods or Services Through Related Web Pages, etc.

⑴ Imposing Unreasonable Technical Restrictions on Individual App Providers Who Provide or Seek to Provide Goods or Services Through Related Web Pages, etc.

A designated provider refuses to offer APIs, templates, or other development tools necessary for individual app providers to display external promotional information—such as sales or special offer details—or to provide link-out capabilities within their individual software.

⑵ Imposing Excessive Financial Burdens on Individual App Providers Who Provide or Seek to Provide Goods or Services Through Related Web Pages, etc.

A designated provider, when individual app providers facilitate transactions through link-outs to related web pages, etc., demands fees or other financial burdens at a level that creates a high likelihood of making such transactions practically difficult.

Hypothetical Scenarios of Justifiable Reasons for Actions That Prevent the Provision of Goods or Services Through Related Web Pages, etc.

⑴ Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

A designated provider, as a provider of basic operation software and an application store, displays a pop-up warning smartphone users that clicking on a link-out may redirect them to external websites that mimic legitimate ones in an attempt to deceive users or cause misunderstandings. The pop-up also informs users that once redirected, the designated provider no longer controls the external website.

⑵ Hypothetical Scenario Where Justifiable Reasons Are Not Accepted and Constitute Violations

If there are no restrictions on the content displayed as external promotional information or the destination websites accessed through link-outs, there is a risk that individual app providers may display pricing information that differs from the actual prices on external websites—including sale prices, discount amounts, and discount rates—or may mislead smartphone users by directing them to payment screens for goods or services different from what they intended to purchase. Under the justification of preventing unintended purchases by smartphone users—that is, from the perspective of preventing criminal activities using smartphones—a designated provider cannot impose a blanket prohibition, without conducting proper reviews, on including price information in external promotional content within individual software or on setting payment screens as the destination for link-outs.

※ The desirable practices by designated providers to prevent violations are the same as those under Article 8, Item 1.

Basic Approach

◆ Article 8, Item 3 of this Act prohibits designated providers of application stores from imposing conditions that require individual app providers to use the browser engine offered by the designated provider as a component of their individual software. Additionally, it forbids designated providers from preventing individual app providers from using alternative browser engines (i.e., browser engines other than those provided by the designated provider) as a component of their individual software.

◆ By prohibiting actions that prevent the adoption of alternative browser engines as components of individual software, this Act aims to enhance competition in individual software by allowing app providers to offer diverse browser engine choices.

Understanding Actions That Prevent the Adoption of Alternative Browser Engines

- Actions that prevent the adoption of alternative browser engines refer to conduct that creates a high likelihood of making it difficult for individual app providers to incorporate such engines into their individual software when providing it via a designated provider's application store.
- Such actions may include: imposing unreasonable technical restrictions on individual app providers while allowing them to adopt alternative browser engines, placing excessive financial burdens on individual app providers for adopting alternative browser engines, and steering smartphone users away from using individual software that incorporates alternative browser engines.
- The degree of likelihood of causing difficulty is assessed comprehensively based on various factors, including: the nature of the designated provider's actions, the duration of such actions, the impact on individual app providers seeking to adopt alternative browser engines, and the extent of impact on smartphone users utilizing such individual software.

Hypothetical Scenarios of Actions That Prevent the Adoption of Alternative Browser Engines

⑴ Refusing to provide app development tools necessary for individual app providers to distribute their software through the designated provider's application store when they adopt an alternative browser engine.

⑵ Steering smartphone users away from using individual software that incorporates alternative browser engines within the designated provider's application store.

Hypothetical Scenarios of Justifiable Reasons for Actions That Prevent the Adoption of Alternative Browser Engines

⑴ Hypothetical Scenario Where Justifiable Reasons are Accepted and Not Considered Violations

In the situation of a very large number of individual software providers distributing non-browser software through the application store, a designated provider standardizes the browser engine used to display web pages through such software to its own browser engine by default. However, for individual app providers seeking to adopt alternative browser engines, the designated provider establishes certain cybersecurity-related requirements and conducts a prior review or examination (for example whether or not they address vulnerabilities at the same level as the designated provider, or to confirm whether or not parental controls function) to assess whether those requirements are met before deciding whether to allow the adoption of the alternative browser engine.

