プラットフォームサービスに関する研究会

中間とりまとめ（案）

令和3年7月

事務局

目次

はじめに 4

第１部　誹謗中傷や偽情報を含む違法・有害情報への対応について 6

第１章　誹謗中傷への対応に関する現状と課題 6

１　現状と課題 6

（１）　これまでの対策の方向性 6
（２）　流通状況 6
（３）　各ステークホルダーの取組状況 8

２　プラットフォーム事業者等による対応のモニタリング結果 13

（１）　モニタリングの概要 13
（２）　モニタリング結果 15

３　海外動向 24

（１）　欧州連合（EU） 24
（２）　英国 25
（３）　ドイツ 26
（４）　フランス 27
（５）　米国 28

第２章　偽情報への対応に関する現状と課題 30

１　現状と課題 31

（１）　これまでの対策の方向性 31
（２）　流通状況 31
（３）　各ステークホルダーの取組状況 36

２　プラットフォーム事業者等による対応のモニタリング結果 41

（１）　モニタリングの概要 41
（２）　モニタリング結果 43

３　海外動向 50

（１）　欧州連合（EU）..... 50

第３章　今後の取組の方向性 51

１　違法・有害情報への対応 51

①　ユーザに対する情報モラル及び ICT リテラシーの向上のための啓発活動..... 52
②- 1　プラットフォーム事業者の自主的取組の支援 53
②- 2　プラットフォーム事業者による取組の透明性・アカウンタビリティの向上 54
③　発信者情報開示関係..... 59
④　相談対応の充実 59

２　偽情報への対応..... 61

①　自主的スキームの尊重 61
②　我が国における実態の把握..... 62
③　多様なステークホルダーによる協力関係の構築 63
④　プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保63
⑤　利用者情報を活用した情報配信への対応 64
⑥　ファクトチェックの推進..... 65
⑦　情報発信者側における信頼性確保方策の検討..... 67
⑧　ICT リテラシー向上の推進..... 68
⑨　研究開発の推進 69
⑩　国際的な対話の深化..... 70

第２部　利用者情報の適切な取扱いの確保について 71

第１章　プラットフォームサービスに係る利用者情報を巡る現状と課題 71

１　プラットフォームサービスに係る利用者情報の現状と課題..... 71

２　現行制度と政策..... 79

（１）　個人情報保護法及び電気通信事業 GL..... 79
（２）　SPI 及び SPO 80
（３）　位置情報プライバシーレポート 81
（４）　一般社団法人日本インタラクティブ広告協会（JIAA） 81
（５）　デジタル広告市場..... 82
（６）　競争政策とデータ保護・消費者保護の関係 82

３　海外動向 83

（１）　米国 83
（２）　EU 85
（３）　ISO/IEC 90

第２章　プラットフォーム事業者等による利用者情報の取扱いの 92

モニタリング結果 92

１　モニタリングの概要 92

２　モニタリングの結果 94

（１）　利用者情報の取扱いの状況について 94
（２）　利用規約・プライバシーポリシーについて 95
（３）　他アプリやサイトを経由した情報収集 97
（４）　他社へのデータ提供他社との連携の状況 97
（５）　サードパーティーによる情報取得への対応（デジタル広告） 98
（６）　アプリ提供マーケットについて 98
（７）　PIA・アウトカムについて 99

第３章　今後の取組の方向性 100

１　利用者情報の適切な取扱いの確保に向けた論点 100

２　今後の対応の方向性 105

（１）　電気通信事業法・個人情報保護法等を踏まえた対応 105
（２）　電気通信事業 GL・指針等における対応 107
（３）　定期的なモニタリングの実施 114
（４）　専門的な知見の蓄積と発信の重要性 115
（５）　利用者の理解促進・外部レビュー 115
（６）　国際的な対話と連携の推進に向けて 117

おわりに 119

はじめに

インターネット及び携帯電話・スマートフォン等の急速な普及は、個人間のコミュニケーションを容易にするとともに、個人がソーシャルメディアにおいて様々な発信を行うことを可能とした。特に、SNS（ソーシャルネットワーキングサービス）等のソーシャルメディアの利用時間や利用率は近年大きく伸びており、我が国の日常生活や社会経済活動において大きな役割を果たしている。

しかし、インターネット上では、依然として、違法な情報や有害な情報の流通も認められ、昨今、特定の個人に対して多くの誹謗中傷の書き込みが行われるいわゆる「炎上」事案や、震災や新型コロナウイルス感染症などの社会不安に起因する誹謗中傷が行われるなど、特に SNS 上での誹謗中傷等の深刻化が問題となっている。

また、インターネット上でのフェイクニュースや偽情報（以下「偽情報」という。）の流通の問題が顕在化しており、例えば新型コロナウイルス感染症や米国大統領選挙に関するものも含め SNS 上で偽情報が拡散する等これに接触する機会が増加している。

これらの状況を踏まえ、誹謗中傷の問題に関しては、プラットフォームサービスに関する研究会（以下「本研究会」という。）において、2020 年８月に「インターネット上の誹謗中傷への対応の在り方に関する緊急提言」（以下「緊急提言」という。）を公表し、これを受けて、総務省において 2020 年９月に「インターネット上の誹謗中傷への対応に関する政策パッケージ」（以下「政策パッケージ」という。）を策定・公表した。

また、偽情報の問題に関しては、本研究会において、我が国における偽情報への対応の在り方について記載した本研究会の報告書を 2020 年２月に策定・公表した。

本研究会では、誹謗中傷や偽情報の問題への対応に関するこれらの緊急提言、政策パッケージ及び本研究会の報告書を踏まえ、プラットフォーム事業者の取組が十分かどうか、官民の取組が適切に進められているかどうか等について、プラットフォーム事業者からヒアリング等を通じてモニタリングを行うとともに、検証評価を行った。

近年では、スマートフォンや IoT 等を通じた情報流通及び AI を活用したデータ解析による Society 5.0 の実現が志向されており、ポストコロナ時代に向けて、デジタルシフトは更に進んでいくことが想定される。

また、生活のために必要なサービスがスマートフォン等経由でプラットフォーム事業者により提供され、人々の日常生活におけるプラットフォーム事業者の重要性が高

まる中で、より機微性の高い情報についても取得・蓄積されるようになってきている。その中で、様々なサービスを無料で提供するプラットフォーム事業者の存在感が高まっており、プラットフォーム事業者等により利用者情報が取得・集積・活用される傾向が強まっている。

本研究会では、イノベーションや市場の発展を維持しつつ、利用者が安心してスマートフォンやインターネットを通じたサービスを利用していくことができる環境を確保していくことを目的に、我が国における利用者情報の適切な取扱いの確保の在り方について記載した本研究会の報告書を 2020 年２月に策定・公表した。

本年２月には、新たに「プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ」（以下「利用者情報ＷＧ」という。）を立ち上げ、利用者情報の適切な取扱いの確保に関して、プラットフォーム事業者等の取組の状況について把握するためにヒアリング等を通じてモニタリングを行うとともに、検討を進めてきたところである。

本中間とりまとめ（案）は、これまでの検討結果を踏まえ、それぞれのテーマについて、具体的な方策の在り方や今後の検討の具体的な方向性を示すものである。

第１部　誹謗中傷や偽情報を含む違法・有害情報への対応について

第１章　誹謗中傷への対応に関する現状と課題

１　現状と課題

（１）　これまでの対策の方向性

昨今、特定の個人に対して多くの誹謗中傷の書き込みが行われるいわゆる「炎上」事案や、震災や新型コロナウイルス感染症などの社会不安に起因する誹謗中傷が行われるなど、特に SNS 上での誹謗中傷等の深刻化が問題となっていることを踏まえ、本研究会において、2020 年７月にプラットフォーム事業者から誹謗中傷への対策状況についてヒアリングを行い、2020 年８月に「緊急提言」を公表した。その後、「緊急提言」を受けて、総務省において 2020 年９月に「政策パッケージ」を策定・公表し、官学産民で連携を行い、取組を進めてきた。

（２）　流通状況

インターネット上の誹謗中傷対策を進めていく前提として、我が国におけるインターネット上の誹謗中傷の実態を適切に把握することが必要である。

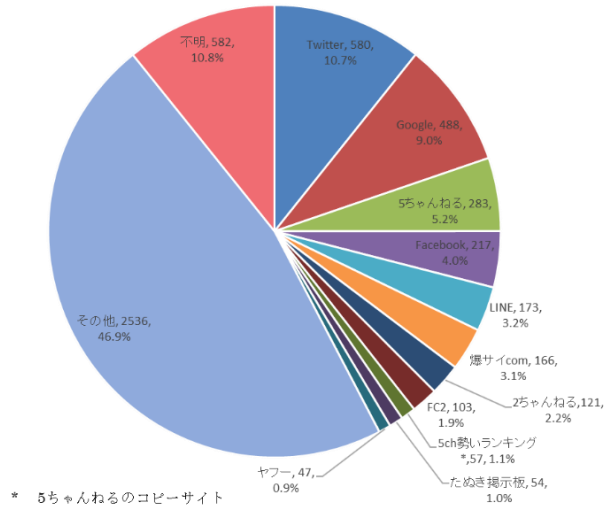
総務省が委託運営を行っている「違法・有害情報相談センター」で受け付けている相談件数は高止まり傾向にあり、令和２年度（2020 年度）の相談件数は、受付を開始した平成 22 年度（2010 年度）の相談件数の約４倍に増加している。総務省は、令和３年（2021 年）２月に、相談（作業）件数の事業者別の内訳を公表した。令和２年度（2020 年度）における相談件数の上位５者は、Twitter、Google、５ちゃんねる、Facebook、LINE となっている。

法務省におけるインターネット上の人権侵害情報に関する人権侵犯事件は、平成 29 年（2017 年）に過去最高（平成 13 年（2001 年）の現行統計開始以降）の件数を更新し、令和２年（2020 年）についても、引き続き高水準で推移している。法務省は、インターネット上の人権侵害情報について、法務省人権擁護機関による削除要請件数と削除対応率について、事業者別の数値（個別の事業者名は非公表）を令和３年（2021 年）２月に公

表した。平成 30 年（2018 年）１月～令和２年（2020 年）10 月の期間内に、5,223 件の事案が人権侵犯事件として立件された。法務局においては、これらについて当該情報の違法性を判断し、そのうち 1,203 件について削除要請を実施したところ、プロバイダ等による削除対応率は 68.08%であった。さらに、法務省は、投稿の類型別（私事性的画像情報、プライバシー侵害、名誉毀損、破産者情報、識別情報の摘示）の削除要請件数及び削除対応率についても公表を行った。

違法・有害情報相談センターの相談（作業）件数の事業者別の内訳

相談（作業）件数の内訳（n=5,407）
＜令和2年度＞



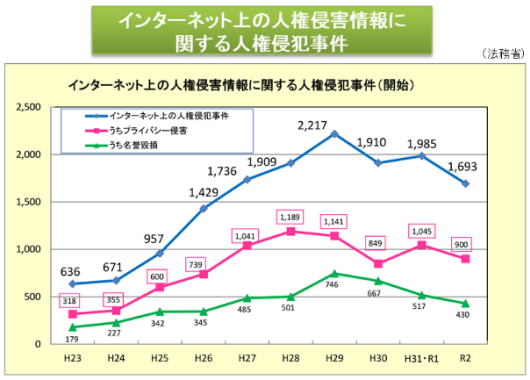
* 5ちゃんねるのコピーサイト

内訳		相談件数	割合
Twitter		580	10.7%
Google（合計）		488	9.0%
	検索	224	
	YouTube	134	
	マップ	103	
	その他	27	
5ちゃんねる		283	5.2%
Facebook		217	4.0%
	Instagram	168	
	Facebook	49	
LINE（全体）		173	3.2%
	livedoor blog/News	120	
	LINEアプリ内サービス	52	
爆サイcom		166	3.1%
2ちゃんねる		121	2.2%
FC2		103	1.9%
5ch勢いランキング＊		57	1.1%
たぬき掲示板		54	1.0%
ヤフー		47	0.9%
	検索	6	
	知恵袋	21	
	ファイナンス	3	
	オークション	6	
	その他	11	
その他		2536	46.9%
不明		582	10.8%

注1　相談（作業）件数を集計したものであり、個別の相談が権利侵害にあたるか相談センターでは判断していない。
注2　作業件数1件ごとの代表的なドメインを入力し集計したものであるため、該当箇所が複数サイトに及ぶ場合などがあり、厳密な統計情報とはならない。
注3　独自ドメインを利用しているものがあり、実際のドメインが判明しない場合がある。

出典：本研究会（第 23 回）資料４（違法・有害情報相談センター提出資料）
をもとに時点更新を行い総務省作成

インターネット上の違法・有害情報の流通状況



・平成30年１月～令和２年10月の期間内に、人権侵犯事件として立件された事案が5223件。法務局においては、これらについて当該情報の違法性を判断し、そのうち1203件について削除要請を実施したところ、プロバイダ等による削除対応率は68.08%。

また、有識者の分析結果[1]によると、2020 年４月のネット炎上件数は前年同月比で 3.4 倍であり、2020 年の炎上件数は 1,415 件となっている。

インターネットのような能動的な言論空間では、極端な意見を持つ人の方が多く発信する傾向がみられる。過去１年以内に炎上に参加した人は、約 0.5%。１件当たりで推計すると 0.0015%（７万人に１人）。書き込む人も、ほとんどの人は炎上１件に１～３回しか書き込まないが、中には 50 回以上書き込む人もいるなど、ごく少数のさらにごく一部がネット世論を作る傾向が見られるとの指摘がある。

また、炎上参加者の肩書き分布に特別な傾向は見られない。書き込む動機は 「正義感」（どの炎上でも 60～70%程度）。社会的正義ではなく、各々が持っている価値観での正義感で人を裁いており、多くの人は「誹謗中傷を書いている」と気付いていないという分析結果が挙げられた。

（３） 各ステークホルダーの取組状況

① ユーザに対する情報モラル及び ICT リテラシー向上のための啓発活動

総務省では、ユーザに対する情報モラル及び ICT リテラシーの向上のための様々な啓発活動を実施している。

具体的には、2020 年９月にインターネット上の誹謗中傷に関する注意事項等をまとめた「インターネットトラブル事例集（2020 年版） 追補版」を作成・公表し、学校等への周知を実施した。追補版公表にあたっては、総務省としてスマートフォンでの閲覧を考慮した啓発ウェブページを作成したほか、内閣府大臣官房政府広報室と連携して広告を掲載、関係省庁・関係団体と連携して全国の学校等や SNS ユーザ等へ周知するなど、様々なチャネルを活用して周知を実施した。

また、学校等での出前講座「e-ネットキャラバン」の講座内容にインターネット上の誹謗中傷に関するものを追加した。

さらに、SNS のより良い利用環境実現に向けたスローガンとして、また、SNS で悩んでしまった際に役立ててもらうため、「#NoHeartNoSNS」の特設サイトを開設し、周知を実施した[2]。

---

[1] 山口真一准教授発表（本研究会（第 26 回）資料３「わが国における誹謗中傷・フェイクニュースの実態と社会的対処」）

[2] 主催：法務省人権擁護局、総務省、一般社団法人ソーシャルメディア利用環境整備機構、一般社団法人セーファーインターネット協会。後援：消費者庁。協力団体：電気通信事業者団体等７団体

② プラットフォーム事業者の自主的取組の支援と透明性・アカウンタビリティの向上

法務省人権擁護機関は、重大な人権侵害事案において、名誉毀損、プライバシー侵害等に該当する場合には、被害者からの人権相談を端緒として削除要請をサイト運営者に対して行っている。

この点、総務省は法務省と連携し、法務省人権擁護機関からの削除依頼を踏まえサイト運営者による迅速な削除等の対応が行われる環境を整備するため、プラットフォーム事業者や業界団体等との意見交換の場となる実務者検討会を継続的に開催している。法務省人権擁護機関への相談事案に関する認識について関係者間で共有を図るとともに、法務省人権擁護機関からの申告について透明性の向上を行い、サイト運営者による円滑な対応を促進している。

また、法務省人権擁護局は、公益社団法人商事法務研究会が主催し、2021 年４月から開催されている「インターネット上の誹謗中傷をめぐる法的問題に関する有識者検討会」に参加し、削除要請に関する違法性の判断基準や判断方法等の議論に積極的に関与している。なお、同有識者検討会には、総務省も参加している。

さらに、官民連携の取組として、2021 年４月には、「YouTube 公認報告者プログラム」に法務省人権擁護局が参加した。コミュニティガイドライン違反報告に資するツールが使用可能となり、法務省人権擁護機関からの報告が優先的な審査の対象とされるなどすることにより、法務省人権擁護機関から YouTube に対する削除要請への円滑な対応が期待される。

民間における取組としては、一般社団法人セーファーインターネット協会（SIA）は、2020 年 6 月より、「誹謗中傷ホットライン」の運用を開始した。インターネット上で誹謗中傷に晒されている被害者からの連絡を受け、コンテンツ提供事業者に、各社の利用規約に基づき削除等の対応を促す通知を行っている。

2020 年の連絡件数は 1,237 件であり、そのうち、ガイドラインに基づき削除通知対象となる「特定誹謗中傷情報」に該当するものが 293 件

（22.4%）、非該当が 944 件（77.6%）[3]であった。293 件のうち、973URL に対して削除通知を行い、削除確認されたものが 836URL（削除率 85.9%）であった。

誹謗中傷等への対応に関しては、国際的な対話が深められることも重要である。この点、総務省では、誹謗中傷を始めとしたインターネット上の違法・有害情報対策に関する国際的な制度枠組みや対応状況を注視し、対応方針について国際的な調和（ハーモナイゼーション）を図るため、国際的な対話を実施している。

具体的には、2021 年２月～６月に、第 26 回日 EU・ICT 政策対話、第 11 回日 EU・ICT 戦略ワークショップ、第５回日独 ICT 政策対話、第 21 回日仏 ICT 政策協議を実施した。日本側からは、「インターネット上の誹謗中傷（Online Harassment）」及び「フェイクニュース（“Fake news” & disinformation）」に関する政策動向を紹介した。

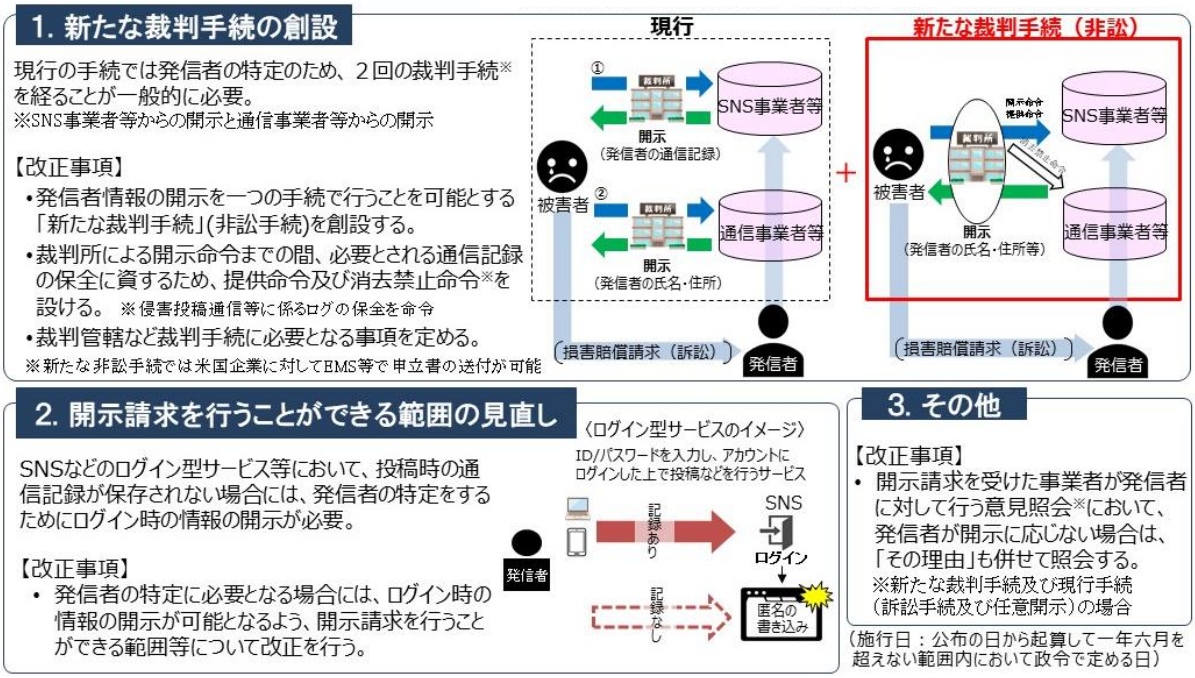
また、2021 年４月に、Ｇ７デジタル・技術大臣会合が開催され、「Internet Safety Principles」に関する合意文書を含む大臣宣言が採択された。「Internet Safety Principles」の中で、特に、事業者の違法・有害情報への対応措置に関する透明性・アカウンタビリティを世界・国・地域のレベルにおいて果たすことが求められるとされた。

③　発信者情報開示に関する取組

総務省は、インターネット上の誹謗中傷等による権利侵害についてより円滑に被害者救済を図るため、①発信者情報開示について新たな裁判手続（非訟手続）を創設し特定の通信ログを早期保全すること、②開示対象となるログイン時情報を明確化すること等を内容とする、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号。以下「プロバイダ責任制限法」という。）の改正を実施し、2021 年４月に改正法が公布された。

[3] 集計期間：2020 年 6 月 29 日～2020 年 12 月 31 日

プロバイダ責任制限法の一部を改正する法律（概要）（令和３年４月 28 日公布）



民間における取組としては、SIA において設置された有識者会議において、2020 年７月から 2021 年３月までの間に、任意開示の促進に向けた施策の検討が行われ、同年４月に「権利侵害明白性ガイドライン」が策定・公表された。また、同ガイドラインに関する理解を深めるため、プロバイダからの同ガイドラインに関する相談を受け付ける窓口が設置された。同ガイドラインは、プロバイダにおける任意開示の判断に際して参照することで、適切な任意開示の促進につながるよう、プロバイダが容易に名誉毀損が明白であると判断可能な類型を示すとともに、参考となる判例を集積したものである。

また、官民連携の取組として、コンテンツプロバイダ・アクセスプロバイダ・有識者・専門性や実務的知見を有する者が協力して発信者の特定手法について支援協力を行える体制やノウハウ共有を行う場として、2021 年２月以降、「発信者情報開示に関する実務者勉強会」が継続的に開催されている。

④　相談対応の充実に向けた連携と体制整備

相談対応の充実に関して、総務省は、2021 年度より、「違法・有害情報相談センター」における相談員の増員等による体制強化を図るとともに、相談件数・内容の更なる分析を実施予定である。

また、相談内容に応じて相談機関間（法務局、警察、インターネット

ホットラインセンター、セーフライン、誹謗中傷ホットライン、消費者生活相談窓口等）で紹介を行うなど、他の相談機関との連携対応の充実を図ることとしている。

地方自治体においては、人権侵害への取組が重要課題であり、独自の相談窓口が設けられている自治体も存在する。例えば、群馬県は 2020 年 12 月に「インターネット上の誹謗中傷等の被害者支援等に関する条例」を制定・施行し、「被害者への支援」及び「県民のインターネットリテラシー向上」に向けた対策を行うこととしている。「違法・有害情報相談センター」において、群馬県インターネット上の誹謗中傷相談窓口に対して、研修会の実施や、問い合わせを受け付ける体制の整備などの連携を行っている。その他、全国の自治体におけるインターネット関連の啓発資料への同センターの掲載やホームページへの URL 掲載等を実施した。

さらに、ユーザにとって分かりやすい相談窓口の案内を実施するため、インターネット上の誹謗中傷に関する複数の相談窓口に係る案内図を作成し、2020 年 12 月に公表した。その後、案内図を様々な方法で全国に周知広報を実施している。

２　プラットフォーム事業者等による対応のモニタリング結果

（１）　モニタリングの概要

主要なプラットフォーム事業者における誹謗中傷等への対策状況について、サービス概要とポリシー、削除等の対応、削除要請や苦情に関する受付態勢・プロセス、発信者情報開示への対応、その他の取組及び情報分析・公開に関して、ヒアリングシートに基づく回答を求め、モニタリングを行った。

プラットフォーム事業者における
誹謗中傷等への対策状況に関する主なモニタリング項目

項目１　サービス概要とポリシー
項目２　削除等の対応
項目３　削除要請や苦情に関する受付態勢･プロセス
項目４　発信者情報開示への対応
項目５　その他の取組
項目６　情報分析･公開

モニタリングにおける主な論点は以下のとおり。

・プラットフォーム事業者の削除等の取組が適切に行われているかどうかについて、主な評価項目に関して、透明性・アカウンタビリティの確保が図られているか。
・特に、海外事業者において、諸外国で行われている取組は我が国においても行われているかどうか。
・AI を用いた削除対応が行われているか。
・過剰な削除や不当なアカウント停止等の行き過ぎた対応が行われていないか。
・各事業者や事業者団体における啓発活動は十分か。
・削除以外の対策（事業者の創意工夫による対応）が行われているか。
・誹謗中傷等の流通状況に関する分析・調査や、研究者への情報提供が行われているか。

プラットフォームサービス事業者における誹謗中傷等への対策状況ヒアリング　質問項目

1．サービス概要とポリシー
① 対象サービス名
② 加入者数、月間アクティブユーザ数又は書き込み数
③ (i)誹謗中傷等に関して禁止とする情報や行為【★】
(ii)削除等の対応【★】

2．削除等の対応
① 誹謗中傷等に関する申告や削除要請の件数【★】
② 誹謗中傷等に関する申告や削除要請に対する削除件数、削除割合、削除までの平均時間【★】
③ ②以外の誹謗中傷等に関する主体的な削除件数（AIを用いた自動検知機能の活用等）【★】
④ ③についての削除の方法・仕組み（AIを用いた自動検知機能の活用等）
⑤ 不正な申告や削除要請への対策の方法・仕組み、対応件数

3．削除要請や苦情に関する受付態勢・プロセス
① 一般ユーザからの申告・削除要請への受付窓口・受付態勢、対応プロセス【★】
② 申立時における申立者や発信者への通知の有無
③ 対応決定時における通知の内容、理由の記載の程度
④ 一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数【★】
⑤ ④の部署・チームに関する日本国内の拠点の有無、日本における責任者の有無【★】
⑥ 削除等への苦情や問い合わせに対する苦情受付態勢及び苦情処理プロセス
⑦ ⑥の苦情・問い合わせ件数

4．発信者情報開示への対応
①発信者情報開示請求を受けた件数【★】
②開示を行った件数【★】

5．その他の取組
① 普及啓発
② その他の対策（警告表示・ミュート機能等）
③ 取組の効果分析【★】

6．情報分析・公開
① 誹謗中傷等の流通状況に関する分析・調査
② 研究者への情報提供、利用条件
③ 透明性レポートの公開、日本語で閲覧可能か【★】
④ 意見・補足

※【★】は「主な評価項目」

本年については、このヒアリングシートに基づき、本研究会において以下のとおりヒアリングを行うことにより、モニタリングを行った。ヒアリングシートの内容の詳細については、参考３の通りである。

・2021 年２月 25 日　本研究会（第 23 回）
ヤフー、Facebook、Google、LINE、Twitter、SIA、SMAJ

（２）　モニタリング結果

①　総論

モニタリングの結果、プラットフォーム事業者の誹謗中傷等への対応に関する透明性・アカウンタビリティ確保状況には差異が見られた。

ヤフー・LINE は、我が国における誹謗中傷への対応について、具体的な取組や定量的な数値を公表しており、透明性・アカウンタビリティ確保に向けた取組が進められている。

Google は、一部、我が国における定量的な件数が新たに示されているが、構成員限りで非公開となっている情報も残されており、部分的に透明性・アカウンタビリティ確保に向けた取組が進められている。

Facebook・Twitter は、グローバルな取組や数値は公表しているが、我が国における具体的な取組や定量的な数値を公表しておらず、我が国における透明性・アカウンタビリティ確保が果たされていない。

②　各論

主な評価項目（質問項目【★】箇所）に関する各事業者の状況は以下のとおり。

誹謗中傷対策に関するプラットフォーム事業者における透明性・アカウンタビリティ確保状況の主な評価項目の比較

	ヤフー	Facebook	Google	LINE	Twitter
1 対応ポリシーの策定及び公表（1．③(i)(ii)関係）	◎	◎	◎	◎	◎
2 削除要請件数や削除件数（国内）の公表（2．①②③関係）	◎	×	○	◎	×
3 削除要請対応チームや拠点（国内）の公表（3．①④⑤関係）	◎	×	×	○	×
4 発信者情報開示の件数の公表（4．①②関係）	◎	×	×	◎	×
5 取組の効果分析の実施（5．③関係）	○	△	△	△	△
6 透明性レポートの公開（6．③関係）	×	△	○	◎	○

※　令和3年2月25日モニタリング実施時に事業者から提出されたヒアリングシートにおいて、当該項目について、
◎：十分かつ詳細な記載があった、　○：概ね記載があった、△：一部記載があった、×：記載がなかった
「日本における削除要請件数や削除件数」は一般ユーザからの申告に関する評価、「透明性レポートの公開」については一般ユーザ及び司法機関・行政機関からの申告・要請に関する評価を記載。

また、ヒアリングの質問項目について、事業者が「回答を控えた理由」及び「今後の対応方針」は以下のとおり。

事業者が「回答を控えた理由」及び「今後の対応方針」

事業者名	回答を控えた理由及び今後の対応方針
ヤフー	2．⑥不正な申告や削除要請への対応件数 理由：何をもって「不正な申告や削除要請」であると判断するのかが難しく、数値は計測していない 対応方針：今後、大量申告等の問題が生じた場合は適宜対応を検討していく
Facebook	・コミュニティ規定施行レポートにおいて、国別の内訳を公表していない理由： ①悪意のある利用者が意図的にサービスを悪用する場合、VPNを使って発信元の国を隠すことが多いため、国レベルのデータは信頼性が低くなる ②1つのコンテンツが複数の場所で見られる可能性があるため、コンテンツの数や事前対応率を国別に報告することは困難 ③国レベルのデータではサンプルサイズが小さくなり、データの精度や信頼性が低下する可能性がある ・データの報告義務を規定すると、企業が直面する様々な技術的制限、利用可能なリソース、法的およびプライバシーに関する考慮事項（各国のデータ保護法を含む）を適切に考慮できない可能性がある。特定のデータセットを追跡し報告するための過度に規定的で義務的な要件は、企業側、そして規制当局の両方にとってコストがかかり負担となる可能性があり、そのプラットフォームの安全性を正確に反映していない可能性もある。その結果、イノベーションと成長が損なわれ、テクノロジーの圧倒的な活用がもたらす利益が制限されることになる ・利用者の皆様のためにサービスを向上させ、利用者の皆様の安全性を確保するための投資を継続的に行っていく
Google	2．①(i)一般ユーザーからの報告件数 →YouTubeについて、構成員限りでの公開。報告件数というデータから何らかの有意義な評価を導くことは困難であり、むしろ、受け手をミスリードする可能性が高い。今後、ユーザーに対する透明性を高めていくために適切なデータかどうかという観点で、公開について検討 2．①(i)一般ユーザーからの報告件数、②(i)申告や削除要請に対する削除件数、③主体的な削除件数 →googleマップについて、構成員限りでの公開。政府や裁判所命令以外の要請に関連する数はグローバルでも未公開。今後どのように背景などの説明も含めてわかりやすく公開していくかについて、社内でもう少し議論が必要 2．②削除割合 →コンテンツを削除しない理由は状況によってさまざまであり、削除割合にとらわれることはユーザーが全体像を理解する上で必ずしも得策ではないことから非公開 2．②削除までの平均時間 →施策の有効性を評価するための最も効果的な指標ではない可能性、プラットフォームに対して迅速かつ慎重に作業するよりも対処にかかる時間を早めることを奨励することとなる可能性、平均所要時間の中央値のようなデータと比較をするなど不用意にデータを歪めることを誘導しかねない、といった理由により非公開 2．③主体的な削除件数 →YouTubeについて、グローバルの数字のみ公開。常により良い透明性の在り方を検討しており、フォーマットや日本を含む各国データの取扱についても継続的に検討をし、随時更新していく 3．④一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数 →グローバルな数字のみ公開。常に各拠点のチームが連携して従事しているため、日本だけで切り分けして提示することはできない 4．①発信者情報開示請求を受けた件数、②開示を行った件数 →現在透明性レポートなどで開示している情報以外については、開示を想定しておらず、数字をトラックしていないため非公開
Twitter	・日本における一般ユーザからの誹謗中傷や偽情報に関する申告・削除要請の件数ならびに削除件数については、今後順次公開する予定 ・なお、データの集計頻度や分類方法、公開範囲については社内で検討中 ・一般ユーザからの申告や削除要請に対応する部署の規模については、非公開。サービスごとに直面する課題や受け取る申告・要請は異なっており、求められる対応も異なるため、サービス間の担当者の体制や人数を比較するのは文脈上適切でなく、また、偏った比較となる ・対応部署の拠点については安全性やセキュリティの観点から非公開

