

Competition Assessment of the Mobile Ecosystem Final Report : Summary

June 16, 2023

Secretariat of the Headquarters for Digital Market Competition
Cabinet Secretariat, Japan

1. Importance of Mobile Ecosystem to economy and society

- ◆ Smartphones are rapidly spreading in our society, and through smartphones, people are able to enjoy a variety of services necessary for their daily lives. For **consumers, they can keep them on hand and use services anytime, anywhere. For businesses, smartphones provide an unprecedented opportunity to access a wide range of users as a strong customer contact point.** Accordingly, smartphones have brought **tremendous benefits** to both parties, serving as the **foundation of economy and society.**

2. Influence of Platform Operators in Mobile Ecosystem

- ◆ Businesses that access customers through smartphones need to **provide services in accordance with specifications and “rules” set by OS , app store, browser, etc.**
⇒ Platform operators that form Mobile Ecosystem have a **strong influence in determining nature of digital space .**



This competition assessment has been conducted on **how layer structure in Mobile Ecosystem affects competition environment .**

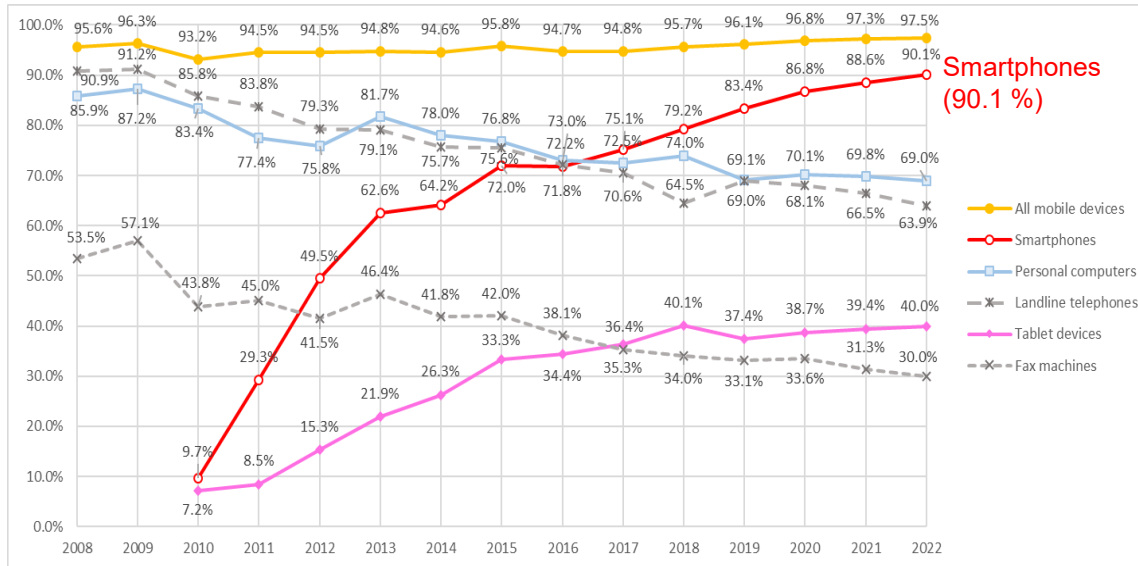
3. Draft development process and Goal

Interim report was published in April 2022, soliciting public comments. This final report has been completed, with participations of security and privacy experts, and a representative from the consumer related stakeholder group in Working Group, while considering the large number of domestic and foreign feedbacks received during public comment period, conducting interviews to various stakeholders inside/outside the country, conducting surveys to businesses and consumers, and exchanging views with relevant foreign governments,.

- ◆ **GOAL:** By realizing fair and equitable competition environment in Mobile Ecosystem, while ensuring security and privacy, innovation by various entities is activated, and users can choose various services created and benefit from them

- ◆ Smartphones spread rapidly, reaching **90.1 %** of households (2022)
- ◆ Average time spent for daily mobile internet use has also increased significantly both weekdays and holidays.
 - ✓ Weekdays : 37.6 minutes (2012) → **110.0 minutes, about three times** (2021)
 - ✓ Holidays : 53.7 minutes (2013) → **126.8 minutes, more than double** (2021)
- ◆ Mobile content-related market is also expanding (over **7.7 trillion yen**, 108% from previous year) (2021)

Smartphone penetration rate



Created from "2022 telecommunication usage trend survey", Chart 1-1

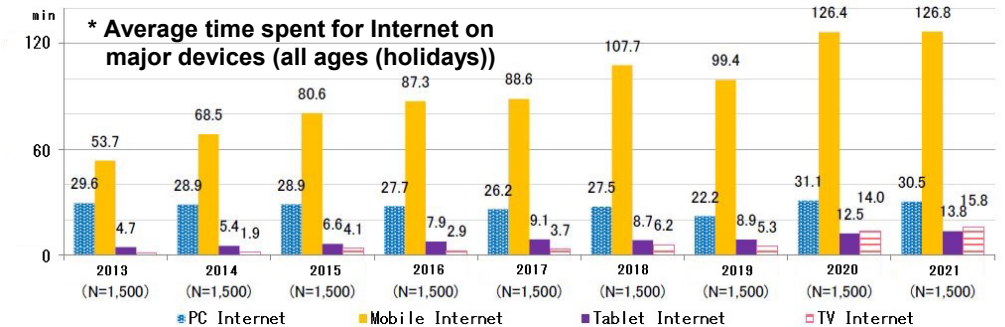
Mobile content-related market

Unit: Billion yen

| Year | 2018 | 2019 | 2020 | YoY | 2021 | YoY |
|-------------------------------|--------|--------|--------|------|--------|------|
| Mobile content market | 2226.1 | 2337.8 | 2629.5 | 112% | 2822.4 | 107% |
| Mobile commerce market | 3994.1 | 4549.3 | 4486.3 | 99% | 4883.7 | 109% |
| Mobile content-related market | 6220.2 | 6887.1 | 7115.8 | 103% | 7706.1 | 108% |

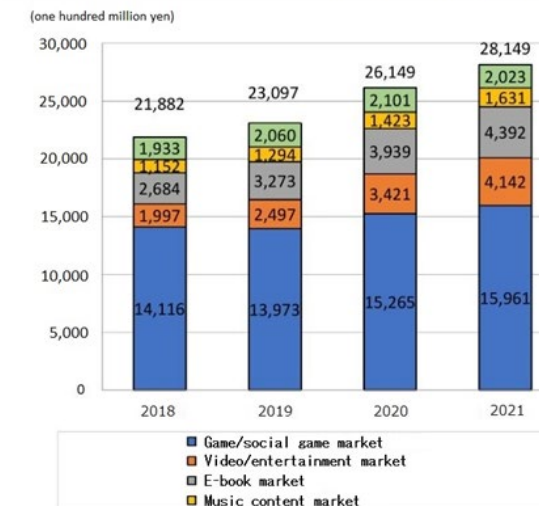
Mobile Content Forum Research

Changes in average time spent for Internet



Survey on information and communication media usage time and behavior (Figure 3-1-1-2)

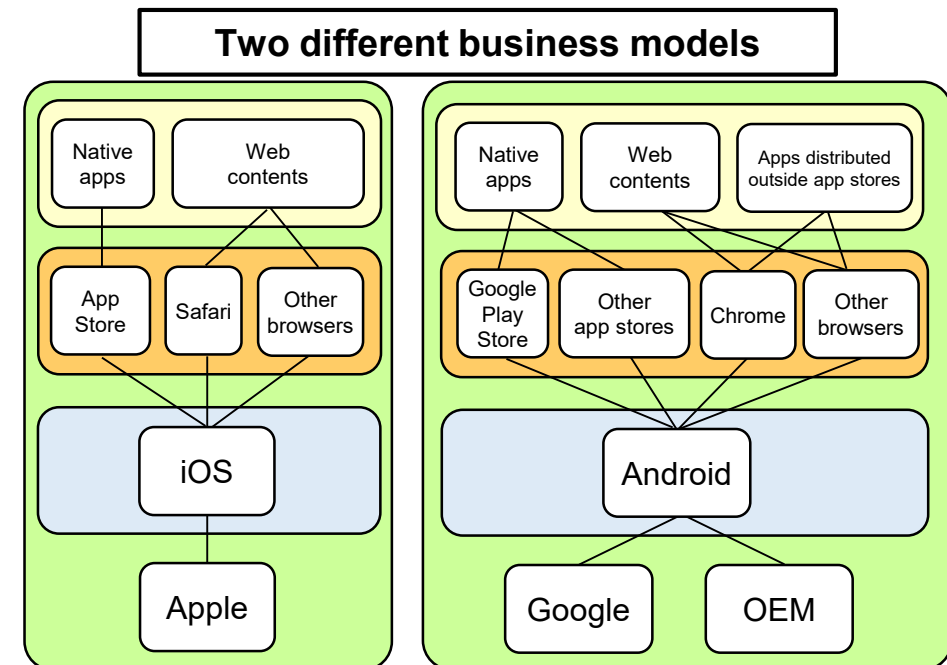
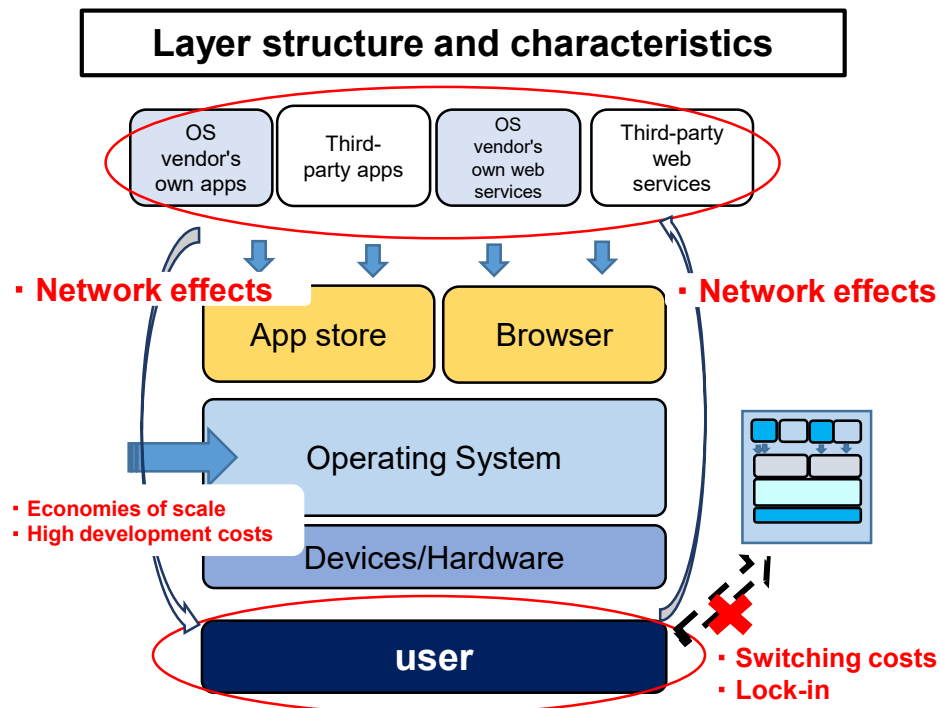
Mobile Content Forum Research



Mobile content market

- *1 Games/social game market: Billed content in online games, SNS, etc. Includes avatars, items, and other purchasable tools.
- *2 Video/entertainment market: Video and other content available on smartphones and other devices.
- *3 E-books, etc. market: Book, comic and magazine content available on smartphones and other devices.
- *4 Music content market: Music content available on smartphones and other devices.