⑵ Hypothetical Scenario Where Justifiable Reasons Are Not Accepted and Constitute Violations

An individual app provider develops its own browser engine and implements vulnerability management measures equivalent to those of the designated provider. Despite there being no cybersecurity concerns beyond those already present in software that adopts the designated provider's browser engine, the designated provider refuses to allow the individual app provider to adopt its own browser engine in its software under the justification of ensuring cybersecurity and protecting information related to smartphone users.

Basic Approach

◆ Article 8, Item 4 of this Act prohibits designated providers of application stores from making the display of the user verification method they provide a condition for individual app providers to distribute their software through the application store.

◆ By preventing designated providers from imposing this requirement, the Act ensures that individual app providers can choose their preferred user verification methods, promoting fair and open competition.

Understanding How Article 8, Item 4 Applies

➢ Even if an application store's terms of use do not explicitly state that third-party app providers must display the designated provider's user verification method as a condition for distribution, certain actions can still qualify as imposing such a condition. For example, during the app review or examination process, if the designated provider refuses to approve individual software unless the app provider modifies it to display the designated provider's user verification method, this would effectively impose a requirement for distribution through the application store, violating Article 8, Item 4.

Article 9 (Prohibition of Self-Preferencing in Search Services) ①

Basic Approach

- ◆ Article 9 of this Act prohibits designated providers of search engines from giving preferential treatment to their own goods or services over competing goods or services without a legitimate reason when displaying search results that smartphone users request.
- ◆ If a designated provider prioritizes its own goods or services in search result rankings over those of competitors without legitimate reason, it disrupts fair competition for those goods or services. This provision aims to prevent such preferential treatment and promote equal competitive conditions for relevant goods and services.

Regarding "Displaying Information on Goods or Services Sought by Smartphone Users Through Search"

- ➢ This phrase refers to the act of presenting information that smartphone users are actively searching for, specifically on the screen showing the results of their search query.
- ➢ Search-linked advertising, or keyword-targeted advertising, does not typically fall under Article 9 as long as transparency and fairness in such transactions are adequately ensured under the Act on Improving Transparency and Fairness of Digital Platforms.
- ➢ However, if only information related to the designated provider's own goods or services is displayed under an “Ad” label, it may be subject to regulation under Article 9.

Understanding Preferential Treatment Over Competing Goods or Services

- ➢ If search results are displayed in what is regarded as a highly visible position, but the search engine’s algorithm and processing methods are fair and non-discriminatory, the display does not constitute preferential treatment.
- ➢ However, if a designated provider engages in arbitrary search algorithm adjustments or creates a separate section exclusively for displaying its own goods or services in a way that makes them regarded as more noticeable to smartphone users, this qualifies as preferential treatment.
  - ◆ If a designated provider modifies its search engine algorithm to favor its own goods or services by including specific parameters—such as criteria that apply only to the provider’s owned video service—this creates an advantage in search result rankings over competing goods or services and constitutes preferential treatment under Article 9.
  - ◆If a designated provider establishes a separate section for displaying its own goods or services and places them in a higher or more prominent position or format than fairly ranked general search results, or conversely, places competing goods or services lower or in a less visible position than fairly ranked general search results, this qualifies as preferential treatment under Article 9.

Article 9 (Prohibition of Self-Preferencing in Search Services) ②

Hypothetical Scenarios of Preferential Treatment

A Locking place the display of a download prompt for the designated provider's app store at the top of search results when a user enters the name of a specific individual software as a search query.

B Creating a separate section for displaying news, where only the designated provider's news service is shown, while ensuring that other web pages providing news content do not appear in that section.