※LINEはヒアリングにおいて日本における取組に関する全ての項目に回答済み

事業者からの回答をもとに総務省作成

ア　主な評価項目関係

主な評価項目に関する各事業者の状況は以下のとおり。

誹謗中傷等に関するポリシーについて（１．③(i)(ii)関係）

すべての事業者において、誹謗中傷を含む一定の類型について禁止規定を定めており、削除・警告表示・アカウント停止等の対応を規定し公表している。

日本における削除要請件数や削除件数について（２．①②③関係）

ヤフー・LINEは、2020年７月の本研究会（第19回）でのヒアリングシートと比較して、我が国における一般ユーザからの申告に関する定量的な件数が新たに示されているなど、透明性・アカウンタビリティ確保に向けた取組を進めている。

Googleは2020年７月の本研究会（第19回）でのヒアリングシートと比較して、一般ユーザからの申告に関する件数など、一部、我が国における定量的な件数が新たに示されているが、構成員限りで非公開となっている情報も残されており、日本向けデータ公表のフォーマットについて検討中。

Facebook・Twitter は、2020 年７月の本研究会（第 19 回）でのヒアリングシートと比較して、新たな情報を示していない。グローバルでの数値については公表されているものの、我が国における一般ユーザからの申告に関する定量的な数値を示していない。

一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数や、日本国内の拠点・責任者について（３．①④⑤関係）

すべての事業者において、一般ユーザからの申告・削除要請への受付窓口・受付態勢、対応プロセスが整備されている。ただし、対応する部署・チームの規模・人数や、日本国内の拠点・責任者についての公開状況には差が見られる。

ヤフー・LINE は、我が国における態勢について、定量的な数値により示している。なお、ヤフーは LINE と比較してより詳細な態勢を示している。

他方で、Facebook・Google は、グローバルな態勢については公表しているものの、我が国における具体的な態勢を示していない。Twitter は、日本及びグローバルな態勢について、ともに情報を公開していない。

発信者情報開示の件数について（４．①②関係）

ヤフー・LINE は、我が国におけるプロバイダ責任制限法における発信者情報開示請求に関して、裁判上/裁判外それぞれの請求件数及び開示件数を公表している。

Facebook・Google・Twitter は、我が国におけるプロバイダ責任制限法における発信者情報開示請求に関する数値を公表していない。

取組の効果分析について（５．③関係）

ヤフーは、AI を活用した取組に関して、我が国における取組の効果分析を定量的に示している。

LINE は、サービス上の取組の効果分析を示していないが、相談対応事業の取組の実施件数は示している。

Facebook・Google・Twitter は、取組の効果分析を公開しているが、グローバルの数値であり、我が国における数値を公開していない。

透明性レポートについて（６．③関係）

ヤフーは現時点では作成・公開しておらず、夏頃公開予定としてい

る。

LINE は日本語による透明性レポートを公開しており、我が国における一般ユーザからの申告に関する件数及び司法機関・行政機関からの要請に関する件数を公表している。

Google・Twitter は日本語による透明性レポートを公開しているが、一部を除き[4]、グローバルの数値のみを公開している。

Facebook は日本語によるコミュニティ規定施行レポートを公開しているが、すべてグローバルの数値であり我が国における数値は公開していない。

イ　AI を用いた削除対応関係

主な評価項目以外の項目に関して、AI を用いた削除対応が行われているかという観点については以下のとおり。

AI 等を用いた削除対応について（２．④関係）

各事業者において、積極的に AI を活用した削除等の取組が進められている。

ヤフーは、「Yahoo!ニュース コメント」において 2014 年から機械学習による不適切投稿への対応を開始。AI による検知を通じて、1 日平均約 29 万件の投稿のうち、約 2 万件の不適切な投稿（記事との関連性の低いコメントや誹謗中傷等の書き込みなど）の削除を実施している。

Facebook は、AI を活用して不適切なコンテンツを検出。AI は、コンテンツレビュアーがレビューするケースに優先順位をつけて、最も有害で時間的な問題のあるコンテンツを最初に処理できるようにしている。

Google は、機械学習を活用して不適切なコンテンツを検出している。有害なコンテンツのほとんどがシステムによって一度も視聴されずに削除されている。

LINE は、機械的なチェックにより、禁止用語やルールと照合し、規約や法令に反した投稿かどうか確認し、自動で非表示化している。全サービスにおいて、わいせつ、出会い系、不快画像等について、AI を活用した「違反画像」を検知している。

Twitter は、テクノロジー（PhotoDNA、社内の独自ツールなど）を活

[4] Google は YouTube の我が国における一般ユーザからの申告に関する削除件数と、日本の司法機関・行政機関からの要請に関する件数を公表している。Twitter は日本の司法機関・行政機関からの要請に関する件数を公表している。

用し、違反コンテンツを特定している。

ウ　過剰な削除や不当なアカウント停止の防止関係

主な評価項目以外の項目に関して、過剰な削除や不当なアカウント停止等の行き過ぎた対応が行われていないかという観点については以下のとおり。

不正な申告や削除要請への対策の方法・仕組み、対応件数について （２．⑤関係）

一部事業者から不正な申告や削除要請への対策の方法・仕組みについて回答があった（ヤフーは、すべて人の目で内容を確認、Facebook は、システムの悪用（大量の報告）を防ぐため重複報告を認識する技術を導入）。濫用的な報告に関する定量的な件数については、LINE のみが数値を公表している。

対応決定時における通知の内容、理由の記載の程度について （３．②③関係）

すべての事業者において、システム上可能な場合には対応決定時において報告者や利用者に通知を行っている。理由の記載の程度については、濫用防止を理由に削除可否について詳細な理由を伝えることはできない、どのガイドラインに抵触したかについての情報を記載しているといった回答があった。

削除等への苦情や問い合わせに対する苦情受付態勢 及び苦情処理プロセス、それらに係る件数について（３．⑥⑦関係）

ヤフーは、削除されたユーザからの専用窓口の設置や削除理由の開示フローなどについて検討を進める予定としている。

Facebook・Google・Twitter は、削除等の対応についてシステム上異議申立が可能。特に、Google では、YouTube における削除対応に関して、投稿者に対して再審査を請求するための手順が記載されたリンクを提供し、再審査は最初の削除判断を行った審査担当者とは異なる担当者によって行われるといった工夫が行われている。

LINE は、異議申し立てについて適宜対応することとしている。

なお、すべての事業者において、一度決定が行われた後に異議があった詳細な件数等については公開していない。

エ　啓発活動

主な評価項目以外の項目に関して、各事業者や事業者団体における啓発活動は十分かという観点については以下のとおり。

普及啓発について（５．①関係）

各事業者や団体において、自らのサービスのガイドの公開や、情報モラル教育等、様々な啓発活動が行われている。

ヤフーは、サービスの理解を深めるための各種ガイドをウェブサイトで公開している。各ガイドでは削除される投稿例の追記などを行い、ユーザの理解を推進し、コメントポリシーの遵守を呼びかける文言を投稿ページの目立つ位置に表示している。

Facebook は、サービスの理解を深めるための各種ガイドをウェブサイトで公開している。いじめ防止やオンラインでの嫌がらせなどのリソースを提供するプログラム「みんなのデジタル教室」を公開している。特定非営利活動法人企業教育研究会の協力のもと、デジタルリテラシーに関する授業を提供。若年層の利用者やクリエイターと一緒に安全な利用を考える取組「#インスタ ANZEN カイギ」を実施している。

Google は、無料のデジタルスキルトレーニングプログラム「Grow with Google」を実施している。その他、各種オンライン教材や、サービスの理解を深めるためのウェブサイト「YouTube のしくみ」を公開している。ネット利用に関する調査結果を「中高生インターネット利用白書 2021」として公開し、オンライン教材を拡充している。

LINE は、サービスの理解を深めるための各種ガイドをウェブサイトで公開している。全国の学校や自治体に講師を派遣するワークショップ授業・講演活動等を 2012 年から累計で約 10,000 回以上実施している。LINE みらい財団では、研究者共同で、独自の情報モラル教育教材の開発を行い、ウェブサイトで公開している。

Twitter は、サービスの理解を深めるためのガイドをウェブサイトや公式アカウントで公開している。UNESCO と合同でメディア情報リテラシーのハンドブック「Twitter を活用した教育と学習」を作成している。また、悩み相談を行う NPO への無償広告枠提供等を通じた支援を行っている。

一般社団法人ソーシャルメディア利用環境整備機構（SMAJ）は、法務省人権擁護局・総務省と共同で、SNS のより良い利用環境実現に向けたスローガンである「#NoHeartNoSNS」を発表している。特設サイトを開

設し、被害を防ぐ仕組みや相談先を掲示し、会員社による周知を実施している。また、SMAJのウェブサイトにおいて、会員社が運営するサービスについて、統一されたフォーマットにより、サービスの概要、利用上の注意点、ユーザを保護する機能を紹介している。

オ　削除以外の対策（事業者の創意工夫による対応）

主な評価項目以外の項目に関して、削除以外の対策（事業者の創意工夫による対応）が行われているかという観点については以下のとおり。

削除以外の対策（事業者の創意工夫による対応）について（５．②関係）

ユーザ自らが他のユーザのアカウントやコメント等を非表示・ブロックする機能については、多くのサービスですでに導入されている（ヤフー、Facebook、LINE、Twitter）。

投稿内容について投稿時等に再考・再検討を行う機会を設ける機能（ヤフー導入済、LINE検討中）、ユーザの選択に応じたコンテンツフィルタリング機能（Facebook・Twitter）、返信相手を選択できる機能（Facebook・Twitter）などについては、一部のサービスで導入が進められている。その他、サービスの性質に応じた様々な仕組みが設けられている。

上記の仕組みにより誹謗中傷全般について対応できる可能性はあるものの、一定の短期間の間に大量の誹謗中傷が集まった場合に対応する特別な仕組みを導入している例は見られなかった。

各社の具体的な取組は以下のとおり。

ヤフー：自身の選択により書き込みや利用者の非表示・ブロック、低品質投稿の機械的検出と折りたたみ表示（知恵袋）、AIを活用した投稿時における注意メッセージの掲出（ニュースコメント、2020年度開始）、一度投稿停止措置を受けたユーザが再度アカウントを作成した場合の投稿制限等

Facebook：自身の選択により書き込みや利用者の非表示・ブロック、タグ付けや返信等を許可する相手を選択する機能、ブロックした人の別アカウントによる望まないやりとりの自動検知・防止、ポジティブなコメントを固定、不適切なコメントを自動的に非表示するフィルタ機能

Google：利用規約上ボーダーライン上のコンテンツ等をおすすめ機能

に表示しない機能

LINE：自身の選択により書き込みや利用者の非表示・ブロック、18 歳未満のユーザ検索機能制限、誹謗中傷やスパムなどについて AI を活用して検知し投稿前に警告する機能を開発中（2021 年下半期までに全てのサービスに実装予定）、一般社団法人全国心理業連合会と連携した無料相談窓口（心のケア相談）の開設

Twitter：自身の選択により書き込みや利用者の非表示・ブロック、返信できるユーザの範囲を選択する仕組み、センシティブな内容を非表示にするフィルタ機能（セーフサーチ）

カ　分析・調査

主な評価項目以外の項目に関して、誹謗中傷等の流通状況に関する分析・調査や、研究者への情報提供が行われているかという観点については以下のとおり。

誹謗中傷等の流通状況に関する分析・調査について（６．①関係）

一部事業者から、有識者との意見交換や、内部での分析・検討が行われているという回答があった。分析結果については、透明性レポート等により公開している事業者が見られた。

研究者への情報提供について（６．②関係）

Twitter では、無償の学術研究プロダクトトラックによる研究者への情報提供が行われているとの回答があった。その他の一部事業者からは、外部有識者との連携が行われているという回答があった。

（３）　事業者団体等のその他の取組

業界団体等の取組により、ノウハウやベストプラクティスを事業者間で共有されているかという観点については以下のとおり。

ヤフーは、不適切コメントへの対策として導入している AI の API を他社に対して無償提供し、業界全体の不適切投稿の削減につなげようという取組を行っている。

SIA は、前述のとおり、「誹謗中傷ホットライン」を運営し、被害者からの誹謗中傷に関する連絡を受け付け、他の事業者に対し、各社の利用規

約に沿った削除等の対応を促す通知を行っている。

SMAJ は、SMAJ 会員各社の SNS 等のサービスにおいて、名誉毀損や侮辱等を意図したコンテンツを投稿するなどの行為を禁止し、利用規約に記載するとともに、禁止事項について啓発広報を実施することを推進している。禁止行為への対応の実効性向上のため、これまで各事業者が実施してきたソーシャルメディアにおける課題に対する取組を体系化した「ユーザー保護ナレッジデータベース」構築等を通じて、継続的かつ実効性のある利用者保護施策を検討・実施している。

３　海外動向

欧州や米国における諸外国の政策動向として、我が国と同様に、プラットフォーム事業者の違法・有害情報対策に関する透明性やアカウンタビリティ確保を求める方向性で検討が進められている。ただし、透明性・アカウンタビリティ確保の方法論として、法的規制によるか否かでは差異がある（欧州では法的規制の検討が行われている）。

また、欧州のうちドイツやフランスなど一部では立法によりプラットフォーム事業者に対して削除の義務付け等の法的規制が導入・検討されているが、表現の自由への萎縮効果の懸念の声があがったり、立法後に違憲判決により当該規定が削除されたりするといった状況となっている。

（１）　欧州連合（EU）

2020 年 12 月、欧州委員会は Digital Services Act (DSA)の法律案を公表。DSA は全ての仲介サービス提供者(プラットフォーム事業者等)に対して、違法コンテンツの流通に関する責任を規定するとともに、事業者の規模に応じたユーザ保護のための義務を規定している。

対象事業者は、仲介サービス（ISP 等)、ホスティングサービス、オンライン･プラットフォーム(オンラインマーケットプレイス､アプリストア、SNS 等)、超大規模オンラインプラットフォームを提供する事業者となっている。

仲介サービス提供者の違法コンテンツに対する責任について、「単なる導管」､「キャッシング」､「ホスティング」の 3 類型に分けて違法コンテンツに対する免責条件を規定。一般的モニタリング義務は無いものの、司法及び行政当局からの削除等の措置命令･情報提供命令への報告義務を規定している。

透明で安全なオンライン環境のため、事業者の希望に応じて、具体的に以下の義務を規定している。

・全ての仲介サービス提供者に対する義務：コンテンツモデレーション

措置を定めた利用規約の公開、透明性報告義務[5]、連絡窓口・国内法定代理人の設置等

・ホスティングサービス提供者の義務：違法コンテンツの通知受付態勢整備、違法コンテンツへの対応に関する理由の通知等

・オンライン・プラットフォームの義務：違法コンテンツへの対応に関する苦情受付態勢整備、裁判外紛争解決機関の利用、信頼された旗手（trusted flagger）、不正な通知・反論に対する対策、オンライン広告の透明性確保[6]等

・超大規模オンライン・プラットフォームの義務：サービスのリスク評価実施・リスク軽減措置の実施、外部監査の実施・公表、レコメンダー・システム、オンライン広告の透明性の追加[7]、規制当局及び研究者のデータアクセス、コンプライアンス・オフィサー設置、行動規範、危機対応等

モニタリング及びエンフォースメントに関して、各加盟国は DSA の執行責任者であり調査権限等を持つデジタルサービス調整官を設置しなければならないとされている。欧州委員会は超大規模オンライン・プラットフォームに対してモニタリングを行い、義務違反の場合、前年度の総売上高の最大 6%の罰金等を科すことが可能となっている。

（２）　英国

2019 年 4 月 8 日、デジタル・文化・メディア・スポーツ省(DCMS)と内務省が共同で「Online Harms White Paper」を作成し、公表した。英国における安全なネット環境の確保を目的とした将来の政府の対策を明示している。主な内容は以下のとおり。

・オンライン上の有害コンテンツ・行為への対処を求めることを目的とする法定の注意義務を策定し、プラットフォーム事業者は、当該注意義務を遵守することが求められる。

・注意義務が遵守されているか監視・評価するために、罰則や罰金等の執行権限を持つ独立規制機関を設置。

---

[5] 違法コンテンツの通知件数・削除件数、自発的なコンテンツモデレーションの内容、対応に関する苦情の件数等。事業者の規模に応じ、透明性義務の内容を追加。

[6] 広告であること、広告主及び広告表示決定に用いられた主なパラメータ等を表示。

[7] 広告表示から１年後まで、広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂・API を介して一般に利用可能とする。

・規制機関は、設定された注意義務の履行・遵守方法を概説したものを行動規範として作成・提示。プラットフォーム事業者は、行動規範に規定されているガイドラインに従うか、あるいは自社の代替アプローチがどの程度効果的に同等以上の影響をもたらすかを説明し、正当化する必要がある。

2020 年 12 月、Online Harms White Paper のパブリックコメント結果に対する政府の完全な対応を公表。主な内容は以下のとおり。

・対象とする情報の範囲については、白書の案と同様に、違法なコンテンツだけでなく、違法ではないが有害なコンテンツも規制。ただし、具体的な有害なコンテンツ・行為は示さず、有害なコンテンツや活動の一般的な定義（オンライン上のコンテンツ・行為が、個人の身体的または心理的に重大な悪影響を及ぼすと合理的に予見可能なリスクを生じさせる場合）を規定。これに該当する誤情報・偽情報も範囲に含むと規定。

・サービスの規模等に応じた段階的な規制を規定（低リスクのサービスに対する免除を導入、リスクが高くリーチ力のある少数のサービスをカテゴリー１と分類し、当該サービスを提供する企業の規制を強化）。

・執行機関については、OFCOM がその役割を担う。

2021 年５月、オンライン安全法案のドラフト（draft Online Safety Bill）を公表した。

（３）　ドイツ

ドイツ国内の登録者数が 200 万人以上のソーシャルネットワーキングサービスは、「ネットワーク執行法」（2017 年 10 月発効）に基づき、透明性レポートを半年に 1 回公開する義務がある。ネットワーク執行法に基づく透明性レポートでは、違反報告数、削除件数、違法な投稿の防止のための取組、報告への対応に関する社内態勢などの事項等について記載が求められる。

削除の要否等について各事業者で判断しかねる事例については、認定自主機関(FSM)に相談して、判断を委ねる仕組みとなっており、2020 年には 13 件の相談があった。

連邦司法庁は、コンテンツが削除されなかったことが「制度上の機能不

全」に基づく場合に、秩序違反が認められるとの判断を行う。過料の執行事例としては、Facebook の 2018 年上半期の透明性レポートについて内容に不備があるとの理由により、Facebook に 200 万ユーロの罰金支払いを科した[8]。

2020 年 9 月に閣議決定された同法の評価レポートでは、法の目的はかなりの程度で達成されており、プラットフォーム事業者の違反報告の管理と公的説明責任が大幅に改善されたこと、規則の詳細な実行はまだ不十分であるが、法の構造的な脆弱性によるものではなく、プラットフォーマによる実施の部分的な不十分さによるものであること等が挙げられた。また、法による過剰な削除（オーバーブロッキング）の懸念については、現時点ではオーバーブロッキングの兆候は認められないが、その危険については、常に、また、将来においても真摯に考慮しなければならないこと等が挙げられた。

2021 年４月に、SNS 事業者に対し、特定の重大事案について、投稿を削除するのみならず、犯罪構成要件に該当する投稿内容及び投稿者に割り振られた IP アドレス等について捜査機関に通報する義務を課すネットワーク執行法の改正法が施行された。

（４）　フランス

2020 年 5 月に、オンライン・ヘイトスピーチに対処することを目的として、インターネット上のヘイトコンテンツ対策法が議会で可決されたが、憲法院に付託され合憲性の審査が行われた結果、コンテンツの過剰削除を促進する可能性があるとして、大半の条項が違憲とされた。その後、違憲とされた条文を削除する形で 2020 年６月に同法は公布・施行された。

改正法の原案では、

①違法コンテンツの削除等（コンテンツ編集者・ホスティング事業者に対し、テロの扇動・称揚や児童ポルノ拡散に係る違法コンテンツについて、行政機関からの通知受領後 1 時間以内の削除又はアクセス不能化を義務付け）

②罰金額引上（上記①や違法コンテンツ対策に関するプロバイダの既存の各種義務に違反した者に課す罰金の額を 7 万 5000 ユーロから 25 万ユーロ（法人の場合は最大 125 万ユーロ）に引き上げ）

[8] これまで罰金が課せられた事例はこの 1 件のみとされている。

③違法コンテンツの削除等(オンライン・プラットフォームに対して、ヘイトスピーチ等を含む明らかな違法コンテンツについて、通報から24時間以内の削除等を義務付け、当該義務に違反した者に25万ユーロの罰金)

④オンライン・プラットフォームへの命令・罰金（視聴覚高等評議会(CSA)は、ヘイトスピーチ等に関する明らかな違法コンテンツのオンライン拡散対策に係る各種義務を遵守させるため命令を行うことができ、従わない場合に最大で2,000万ユーロ又は前年度世界年間売上高の 4%のいずれか高い方を超えない額の金銭的制裁を科すことができる）

といった４つの内容が規定されていたが、①・③・④について違憲判断が下され、条文が削除された。

（５）　米国

通信品位法(1996年)第230条では、プロバイダは、①第三者が発信する情報について原則として責任を負わず、②有害なコンテンツに対する削除等の対応(アクセスを制限するため誠実かつ任意にとった措置)に関し、責任を問われないとされており、プロバイダには広範な免責が認められてきた。

近年、プラットフォーム事業者が米国議会の公聴会に出席を求められ、インターネット上の違法・有害情報対策及び通信品位法 230 条に関して議論が行われている。

共和党政権時代には、プラットフォーム事業者の政治的偏向や、政治的発言に対する検閲への懸念から、2020 年５月にトランプ大統領（当時）が、「プラットフォーマによるオンラインの検閲の防止に係る大統領令」に署名した。オンライン上の言論の自由を確保するため、プラットフォーマによる、恣意的なユーザ投稿の削除等を限定する方向の規制の提案や明確化を連邦通信委員会(FCC)に要請するよう、国家電気通信情報庁(NTIA)に指示を行った。その後、FCCでは同法230条の改正について検討が行われていたが、2021年1月、FCCはトランプ元大統領の選挙敗北を受けて方針を変更し、同法230条を明確化する意向は無いと表明した。

他方、民主党では、テクノロジー企業のモデレーションの欠如と、フェイクニュースや違法・有害コンテンツの発信・拡散に対して同法第230条

が提供する広範な免責規定について懸念が示されている。

2021 年 1 月、大統領選挙結果を巡り、トランプ大統領（当時）の支持者らが米連邦議会議事堂を襲撃する事件が発生した。これを受けて、プラットフォーム事業者各社は、トランプ大統領の行為が暴動を煽ったとして、トランプ大統領の関連アカウントの凍結を行った。加えて、アプリマーケット事業者やホスティング事業者は、トランプ大統領の支持者が利用する SNS サービスに対して、アプリの利用停止やサーバーの利用停止などの措置を取った。

第２章　偽情報への対応に関する現状と課題

近年、インターネット上での偽情報の流通の問題が顕在化している。偽情報に関しては、インターネット上に限った問題ではなく、真偽が不明で信頼性の低い情報（例えばデマや流言飛語など）が人々の間の口コミ等で拡散される事例はこれまでも存在したが、SNS 等のプラットフォームサービスの特性がインターネット上において偽情報を顕在化させる一因になっている[9]と考えられる。

プラットフォーム上において多くの不確かな情報や悪意のある情報が容易に流通・拡散することは、利用者が多様な情報をもとに物事を正確に理解して適切な判断を下すことを困難にし、結果として、利用者が安心・信頼してプラットフォームサービスを利用することができなくなる、また、利用者に直接的な損害を与え得るなど、利用者にとって様々な不利益が生じるおそれがある。さらに、偽情報の流通により社会の分断が生じ、結果として民主主義社会への危機につながるおそれがある[10]との指摘もある。

SNS を始めとするプラットフォームサービスは、経済活動や国民生活などの社会基盤になりつつあり、情報流通の基盤にもなっていることから、また、プラットフォームサービスの特性が偽情報の生成・拡散を容易にし、偽情報を顕在化させる一因となっていると考えられることから、特にこうしたプラットフォーム上の偽情報への適切な対応が求められる。

---

[9] ①SNS では一般の利用者でも容易に情報発信（書込み）や拡散が可能であり、偽情報も容易に拡散されやすいこと、②情報が広範囲に、かつ、迅速に伝播されるなど、影響力が大きいこと、③偽情報は、SNS 上において正しい情報よりもより早く、より広く拡散する特性があることや、SNS 上の「ボットアカウント」が拡散を深刻化させていること、④自分と似た興味・関心・意見を持つ利用者が集まるコミュニティが自然と形成され、自分と似た意見ばかりに触れてしまうようになる（＝「エコーチェンバー」）、パーソナライズされた自分の好み以外の情報が自動的にはじかれてしまう（＝「フィルターバブル」）などの技術的な特性があること、⑤各利用者の利用者情報の集約・分析によって、個々の利用者の興味や関心に応じた情報配信（例：ターゲティング広告）が可能であるなど、効果的・効率的な利用者へのアプローチが可能であることなど。

[10] 選挙の候補者等に関する不正確な情報が流布されることなどによって有権者の理性的な判断が妨げられることで投票結果が歪められたり、政治的分断が深まるおそれや、外国政府が誤った情報を流布することで国家安全保障が揺るがされたりするおそれなども考えられる。

１　現状と課題

（１）　これまでの対策の方向性

近年、米国や欧州において偽情報が社会問題になっていることから、我が国においても近い将来同様の問題が生じ得ることを念頭に、今後の対策を検討すべく、本研究会では、我が国における偽情報への対応の在り方について記載した本研究会の報告書を 2020 年２月に策定・公表した。

報告書に基づき、偽情報への対応の在り方について、多様なステークホルダーによる協力関係の構築、プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保、ファクトチェックの推進、ICT リテラシー向上の推進など、10 の方向性について、官学産民で連携を行い、取組を進めてきた。

プラットフォームサービスに関する研究会 最終報告書（2020年２月）
第６節　我が国におけるフェイクニュースや偽情報への対応の在り方

1　自主的スキームの尊重
2　我が国における実態の把握
3　多様なステークホルダーによる協力関係の構築
4　プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保
5　利用者情報を活用した情報配信への対応
6　ファクトチェックの推進
7　ICTリテラシー向上の推進
8　研究開発の推進
9　情報発信者側における信頼性確保方策の検討
10　国際的な対話の深化

（２）　流通状況

①　偽情報に関する流通状況調査（アンケート調査）の結果

2021 年３月の調査結果[11]によると、直近１か月での偽情報への接触率は 75%であり、３割程度の人は、偽情報に週１回以上接触している。偽情報を見かけることが多いジャンルは、新型コロナウイルス及びスポー

[11] https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_05.html（本研究会（第 26 回）資料１「『フェイクニュース』に関するアンケート調査結果」（NRI））

ツ・芸能系関連となっている。特に、直近１ヶ月の間での新型コロナウイルス関連の偽情報に接触した層は半数程度であり、拡散経験層は３割弱程度となっている。

新型コロナウイルス及び米国大統領選挙に関して間違った情報や誤解を招く情報と判断された[12]個別の 18 個の情報について、それらを信じた場合や真偽不明だと思った際、４割の回答者は情報を共有・拡散していた。2020 年６月の過去調査[13]と比較し、共有・拡散割合は減少傾向（５%減）となっている。共有・拡散した理由は、「情報が正しいものだと信じ、他人に役立つ情報だと思った」(37%)、「真偽不明だが、他人に役立つ情報だと思った」(34%)、「真偽不明だが、情報が興味深かった」(30%)、「他人への注意喚起」(29%) の順に多い。

Twitter (53%)、YouTube (30%) の利用者は、当該サービスにおいて、それらの情報があたかも真実又は真偽不明として投稿されているのを見かけることが多い。過去調査と比較すると、各主要メディア毎に割合は減少傾向にあるが、YouTube は増加（８%増)。

他方、Twitter (40%)、民間放送 (21%) の利用者は、当該サービスにおいて、それらの情報が真実ではない・誤解を招くといった注意喚起を見かけることが多い。過去調査と比較すると、各主要メディア毎に割合は減少傾向となっている（特に民間放送：17%減)。

新型コロナウイルス関連の各プラットフォーム事業者のインフォデミック対策の認知度は全体的に低く、１割程度となっている。

② 偽情報に関する流通状況及び接触状況調査の結果[14]

上記①とは別の調査結果によると、2020 年には、年間 2,615 件（１日平均 7.2 件）の疑義言説が拡散しており、主に新型コロナウイルス関連・米国大統領選挙関連の偽情報が拡散している。

新型コロナウイルス関連 10 件・国内政治関連 10 件の実際の偽情報に

---

[12] 2020 年 4 月 28 日時点で、メディアやファクトチェック機関によるファクトチェックの結果、間違った情報や誤解を招く情報であると判断された情報。

[13] https://www.soumu.go.jp/main_content/000693295.pdf（総務省「新型コロナウィルス感染症に関する情報流通調査」)

[14] 山口真一准教授発表（本研究会（第 26 回）資料３「わが国における誹謗中傷・フェイクニュースの実態と社会的対処」)

関する調査の結果、特に新型コロナウイルス関連の偽情報接触率が高い（45.2%）。10 代の接触率が最も高いが、あらゆる年代層で接触しており、全体で 51.7%の人は 1 つ以上の偽情報に接触している。

偽情報と気づいた割合は、新型コロナウイルス関連が 58.9%、国内政治関連は 18.8%と、ファクトチェック済みの偽情報でも多くの人が偽情報と気付けていない。情報リテラシー（読解力・国語力）が高い人は偽情報に騙されにくい。他方、ソーシャルメディアやメールへの信頼度が高いと偽情報に騙されやすい。また、マスメディアへの不満や自分の生活への不満が高いと偽情報に騙されやすい（特に、国内政治関連の偽情報）。

偽情報の種類によって有効な行動は大きく異なる。新型コロナウイルス関連では「1 次ソースを調べる」「情報発信者の姿勢やトーン、感情を考える」が有効。国内政治関連では「情報の発信主体を確認する」「情報が発信された目的を考える」が有効。また、「ネットで他の情報源を探し、確認する」も全体的に有効。

拡散手段として最も多いのは 「家族・友人・知り合いに直接話した」が 10.3%。次いでメッセージアプリが多く、身近な人への拡散が多い。Twitter は 3 位の 4.3%となっている。

大量の人に拡散した「スーパースプレッダー」は全体で 1%以下しかいないが、拡散数では約 95%を占めるなど、ごく一部の拡散者が偽情報拡散の大部分を広めていた。一方、スーパースプレッダーはソーシャルメディアからの訂正情報で考えを変えやすい傾向にある。

③　偽情報に関するニュースの生態系に関する分析結果[15]

有識者による偽情報に関するニュースの生態系に関する分析結果によると、偽情報は、マスメディアも含めたインターネットにおけるニュースの生態系（生成・拡散の構造）の問題であり、インターネットのニ

[15] 藤代裕之准教授発表（本研究会（第 27 回）資料４「フェイクニュース生成・拡散のメカニズム」）

ュースでは、ミドルメディア[16]が話題や議論の流れに影響を与えているとの指摘がある[17]。

偽情報は、ミドルメディアを中心に、メディア間の相互作用で成長する例が見られ、具体的には、①ソーシャルメディアでの話題をニュースサイト・まとめサイトなどのミドルメディアが編集し、それをマスメディアが取り上げる、②ミドルメディアが、マスメディアの話題とソーシャルメディアの反応を組み合わせてソーシャルメディアに拡散する、③記事配信を通して大きな影響力を持つポータルサイトに到達し、ポータルサイトから、ミドルメディアやソーシャルメディアに拡散する（フェイクニュース・パイプライン）、といった流れの存在が指摘されている。

また、ミドルメディアの典型的な記事の作り方として、「こたつ記事（取材が不十分な、こたつでも書ける低品質な記事）」の問題があり、ネットの反応は多くの場合情報源やデータが提示されておらず、話題の捏造が可能であるとの指摘がある。