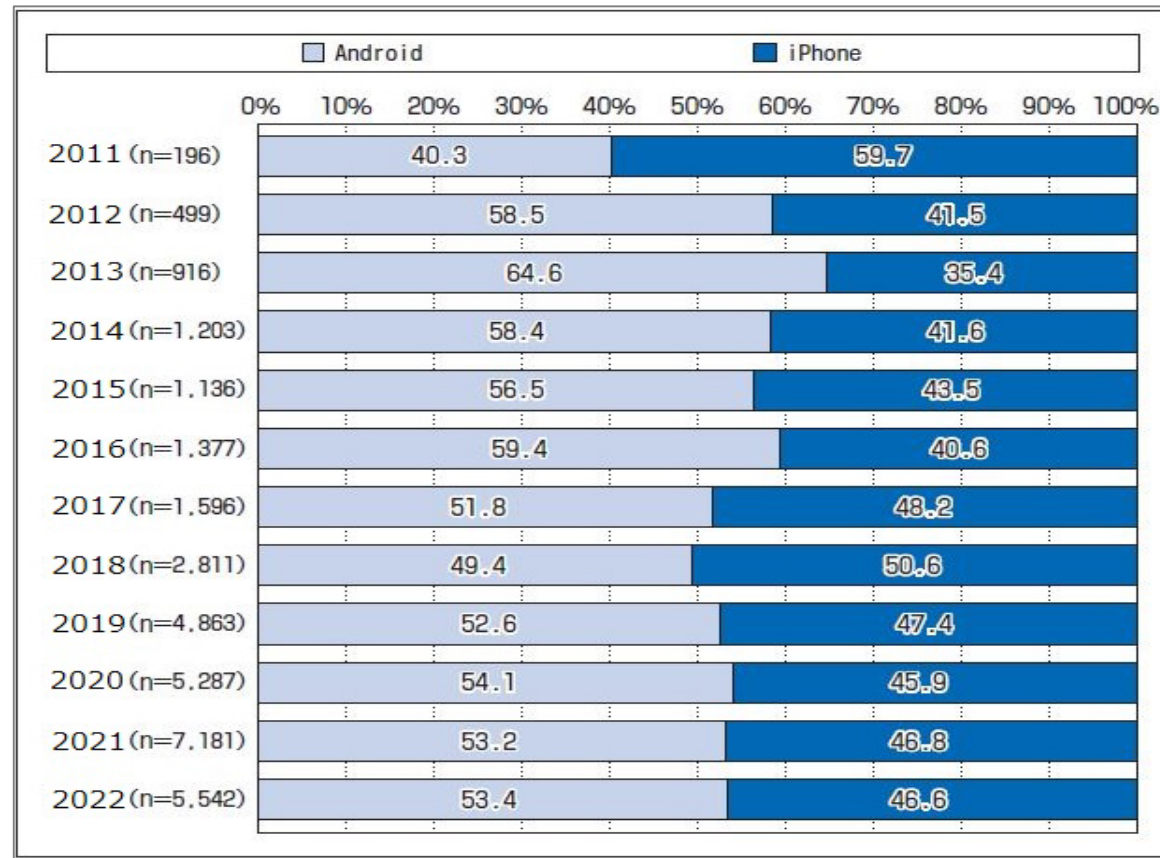
- ◆ **Layer structure:** Consists of **OS layer** where only a handful of players exist, and **other layers** (app store, browser, etc.) with foundation of OS layer
 - ◆ Characteristics of Mobile Ecosystem
 - ✓ **Network effect : Increase** in users by bringing in attractive apps . As the number of users increases, the number of apps and developers in the ecosystem further increases
 - ✓ **Switching costs** : User lock-in due to familiarity with UI design, and hassle of migrating data and reinstalling apps
 - ✓ **Economy of scale** : Huge cost of development
 - ✓ **Data Accumulation** : Data, which cannot be obtained by other businesses, is collected and used in each layer. Further increase competitiveness of platform operator in each layer
- ⇒ **High barrier to entry. Oligopoly with a small number of platform operators**



Apple : Strength in devices, vertical integration (App store, browser engine)
Google : Strength in searches, etc. , pre-installation and default setting with contracts

◆ Oligopoly by iOS (Apple) and Android (Google)

- ✓ According to “the White Paper on Mobile Society 2022,” market share of the most frequently used OS is **53.4 % for Android** and **46.6 % for iOS** (2022) [Figure below] * Web survey based on the number of units in operation
- ✓ **Oligopolistic state of Android and iOS. No big change in this trend.**



Note: Answered by Android or iPhone users

Source: 2011-2022 Mobile Trends Survey to General Use

White Paper on Mobile Society 2022 (Mobile Society Research Institute)

Role and Characteristics of Each Layer

| layer | example | role | Characteristics |
|----------------|------------------------------|--|--|
| OS | iOS , Android | <ul style="list-style-type: none"> Get softwares in each layer above OS work to function on mobile devices Significant influence across whole Mobile Ecosystem | <ul style="list-style-type: none"> Indirect network effect (getting more users leads to more developers, attracting more users) High barrier to entry (large-scale development resources required, etc.) Switching cost (UI , replacement cost, data accumulation, etc.) <p><u>*Questionnaire result:</u> Continued use of the same OS as most recent one iOS (88.1%), Android (96.8 %)</p> |
| app store | App Store, Google Play store | <ul style="list-style-type: none"> Gateway for app developers to deliver apps to mobile device users Platform operator reviews apps based on its guideline, and decides on distributable apps | <ul style="list-style-type: none"> Indirect network effect High barrier to entry (prohibiting other app stores (Apple), preinstallation and default settings through offering monetary benefits to OEMs (Google), etc.) Switching cost |
| browser | Safari, Chrome | <ul style="list-style-type: none"> Gateway for website operators to present website to mobile device users Browser's function affects websites' functions, etc. Influence on development of web services including as web app | <ul style="list-style-type: none"> Indirect network effect (Websites tend to adapt their functionality to browser that has acquired many users (compatibility), making the browser more attractive to users) High barrier to entry (difficult to enter for browser with limited website compatibility, superiority of defaulted browsers, large-scale development costs, etc.) Switching cost (due to data such as ID/ password, bookmarks, etc.) <p><u>*Questionnaire result:</u> The most frequently used browser Safari for iOS (66.3 %), Chrome for Android (66.6 %)</p> |
| search service | Google search | <ul style="list-style-type: none"> Gateway to web for users Search results, display, etc. are critically important for web services to reach users | <ul style="list-style-type: none"> Network effect ((The more users for the search service, the more websites focus on responding to that search service. In addition, accumulation of data ffrom many users improves search result quality and accuracy, leading to more users acquired.) High barrier to entry (large-scale development and maintenance costs, data accumulation of query and index), Switching cost (advantageous position from pre-installation, default settings) <p><u>*Statcounter survey:</u> Search service market share in mobile devices Google (80.7 %), Yahoo! (17.8 %), Bing (0.5 %)</p> |

Recognition of Mobile Ecosystem as a whole

Perspective characteristics of mobile ecosystem

- ◆ **Each major** layer of ecosystem is **an oligopoly** of a small number of platform operators
 - ✓ Google : Adopt a strategy of widely providing major products such as mobile OS and search engines to third parties, having a strong position in each layer
 - ✓ Apple : Adopt vertically integrated model, determining pre-installed softwares on its devices and OS
- ◆ Platform operators **leverage their strengths in each layer to effectively determine various rules** that stipulate competition conditions in other layers.
 - ✓ **Ensure and fortify its position** in layer where advantages exist
 - ✓ **Reinforce its competitiveness** of its services in **other layers**
- ◆ **Multiple and synergistic inter-layer-actions of a handful of platform operators enhance their dominant position in each layer**, in conjunction with which, **influence in the whole ecosystem is reinforced, and even entrenched**



Various competitive concerns in each layer and whole Mobile Ecosystem

- ◆ **Deterioration of level playing field** (between platforms and third parties, and between third parties)
- ◆ **Rising business costs** and **depreciating commercial viability** in each player
- ◆ **Exclusion from and suppressed entry** in each layer as well as whole Mobile Ecosystem, and **Elimination of competition pressure** through technological innovations, etc.

Our vision of whole Mobile Ecosystem, and Direction toward realization

Our vision of whole Mobile Ecosystem

- ◆ Ensure **opportunities of innovation by diverse entities** and **consumer's choice**, in each layer of Mobile Ecosystem
 - ✓ **Encourage innovation** by technology advance, etc., by means of function of **competitive pressure** to whole Mobile Ecosystem and to individual layer. Furthermore, Ensure competitive environment not eliminating possibility of upcoming paradigm shifts by which existing Mobile Ecosystem are changed to considerable degree
 - ✓ In cases where one layer affects competition in others, **ensure an equitable and fair competitive environment in the other layers.**
 - ✓ Ensure not to impair **an equitable and fair competitive environment**, which can be influenced by leverage in Mobile Ecosystem in **competition for extending to new customer contact points.**
- ◆ Importantly, Ensure **security and privacy** .

Direction toward realizing the vision

- ◆ Combine measures according to characteristics of each layer and impact it has on other layers or ecosystem as a whole
 - ✓ **Measures to increase competitive pressure** in the layer
 - ✓ **Measures to remove concerns due to conducts or influences** to other layers
- ◆ **Matters to be fully considered**
 - ✓ As smartphones have become ubiquitous and indispensable for many, and they handle various types of information including highly sensitives, it is **extremely important to ensure security and privacy in Mobile Ecosystem**
 - ✓ Necessary to give **sufficient consideration to impact** of competition policy measures **on security and privacy**

Perspectives in addressing issues: Difficulties in solving problems, and Further concerns in the future

- ◆ In transactions using digital technology, cost associated with transaction is generally small, **network effect** is strong and it functions rapidly. Therefore, **once tipping occurs**, it will lead to a **monopoly (or oligopoly)**, and **this problem is difficult to solve through the market function**
 - ⇒ These digital characteristics are exhibited in **multiple layers**, resulting in **position** of platform operators established as **extremely entrenched and fixed**
- ◆ Due to use of algorithms, etc., **the business decision process becomes untransparent** (information asymmetry)
 - ⇒ Platform operators can **easily exercise influence** in each layer of Mobile Ecosystem
- ◆ Transactions using digital technology are likely to form a **large two-sided market, consisting of businesses and consumers**, due to **strong network effect**.
 - ✓ While presenting **low-priced or free of charge to consumers**, presents **conditions unfavorable to businesses**. In between, platform operators can enjoy the rent
 - ✓ As platform operators control access to consumers, **businesses are locked in, making it difficult for issues to be cure from business side**
 - ✓ **As whole picture and issues do not tend to become apparent for consumers, making it difficult for issues to be cure from consumer side**
 - ⇒ **Difficult to expect autonomous solution by market function**
- ◆ **Limited rationality of consumers** (Limited recognition of choices, Constraints on rationality of choices and judgments due to status quo bias)
 - ✓ Limitations on screen size of mobile devices, characteristics of usage situations (while moving, etc.) and operability
 - ✓ Concerns grow even greater as constant connectivity is linking with purchasing activities and payments
 - ⇒ If platform operator **restricts or induces consumers choices, more concern arises as to deteriorating rational judgment of consumers**
- ◆ **Expand influence** in Mobile Ecosystem by leveraging mobile devices, as powerful and **always-connected customer touchpoint**
 - ⇒ Concerned about **deepening influence** on activities of consumers and businesses

Challenges in addressing by existing legal frameworks, and Need for renewed approach

◆ Conventional competition law approach

1. Identify theory that **a particular conduct causes a harm to competition in a relevant market**
2. **Specifically prove that the harm is occurring** in accordance with the theory, and
3. **Implement remedy to eliminate** the harm

Challenges of Competition Law Approaches to Mobile Ecosystem

- ◆ Typically, a platform operator in a position, enabling it to exert influence to other multiple layers, causes competition problems by **an indefinite and simultaneous (and usually) multiple conducts, implemented at any layer that it can leverage.**
 - ✓ Even if competition harm caused by a single conduct is relatively minor, multiple conducts work in a **combined and synergistic manner**, to manifest the competition harm.
 - ✓ **Impact is brought in on a different layer** than the one in which conduct is performed.
- ◆ **Difficult to define market**
 - ✓ Many **zero-price markets** and **multi-sided markets**, making it hard to use conventional methods.
 - ✓ Difficulty in envisioning future competitors, due to **difficulty in predicting technological innovations**
- ◆ Difficult (1)to **identify theories** regarding the process by which numerous conducts cause competition harm, (2)to **specifically prove that harm is caused in accordance with the theories**, and (3)to **consider justifications** and to **make a judgment**
 - ✓ **Information** necessary for evaluation is **unevenly distributed on the side of platform operator**
 - ✓ **Difficulty in evaluating qualitative factors** such as privacy and customer experience, other than price

Need for renewed approaches

- ◆ **Considerable amount of time** to reach a final conclusion (during which time competitive environment may change)
 - ◆ Even if illegality can be proven, the same kind of harmful effects on competition may be repeated **by means of circumventing conducts** outside the scope pointed out by the enforcement agency
- New approach needed different from conventional competition law approach**

Approach for consideration of measures

As is seen previously, it is necessary to consider different approach to competition issues in Mobile Ecosystem, **other than conventional competition law approach** .

Measures by means of “ex-ante regulation”

- ◆ Once tipping occurs, it leads to a winner-takes-all situation, which is **difficult to be overcome through market function**
- ◆ **It has become clear what types of conducts by platform operators are at high risk of adversely affecting competition**

⇒ Appropriate to address issues by means of **prohibiting or obligating certain acts in advance**, “**Ex ante regulatory framework**”.

- ◆ Specific conducts by platform operators that may adversely affect competition might be **measures taken for ensuring security and privacy**. Such measures are permissible as **justifiable ones in certain cases, even though they may have adverse** impact on competition.