Understanding the Concept of "Without Legitimate Reason"

- Whether preferential treatment has a legitimate reason is determined by examining: the purpose of the preferential treatment (the purpose of the preferential treatment cannot simply be something that benefits business operations. Rather, it must be justified by Article 9's intent, which is to maintain fair competition between the designated provider's goods or services and those of its competitors), the availability of alternative measures that achieve the same purpose without restricting competition to the same degree, and other relevant considerations regarding competitive fairness.
- Self-preferencing does not qualify as having a legitimate reason if: it does not clearly or meaningfully improve the quality of search results for smartphone users or if the rationale for the improvement of search results is abstract, it is done with the intent to exclude competing goods or services, it is unjustifiably places competing goods or services in an inferior position, or it is not necessary and reasonable for improving the quality of search results.

Hypothetical Scenario Where a Legitimate Reason Is Recognized

○ If a third-party website offering a certain good or service is found to have security vulnerabilities that expose users to malicious content through hacking, and the designated provider temporarily excludes that website from search results for cybersecurity purposes until the issue is resolved, leading to the designated provider's competing goods or services being relatively more visible in search rankings, this may qualify as a legitimate reason for self-preferential treatment.

Article 10 (Disclosure of Conditions for Acquiring Data) ①

Basic Approach

◆ Article 10 of this Act seeks to resolve the difficulty in externally verifying how designated providers use acquired data by requiring them to disclose the conditions under which they obtain or use data, as well as the conditions for data acquisition by businesses using specified software, leading to compliance with the prohibited conduct set forth in Article 5.

◆ Additionally, by enhancing transparency in transactions conducted through specified software and making it easier for businesses using specified software to acquire data, Article 10 is expected to contribute to the promotion of innovation.

Regarding Data Covered by Article 10

➢ JFTC Rules define the types of data subject to Article 10 as follows:

Enforcement Rules (relevant JFTC Rules)

◆ Data Subject to Disclosure to Businesses:

The data that must be disclosed to businesses using specified software, including the conditions under which designated providers can acquire or use such data, is defined in the Rules as the data specified in Article 5 of this Act.

◆ Data Subject to Disclosure to Users:

The data that must be disclosed to smartphone users regarding designated providers' acquisition and usage conditions includes data related to smartphone users themselves, as well as data generated or provided when users engage with individual software or browse web pages.

Article 10 (Disclosure of Conditions for Acquiring Data) ②

Regarding Disclosure Methods

- Enforcement Rules specify the methods of disclosure that designated providers must implement:

Enforcement Rules (relevant JFTC Rules)

① Information must be written in clear and simple language so that third-party app providers and website operators can easily understand them. Information intended for smartphone users must be presented clearly to ensure they can easily comprehend the conditions under which designated providers acquire and use data.

② The disclosed information must be readily and easily accessible to third-party app providers both before and during the use of the basic operation software or the application store provided by the designated provider by other third-party app providers, before and during the use of browsers by other website operators, and before and during the use of specified software by smartphone users.

③ If the disclosed information is not originally prepared in Japanese, a translated version must be provided. However, if providing the Japanese translation immediately is not possible, the designated provider must specify a deadline at the time of disclosure and ensure the translation is completed by that deadline.

- While businesses are responsible for determining their disclosure methods, it is essential that third-party app providers can easily understand and verify the conditions for data acquisition. Therefore, the disclosed information should be placed in an easily recognizable location on a website or in another clearly accessible format, ensuring businesses using specified software can reference it at all times.
- Disclosures intended for smartphone users should be presented in a manner that makes them particularly easy to understand.

Regarding Contents of What is Disclosed

- The guidelines provide examples of the conditions for data acquisition by designated providers, including the type of data acquired and the purpose of acquisition. Similarly, the guidelines illustrate the conditions for data usage, specifying the type of data used, its purpose, and, if a data management framework is in place, details of that framework. While Article 10 of this Act does not oblige the establishment of a data management framework, the guidelines indicate that maintaining such a framework is desirable, stating that if a framework is established, it is desirable for information to be disclosed to an extent that does not harm business activities of the designated provider or relevant businesses.
- The guidelines also provide examples of conditions for data acquisition by third-party app providers and website operators.
- Regarding smartphone users, designated providers must disclose both the conditions for data acquisition and the conditions for data usage as outlined above.