この点、コンテンツの内容が間違っていてもページビューを稼げば広告収入で儲かる仕組みにより、正確な記事を書くインセンティブがないため、偽情報の方が「得」な状況となってしまっているとの指摘や、ミドルメディアの多くが運営元がサイトに表示されておらず正体不明であり、運営元を表示しなくても検索結果に表示され、広告収入が得られるとの指摘もある。

さらに、記事の配信や検索表示によりアクセスが流入し、広告収入がミドルメディアの活動を支えており、偽情報を拡散する特定のサイトやソーシャルメディアのアカウントへの対応が不十分で生成・拡散を助長している点や、対策が不十分なことで、既存メディアの記事や映像は偽情報に使われ、間違ったり、歪んだりした内容が拡散してしまっているといった指摘もある。

---

[16] マスメディアとパーソナルメディア（ソーシャルメディアを含む）の中間的存在。ネットの話題や反応を取り上げるニュースサイト、まとめサイト、トレンドブログなどが代表例。

[17] 2017 年の衆議院選挙の偽情報の分析によると、15 個のうち 10 個が twitter、 5 個がミドルメディアが発信源となっていた（https://www.jstage.jst.go.jp/article/jsicr/37/2/37_93/_article/-char/ja/）。

④　SNS における偽情報の拡散状況や人間の認知に関する分析結果[18]

偽情報の拡散要因として、①メディアによる拡散、②人間の非合理性が指摘されている。

具体的な偽情報に関して twitter 上の拡散状況を分析すると、似たような発信・拡散を行う人々の集まり・ネットワーク（クラスター）が複数存在しており、主に陰謀論を発信するクラスター、偽情報を否定するクラスター、面白おかしく反応するクラスターなどが存在している。また、それぞれのクラスターにおいて、政権支持・政権批判を行う人々が積極的に拡散しているケースがみられる。偽情報に触れて積極的に拡散しているのは偏った一部の人々である可能性が指摘されている。

また、以下のとおり、人間の非合理性が、偽情報の拡散に寄与するとの指摘がある。

確証バイアス：先入観の影響により、自らに都合のいい情報に触れると真実だと信じてしまう。

認知的均衡理論：人間には、好きと嫌いとの均衡状態を維持したいという心理があり、自分が好きな人が好きなものを好きなことは安定状態、その逆が不安定な状態となる。偽情報に触れた際、真実性よりも認知的均衡を保つために、自分が好きな人の発言が偽情報であってもそれを信じてしまうことがある。

ソーシャルポルノ仮説：コンテンツを消費して快感を得ることが目的であり、ニュース等を見るときに、情報を得ようという観点よりも楽しもうという観点を重視する態度。この観点により、偽情報が消費・拡散されることがある[19]。

⑤　ディープフェイクの拡散状況

「ディープフェイク」は、「ディープラーニング」と「フェイク」を組み合わせた造語である。現在では人工知能を用いて、実際には存在しないリアルで高精細な人物の映像・動画を制作する行為や、それらで制作

---

[18] 鳥海教授発表（本研究会（第 26 回）資料 2「データから見るフェイクニュース」）

[19] 調査結果によると、偽情報を拡散した人のうち 32.7%は「情報が興味深かったから」という理由で拡散している。

された映像・動画について指すことが多い。対義語として「チープフェイク」[20]が存在する。

ディープフェイクは、海外の事案が多いが、我が国の事例としては、2020 年 10 月にディープフェイクポルノ動画をアップロードしていた 2 人が逮捕された。2021 年４月には、加藤官房長官が福島県及び宮城県を襲った地震に関する記者会見で笑みを浮かべる画像が Twitter に掲載された[21]。

ディープフェイクで作成された動画は増加傾向であり、オランダの情報セキュリティ調査会社によると、2020 年 12 月には 8.5 万件の動画が検出された。2018 年以降、6 か月ごとに約 2 倍のペースで検出数が増加している。国別にみると、米国が 42%と最も高いが、日本は５番目の 5.6%。分野別に見ると、「エンタテイメント」55.9%、「ファッション」23.9%、「政治」4.6%となっている。

（３）　各ステークホルダーの取組状況

①　多様なステークホルダーによる協力関係の構築

偽情報の問題に対しては、多様なステークホルダーによる多面的な議論が行われ、プラットフォーム事業者、ファクトチェック機関、メディアなど関係者間の協力が進められることが必要である。

この点、産学官民が連携した取組として、偽情報流通の実態を正確に把握し、その対応について多面的に検討すべく、産学官民の多様なステークホルダーによる協力関係の構築を図り、対話の枠組みを設けることを目的として、2020 年６月に「Disinformation 対策フォーラム」が設立された[22]。

フォーラムにおける議論のスコープについては、インターネット上の SNS 等で個人のユーザが発信する「デマ」の類を対象とし、①フェイク

---

[20] 動画の再生速度を調整したり、画像編集ソフトを用いて画像の必要な部分を切り取る等の簡単な処理で作成する技術等。

[21] のちに削除されたことが確認されている。

[22] 事務局：一般社団法人セーファーインターネット協会

ニュースを巡る実態・最新の研究成果、②事業者における取組、③関連団体における取組、④今後の取組の方向性を内容とする中間とりまとめが 2021 年３月に公表された。

中間とりまとめの今後の取組の方向性として、①ファクトチェックの取組に関する今後の取組、②リテラシー向上の取組に関する今後の取組、③シンポジウム等の公開のイベントを開催検討する旨が示され、2021 年６月にシンポジウムが開催された。

② ファクトチェックの推進

偽情報の問題に対しては、プラットフォーム事業者の取組だけでなく、ファクトチェックの活性化のための環境整備が進められることが必要である。

この点、ファクトチェックの普及活動を行う非営利団体である「ファクトチェックイニシアティブ（FIJ）」において、我が国におけるファクトチェック普及活動が進められている。

2020 年２月に、FIJ の新型コロナウイルス特設サイトが設置され、日本で流通する新型コロナウイルスに関連する言説・情報のうち、これまでにメディアやファクトチェック機関によってファクトチェックや検証が行われた情報の一覧を表示している。加えて、国外における新型コロナウイルスに関する国外のファクトチェック情報を掲載している。これらの情報は、Yahoo!ニュース、LINE ニュース、グノシー、goo ニュースに掲出されている。

また、2020 年 4 月に、新型コロナウイルスをめぐる日本関連のファクトチェック情報を海外向けに発信するため、FIJ が英語版特設サイトを開設した[23]。日本に関連するファクトチェック情報を英語で公開し、国際ファクトチェック・ネットワークのメンバーに情報提供。海外の団体への調査協力や、日本国内のメディアパートナーのファクトチェック活動に対する支援を強化している。

さらに、FIJ において、メディアパートナーによるファクトチェックの容易化及びファクトチェックの質・量の向上を目的とし、疑義言説集

[23] COVID-19 Japan-related Fact-checks（https://en.fij.info/covid-19/）

約システム（FCC）、疑義言説データベース（Claim Monitor）、ウェブアプリ（FactCheckNavi）等のファクトチェック支援システムを運用している。

Claim Monitor では 2020 年に合計 2615 件の疑義言説を捕捉した。FIJ メディアパートナー（毎日新聞・InFact・BuzzFeed 等）のファクトチェック記事数は、2019 年の計 34 本から 2020 年には計 164 本に増加した。

③　情報発信者側における信頼性確保方策の検討

偽情報の問題に対しては、インターネット上におけるメディア全体の情報の信頼性の確保方策について、メディアやプラットフォーム事業者等の関係者間で検討が進められることが望ましい。

この点、「Disinformation 対策フォーラム」において、一般社団法人日本新聞協会・日本放送協会・一般社団法人日本民間放送連盟がオブザーバ参加し、プラットフォーム事業者・メディア関係団体・有識者との対話や情報共有が進められている。

フォーラムで共有されたメディア関連団体の取組は以下のとおり。

新聞社の取組：全国に取材網や取材拠点を有し、発信前に社内で何重にもチェックするほか、不確かな情報に対する取材や検証、デマを打ち消す記事の発信とともに、誤った情報によって引き起こされた差別や偏見に対しても、対応する記事を発信している。教育界と協力し、NIE（Newspaper in Education）という、教育現場で新聞を活用して情報リテラシーの向上を推進する取組を実施している。

放送事業者の取組：放送法の規律に加え自律的な取組を行っており、日本民間放送連盟は放送倫理基本綱領（日本放送協会と共同作成）、放送基準、報道指針等を定めるほか、SNS 上の情報については、投稿者のプロフィールの確認や投稿者へのコンタクト等を通じて、事実か否か確認の上での報道を行う等の対応を実施している。日本放送協会は SoLT（Social Listening Team）というチームを立ち上げ、SNS の情報をリアルタイムで観察し、事件事故の最新の状況や変化をいち早く捉え、キャッチした一次情報を報道に繋げている。また、「フェイク・バスターズ」という番組の放送により、積極的にファクトチェック情報を発信し、これら取組の方針は、「NHK 放送ガイドライン 2020（インターネットガイドライン統合版）」において公表している。

④　ICT リテラシー向上の推進

偽情報の問題に対しては、政府や各ステークホルダーはリテラシー向上の推進に向けた活動を行い、また、既存の ICT リテラシー向上の取組に係る整理や様々な主体の連携促進が行われることが重要である。

この点、総務省では、偽情報に対抗するリテラシーの向上のための様々な啓発活動を実施している。

具体的には、「インターネットトラブル事例集(2021 年版)」において、エコーチェンバー・フィルターバブル等の SNS の仕組みや、情報を鵜呑みにしないための確認方法を記載し、関係省庁・関係団体と連携して全国の学校等や SNS ユーザ等へ周知するなど、様々なチャネルを活用して周知を実施している。

また、総務省 HP において「上手にネットと付き合おう！～安心・安全なインターネット利用ガイド～」を公開し、ネットの時代における偽情報に関する特集ページに、情報を鵜呑みにしないための確認方法や我が国における偽情報の実態などを周知している。

さらに、「e-ネットキャラバン」の講座内容に、偽情報への対応を追加した。

他方で、既存の ICT リテラシー向上の取組に係る整理や様々な主体の連携促進については、前述の「Disinformation 対策フォーラム」における中間とりまとめにおいて、今後の取組の方向性として、リテラシー向上の取組に関する今後の取組について言及があるものの、現時点では具体的な取組は進められていない。

⑤　研究開発の推進

偽情報の問題に対して、プラットフォーム事業者は、コンテンツモデレーションに関して、AI を活用した技術について研究開発を推進していくことが望ましく、また、ディープフェイクなどの新たな技術による偽情報に対抗する技術に関する研究が進められることが望ましい。

この点、諸外国では、ディープフェイクで作成された動画を検出する

技術・ツールの開発が進められている[24]。マカフィーはAIを活用しディープフェイクの検出を行う「ディープフェイクラボ」を2020年10月に設立した。また、Facebook、Microsoft、米国の大学等が設立したディープフェイク検出技術の公募コンテスト「deepfake detection challenge」が2019年12月～2020年5月に開催された。

我が国では、2020年に科学技術振興機構（JST）の戦略目標「信頼されるAI」のもとで、「インフォデミックを克服するソーシャル情報基盤技術」が採択された[25]。同研究は、「AIにより生成されたフェイク映像、フェイク音声、フェイク文書などの多様なモダリティによるフェイクメディア（FM）を用いた高度な攻撃を検出・防御する一方で、信頼性の高い多様なメディアを積極的に取り込むことで人間の意思決定や合意形成を促し、サイバー空間における人間の免疫力を高めるソーシャル情報基盤技術を確立する。」ことを目的としている。

⑥　国際的な対話の深化

偽情報の問題に対して、国際的な対話を深めていくことが望ましい。

この点、前述のとおり、総務省では、偽情報も含めたインターネット上の違法・有害情報対策に関する国際的な制度枠組みや対応状況を注視し、対応方針について国際的な調和（ハーモナイゼーション）を図るため、国際的な対話を実施している。

具体的には、2021年２月～６月に、第26回日EU・ICT政策対話、第11回日EU・ICT戦略ワークショップ、第５回日独ICT政策対話、第21回日仏ICT政策協議を実施した。日本側からは、「インターネット上の誹謗中傷(Online Harassment)」及び「フェイクニュース(“Fake news” & disinformation)」に関する政策動向等を紹介した。

また、2021年４月に、Ｇ７デジタル・技術大臣会合が開催され、「Internet Safety Principles」に関する合意文書を含む大臣宣言が採択された。「Internet Safety Principles」の中で、特に、事業者の違法・有害情報への対応措置に関する透明性・アカウンタビリティを世界・国・地域のレベルにおいて果たすことが求められるとされた。

---

[24] 例えば、Microsoftの「Video Authenticator」、 Sensityの「DEEPFAKE DETECTION」等が実用化されている。

[25] 研究代表者：国立情報学研究所（NII）越前功教授。 2020年12月から5.5年間。

２　プラットフォーム事業者等による対応のモニタリング結果

（１）　モニタリングの概要

主要なプラットフォーム事業者における偽情報への対策状況について、2020 年２月の本研究会の報告書に記載の項目に沿って、ヒアリングシートに基づく回答を求め、モニタリングを行った。

プラットフォーム事業者における
偽情報への対策状況に関する主なモニタリング項目

項目１　前提（サービス概要）
項目２「我が国における実態の把握」関係
項目３「多様なステークホルダーによる協力関係の構築」関係
項目４「プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保」関係
（1）偽情報等に関するポリシー
（2）削除等の対応
（3）削除要請や苦情に関する受付態勢・プロセス
（4）透明性・アカウンタビリティの確保
項目５「利用者情報を活用した情報配信への対応」関係
項目６「ファクトチェックの推進」関係
項目７「ICT リテラシー向上の推進」関係
項目８「研究開発の推進」関係
項目９「情報発信者側における信頼性確保方策の検討」関係
項目 10　その他

プラットフォームサービス事業者におけるフェイクニュースや偽情報への対策状況ヒアリング　質問項目

1．前提(サービス概要)
① 対象サービス名・サービス分類
② 加入者数、月間アクティブユーザ数又は書き込み数

2．「我が国における実態の把握」関係
① 偽情報等の発生・拡散状況を把握できる体制 分析・調査の有無
② 日本における偽情報等の発生・拡散状況、結果公表
③ 研究者への情報提供、利用条件
④ ③についての削除の方法・仕組み(AIを用いた自動検知機能の活用等)
⑤ 不正な申告や削除要請への対策の方法・仕組み、対応件数

3．「多様なステークホルダーによる協力関係の構築」関係
①産学官民の協力関係の構築
②具体的な役割
③議論を踏まえた取組

4．「プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保」関係
(1)偽情報等に関するポリシー
①(i)禁止行為 (ii)削除等の対応
(2)削除等の対応
①偽情報等に関する申告や削除要請の件数
② (i)偽情報等に関する申告や削除要請に対する削除件数、(ii)アカウントの停止数
③偽情報等に関する主体的な削除件数(AIを用いた自動検知機能の活用等)
④③についての削除の方法・仕組み(AIを用いた自動検知機能の活用等)
⑤削除以外の取組 (i)警告表示 (ii)表示順位の低下 (iii)その他の取組内容
⑥不正な申告や削除要請への対策の方法・仕組み、対応件数
(3)削除要請や苦情に関する受付態勢・プロセス
①一般ユーザからの申告・削除要請への受付窓口・受付態勢、対応プロセス
②対応決定時における通知の内容、理由の記載の程度
③一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数
④ ③の部署・チームに関する日本国内の拠点の有無、日本における責任者の有無
⑤ 削除等への苦情や問い合わせに対する苦情受付態勢及び苦情処理プロセス
(4)透明性・アカウンタビリティの確保
①コンテンツモデレーションのアルゴリズムに関する透明性・アカウンタビリティ確保方策、AI原則・ガイドライン等の参照
② 透明性レポート 日本語で閲覧可能か
③ 取組の効果分析

5．「利用者情報を活用した情報配信への対応」関係
①広告表示先の制限
②広告出稿制限
③ターゲティング技術の適用に関する規定
④広告のアルゴリズムに関する透明性・アカウンタビリティ確保方策、AI原則・ガイドライン等の参照
⑤出稿者の情報や資金源の公開
⑥広告とコンテンツの分離
⑦その他の透明性・アカウンタビリティ確保方策 ユーザへのツール提供

6．「ファクトチェックの推進」関係
①ファクトチェック結果の表示 具体的な仕組み・基準
②ファクトチェックを容易にするツールの開発及び提供
③ファクトチェックを実施する人材の育成
④ファクトチェック機関との連携

7．「ICTリテラシー向上の推進」関係
①普及啓発の取組・投資
②他のステークホルダーとの連携・協力・投資

8．「研究開発の推進」関係
①AI技術に関する研究開発
②「ディープフェイク」対策の研究開発

9．「情報発信者側における信頼性確保方策の検討」関係
①信頼性の高い情報の表示
②ニュースの選別・編集に関する透明性・アカウンタビリティ確保方策
③メディアとの連携体制構築具体的検討・取組
④情報源のトレーサビリティ確保、なりすまし防止・認証

10．その他
①意見・補足

本年については、このヒアリングシートに基づき、本研究会において以下のとおりヒアリングを行うことにより、モニタリングを行った。詳細のヒアリングシートの内容については、参考４の通りである。

・2021 年３月 30 日　本研究会（第 25 回）
　ヤフー、Facebook、Google、Twitter、SIA
・2021 年５月 13 日　本研究会（第 27 回）
　LINE

（２）　モニタリング結果

①　総論

モニタリングの結果、全体的な傾向として、プラットフォーム事業者の偽情報への対応及び透明性・アカウンタビリティ確保の取組の進捗は限定的であった。

他方、多様なステークホルダーによる協力関係の構築、ファクトチェック推進、ICT リテラシー向上に関しては、まだ十分とは言えないものの、我が国においても取組が進められつつある。

②　各論

主な評価項目に関する各事業者の状況は以下のとおり。

偽情報対策に関するプラットフォーム事業者における透明性・アカウンタビリティ確保状況の主な評価項目の比較

項目	
我が国における実態の把握（2．関係）	・すべての事業者について、我が国における偽情報の実態把握及び結果の分析・公開は未実施
多様なステークホルダーによる協力関係の構築（3．関係）	・「Disinformation対策フォーラム」や「Innovation Nippon」により一定の進捗がみられる
プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保（4．関係）	・ヤフー（CGMサービス）は偽情報を直接禁止するポリシーが設けられておらず、対応件数等も非公開 ・LINEは、虚偽の情報の流布を包括的に禁止している。対応件数は一部公開 ・Googleはコロナ関連偽情報に関してポリシーがあり、我が国における削除件数等について一部公開 ・Facebook・Twitterは、削除ポリシーの整備や削除結果の公表等がグローバルでは進められているが、我が国における取組状況やその効果については非公開
利用者情報を活用した情報配信への対応（5．関係）	・いずれの事業者も、偽情報に関する広告や政治広告について、広告配信先の制限や、広告内容に関する何らかの制限を規定するなど、一定の対応は行われている ・LINE及びTwitterでは政治広告禁止。Googleでは日本において選挙広告は禁止 ・政治広告についてのターゲティング技術の適用については明確になっていない
ファクトチェックの推進（6．関係）	・ヤフーやgoogleなど一部のプラットフォーム事業者において、プラットフォーム上の情報へのファクトチェック結果の紐付けや、資金提供等の取組が開始されている ・Facebookでは、グローバルな取組は進められているが、我が国において国際ファクトチェックネットワーク（IFCN）に加盟しているファクトチェッカーがいないため、ファクトチェッカーとの連携は行われていない ・LINE、Twitterでは、取組は未実施（LINEは台湾では取組を実施）
情報発信者側における信頼性確保方策の検討（9．関係）	・「Disinformation対策フォーラム」において、既存メディアや有識者との情報共有や協議が進展 ・いずれの事業者も、新型コロナウイルス感染症関係の政府（内閣官房や厚労省等）の情報をサービス内で優先表示させる仕組み等を積極的に実施しているが、認知度は低い ・Googleでは、ジャーナリズムの支援策を実施
ICTリテラシー向上の推進（7．関係）	・Facebook・Google・LINEでは、我が国において偽情報の問題に対応したリテラシー教育に関する取組を実施 ・Twitterの取組は、偽情報対策に資する内容となっているか不明。ヤフーは今後実施予定
研究開発の推進（8．関係）	・Facebook、Google、Twitterではグローバルな取組としてディープフェイク対策のための研究開発が行われているヤフー、LINEではディープフェイク対策の研究開発は行われていない

また、モニタリングの質問項目について、事業者が「回答を控えた理由」及び「今後の対応方針」は以下のとおり。

事業者が「回答を控えた理由」及び「今後の対応方針」

事業者名	回答を控えた理由及び今後の対応方針
ヤフー	4.(2)削除等の対応 理由:「偽情報」という切り口から対応件数をカウントしているサービスはないため。 対応方針:対処すべき投稿がどのようなものかを含め、偽情報への対応につき有識者の意見も聞きながら検討を進める。 8.研究開発の推進 理由:現在は行っていないため。 対応方針:今後の事情に応じて、研究の要否も検討していく。
Facebook	(誹謗中傷関連回答の再掲) ・コミュニティ規定施行レポートにおいて、国別の内訳を公表していない理由: ①悪意のある利用者が意図的にサービスを悪用する場合、VPNを使って発信元の国を隠すことが多いため、国レベルのデータは信頼性が低くなる ②1つのコンテンツが複数の場所で見られる可能性があるため、コンテンツの数や事前対応率を国別に報告することは困難 ③国レベルのデータではサンプルサイズが小さくなり、データの精度や信頼性が低下する可能性がある ・データの報告義務を規定すると、企業が直面する様々な技術的制限、利用可能なリソース、法的およびプライバシーに関する考慮事項(各国のデータ保護法を含む)を適切に考慮できない可能性がある。特定のデータセットを追跡し報告するための過度に規定的で義務的な要件は、企業側、そして規制当局の両方にとってコストがかかり負担となる可能性があり、そのプラットフォームの安全性を正確に反映していない可能性もある。その結果、イノベーションと成長が損なわれ、テクノロジーの圧倒的な活用がもたらす利益が制限されることになる ・利用者の皆様のためにサービスを向上させ、利用者の皆様の安全性を確保するための投資を継続的に行っていく
Google	プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保(4.関係) ・グーグルでは、コンテンツを「偽情報」として特別に分類をしておらず、Google のプラットフォーム上での詐欺的または低品質のコンテンツを防止することを目的に、長年にわたり多数のコンテンツポリシーを設けており、例えば、スパム、なりすまし、意図的な情報操作に関するポリシーを定めている。このため、「偽情報」という分類でのデータを有していない ・偽情報への対処を目的とした政策立案・実施のため、どのような透明性の確保が有益なのか等について、プラットフォームサービス研究会、有識者等の意見を考慮しつつ、検討を行っていく
Twitter	・アルゴリズムに関する透明性・アカウンタビリティについて:「責任ある機械学習イニシアティブの開始」というブログ記事を公表 (https://blog.twitter.com/ja_jp/topics/company/2021/introducing-responsible-machine-learning-initiative) (以下、誹謗中傷関連回答の再掲) ・日本における一般ユーザからの誹謗中傷や偽情報に関する申告・削除要請の件数ならびに削除件数については、今後順次公開する予定 ・なお、データの集計頻度や分類方法、公開範囲については社内で検討中 ・一般ユーザからの申告や削除要請に対応する部署の規模については、非公開。サービスごとに直面する課題や受け取る申告・要請は異なっており、求められる対応も異なるため、サービス間の担当者の体制や人数を比較するのは文脈上適切でなく、また、偏った比較となる ・対応部署の拠点については安全性やセキュリティの観点から非公開

※LINEはヒアリングにおいて日本における取組に関する全ての項目に回答済み

出典：事業者の回答をもとに総務省作成

「我が国における実態の把握」関係（２．関係）

我が国において適切に実態把握を行ってその結果を分析・公開しているプラットフォーム事業者は見られなかった。総務省等によるユーザへのアンケート調査や研究者によるサービス上の情報流通についての調査によると、我が国において偽情報の問題が顕在化しているにもかかわらず、モニタリング結果によると、プラットフォーム事業者は自らのサービス上の偽情報の流通状況についてそもそも実態把握ができていない場合や、「偽情報の問題は生じていない」旨の回答があったため、プラットフォーム事業者の認識や実態把握と調査結果とのギャップが生じている。

実態把握に資する取組として、Twitter は研究者に向けて無償の学術研究用データ提供を実施している。

「多様なステークホルダーによる協力関係の構築」関係（３．関係）

SIA は「Disinformation 対策フォーラム」を主催し、Facebook、Google、ヤフー、Twitter が当該フォーラムに参加している。

Z ホールディングスは「デジタル時代における民主主義を考える有識者会議」を開催している。

Google は、ジャーナリズム支援や、国際大学 GLOCOM の研究プロジェクト「Innovation Nippon」の支援などを実施している。

「プラットフォーム事業者による適切な対応及び透明性･アカウンタビリティの確保」関係（４．関係）

いずれの事業者も､我が国におけるプラットフォーム事業者による偽情報への対応及び透明性･アカウンタビリティ確保の取組の進捗は限定的であった。具体的な取組状況は以下のとおり。

ヤフーは、ヤフーニュースには掲載情報の正確性・信頼性確保を目的とするポリシーは存在するが、一般ユーザが投稿する CGM サービスでは偽情報を直接禁止するポリシーが存在しないため、偽情報という切り口からの削除件数等は示していない（関連する他のポリシーでの対応）。

Facebook は、新型コロナウイルス関係や選挙・政治関係等に関して、グローバルのポリシーを具体的に設けており、削除・警告表示・表示順位抑制等の対応を行っている。他方で、偽情報に関する削除件数等については、我が国の件数も、グローバルの件数も示していない。

Google は、新型コロナウイルス関係の偽情報に関するグローバルなポリシーを具体的に設けており、削除等の対応を行っている（新型コロナウイルス関係以外は関連する他のポリシーでの対応）。グローバルな対応件数を公開しており、それに加えて、構成員限りとして日本での数値を公開している。

LINE は、利用規約において偽情報の意図的な流布行為を包括的に禁止している（ただし、偽情報に特化したポリシーは存在しない）。新型コロナウイルス関連として、食料品等の買い占めを煽るものについて臨時的に対応した件数についてのみ公開している。

Twitter は、新型コロナウイルス関係・選挙関連・ディープフェイク等に関して、グローバルのポリシーを具体的に設けており、削除やラベルの付与を実施。グローバルの削除件数も具体的に公開しているが、我が国の件数は公開されていない。

「利用者情報を活用した情報配信への対応」関係（５．関係）

広告表示先（配信先）の制限：

いずれの事業者においても､一定の禁止規定や特定の基準に満たない媒体・サイトへの広告配信を制限する規定が設けられている。

広告の出稿内容に関する制限：

いずれの事業者においても、偽情報を内容とする広告について、一定の禁止規定が設けられている。

政治広告に関する制限：

LINE 及び Twitter では政治広告が禁止されている。Google では、日本において一般的な政治広告は許可されているが、選挙広告は禁止されている。

ターゲティング技術の適用に関する規定：

上記の「広告の出稿内容に関する制限」に該当する偽情報の広告や政治広告はそもそも配信が禁止されているためターゲティング技術の対象とならない旨を説明している事業者が多い。なお、ヒアリング結果からは、（出稿が許されている）政治広告について、どのようなターゲティング技術に関する対応が行われているかについては明確になっていない（ヤフーは政治広告に関するターゲティング技術の適用に関する規定を設けるべきか検討中）。

出稿者の情報や資金源の公開、透明性レポートの公開等：

すべての事業者において、広告に関する何らかの透明性確保方策が行われている。具体的な取組は以下のとおり。

ヤフーは、広告出稿者の情報の明示を広告サイト内に明示することを広告掲載基準に規定している。政治広告の資金源公開については、今後必要に応じて検討予定。また、広告審査等に関する透明性レポートを公開している。

Facebook は、「広告ライブラリ」において、出資者・金額・リーチした利用者層などの情報を７年間保存し検索可能である。

Google は、広告主や所在を公開する広告主認証プログラムを導入し、2021 年５月に日本でも導入済み。米国等では選挙に関する透明性レポートを公開している（日本では選挙広告は禁止のため未提供）。

LINE は、ターゲティング広告に使用される「みなし属性」について、推定のためのアルゴリズムに影響する要素（友だち登録した公式アカウント、購入したスタンプ等）に関する説明をプライバシーポリシー等において明記している。

Twitter は、現在政治広告について全面禁止しているが、以前配信されていた政治広告や論点広告について、広告透明性センターにおけるアーカイブ情報を提供している。

「ファクトチェックの推進」関係（６．関係）

ヤフーや google は、我が国におけるファクトチェック推進団体やファ

クトチェッカーとの連携等が進められている。Facebook や LINE では、我が国における具体的な取組は行われていないが、諸外国では取組が行われている。事業者の具体的な取組は以下のとおり。

ヤフーは、ヤフーニュースにおいて、FIJ と情報共有連携を行い、メディアや専門家の記事を掲載するほか、2020 年度に引き続き、2021 年度も情報連携及び資金面での支援を実施。UGC サービスでは、ファクトチェッカーとの連携は行われていない。

Facebook は、グローバルな取組として、独立したファクトチェッカーがコンテンツを審査し、ラベル付けを行っている。ラベル付けされたコンテンツをシェアしようとする利用者や過去にシェアした利用者に通知している。ファクトチェッカーが偽情報と評価したコンテンツは、表示順位低下などの表示抑制を実施している。偽情報を繰り返し配信する違反者に対して、配信数抑制や収益化や広告機能停止など措置を実施している。国際ファクトチェックネットワーク(IFCN)に認定された独立した第三者ファクトチェッカーと提携を行っているが、我が国では、IFCN 認定ファクトチェッカーが存在しないため実施していない。

Google では、Google 検索及び Google ニュースにおいて、一定の基準を満たす第三者ファクトチェッカーにより作成されたファクトチェックのラベルが表示される。グローバルな取組に加えて、我が国においては、FIJ、InFact 及び BuzzFeed Japan 等に対し、Fact Check Tools の利用方法に関するワークショップを実施している。この結果、2021 年 3 月、Buzz Feed Japan が Google Fact Check Tools を使用を開始した。

Twitter では、特段の取組は行われていない。

LINE は、LINE Taiwan では、偽情報等を抑制するための官民パートナーシップを 2019 年に締結し、台湾行政院および 4 つのファクトチェック機関と協力し、ニュース配信プラットフォームである LINE TODAY 上に偽情報等のファクトチェック検証の結果を表示する取組を実施している。ユーザ自らが疑わしい投稿等を LINE から送信し、検証結果を得ることができるチャットボットを提供している。なお、我が国ではファクトチェッカーとの連携は行われていない。

「情報発信者側における信頼性確保方策の検討」関係（９．関係）

「Disinformation 対策フォーラム」において、既存メディアや有識者

との情報共有や協議が進められている。

また、いずれの事業者も、新型コロナウイルス感染症関係の政府（内閣官房や厚生労働省等）など、公共性の高い情報をサービス内で優先表示させる仕組み等を積極的に実施している。ただし、前述の調査結果によると、取組の認知度は１割程度となっている。

各ニュースサービスでは、提携媒体の選定基準策定やテクノロジーの活用等により信頼性の高い情報を掲載している。

その他、Google では、質の高いジャーナリズムの支援として、2019 年に、新型コロナウイルス感染症の拡大に対応し報道機関を支援するため、ジャーナリズム緊急救援基金を通じ、日本の 28 の報道機関に助成金を提供している。Google ニュースラボはジャーナリスト及び大学生に対し、偽情報を認識するスキル等のジャーナリズムにおけるデジタル技術提供及び活用ワークショップを提供しており、2015 年以来、１万人以上がトレーニングに参加している。今後、FIJ とのファクトチェックスキルや経済的支援などのさらなる提携を検討している。

「ICT リテラシー向上の推進」関係（７．関係）

Facebook・Google・LINE は、我が国において偽情報の問題に対応したリテラシー教育に関する取組が行われている。ただし、Twitter の取組は、偽情報対策に資する内容となっているか不透明となっている。ヤフーは、今後実施予定。事業者の具体的な取組は以下のとおり。

ヤフーは、2021 年度において教育現場（大学）において情報リテラシー教育を実施予定。こうしたリテラシー教育の授業・研究を通じて、啓蒙コンテンツを作成しヤフーを中心にグループで活用する予定。

Facebook は、アジア太平洋地域の専門家と協力して、「みんなのデジタル教室」を立ち上げた。日本の中学生・高校生を対象に、偽情報が発信される動機や、情報を受け取る側の視点を考え、偽情報を見分けるための様々なポイントについて、アクティビティを通じて学ぶ授業を展開している。