Measures through a “co-regulatory framework”

- ◆ There are other issues that **should be dealt with “co-regulatory framework,”** adopted by existing “Act on Improving Transparency and Fairness of Digital Platforms” (“the Transparency Act”)

⇒ Such issues is to be **dealt with through a “co-regulatory framework”**



Policy Mix of two approaches
“ Ex Ante regulatory framework” and “Co-Regulatory framework”

Major Points of New Frameworks

Business to be regulated

- ◆ **Mobile OS providers can acquire a position in each layer by providing a mobile OS or by designing a mobile device including an OS themselves. They shape, strengthen, and entrench Mobile Ecosystem by exerting a strong influence on competitive landscape across layers as well as ecosystem as a whole**
⇒ **Platform operators that provide mobile OS (*) of a certain size or larger should be subject to regulation.**
- ◆ Currently, mobile OS providers are leveraging their positions to gain dominant positions in each layer in Mobile Ecosystem
- ◆ However, depending on type of conducts, even if it is not a mobile OS provider, a platform operator, who has developed a service of a certain size or larger, can gain its potent position, in backdrop of which it may engage in conduct causing harmful effects on competition.
- ◆ Thus, it is also imperative to secure **equal footing**, in case **even operators not providing mobile OS will have solidified position in certain layer** in the future.
⇒ **Platform operators that provide services of a certain size or larger in app store, browser, or search engine should also be subject to regulation** according to the characteristics of the regulated conducts

(*)When use the term “operators that provide OS” without any annotations, “OS” means “mobile OS”.

Submission and publication of compliance report with regulation by platform operators

- ◆ As it may be difficult for enforcement agencies, etc., to grasp the status of compliance, it is **important for regulated operators to explain the status of compliance**.
- ◆ By having **regulated operators check their own compliance** with new regulations, deterrence of violations is expected.
- ◆ To ensure effectiveness of regulations, it is important to make **the status of compliance known to stakeholders** and to create a system that allows **stakeholders to check it**
⇒ Regulated operators shall **submit a report to the enforcement agency on status of compliance** with new regulations, and the report shall be made **public**

Countermeasures to circumvention

- ◆ Make sure that conducts outside the scope specified by enforcement agencies do not cause similar harm to competition.
⇒ Need for **rules to prohibit circumvention**

| | Specific Issues | Slide # |
|--|--|--|
| 1. Specification changes, etc. in OS, browser, etc. | 1-1. OS and browser updates, specification changes, and rule changes 1-2. Tracking rule change in OS (representation to end users) 1-3. Standardization of technologies that give the company an advantage in search (changes in other major parameters, etc.) | 13 15 16 |
| 2. Application store related issues | 2-1. Mandatory use of payment/billing system 2-2. Restrictions on information provision, steering, etc. of other billing systems, etc. within app 2-3. Establishing competitive environment among reliable application stores (allowing alternative distribution channels for apps) 2-4. Closed middleware | 17 19 20 24 |
| 3. Browser functionality restrictions | 3-1. Mandatory use of WebKit and reluctance to support web applications 3-2. Access restrictions on browsers to functions of OS, etc. 3-3. Limitations in browser extensions | 25 25 27 |
| 4. Pre-installation, default settings | 4-1. Pre-installation, default settings 4-2. Preferential treatment of its own services in its own search service | 28 30 |
| 5. Acquisition and use of data | 5-1. Use of acquired data 5-2. Opacity of data acquired, etc. 5-3. Ensuring data portability by end users 5-4. Social Login (" Sign in with Apple ") | 31 32 32 33 |
| 6. Access to functions of OS, etc. | 6-1. Access restrictions on apps to functions of OS, etc.(MiniApp) 6-2. Access restrictions to UltraWideBand 6-3. Access restrictions to NFC (Near Field Communication) 6-4. Time advantage of app development associated with OS updates, etc. 6-5. Access restrictions on voice assistants 6-6. Links with Siri using SiriKit 6-7. Access restrictions to functions of mobile OS, etc, from smartwatch | 34 35 36 37 38 39 39 |
| 7. Other concerns about voice assistant and wearable devices | 7-1. Monitoring scheme | 40 |

1. Specification change of OS , browser, etc.

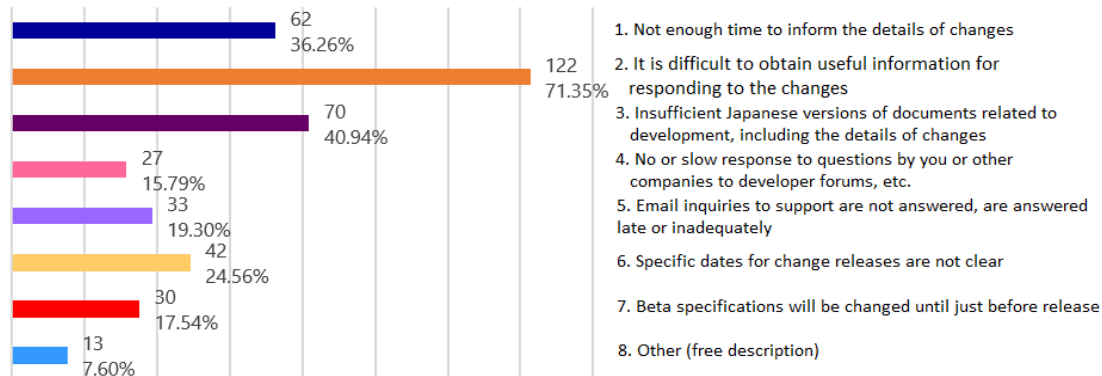
1-1. OS and browser updates, specification changes, and rule changes①

Issues

- ◆ Apple and Google provide a system to accept inquiries and feedback from developers, etc. to a certain extent when changing rules, etc. in OS and browser.
- ◆ However, there are concerns from developers, etc. that **sufficient preparation time is not secured**, the **scope of information provided is insufficient**, and **responses to inquiries and requests for consultation are insufficient**.
 - ✓ Time that should be devoted to quality improvement is deprived due to being busy with responses to rule changes etc. in a short period of time
 - ✓ For major updates, the specifications of the new version are not finalized until just before the release, and a few days after the final update version is released, the new version is distributed to users.
 - ✓ Information on when the new OS update is released and how the update would work is not sufficient.
 - ✓ Even if developers make an inquiry or request to discuss the extension of the preparation period, they only receive responses in fixed form, and effective consultation is insufficient
- ◆ From survey results, problems related to rule changes, etc. in OS and browser have been identified.
 - ✓ Questioned, on OS specifications changes or updates, whether there were problems, such as **bugs in apps, delays in apps' revision or release, and more workload than the initial business plan**, more than 60% answered "often" or "occasionally" .
 - ✓ In response to questioning what kind of problem it was (multiple answers allowed), "It is **difficult to obtain useful information** for responding to the changes" [iOS : 71.35 % , Android : 69.74 %] , " Insufficient Japanese versions of documents related to development, including the details of changes" [iOS : 40.94 % , Android : 35.53 %] , "Not enough time to be informed on the details of changes" [iOS : 36.26 % , Android : 36.18 %] (See Figure below)

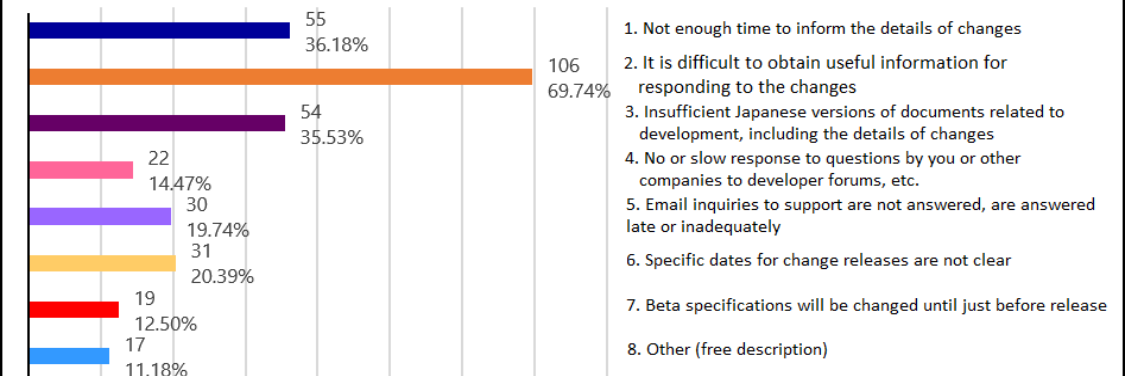
iOS

Q4: Please select all that apply as to why there was/is a problem (multiple answers allowed)



Android

Q14: Please select all that apply as to why there was/is a problem (multiple answers allowed)



1. Specification change of OS , browser, etc.

1-1 . OS and browser updates, specification changes, and rule changes ②

Competition assessment

- ◆ **Predictability and transparency** of app developers, website operators, etc. **may be hindered**, resulting in **excessive burdens** and **business uncertainties and risks for them**. This may **hinder innovation** by developers and **reduce consumer choices**.

Direction of addressing issues

- ◆ As to rule changes, etc. in OS and browser (*),, to improve fairness and transparency, and to make the process of dialogue with developers more effective, **platform operators that provide operating systems of a certain size or larger or browsers of a certain size or larger** shall be subject to the following **co-regulatory framework**:
 - ✓ **Requirement to disclose in advance** details and reasons for rule changes, etc.
 - ✓ Since the content of rule changes, etc., varies, the timing of disclosure will not be uniform, but will be “a date for ensuring a reasonable number of days” according to the content of the changes.
 - ✓ As specification changes are frequent and numerous, exceptions are allowed, in case of extremely minor changes, security risks that require urgent action, etc.
 - ✓ **Development of procedures and systems for responding to inquiries and dialogues**, to the extent necessary and reasonable
 - ✓ **Organizations** representing developers, etc. are also **allowed to become parties** for dialogues.
 - ✓ **Recommendations and publication** by the government regarding the procedures and systems necessary to promote information disclosure and mutual understanding, when deemed particularly necessary
 - ✓ **Reporting** of operational status to the government **and monitoring and review** by the government

* As to browsers, above is not limited to mobile devices, but applicable to PCs , etc.

1. Specification change of OS , browser, etc.

1-2 . Tracking rule change in OS (Representation to end users)

Issues

- ◆ Apple requires developers (1) to **display a phrase (ATT prompt)** that **emphasizes the risk** that an unspecified number of other companies **will track users**, and (2) to obtain permission from the users to track them, when the app tracks the users using the IDFA (Identifier for Advertisers), which is a unique ID assigned to each iOS device.
 - ✓ ATT Prompt: “**Allow ‘(app name)’ to track your activity across other companies’ apps and websites ?**”
- ◆ In the case of Apple's own apps, it is not required to display ATT prompts because **they do not track users using IDFA**, and Apple shows another notification for choices. But **the tone of that notification is positive, emphasizing the merits of personalized advertisements** compared to ATT prompts, when asking if they want to "Turn on personalized ads".
 - ✓ Notifications in Apple's own apps: “Personalized ads: Personalized ads in Apple’s apps such as the App Store and Apple News **help you discover apps, products and services that are most relevant to you. We protect your privacy** by using device-generated identifiers and not linking advertising information to your Apple ID.”
- ◆ Apple says it doesn't track users, but it may use user account information, App Store information, and other information to assign users to segments in order to display personalized ads .

▼ Apple 's own display

パーソナライズされた広告

App StoreやApple NewsなどのAppleのAppでパーソナライズされた広告は、あなたと関連性の高いApp、製品やサービスを見つけるのに役立ちます。Appleは、広告情報をApple IDに関連付けずにデバイス生成識別子を使用することによってあなたのプライバシーを保護します。

▼ ATT prompt (example)

app name が他社のAppやWebサイトを横断してあなたのアクティビティの追跡することを許可しますか？

これにより、 app name より優れた広告エクスペリエンスを提供できます。

Appにトラッキングしないように要求

許可

Competition assessment

- ◆ While ATT prompts require the text emphasizing the risks of tracking users, Apple emphasizes its benefits in a positive tone when asking for permission for Apple's own personalized ads. Although there is no need for the two displays to be the same, it is **difficult to say that they are treated fairly**.
- ◆ There are concerns that Apple is using its position as an app store rule maker to determine how the prompt should be displayed, creating a favorable environment for its own advertising business model. If so, there is a risk that fair competition in the field of advertising business will be hindered.

Direction of addressing issues

- ◆ Apple's obligation of ATT prompt is a condition of app review or its operation. Therefore, this issue will be dealt with the framework of the obligation **to make the terms of use for business users of app stores fair, reasonable and non-discriminatory**, as described in 2-1.

1. Specification change of OS , browser, etc.

1-3. Standardization of technologies that give the company an advantage in search (changes in other major parameters, etc.)

Issues

- ◆ From February 2016 to May 2020, Google made it a requirement to adopt the AMP (*) format for being displayed in the top news carousel in Google search.