Article 11 (Measures Related to the Transfer of Acquired Data) ①

Basic Approach

◆ Article 11 of this Act obliges designated providers to implement necessary measures to ensure that smartphone users' data – acquired through specified software (basic operation software, application store, or browser; the same applies to other points below for Article 11) – can be seamlessly transferred to the user or a designated recipient upon the user's request.

◆ This provision aims to facilitate users switching to other business operators' services and promote competition among specified software.

Regarding Data Transfer Methods

➢ Enforcement Rules define the data transfer methods that designated providers must implement.

Enforcement Rules (relevant JFTC Rules)

① Ensure that smartphone users using specified software can request the transfer of data covered under the provision (hereinafter referred to as "transfer-eligible data") at any time.
② Enable smartphone users to transfer transfer-eligible data through simple operations
③ Ensure that the transfer-eligible data remains up to date and is formatted in a widely used format
④ Ensure that the duration required to transfer transfer-eligible data does not exceed a reasonable period
⑤ If a designated provider imposes fees for the transfer of transfer-eligible data, those fees must not exceed a reasonable range
⑥ Implement encryption and other necessary security measures for data transfers in accordance with the "Ensuring Cybersecurity, etc." provisions stipulated in the proviso of Article 7 of this Act.

Regarding What Kind of Data is “Transfer-Eligible”

➢ Enforcement Rules define the categories of data eligible for transfer under Article 11 as follows:

Enforcement Rules (relevant JFTC Rules)

◆ Data defined under Article 11, Item 1

Data related to phone calls and internet usage on smartphones equipped with basic operation software specified by the designated provider, data related to smartphone settings, other data that is useful for smartphone users when switching to basic operation software provided by other business operators.

◆ Data defined under Article 11, Item 2

Data related to individual software installed through the designated provider’s application store on the smartphone, data related to smartphone users using the designated provider’s application store, other data that is useful for smartphone users when switching to an application store provided by other business operators.

◆ Data defined under Article 11, Item 3

Data related to web browsing activity when using the designated provider’s browser, other data that is useful for smartphone users when switching to a browser provided by other business operators.

Specific Examples of Data

➢ Examples of data for Basic Operation Software

① Contacts ② call history ③ eSIM ④ display settings ⑤ home screen layout ⑥ Email accounts ⑦ messages ⑧ list of installed individual software ⑨ photos, videos, and albums ⑩ calendars ⑪ wallpaper ⑫ password related data

➢ Examples of data for Application Stores

① Individual software download history or data related to downloaded individual software ② account information (email address, payment methods, age verification data, etc.) ③ data input or registered by smartphone users

➢ Examples of data for Browsers

① Bookmarks ② browsing history ③ list of installed extensions ④ credit card information ⑤ password related data

Basic Approach

◆ Article 12, Item 1(a) of this Act obliges designated providers of basic operation software (OS) to implement necessary measures to ensure that when individual software provided by the designated provider (including its subsidiaries) are launched as default settings, smartphone users can easily change the default settings through simple operations.
◆ By making it easier for smartphone users to switch between individual software set in the OS's default settings, this provision aims to promote competition among individual software.

Measures Required for Enabling Smartphone Users to Change Default Settings Through Simple Operations

➢ Enforcement Rules specify the measures that designated providers must implement to ensure that smartphone users can easily change default settings:

Enforcement Rules (relevant JFTC Rules)

① A screen that allows smartphone users to change the default settings for individual software related to basic operation software must be displayed on the smartphone interface. This screen (hereinafter referred to as the "settings screen") should be centralized in a single location or otherwise arranged in a way that ensures smartphone users can easily find it.
② Provide explanations on the settings screen regarding the ability to change default settings within the OS
③ Ensure that smartphone users can change default settings with the minimum number of required operations.

➢ Specifics of ①～③ above are written in the Guidelines.