Google は、「Google News Initiative」を筆頭に、数多くのメディア・リテラシープログラムを立ち上げている。我が国において、ファクトチェックを含む主要なオンラインリテラシーのトピックを扱うオンライン・リテラシー・カリキュラムをこれまでに 10 万人以上の中学生・高校生に提供している。その他、「Grow with Google」「ウェブレンジャー」等のプロジェクトを実施している。

LINEは、ワークショップ授業・講演活動等を2012年より累計で約10,000回以上実施している。LINE みらい財団では、教育工学や授業デザインを専門とする研究者と共同で、独自の情報モラル教育教材の開発を行い、ウェブサイトで公開している。

Twitterは、公式アカウントやヘルプセンターページでの情報提供を実施している。

「研究開発の推進」関係（９．関係）

Facebook・Google・Twitterはそれぞれグローバルな取組としてディープフェイク対策のための研究開発が行われている。他方、ヤフー・LINEではディープフェイク対策の研究開発は行われていない。事業者の具体的な取組は以下のとおり。

Facebook は、2019 年 9 月に 100 万ドルの助成金により「Deep Fake Detection Challenge」を立ち上げ、ディープフェイクを検出するための研究やオープンソースツール開発を支援している。

Googleは、2019 年、高性能なフェイクオーディオ検出器を開発するための国際的な取組を支援するため、合成された音声に関するデータセットの公開を発表した。また、Jigsaw と共同で、Google が作成したビジュアルディープフェイクの大規模なデータセットを発表した。

Twitterは、Adobe、ニューヨークタイムズと協力し、ディープフェイク対策に関して、デジタルコンテンツの信頼性確保を目的とした業界標準開発のためのイニシアティブを発表した。

３　海外動向

（１）　欧州連合（EU）

欧州委員会は、EU 全域でより強靭な民主主義を構築することを目的に、2020 年 12 月に欧州民主主義行動計画（EDAP）を公表した。EDAP の内容は、①自由で公正な選挙の促進、②メディアの自由の強化、③偽情報への対抗措置の３つの柱により構成される。

偽情報への対抗措置に関しては、

・偽情報の発信者に対するコストを科すための取組

・プラットフォーム事業者が署名した「the Code of Practice on Disinformation(偽情報に関する行動規範)」の見直し、co-regulatory framework（共同規制）化

・上記に伴い、オンラインプラットフォーマーに向けて、「行動規範を強化するためのガイダンス（guidance to enhance the Code of Practice)」を発行（2021 年春)。その後、EU は新たな行動規範の実施状況をモニタリング

・EU 内外の偽情報へのメディア・リテラシー向上プロジェクトへ支援と資金提供

等の取組について記載されている。

プラットフォームの偽情報への取組は、自主的な取組である「偽情報に関する行動規範」に加え、前述の Digital Services Act (DSA) が加わり、2 段構造となる。EDAP は DSA を補完するものであり、DSA に示された措置を EDAP において具体化したものとされている。

EDAP の 3 つの柱のうち、「自由で公正な選挙の促進」、「偽情報への対抗措置」が DSA と関連している。広告に関して、DSA ではすべての広告についての透明性規律等が規定されているが、EDAP では、政治広告について、政治的文脈におけるスポンサー付コンテンツの分野における透明性の向上を確保するための法律について提案されている。

第３章　今後の取組の方向性

インターネット上の誹謗中傷及び偽情報の問題に対して、現状と課題、プラットフォーム事業者等による対応のモニタリング結果及び海外動向を踏まえ、以下のとおり今後の取組の方向性を示すこととする。

１　違法・有害情報への対応

インターネット上の誹謗中傷や偽情報といった違法・有害情報の流通に関しては、依然として SNS 等のプラットフォームサービスの影響が大きく、プラットフォーム事業者を中心とした対応が求められる。

しかしながら、現在のインターネット環境においては、CDN 事業者によるコンテンツのキャッシュや、ホスティング事業者によるコンテンツのホストなど、インターネット環境の担い手が多岐にわたっており、情報の削除や発信者特定など、違法・有害情報対策の実務では、これらのインターネット環境の複雑化に伴う実効性の低下等が問題となっている。また、プラットフォームサービス以外の掲示板や、まとめサイト等のミドルメディアにおける違法・有害情報も問題となっている。

したがって、プラットフォームサービス以外の、CDN・ホスティング（クラウドサービス）・アプリマーケット・ミドルメディア等も射程に含め、コンテンツ流通メカニズム全体を踏まえながら、引き続き違法・有害情報対策に関する検討を行っていくことが必要である。

さらに、ヘイトスピーチ、部落差別、性被害、自殺誘引等、様々な類型の違法・有害情報が問題となっていることから、これらの誹謗中傷や偽情報以外も含む違法・有害情報全般について対策を行っていくことが必要である。

違法有害情報対策全般に関する今後の取組の方向性

1. ユーザに対する情報モラル及びICTリテラシーの向上のための啓発活動

・実態把握や分析結果に基づき、産学官民が連携し、引き続きICTリテラシー向上施策が効果的となるよう取り組む必要
・e-ネットキャラバン等の青少年向けの取組に加え、大人も含め幅広い対象に対してICTリテラシー向上のための取組を実施することを検討していくことが必要
・総務省や各ステークホルダーによるICTリテラシー向上の取組状況を把握し、ベストプラクティスの共有や更なる効果的な啓発を行うことが必要

2. プラットフォーム事業者の自主的取組の支援と透明性・アカウンタビリティの向上

＜プラットフォーム事業者の自主的取組の支援＞
・プラットフォーム事業者が自らのサービス上での違法・有害情報の流通状況について実態把握とリスク分析・評価を行うことが必要
・トラステッドフラッガーの仕組みの導入・推進にむけて検討を行うことが望ましい。人権擁護機関からの削除要請に関し、削除に関する違法性の判断基準・判断方法や個別の事業者における削除実績等について関係者間で共有し、行政側・事業者側双方の削除に関する対応についての透明性を向上させ、円滑な削除対応を促進することが必要
・プラットフォーム事業者は、一定の短期間の間に大量の誹謗中傷が集まった場合へのアーキテクチャ上の工夫について、既存の機能や取組の検証や新たな対応の検討を行うことが望ましい
＜プラットフォーム事業者による取組の透明性・アカウンタビリティの向上＞
・我が国における透明性・アカウンタビリティ確保が図られていない事業者に関しては、特に透明性・アカウンタビリティ確保の取組を進めることが強く求められる。総務省はモニタリングと検証評価を継続的に行っていくことが必要

3. 発信者情報開示に関する取組

・法施行に向けて関係政省令の策定を進め、関係事業者及び総務省の間で新制度の具体的な運用に関する協議を進めることが必要
・プラットフォーム事業者・行政側の双方で、発信者情報開示に関する申請や開示件数等について集計・公開することが求められる

4. 相談対応の充実に向けた連携と体制整備

・違法有害情報相談センターにおいて引き続き相談対応を行い、システム更新、相談機関間の連携強化、相談窓口の周知が必要

⇩

・プラットフォーム事業者による取り組みの透明性・アカウンタビリティ確保について、**次回以降のモニタリングにおいて、依然として事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要**
・①リスクベースアプローチ、②リスク分析・評価と結果公表、③適切な対応の実施と効果の公表、④継続的モニタリング、⑤データ提供、といったといった大枠としての**共同規制的枠組みの構築を前提に検討を進めることが適当**

① ユーザに対する情報モラル及び ICT リテラシーの向上のための啓発活動

誹謗中傷を始めとするインターネット上の違法・有害情報の問題に関しては、まず、それぞれのユーザが他人を個人として尊重し、SNS を始めとするインターネット上での自らの書き込みに対して他人が傷つく可能性を想像し、誹謗中傷を行わないよう心がけるなど、ユーザ自身の情報モラルが最も重要である。その際、誰もが誹謗中傷の加害者になり得るし、誰もが偽情報を拡散する可能性があることを認識することが重要である。

次に、実態把握や分析結果に基づき、産学官民が連携し、引き続き ICT リテラシー向上施策が効果的となるよう取り組み、体系的で多元的なリテラシー啓発を実施することが必要である[26]。

具体的には、青少年だけでなく大人であっても誹謗中傷等のネット炎上に加担しているという分析結果を踏まえ、総務省は、情報の受信側・発信側の双方に関する啓発を推進し、これまでの「e-ネットキャラバン」等の青少年向けの取組に加え、大人も含め幅広い対象に対して ICT リテラシー向上のための

[26] 分析結果の例：ごく少数の者がネット炎上によるネット世論を作る、書き込む動機は正義感、多くの人は誹謗中傷を書いていると気づいていない、等

取組を実施することを検討していくことが必要である。また、様々な主体により行われている既存リテラシー施策について整理し、様々な主体の連携を促進するとともに、こうした総務省及び各ステークホルダーによる取組状況を把握し、ベストプラクティスを共有し、更なる効果的な啓発活動につなげていくことが必要であると考えられる。

②-１ プラットフォーム事業者の自主的取組の支援

違法・有害情報対策の前提として、まず、プラットフォーム事業者が、自身のサービス上でどのような違法・有害情報が流通しているのか、自ら実態把握とリスク分析・評価[27]を行うことが必要である。

行政は、引き続きプラットフォーム事業者等による自主的な削除等の対応を促進することとし、プラットフォーム事業者等に対して削除義務を課すことや、個別のコンテンツを削除しなかったことに対して罰則等を設ける法的規制を導入することは極めて慎重な検討を要する。

他方で、取組の透明性・アカウンタビリティの確保方策が図られない場合は、それらに関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与が必要である。

誹謗中傷や偽情報のみならず、ヘイトスピーチ、部落差別、自殺誘引等も含めて、違法・有害情報全般に共通する対応として、まず、違法な情報に対して、プラットフォーム事業者をはじめとするサイト運営者は、プロバイダ責任制限法による免責規定を踏まえ、迅速に削除等の対応を行うことが求められる。

その際、法務省人権擁護機関等の関係機関からの削除要請を受けた場合には、それらの手続の正当性や専門性も踏まえ、迅速に削除等の対応を行うことが求められることから、プラットフォーム事業者は、我が国におけるトラステッドフラッガーの仕組みの導入や、適切な報告者の認定について検討することが望ましい。

この点、プラットフォーム事業者・総務省・法務省による実務者検討会の

[27] 例えば、誹謗中傷以外にも、ヘイトスピーチ、部落差別、性被害、自殺誘引等、様々な類型の違法・有害情報の流通状況を分析し、それがどのような利用者（例えば青少年、女性、国籍、地域などの属性）に対してどのような被害を生じさせているのかについて分析を行った上で、対応策を検討することが考えられる。

継続的な開催等により、削除に関する違法性の判断基準・判断方法や個別の事業者における削除実績等について関係者間で共有し、行政側・事業者側双方の削除に関する対応についての透明性を向上させ、円滑な削除対応を促進することが必要である。

また、個別の書き込みが違法な情報か有害な情報かどうかの判断が難しい場合も多いこと等を前提に、違法ではないが有害な書き込みについては、プラットフォーム事業者は、自らのポリシーや約款に基づき、適切に削除等の対応を行うこと求められる。

加えて、削除以外にも、それぞれのサービスの特性に応じた、アーキテクチャ上の工夫による違法・有害情報対策を進めることが期待されるところ、ヒアリング結果を踏まえ、特に一定の短期間の間に大量の誹謗中傷が集まった場合に、既存の機能・取組において効果的に対応が可能なのかという点について、プラットフォーム事業者は自ら検証を行い、仮に効果が見られない場合には、更なるアーキテクチャ上の工夫の導入について検討を行うことが望ましい。

②-２　プラットフォーム事業者による取組の透明性・アカウンタビリティの向上

ア　モニタリング結果

モニタリング結果によると、プラットフォーム事業者の誹謗中傷等への対応に関する透明性・アカウンタビリティ確保状況には差異が見られる。

ヤフー及びLINEは、我が国における誹謗中傷等への対応について、具体的な取組や定量的な数値を公表しており、透明性・アカウンタビリティ確保に向けた施策が進められている。

Google は、一部、我が国における定量的な件数が新たに示されているが、構成員限りで非公開となっている情報も残されており、部分的に透明性・アカウンタビリティ確保に向けた施策が進められている。

他方、Facebook 及び Twitter は、グローバルな取組や数値は公表しているが、我が国における具体的な取組や定量的な数値が公表されておらず、我が国における透明性・アカウンタビリティ確保が果たされていない。

これらの状況を踏まえ、我が国における透明性・アカウンタビリティ確

保が図られていない事業者に関しては、特に透明性・アカウンタビリティ確保の取組を進めることが強く求められる。

イ　モニタリングの枠組み

我が国の利用者が安心してプラットフォームサービスを使えるように、引き続きプラットフォーム事業者の自律的な対応及び透明性・アカウンタビリティ確保に関する自主的な報告を求め、総務省はモニタリングと検証評価を継続的に行っていくことが必要である。

また、依然として透明性・アカウンタビリティ確保が図られない事業者について、その理由を深掘りした上で対応策を検討するとともに、いつまでに我が国において取組が実施されるのか把握することが必要である[28]。

ウ　共同規制的枠組みの構築

次回以降のモニタリングにおいて、依然として事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要である。

この点、透明性・アカウンタビリティ確保に関して、プラットフォーム事業者の自主的な対応及び自主的な報告に委ねた際、プラットフォーム事業者が果たすべき透明性・アカウンタビリティ確保の基準や水準が不明確となる可能性があることから、モニタリングの手続及び内容の妥当性を高め、事業者が行うべき取組や従うべきルールの確実性及び将来にわたる予見可能性を高めるという観点も踏まえ、法的枠組みの検討を行うことも必要であると考えられる。

行政からの一定の関与の検討に際しては、①リスクベースアプローチに

[28] 本研究会（第 29 回）参考資料 2「第 28 回会合における構成員等からの主なご意見（追加質問回答）」のとおり、ヒアリングシートにおいて回答を控える「理由」及び「今後の対応方針」についてプラットフォーム事業者から追加で聞き取りを行った。その際、必ずしも明確な回答が見られない場合もあった。

基づく検討[29]、②特に、リスクの大きい巨大プラットフォームサービスについて、自らのサービスのリスク評価の実施及び結果の公表、③リスクを低減するための合理的・比例的・効果的な対応の実施とその結果及び効果の公表、④政府及び外部研究者等による継続的なモニタリング、⑤モニタリングを可能とするデータ提供、といった大枠としての共同規制的枠組みの構築を前提に検討を進めることが適当であると考えられる。

具体的なモニタリング事項や法的枠組みの検討に関しては、既存のヒアリングシートを基本として、海外における制度や検討状況[30]も参考にしつつ、我が国における有識者との議論を通じて、プラットフォーム事業者と対話を行いながら検討することが適当である。

その際、より適切な指標や項目があると考えられる場合には、プラットフォーム事業者は、自らのサービスの特性を踏まえ、代替案となる指標や取組を積極的に示すことが望ましい。

また、総務省は、継続的に国際的な法的規制枠組みの検討状況を把握し、国際的対話を深めていくことが適当である。具体的には、グローバルにサービスを提供するプラットフォーム事業者における適切な対応について、諸外国の情報通信担当部局等と連携しながら、実効的な対応を検討していくことが必要である。

この点、Ｇ７デジタル・技術大臣会合における「Internet Safety」の成果文書も踏まえ、グローバルにサービスを提供するプラットフォーム事業者においては、グローバルのみならず我が国における透明性・アカウンタビリティ確保が行われることが重要である。

エ　透明性・アカウンタビリティ確保に関するビジョン

今後のモニタリングの実施や、行政からの一定の関与を検討するに当た

---

[29] 例えば、広く一般のサイト管理者が果たすべき内容と、利用者が多く社会的影響力も大きい一部の大手プラットフォーム事業者のみが果たすべき内容を区別して検討することが考えられる。また、誹謗中傷以外にも、ヘイトスピーチ、部落差別、性被害、自殺誘引等、様々な類型の違法・有害情報の流通状況を分析し、それがどのような利用者（例えば青少年、女性、国籍、地域などの属性）に対してどのような被害を生じさせているのかについての分析を踏まえた上で、プラットフォーム事業者に求められる取組の内容を検討することが考えられる。

[30] 今回のモニタリング事項と諸外国における透明性・アカウンタビリティ確保に関する法的枠組みとの比較については参考５を参照。

って、我が国において、プラットフォーム事業者に対してどのような透明性・アカウンタビリティが必要かについて、明確な「ビジョン」が示されることが重要である。

この「ビジョン」としては、「緊急提言」やこれまでの議論を踏まえ、

- 利用者が安心・信頼してプラットフォームサービスを利用することができるよう、プラットフォーム事業者による自律的な情報の削除等の対応に加えて、それらの取組が適切に行われていることが利用者や社会全体に対して明らかにされること
- 他方で、利用者の表現の自由を確保する観点から、プラットフォーム事業者によってそれぞれのサービスの規約やポリシーに照らして過剰な削除や不当なアカウント停止等の行き過ぎた対応が行われていないかという点についても明らかにされること
- 違法・有害情報に関する利用者や第三者からの削除要請・苦情受付態勢及び苦情処理プロセスを適切に定め、わかりやすく公開し、適切に運用を行うこと

などが挙げられる。

また、具体的な方策としては、例えば、

① 違法・有害情報対策として、どのような種類・性質の情報又はアカウントに対して、どのような対応を行うのか、自らが提供するサービスの全体的な考え方や具体的な対応に関する規約やポリシーをあらかじめ明確に定めてわかりやすく公開すること

② 規約やポリシーに基づいて自らが実際に行った削除等の取組、アーキテクチャ上の工夫、AI を活用した取組等の結果を具体的・定量的なデータにより公開すること

③ 削除要請や苦情に関する受付態勢・プロセスを設けるとともに、申立者及び利用者（発信者）に対して対応の可否に関する通知や適切な理由説明を行うこと

④ 取組の効果について分析を行い、公開すること

⑤ 自らのサービスにおける違法・有害情報の流通状況及びリスクについて分析を行い、公開すること。また、外部の研究者等が調査分析を行う際に必要な情報を提供すること

などの取組を実施することが望ましい。

さらに、自主的な報告では、特に海外事業者において、グローバルな取組状況について示されていても、我が国における取組状況が示されていない傾向にあることから、諸外国と我が国との間の誹謗中傷の流通状況、社会状

況、法制度等の違いに留意しつつ、我が国における取組状況が我が国の利用者に対して適切かつ具体的に示されることが必要である。

具体的には、

① 日本語で我が国の利用者にもわかりやすい形で規約やポリシー、透明性レポートなどの情報を公開すること

② 我が国に特有の違法・有害情報に関する情報流通の問題にも適切に対応できる規約やポリシーを策定すること

③ 透明性レポートを公開する際には、グローバルな対応件数の総数だけではなく、我が国の国内における対応件数についても併せて公開すること

④ 日本語を正しく理解できるスタッフを十分確保した上で、日本語で手続可能な適切な削除要請・苦情受付態勢及び苦情処理プロセスを整備するとともに、国内での迅速かつ適切な救済メカニズムを確保すること。その上で、それらの態勢やプロセスについて国内のユーザにわかりやすく公開すること

などの取組を実施することが望ましい。

オ　その他の観点

プラットフォームサービス以外のサービス（CDN・ホスティング（クラウド）・アプリストア等）における違法・有害情報対策に係る取組についても、必要に応じて今後ヒアリングを行い、透明性・アカウンタビリティ確保を求めていくことが望ましい。

また、SNS 等の投稿型のプラットフォームサービス以外においても、例えば検索サービスにおいては、アルゴリズムによりコンテンツについて評価を行った上で表示順位を決定していることから、違法・有害情報や信頼性の低い情報が表示されにくくする仕組みを引き続き改善していくとともに、それらの対応が適切に行われているかどうかについて、悪用の懸念にも留意しつつ、透明性・アカウンタビリティ確保を果たされることが望ましい。

加えて、モニタリング結果によると、AI の活用に関して、各社において深層学習を用いた自然言語処理モデルを活用した違法・有害情報への対応がすでに進められていることから、引き続き、これらの取組を進めることが有用であると考えられる。

他方で、AI の活用によるオーバーブロッキング等の懸念もあることから、

AI の活用に関して具体的に透明性・アカウンタビリティ確保を図っていくことが望ましい。

③　発信者情報開示関係

発信者情報開示関係については、改正プロバイダ責任制限法の法施行に向けて、関係政省令の制定を進めるとともに、関係事業者及び総務省の間で、円滑な新制度の施行に向けて、具体的な運用に関する協議を進めることが必要である。

その際、現在のインターネット環境においては、CDN 事業者によるコンテンツのキャッシュや、ホスティング事業者によるコンテンツのホストなど、インターネット環境の担い手が多岐にわたっており、情報の削除や発信者特定など、違法・有害情報対策の実務では、これらのインターネット環境の複雑化に伴う実効性の低下等が問題となっていることを踏まえ、プラットフォームサービス以外の、CDN・ホスティング（クラウドサービス）事業者等も加えて協議を進めていくことが適当である。

また、円滑な発信者情報開示制度の運用にむけて、プラットフォーム事業者は、前述の②-２に記載の透明性・アカウンタビリティ確保の取組の中で、我が国における発信者情報開示に関する申請や開示件数等について集計・公開することが望ましい。
総務省は、法務省や裁判所等と連携し、行政側でも現行制度及び新制度に関する発信者情報開示の件数等を把握することが適当である。

④　相談対応の充実

総務省は、相談対応の充実に関して、「違法・有害情報相談センター」において、引き続き被害者救済のための円滑な運用を行うとともに、ユーザビリティに資するシステム更新等を随時検討していくことが望ましい。

また、「違法・有害情報相談センター」において、複数の相談機関間における連携強化を一層深めていくことが適当である。

さらに、相談を必要としている被害者に対して「違法・有害情報相談センター」等の必要とされる相談機関の相談窓口に関する情報が届くよう、複数の

相談窓口の案内図について広く周知を行うなど、引き続き、被害者にとって相談窓口を分かりやすく示すための取組を行うことが必要である。

２　偽情報への対応

偽情報への対応については、2020 年２月にとりまとめた報告書において記載の偽情報への対策に関する 10 の方向性について、継続的に議論を深めていくことが適当である。

この際、違法・有害情報対策全般にも共通する点は、本章１の中で対策を進め、それ以外の偽情報固有の対応については、以下のとおり取組を進めることが適当である。

偽情報対策に関する今後の取組の方向性

１　自主的スキームの尊重
・民間による自主的な取組を基本とした対策を進めていくとともに、総務省はモニタリングと検証評価を継続的に行っていくことが必要

２　我が国における実態の把握
・PF事業者の認識や実態把握と調査結果とのギャップが生じていることから、プラットフォーム事業者は、自らのサービス上で生じている我が国における偽情報の問題について適切に実態把握を行い、研究者が分析を行うために必要な情報の無償で情報提供が行われることが望ましい

３．多様なステークホルダーによる協力関係の構築
・「Disinformation対策フォーラム」「Innovation Nippon」等において継続的に議論・研究が行われることが望ましい

４　プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保
・プラットフォーム事業者は、リスク分析・評価に基づき偽情報への対応を適切に行い、それらの取組に関する透明性・アカウンタビリティ確保を進めていくことが求められる
・総務省は、これらの取組に関するモニタリングと検証評価を継続的に行っていくことが必要。どのような方法や情報により偽情報への適切な対応が図られているかどうかを評価することが可能かについて引き続き検討が必要

５　利用者情報を活用した情報配信への対応
・広告の種類・対応に応じてリスクや問題の差異を分析したうえで、特に、偽情報を内容とする広告の配信やターゲティング技術の適用については、そのリスクを踏まえ、より注意深い対応と、それに伴う透明性・アカウンタビリティ確保が求められる

６　ファクトチェックの推進
・プラットフォーム事業者・ファクトチェッカー・ファクトチェック推進団体・既存メディア等が連携し、取組がさらに進められることが期待される
・我が国におけるファクトチェック結果を積み重ねて分析を行うことにより、偽情報の傾向分析やそれを踏まえた対策の検討が行われることが望ましい

７　情報発信者側における信頼性確保方策の検討
・現代のメディア環境に対応した情報の信頼性の確保の在り方について、既存メディア・ネットメディア・プラットフォーム事業者など関係者の間で検討を深めていくことが望ましい
・ミドルメディアを中心とした偽情報の生成・拡散・流通メカニズムに関する実態把握と分析も踏まえ、検討を深めていくことが望ましい

８　ICTリテラシー向上の推進
・偽情報の特徴を踏まえながら引き続きICTリテラシー向上施策が効果的となるよう取り組むことが必要

９　研究開発の推進
・ディープフェイク等に対抗にするための研究開発や事業者の対応が進められることが望ましい

10　国際的な対話の深化
・偽情報に関する政策について国際的な対話の深化を深めていくことが望ましい

⇩

・次回以降のモニタリングにおいて、偽情報への対応に関して、事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要

①　自主的スキームの尊重

我が国における偽情報への対応の在り方の基本的な方向性としては、引き続き、まずはプラットフォーム事業者を始めとする民間部門における関係者による自主的な取組を基本とした対策を進めていくとともに、プラットフォーム事業者等による自律的な対応及び自主的な報告を求め、総務省はモニタリングと検証評価を継続的に行っていくことが必要である。

特に、プラットフォーム事業者等に対して削除義務を課すことや、個別のコンテンツを削除しなかったことに対して罰則等を設ける法的規制を導入することは極めて慎重な検討を要する。

他方で、違法・有害情報全般に関する透明性・アカウンタビリティ確保と同様に、次回以降のモニタリングにおいて、偽情報への対応に関して、事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要である。

② 我が国における実態の把握

偽情報に関して、研究者による実態把握や分析が進められているものの、依然として我が国における偽情報の流通状況が明らかになっているとはいえないため、偽情報特有の問題の検討に資するよう、以下の点に着目して、引き続き偽情報の実態把握を行うことが適当である。

特に、研究者によるサービス上の情報流通についての調査によると、我が国において偽情報の問題が顕在化しているにもかかわらず、モニタリング結果では、プラットフォーム事業者は自らのサービス上の偽情報の流通状況についてそもそも実態把握ができていない場合や、「偽情報の問題は生じていない」旨の回答があったため、プラットフォーム事業者の認識や実態把握と調査結果とのギャップが生じている。

したがって、プラットフォーム事業者は、自らのサービス上で生じている我が国における偽情報の問題について適切に実態把握を行うとともに、研究者が分析を行うために必要な情報についてプラットフォーム事業者から無償で情報提供が行われることが望ましい。

コンテンツ側の偽情報流通の実態把握・分析に当たっては、プラットフォームサービスのみならず、ミドルメディア等も含めた情報流通環境全体を捉えた視点により実施されることが望ましい。特に、ミドルメディアを中心とした偽情報の生成・拡散・流通メカニズムに関して、実態把握と分析を進めていくことが必要であると考えられる。

また、SNS 上の偽情報が偏った複数の集団・ネットワーク（クラスター）に分かれて拡散しているケースが見られることから、これらの既存の分析をもとに、引き続き偽情報の拡散状況や特徴について実態把握及び分析を行い、偽情報の拡散に有効なプラットフォームサービス上のアーキテクチャ上の工夫や、偽情報に関するリテラシー向上に関する取組など、必要な対応につい

て検討していくことが望ましい。

③　多様なステークホルダーによる協力関係の構築

偽情報への対応に当たっては、多面的な解決策を検討していくことが必要であり、その際、プラットフォーム事業者のみならず、産学官民の多様なステークホルダーによる協力関係の構築を図り、対話の枠組みを設けることが重要と考えられる。

モニタリング結果によると、「Disinformation 対策フォーラム」や「Innovation Nippon」などにより、我が国において、産学官民の多様なステークホルダーによる協力関係の構築や偽情報への対策の検討が進められている。

したがって、引き続き、「Disinformation 対策フォーラム」や「Innovation Nippon」等の産学官民の連携の場において、継続的に偽情報への対策に関する議論や研究が行われることが望ましい。

特に、「Disinformation 対策フォーラム」においては、このフォーラムによる中間とりまとめの記載のとおり、今後、①伝統的なメディア・学術研究機関等と協力を行いながら、ファクトチェックを持続的かつ総合的に行う主体についての具体的検討を進めること、②情報リテラシーの向上のため、多様な主体によるコンテンツの作成や、総務省や関連団体とも協力して総合的な普及啓発の取組を促進することが期待される。

また、総務省は、多様なステークホルダー間の協力関係の構築を支援するコーディネーターとしての役割を果たしていくことが適当である。

④　プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保

モニタリング結果によると、いずれの事業者においても、自らのサービス上で生じている我が国における偽情報の問題について適切に実態把握が行われていない。また、我が国における偽情報への対応及び透明性・アカウンタビリティ確保の取組の進捗は限定的であった。

これらの状況を踏まえ、プラットフォーム事業者は、我が国において生じている自らのサービス上の偽情報の問題について適切に実態把握とリスク評

価を行った上で、そのリスクに応じて偽情報への対応を適切に行うことや、具体的にどのような取組が効果的かについて分析を行うことが求められる。

さらに、プラットフォーム事業者は、前述の（１）②-２の記載内容と併せて、自らの取組に関する透明性・アカウンタビリティ確保を進めていくことが求められる。

この点、Ｇ７デジタル・技術大臣会合における「Internet Safety」の成果文書も踏まえ、グローバルにサービスを提供するプラットフォーム事業者においては、グローバルのみならず我が国における透明性・アカウンタビリティ確保が行われることが重要である。

総務省は、これらの取組に関するモニタリングと検証評価を継続的に行っていくことが必要である。この際、プラットフォーム事業者に対して具体的にどのような対応や情報公開を求めることにより、偽情報への適切な対応が図られているかどうかを評価することが可能かについて、依然として検討が深まっていないことから、引き続き検討が必要である。

違法・有害情報全般に関する透明性・アカウンタビリティ確保と同様に、次回以降のモニタリングにおいて、偽情報への対応に関して、事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要である。

⑤　利用者情報を活用した情報配信への対応

ア　ターゲティング技術の悪用による問題について

行動ターゲティングの技術による政治広告における悪用事例のように、利用者の脆弱性につけ込み偽情報を拡散する使い方が可能であるといった指摘がある。

モニタリング結果によると、いずれの事業者においても、偽情報を内容とする広告や、政治広告の出稿について、一定の制限を設けている。特に、LINE 及び Twitter では政治広告が禁止されており、Google では日本において選挙広告は禁止されている。この点、複数の事業者が、偽情報を内容とする広

告や政治広告はそもそも配信が禁止されているためターゲティング技術の対象とならない旨を説明している。なお、（出稿が許されている）政治広告について、どのようなターゲティング技術に関する対応が行われているかについては明確になっていない。

したがって、行動ターゲティング広告における利用者情報の取扱いについては、利用者情報ＷＧにおいても議論が行われているところ、広告の種類・対応に応じてリスクや問題の差異を分析したうえで、特に、偽情報を助長しうるターゲティング技術の適用については、そのリスクを踏まえ、より注意深い対応と、それに伴う透明性・アカウンタビリティ確保が求められる。

イ　偽情報を掲載しているサイトへの広告配信の問題について

コンテンツの内容が正しくなくてもページビューを稼げば広告収入で儲かる仕組み（アテンションエコノミー）が偽情報の生成を支えているといった指摘がある。

この点に関して、モニタリング結果によると、複数の事業者において、偽情報に関連する内容の媒体・サイトや、特定の信頼性基準に満たない媒体・サイトへの広告配信を制限する規定が設けられている。

したがって、広告収益を絶つことにより偽情報を拡散防止するという観点も踏まえ、これらのポリシーに基づき、アテンションエコノミーの弊害を防止するための実効性のある対応が行われることが求められる。

次回以降のモニタリングにおいて、偽情報に関する行動ターゲティング広告についての対応及び偽情報を掲載しているサイトへの広告配信の問題に関して、事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要である。

⑥　ファクトチェックの推進

ヒアリングによると、我が国においても、ファクトチェックの取組が徐々

に広がってきているものの、ファクトチェッカーやファクトチェック記事件数は十分とはいえず、ファクトチェックの担い手や社会的認知度・理解度が不足しているという課題は依然として残されている。

したがって、引き続き、プラットフォーム事業者、ファクトチェッカー、ファクトチェック推進団体等が連携し、ファクトチェックの活性化のための環境整備を推進していくことが望ましい。

プラットフォーム事業者においては、①ファクトチェッカー・ファクトチェック推進団体との連携強化（サービス上の情報へのファクトチェック結果の紐付け等）、②資金提供等の取組がさらに進められることが期待される。