* Accelerated Mobile Pages : Technology that promotes high-speed loading of content

Competition assessment

- ◆ For website operators, whether or not their own websites are **displayed at the upper place in Google search** has a **great impact**.
 - ✓ There is concern that Google has given the competitive advantage to its search business by imposing the above requirements, distributing news services, etc. via its own servers and spreading the data formats that are easy for its own search engine to handle.
 - ✓ As indicated in the "Final Report on Evaluation of Competition in the Digital Advertising Market" (April 27, 2021 Digital Market Competition Council), there are **concerns about the transparency and fairness of changes to major factors in search engines**.

Direction of addressing issues

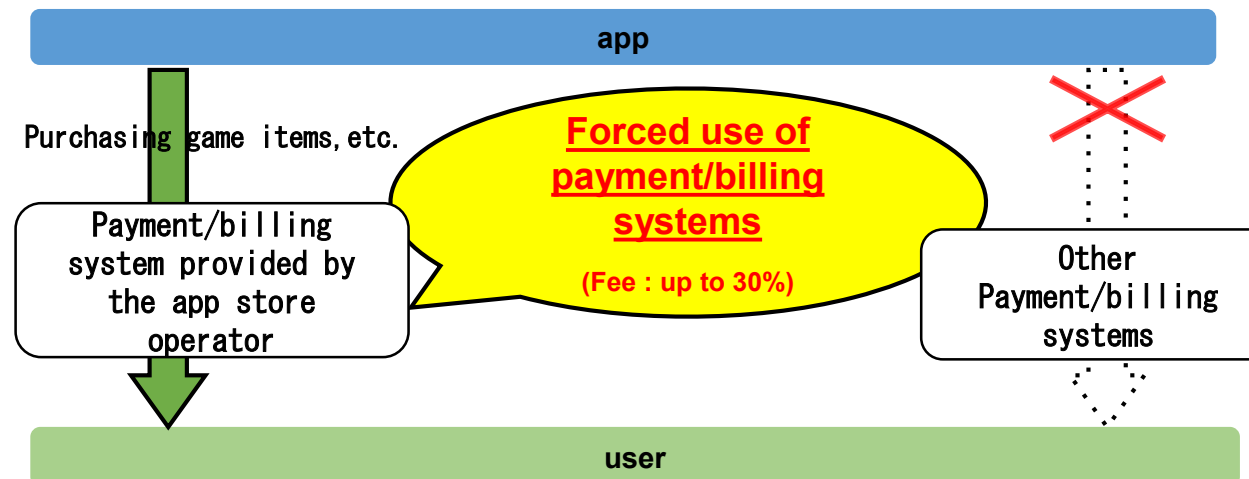
- ◆ In order to ensure the transparency of changes in major factors in search engines and to **ensure the predictability** for the business of website operators, **platform operators that provide search engines of a certain size or larger** shall be subject to the following **co-regulatory framework**: (*)
 - ✓ **Disclosure of major factors such as search engine parameters** used to determine website display rankings
(Always keep the description of disclosure up to date. Prior disclosure is not a legally obliged, but is described in guidelines, etc.)
 - ✓ Establish a **mechanism to respond to complaints and consultations** regarding search algorithm changes, etc. to the **extent necessary and reasonable**
 - ✓ Reporting of operational status to the government and **monitoring and review** by the government
etc
 - ※ Measures in line with the direction of addressing issues to issue 9 (Changes to the Main Parameters of Search Engines) in the "Final Report on Evaluation of Competition in the Digital Advertising Market" (April 27, 2021 Digital Market Competition Council). Accordingly, above framework is not limited to mobile devices, but applicable to PCs, etc..

2. Application store related issues

2-1. Mandatory use of payment/billing systems①

Issues

- ◆ Third parties that sell in-app content, etc., using the App Store and Google Play Store, **are obliged to use Apple and Google's payment/billing systems and are obliged to pay a certain fee (30%, 15%, etc.) through the systems.** (In September 2022, Google launched the pilot program, called User Choice Billing, which allows developers to choose other payment/billing systems under certain conditions.)
- ◆ Apple and Google explain that the **fee is the price for using app store**, and **very few of all developers bear the 30% fee.** (Apple: 0.3%, Google: less than about 0.1%)
- ◆ There are strong complaints from developers about the **appropriateness and fairness of fee burden**, such as the following:
 - ✓ Heavy burden of fees is putting **pressure on profits**
 - ✓ **Services** received through app stores or payment/billing systems **do not match fees paid**
 - ✓ Fees are **disproportionately borne** by a part of developers
- ◆ The followings have been pointed out regarding the mandatory use of Apple and Google's payment/billing systems:
 - ✓ **Unable to provide diverse price plans** and services
 - ✓ When using Apple's **IAP**, **flexible pricing is not able to be provided** because the price is set by the Tier.
- ◆ **App user information is managed by Apple and Google's payment/billing systems, and developers do not have sufficient information**, the followings have been pointed out.
 - ✓ **Direct communication** between users and developers are **not smooth** regarding refunds, cancellations, etc.
 - ✓ Developers find it **difficult to provide attentive customer service**



2. Application store related issues

2-1. Mandatory use of payment/billing systems②

- ◆ From the survey results, as shown below, problems related to fees and payment/billing systems have been identified.
 - ✓ Developers who pay 30% fee were asked how to think of it as a price for the service provided by the app store.
 - **"Expensive" (Apple: about 59.5%, Google: about 48.3%)**
 - **"Relatively expensive" (Apple: about 23.8%, Google: about 27.6%)**
 - and the sum of the answers, for each company, **well exceeds 70%**.
 - ✓ When the respondents to the questionnaire were asked why "it's expensive" or "relatively expensive," the following answers (multiple answers allowed) were chosen by many respondents.
 - **" I feel that the profit margin of Apple/Google is large" (Apple: about 73.8%, Google: about 67.5%)**
 - **"The grounds for fees are not clear" (Apple: about 60.2%, Google: about 56.3%)**
 - ✓ **Approximately 60% of developers that pay fees request the use of payment/billing methods provided by companies other than Apple and Google.**
 - ✓ Regarding the reasons for this (multiple answers allowed), the following answers were particularly frequently chosen.
 - **"I want to keep the fees for app sales and in-app purchases low" (90 %)**
 - **"I want users to be able to choose from a variety of payment methods" (71.6 %)**

Competition assessment

- ◆ Mandatory use of payment/billing systems **hinders the entry of businesses that provide alternative payment/billing methods**, hinders developers from providing diverse rate plans and services, and reduces **innovation**. **Users are deprived of choices** and cannot receive a variety of services.
- ◆ Fee burdens can squeeze developers' profits and adversely affect their investment capacity, leading to **reduction of new value through innovation and competition**.

Direction of addressing issues

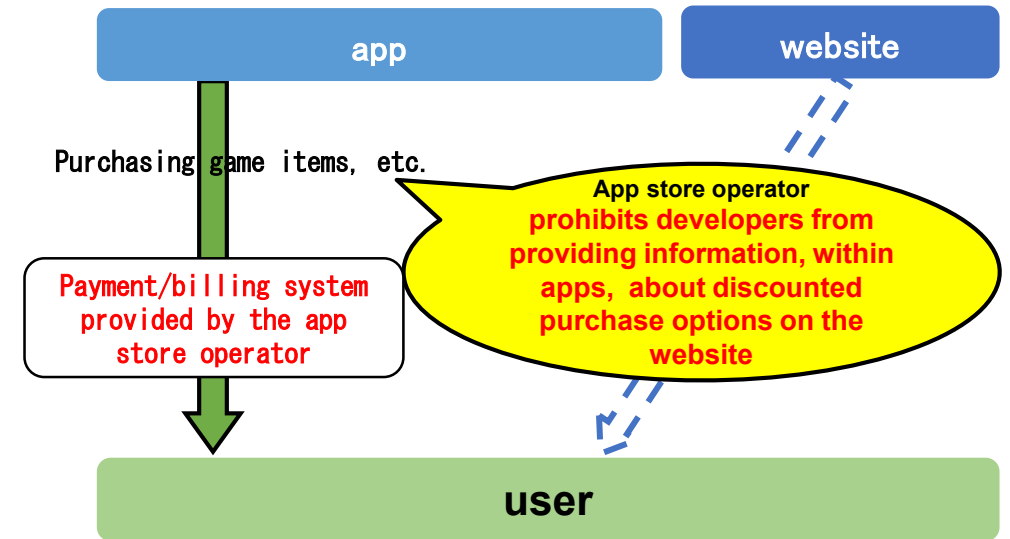
- ◆ **Platform operators that provide app stores of a certain size or larger shall be prohibited from obliging developers who use the app stores to use app store providers' own payment/billing systems.**
- ◆ **They shall be required to apply fair, reasonable and non-discriminatory usage conditions (including fees)** for app store business users
 - ✓ Although third-party payment/billing systems can be used in other countries, a fee of 30% ⇒ 27% (Netherlands) or 26% (Korea) is collected, and various other conditions are imposed. This requirement will preclude other payment/billing systems from fully being utilized.
- ◆ Concerns about impediments to communication regarding refunds, etc. will be addressed by monitoring based on the Transparency Act

2. Application store related issues

2-2. Restrictions on information provision, steering, etc. of other billing systems, etc. within app

Issues

- ◆ **Apple and Google restrict information provision, steering, etc. within apps** by developers using the App Store and Google Play Store.
 - ✓ Using language, within the app, that encourages users to purchase digital goods outside of the app.
 - ✓ Posting outlinks within the app or otherwise inducing users to transact outside of the app.
- ◆ As a result, users will to make purchasing decisions based solely on information within the app, **without knowing other plans or pricing on the website.**
- ◆ **Apple and Google explain** the reasons for this restriction as follows:
 - ✓ To prevent “free rides” that avoid paying fees while using the app store
 - ✓ To prevent users from mistaking external sites that seamlessly migrate from the app to be safe and leading them to malicious sites



Competition assessment

- ◆ **For users, the options** of payment/billing service to use and the options of using an app or a service on the web are **narrowed**, and the user's interests will be damaged.
- ◆ **Opportunity for transaction of any payment/billing service of other than Apple and Google have significantly limited**, adversely affecting efforts by developers to provide a variety of services, such as improving user convenience.
- ◆ The reasons explained by Apple and Google lack validity and rationality as follows.
 - ✓ **The purchase of digital content within downloaded apps is largely dependent on content development by developers**, and the contribution of app store operators is relatively small, compared to the purchase of apps themselves. Under such circumstances, restricting the provision of information to users is highly detrimental in the sense that it impairs the opportunities for users' choices.
 - ✓ Risks such as users being redirected to malicious sites can be dealt with through **app review, bridge pages**, etc.

Direction of addressing issues

- ◆ **Platform operators that provide app stores of a certain size or larger shall allow developers, for free, to provide information or offer transactions**, including different purchase conditions (including outlinks, and including within the app), to users acquired on the app store.
 - ✓ Various restrictions are imposed on outlinks currently approved by Apple, which hinder smooth use. Therefore, such restrictions can be dealt with by prohibiting anti-circumvention measures.

2-3. Establishing competitive environment among reliable application stores (allowing alternative distribution channels for apps)

Issues

- ◆ In principle, Apple does **not allow installation of apps other than via App Store** on the iPhone.
- ◆ On the other hand, as seen in “2-1”, regarding **App Store fees**, various points have been pointed out, such as (1) heavy burden, putting **pressure on developers’ profits**, (2) **beared by a part** of developers, (3) App Store operator's **profit margin seems to be too high**, and (4) the **rationale for the fee level is opaque**.
- ◆ For app developers, **whether or not to be posted on App Store is virtually a decisive factor in whether or not they can provide services**. Accordingly, developers are **forced to be conservative, and this hinders innovation**
- ◆ **Survey to consumers** indicates alternative distribution channels for apps will be used if they are beneficial to users and ensure security and privacy.
 - ✓ “I like to use it **if it is more secure** than App Store” (34.9%), “I would like to use it if the price of the apps is **cheaper than** in App Store” (32%)
- ◆ Developers pointed out that if they can provide apps for both iOS and Android through official third-party application stores under the multi-platform trend, it will open up a variety of possibilities.

Competition assessment

- ◆ Restrictions on alternative distribution channels for apps have created **various competition issues**;
 - ✓ **Loss of opportunities** for the companies other than Apple to **enter** iOS application store business
 - ✓ **No competitive pressure on App Store fees**
 - ✓ **App review** in App Store is not always **transparent and fair, hindering innovation and user choices**
- ◆ Effectiveness is ensured by designing a system enabling emergence of alternative app distribution channels which can be used by users and developers.
 - ✓ **Provided in a manner that demonstrates benefits to users and ensures security and privacy**
- ◆ It is important that apps are reviewed by third parties that operate alternative distribution channels **to ensure security and privacy** (See P.21-23).