Regarding ①: If reaching the settings screen takes a significant amount of time, the measures do not meet the requirements set forth in this provision.
Regarding ②: Some smartphone users may have sufficient knowledge about default settings and OS functions, while others may not. Therefore, the explanations provided on the settings screen must be written in a way that ensures all users, regardless of their level of familiarity, can easily understand that they can take actions to change default settings on that screen.
Regarding ③: If changing default settings requires navigating through multiple screens or involves a large number of steps, the measures generally do not fulfill the requirements set forth in this provision.

Basic Approach

◆ Article 12, Item 1(b) of this Act obliges designated providers of basic operation software (OS) to implement measures that assist smartphone users in making selections, ensuring that when configuring default settings, multiple individual software options of the same type—as specified by the relevant Cabinet Order—are displayed as choices.

◆ For certain individual software where ensuring selection opportunities for smartphone users is particularly necessary, this provision aims to secure those selection opportunities and make it easier for users to switch between individual software, thereby promoting competition among them.

Categories of Individual Software Where Selection Is Particularly Necessary

➢ The Enforcement Order specifies the categories of individual software where selection opportunities (choice screens) are to be provided:

Enforcement Order (Relevant Cabinet Order)

① Browser
② Search applications (individual software used to enter search queries for services utilizing a specific search engine)

➢ Designated providers of basic operation software are required to display a choice screen screen for browsers and search applications.

"Measures that contribute to selection by the smartphone user" as defined in Enforcement Rules

➢ Enforcement Rules specify the measures that must be implemented to assist smartphone users in making selections:

Enforcement Rules (relevant JFTC Rules)

① Ensure that a choice screen is displayed on the smartphone interface that meets the following requirements: the screen must allow users to set default services and must present multiple service options of the same type, enabling users to select and configure default settings.

(a) Multiple service options must be displayed based on objective and reasonable criteria to ensure smartphone users have meaningful selection opportunities. However, only one service option per business operator may be displayed on the choice screen.

(b) The choice screen must display the name, logo, and description of each service option.

(c) The order in which options appear, as well as the way the choice screen is displayed, must not interfere with smartphone users' ability to make a selection.

② Ensure that, promptly after the smartphone's first activation by the user (or, in cases where the smartphone had already been activated as of the date on which the provider was designated, within one year from that designation date (Note 1)), the smartphone user selects a specific service from among the options displayed on the choice screen (Note 2).

(Note 1) If the smartphone had already been activated before the enforcement of this Act, the choice screen must be displayed within one year from the enforcement date.

(Note 2) However, if the smartphone user has already selected a specific service from among the options displayed on a choice screen on another smartphone, and the default settings for that selected service on the user's other smartphone are configured as the default settings on the user's current smartphone, the user does not need to go through the selection process again.

③ Display an information screen preceding the choice screen, containing the following details:

(a) The types of individual software.

(b) The meaning and significance of default settings.

(c) An explanation that users will be choosing individual software that will become the default setting on their smartphone.

(d) Information on how users can change the default settings for selected individual software after making their choice.

④ In addition to the provisions in ①～③, ensuring that nothing prevents smartphone users from configuring default settings through the choice screen.

Basic Approach

◆ Article 12, Item 1(c) obliges designated providers to implement necessary measures to obtain the smartphone user's consent when installing additional individual software provided by the designated provider onto the smartphone.

◆ By requiring user consent for such additional installations, this provision aims to promote competition between the designated provider's individual software and similar alternatives.

Measures Required to Obtain Smartphone User Consent, as Defined in the Enforcement Rules

➢ Enforcement Rules specify the following measures that must be implemented to obtain smartphone user consent:

Enforcement Rules (relevant JFTC Rules)

① Inform the smartphone user of the name and function overview of the individual software to be additionally installed.
② Confirm the smartphone user's consent regarding the additional installation of the individual software.

Guidelines for Implementation

➢ Regarding ①: The overview provided to the smartphone user must be detailed enough for the user to make an informed decision about whether or not to give consent.