ファクトチェッカーにおいては、③国際ファクトチェックネットワーク（IFCN）への加盟、④ファクトチェック態勢等に関する透明性・アカウンタビリティ確保が進められることが期待される。

ファクトチェック推進団体においては、⑤人材の育成、⑥市民のリテラシー向上、⑦ファクトチェック支援システム等によるファクトチェックの容易化、⑧透明性・アカウンタビリティ確保、⑨複数のファクトチェッカーによる複合的なファクトチェック環境の構築に向けた取組等を推進していくことが期待される。

そのほか、今後、我が国におけるファクトチェック結果を積み重ねて分析を行うことにより、偽情報の傾向分析やそれを踏まえた対策の検討[31]が行われることが望ましい。

加えて、「Disinformation 対策フォーラム」において、引き続き、プラットフォーム事業者・新聞や放送などの既存メディア・学術研究機関等との間で協力を行いながら、上記の観点を踏まえながらファクトチェックを持続的かつ総合的に行う主体についての具体的検討を進めることが望ましい。

その際、新聞や放送などの既存メディアにおいても、これまでの信頼性のある情報発信の取組の一環として自律的なファクトチェックの担い手となるとともに、ファクトチェッカーやファクトチェック推進団体等に対して、これまで培ってきた知見やノウハウの共有等の支援を行うことなどが期待される。

---

[31] 例えば、更なるファクトチェック支援のための技術導入、プラットフォーム事業者におけるポリシー策定や削除等の対応など。

⑦　情報発信者側における信頼性確保方策の検討

プラットフォーム上における偽情報の問題に対抗するためには、前述のファクトチェックの推進とともに、信頼性の高い情報の流通を増やし、利用者が容易にそれらを参照できるような環境整備が必要である。

この点、我が国においては、全国的に大きな影響力を持つ新聞社や放送事業者等の既存メディアにおいて、自律的なチェック態勢に基づく信頼性のある情報発信がこれまで行われてきたほか、例えば日本放送協会における「SoLT」のような SNS 時代に対応した報道態勢が構築されつつある。その他、「Disinformation 対策フォーラム」におけるプラットフォーム事業者等との対話も進められている。

これらの状況も踏まえつつ、新聞社や放送事業者等の既存メディアにおける情報の信頼性の確保のための取組やノウハウも参考とし、これをネットメディアにも広げていくという考え方も取り入れつつ、引き続き、現代のメディア環境に対応した持続可能性のある情報の信頼性の確保の在り方について、メディア関係者の知見や経験を活用しつつプラットフォーム事業者との間で検討を深めていくことが望ましい[32]。

プラットフォーム事業者においては、新型コロナウイルス感染症等に関して信頼できる政府機関・専門機関・メディア等の情報やそれらへのリンクをサービスの目立つ場所に掲示するなどの取組が積極的に行われているが、認知度が低い（１割程度）ことから、これらの取組を引き続き積極的に行うことが望ましい。また、前述のとおり、我が国におけるファクトチェックメディア等との連携により、偽情報に対してファクトチェック結果を紐付けて表示する等の取組を進めていくことが望ましい。

ニュース配信プラットフォームサービスにおいては、ニュースや情報に関する選別・編集責任等に関するサービスの性質を踏まえながら、利用者のニ

[32] 例えば、前述のとおり、Google では、ジャーナリズムの支援として、2019 年に、新型コロナウイルス感染症の拡大に対応し報道機関を支援するため、ジャーナリズム緊急救援基金を通じ、日本の 28 の報道機関に助成金を提供している。その他、ニュースに関するコンテンツ使用料についてプラットフォーム事業者とニュースメディア間で協議が行われており、一部の諸外国においては、プラットフォーム事業者に対して、ニュースメディアへのコンテンツ使用料の支払いや交渉を義務づける動きが広がっている。

ーズに応じて信頼性の高い情報配信が行われるよう引き続き努めるとともに、情報配信に関する透明性やアカウンタビリティの確保方策を適切に実施することが望ましい。

また、偽情報の拡散要因について、インターネットにおけるニュースの生態系の問題として、ミドルメディアが大きな影響を与えていることがこれまでの分析により判明しつつある[33]。

したがって、インターネット上におけるメディア全体の情報の信頼性をどのように確保していくかについて、ミドルメディアを中心とした偽情報の生成・拡散・流通メカニズムに関する実態把握と分析も踏まえ、「Disinformation対策フォーラム」等の場も活用しつつ、伝統的なメディア・ネットメディア・プラットフォーム事業者等の関係者間で、ミドルメディア運営事業者との連携可能性等も含め、今後検討をさらに深めていくことが望ましい。

⑧ ICT リテラシー向上の推進

モニタリング結果によると、総務省や一部のプラットフォーム事業者においては我が国においても偽情報に資するリテラシー向上の取組が行われているが、その他の事業者においては、既存のリテラシー向上に関する取組が偽情報に効果的な内容となっているか不透明、また、現時点では未実施となっている。

したがって、違法・有害情報全般に関する ICT リテラシー向上の推進に向けた取組に加えて、偽情報特有の問題への対応のため、以下の点に着目して、偽情報に対抗するリテラシー向上の推進に向けた取組が行われることが望ましい。

具体的には、偽情報の実態把握や分析結果に基づき、スーパースプレッダーへの効果的な働きかけ、偽情報に対して効果のある「情報リテラシー」の分析、人間の認知の仕組み、偽情報のジャンル別に異なる有効な情報検証行動、インターネット上の情報の偏りやメディア環境の分析など、偽情報自体の特徴や偽情報が拡散する要因等を踏まえながら引き続き ICT リテラシー向上施策が効果的となるよう取り組み、産学官民が連携し、体系的で多元的なリテ

[33] いわゆる「こたつ記事」や「フェイクニュース・パイプライン」に関する問題が指摘されている。

ラシー啓発を実施することが必要である。

また、偽情報に対抗するために必要なリテラシーについては、例えば、EU等で先行する取組も参考にしつつ、コンテンツを作成し実施していくことが望ましいと考えられる。

さらに、偽情報は青少年だけでなく大人であっても拡散しているケースが見られるという分析結果を踏まえ、青少年だけでなく、大人も含め幅広い対象に対して実施することが必要である。
その際、総務省は、「e-ネットキャラバン」や「インターネットトラブル事例集」等の青少年向けの取組に加え、例えば、デジタル活用支援員の仕組みも活用した取組を検討していくことが必要である。

プラットフォーム事業者は、日本向けのリテラシー向上のための取組を実施するとともに、多様な利用者に対して効果的にアプローチするため、行政機関・関連団体・研究者等と協力し、「Disinformation 対策フォーラム」等も活用して、総合的な普及啓発の取組を促進することが望ましい。

⑨　研究開発の推進

モニタリング結果によると、ディープフェイクなどの新たな技術を悪用した偽情報が我が国においても出現しており、Facebook・Google・Twitter では、ディープフェイク対策の研究開発が行われている。
我が国においては、プラットフォーム事業者によるディープフェイク対策の研究開発は現時点で行われていないものの、研究者による偽情報対策の研究開発が行われている。

したがって、ディープフェイクに対抗にするための研究開発や技術コンテスト等の取組が我が国においても進められることが望ましい。

プラットフォーム事業者は、ディープフェイク対策のための研究開発を引き続き行うとともに、ディープフェイク等の偽情報に対応したポリシーを設けて、悪質度合いに応じて削除やラベルの付与等の適切な対応を行うことが望ましい。この際、日本語への対応や、日本人ユーザに対しても適切な形で対応可能な技術について研究開発を推進していくことが望ましい。

総務省は、諸外国及び国内での偽情報対策に資する研究開発の状況を継続的に把握し、関係者に対して情報共有を行うとともに、我が国における研究者が偽情報への対応に関する研究開発を行う際に必要なデータがプラットフォーム事業者から適切に提供されるよう、プラットフォーム事業者及び研究者と継続的な協議を行うことが望ましい。

⑩　国際的な対話の深化

違法・有害情報全般に関する政策に加えて、偽情報に関する政策についても、国際的な対話の深化を深めていくことが望ましい。

引き続き、諸外国における検討状況を把握しつつ、我が国においても、偽情報に特有の問題や政策的対応について引き続き検討していくことが適当である。同時に、我が国における偽情報の流通状況や、官学官民の検討状況について諸外国に共有を行い、それらの対話を通じて、特にグローバルにサービスを提供する事業者における適切な対応について、諸外国の情報通信担当部局等と連携しながら、実効的な対応を検討していくことが適当である。

第２部　利用者情報の適切な取扱いの確保について

第１章　プラットフォームサービスに係る利用者情報を巡る現状と課題

１　プラットフォームサービスに係る利用者情報の現状と課題

スマートフォンや IoT 等を通じて、様々なヒト・モノ・組織がインターネットにつながり、大量のデジタルデータの生成・集積が飛躍的に進展するとともに、AI によるデータ解析などを駆使した結果が現実社会にフィードバックされ、様々な社会的課題を解決する Society 5.0 の実現が志向されている。

インターネットへの接続についても大半がモバイル経由で行われており、SNS、動画共有サイト、ニュース配信、検索等含めた多くの情報流通がスマートフォン等経由で行われている。スマートフォン等を通じたインターネットの活用は社会経済活動のインフラとなるとともに、今後 AI の活用や IoT 化の進展に伴いデータ流通環境等が大きく変化することが想定される。ポストコロナ時代に向けて、デジタルシフトは更に進んでいくことが想定される。

この中で、様々なサービスを無料で提供するプラットフォーム事業者の存在感が高まっており、利用者情報[34]が取得・集積される傾向が強まっている。また、生活のために必要なサービスがスマートフォン等経由でプラットフォーム事業者により提供され、人々の日常生活におけるプラットフォーム事業者の重要性が高まる中で、より機微性の高い情報についても取得・蓄積されるようになってきている。

利用者の利便性と通信の秘密やプライバシー保護とのバランスを確保し、プラットフォーム機能が十分に発揮されるようにするためにも、プラットフォーム事業者がサービスの魅力を高め、利用者が安心してサービスが利用できるよう、利用者情報の適切な取扱いを確保していくことが重要である。

イノベーションや市場の発展を維持しつつ、利用者が安心してスマートフォンやインターネットを通じたサービスを利用していくことができる環境を確保していく上でも、関係する事業者それぞれにおいて利用者情報の適切な取扱いが確保されることが重要であると考えられる。

---

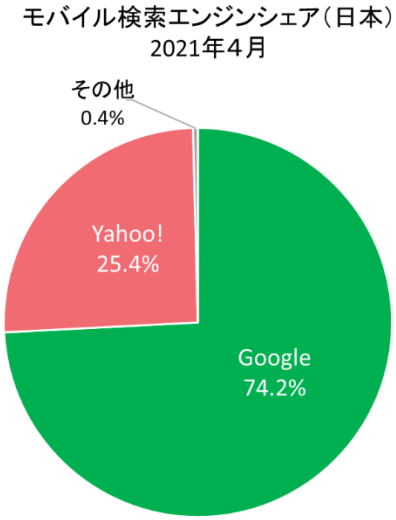
[34] 利用者情報としては、①利用者の識別に係る情報（氏名、住所等の契約者情報、ログインに必要な識別情報、クッキー技術を用いて生成された識別情報、契約者・端末固有 ID)、②通信サービス上の行動履歴や利用者の状態に関する情報（通信履歴、ウェブページ上の行動履歴、アプリケーションの利用履歴、位置情報、写真、動画、システム利用ログ、端末の設定等)、③第三者の情報（電話帳）等が含まれる。

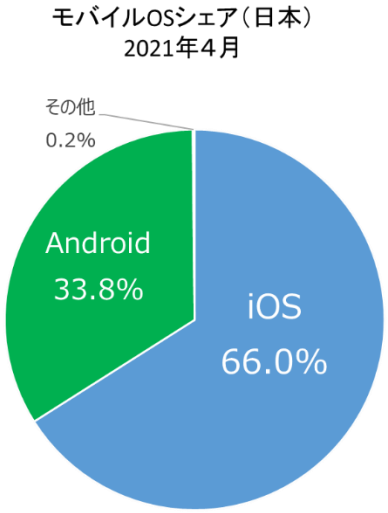
そのため、スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末 ID やクッキーなどの端末を識別する情報等の実態を把握した上で検討を行うことが適切である。

① プラットフォーム事業者の重要性

現在の我が国における市場の動向として、モバイルの検索エンジンのシェアは約 74%が Google であり、約 25%が Yahoo![35]となっている。

また、モバイル OS のシェアは、約 66%が Apple の提供する iOS(iPhone)であり、約 34%が Google の提供する Android である。各 OS に対応したアプリは、OS 提供事業者である Apple が運営する AppStore(iOS) 又は Google が運営する Google Play(Android)から入手可能となっている。





出典:StatCounter Global Statsから総務省作成

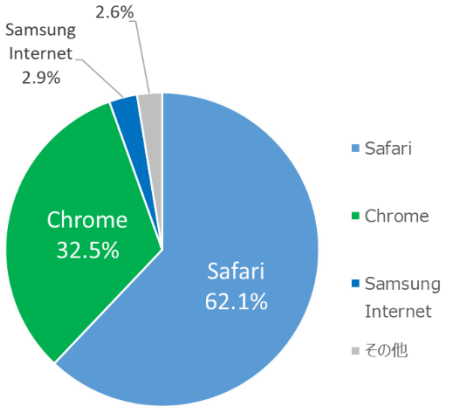
インターネット閲覧に用いるブラウザについては、モバイルブラウザのシェアは、約 62%が Apple の提供する Safari、約 33%が Google の提供する Chrome である。デスクトップ (PC)ブラウザのシェアは、約 59%が Google の提供する Chrome、約 23%が Microsoft の提供する Edge 又は IE、約 9%が Apple の提供する Safari である。

なお、インターネット広告のうち、約 76%がモバイル広告となっており、約 24%がデスクトップ広告となっているとされ、スマートフォンなどのモバイル経由でインターネットに接続し、プラットフォーム事業者

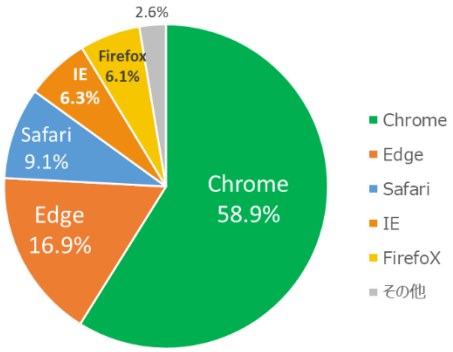
[35] Yahoo! Japan は、2010 年から Google の検索技術を利用している。

の提供するサービスを活用する場合が多くなってきていると考えられる。

モバイルブラウザシェア（日本）
2021年４月

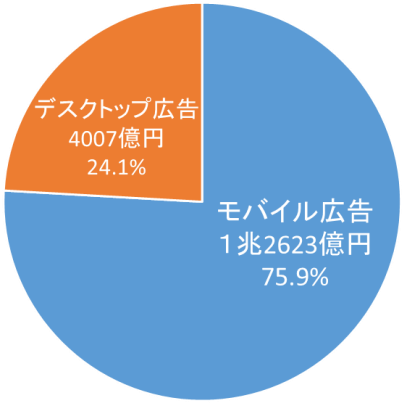


デスクトッププブラウザシェア（日本）
2021年４月



出典：Stat Counter Global Statsから総務省作成

インターネット広告媒体費（日本）
2019年　総額１兆6630億円



出典：2020 年４月３日 電通報
「日本の広告費 インターネット広告媒体費詳細分析 No.2」
から総務省作成

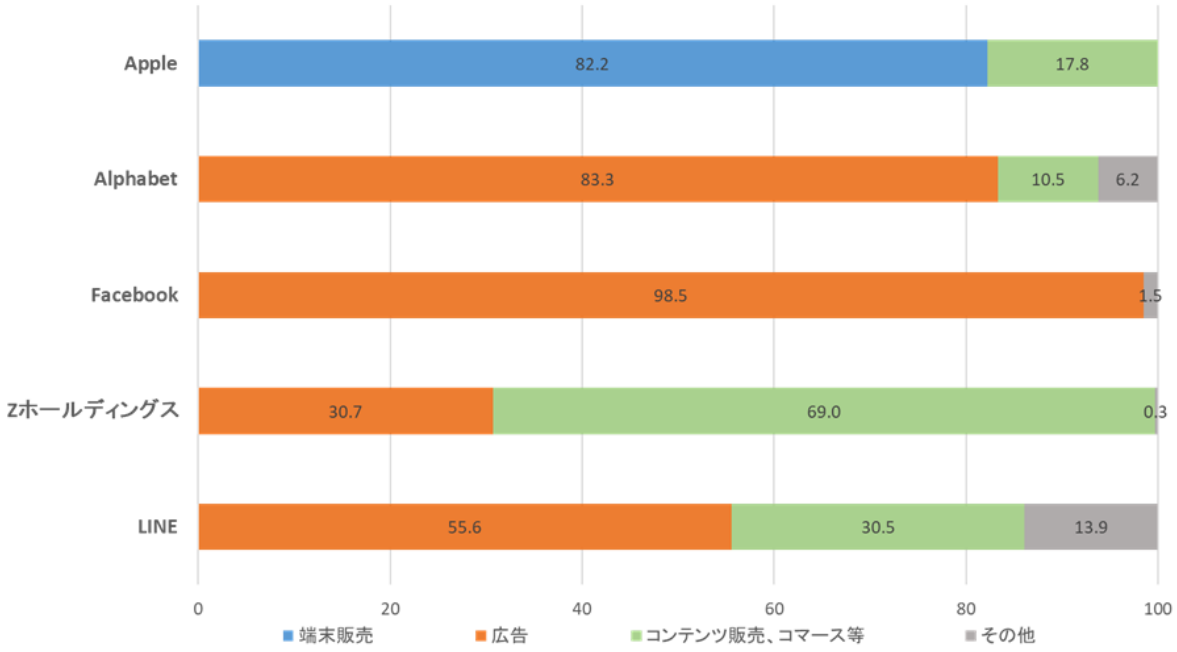
このように、検索、OS、ブラウザなどのインターネットを利用する際に不可欠な各分野において、プラットフォーム事業者は大きな役割を果たしている。

プラットフォーム事業者のセグメント別売上比率を見ると、広告の売上については、Facebook 及び Alphabet(Google)はそれぞれ約 99%、約

83%と大きな割合を占めており、LINE、Z ホールディングスもそれぞれ約56%、約 31%と相当の割合を占めている。また、コンテンツの売上については、会社によって割合に差異があるものの、Z ホールディングスが約 69%、LINE が約 31%、Apple が約 18%、Alphabet(Google)が約 11%と重要な位置づけとなっている。端末販売については、Apple が約 82%と大きな割合を占めている。

プラットフォーム事業者の事業領域には共通している部分と独自の部分があり、利用者情報の取得・蓄積・利用についてもそれぞれのプラットフォーム事業者による事業活動を踏まえたものとなることが想定される。

プラットフォーム事業者のセグメント別売上比率[36]



② 利用者情報の取扱いに関する動向

【スマートフォンにおけるアプリケーションに関連する動向】

スマートフォンにおいては、様々なアプリケーションが利用されているが、アプリケーションのプライバシーポリシーの掲載率は 2016 年

[36] Apple、Alphabet、Facebook については「How Big Tech Makes Their Billions」から 2019 年のデータにより総務省作成。 Z ホールディングスについてはセグメント別連結損益計算書推移表（IR 情報）から 2020 年度のデータにより総務省作成。LINE については決算補足説明資料（IR 情報）から 2019 年度第 4 四半期～2020 年度第 3 四半期のデータにより総務省作成。

以降大幅に向上してきている[37]。これは、スマートフォンの OS を提供するとともにアプリケーション提供マーケットを運営している Apple 及びGoogleがプライバシーポリシー掲載に関するガイドラインの策定や規制強化を実施しアプリケーション提供者に働きかけを強めてきたことによる影響が大きいと考えられる[38]。

一方で、会社全体やサービス全体を対象としたプライバシーポリシーを掲載するアプリケーションも多く、当該アプリケーションどの情報をどの目的のために取得するかは読み取りにくいとの指摘があり、簡略版の掲載率についても低水準で推移しており課題がある。

OS により、位置情報、カメラ、マイク、センサー、電話帳、カレンダー、フォトライブラリー、ヘルスデータ等のプライバシー性の高い情報へのアクセスを行う場合には、アプリケーション内で利用者に個別許可を求める機能等[39]も導入されている。

【Cookie[40]、広告 ID、タグ等に関連する動向】

Cookie には、First Party Cookie[41]と Third Party Cookie[42]があり、Third Party Cookie には、SNS 事業者、広告事業者、アクセス解析事業者、データ仲介事業者等に対する情報送信に利用されるものが多

---

[37] 本研究会（第 21 回）資料 5「スマートフォン　プライバシー　アウトルックの取組内容の紹介」(2020 年 11 月 5 日　(株)日本総合研究所)　P6 等

[38] Apple は 2016 年 6 月に App Store 審査ガイドラインを大幅に改正しデバイスからの利用者情報（位置情報、連絡先、カレンダー等）のアクセスを実施するアプリケーションはプライバシーポリシーを明示すべきとし、2018 年 8 月には全てのアプリにプライバシーポリシーの掲載を義務付けており、2020 年 12 月以降新規アプリの提出/更新時にアプリのプライバシー情報（取得するデータ等）について提出するように義務づけており提出されたアプリのプライバシー情報は App Store のアプリ紹介ページで表示される。また、Google は 2016 年 12 月にプライバシーポリシーが掲載されていないアプリへの警告、2017 年には個人情報をユーザーの同意なく収集するアプリに対する警告を行っている。(本研究会（第 21 回）資料 5　P7-8、利用者情報WG（第 4 回）資料 2「スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る調査・分析」(2021 年 5 月 18 日(株)日本総合研究所）P21)

[39] Apple の提供する iOS の場合には、数年前から個別同意を取得する仕様が導入されており、iOS10 では同意を取得する際に情報の取得理由・利用目的等の説明文の記載が必須となっている。Google の提供する Android の場合には、Android6.0 ではパーミッションモデルが変更され、インストール時には危険でないパーミッションのみ付与し、危険なパーミッションはアプリ内で個別に利用者の同意を取得するモデルに変更された（本研究会（第 21 回）資料 5　P12-13）

[40] ウェブサイトを訪問した際、ブラウザ上に一時的に情報を保存する仕組み。Cookie によって保存された情報を Cookie 情報とも言う。

[41] Cookie のうち、利用者が訪問したウェブサイトにおいて一時的に保存される情報を特に First Party Cookie という。

[42] Cookie のうち、利用者が訪問したウェブサイトにおいて、当該ウェブサイトの運営者ではなく、第三者である SNS 事業者、広告事業者、アクセス解析事業者、データ仲介事業者等によって一時的に保存される情報を特に Third Party Cookie という。

く見られる。また、イメージタグや JavaScript のタグ[43]、OS が発行する広告 ID[44]等による情報収集も多く行われている。

広告事業者等は、このような Third Party Cookie、タグ、広告 ID 等をキーに、クロスサイトでトラッキングを行いウェブサイトの閲覧履歴[45]を取得・蓄積・分析等行った上で、広告配信等に活用していると考えられる。一方、このような情報取得が行われる Third Party Cookie やタグ等については、それが設置されるウェブサイト管理者が実情を把握しにくく、そのためプライバシーポリシーがきちんと書けていない場合[46]も多いとの指摘がある。また、利用者にとってもプライバシーポリシーが分かりにくく、自分のデータがどう扱われているか把握することが難しいという課題がある。

近年、オンライン広告におけるプライバシー侵害への危機感が高まり、欧米において利用者情報の取扱いに関する透明性やアカウンタビリティを高める法制度の適用が見られることも背景とし、プラットフォーム事業者等関係事業者においてクロスサイトトラッキングをブロック又は抑制する方向で様々な検討が行われている。

例えば、モバイル及び PC ともにプラットフォーム事業者が高いシェアを有しているブラウザにおいては、Apple が提供する Safari（モバイル/PC）において ITP(Intelligent Tracking Prevention)が実装され Third Party Cookie をはじめクロスサイトトラッキングが既にブロック[47]されている。このような動きは他のブラウザでも見られ、Firefox は ETP(Enhanced Tacking Protection)が実装されクロスサイトトラッキングクッキー等が制限され、初期設定（デフォルト）でリダイレクト

---

[43] 現在は Java Script のタグ（JS タグ）が主流であり、従来のイメージタグより多くの情報（例：ページに表示される情報、画面サイズなどの環境情報、フォーム入力情報等）が取得可能であり、ほかの JS タグの強制的読み込み等も可能で、ウェブサイト運営者が知らないうちに JS タグが増える場合もあると指摘される。（本研究会（第 22 回）資料 3「利用者情報取扱いの実態」（2020 年 12 月 4 日　太田祐一）P12-14）

[44] Apple が発行する IDFA、Google が発行する AAID 等

[45] 利用者情報 WG（第 3 回）資料 1「オンライン広告における利用者情報取扱いの動向」（2021 年 4 月 22 日　寺田構成員）P 2、利用者情報WG（第 4 回）資料 3「利用者端末情報等に関する規制の方向性」（2021 年 5 月 18 日　森構成員）P6-P9

[46] ネット通販など消費者向けサイトを運営する主要 100 社のうち 5 割が、Cookie 等により、具体的な提供先を明示せずに外部とユーザーの利用データを共有していたとされる（日本経済新聞 2019 年 2 月 26 日 1 面）。また、国内の消費者向け主要サイトの約 2 割で外部から分かりにくいデバイスフィンガープリント等の利用者追跡技術が使われているとされる（日本経済新聞 2020 年 12 月 19 日）。

[47] Apple は 2017 年に Safari に ITP(Intelligent Tracking Prevention)を実装することを発表し、段階的に実装が進められ、2020 年 3 月に発表された Full Third-Party Cookie Blocking and More では完全な Third Party Cookie のブロックが行われているほか、すべてのスクリプトが書込み可能なストレージの有効期間を 7 日間に制限している。

トラッキングも制限されている。また、Google は Chrome における Third Party Cookie の段階的廃止を計画(2023 年後半に廃止見込み[48])していることを発表している。

また、OS が提供する広告 ID については、Apple の提供する IDFA(Identifier For Advertisers)については、これを利用するために 2021 年 4 月 26 日以降、利用者の同意を取得することが必要となった（ATT：App Tracking Transparency Framework)。

Google は、2019 年５月に Web 上のプライバシーを強化する一環として、Privacy Sandbox Project を発表している。従来のようにクロスサイトのトラッキングにより、個人の閲覧データを企業等が独自で収集することを防ぐとともに、FLoC (Federated Learning of Cohorts)としてブラウザがインストールされた端末中で機械学習を利用して行動履歴を AI により分析し、同種の興味関心を持つ数千人のグループ（Cohorts）を作成しこれをターゲティング広告の対象とすることを提案している。広告配信主は、Cohorts が配信先として選択できるように提供[49]されるとしている。Google は、自らが提供するブラウザである Chrome[50]において、オリジントライアル（Origin Trial）を開始[51]している。

また、Google は TURTLEDOVE[52]でアドサーバーではなく利用者の端末

---

[48] Google は従来 Chrome における Third Party Cookie の廃止期限を 2022 年としていたが、2021 年 6 月に発表したブログポスト“An updated timeline for Privacy Sandbox milestones”において、Chrome における Third Party Cookie の廃止期限を 2023 年後半まで延長したと発表。同ブログポストにおいて、英国 CMA（Competition and Market Authority）との関係も踏まえ、Privacy Sandbox のウェブコミュニティーへの影響を見定め第一段階として 2022 年後半以降に Chrome の技術的仕様を固めた上で、第二段階として 2023 年中盤以降に 3 ヶ月かけて 2023 年後半までに Third Party Cookie を廃止する見通しが言及されている。（https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/ 2021 年 6 月 24 日）

[49] Google は Privacy Sandbox Project としてオープンスタンダードを開発するとしており、World Wide Web Consortium(W3C)の場においても議論を進めており、2021 年 1 月 25 日に Chromium Blog 記事やホワイトペーパが発表されている。Google の広告チームによると、Chrome の FLoC の技術使用に定義された原則に基づくシミュレーションを実施した結果、Third Party Cookie を利用した広告と比べて投資 1 ドル当りの広告効果（コンバージョン率）は 95%近い値であったとしている。

[50] Privacy Sandbox は、世界的に高いシェアを持つブラウザの Chrome があるからこそできる構想であるとの指摘もあり、英国の CMA はこの件について正式な調査手続を開始することを発表した。

[51] 2021 年 3 月に Chrome の新バージョンリリースではオリジントライアル（Origin Trial）を通じて公開テストを開始し、今後広告プロバイダを交えた検証を実施する予定としている。なお、利用者による FLoC からのオプトアウトについて、ブラウザの中に UI として含める予定としているが、詳細は現在検討中とされている。

[52] TURTLEDOVE は、“Two Uncorrelated Requests, Then Locally-Executed Decision On Victory”の頭文字の略語。広告の入札オークションを、広告事業者等のサーバーから、ブラウザ（ブラウザがインストールされた個人の端末内）に移行させる提案。

内のブラウザ上で広告オークションを実行することを実現する提案を発表している。この TURTLEDOVE の実現に向けて、FLEDGE（First Locally-Executed Decision over Groups Experiment)が提案されており、広告のオークションを「信頼できるサーバー」で行うとしている[53]。

【業界団体等の動向】

業界団体である欧州インタラクティブ広告協議会（IAB Europe）とIAB テックラボ（IAB Tech Lab）は、GDPR に準拠しながら、従来からのプログラマティック広告を利用し続けられるようにするための業界標準基準として TCF(Transparency and Consent Framework）を 2016 年に策定、2019 年に TCF 2.0 に改訂している。TCF をベースとした、同意管理プラットフォーム（CMP：Consent Management Platform[54]）の導入の動きが進んでいる。

上記でみたようなグローバルなプラットフォーム事業者によるクロスサイトトラッキングを規制する方向の動きを踏まえ、オンライン広告市場におけるアドテク企業やパブリッシャーが様々な対応を検討する動きが見られる。

業界団体はデジタル広告のアーキテクチャーの再構築（re-architect）が必要であるとして、Project Rearc[55]を立ち上げるとともに、PRAM（Partnership for Responsible Addressable Media）としてデジタル広告に係わる業界団体[56]、広告主、エージェンシー、パブリッシャー、アドテク企業等が横断的に参加した取組についても進めている。代替 ID としてフィンガープリントや Unified ID2.0（メールアドレスハッシュ化）を用いて、クロスサイトラッキングを検討する動きもある。これについては、同意取得の在り方やオプトアウトの在り方

---

[53] GOOGLE ADS へのブログポスト“Building a privacy-first future for web advertising”(2021 年 1 月 25 日)https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/より。

[54] IAB Tech による CMP の概要としては、利用者が何について同意又は拒否したかが記録され、ベンダー間で流通するとされている。データにアクセスできるベンダーは登録されており、同意取得のステータスに従って対応することとされている。一方、TCF に準拠していないものも CMP と称しており、一般の利用者には判別が難しい状況であることについても注意が必要である。（利用者情報WG（第 3 回）資料 1 P6-7）

[55] ①TCF 2.0 をベースにした各国の規制に対応する規格としての Global Privacy Platform(GPP)、②同意や設定を広告サプライチェーン全域で監督可能とする仕様としての Accountability Platform、③ユーザーが使用可能な ID トークンのベストプラクティス、④売り手側により定義されたオーディエンスや文脈によるシグナリングを助けるための分類法とデータ透明性基準等が提案されており、3 月に意見募集草案が発表されている。（利用者情報 WG（第 3 回）資料 1 P11）（“Standards for Responsible Addressability and Predictable Privacy”、IAB Tech Labo、2021 年 3 月 https://iabtechlab.com/standards/addressability-accountability-privacy/）

[56] 全米広告業協会（4 A's)、全米広告主協会（ANA)、インタラクティブ広告協議会（IAB)、IAB Tech Lab、Network Advertising Initiative(NAI)、世界広告主連盟（WFA）

をどのようにするのかという課題も指摘される[57]。

また、パブリッシャーが 1st Party Cookie によるターゲティングを重視する動きも活発化している。また、ユーザーが閲覧している Web ページを AI で分析し、そのページのコンテキストに合致する広告を出稿する Contextual Targeting についても検討が行われている[58]。