Direction of addressing issues

- ◆ **Platform operators that provide OS of a certain size or larger shall allow effective use of alternative app distribution channels which ensure security and privacy.**
 - ✓ **OS providers can take necessary and proportional measures to ensure security and privacy, etc... A framework for the regulatory authorities to determine whether the measures are excessive**, when there is concern that alternative app distribution channels are not being used effectively
 - ✓ **OS providers shall not be obliged to allow direct downloads of apps from websites.**
 - ➔ **Application stores that ensure security and privacy, etc. are allowed to enter the market**, aiming at creating “**competitive environment among reliable application stores**”
- ※ It would also be useful to have a certain guideline for app reviews, etc. that should be handled by application stores. Such guidelines, etc., may be presented by security expert groups, etc. (See P.23)

2. Application store related issues

2-3. Examples of threats posed by apps and risk assessment for each type of app alternative distribution channel

- ◆ Effective defense methods differ depending on the threat
 - ✓ Malicious apps **attacking other apps and storage** can be protected to some extent **by sandbox**.
 - ✓ Sandbox is difficult to defend against certain threats, such as **data being stolen as a result of the user granting an app access permission** to various types of data, or placing an unnecessary load on the device. Those threats can be **dealt with by app review by application store**.
 - ✓ **Attacks that exploit unknown vulnerabilities** are difficult to deal with in advance through application store reviews. It can be dealt with by ex-post OS update or removing them from the application store.
- ⇒ **Dealing with a combination** of sandbox, app review by the application store, and ex-post measures, etc. (see below left table)
- ◆ **Following types are assumed** as alternative distribution channels for apps other than the App Store on iPhone (types other than these are not excluded)
 1. App distribution through alternative application stores downloaded through the App Store subject to review by Apple
 2. App distribution through alternative application stores pre-installed on the iPhone
 3. App distribution through alternative application stores that are downloaded using a browser
 4. App distribution by downloading the app itself via a browser without going through any application store
- ⇒ In order to **assess the risks in each type** of alternative distribution channel for apps, **sort out responses to threats** based on **whether third-party stores and apps can be reviewed and how they can be** (see below right table).

Examples of threats posed by smartphone apps

| Threat (broad classification) | abbreviation for convenience | sandbox | a current response which is supposed | Potential Actions by Stores When Third-Party Stores Are Allowed |
|---|------------------------------|---------------------|--------------------------------------|---|
| Attacks on other apps and storage (Note 1) | simple attack | Defendable (Note 2) | dealt with by sandbox | dealt with by sandbox |
| Data theft with user's permission, unnecessary resource load | theft | not defendable | dealt with by app review | dealt with by app review |
| Criminal assistance (prohibition of use of matching apps under the age of 18, etc.) | Aiding | not defendable | Dealt with by app review | Dealt with by app review |
| The app store itself is fake, etc. | fake store | not defendable | — | — |
| Advanced attacks that exploit unknown vulnerabilities, etc. | advanced attack | not defendable | Post-incident response | Post-incident response |

(Note 1) Excludes other threat items in the table.

(Note 2) Note that sandbox has also vulnerabilities.

It is appropriate to conduct the risk assessment based on the people with low literacy.

In particular, there were opinions from consumer groups that the attention should be paid to the fact that smartphones, unlike PCs, have many elderly users.

Risk assessment for each type of application alternative distribution channel

| Types of alternative distribution channels for apps | Screening of third-party stores | | App review | | | | |
|---|---------------------------------|------------|-------------------|---------------|-----------------------|-----------------------|------------------------|
| | Reviewer | threat | Reviewer | threat | | | |
| | Apple | fake store | | simple attack | theft | Aiding | Advanced attack |
| (2) App distribution through alternative app stores pre-installed on the iPhone | Yes | Defendable | third party store | Defendable | Depends on app review | Depends on app review | Post-incident response |
| (1) App distribution through alternative app stores downloaded through the App Store subject to review by Apple | Yes | Defendable | third party store | Defendable | Depends on app review | Depends on app review | Post-incident response |
| 3) App distribution through alternative app stores that are downloaded using a browser | * | * | third party store | Defendable | Depends on app review | Depends on app review | Post-incident response |
| ④ App distribution by downloading the app itself via a browser without going through any app store | — | — | * | Defendable | Difficult to defend* | Difficult to defend* | difficult to deal with |

*On macOS, Apple provides a "notarization" process even if it is installed via a browser. As for app screening, the current notarization system does not support defense against theft or aiding, and it is thought that some additional measures are necessary.

2. Application store related issues

2-3. From the perspective of ensuring security and privacy ①

Perspectives of ensuring security and privacy

- ◆ There are **two main points** of view for ensuring security and privacy regarding alternative distribution channels for apps.
 - ✓ **Vulnerability verification** perspective to prevent apps from being exploited
 - ✓ Perspective of **preventing distribution of malicious apps** that fraudulently use user data, devices, etc.
- ◆ In principle, **vulnerability verification** should be performed by the **app developer** themselves or by being outsourced.
- ◆ **Application store operators need to take action to prevent the distribution of malicious apps**
 - ✓ Due to its nature, it cannot be expected that it will be handled by the app developer (creator of the malicious app).

Measures that application store operators themselves can take from the perspective of ensuring security and privacy

- ◆ Examples of measures for vulnerability verification (*In principle, efforts should be made by the app developers themselves)
 - ✓ Provide app developers with **secure coding guidelines** for their apps
 - ✓ Actively **share critical vulnerability information** with app developers
- ◆ Examples of measures to **prevent distribution of malicious apps**
 - ✓ Effective dynamic analysis for verification of malicious apps
 - ✓ In order to further improve the validity and effectiveness of verification, conduct static analysis; such as listing the APIs used by partially analyzing the binary of the application.
- ◆ Examples of measures **other than technical verification**
 - ✓ As application store policy, security and privacy are ensured **by limiting the apps they distribute to the ones developed by app developers who can be trusted**, together with some **contractual requirements**
 - ✓ Streamline app reviews **by means of limiting apps to specific categories**

2-3. From the perspective of ensuring security and privacy ②

Measures that can be used as a reference

- ◆ It would also be useful to present a **certain guideline for app reviews, etc. that should be handled by application stores**. The guidelines, etc., can be presented by security expert groups, etc.
 - ✓ As similar effort, Android Application Secure Design/Secure Coding Guidebook is published by the Japan Smartphone Security Association.
 - ✓ **Code of Practice for application stores**, etc. published by DSIT (Department for Science, Innovation and Technology) in the UK (see below)
- ※ The Secretariat of the Digital Market Competition Headquarters, Cabinet Secretariat, and the UK's DSIT have issued the "**Japan-UK Joint Statement on Ensuring App Security and Privacy**" (February 28, 2023), which states cooperation as to sharing insights to ensure protections when users access and use apps and application stores.

Code of Practice for application stores, etc. published by DSIT in the UK (partial excerpt)

The **roles of application store operators and app developers** in app distribution are listed from the perspective of ensuring security and privacy (published in December 2022)

- ◆ Application store operator role (summary)
 - ✓ Application store operators shall clearly set out and publish **security and privacy requirements** for apps posted on the application store.
 - ✓ Application store operators shall have a **vetting process** which includes security checks in which the above requirements are reviewed prior to approving app submissions and updates. Operators shall notify the developer if an app or update is rejected for security reasons.
 - ✓ Application store operators shall provide an overview of the **security checks** that are undertaken for apps and updates in a **publicly accessible location**.
 - ✓ Application stores shall have an **app reporting system** so that users and security researchers can report malicious apps, and developers can report fraudulent copies of their own apps to the application store.
 - ✓ **Once an application store operator verifies that an app is clearly malicious**, they shall **make the app unavailable on the application store** as soon as possible but no later than 48 hours. Operators shall notify the developer that their app has been made unavailable
 - ✓ Once an application store operator verifies that an app or an update is malicious, they should **initiate a proportionate review of other apps that have been produced by the same developer**.
 - ✓ Application store operators and developers should consider **working with independent parties** to assess app security and privacy.

[Examples of information provided by an operator on their **security checks**]

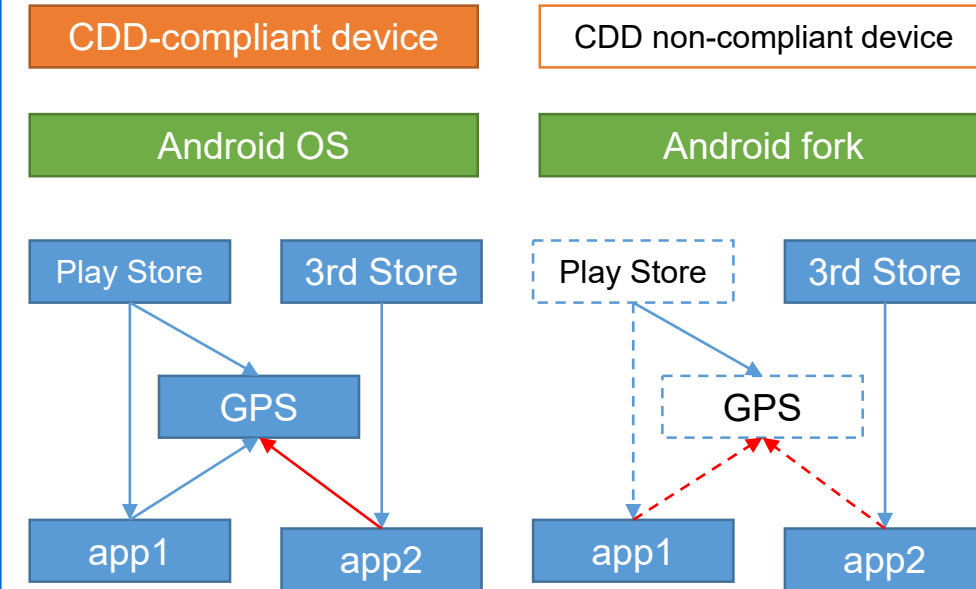
Apps undergo security check which consists of both automated and manual activities. The following activities will be undertaken

- Use of static analysis tools
- Confirmation of requirement of permission
- Confirmation of Software Development Kit versions
- Scanning for default credentials
- Sharing of submission with a third party for further static analysis and vulnerability scanning

2-4. Closed middleware

Issues

- ◆ Android Open Source Project (AOSP) is open source for mobile devices. **Google Play Services (GPS) is not open source**, and it was pointed out that some of GPS should be open source.
- ◆ It is **unavoidable that there is a high risk that GPS will not function properly** on devices that do **not comply with the Android Compatibility Definition Document (CDD)**.
- ◆ On the other hand, app stores other than the Google Play store pre-installed in CDD-compliant devices can also use some functions of GPS (solid red arrow in the right figure), but there is **no clear line of demarcation of functions that can be used/cannot be used**.
- ◆ On CDD-compliant devices, GPS also has features necessary for app stores. Thus, to **generate competition among app stores**, it is necessary to **provide such functions**.
 - ✓ When an app developer selects a store to distribute its app, it is important whether the app store provides payment functions and ID linkage as GPS functions necessary for the app to function.



Competition assessment

- ◆ If OS providers refuse to provide APIs required for app stores to third-party app store operators, **a fair and equitable competitive environment among app stores will be hindered**.