➢ Regarding ②: Designated providers must confirm the user's consent before installing additional individual software. They must also determine the most appropriate timing and method for obtaining this confirmation.

Basic Approach

◆ Article 12, Item 1(d) obliges designated providers to implement the necessary measures to ensure that smartphone users can delete individual software provided by the designated provider from their smartphones through simple operations.

◆ By enabling smartphone users to delete individual software provided by the designated provider, this provision aims to promote competition between that software and other similar individual software.

Measures Necessary to Enable Smartphone Users to Delete Individual Software Through Simple Operations

➢ Enforcement Rules specify measures that must be implemented to facilitate the deletion of individual software through simple operations:

Enforcement Rules (relevant JFTC Rules)

① Ensure that the screen allowing deletion of individual software provided by the designated provider is displayed on the smartphone interface in a way that makes it easy for users to locate it.

② Ensure that users can complete the deletion of the individual software with the minimum necessary operations on the deletion screen.

Guidelines for Implementation

➢ Regarding ①: For example, when a smartphone user long-presses the icon of the individual software, a popup option for deletion could appear.

➢ Regarding ②: The deletion process should be designed so that users can complete it with the minimum necessary steps, including any necessary explanation of the effects of deletion.

Basic Approach

◆ Article 12, Item 2(a) obliges designated providers of browsers to implement necessary measures to ensure that when the browser provided by the designated provider (including its subsidiaries) launches, smartphone users can change the default browser settings through simple operations.

◆ By allowing seamless switching between default browser services, this provision aims to promote competition among browser services.

Measures Necessary to Enable Smartphone Users to Change Default Browser Settings Through Simple Operations

➢ Enforcement Rules specify the measures that designated providers must implement to ensure that smartphone users can easily change default browser settings:

Enforcement Rules (relevant JFTC Rules)

① Provide a centralized settings screen where smartphone users can change default browser settings for individual software related to the browser. This screen (hereinafter referred to as "settings screen") should be easily accessible and displayed in a way that ensures users can easily locate it.

② Include explanations on the settings screen regarding the ability to change default browser settings.

③ Ensure that smartphone users can change default browser settings with the minimum number of required operations.

➢ Specifics for ①～③ above as written in the Guidelines:

Regarding ①: If reaching the settings screen requires an excessive amount of time, the measures do not meet the requirements set forth in this provision.

Regarding ②: Some smartphone users have sufficient knowledge about default settings and browser functions, while others may not. Therefore, the explanations provided on the settings screen must be written in a way that ensures all users, regardless of their level of familiarity, can easily understand that they can take actions to change default settings on that screen.

Regarding ③: If changing default browser settings requires navigating through multiple screens or involves a large number of steps, the measures generally do not fulfill the requirements set forth in this provision.

Basic Approach

◆ Article 12, Item 2(b) obliges designated providers of browsers to ensure that smartphone users have meaningful selection opportunities regarding services related to default browser settings, as specified by Cabinet Order.

◆ For certain services where ensuring selection opportunities for smartphone users is particularly necessary, by ensuring that users can choose among multiple services of the same type and easily switch between them, this provision aims to promote competition among browser-related services.

Services Related to Default Browser Settings that are "Particularly Necessary to Ensure The Opportunity for Choices"

➢ According to the Cabinet Order, the following service requires a selection opportunity (choice screen):

Enforcement Order (Relevant Cabinet Order)

○ Search services using a search engine

➢ Hence, designated providers of browsers are obligated to display a choice screen for search services using a search engine, as part of the measures that assist smartphone users in making selections.

"Measures that contribute to selection by the smartphone user" as defined in Enforcement Rules

- Enforcement Rules specify the measures that must be implemented to assist smartphone users in making selections:

Enforcement Rules (relevant JFTC Rules)

① Ensure that a choice screen is displayed on the smartphone interface that meets the following requirements: the screen must allow users to set default services and must present multiple service options of the same type, enabling users to select and configure default settings.