このように、パーソナルデータの取扱いを巡っては各国における法規制や自主規制の動きがある中で、先に見たような OS やブラウザーを提供するプラットフォーム事業者による広告 ID やブラウザの Third Party Cookie の規制などクロスサイトのトラッキング制限の検討が行われており、これはデジタル広告業界に大きな影響を与えるものである。このような動きに対応しつつ、業界団体や業界内でも利用者の関与を可能にするサービスやソリューションの開発、事業連携を進める動きも検討されつつある状況であり、現在は大きな転換期にあるものと指摘される[59]。

２　現行制度と政策

（１）　個人情報保護法及び電気通信事業 GL

事業者による個人情報の取扱いについて個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）により規律されている。令和２年改正で、違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならないこと、漏えい等事案の報告及び通知の義務化、個人関連情報の第三者提供規制、保有個人データの開示方法や利用停止・消去等の請求権の要件緩和、仮名加工情報の新設、域外適用の拡大、特定部門を対象とする認定団体、罰則等の個人の権利の在り方及び事業者の守るべき責務の在り方について見直しが行われた。また、令和３年にはデジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第 37 号）が成立した。両改正とも令和４年４月

---

[57] Apple は Device Fingerprint は規約で禁止するとしており、Privacy Sandbox 構想を提案している Google は個々のユーザーレベルのトラッキングに賛成していないとされ、Third-party cookie のサポートを終了した時点で他の代替 ID もサポートしないと表明している。(第３回 WG 資料１　P11 等) 一方、プラットフォーム事業者は自社の中ではメールアドレスやログイン情報等のアカウント情報をキーとした上で顧客情報を集約・分析できるためウォールドガーデンになっているという指摘がある。また、プラットフォーム事業者がルールメイカーとなることによる業界構造や市場競争への影響についても留意すべきとの指摘もある。

[58] 利用者情報 WG（第３回）資料１　P10 等

[59] 利用者情報WG（第１回）資料４「インターネット広告市場の動向と利用者情報の取扱いに関する取組について」(2021 年 3 月 18 日、(一社) 日本インタラクティブ広告協会 (JIAA)) P27-28

施行予定である。

電気通信事業法（昭和 59 年法律第 86 号）に通信の秘密が規定されており、本年４月から令和２年改正（域外適用）が施行された。

電気通信事業における個人情報保護に関するガイドライン（平成 29 年総務省告示第 152 号。以下「電気通信事業 GL」という。）において、電気通信事業分野の個人情報保護及び通信の秘密等について規定されている。（電気通信事業 GL において、電気通信事業の性質などを踏まえ、個人情報保護管理者、プライバシーポリシー、各種情報の取扱い（通信履歴の記録、位置情報等）についても規定されている。）個人情報保護法の令和２年改正及び電気通信事業の性質等を踏まえた上で、電気通信事業 GL の見直しを検討する必要がある。

（２）　SPI 及び SPO

総務省の「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」（座長：堀部政男一橋大学名誉教授）は、利用者が安心安全にスマートフォンのアプリを利用できる環境を確保するため、スマートフォンの利用者情報の適切な取扱いについて検討し、スマートフォン　プライバシー　イニシアティブ（SPI）を２012 年に公表。スマートフォン利用者情報取扱指針として、６つの基本原則とアプリ提供者、情報収集モジュール提供者等の利用者情報取得者における取組、アプリ提供サイト運営者等の関係事業者における取組を示した。

SPI の実施状況等について 2013 年からスマートフォン　プライバシーアウトルック（SPO)として毎年継続的に調査を実施しこれを公表してきている。主に、人気アプリ 100、新着アプリ 100 についてプライバシーポリシーの掲載有無、掲載の場合には SPI に定められた８項目が記載されているか等を調査しており、プライバシーポリシーの掲載率などは向上してきている。

直近とりまとめられた SPOⅧにおいて、人気アプリは Android、iOS ともにプラポリの掲載率は昨年同様 100%に近い形であり、重要とされる事項（アプリ提供者名、取得項目、利用目的、第三者提供の有無等）も記載率は高い。一方、新着アプリは、Android のプラポリ掲載率が 60%台まで大きく下がっており、SPI に定められた項目の記載率も Android/iOS ともに下がっており少し質の低下が見られる。

電気通信事業 GL においても SPI を踏まえた規定（アプリケーションポリシーを提供する場合、アプリケーションを提供するサイトを運営する場合、アプリケーションのプライバシーポリシーに記載すべき具体的項

目）が設けられており、SPI の内容を踏まえた事業者団体のガイドライン等も策定されている。

アプリマーケット運営事業者の取組としては、Google、Apple ともに OS のバージョンを上げるたびに、プライバシー関連機能は強化されている。Apple は、App Store のアプリ紹介ページに、アイコンで取得される情報と利用目的について分類して表示しており、アプリ提供者にはアプリ更新や新規アプリの際に情報提出が義務化されている。

（３） 位置情報プライバシーレポート

位置情報プライバシーレポートは 2014 年に策定され、電気通信事業者が取り 扱う位置情報として基地局に係る位置情報、GPS 位置情報、Wi-Fi 位置情報の概要について整理した上で、十分な匿名化の枠組みについて検討。これを踏まえ、「十分な匿名化」の加工基準等がまとめられ、民間ガイドラインが作成された。また、利活用モデルなどについて検討された。

位置情報について端末から直接取得されるものだけでなく、他の色々な手段や情報から位置情報が取得できるようになってきている（例えば、リアル店舗での購買履歴はすべて位置情報になるのが実情である。）ことを前提とした上で、位置情報の精度・種類・性質等も踏まえた上で、その取扱いの在り方について検討していくことが重要であるとの指摘がある。

電気通信事業 GL・解説において、位置情報プライバシーレポートを踏まえた記載（通信の秘密に該当する位置情報及び通信の秘密に該当しない位置情報等の取扱いについて）があり、これを踏まえ事業者団体のガイドライン等も策定されている。

（４） 一般社団法人日本インタラクティブ広告協会（JIAA）

JIAA において、インターネット広告ビジネスにおいて取得・利用されている個人に関する情報の取扱いについて、事業者向けの指針として、「プライバシーポリシーガイドライン」（2004 年策定、2017 年再改定）、「行動ターゲティング広告ガイドライン」（2009 年策定、2016 年再改定）を策定。JIAA はガイドラインの啓発活動を行うとともに、技術の進展やビジネスの実態の変化に応じ見直しを行っている。行動ターゲティング広告ガイドラインでは、行動ターゲティング広告でのユーザーへの「透明性の確保」と「関与（オプトアウト）の機会の確保」の徹底を原則とし、媒体運営者、情報取得者、配信事業者に区分してその事業領域ごとに遵守事項を規定している。

JIAA 会員社は広告配信事業者がメインであり、会員社ではない媒体社や広告主にまでは直接規律が及ばないという課題が指摘される。

アドフラウドを含む無効配信の除外と広告掲載先品質に伴うブランドセーフティの確保に関して事業者を認証し公開するJICDAQの取組が2021年４月開始された。

（５） デジタル広告市場

本年４月にデジタル市場競争会議により「デジタル広告市場の競争評価　最終報告」が発表されており、同報告書中で「課題⑩：[パーソナル・データ］パーソナル・データの取得・利用に係る懸念」への対応については、電気通信事業における個人情報保護に関するガイドラインなどの見直しにより対応することとされており[60]、同報告書における検討内容も踏まえ総務省において検討を進めることが求められている。

（６） 競争政策とデータ保護・消費者保護の関係

公正取引委員会競争政策研究センターは昨年 11 月より「データ市場に係る競争政策に関する検討会」を開催し、本年６月に報告書を発表している。同報告書において、これまでの検討結果等[61]も踏まえ、競争政策の観

---

60 「デジタル広告市場の競争評価　最終報告」（2021 年 4 月 27 日、デジタル市場競争会議）「課題⑩：[パーソナル・データ］パーソナル・データの取得・利用に係る懸念」の「7　対応の方向性」において、「プラットフォーム事業者をはじめとするターゲティング広告に関係する事業者等による消費者のパーソナル・データの取得・利用に係る懸念を払拭するために一定の対応が必要である」とされ、具体的には以下のような情報の開示が適切になされていることが求められる。

- 消費者が自らのパーソナル・データに係る取扱いについて予見可能性をもって理解し得る程度の情報として、①「取得する情報の内容」、②「取得の条件」（取得方法等）、③「使用の条件」（利用目的、利用の方法、第三者に提供する場合の条件、本人の関与等）の開示（＊開示に当たっては、併せて、クロスデバイスでのデータ利用などにおいて複雑なデータの流れや使用方法についての説明の検討も必要となる）。
- ターゲティング広告を実施する旨及び事前の設定の機会やオプトアウト機会の提供についての開示。
- 消費者がデータの取得・利用を拒否した場合でも、サービスを利用するオプションが提供されるか否かについての開示。
- データ・ポータビリティの可否・方法についての開示。

これらの４つの項目については、「総務省においては、「電気通信事業における個人情報保護に関するガイドライン」等の指針等の今秋に向けた見直しを検討しているところ、その見直しにおいて、盛り込むよう求めることとする。」とされるとともに、「総務省の同ガイドラインの見直し改定・運用に当たっては、個人情報保護委員会との連携も引き続き行い、関係省庁の間での対応に齟齬が生じないようにすることとする」とされていることを踏まえて、今後総務省において検討を進めていくことが必要である。

61 「データと競争政策に関する検討会　報告書」（平成 29 年 6 月 6 日、公正取引委員会競争政策研究センター）、「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」（令和元年 12 月 17 日、公正取引委員会）、「デジタル広告分野の取引実態に関する最終報告書」（令和 3 年 2 月 17 日、公正取引委員会）“Privacy and competitiveness in the age of big data”（2014 年 3 月 26 日、European

点から「パーソナルデータが取り扱われるデータ市場に係る議論を行う際」には、「「Competition（競争）」、「Data Protection（データ保護）」及び「Consumer Protection（消費者保護）」の３つについて別個に議論するのではなく、三位一体での議論を行い、３つのバランスを欠かないようにすることが重要である」と指摘[62]されている。また、この観点を踏まえ、パーソナルデータを含めたデータポータビリティの確保や情報銀行に係る取組等について検討されている。

３　海外動向

（１）　米国

①　米国の個人情報保護関係規制

米国では、公共部門と民間部門毎に、連邦や州の個別法（例：金融、子供　のデータ、健康データ等）に個人情報に関する規定が設けられている。

FTC （Federal Trade Commission）は「不公正若しくは欺瞞的な行為又は慣行を禁止」するFTC法第５条に基づき、企業のプライバシーポリシーやITセキュリティ等に関しても規制・執行。

②　カリフォルニア州CCPA/CPRA

カリフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act）は、2020年１月施行、７月当局による執行開始（CCPA規則は2020年８月発効[63]）。CCPAにおいて、個人情報[64]の収集やオプトア

Data Protection Supervisor（EDPS））等

[62] 同報告書において、「競争、データ保護及び消費者保護の３つが対立し得るデータ市場の構造を見極めながら、当該三位一体のフレームワークを意識して取組を進めていく必要がある」、「仕組み作りに際して、幅広い関係者を交えて丁寧に検討したり、政府等も関与をして検討・・取組は、安心感・信頼性を高め有効」等と指摘されている。

[63] CCPA規則では通知とプライバシーポリシーを別のものとして規定している。

[64] CCPA第1798.140条(o)にて「「個人情報」とは「特定の消費者又は世帯を、識別し、関連し、叙述し、合理的に関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできる情報を意味する。」とされており、具体的には、同条中「(A) 識別子。例えば、・・一意個人識別子、オンライン識別子・・又は類似の識別子。」、「(F) インターネット又はその他の電子的なネットワーク活動の情報。閲覧履歴、検索履歴、及び、インターネット・ウェブサイト、アプリケーション又は広告との消費者のやりとりの情報を含む」、「(K) 消費者のプロファイルを作成するために本項で識別された情報から引き出された、推定。」等が含まれると規定され、同条（x）にて「一意個人識別子」とは、デバイス識別子、インターネット・プロトコル・アドレス、クッキー、ビーコン、ピクセルタグ、モバイル広告識別子等が含まれるとされている。

ウト権に関しては、プライバシーポリシーへの記載だけではなく、これとは別に消費者への通知が必要とされる。 例えば、個人情報の収集に係る通知を行う際のルールとして、専門用語を避けた簡潔でわかりやすい表現、小さな画面でも読みやすく目立つ形式とすること等を定めている。また、通知内容として個人情報の種類一覧、個人情報の種類ごとの利用目的、オプトアウトページ及びプライバシーポリシーへのリンク（オフラインの場合は URL）等を定めている。これらは、ある意味階層表示の一つと分類できる。

2020 年 11 月住民投票が行われ、CCPA を改定するカリフォルニア州プライバシー権法（CPRA：California Privacy Rights Act）が成立[65]。CPRA では、通知項目としてクロスサイトトラッキングに関する事項[66]や個人データの保存期間等が含まれることとなった。また、Third Party Cookie 等を利用したクロスサイトトラッキングに対応した「共有するな」ボタンの義務化[67]が定められた。

③　NIST　Privacy Framework

米国国立標準技術研究所（NIST)によって NIST　Privacy　Framework（NIST PF)は、個人のプライバシー保護を実現する上で参考にすべき枠組みとして、セキュリティ分野の枠組みである NIST　Cybersecurity Framework（NIST CF)の姉妹編として作成され、NIST CF と NIST PF をシームレスに統合した文書として SP800-53 が提示されている。この中で、同意取得を行う際の推奨手法として、同意をよりカスタマイズする Tailored Consent、ジャストインタイムの同意、同意の撤回などを記載。通知を行う際の推奨手法として、ジャストインタイムの通知などを記載。プライバシー影響評価についても言及している。

④　その他

---

[65] 2022 年 1 月以降に取得した個人情報に CPRA 適用、2023 年 1 月に CPRA 全面施行、2023 年 7 月以降当局の執行開始予定

[66] アドネットワーク運営者、個人情報を間接取得する者等についても、CPRA に基づき、取得時通知を直接行うか、又は取得時通知で通知すべき事項をプライバシーポリシーとして公表する義務を有する。

[67] 消費者の「共有」のオプトアウト（停止請求）権、(16 歳未満の消費者についてはオプトイン）が規定された。これにより、行動ターゲティング広告目的の開示を確実に消費者のオプトアウト権の対象となると考えられる。また、オプトインその他の「同意」に関し、GDPR の「同意」（4(11)）とほぼ同じ要件（自由意志性、明確性等）が規定され、いわゆる「ダークパターン」による同意取得は無効とされている。

米国において連邦レベルで複数の利用者情報の取扱い等に関する法案が提出されている。例えば、本年５月に提出されたソーシャルメディアアクト（Social Media Disclosure and Transparency of Advertisements Act of 2021[68]）において、大規模な事業者に学術経験者やFTCがプロファイリングやカテゴリーのライブラリーにアクセスできるようにすることを求めている。

（２） EU

① GDPR

EU では、個人データやプライバシーの保護を 1995 年から適用されていた「EU データ保護指令（Data Protection Directive 95)」より厳格に規定し加盟各国に直接適用する法として、一般データ保護規則（GDPR: General Data Protection Regulation)が 2018 年５月に施行された[69]。

GDPR の規定に関して、同意、透明性、自動化された個人に対する意思決定とプロファイリング、データ保護影響評価（DPIA)、データポータビリティの権利[70]等についてガイドラインが定められ、詳細に解説されている。

同意については、「同意に関するガイドライン」において、GDPR 第４条(11) に規定する有効な同意の要素である、「自由/自由に与えられた」、「特定の」、「説明を受けた」、「不明瞭でない意思表示」について解説し、情報を提供する在り方や有効な同意を得るための追加的条件（同意の証明、同意の撤回）を定めている。

同ガイドラインにおいて、有効な同意の要素である「自由/自由に与え

[68] ロリ・タラハン（Lori Trahan）下院議員（マサチューセッツ州３区選出・民主党）議員が 2021 年 5 月 20 日に提出。

[69] GDPR 第 4 条(1)において「個人データ」とは、「識別された自然人又は識別可能な自然人（データ主体）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、・・・直接的又は間接的に識別されうる者をいう。」と規定されている。

[70] 豪州では、個人情報保護については 1988 年連邦プライバシー法により規制されている一方で、2017 年に消費者データ権（Consumer Data Right。企業が保有する個人情報へ安全にアクセスする権利を消費者に付与するもの。）が導入されている。また、OECD では、競争委員会において、データポータビリティと相互運用方策の実施に関わる調査をするための討議が本年６月に行われている。

られた」について、力の不均衡、条件性[71]、粒度[72]、不利益を受けずに同意を拒否又は撤回できることが考慮事項として示されている。また、同意が「説明を受けた」上でのものとなる最小限の内容としては、管理者の身元、同意が求められるそれぞれの取扱い業務の目的、収集され利用されるデータ（そのタイプ）、同意を撤回する権利の存在、関連する場合GDPR第22条(2)(c)に従い自動化された意思決定のためのデータ利用についての情報及び十分性認定及び第46条で述べられる適切な保護措置がないことによるデータ移転の起こりうるリスクについて情報を提供する必要があるとされている。

また同ガイドラインにおいて、情報を提供する在り方として、メッセージが法律家だけでなく標準的な人にも容易に理解できるように明確かつ平易な用語を用いること、理解が困難な長文のプライバシーポリシーや法律の専門用語の多い説明を使用することができないとされている。同意は、他の事項とはっきり区別できるように[73]し、理解しやすく容易にアクセスできる方法で提供しなければならないとされている。また、同意を取得する対象がどのような種類の人々かを評価することが求められており、それを踏まえ理解できるように情報を示し説明することとされている。更に、小さなスクリーン又は限定されたスペースの中に情報を入れるときには、階層化された情報提示の方法が考えられるとされている。

更に、(事業者はそのサービスに合わせた同意フロー、同意メカニズムを自由に作ることができるものの）有効な同意は「陳述又は明確な積極的行為」による「不明瞭でない表示」を必要とすることとし、例えば、予めチェックの入ったオプトインのチェックボックスの利用やデータ主体の沈黙、アクティブ化しないこと、単にサービスを利用することは、選択についての積極的な表示とみなすことはできないとしている。また、同意の撤回については、実際上、同意と同等の容易さでその同意の撤回をできなければならない[74]としている。

透明性は、市民が自らに影響を及ぼすプロセスについて理解し、必要

---

[71] GDPR第7条(4)にあるように、サービス提供を含む契約がそれに結びついた個人データを取り扱うための同意を要求している場合には、最大限これを考慮される。

[72] 粒度（Granularity）として、一つのサービスが複数の目的のためにいくつもの取扱業務を行う場合、データ主体はひとまとまりの取扱いの目的に同意しなければならないのではなく、どの目的に対して承諾するのか選択できるようにすべきとされている。

[73] 同意するかどうかについて説明を受けた上での決定をすることに関連する情報が、一般的な条件の中に隠されてはならないことを意味している。

[74] 撤回のためだけに他のインターフェースへ変えることは不当な努力を求めるとされている。また、同意が撤回される場合、撤回前のデータ取扱業務は適法であるが、撤回後は関係するデータの取扱いを中止し、そのデータを消去しなければならないとしている。

に応　じてこれに異議を唱えられるようにすることで、そうしたプロセスへの信頼を生み出すためのものと位置づけられている。「透明性に関するガイドライン」において、GDPR 第 12 条に規定する「簡潔で、透明性があり、理解しやすく、容易にアクセスできる」、「明瞭かつ平易な文言が使われなければならず」などについて解説している。

同ガイドラインにおいて、「簡潔で、透明性がある」については、階層的なプライバシーステートメント/プライバシー通知を用いることが推奨[75]されている。GDPR 第 13 条及び第 14 条に基づく情報全体を包括的に提供する要件[76]がある一方、その情報を簡素で、透明性があり、理解しやすく容易にアクセスしうる形式でデータ主体に提供するという要件の間で緊張関係がある中でこれを両立する観点から、階層的なプライバシーステートメント/プライバシー通知が推奨されている。階層的なアプローチにおいて、第一の階層に、最も重要な情報である、取扱目的の詳細、管理者の身元、データ主体の権利の説明、データ主体への影響が最も大きい取扱いや不意打ちとなりかねない取扱いに関する情報も含めることが勧告されている。また、プッシュ及びプル通知の事例としてのプライバシーダッシュボード、ジャストインタイムの通知、視覚化ツールの事例としてのアイコンなどが手法として推奨されている。

「理解しやすく」については、対象とする者の平均的な人々に理解されるも　のであることが求められ、ユーザーインターフェイス/通知/ポリシーなどの有効性について確信できない場合にはユーザーによる公開討論、可読性テスト、業界団体・消費者擁護団体・規制当局との対話の仕組みを通じた試験を行うことができるとされている。対象とする者が自らの個人データの使途に関して理解することにより、後の時点で不意をつかれることとならないようにすることが必要[77]とされている。

「容易にアクセスできる」については、データ主体が情報を探す必要がないことを意味し、階層的なプライバシーステートメント、アプリの場合ダウンロード前やダウンロード後２タップ以内にアクセスでき、アプリ固有のプライバシー情報を示すことなどが示されている。

---

[75] 同ガイドラインにおいて、データ主体が、オンラインの文脈において大量のテキストをスクロールすることを要せず、プライバシーステートメント／プライバシー通知のアクセスしたい箇所を直ちに表示できるようになると指摘されている。

[76] 管理者の身元と連絡先の詳細、データ保護オフィサーの連絡先の詳細、取得目的とその法的根拠、正当な利益、関係する個人データの種類、個人データの取得者、第三国への移転の詳細、保存期間、データ主体の権利（アクセス、訂正、消去、取扱いの制限・異議、ポータビリティ）、同意撤回の権利、監督機関に不服を申立てる権利、契約上の要件、個人データが発生した情報源、プロファイリングを含む自動化された意思決定の存在や使われているロジックや想定される結果に関する情報等

[77] 同ガイドラインにおいて、特に、複雑なデータ、技術的データ、又は予期せぬデータの取扱いの場合、第 29 条作業部会が示している見解は、取扱いによる最も重大な結果としてどのようなものが生じるのかを、明確な文言で別途明記すべき、すなわち、データ主体が実際に被る影響はどのようなものか明記するとされている。

これらについては、実装例を含め国際的なベストプラクティスが参考になると考えられる。

英国データ保護機関（ICO：Information Commissioner’s Office）はGDPR を踏まえ、より効果的に通知・同意取得を行うことができるために推奨する工夫として、以下の５つの手法を挙げている：①階層的アプローチ、②ダッシュボード、③ジャストインタイム、④アイコン、⑤モバイル及びスマートデバイスの機能性。

また、仏国データ保護機関（CNIL）も Google の Agreement の中にプライバシーポリシーの仕組みとして階層的アプローチを含めている。

ICO において推奨される通知・同意取得における工夫

1. **階層的アプローチ（ A layered approach ）**
   重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。

2. **ダッシュボード（ Dashboards ）**
   管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。

3. **ジャストインタイム通知（ Just-in-time notices ）**
   個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。

4. **アイコン（ Icons ）**
   特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。

5. **モバイルおよびスマートデバイスの機能性（ Mobile and smart device functionalities ）**
   ポップアップ、音声アラート、モバイルデバイスのジェスチャーなど。

出典：第２回 WG　資料１「実効性のある通知・同意取得方法の在り方に関する実証事業の報告」（2021 年４月６日　（株）野村総合研究所）

また、GDPR はプロファイリング[78]及び自動化された個人に関する意思決定[79]が個人の権利に正当化されない影響を与える形で使用されないことを確保する規定[80]を導入している（透明性と公平性、アカウンタビ

[78] プロファイリングは、①自然人についての個人的側面を評価(evaluate)するためのもの、②個人データについて実施されるもの、③自動的な処理によるものという３つの要素があると定義されている。(GDPR 第４条（４))

[79] 部分的にプロファイリングと重なっているかプロファイリングによって生じているかもしれないとされる。自動化された意思決定には、①関係する個人により直接提供されたデータ、②個人について観察されたデータ（アプリケーションを通じて集めた一データなど)、③既に作成されている個人のプロファイルのような派生データ又は推定データなどが用いられるとされている。

[80] プロファイリングの利用には、潜在的に、①一般的なプロファイリング、②プロファイリグに基づく意思決定、③データ主体に対して法的効果又は同様の大きな影響を与える、プロファイリングを含む、もっぱら自動化された意思決定の３つの方法があるとされている。

リティ、情報を持つ権利（第５条(1)（ａ）、第 12 条、第 13 条、第 14 条)、取扱いの根拠としての同意(第６条(1)(a))、アクセス権(第 15 条)、訂正の権利（第 16 条)、異議を述べる権利（第 21 条(1)、(2))、適切な保護措置（第 22 条、全文第 71 項)、データ保護影響評価（DPIA)、データ保護オフィサー（DPO）等)。

② e プライバシー指令／e プライバシー規則案

2002 年の e プライバシー指令に基づき Cookie 設定について情報提供、拒否権の提供が義務づけられ、2009 年同指令改正により Cookie 設定について同意取得を義務付けた。2018 年 GDPR により同意の要件が厳格となった[81]。

EU 閣僚理事会で e プライバシー規則案について合意され、2021 年２月に公表された。EU 閣僚理事会及び欧州議会による正式な立法手続が開始されている。

e プライバシー規則案は、GDPR の特別法であり、電子通信サービス（ECS)及び利用者の端末装置の情報の取扱いを規制している。域外適用の明文化（第３条)、規制対象となる電子通信サービスの範囲拡大・適用対象の明確化と電子通信データ処理を規制（第５条～第７条)、端末装置のデータ処理・蓄積機能の利用、端末装置からの情報取得を規制（第８条「いわゆるクッキー等規制」）を規定[82]している。クッキー等に係る同意取得方法（第三者による代行やブラウザ設定による同意も可能)、同意を取得せずクッキー等を設定できる場合の明確化、同意証明方法、同意撤回権の通知等を明確化している。同意がなくとも「正当な利益」で広く許容されるという考え方は採用されなかった。

欧州司法裁判所の考え方が取り込まれており、最初からチェックされたチェックボックスを示し利用者が同意を拒否するためチェックを外さなければならない状況では有効な同意は取得しえないとされている。また、広告最適化のために Third Party Cookie を設置するウェブサイト管理者は、当該 Cookie の設定元の第三者であるネット広告エージェンシー、ソーシャルメディアなどとともに、GDPR 上の共同管理者の立場に立ち、個人データの利用目的について利用者に情報提供し、利用者から同意を取得する義務を負うこととされている。

---

[81] 曖昧でない明確で肯定的な意思表示が求められることとなり、オプトアウト、暗黙の同意、みなし同意が不可となった。

[82] 端末装置が有する処理機能の利用というのが新たに規則範囲に加えられた。スマートフォンなどの端末の処理機能が高度化したことに対応したものと思われる。グーグル社の Privacy Sandbox のように端末装置で AI 処理を利用したターゲティング広告や IoT 機器やコネクテッドカー等についても対象となる可能性が出てきた。

③　DSA/DMA（規則案）

【DSA】

2020 年 12 月に公表された Digital Services Act (DSA)（規則案）において、オンライン・プラットフォーム及び超大規模オンライン・プラットフォームに対しては、事業者の規模に応じた利用者保護のための義務が規定されている。オンライン広告の透明性確保に関するオンライン・プラットフォームに対する規律（広告であること、広告主及び広告表示決定に用いられた主なパラメータ等を表示する義務）、超大規模オンライン・プラットフォームに対する規律（広告表示から１年後まで広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂･API を介して一般に利用可能とする義務、レコメンダー・システムを利用する場合は利用規約においてパラメータ等を明確かつアクセスしやすく理解しやすい方法で明示する義務等）が提案されており、多くのセンシティブデータ処理について透明性が求められていく方向である。オンライン広告の透明性をさらに向上させるため、行動規範の策定を奨励・促進している。

欧州委員会は、超大規模オンライン・プラットフォームが DSA の規則を実施し遵守しているかどうかをモニタリングし、不遵守の場合などには罰金・違約金などを課すこともできることとしている。

【DMA】

2020 年 12 月に公表された Digital Market Act (DMA)（規則案）において、ゲートキーパーの義務として複数サービス間の個人データの組み合わせやサインイン強制の抑制（第５条 a)、エンドユーザーの活動を通じて生成されたデータの効果的なポータビリティの提供（第６条 h)、コア・プラットフォームサービス等に適用する消費者のプロファイリングの技術について独立した監査を受けた説明の欧州委員会への提出（第 13 条）等の規定が定められている。

（３）　ISO/IEC

ISO (the International Organization for Standardization)は、各国の標準化団体の世界的な連合。2020 年６月に出版された ISO/IEC29184[83]

[83] 2014 年 10 月に経済産業省が公表した「消費者向けオンラインサービスにおける通知と同意・選択に関するガイドライン」をベースとした日本提案の規格案。通知内容として、目的の記

（消費者向けオンラインサービスにおける通知と同意・選択）において、レイヤードアプローチを推奨。通知は処理の根拠に関わらず常に必要でありその内容は第三者にも示されるべきであると考えられる。同意は適切な状況において、PII[84]主体に十分な情報が与えられた上で自由にされる必要があり、意図的な行動により同意を得るとともに、同意の修正や撤回が簡単にできることが望ましい。

付属書において、PC やスマートフォンで同意を得る場合のユーザインタフェースの例や、同意領収書（Consent Receipt）又は同意記録（Consent Record）の例が示されている。

述、PII 管理者、PII の収集、収集方法、PII 収集のタイミングと場所、使用方法、保管 PII の位置情報及び法的管轄権、第三者への移転、保管期間、PII 主体による関与、同意のために行った選択へのアクセスに関する情報、処理の根拠、リスク等の 16 項目について規定されている。

[84] 個人識別可能情報（PII：Personal Identifiable Information）、

第２章　プラットフォーム事業者等による利用者情報の取扱いのモニタリング結果

１　モニタリングの概要

主要な電気通信事業者及びプラットフォーム事業者における利用者情報の取扱いについて、利用者情報の取扱いの状況、利用規約・プライバシーポリシー、アプリやサイトを経由した情報収集の状況、他社へのデータ提供、他社との連携の状況、サードパーティーによる情報取得への対応方針、アプリ提供マーケット、PIA ・アウトカムについての考え方についてヒアリングシートへの記入及びモニタリングを行った。

利用者情報の取扱いに関する主なモニタリング項目

項目１　利用者情報の取扱いの状況について
項目２　利用規約･プライバシーポリシーについて
　（1）プライバシーポリシーの内容
　（2）透明性確保のための工夫
　（3）オプトアウトやダッシュボードの導入状況
　（4）データポータビリティ―等への取組状況
項目３　他アプリやサイトを経由した情報収集の状況
項目４　他社へのデータ提供、他社との連携の状況
項目５　サードパーティーによる情報取得への対応方針について
項目６　アプリ提供マーケットについて（※アプリ提供マーケットを運営している場合）
項目７　PIA ・アウトカムについての考え方

モニタリングにおける主な論点は下記のとおり。

プラットフォーム事業者による利用者情報の取扱いの状況はどのようになっているか。【項目１】

利用規約やプライバシーポリシーの内容はどのようになっているか。特に、各事業者において様々な形で利用者へ分かりやすく伝えるための工夫、透明性確保のための工夫はどのようになっているか。（階層的アプローチ、ダッシュボード、ジャストインタイム、アイコン、モバイル及びスマートデバイスの特徴の利用等プライバシーポリシーにおける工夫はどのようになっているか。）【項目２(1)、(2)】

ユーザーテストの実施や有識者の意見を聴くなどしながら対応が行われているか。利用者にとってそれぞれ異なる各取組を見つけにくい点やより分かりやすくするための課題があるか。　【項目２(2)】

利用者が利用者情報の提供や利用を希望しない場合のオプトアウト等、利用者による事後的なコントロールの提供状況はどうなっているか。データポータビリティについてどのような取組を行っているか。（オプトアウトやデータポータビリティがある場合、利用のしやすさに課題はないか）【項目２(3)、(4)】

位置情報などプライバシー性の高い情報についてスマートフォンやウェブから取得する際に、どのような形で利用者の同意を得た上で、どのような配慮を行っているか。

他アプリやサイトを経由してどのように情報収集を行っているか。【項目３】

他社へのデータ提供、他社との連携の状況はどのようになっているか。【項目４】

サードパーティーによる情報取得に関してどのような対応方針であるか。【項目５】

アプリ提供マーケットにおいて、アプリ提供者にどのような働きかけをしているか。【項目６】

PIA についてどのように実施されているか、利用者へ与えうる影響（アウトカム）についてどのように考えてサービス設計をしており、利用者への説明が行われているか。プロファイリングがどのように行われており、どう使われているか。【項目７】