Direction of addressing issues

- ◆ Concerns pointed out in the competition assessment may become apparent, when other app stores are allowed by framework described in "2-3"
 - ✓ This concern will be addressed by the **framework described in "2-3"**. Under that framework, providing a development environment that enables apps to be posted on app stores is one of the considerations **regarding whether it is possible to "effectively use" of other app stores**.
 - ✓ Depending on the specific case, the **obligation to allow equivalent access to functions of OS, etc., described in "6-1"**, will be applied

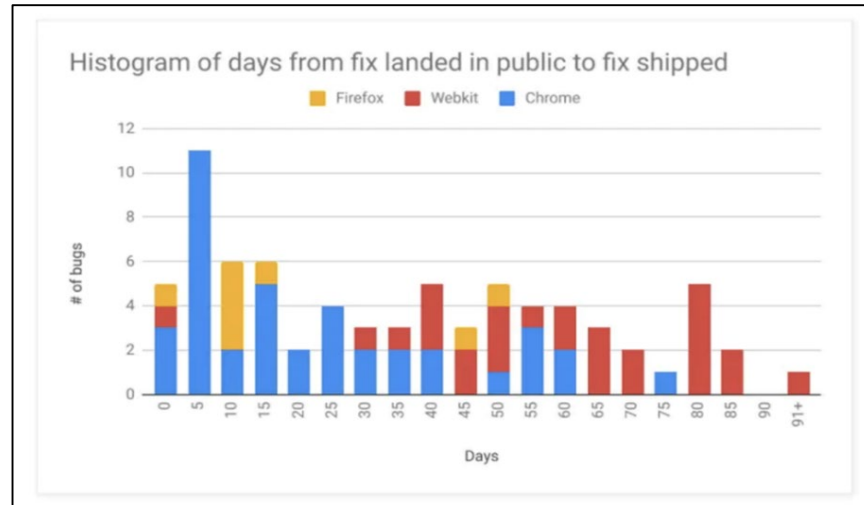
3. Browser functionality restrictions

3-1. Mandatory use of WebKit and reluctance to support web applications ①

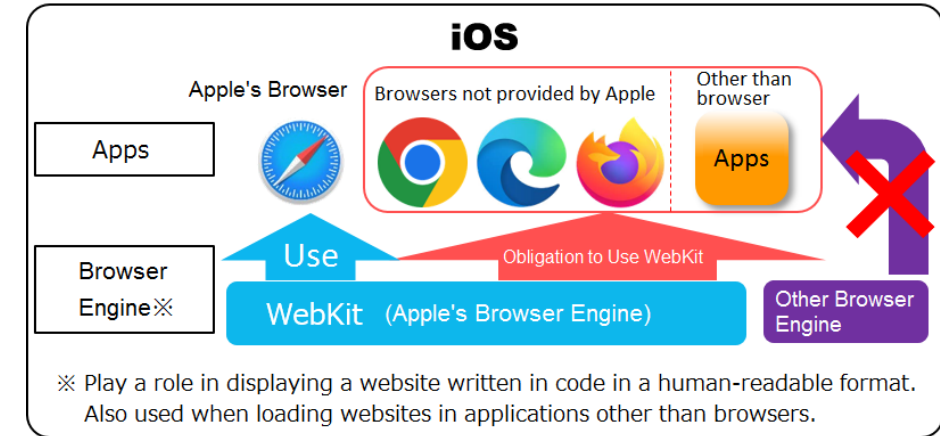
3-2. Access restrictions on browsers to functions of OS, etc. ①

Issues

- ◆ Apple **restricts browser engine on iOS to WebKit** provided by Apple
- ◆ Safari or WebKit has **many unavailable features and poor performance**
 - ✓ **Slower to respond to bugs** when compared to other browser engines
 - ✓ Due to the mandatory use of WebKit, browsers other than Safari on iOS are forced to have the same bugs and functional defects as Safari, and users are **exposed to security risks**.
- ◆ On iOS, **some features** are available only for Safari, and **are/were not available for 3rd party browsers**
 - ✓ Full-screen video, web/app installation capabilities, access to Apple Pay, etc.
- ◆ Safari **lags behind web app support**
 - ✓ The install prompt function is more than 7 years behind native apps in Safari
 - ✓ PWA can be posted on the app store on Android, but iOS does not support this function
 - ✓ Notifications are 7+ years behind other browsers on Android and 13+ years behind native apps



A graph showing the number of days taken to fix issues by browser
(Source: Metrics about bugs reported by Google's Project Zero team)



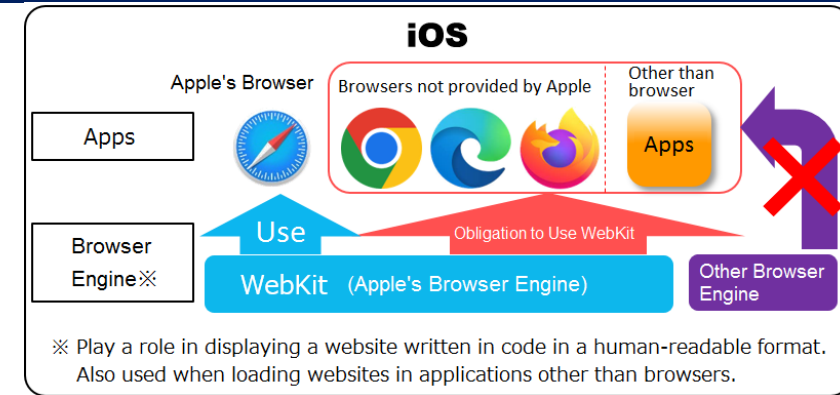
Status of support for web apps by browsers
(Source: Open Web Advocacy)

| | iOS | | | | | |
|------|-------------------------|--------|---------------------------------|------------------|------------------|------------------|
| Rank | Features | Native | Safari | Chrome | Firefox | Edge |
| 1 | Install Prompts | Yes | Rejected (7+Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 2 | Notifications | 2009 | In Development (7+Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 3 | First Class Web Apps | N/A | No Signal (5+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 4 | App Store Support | 2008 | Rejected (14+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 5 | Fullscreen API | 2008 | Rejected (11+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 6 | Badging | Yes | No Signal (5+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 7 | Deep Links | Yes | No Signal (7+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 8 | Screen Orientation Lock | Yes | No Signal (10+ Years) | #AppleBrowserBan | #AppleBrowserBan | #AppleBrowserBan |
| 9 | Bluetooth | Yes | Rejected (5+Years) | #AppleBrowserBan | Rejected | #AppleBrowserBan |
| 10 | NFC | Yes | Rejected (1+Years) | #AppleBrowserBan | Rejected | #AppleBrowserBan |
| | | | | | | |
| | Android | | | | | |
| Rank | Features | Native | Safari | Chrome | Firefox | Edge |
| 1 | Install Prompts | Yes | Apple chose not to port browser | 2015 | No Signal | 2020 |
| 2 | Notifications | Yes | Apple chose not to port browser | 2015 | | 2016 |
| 3 | First Class Web Apps | N/A | Apple chose not to port browser | 2017 | Google Web APK | Google WebAPL |
| 4 | App Store Support | Yes | Apple chose not to port browser | 2019 | Rejected | 2020 |
| 5 | Fullscreen API | Yes | Apple chose not to port browser | 2011 | 2011 | 2015 |
| 6 | Badging | Yes | Apple chose not to port browser | 2020 | Google Web APK | Google Web APK |
| 7 | Deep Links | Yes | Apple chose not to port browser | 2015 | 2017(?) | 2017(?) |
| 8 | Screen Orientation Lock | Yes | Apple chose not to port browser | 2014 | 2012 | 2015 |
| 9 | Bluetooth | Yes | Apple chose not to port browser | 2017 | Rejected | 2017 |
| 10 | NFC | Yes | Apple chose not to port browser | 2021 | Rejected | 2021 |

3. Browser functionality restrictions

3-1. Mandatory use of WebKit and reluctance to support web applications ②

3-2. Access restrictions on browsers to functions of OS, etc. ②



Competition assessment

- ◆ Mandatory use of WebKit **impedes fair and equitable competition between Safari and third-party browsers**
 - ✓ It is difficult to provide functions of third-party browsers, including security, and **the opportunity to select other browsers with excellent security, etc. is deprived**
 - ✓ Users lose the choice of browsers that use browser engines other than WebKit, and are **exposed to security risks**.
- ※ Requiring the use of WKWebView for native apps other than browsers is justified to a certain extent in light of security risks.
- ◆ **Hindering the development of web apps**, the **competition between web apps and native apps is not working well**, adversely affecting the competitive environment in entire mobile ecosystem.
- ◆ If there are features that are only available to OS provider's browser, it **prevents equal footing of competition among browsers**, even if those features become available for the third-party browsers in the future.

Direction of addressing issues

- ◆ **Platform operators that provide OS of a certain size or larger** shall be **prohibited from requiring app developers to use OS providers' own browser engines**
 - ✓ For apps other than browsers, it is acceptable to take necessary and proportional measures to ensure OS and hardware security and privacy.
 - ✓ It is expected that the problem of insufficient support to web apps will be solved by a level playing field among browsers by this obligation.
- ◆ Issues that platform operators that provide OS of a certain scale or larger may **not allow (or delay allowing) other browser vendors to access to the functions of OS, etc. used for their own browsers** is to be dealt with by **obligation to allow equivalent access** to the functions of the OS, etc., as described in "6-2"

3-3. Limitations in browser extensions

Issues

- ◆ Extensions to Chrome are not supported on Android (Nevertheless, third-party browsers other than Chrome are not prevented from supporting extensions)
- ◆ On iOS, extensions to Safari can be installed through App Store, but **third-party browsers are not allowed to support extensions**.
 - ✓ Apple explains that there are time and technical constraints to the testing required to deliver extensions for third-party browsers at present

Competition assessment and Direction of addressing issues

- ◆ For Android, there are third-party browsers with extensions and users already have choices, thus no particular framework is needed
- ◆ For iOS, for the following reasons, this issue is to be dealt with by framework of the obligation to **make the terms of use for business users of app stores fair, reasonable and non-discriminatory**, as described in 2-1
 - ✓ While supporting extensions to Safari, not supporting them to third-party browsers **hinders fair and equitable competition among browsers** on iOS.
 - ✓ It is not reasonable explanation that, for extensions to be allowed, Safari is handled by App Store review and third-party browsers cannot be reviewed due to lack of resources.

4. Pre-installation, default settings

4-1. Pre-installation, default settings ①

Issues

[Android]

- ◆ Google concludes **license agreements, etc. with OEMs**, etc., and **Google's own browsers, search engines, voice assistants, etc. are pre-installed and are set as defaults**, through the decisions of OEMs to which the **monetary incentive are offered by Google** based on a large amount of advertising revenue, etc.
- ◆ OEMs, abiding by contracts with Google, are required to have certain apps non-deletable, while users can remove or disable all pre-installed apps

[iPhone]

- ◆ Apple **pre-installs its own apps**, including Safari, and **sets them as defaults**. Apple adopts Google search as default search engine for iPhone through a revenue sharing agreement with Google
- ◆ About 40 built-in apps are preinstalled, **about a third of which are "operating system apps" that users cannot remove**.
- ◆ When updating iOS, **Apple's apps are sometimes added automatically** without asking for user's consent. Recently, there are many cases where third parties' apps exist, competing Apple's apps being added when updates (fitness, whiteboard apps, etc.)

[Impact on users]

- ◆ Users can switch their default browser or search engine
- ◆ However, according to the survey results, the **status quo bias tends to work** on mobile devices, and the **default settings tend to be difficult to change**.
 - ✓ Browser: As for reason for using the most Safari or Chrome, **over 80%** answered "**since it was installed** from the beginning of use on smartphones" (see graph on next page).
 - ✓ Voice assistant: As for reason for using Siri or Google Assistant, **over 60%** answered "**since it was installed when purchased the device**"
 - ✓ Search engine: **Over 70%** answered they **never changed their default search engine** on their browsers. As for the reason, about 50% answered "since it is hassle to switch to another search engine."

[Impact on businesses]

- ◆ As for reason for conceiving that the **apps provided by Google or Apple** have **competitive advantages** over other apps, **about 55%** answered "because they are **pre-installed**."

4. Pre-installation, default settings

4-1. Pre-installation, default settings ②

Figure 8-17. The reason to have chosen Chrome (Android user)

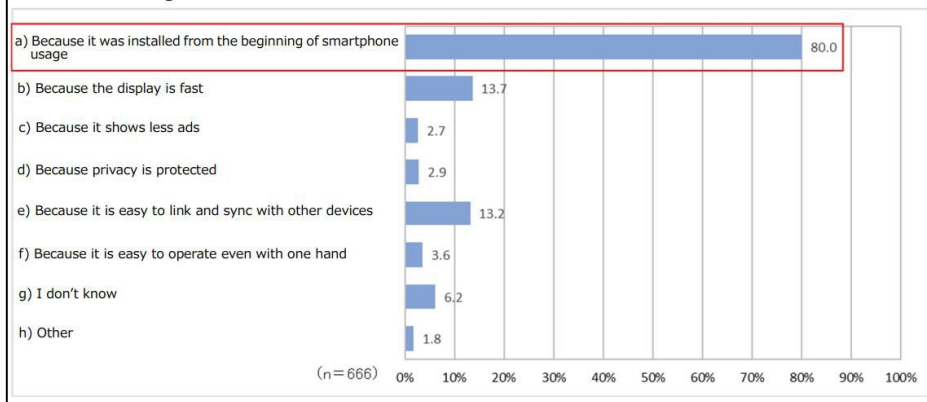
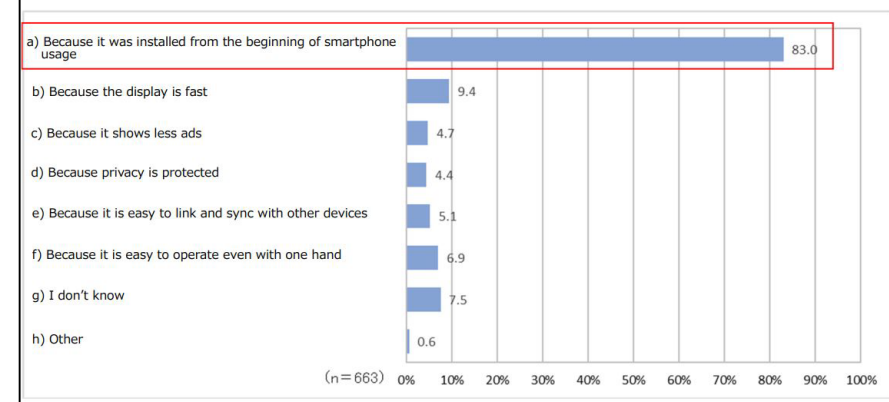


Figure 8-19. The reason to have chosen Chrome (iOS User)



Competition assessment

- ◆ Since (1) Contracts, etc. concluded by OS providers have **an exclusive effect** on competitors, and (2) Users tend to continue to use default services due to the **status quo bias**, **services set as defaults have competitive advantages, hindering user's autonomous decision-making and choice opportunities.**
- ◆ **Automatically installing** their own apps without clearly asking users whether or not to install the apps **puts third parties at a competitive disadvantage, hindering user's autonomous decision-making and choice opportunities.**
- ◆ If **applications cannot be uninstalled** and there is not enough data space, it becomes difficult for third-party applications to be installed. This directly or indirectly causes **disadvantageous situations for third parties.**

Direction of addressing issues

- ◆ **Platform operators that provide OS or browser of a certain size or larger** shall be obliged to do as follows:
 - ✓ Shall **allow and technically enable users to easily change default** settings on their OS or browser, that direct or steer users to their services
 - ✓ Shall **display choice screens** for ① browser, search engine and voice assistant set as default on OS, ② search engine set as default on browser (regardless of whether these apps are theirs or not).
- ◆ Platform operators that provide OS of a certain size or larger shall **display a screen that allows users to choose whether or not to install OS providers' own apps when installing them at the time of OS update.**
- ◆ Platform operators that provide OS of a certain size or larger shall **allow and technically enable users to easily uninstall** pre-installed apps (In certain cases, restrictions on uninstallation are allowed.)