(a) Multiple service options must be displayed based on objective and reasonable criteria to ensure smartphone users have meaningful selection opportunities. However, only one service option per business operator may be displayed on the choice screen.

(b) The choice screen must display the name, logo, and description of each service option.

(c) The order in which options appear, as well as the way the choice screen is displayed, must not interfere with smartphone users' ability to make a selection.

② Ensure that, promptly after the smartphone's first activation by the user (or, in cases where the smartphone had already been activated as of the date on which the provider was designated, within one year from that designation date (Note 1)), the smartphone user selects a specific service from among the options displayed on the choice screen referred to in the preceding clause (Note 2).

(Note 1) If the smartphone had already been activated before the enforcement of this Act, the choice screen must be displayed within one year from the enforcement date.

(Note 2) However, if the smartphone user has already selected a specific service from among the options displayed on a choice screen on another smartphone, and the default settings for that selected service on the user's other smartphone are configured as the default settings on the user's current smartphone, the user does not need to go through the selection process again.

③ Display an information screen preceding the choice screen, containing the following details:

(a) The types of services covered.

(b) The meaning and significance of default settings.

(c) An explanation that users will be choosing services that will become the default setting on their smartphone.

(d) Information on how users can change the default settings for selected services after making their choice.

④ In addition to the provisions in ①～③, ensuring that nothing prevents smartphone users from configuring default settings through the choice screen.

Basic Approach

◆ Article 13 obliges designated providers to take necessary measures to ensure that third-party app providers and website operators (hereafter referred to as “other businesses”) can respond seamlessly when changes are made. This applies to the specifications or conditions of use (hereafter referred to as "specifications, etc.") or to instances where the use of the designated provider’s specified software (referring to basic operation software, application stores, or browsers, collectively referred to hereafter as "specified software") is entirely or partially rejected during the provision of such specified software to other businesses.

◆ This provision aims to ensure that other businesses can seamlessly adapt to specification or usage changes, preventing unexpected disadvantages for them.

Measures and Methods to Be Taken by Designated Providers of Designated Software

➢ Enforcement Rules specify the measures that designated providers must implement, as follows:

Enforcement Rules (relevant JFTC Rules)

◆ Measures to be taken by Designated Providers of Basic Operation Software
① Disclosure of information regarding specifications and usage conditions.
② Providing advance notice and ensuring an appropriate adaptation period when changing specifications
③ Providing advance notice and ensuring an appropriate adaptation period when rejecting access entirely.
④ Providing advance notice when rejecting access partially.
⑤ Handling complaints and establishing necessary organizational structures and procedures related to Items ① to ④

◆ Measures to be taken by Designated Providers of Application Stores
All measures ① to ⑤ listed above

◆ Measures to be taken by Designated Providers of Browsers
Measures ① and ② (limited to specification settings and changes) and ⑤ (limited to certain aspects)

Necessary Measures as Defined in the Enforcement Rules

➢ Further details on the specific measures to be taken by designated providers are stipulated in the Enforcement Rules, as outlined below:

Enforcement Rules (relevant JFTC Rules)

① Disclosure of information regarding specifications and usage conditions
✓ Method of disclosure: Must be written using clear and easily understandable language.
✓ Required disclosure contents: Must include criteria for determining rejection of usage, among other necessary details.

② Providing advance notice and ensuring an appropriate period of time when changing specifications
✓ Method of disclosure: Must be written using clear and easily understandable language and include deadlines for disclosure.
✓ Exceptions for not ensuring a certain time period is not required

③ Providing advance notice and ensuring an appropriate period of time when rejecting access entirely.
✓ Method of disclosure: Must be written using clear and easily understandable language and include deadlines for disclosure.
✓ Exceptions for not ensuring a certain time period, and exceptions for not disclosing reasons for rejection.

④ Providing notice when rejecting access partially.
✓ Method of disclosure: Must be written using clear and easily understandable language and include deadlines for disclosure.
✓ Exceptions for not disclosing rejection reasons before rejection, and exceptions for not disclosing rejection reasons.