プラットフォームサービス事業者等における利用者情報の取扱いヒアリング　質問項目

1．利用者情報の取扱いの状況について
① 取得される利用者情報と取得場面
② 取得した情報の加工・分析・利用
③ 利用者情報の第三者提供
④ 広告ビジネスモデルへの利用者情報の活用
⑤ 利用者情報に基づくプロファイリング・セグメント化

2．利用規約・プライバシーポリシーについて
（1）プライバシーポリシー等
① 利用者情報の取扱いに係るプライバシーポリシー
② サービス開始前の通知公表・同意取得（導線・掲載場所）
③ プライバシーポリシーの変更に係る通知・同意取得
④ 利用開始後にも定期的に通知を行うなどの工夫

（2） 透明性確保のための工夫
① 透明性確保のための工夫や対処（ユーザーテスト実施他）
② 同意取得や通知に当たっての具体的な工夫（階層的アプローチ、ダッシュボード、ジャストインタイム、アイコン等）

（3）オプトアウト
① オプトアウトを設けているか（方法・対象範囲等）
② オプトアウトをしてもサービス利用継続が可能か
③ ダッシュボード等を設けているか（方法・対象範囲等）

（4）データポータビリティ
① データポータビリティの取組み（方法・対象範囲等）
② 対象情報、方法、提供フォーマット、提供先、相互運用性等
③ 電磁的開示請求への対応、開示方法、提供フォーマット等

3．他アプリやサイトを経由した情報収集の状況
① 他アプリやサイトを経由した情報収集の状況
② 他アプリ提供者やサイト運営者に対する情報提供
③ JavaScriptに係る情報提供
④ 複数の他アプリやサイトから収集した情報の管理

4．他社へのデータ提供、他社との連携の状況
① 他社に対するデータ提供の状況
② 他社との連携、留意点（利用者説明、安全管理等）

5.サードパーティーによる情報取得への対応（※PF事業者）
① サードパーティーによる情報取得に関する方針
② クッキーの代替手段の情報取得の動きへの考え方
③ Privacy Sandboxの導入目的、設計、説明（※Google）

6．アプリ提供マーケットについて（※Google, Apple）
① アプリ提供マーケットにけるSPIに関する取組
② アプリ提供者に対する働きかけ

7．PIA・アウトカムについての考え方
① PIAの導入状況
② 利用者情報の取扱いに関するアウトカムに係る検討
③ 利用者にPIAの結果やアウトカムを説明しているか

※１．で電気通信事業者には、取得される位置情報、アプリやサイト経由の取得の状況、端末からの取得情報、位置情報と加入者情報を組み合わせた分析、参考にしているＧＬも聞いた。

本年については、このヒアリングシートに基づき、本 WG において下記のとおりヒアリングを行うことにより、モニタリングを行った。詳細のヒアリングシートの内容については、参考９－１及び９－２のとおりである。

2021 年 ３月 18 日第１回 WG　NTT ドコモ、KDDI、ソフトバンク、楽天モバイル
４月 ６日第２回 WG　Apple、Yahoo！
４月 22 日第３回 WG　Facebook、Google、Agoop
５月 18 日第４回 WG　LINE

２　モニタリングの結果

項目	
1. 利用者情報の取扱いの状況	・提供するサービスや事業モデルやデータ取扱いに当たっての考え方等に応じて、個別の電気通信事業者やプラットフォーム事業者の取得している情報がそれぞれ異なっている。 ・全ての事業者が、**利用者情報を広告表示に活用**する場合がある。**広告及び測定の目的で、利用者のブラウザやデバイスから情報を直接第三者に取得**させ、広告の効果や測定結果などを提供する事業者もある。
2. 利用規約・プライバシーポリシー （1）プライバシーポリシーの内容 （2）透明性確保のための工夫 （3）オプトアウトやダッシュボード （4）データポータビリティ等	・プライバシーポリシーについて、どの事業者もＨＰに掲載があり、アプリ内などから呼出せる場合が多い。
	・各事業者において、プライバシーポリシーだけではなく、プライバシーポリシーの内容を分かりやすく簡潔に説明したプライバシーセンターを設けたり、プライバシーのガイダンスやヘルプセンターを設けるなど説明を工夫している。 ・アカウント管理画面（ダッシュボード等）から、利用者が利用者情報の取得や第三者提供や連携を含む取扱いについて事後的に把握・管理できるようにしている事業者もある。
	・オプトアウトの提供の有無については、全ての事業者が回答。オプトアウトの仕組みはダッシュボードやアカウント設定などを通じて大半の事業者において提供されている。
	・データポータビリティの提供の有無については、全ての事業者が回答。海外プラットフォーム事業者は全てデータポータビリティに対応済との回答であり、利用者のコンピューターへのダウンロードや一部の第三者への転送等が可能とされる。
3. 他アプリやサイトを経由した情報収集の状況	・**情報収集モジュール（イメージタグ、JavaScriptのタグ、SDK等）が設置**されている場合等に、**当該アプリやサイトを訪問する利用者に関する利用者情報（端末情報、訪問サイト、購入履歴、閲覧した広告、他サービス利用状況等）が送付**される場合がある。 ・広告商品利用時に、広告主や他アプリやサイトの提供者等との利用規約において、利用者情報を提供する前に、利用者から必要な同意等を取得していることを要求する事業者がある。
4. 他社へのデータ提供、他社との連携の状況	・自社の利用者情報の取扱いはプライバシーポリシーに記載があるとしている。他社へのデータ提供は、利用者から同意を取得した場合に行われている。
5. サードパーティによる情報収集への対応	・広告サービスを利用するサイト運営者や広告主等が、自らを経由し提供される個人情報等について、利用者に対してどのような説明や同意取得等をするべきかを必ずしも明確に把握・理解していない場合もあると考えられる。
6. アプリ提供マーケットについて	・アプリ提供者（デベロッパー）に義務付けを行ったり、情報提供を行なうなどの支援を行なっている。
7. PIA・アウトカムについての考え方	・PIAの実施状況については、全ての事業者が何らかの形で回答。一方、独自のPIAを行なっているとしているが、その基準が明確ではない場合がある。また、PIAの結果も公表されていない場合が多い。

（１）　利用者情報の取扱いの状況について

・ 提供するサービスや事業モデルやデータ取扱いに当たっての考え方等に応じて、個別の電気通信事業者やプラットフォーム事業者の取得している情報がそれぞれ異なっている。広範な取扱いの全体像を一般の利用者に説明・理解させることは容易ではない場合も多い。

【利用者情報の第三者提供の状況】

・ 個人を特定する情報については、他社と共有しないとする事業者や、ユーザー本人の同意がない限り共有しないとする事業者がいる。
・ 広告及び測定の目的で、利用者のブラウザやデバイスから情報を直接第三者に取得させたり、広告の効果や測定結果などを提供する事業者もある。
・ グループ内における共有を行う事業者もある。

【広告ビジネスモデルへの活用状況】

・ 全ての事業者が、利用者から取得した利用者情報を広告表示に活用する場合があるとしている。
・ 広告設定について、利用者自身が一定の管理をできる事業者もある。
・ パーソナライズされた広告をオプトアウトする機能を提供する事業者もある。

【プロファイリング・セグメント化情報】

・ プロファイリングやセグメント化を行うために、ユーザー登録情報、サービスの利用状況や閲覧情報などが用いられている場合が多い。
・ プロファイリングやセグメント化した結果については、ターゲティング(パーソナライズ)広告の表示のみに用いている場合もあれば、機能やコンテンツのパーソナライズ、おすすめの表示、マーケティングなどに用いられる場合がある。
・ 人種、宗教、健康などのセンシティブ情報について、保有しないとする事業者や用いないとする事業者がいる。

【位置情報等】

・ 位置情報はプライバシー性の高い情報として、厳密な管理を行っている。位置情報の種類に応じて、取得する際に同意を取得するかオプトアウトを提供等をしている。住所等を推定されないように、位置情報の加工や取扱いにおいても注意が払われている。端末から GPS 等の位置情報を取得する場合、OS の機能により同意取得が行われる。
・ 一方、ビーコンや店舗における電子マネー決済など端末情報と別の情報を組み合わせ位置情報が取得できる手段が増えてきている。これらの位置情報についての通知・公表や利用者の同意の在り方などについて新たな課題がある。

（２） 利用規約・プライバシーポリシーについて

① プライバシーポリシー

・ プライバシーポリシーについて、どの事業者もＨＰに掲載があり、アプリ内などからも呼び出せるようになっている場合が多い。分かりやすく伝えられるように、具体例などを示している事業者も

ある。

- プライバシーポリシーに重要な変更を行う場合には、通知を公開したり、告知している事業者もあり、同意を取得している事業者もある。
- 利用開始後、定期的な通知は一般に行われていないが、新規加入時等や重要な変更時にデータ設定に関する設定について確認する機会を設けたり、アカウント管理画面（ダッシュボード等）で確認が可能となっている事業者もある。

② 透明性確保のための工夫

【各事業者による工夫】

- 各事業者において、プライバシーポリシーだけではなく、利用者に伝えるための工夫としてプライバシーポリシーの内容を分かりやすく簡潔に説明したプライバシーセンターを設けたり、プライバシーのガイダンスやヘルプセンターを設けるなど説明を工夫している。
- アカウント管理画面（ダッシュボード等）から、利用者が利用者情報の取得や第三者提供や連携を含む取扱いについて事後的に把握・管理できるようにしている事業者もある。
- 利用者がプラットフォーム事業者による情報取得や取扱い、第三者提供や連携の影響（集められる情報、利用目的、利用されるリスク等）を簡単に把握し、どのプラットフォームを使っても不利益を被らないことが重要と指摘される。

【利用者や外部からの意見、ユーザーテスト】

- 利用者は多様であり、背景、知識、経験などが異なるため、それを踏まえて利用者が理解できるように、多様な方法を用意する必要があると指摘される（例えば、金融商品は法律の中で消費者の多様性を考慮した規制がある）。
- 消費者が想定しづらいものやプライバシー性が高い情報の取得等について、注意喚起をする仕組みが必要であると指摘される。
- 情報開示が進展する中で、情報開示の視点で外部レビューやモニタリングを行っていくことが重要であると指摘される。

③ オプトアウトやダッシュボードの導入状況

- オプトアウトの提供の有無については、全ての事業者が回答。オ

プトアウトの仕組みはダッシュボードやアカウント設定などを通じて大半の事業者において提供されている。また、この他、データの保存や保存期間、広告への利用の設定などを通じ、データの取扱いを一定程度コントロールする仕組み等を提供している場合がある。

・ オプトアウトを行うと、オプトアウトした情報の取得が停止されるとともに、オプトアウト前に取得されたデータは利用されなくなるとしている。一方、当該データが消去されるのかどうかははっきりしない場合もある。

④ データポータビリティー等への取組状況

・ データポータビリティの提供の有無については、全ての事業者が回答。海外事業者は全てデータポータビリティに対応済との回答であり、利用者のコンピューターへのダウンロードや一部の第三者への転送等が可能とされている。電気通信事業者及び国内プラットフォーム事業者はデータポータビリティに対応していない、又は一部のデータのみダウンロード可能との回答であった。

・ 改正個人情報保護法の施行に向け、電子的手法による開示請求対応の準備を進めるとの回答が複数みられた。

（３） 他アプリやサイトを経由した情報収集

情報収集モジュール（イメージタグ、JavaScript のタグ、SDK 等）が設置されている場合等に、当該アプリやサイトを訪問する利用者に関する利用者情報（端末情報、訪問サイト、購入履歴、閲覧した広告、他サービス利用状況等）が送付される場合がある。

広告商品利用時に、広告主や他アプリやサイトの提供者等との利用規約において、利用者情報を提供する前に、利用者から必要な同意等を取得していることを要求する事業者がある。

広告商品利用時に、広告主や他アプリやサイトの提供者に、プライバシーポリシー等における記載事項、オプトアウトの提供、掲載場所等の詳細を示して対応を要求する事業者もある。

（４） 他社へのデータ提供他社との連携の状況

自社の利用者情報の取扱いはプライバシーポリシーに記載があるとしている。他社へのデータ提供は、利用者から同意を取得した場合に行われ

ている。

（５）　サードパーティーによる情報取得への対応（デジタル広告）

広告主がメールアドレスや電話番号をアップロードし、ハッシュ化した上で当該事業者が保有するメールアドレスや電話番号と突き合わせするタイプの広告サービスを提供する事業者がある。当該事業者はハッシュ化した形で受領するものであり、広告主側に提供する情報に関して適切な対応を行った上で提供するよう促していると説明[85]があった。

様々な形でクロスデバイスの情報が取得されており、一般利用者にとって全体像を理解することが容易ではない状況。また、広告サービスを利用するサイト運営者や広告主等が、自らを経由し提供される個人情報等について、利用者に対してどのような説明や同意取得等をするべきかを必ずしも明確に把握・理解していない場合もある[86]と考えられる。

（６）　アプリ提供マーケットについて

Apple 及び Google のアプリ提供マーケットともに、アプリがアクセスしようとしている利用者情報について、利用者が十分な情報を得た上で判断できるように、アプリ提供者（デベロッパー）に義務付けを行ったり、情報提供を行うなどの支援を行っている。SPI を参照すべき政府のガイドラインの一つとして提示しているアプリ提供マーケットもあった。

App Store Review ガイドラインにおいて、アプリのプライバシーポリシーおいて利用者情報の取扱いについて詳細に規定すること、データ収集についての同意取得や同意の撤回の提供、目的でデータの用途を十分説明すること、ユーザーのアクセス許可設定を尊重すること、不要なデータアクセスに同意するよう誘導や強制しないこと等を示している。

Google API 利用規約は、アプリ提供者が収集、使用、他社と共有する利用者情報について明確かつ正確に定めたプライバシーポリシーを提供し遵守することを義務づけている。また、明示的な同意なく、利用者の非公開データを第三者に開示すること、スクレイピング、データベース構築その他利用者情報の恒久的コピー作成等を禁止している。

---

[85] 例えば、Facebook の場合、「パートナーが当社にデータを提供する前に、パートナーが利用者のデータを取得、利用、共有する正当な権利を有していることを当社は当該パートナーに要求する」としている。

[86] 実際にどのような対応が行われているかプラットフォーム事業者において確認していないことが問題ではないかとの指摘があった。

（７）　PIA[87]・アウトカムについて

PIA の実施状況については、全ての事業者が何らかの形で回答。一方、独自の PIA を行っているとしているが、その基準が明確ではない場合がある。また、PIA の結果も公表されていない場合が多い。

今回モニタリングの対象とした各事業者において、プライバシーポリシーの内容を分かりやすく説明するための工夫を行っている。アカウント管理画面やダッシュボード等から、利用者が情報取得や第三者提供等を事後的に把握・管理できるようにしている事業者もある。

一方で、広範な利用者情報の取扱いの全体像を一般の利用者に説明・理解させることは容易ではない。全ての事業者が、利用者から取得した利用者情報を広告表示に活用する場合があるとしており、情報収集モジュール等により、クロスサイトトラッキング等が幅広く行われている。

利用者情報を取得・集約・分析することにより、当該利用者の詳細なプロファイリングを行いうる状況であることを鑑みると、利用者情報の取扱いについて一定のルール整備を検討していくことが必要であると考えられる。また、各事業者において、今後更に利用者情報の取扱いについて分かりやすい通知・説明や同意取得を工夫していくことが求められるものであり、その状況について継続的にモニタリングを行っていくことが必要であると考えられる。

[87] PIA(Privacy Impact Assessment、個人情報保護評価)：個人情報保護委員会が令和 3 年 6 月 30 日に公表した「PIA の取組の促進について－PIA の意義と実施手順に沿った留意点―」によれば、「PIA は、個人情報等の収集を伴う事業の開始や変更の際に、個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法。」とされており、「個人情報のフローの整理」を行った上で、「事業者側のオペレーションなどに伴い想定されるリスク要因、消費者・利用者側の利用方法等に伴うリスク要因なども踏まえて、リスクを洗い出し、整理」し、「特定したリスクについて「影響度」及び「発生可能性」の観点で評価を実施」した上で、リスクへの対応方針・対応策を検討するとしている。また、「報告書のサマリーを作成」「公表することが有効」、事案に応じて「第三者機関のチェック」を得ることが有用と指摘されている。(https://www.ppc.go.jp/files/pdf/pia_overview.pdf)
(https://www.ppc.go.jp/files/pdf/pia_promotion.pdf)

第３章　今後の取組の方向性

１　利用者情報の適切な取扱いの確保に向けた論点

①　利用者情報を取巻くグローバルな情勢の変化

第２章のモニタリング結果からも見てきたように、電気通信事業者やプラットフォーム事業者は、個人情報保護法や電気通信事業 GL なども踏まえつつ、網羅的なプライバシーポリシーを作成するだけではなく、利用者情報の取扱いの説明について既に様々な工夫を行ってきている。しかしながら、一般利用者にとって、利用者情報の取扱いについて理解し把握することは困難である場合も多いとの指摘もある。

第１章で見てきたように、日々の生活の中においてスマートフォン等の利用が不可欠になる中で、スマートフォン等で取り扱われる利用者情報の質や量が拡大し、機微情報や機密情報も含まれる可能性もある。更に、スマートフォン等の利用者情報と、電子マネーを使った決済や購買履歴などの外部情報についても結びついた上で利活用される可能性がある。

これら利用者情報等がクロスデバイスで取得・集積・分析され、プロファイリングやターゲティングも高度化・精緻化している。適切に用いられれば利用者へのサービス提供やレコメンドの向上につながるなどイノベーションの促進に役立つという指摘もある。一方、商品広告の表示目的だけではなく、様々なマイクロターゲティング、プロファイリング結果を踏まえた採用や与信などの個人に影響を与えうる意思決定にも用いられるおそれもあり、利用者情報を提供した結果の本人に対する影響・アウトカムを予め説明することが困難となる場合もあることが指摘される。また、このような利用者情報の取扱いが社会へ様々な影響を与える可能性も指摘される[88]。

このような情勢等も踏まえ、各国はクロスデバイスの情報の取扱いに関して、特に本人へのサービス提供と直接関係がない本人が意図しない取扱いや本人の合理的な期待を超える取扱いを行おうとする際は本人にこれを知らせ、本人同意を求めること、事後的な検証可能性を高めるための透明性確保や報告・公表義務を課すこと等規制強化を進めているところであり、グローバル展開するプラットフォーム事業者もこれに対

[88] 利用者情報を活用したターゲティング技術の悪用による問題については、P64「⑤利用者情報を活用した情報配信への対応」を参照。

応しつつある。

我が国においても、利用者保護の観点から、このような業界の状況やグローバルな規制状況なども踏まえつつ、適切な対応を検討していくことが求められていると考えられる。

② 利用者情報の適切な取扱いの確保

スマートフォンやタブレットなどの通信端末の位置情報や、ウェブサイト上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末 ID やクッキーなどの端末を識別する情報等については、通信の秘密やプライバシー保護の関係で、その適切な取扱いの確保のための規律を検討していく必要がある。

特に第１章及び第２章でも見たように、異なるアプリやウェブサイトを通じた横断的なパーソナル・データの取得・収集・分析が進んでおり、利用者のサービス提供に直接結びつくものではないため利用者が指示したり意識したりしていないものが多くある。このような利用者が十分認識しない中でのパーソナルデータの取得・収集・利活用について、利用者情報の取扱いに係る通知・公表や同意取得の在り方について、検討を行い、指針やルールを明確化していく必要があると考えられる。また、様々な機会を通じて取得したパーソナルデータについて、何等かの ID などに基づき名寄せを行い、多角的にプロファイリングを行う場合は今後増えてくると考えられる。このプロファイリングの実施や特定の個人への適用、それによるサービスや判断についてどう考えるべきか検討が必要であると指摘される。

利用者に適切に通知・公表や同意取得を行っていく観点から、下記のような点が重要であると考えらえる。

第一に、利用者と直接の接点があるアプリ提供者やウェブサイト運営者等のサービス提供者が、第１章で指摘されたように当該アプリやウェブサイトにおいて、取得者が誰かも含めどのような情報取得や情報提供を行っているか把握していない場合があるという問題がある。まずは、当該アプリやウェブサイト等のサービスを提供する際において、誰がどのような情報取得を行うとともに、第三者にどのような情報提供を行う必要があるのかについて検討した上で、これを把握することが必要[89]である。

[89] 適切なデータやプライバシーのガバナンスを行う上でも、そもそも、自らがどのような情報取得を行い、第三者にどのような情報提供を行うのか把握することは、前提条件となると考えられる。

第二に、アプリ提供者やウェブサイト運営者等のサービス提供者が、上記のプロセスを経た上でこれを踏まえ、取得者や取得・提供する情報の種類や用途などに応じて、利用者が理解できるように通知・公表又は同意取得を行っていく必要がある。この際、内容に応じて、通知・公表や同意の取得等について検討を行う必要があると考えられる。

更に、第１章でも指摘されたようにプロファイリング[90]の有無や情報利用による利用者へ与えうる影響（アウトカム）が重要であり、これを利用者に伝えていく必要があると考えられる。特に利用者が受けうる不利益についての情報については重要であると考えられる。このような影響について利用者に分かりやすく伝えていくよう促していく必要があると考えられる。

③　分かりやすい通知や同意取得のあり方

第２章で見たように、プライバシー・ポリシー等について、分かりやすく見せるための仕組みや工夫については、大手のプラットフォーム事業者や電気通信事業者においては一定の検討が行われている。利用者の意見や外部レビューなども踏まえながら継続的にこのような工夫を行い、利用者に分かりやすく通知・公表や同意取得を行うとともに、利用者が理解した上で有効な選択を行える環境を整えていく必要があると考えられる。

第２章でも見たように、例えば、階層的な通知、個別同意、プライバシー設定の工夫などについては、EU の GDPR に基づく同意取得や透明化のガイドラインや米国の NIST Privacy Framework において推奨されるとともに、カリフォルニア州 CCPA においても規定された重要な事項[91]を示す階層的通知が求められるなど、欧米において共通的な認識が形成されていると考えられる。

このような階層的な通知、個別同意、プライバシー設定の工夫については、我が国における当該サービスの利用者に合わせた形で、必要に応じてユーザー調査なども実施した上で、導入されることが望ましい。

一例として、(株) 野村総合研究所により、我が国のインターネットの利用者について、通知・同意取得における利用者の考え方について、因

[90] 断片的な情報等により、誤ったプロファイリングが行われそれが適用されることによる問題が発生する可能性も指摘される。
[91] 個人情報の種類一覧や個人情報の種類ごとの利用目的、オプトアウトページ及びプライバシーポリシーのリンク等

子１：企業の情報利用に対する抵抗感、因子２：ネットサービスの利用における自己効力感により４種類のパーソナリティに分類し、そのパーソナリティに応じた工夫の効果に係る調査結果[92]がある。

【参考：（株）野村総合研究所による分析】

自己効力感が高く、抵抗感が強い利用者（Seg.　１）は、先進的なネットサービスの利用に意欲的であるものの、抵抗感が強い利用者（Seg.　１及び Seg.　３）は自身の情報の取扱いに敏感[93]でありその内容によりサービスそのものの利用を忌避する傾向がある。

通知・同意取得における利用者の考え方の違い

		企業の情報利用に対する抵抗感（因子１）	
		抵抗感が弱い	抵抗感が強い
ネットサービスの利用における自己効力感（因子２）	自己効力感が高い	Seg.2	Seg.1
	自己効力感が低い	Seg.4	Seg.3

出典：利用者情報ＷＧ（第２回）資料１「実効性のある通知・同意取得方法の在り方に関する実証事業の報告」（野村総合研究所）

[92] この他、因子３：面倒と感じる気質（先延ばし・怠慢・依存）が指摘されている。
[93] 抵抗感が強い利用者は情報の利用停止意向も強く、不要な情報提供に対して否定的であることが指摘される。

通知・同意取得にあたり利用者の理解や安心に資すると思われる工夫

#	工夫	工夫の概要
1	階層的な通知	• プライバシーポリシー等の全文をもって通知を行うのではなく、利用者の関心の範囲や粒度に合わせて通知内容を階層化する。 • 階層の考え方や実装方法には、大きく以下の３つが考えられる。 1-1 目次（見出し）と詳細： 第１階層にプライバシーポリシー等の目次や見出しを示し、利用者が関心に基づきクリック・画面タップ等を行うことで、該当項目の詳細内容（第２階層）を通知する。 1-2 重要事項と全文： 利用者の関心が特に高いと思われる項目（取り扱う情報の種類、利用目的等）について第１階層において通知する。また、利用者が第１階層で示される項目以外に関心を持った場合、容易に確認できるように、プライバシーポリシー等の全文（第２階層）へのリンクを第１階層に用意する。 1-3 サービス・アプリ単体としての通知と企業全体としての通知： サービスやアプリ固有のプライバシーポリシー等を企業としての通知とは別に整備する。 • 階層的な通知を行う際に、モバイル端末の画面上の制約等から、アイコンを用いて利用者の注意をひく方法も考えられる。
2	サービスの利用タイミングに合わせたタイムリーな通知	• 一定期間サービスの利用がない場合や位置情報・閲覧履歴等の利用者自身が提供していることを認識しづらい情報を取得する場合は、サービスの利用開始時・アカウント作成時における通知とは別に、適宜利用者の認識がしやすいタイミングで通知を行う。 • 通知の方法として、サービス利用画面におけるポップアップの表示やプッシュ通知等が挙げられる。 • 工夫＃４の「プライバシー設定」を併せることで、利用者自身が通知の有無や頻度を変更できるようにすることも有効と考えられる。
3	個別同意 （情報種別・利用目的・第三者提供先別等）	• 取り扱う情報の種類や利用目的、第三者提供先等に応じて、個別に利用者が同意できるフォーマットを提供する。 • ただし、利用目的や第三者提供先等について詳細・具体的に同意を求めることが、かえって利用者の煩わしさにつながる可能性があるため、同意を求める際の粒度について、検討が必要となる。
4	プライバシー設定 （同意状況の確認・撤回、履歴の消去、情報の更新等）	• 利用者がサービス利用にあたり、同意した内容を確認することや同意を撤回（オプトアウト）することを容易にさせるための設定を提供する。 • 利用履歴の消去や企業からの通知頻度の変更等の機能についても、一体的に設定・管理することを可能とする画面（ダッシュボード）を提供することも想定される。
5	同意の証跡 （コンセントレシート）	• 利用者が同意内容について、後から振り返ることができるように、同意項目や同意取得する際の通知内容をメール等で利用者に還元する。

上記にある挙げられる通知・同意取得にあたり利用者の理解や安心に資すると思われる工夫のうち、「１階層的な通知」、「３個別同意」、「４プライバシー設定」について、実際に利用者インタビューを行った上で、利用者の考え方の違いを踏まえてその有効性についての分析を行った。

その結果、プライバシーポリシーの内容を何ら変更せず、表示方式の工夫だけを行った場合であっても、階層的な通知のうち、「1-1 目次（見出し）と詳細」の工夫を講じた場合には、利用者全体の 25%が「現状よりしっかり読む」と回答し、特に抵抗感が強い利用者（Seg. １及び Seg. ３）30%以上が「現状よりしっかり読む」と回答している。「1-2 重要事項と全文」の工夫を講じた場合には、利用者全体の 22%が「現状よりしっかり読む」と回答し、特に抵抗感が強い利用者（Seg. １及び Seg. ３）は 26%が「現状よりしっかり読む」と回答している。

また、取り扱う情報の種類や利用目的、第三者提供先等について、個別に利用者が同意できるフォーマットを提供する「3 個別同意」は、利用者全体の 64%が「利用したい」と回答しており、実装に対してニーズの高い工夫である。

更に、利用者がサービス利用にあたり、同意した内容を確認することや同意を撤回（オプトアウト）することを容易にさせるための設定を一覧的に設定・管理することを可能とする画面（ダッシュボード）等を提供する「4 プライバシー設定」は、利用者全体の 67%が「利用したい」と回答しており、また、抵抗感の強弱や自己効力感の高低にかかわらず全てのセグメントの利用者（Seg. １～Seg. ４）において５割以上の利用者が利用意向を示している。

このような利用者調査等の結果も参考にしながら、プライバシーポリシーに階層別の表示や簡略版の作成などの工夫を行い読みやすさを高めることが期待される。

また、取得される情報の種類や利用目的、第三者提供先などに関する個別同意や同意した内容の確認を可能とする Consent Receipt[94]のような仕組みや、サービス開始後の随時に可能なオプトアウトなどのプライバシー設定を可能とするダッシュボード等の提供等により、個人による理解やコントロールを高めることが期待される。

特に、この設計を行う際に、第三者提供、機微情報の取得・利用、通常は想定されない利用等は特に注意喚起をする仕組みが求められると考えられる。

これらを通じて、各サービスの利用者の知識や性格などの考慮しながら、様々な性格の利用者の理解や安心に資する方法を工夫し導入していくことが求められるものと考えられる。

２　今後の対応の方向性

（１）　電気通信事業法・個人情報保護法等を踏まえた対応

プラットフォームサービスに関する研究会において、電気通信サービス・機能の連携・融合などの進展に対応するための規律の在り方として、政策対応上の基本的方向性として「利用者の端末情報の適切な取扱いを確保することにより、利用者が自らの端末を用いて安心して通信サービスを利用することができるようにすることは重要。」とされており、「利用者の端末情報が OS 事業者、通信事業者、プラットフォーム事業者、アプリ事業者等によって、利用者の意思に反して取得・活用されていたとすると、通信の秘密の対象であるか否かに係わらず、プライバシー上の適切な保護を検討する余地が生じうるところ、端末情報の適切な取扱いの確保のための具体的な規律の在り方については、e プライバシー規則（案）の議論も参考にしつつ、今後検討が必要」と考えられる[95]。

このような通信サービスの利用に関わる利用者端末情報[96]とそれに紐

---

[94] ISO/IEC29184　付属書（第１章参照）
[95] 本研究会中間報告書（2019 年 4 月）P27
[96] 端末に保存された利用者情報（脚注１参照）であって、通信サービスの利用に関わるもの。cookie 等を含む利用者の識別に係る情報や通信サービス上の行動履歴や利用者の状態に関する情報を含む概念。なお、これらは個人関連情報に該当し得るが、提供先が個人関連情報を個人

付く情報の保護については、「通信関連プライバシー」として保護されるべき利用者の権利として、把握されるべきであると考えられる。即ち、情報通信が我が国の経済・社会活動、国民生活の基盤として重要な役割を果たすようになりつつあることを踏まえ、電気通信事業者や電気通信事業者の設備のみに着目するのではなく、電気通信サービスの利用者の権利に着目し、通信の秘密に加えて電気通信サービスの利用者のプライバシー保護を電気通信事業法の目的として考えていく必要があると考えられる。また、このような利用者端末情報等を取り扱う者の全てが、保護すべき義務を負うこととすることが考えられる。

また、ターゲティング広告やプロファイリングを使った利用者への影響について後から検証できる環境を整え、透明性を確保していく観点から、利用者情報の利用の状況についての公表や保存についての仕組みについて考えていく必要があると考えられる。

このため、適切な利用者情報の取扱いを確保する観点から、電気通信事業 GL において必要とされる事項（例：表示や公表、望ましい取扱い等）を定めた上で、当該 GL の遵守状況や事業者の自主的な取組の状況について、定期的にモニタリングを行うべきであると考えられる。

また、変化の激しいデジタル広告などを含めた通信関連プライバシーの保護のためには共同規制が有用である[97]と考えられるがこの共同規制について外縁を明らかにして内外事業者に対する実効性を高めるため、事業者に法律上の義務を課すことが有用であるとの指摘[98]も踏まえ、電気通信事業法等における規律の内容・範囲等について、e プライバシー規則（案）の議論も参考にしつつ、cookie や位置情報等を含む利用者情報の取扱いについて具体的な制度化に向けた検討を進めることが適当である

データとして取得されることが想定されるときは、個人情報保護法による第三者提供規制がかかる。個人データとしての取得が想定される場面以外では同法の規制は適用されないため、そのような利用者端末情報の取得・提供等については、規制のない状態になっていると指摘される。

[97] デジタル広告については、共同規制や自主的取組が望ましいと考えられる。事業者単体ではなく、全体として継続比較できる方法が重要ではないか。(利用者情報WG (第 5 回) 寺田構成員)

[98] 共同規制だとしても法令として表示義務があった方が望ましい、利用者目線による法的義務を前提とした共同規制であるべきとの指摘があった。また、グローバルな状況を見ると、既に同意取得義務やオプトアウト義務がかけられており、モニタリングをしてその結果を踏まえて表示義務をかけるのでは遅いのではないかとの指摘があった。(利用者情報WG（第 5 回）森構成員、生貝構成員、太田構成員等)。