4. Pre-installation, default settings

4-2. Preferential treatment of its own services in its own search service

Issues

- ◆ When searching by query including a certain name of place in Google Search, the search results on **Google Map may be displayed at the top or its vicinity** of the search results.
- ◆ Majority of users are directed from Google search to Google Maps, **putting competing maps at disadvantage**
- ◆ Currently, search results from **various Google's own services (maps, videos, finance, flights, etc.)** are displayed at the top or its vicinity of the organic search results in a separate frames, making it possible to transition to those services.
- ◆ Google explains that it displays search results in different formats to provide more relevant and useful answers. It also explains that this will **improve the quality of search services** and bring **benefits to users and businesses**.

Competition assessment

- ◆ Google Search are set as default and has about 77% market share on the devices including non-mobile devices. In such circumstances, favoring its own services over others of the same type may have **effect of excluding competing services**, which tend to significantly reduce the competition.
- ◆ While Google has a monopoly position in the field of search services, it is in a state of conflict of interest in that it provides its own products and services that compete with other companies. Therefore, it is **highly necessary to deter preferential treatment for its own services**
- ◆ **Differentiation** by means of showing a different frame besides the organic search results will **contribute to user's interests** in terms of improving quality of search results.
- ◆ However, if **only the search results of the company's own service are displayed** in a separate frame and there is **no room for other similar services to be selected**, there is a risk that **competition with competing services will be significantly reduced**.

<Example of display on Google Map>



Direction of addressing issues

- ◆ It is necessary that **platform operators that provide search engines(*) of a certain size or larger should not give their own services any advantage over similar third-party services** in displaying search rankings.
 - ✓ **Concrete framework should be further considered**, based on how to evaluate the display of search engine providers' own services **taking into consideration characteristics and display methods of each service**.
- ◆ Considering the convenience of users, **while allowing Google Map search results to be displayed by default** in a different frame in search result showings, **measures making it easier for users to choose and access other maps** are required * not limited to mobile devices, but applicable to PCs , etc.

5. Acquisition and use of data

5-1. Use of acquired data

Issues

- ◆ Platform operators that provide OS, app stores, or browsers are **in a position to be able to accumulate, use, and retain data** generated on platforms.
- ◆ **Both Apple and Google explain** that they **do not use data** generated or provided by third-party developers to compete with third parties.
- ◆ On the other hand, the **Apple Developer Program License Agreement** prescribes “Apple will be **free to use and disclose any Licensee Disclosures on an unrestricted basis** without notifying or compensating You”.
- ◆ It is pointed out that platform operators **developed and provided apps that have functions equivalent to those provided by third parties’ apps, and incorporated them as OS function**, having a significant impact on the third parties’ business
 - ✓ iPhone's "Find" and "Screen Time", Android's "Step count"
- ◆ From survey results, many developers have concerns about the use of data.
 - ✓ As for reason for conceiving that apps provided by OS providers have competitive advantages over other apps:
 - “**Not only data obtained from app users, but also data (location information, etc.) obtained from OS users can be used**” (50%)
 - “**They are in a position to be able to easily develop apps using their app store usage information (such as data about top-selling apps)**” (35%)

Competition assessment

- ◆ In case platform operators, that provide OS, application store, or browser, **acquire and use data on third-party services** and compete with the third parties **by providing their own services on their own platforms**, those platform operators can compete with the third parties on more advantageous conditions, **hindering a fair and equitable competition environment**.
- ◆ Although Apple and Google acknowledge data should not be used to compete with third parties, **concerns remain unresolved** for the following reasons;.
 - ✓ Uncertainty due to the reliance on voluntary governance by Apple and Google
 - ✓ Difficult to verify the effectiveness of their policies not to use data, from the outside.
 - ✓ Agreement with the developers states that the use of the data is not restricted

Direction of addressing issues

- ◆ **Platform operators, that provide OS, application store, or browser of a certain size or larger**, shall be **prohibited from using non-publicly-available data** generated or provided by third party developers, obtained when the third party developers use the platform provided by the platform operators, **to provide services in competition** with those third parties.
- ◆ Platform operators that provide OS or browser(*) of a certain size or larger shall be **required to disclose** the following:
 - ✓ Disclosure to third parties: Data **acquisition and use conditions** related to products and services provided by third parties, and **governance system** for data acquisition and use
 - ✓ Disclosure to end users: Data **acquisition and use conditions** related to use of OS or browser by users, and **management system** for data acquisition and use

* As to disclosure obligation of browser, it is not limited to mobile devices, but applicable to PCs, etc.

5. Acquisition and use of data

5-2. Opacity of data acquired, etc.

Issues

- ◆ Apple and Google **feedback data to a certain extent to third parties**
- ◆ On the other hand, many developers pointed out that the **types and scope of data** acquired by platform operators **cannot be seen** from outside.
- ◆ As developers are **forced to use the app store provider's payment/billing system**, they are **unable to obtain sufficient information** about users, making it **difficult to smoothly respond to users' requests such as refunds**.

Direction of addressing issues

- ◆ Platform operators that provide OS or browser (*) of a certain size or larger shall be **obliged to disclose** the following::
 - ✓ Disclosure to third parties: Whether data related to products and services provided by third parties **can be obtained by the third parties**, the **content** of the data that can be obtained, the **method and conditions** for obtaining
 - ◆ Concerns about barriers to **communication regarding refunds**, etc. is to **be addressed by monitoring based on Transparency Act**
- * it is not limited to mobile devices, but applicable to PCs, etc.

5-3. Ensuring data portability by end users

Issues

- ◆ **Asymmetrical design** regarding data portability between OSs: Such as iCloud cannot be accessed from Android, and Safari only available on iOS.
- ◆ Browser related data **emigration cannot be completed within a smartphone**: Such as the fact that it is **necessary to use a PC to transfer bookmark data in the case of Safari** on iOS, and **Chrome** on iOS and Android
- ◆ **Lack of data portability** for data related to **application store**: Such as data on app purchases from application stores
- ◆ Questionnaire results show lack or insufficiency of data portability is one of the bottlenecks in switching between OSs.
 - ✓ As for reasons why **chose another smartphone** with the **same OS** (multiple answers allowed), **34%** answered, "it **will take time and effort to transfer data** if change OS."

Competition assessment

- ◆ To facilitate switching and promote competition between OSs, **current state of data portability is lacking in simplicity and sufficiency**.

Direction of addressing issues

- ◆ Platform operators that provide OS, application store or browser of a certain size or larger **shall provide** end users and third parties authorized by end users, at their request and free of charge, **with tools to facilitate the effective exercise of data portability**, and **continuous and real-time access to data**, for enabling effective portability of data provided or generated through the activity of end users in OS, etc.

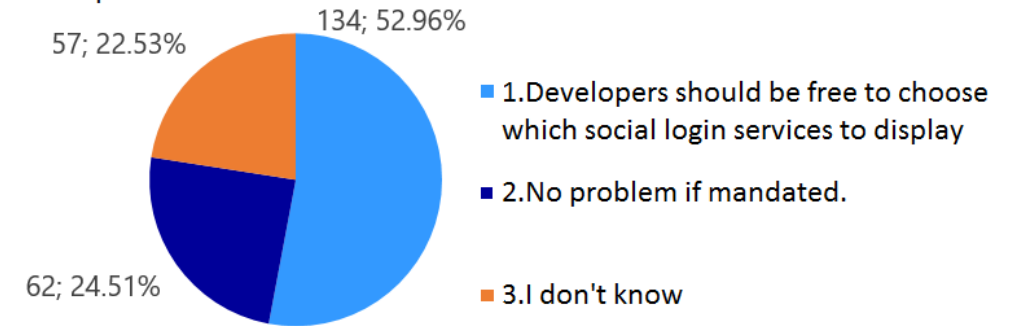
5. Acquisition and utilization of data

5-4. Social Login (“Sign in with Apple”)

Issues

- ◆ **Apple requires app developers to display** Apple's social login option, “**Sign in with Apple**” (SIWA), **only if the app developers offer social login service** provided by other than themselves.
- ◆ Apple explains that **SIWA is a privacy-friendly** login option such that it minimizes the amount of data users need to share and it prevents users from being tracked.
- ◆ On the other hand, regarding SIWA, there are concerns that **maintenance costs have increased** due to the mandatory display of SIWA, that the ID service is **a key for locking in users** and users are prevented from migrating to other services, etc.
- ◆ Survey results from developers show that **more than half** answered that “Developers **should be free to choose** which social login services to display” (see graph on the right).

Q10:In Apple’s App Store, when an app introduces a social login service (a service that enables users to log in with their social network service IDs such as Facebook ID, Twitter ID, etc.), Apple requires app developers to display Sign in with Apple as one of the multiple options. What are your thoughts on this?



Competition assessment

- ◆ This Apple’s conduct is to **use the position of an app store operator to give preferential treatment to its own service.**
- ◆ Social login is **a key factor in locking users into its own service**, and forcing to display its own social login service benefits to Apple
- ◆ Considering the limited display area on smartphone, mandatory display of it also **hinders opportunities for other service to provide services with distinctive privacy functions.**

Direction of addressing issues

- ◆ Platform operators that provide app stores of a certain size or larger **shall not require developers using their app stores to use, to offer, or to interoperate with the platform operators’ own identification service.**

6. Access to functions of OS, etc.

6-1. Access restrictions on apps to functions of OS, etc. (MiniApp)

Issues

- ◆ Apple **prohibits apps** that are subject to app reviews **from implementing MiniApp that call native OS functions** for third parties.
- ◆ It is **difficult to interpret the guidelines accurately**. For example, there is the term "third parties" in the prohibited clause, but the "third parties" for whom is not clear. Furthermore, what specific technical implementations are prohibited are not clear. It leads to **taking time for implementation** in case of such as rejection in app review process.
- ◆ There are also voices of doubt that "**a certain first party is allowed to access** the functions that native apps are allowed to use, by using MiniApp."

Competition assessment

- ◆ If the description of the rules and the judgment of permission are **unclear**, there is a possibility of arbitrary application of the rules and/or differences among app developers, which may **hinder a fair and equitable competition environment among app developers**.