⑤ Handling complaints and establishing necessary organizational structures and procedures related to Items ① to ④
✓ Implementation method: Must include procedures and frameworks to ensure that changes to specifications or usage conditions are carried out fairly.

Article 14 (Compliance Reports)

Measures to Be Taken by Designated Providers as Defined in the Enforcement Rules

➢ Under Article 14 of this Act, the contents required in the compliance reports submitted by designated providers are defined in the Enforcement Rules, as follows:

Enforcement Rules (relevant JFTC Rules)

① Business Overview of the Designated Provider

✓ Terms and conditions related to the provision and usage of specified software, including any changes from the previously submitted report.

✓ Specifications related to specified software (excluding search engines), including any modifications since the last report.

② Measures Taken to Comply with Articles 5 Through 13 of This Act

✓ Details of the measures taken to comply with Articles 5 through 13, including explanations demonstrating compliance.

✓ Actions justified under provisos of Article 7 and Article 8, including explanations of the purpose behind such actions and why achieving the same purpose through alternative means was not feasible.

✓ Thought process and rationale in implementing the above measures.

✓ Overview of complaints or feedback from third-party app providers and smartphone users.

✓ Other necessary information for confirming compliance with the provisions of this Act.

③ Additional Information Necessary to Confirm Compliance Status with This Act outside of items ① and ②, Including:

✓ Main contents of discussions held with stakeholders regarding the implementation of compliance measures.

✓ Other reference materials related to compliance status.

(Note) Compliance reports must be submitted by the last day of the fiscal year or within two months from the date of designation under Article 3, Paragraph 1 of this Act. For designated providers already specified at the time of enforcement, reports must be submitted by the later of either two months from the designation date or the enforcement date of this Act.

Understanding Compliance Reports

➢ Designated providers must include specific explanations in compliance reports detailing: measures taken to prevent violations of prohibitions and comply with enforceable provisions, and other necessary information to confirm compliance, with supporting materials such as explanatory documents and evidence backing up the report's contents.

➢ In particular, regarding justifiable reasons from the perspective of ensuring cybersecurity, etc., when an action is suspected to violate the provisions of this Act, it is important to efficiently grasp the facts of the case and the designated provider’s claims. Therefore, the designated provider is required to provide a reasonable and specific explanation demonstrating that its actions qualify as a justifiable reason.

Basic Approach

- ◆ The enforcement of this Act requires both ensuring cybersecurity etc. and fostering a competitive environment, necessitating close cooperation between the Japan Fair Trade Commission (JFTC) and relevant ministries and agencies.
- ◆ To effectively implement this Act, it is critical for the JFTC to evaluate individual cases while considering expert perspectives from relevant ministries and agencies on cybersecurity and other related concerns.

Cooperation in Practice

➢ For the application of the proviso of Article 7 or Article 8, considering the importance of ensuring cybersecurity etc., cooperation will be carried out based on Article 43, Paragraphs 1 and 3 of this Act, as follows:

A) The JFTC shall, when deemed necessary, request opinions from relevant government ministries and agencies regarding whether the actions of a designated provider fall under the proviso of Article 7 or Article 8.

B) Upon receiving a request under (a), relevant government ministries and agencies shall examine the matter from a specialized perspective and may provide opinions to the JFTC on the applicability of the proviso of Article 7 or Article 8. Furthermore, even in the absence of a formal request under (a), relevant government ministries and agencies may provide opinions to the JFTC if they deem it necessary based on the claims made by the designated provider or other considerations. Additionally, if necessary, the JFTC may confirm the contents of the opinions with the designated provider and provide an opportunity for the provider to express its views.

C) The JFTC shall fully consider the opinions of relevant government ministries and agencies under (b) before determining whether there is a violation of Article 7 or Article 8.

D) The JFTC and relevant government ministries and agencies shall mutually establish contact points to facilitate communication and coordination related to the above cooperation.

➢ Additionally, cooperation shall also be carried out as needed beyond the application of the proviso of Article 7 or Article 8.