Direction of addressing issues

- ◆ Request clarification of guidelines, fair application review, and appropriate response to inquiries, through the **enforcement of the Transparency Act**
- ◆ As an issue of fairness of app store operation rules, this issue can be dealt with by **framework of the duty to make the terms of use for business users of app stores fair, reasonable and non-discriminatory**, as described in 2-1

6. Access to functions such as OS

6-2. Access restrictions to UltraWideBand

Issues

- ◆ Apple owns its own U1 ultra-wideband chip (UWB), and uses it to recognize nearby devices
- ◆ Apple introduced UWB to iPhone 11 in 2019, but at that time, a developer asked for UWB access, but Apple did not approve it.
 - ✓ Later, in 2021/2022, access to UWB was granted to third parties, with **a several years gap until the access was allowed for third parties**

Competition assessment

- ◆ For several years, only Apple has been able to release apps that use the iPhone's UWB chip, and receive feedback to improve and revamp the apps, resulting in that **equal footing is hindered** by Apple's apps gaining a competitive advantage as first movers, putting others at a disadvantage
- ◆ If there are no effective measures to prevent conducts that impede equal footing, restricting access to other functions will be possible, further strengthening competitive advantage of OS providers.
- ◆ Survey results show that app developers conceive that there is a difference in terms of competition condition with Google or Apple.
 - ✓ As for reasons why competition conditions for the apps provided by Google or Apple are more advantageous (multiple answers allowed), **53.3%** answered "(Google and Apple apps') the functionality is better, **as they have easier/smoothen access to OS functions than apps of others.**"

Direction of addressing issues

- ◆ **Platform operators that provide OS of a certain size or larger shall** allow third parties, **interoperability with**, and access for the purpose of interoperability to, the **same functionalities of OS, etc., as are available to their own services.**
 - ✓ It is **permissible for OS providers to take necessary and proportionate measures** to ensure that **security** of the OS, etc. **is not compromised**, or, depending on the functionalities, **to ensure privacy.**
 - ✓ From the perspective of equal footing, whether or not to oblige free of charge access is to be further considered

6. Access to functions such as OS

6-3. Access restrictions to NFC (Near Field Communication)

Issues

- ◆ While technical specifications for near-field communication (NFC) chips are open for Android devices, in case of **iPhone, they are not open**. Also, **Apple Pay must be used** when accessing iPhone's NFC chip.
 - ✓ Developers cannot create their own apps for touch payments, and when making touch payments, payment data always goes via Apple Pay.
- ◆ There are voices of concern from developers:
 - ✓ Unable to provide users with payment services using NFC chips at stores not accepting Apple Pay, **losing an opportunity to enter business areas where Apple has not entered**.
 - ✓ **Diversity of payment methods** offered to users is **hindered**
 - ✓ **Difficult to develop various services** such as campaigns that could be brought if NFC chip were to be accessed directly without via Apple Pay.
 - ✓ Since NFC specifications have not been disclosed, developers must continue **negotiations and development investments** while it is **unclear whether payments using NFC chips can be technically implemented**.
- ◆ **Apple** explains the reasons for such restrictions, such as allowing unrestricted access may leads to impairing security, **stealing user credentials information**, etc.
 - ✓ In this regard, there is an opinion that other measures, **less anti-competitive than the current one that do not uniformly allow third parties to make payments directly using NFC chips**, can be taken. Such as, in order to deal with the security risk when allowing third parties to use payment services using NFC chips without going through Apple Pay, **access is limited to only third parties that ensure security and privacy**.
 - ✓ **In Germany**, under the Payment Services Supervision Act, payment service providers, who pay usage fees that do not exceed the actual cost of access, should be granted access to technological infrastructure such as NFC chips.

Competition assessment

- ◆ For payment app developers, **opportunity to compete on equal footing with Apple Pay on iPhone is hindered, reducing user choice**.
- ◆ **Unclear** business operations in the process of allowing use of NFC may become a factor of increasing **risks and costs** for payment app developers in their businesses, **hindering competition** between existing businesses, and **adversely affect** on incentives of **new entrants**.

Direction of addressing issues

- ◆ This issue is **dealt with by the obligation to allow equivalent access to functions of OS, etc.**, described in "6-2"

6. Access to functions such as OS

6-4. Time advantage of app development associated with OS updates, etc.

Issues

- ◆ For OS providers, it is **possible for their own app development teams to acquire information** on OS updates and specification changes **ahead of time, and use that information to develop their own apps**.
 - ✓ Apple's pre-installed apps on iPhone have been updated along with beta version of iOS, and it is presumed that OS update information is provided preferentially to its own app development teams
- ◆ OS provider's in-house apps are also **widely tested before release** of OS update, and **enjoy benefits of receiving feedback** and evaluation.
- ◆ Survey results show that app developers conceive that there is a difference in terms of competition condition with Google or Apple
 - ✓ As for reasons why competition conditions for the apps provided by Google or Apple are more advantageous (multiple answers allowed), **38.3%** answered "(Google and Apple apps') **can respond quickly to OS updates.**"

Competition assessment

- ◆ OS providers are in an **advantageous position compared to third-party developers** due to a time advantage in developing apps, etc.
 - ✓ In case, while OS providers can develop apps in-house and respond quickly, they do not provide third-party developers access to the same level of functionalities at the same time.
- ◆ **A fair and equitable competition environment** between OS providers, who are in a position to determine OS specifications, and third-party developers is **hampered**
- ※ Nevertheless, for apps that are **essential to functionalities of OS or device** and **cannot be technically provided** independently by third parties, in order **to prevent problems** with apps due to OS updates, **early access to functionalities is permissible**.

Direction of addressing issues

- ◆ This issue is **dealt with by the obligation to allow equivalent access to functions of OS, etc.**, described in "6-2"

6. Access to functions such as OS

6-5. Access restrictions on voice assistants

Issues

- ◆ **Restrictions on access to functions** related to how voice assistants are activated [Table on the right]
- ◆ With release of Android 12, **Google** grants special permissions to wake word API, **limiting access to wake word function to Google, OEMs, and any third party that OEMs choose.**
- ◆ Apple, Google and OEMs indicates **security, privacy and battery consumption** issues as reasons for restrictions of wake word activation
 - ✓ These issues can be solved, by means of, in addition to current efforts (such as, discarding fragments of voice collected in stand-by before activation, and prior verification by OEMs, app review, etc.), taking advantage of a common platform such as Matter, and limiting voice assistants, safety of which have been confirmed, etc.
- ◆ In addition, **on iPhone**, Siri can make use of **text message reading functions**, calendars, etc., but third parties' voice assistants cannot access them.

| For iOS | Activation by wake word | Activation by pressing and holding a button, etc. | Activation by tapping the app icon |
|---|-------------------------|---|------------------------------------|
| Siri | ○ | ○ | — |
| Third-party voice assistant installed later | × | × | ○ |

| For Android | Activation by wake word | Activation by pressing and holding a button, etc. | Activation by tapping the app icon |
|---|---|---|------------------------------------|
| pre-installed voice assistant | ○ However, how to be activated depends on the model. | | — |
| Third-party voice assistant installed later | × | ○ Possible by changing settings later (depending on the model) | ○ |

Competition assessment

- ◆ Wake word activation is an important feature from user needs, which is shown from survey results:
 - ✓ **About 60%** answered that they activated by speaking to them, **and about 51%** answered that the reason why using voice assistant is “**since they are operational even when their hands are unavailable.**”
- ◆ **Voice assistants installed later** cannot be activated by wake word, leaving competitive disadvantage, **hindering equal footing** with OS providers.

Direction of addressing issues

- ◆ This issue is **dealt with by the obligation to allow equivalent access to functions of OS, etc.**, described in "6-2"
 - ✓ Regarding whether to allow third-party voice assistants to access functions for activation by wake word, there are **concerns about privacy**, so it is assumed that **necessary and proportionate measures can be taken to ensure privacy.**
 - ✓ In case, while it seems that implementation of function is left to decision by OEM, OS provider effectively influences OEM's decision by means of contracts, etc., this issue can be dealt with by prohibiting anti-circumvention measures

6. Access to functions such as OS

6-6. Links with Siri using SiriKit

Issues

- ◆ Apple provides "SiriKit", a mechanism that enables third-party developer apps to interact with Siri
 - ✓ "SiriKit" has only 12 categories, such as messages and workouts
 - ✓ In case of Apple's apps, in addition to above 12 categories, a part of iPhone's standard built-in apps (weather, translation, find, maps, etc.) can be interacted with Siri.

Competition assessment

- ◆ Equal footing is hindered by limiting the scope of third-party developer apps' ability to interact with Siri, compared to Apple's apps' ability to interact with Siri.

Direction of addressing issues

- ◆ This issue is **dealt with by the obligation to allow equivalent access to functions of OS, etc.**, described in "6-2"

6-7 Access restrictions to functions of mobile OS, etc, from smartwatch

Issues

- ◆ When **connecting iPhone and a Wear OS smartwatch using, the usage of Bluetooth Classic is limited** to, for example, hands-free calling. Also, iPhone does not provide a profile for serial communication using Bluetooth Classic for a Wear OS smartwatch.
 - ✓ As a result, **large-capacity data transfer, etc. is restricted**. As an alternative, users have no choice but to choose a method consuming a lot of electricity, such as Wi-Fi, affecting product specifications.
- ◆ **Pairing between Apple Watch and iPhone can be easily performed using Apple's automatic detection function**, etc., which is a proprietary protocol developed by Apple exclusively for communication between Apple devices and is **not offered to third parties**.

Competition assessment

- ◆ For **peripherals**, including smartwatches, it is **important that they can work closely with smartphones**. In such a situation, if Apple Watch can do what a third-party smartwatch cannot do to connect and work with iPhone, **equal footing** between the third party and Apple **is hampered**, making it difficult for the third party to compete on par with Apple.

Direction of addressing issues

- ◆ This issue is **dealt with by the obligation to allow equivalent access to functions of OS, etc.**, described in "6-2"
 - ✓ Including an obligation to allow equivalent access by third-party peripherals in case OS provider's peripherals are allowed to access to the functions

7. Other concerns about voice assistant, wearable

7-1. Monitoring scheme

Background of consideration

- ◆ Concerns identified in the “Interim Report on Competitive Assessment of New Customer Contact Points (Voice Assistants and Wearables)” are:
 - **Concerns between voice assistant providers and app developers / device vendors that work with voice assistants**
 - ✓ Concerns about rule setting, interpretation, and operation within the ecosystem, such as opacity of app reviews and how to deal with specification changes, etc.
 - ✓ Concerns about advantages in the order to present choices by voice
 - ✓ Concerns about data acquisition and use, including the handling of raw data, and restrictions on access to data
 - **Concerns between smartwatch providers and app developers / device vendors that work with smartwatches**
 - ✓ Concerns about self-preferential treatment regarding restrictions on third parties in links of healthcare data
 - ✓ Concerns about self-preferential treatment regarding data handling through restrictions on third parties' access to platform operators' data
 - ✓ Concerns about self-preferential treatment by means of pre-installation and default settings of Apple Healthcare
- ◆ These concerns shall be **improved via competition**, by bringing **competitive environment among voice assistant providers, and among smartwatch providers (*)**.
- ◆ On the other hand, even now, these concerns cannot be overlooked, and expected **harm will become more serious as the market develops**.
- ◆ Thus, it is necessary to build a framework (=monitoring scheme) that allows **(1) relevant authorities to monitor the situation closely, and (2) in case problems become serious, to respond swiftly**.
 * by frameworks related to pre-installation and default settings, obligations of equivalent access to functions, etc.

Specific measures

[Establish information collection system]

- ◆ By posting items to be monitored closely and related information on the website, **receive information**, and **conduct hearings** as necessary
- ◆ Information collection, **surveys and research as necessary**, as to changes in competitive environment and trends in new tech with a huge impact
- ◆ Cabinet Secretariat, in cooperation with relevant ministries, analyzes the situation and **reviews** the necessity of actions (report to WG, etc.)
 - ✓ Accelerated development and implementation of **generative AI**, which might lead to **changes in the role and value of voice assistants**

[Countermeasures in case problem becomes serious]

- ◆ Upon collecting information and analyzing, promptly address, in case problems become serious, by the following measures.
 - ✓ To the extent necessary in light of their jurisdiction and roles, relevant ministries' **prompt policy proposals to encourage relevant businesses' voluntary improvement**
 - ✓ **The Fair Trade Commission's prompt, strict, and appropriate actions** with specific cases that are **problematic under the Antimonopoly Act**, including use of emergency suspension orders.

- ◆ This final report presents **policy mix of two approaches** to address competitive concerns in the mobile ecosystem.
 - ✓ The first one is a regulatory framework (**co-regulation**) that respects the voluntary efforts of platform operators, while the government establishes a general framework of discipline, to improve transparency and fairness regarding rule changes, etc..
 - ✓ The other one is a regulatory framework (**ex ante regulation**) that prohibits or obligates certain types of conduct.
- ◆ Subsequent step is, **based on this final report**, to consider the **legal framework necessary** to ensure a fair and equitable competition environment in the mobile ecosystem, while **assessing the situation in other countries** such as Europe and the United States.
- ◆ For this reason, **public comments** on this final report is to be commenced for soliciting opinions from both inside and outside the country. **Dialogues with relevant stakeholders** as well as **cooperation with relevant authorities in other countries** will be continued.
- ◆ In these ways, by realizing **a fair and equitable competition environment** while **ensuring security and privacy**, it will be aimed to **activate innovation by various entities and ensure opportunities for consumers' choices in Mobile Ecosystem**.
- ◆ It would be grateful to have continued cooperation from stakeholders involved.