と考えられる[99][100]。

（２）　電気通信事業 GL・指針等における対応

令和４年(2022 年)４月の令和２年及び令和３年改正個人情報保護法の施行に向けて、電気通信事業 GL について全面的に見直す必要がある。電気通信事業 GL は電気通信事業を営む事業者が利用者情報に係る通信の秘密や個人情報・プライバシー上の適正な取扱いを行う観点から一元的に参照することができる文書としてとりまとめていくことが望ましい。

①　個人情報保護委員会ガイドラインの見直しに対応した改正の検討

令和３年（2021 年）５月に個人情報保護委員会から令和２年改正に対応するための個人情報の保護に関する法律についてのガイドライン（以下「個人情報保護委員会ガイドライン」という。）の改正案が示されている。これを踏まえ、電気通信事業 GL についても対応した改正を検討する。

まず、全体の構造としては、個人情報保護委員会ガイドラインにおいて、「3-2　不適正利用の禁止」、「3-5 個人データの漏えい等の報告等」、「3-7 個人関連情報の第三者提供の制限等」、「3-10 仮名加工情報取扱い事業者等の義務」の４つの項目が新たに設けられることに対応し、電気通信事業 GL においても、「3-2　不適正利用の禁止」、「3-5 個人データの漏えい等の報告等」、「3-8 個人関連情報の第三者提供の制限等」、「3-11 仮名加工情報取扱い事業者等の義務」を設けることとする。

また、新たに法律で規定された事項である不適正利用の禁止、漏えい

---

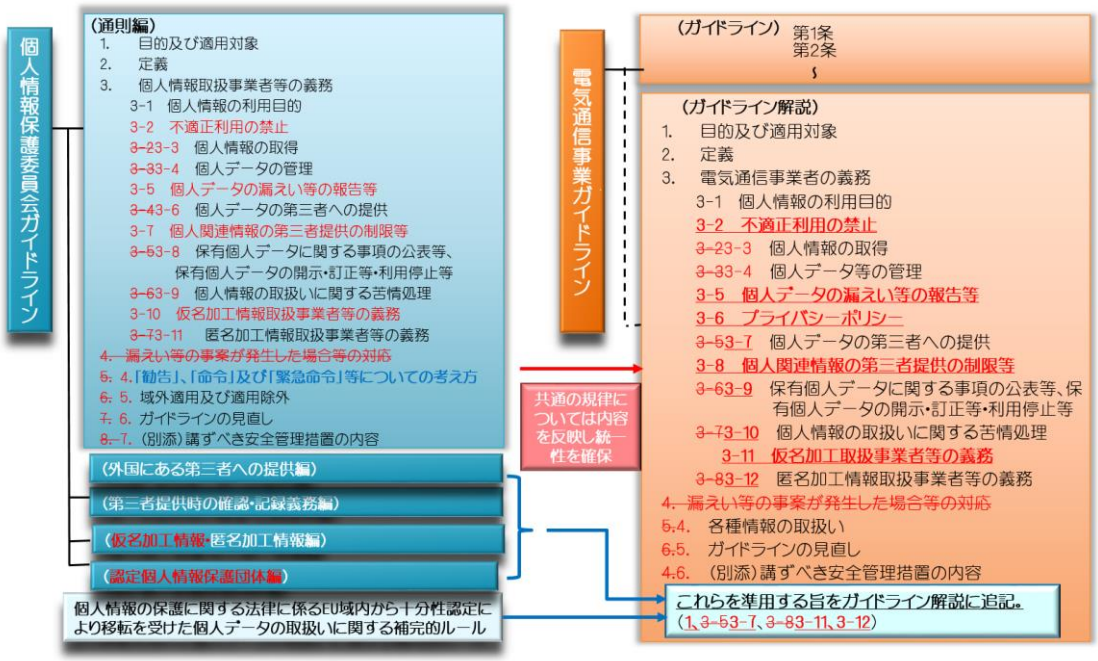
[99] 規模に応じたリスクも考慮に入れ、リスクベース、キャパシティベースでハードローもソフトローも検討していってはどうか、ベースを下げるというわけではなく、トップに対する規制を引き上げていく必要があるとの指摘があった（第５回 WG　生貝構成員）。利用者保護の OTT 規制については、公平性の観点からも大事であり、日本の制度が遅れると、利用者は日本の事業者より海外の事業者の方が信頼できるようになってしまい日本の事業者にとっても良くない、事業者と利用者の認識のズレを埋めていく必要があるとの指摘があった。また、オフラインであれば把握しやすいがオンラインにおいて通知等もされずに取得されていると利用者目線から懸念を持たれるとの指摘があった（第５回 WG　佐藤構成員、太田構成員等）。また、ゆるやかな法規制をかけ、実際にやることは共同規制で自主的取組を尊重されるべきではないかとの意見があった（第５回 WG　沢田構成員）。

[100] 「通信関連プライバシー」は、電気通信事業分野で特に求められるものであり、利用者が最もコントロールしにくい部分についてルール形成が必要である、利用者保護の観点から立法化について前向きに取り組むべきではないかとの指摘があった（第６回 WG　石井構成員）。　e プライバシー規則（案）を踏まえて制度化に関する検討を進めるべきではないか、モニタリングをしてから法改正を検討するのでは少し弱いのではないか等の指摘があった（第６回 WG　森構成員、太田構成員）。

等事案の報告、越境移転時の本人説明の充実、個人関連情報[101]の第三者提供の制限、保有個人データに関する公表事項・開示方法・第三者提供記録の開示請求・利用停止や消去の要件緩和、仮名加工情報の創設、域外適用対象拡大やガイドラインで規定された事項である利用目的の特定などについて、個人情報保護委員会ガイドラインにおいて事例などの記載があるが、電気通信事業の固有の事情などを踏まえ、より適切な事例などの記載について検討することが適当である。

例えば、保有個人データに関する公表事項として、個人情報保護委員会ガイドラインにおいて「プロファイリングを行っていること」を記載することとされているが、そのプロファイリングを行っていることに関連して記載する情報[102]についても具体例を検討していくことが考えられる。また保有個人データの開示における電磁的記録の提供についても、電気通信事業の性質を踏まえた対応の検討が考えられる。

個人情報保護委員会ガイドラインとの関係



---

101 提供先において個人データとして取得されることが想定される情報であり、例えば、Cookie 等の端末識別子を通じ収集されたある個人のウェブサイトの閲覧履歴、ある個人の商品購買履歴・サービス利用履歴、ある個人の位置情報などが考えられる。

102 要配慮個人情報（健康、政治的信条）などの機微情報や感情面に係るプロファイリングの有無や、プロファイリングを用いる対象（個人の意思決定に働きかけるか）などについて記載を検討してはどうかとの意見があった。（第５回 WG　山本構成員）

改正項目	電気通信事業 GL 改正の方向性（案）
短期保存データの保有個人データ化 （法 2 条第 7 項、通則編 2-7）	・「２定義」中の GL 第３条柱書の規定を維持。 ・解説（2-8 保有個人データ）における関連記載を削除。
不適正な方法による利用の禁止 （法 16 条の２、通則編 3-2）	・「3-2 適正利用の禁止」を新設※、同様に規定。※GL 第５条の次 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
漏えい等報告・本人通知の義務化 （法 22 条の２、通則編 3-5）	・「3-5 個人データの漏えい」を新設※、同様に規定。※GL 第 14 条の次 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
オプトアウトによる第三者提供対象 （法 23 条 2 項、通則編 3-6-2-1）	・GL 第 15 条第２項を改正。 ・解説に事例を含め説明記載。
越境移転時の本人説明の充実 （法 24 条 2 項・3 項、通則編 3-6-4、外国第三者提供編５・６　）	・GL 第 16 条を改正。 ・解説においてガイドライン（外国第三者提供編）を参照。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
個人関連情報の第三者提供の制限 （法 26 条の２、通則編 3-7、確認記録義務編５）	・「3-8 個人関連情報の第三者提供の制限等」を新設※、同様に規定。※GL 第 18 条の次 ・解説にてガイドライン(外国第三者提供、確認記録義務編)を参照(P)。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
保有個人データに関する公表事項等 （法 27 条 1 項、通則編 3-8-1）	・GL 第 19 条第１項第１号を改正、同条同項第３号の次に規定を追加。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
保有個人データの開示方法 （法 28 条 1 項・2 項、通則編 3-8-2）	・GL 第 20 条第１項・第２項を改正。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
第三者提供記録の開示請求 （法 28 条 5 項、通則編 3-8-3）	・GL 第 20 条第５項を新設。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
利用停止・消去等の要件緩和 （法 30 条 5 項・６項、通則編 3-8-5）	・GL 第 22 条第５項・第６項を新設。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
仮名加工情報の創設 （法 2 条 9 項・10 項(定義)、法 35 条の２、35 条の３(義務)、通則編 3-10、仮名加工情報・匿名加工情報編２）	・「3-11 仮名加工情報取扱事業者等の義務」を新設※、同様に規定。※GL 第 28 条の次 ・解説でガイドライン（仮名加工情報・匿名加工情報編）を参照。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
域外適用対象拡大 （法 75 条、通則編 5-1）	・電気通信事業法の域外適用との関係も整理の上で規定内容を検討。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
認定団体制度の充実 （法 47 条 2 項・4 項、通則編 1-1、認定個人情報保護団体編）	・解説（1-1 目的）における関連規定を修正。 ・解説でガイドライン（認定個人情報保護団体編）を参照。
利用目的の特定 （法 15 条 1 項、通則編 3-1-1）	・解説（3-1-1 利用目的の特定）における関連規定を修正。 ・解説に事例含め説明記載（必要に応じ電気通信事業特有事例含む）
法定刑等の引上げ（法 83 条、87 条）	―

※法は、個人情報保護法（令和２年改正施行後の条文）

②　利用者情報の適正な取扱いの確保に向けた改正の検討

【全般的な考え方】

電気通信事業 GL において、これまで総務省が作成してきたスマートフォン　プライバシー　イニシアティブや位置情報プライバシーレポート等の指針の内容も踏まえた規定が既に設けられている。これについても、今回記載の充実や見直しを行っていく必要があると考えられる。

特に、スマートフォン及びウェブにおいて、プラットフォーム事業者、アプリケーション提供事業者、ウェブサイト運営者、広告事業者等関係する主体がそれぞれ適切に対応ができるような環境整備について、スマートフォン　プライバシー　イニシアティブの考え方などを参照しつつ電気通信事業ガイドライン等の改正について検討していく必要があると考えられる。

具体的には、プラットフォーム事業者、アプリケーション提供事業者、ウェブサイト運営者、広告事業者等の利用者情報を取得する事業者は、自らが取得する利用者情報及び情報収集モジュールやタグなどについて十分把握した上で、取得する利用者情報の種類や利用目的などに応じて、利用者が理解できるように通知・公表や必要に応じた同意取得を行うことが重要であると考えられる。

また、利用者が実質的に理解した上で必要な判断ができるように、わかりやすい通知・公表又は同意取得の手法を検討することが重要であり、同意と通知について、いわゆるベストプラクティスとしてまとめて事業者が利用者情報の取扱いに関する通知・公表や同意取得を行う際に参照できるようなものとして示していくことが適当である。この際、スマートフォンや各サービスの内容、利用者の特性等も考慮することが有用であり、ユーザーテストやステークホルダーの意見等も適切に活用すべきであると考えられる[103]。

更に、プラットフォーム事業者内に蓄積されたパーソナルデータについての開示・利用条件・選択機会の提供を行っていくことが重要であり、利用者が自らの利用者情報の取扱いについてコントロールができる観点から、ダッシュボード、オプトアウト有無・方法の開示、データポータビリティ有無・方法の開示、選択機会の通知やガイダンス等について導入していくことが期待される。

---

[103] 企業がプライバシーに関する問題に能動的に対応し、消費者やステークホルダーと継続的なコミュニケーションを行い、説明責任を果たしていくことは、プライバシーガバナンスの観点から重要である。(「DX 時代における企業のプライバシーガバナンスガイドブック ver1.0」2020 年 8 月　総務省、経済産業省 https://www.soumu.go.jp/main_content/000704656.pdf)

【具体的に記載の充実などを検討する項目等について】
＜３.電気通信事業者の義務＞

〇個人情報保護管理者（現行電気通信事業ガイドライン第 13 条）

電気通信事業を営み電気通信サービスを提供する者が自ら取り扱う利用者情報の内容について把握し、適切にこれを取り扱うデータやプライバシーのガバナンスを確保していく観点から、個人情報保護管理者は重要であり、必要に応じて記載について充実を検討することが適当である。

〇プライバシーポリシー（同第 14 条）

電気通信事業を営み電気通信サービスを提供する者が自ら取り扱う利用者情報の内容について把握した上で、これを適切に利用者に対して説明していくことは重要であり、記載を見直し充実することを検討することが適当である[104]。

・ プライバシーポリシーの公表（同第 14 条第１項）

既に記載されているプライバシーポリシーに記載すべき内容について精査し整理するとともに、オプトアウトの有無や方法、データポータビリティの有無や方法等プライバシーポリシーに記載すべき事項として電気通信事業 GL や解説に追加を行うことを検討する。

・ アプリケーションソフトウェアに係るプライバシーポリシー（同第 14 条第２項・第３項）

アプリケーション作成者、情報収集モジュール提供者、広告事業者、ウェブサイト管理者等が留意すべき事項も含めた形で、SPI の履行状況なども考慮した上で必要とされる対応を検討し、電気通信事業 GL や解説に記載を検討する。

・ 分かりやすい通知・公表や利用者による選択の提供

分かりやすい通知・公表や同意取得を実現するために考慮すべき点や留意すべき事項について電気通信事業 GL や解説に追加を行うことを検討する。階層的な通知・公表や個別同意、

---

104 「デジタル広告市場の競争評価　最終報告」（2021 年 4 月 27 日、デジタル市場競争会議）「課題⑩：[パーソナル・データ] パーソナル・データの取得・利用に係る懸念」の「７　対応の方向性」（１）に記載されている４つの項目を電気通信事業 GL の改正において盛り込む形で検討を行うことが求められており、今後総務省においてこれを踏まえ検討を進めていくことが必要である。

Consent Record 等による一覧性のある表示やダッシュボードによるオプトインやオプトアウトの機会の提供等のベストプラクティスについて、事例としてまとめた上で、電気通信事業GL や解説に記載を検討する。

・ 要配慮個人情報の扱い

健康、宗教、政治的信条等の要配慮個人情報等について、個人情報保護法において、本人の同意がなければ取得してはならないこととされている。広告等のセグメントとして用いる場合など本人の同意を取得することなくこれを不必要に用いないことが求められると考えられる。

＜４．各種情報＞

〇位置情報（現行電気通信事業 GL 第 35 条）

電気通信事業を営み電気通信サービスを提供する者が自ら取り扱う利用者情報の内容について把握した上で、これを適切に利用者に対して説明していくことは重要である。位置情報であって、GPS、WiFi、基地局、ビーコンなど通信を経由して把握されるものについては、新たに利活用の実態についても把握した上で、通信関連プライバシーの一環として適切な取扱いを確保していく必要がある。

なお、個人情報保護法上、「ある個人の位置情報」が個人関連情報として位置づけられる場合もある。この際、第三者提供をしようとする場合には相手側事業者がその取得について個人から同意取得を行っていることを確認する必要が出てくる。このような新たな規律と、既存の電気通信事業 GL との整合性についても確認をしていくこととする。

〇その他

電気通信事業に固有の各種情報の取扱いについて規定している「４.各種情報」における規定について必要に応じて見直すこととする。その際、本 WG における検討結果などを踏まえ、「通信関連プライバシー」情報に関連して必要とされる記載についても検討することとする。

＜５．モニタリングの実施とガイドラインの見直し＞

〇モニタリングの実施[105]とガイドラインの見直し（現行電気通信事業

[105] 「デジタル広告市場の競争評価　最終報告」「課題⑩：[パーソナル・データ]パーソナル・デー

GL 第 39 条）

共同規制の下で、電気通信事業を営み電気通信サービスを提供する者が自ら取り扱う利用者情報の適切な取扱いを促しこれを確保していく観点から、特にプライバシーポリシーや個人情報保護管理者の関係を中心に、定期的にモニタリングを行うこととし、その状況を踏まえ、今後も必要に応じて電気通信事業 GL 改正等を検討していくこととする。

電気通信事業 GL 及び解説における現行の主な記載

条文	主な記載
第 13 条 （個人情報保護管理者）	**個人情報保護管理者（当該電気通信事業者の個人データ等の取扱いに関する責任者）を設置し、ガイドラインを遵守するための内部規定の策定、監査体制の整備及び個人データ等の取扱いを監督する努力義務を規定。** 電気通信事業者内部における責任体制を確保するため、個人データ等の適正な取扱いの確保について必要な権限を有する役員等の組織横断的に監督することのできる個人情報保護管理者を置き、必要な監督等を行わせよう努める旨を解説に記載（解説 3-3-7）。
第 14 条 （プライバシーポリシー）	**プライバシーポリシー（個人情報保護を推進する上での考え方や方針）を公表する努力義務を規定。（第１項）** 電気通信事業者の個人情報保護についての社会的信頼を確保するため、電気通信事業者は自らの個人情報保護を推進する上での考え方や方針についての宣言をプライバシーポリシーとして公表することが適切であるとした上で、プライバシーポリシーに記載すべき事項について、具体的に解説で言及。（解説 3-4-1） **アプリケーションソフトウェアを提供する場合、当該アプリケーションの情報取得等に係るプライバシーポリシーを公表する努力義務を規定。（第２項）** **アプリケ-ションを提供するサイトを運営する場合、当該サイトにおいてアプリケーションを提供する者に対して、当該アプリケーションの情報取得などに係るプライバシーポリシーを公表するよう促す努力義務を規定。（第３項）** アプリケーションのプライバシーに記載すべき事項について具体的項目を示し、スマートフォン　プライバシー

タの取得・利用に係る懸念」の「７　対応の方向性」において、取引透明化法におけるパーソナル・データの取扱いに関する開示やモニタリングの対応については、総務省の行うヒアリングに透明化法のレビュー担当者がオブザーバ参加する形で対応するなど、連携した形で行うこととされている。

	イニシアティブ等によるものと解説で言及。（解説 3-4-2）
第 35 条 （位置情報）	**電気通信事業者は、あらかじめ利用者の同意を得ている場合、正当業務行為その他の違法性阻却事由がある場合に限り、取得可能。（第１項）** あらかじめ利用者の同意を得ている場合、令状に従う場合その他の違法性阻却事由がある場合に限り、他人への提供その他の利用可能。（第２項） 通信の秘密に該当する位置情報について匿名化して他者へ提供等を行う場合には利用者の同意を得る必要があること、通信の秘密に該当しない位置情報について他者へ提供等を行う場合には利用者の同意又は違法性阻却事由がある場合に限定することが強く求められる（解説 5-4-2） 位置情報サービスの提供にあたっては、利用者の権利が不当に侵害されることを防止するために必要な措置を講ずることが適切。（第３項） ①利用者の意思に基づく提供、②利用者の認識・予見可能性の確保、③適切な取扱い、④提携に関する約款等への記載等。（解説 5-4-3） **捜査機関からの要請により取得を求められた場合は、令状に従う時に限り、取得可能。（第４項）** **救助を行う機関からの要請により取得を求められた場合は、生命又は身体に対する重大な危険が切迫し、早期発見のために不可欠であると認められる場合に限り、取得可能。（第５項）** GPS 位置情報は通信の秘密ではないが、基地局の位置情報よりも高いプライバシー性を有する（解説 5-4-5）
第 39 条 （ガイドラインの見直し）	**本ガイドラインについては、社会情勢の変化、国民の意識の変化、技術動向の変化等諸状況の変化を踏まえ、必要に応じ見直しを行う。**

（３）　定期的なモニタリングの実施

あらかじめ必要とされる事項を法令又はガイドラインなどで一定の基準を示した上で、取り扱う利用者情報の内容や利用目的等も考慮した上で、国内外のプラットフォーム事業者、電気通信事業者など関係者との間で継続的な対話を行い、関係事業者及び事業者団体による自主的取組を進め、その履行状況を政府が定期的にモニタリングするという共同規制的なアプローチを適切に機能させることが重要である[106]。モニタリング結

[106] リスクベースで大規模プラットフォーム事業者や移動通信事業者など利用者への影響が大きい事業者を重点的にモニタリングすることを検討する。

果については公表することにより、透明性・アカウンタビリティを確保していくことが有用であると考えられる。

この際、利用者側が意味のある判断を行うことができるように、取得される情報や利用目的を示す際に利用者側への影響について考慮しそれを分かりやすく示していくことが有用であると考えられる。例えば、利用者情報の取得により何が起こるか示すと分かりやすいとの指摘がある。また、弱者に対する不利益とか差別が起きない観点からも、ベストプラクティスを考えていくことも重要であるとの指摘がある。

更に、このような、利用者へ与えうる影響（アウトカム）を検討する観点からも、PIA やリスク評価を実施することも有用であると考えられる。PIA については、第２章にも述べたように、主な事業者は何らかの形で取り組んでいるが、その基準や結果等が明らかとなっていない場合が多く見られる。今後は、一定の基準[107]を参照するとともに、PIA 報告書を公表するなどの取組が進められることが有用であると考えられる。また、通信の秘密、個人情報、プライバシー等が適切に保護されるためには、情報漏えい等がないことが必要不可欠であり、セキュリティ確保の観点から、適切な安全管理措置やガバナンスが確保されることも重要である。

（４）　専門的な知見の蓄積と発信の重要性

デジタルプラットフォーム事業者による利用者情報の取得・収集・分析やデジタル広告市場の動向等については、技術やサービスの発展が早く、また現在も情勢が変化している状況である。

モニタリングは利用者情報の取扱いに係る技術的な動向を踏まえて行う必要があり、モニタリングを通じて把握した技術的動向について技術的解説や整理としてとりまとめることが望ましい。専門的知見を有する有識者にタスクフォース等として技術的解説や整理をとりまとめいただくとともに、継続的にこれを更新していくことを検討することが望ましい。

このような専門的知見を官民連携し蓄積し必要に応じ発信していくことは、モニタリングのために資するとともに、次に述べる利用者の理解促進のための取組を進める上でも、外部レビュー等を行う上でも有益なものと考えられる。

（５）　利用者の理解促進・外部レビュー

①　利用者の理解促進に向けた取組

[107] ISO/IEC29134 が発表されており、JISX9251：2021 として 2021 年 1 月規格化された。

デジタル広告市場におけるターゲティング広告に対する消費者の不安はその仕組みが見えていないことに由来する側面があるとの指摘がある。事業者団体などによるソフトローによる取組が行われているとしても外部からそれが見えづらい部分もあると指摘される。

インターネットやプラットフォームサービスが、青少年から高齢者まで、様々なリテラシーの者の誰もが安心して使いやすいものとなるように、関係事業者や業界団体等が、外部に開かれた形で対話や情報発信を継続し、透明性を高め利用者に対して周知啓発を推進し、利用者のリテラシー向上を図っていくことが期待される。ターゲティング広告の仕組みを説明する啓発や情報発信を行うことや、オプトアウトサイト等により利用者の選択の機会を提供すると共に利用者の権利を保護するための注意喚起を行うことも重要であると考えられる。

これは、各事業者が利用者に対して通知・公表又は同意取得をしていく際にも、それを利用者が認識し理解を高めるために有用であり、業界全体としての取組が進展することが期待される。

② 外部レビュー

利用者の理解促進を図る上でも、専門的見地から事業者のプライバシーポリシー等の内容や利用者情報の取扱いや説明・同意等の在り方について外部レビューが実施され、その結果が公表されることも有用であると考えられる。

海外において、下記のように消費者団体や財団、コンサルティング企業等がプライバシーポリシー等の外部レビューを行い結果が公表されている[108]。このような取組が我が国においても行われていくことも有用であると考えられる。

また、プライバシー・ポリシーの公表意義は企業活動の透明性やアカウンタビリティの観点からも社会的・制度的に大きいことが指摘される。利用者情報の適切な取扱いについて検討し、プライバシーポリシー等の説明を行い、適切な運用を実現していく企業のプライバシーガバナンスを確立していくことは、今後企業の事業の成長や競争力を向上させる観点からも重要性が高まってきている。

[108] この他、モニタリング指標として、世界広告主連盟（World Federation of Advertisers）のレポンシブルメディア(GARM: Global Alliance for Responsible　Media)などもある。

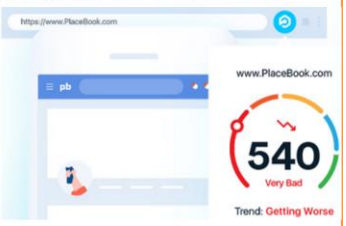
海外におけるプライバシーポリシー等の外部レビューの例

Ranking Digital Rights （米）

- New America（市民プラットフォーム、シンクタンク的な機能を有する財団）のプログラムの一つ。
- 世界的なデジタルプラットフォーマー、通信会社について、プライバシーポリシー等の開示情報に基づき、①ガバナンス、②表現の自由、③プライバシー※1の３つの観点からランキングを作成※2する取組。
  - ※1 プライバシーは、①プライバシーポリシーのアクセスや明確さ、②利用者情報（収集、共有、利用目的、保存期間、ターゲット広告の選択、データ開示、追跡の明確な開示）、③政府の要求、④セキュリティの4つの視点から評価
  - ※2 各事業者や提供サービスを総括したレポートを公表、利用者が見たい項目を選びランキング表示可能
- 2015年よりほぼ毎年実施（2020年までで合計5回）。
  2020年レポートのURL：https://rankingdigitalrights.org/index2020/

privacymonitor（米）

- Osano, Inc.（データプライバシーのコンサルティング等を行う米企業）が無料で提供するプライバシーポリシー評価Webサイト、及びプラグイン（ブラウザ拡張機能）。
- 様々なWebサイトのプライバシーポリシーに５段階評価を付けており、https://www.privacymonitor.com/score/でWebサイトのドメイン名を入力したり、プラグインをインストールしたブラウザでWebサイトを訪れたりすると、当該Webサイトの評価を見ることができる。
- 例えば、最上の「Exceptional」を付けられるWebサイト（全体の5%未満）概ね、①法令の要請又はオプトインの同意がない限りデータを第三者に提供しない、②サービス提供のために必要最小限のデータしか収集しない、などの特徴が認められる。



Claudette（欧）

- 欧州消費者機構（32か国44の独立した消費者団体からなるグループ）が2018年のGDPR施行に合わせて実施したプロジェクト（https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf）。
- AIソフトウェア「Claudette」により、主要テクノロジ企業のプライバシーポリシーを調査。
- 個別の企業のポリシーの評価は明らかにしなかったが、全体のポリシーの条項の3分の1以上は「潜在的問題がある」か「情報不足」と判断。ポリシーの文章の11%には不明瞭な表現が検出され、一部のポリシーは当該企業がデータを共有できるサードパーティーを明示していなかった、と指摘。

（６） 国際的な対話と連携の推進に向けて

利用者情報の取扱いはグローバルに共通した課題であり、主要先進国の規制当局において検討が進んでいる。グローバルに事業活動を展開する複数のデジタルプラットフォーム事業者が大きな存在感を有しており、利用者情報に関するその取組の影響も大きくなる中で、国際的に連携した取組を進めることが有用である。

既に、日 EU の間では、日 EU・ICT 政策対話[109]（第 26 回）（2021 年２月）及び日 EU・ICT 戦略ワークショップ[110]（第 11 回）（2021 年４月）の場において、電気通信事業法の域外適用の規定が 2021 年４月に施行され外国事業者であるプラットフォーム事業者へも電気通信事業法を適用するととも

[109] 総務省と欧州委員会（通信ネットワーク・コンテンツ・技術総局）との間で、ICT 政策全般について、定期的に実施している政策対話

[110] 総務省と欧州委員会（通信ネットワーク・コンテンツ・技術総局）が共催し、日 EU の官民の相互理解と連携協力の推進するために定期的に開催している戦略ワークショップ

に、利用者情報の適切な取扱いに関して検討を行っていること等について日本側から紹介し、欧州側から 2020 年 12 月に公表されたデジタルサービス法（DSA）案及びデジタルマーケティング法（DMA）案の概要について説明があった。独占的地位を占めるプラットフォーマーへの懸念が日 EU で共有され引き続き意見交換を継続[111]することとなるとともに、モニタリングや透明性確保の重要性等が日 EU 双方から指摘された[112]。

二国間の間では、日独ＩＣＴ政策対話[113]（第５回）（2021 年３月）において、改正電気通信事業法（外国法人等に対する法執行の実効性の強化）及び利用者情報の適切な取扱いに関して検討について日本側から紹介し、独側から EU から昨年末公表された DSA/DMA 案を受けたドイツの取組について説明があった。また、日仏 ICT 政策協議[114]（第 21 回）（2021 年６月）において、プラットフォーム政策の一環として利用者情報の取扱いについて日本側から説明し、フランス側からも同国におけるプラットフォーム政策について説明があった。

今後、本中間とりまとめの内容なども踏まえ、我が国における制度的な検討やプラットフォーム事業者等のモニタリング等の取組を進める[115]とともに、積極的に二カ国の枠組みにおける対話と連携を進めることが有用である。

また、更に、多国間連携の場として、OECD、アジア太平洋国際協力（APEC）等の国際的機関[116]や地域連合の場においても我が国における取組を説明し、連携しつつ対応を進めていくことが期待される。

---

111 「日 EU・ICT 政策対話（第 26 回）の結果」（令和 3 年 2 月 26 日総務省報道発表）

112 「日 EU・ICT 戦略ワークショップ（第 11 回）の結果」（令和 3 年 4 月 20 日総務省報道発表資料）

113 総務省とドイツ連邦共和国・連邦経済エネルギー省との間で、ICT 政策に関する情報交換・意見交換の場として、定期的に実施している政策対話

114 総務省とフランス共和国・経済財政復興省との間で、デジタル分野における政策について相互理解を深め連携・協力の推進を目的として、定期的に実施している政策協議

115 国際的に技術的な知見やモニタリングのプラクティスの共有等を行うことも有用であると考えられる。

116 2011 年に国際連合人権理事会で「ビジネスと人権に関する指導原則：保護、尊重及び救済の枠組みにかかる指導原則」が作られ、人権デュー・ディリジェンス（人権への影響の特定、予防、軽減、対象方法について説明するための、企業による一連の流れ）の実施が原則に掲げられている。

おわりに

本中間とりまとめ（案）は、誹謗中傷や偽情報を含む違法・有害情報対策に関して、緊急提言・政策パッケージ・2020 年２月の本研究会の報告書を受けて、その後官学官民のステークホルダーにより取り組んできた対策に関するモニタリング結果も踏まえ、今後の検討の具体的な方向性を示したものである。

また、利用者情報の適切な取扱いに関しては、2020 年２月の本研究会の報告書を踏まえた上で、新たに立ち上げられた「プラットフォームサービスに係る利用者情報の取扱いに関する WG」におけるモニタリング結果や検討を踏まえ、今後の検討の具体的な方向性を示したものである。

本中間とりまとめ（案）において示した提言事項については、プラットフォームサービスの普及・拡大に伴う急速な環境変化に迅速かつ適切に対応する観点から、官学産民の各ステークホルダーにおいて、速やかに取組を進めていくことが適当である。

特に、プラットフォーム事業者においては、提言内容や利用者からの期待を踏まえて、その影響力の大きさに相応した役割を適切に果たすことが期待される。

総務省においては、誹謗中傷及び偽情報を含む違法・有害情報対策及び利用者情報の適切な取扱いの確保に関して、それぞれのプラットフォーム事業者等の取組について、継続的なモニタリングを行うことが適当である。

特に、違法有害情報対策については、次回以降のモニタリングにおいて、依然として事業者が自主的な報告を行わない場合や、我が国における透明性・アカウンタビリティ確保が実質的に図られない場合には、透明性・アカウンタビリティの確保方策に関する行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与について、具体的に検討を行うことが必要である。

また、利用者情報の適切な取扱いの確保については、関係法令やガイドラインに関する制度整備に係る事項に関して、速やかに対応を行うことが適当である。

さらに、総務省においては、今後ともプラットフォームサービスを巡る市場動向が電気通信分野に及ぼす影響や環境変化、さらには国際動向を注視するとともに、必要に応じて、政策対応の在り方について不断の見直しを行い、利用者が安心・信頼してプラットフォームサービス及び電気通信サービスを利用できるよう努めていくことが適当である。

以上

参考資料集

第１部　誹謗中傷や偽情報を含む違法・有害情報への対応について

参考１　プラットフォームサービスに関する研究会　構成員名簿
参考２　プラットフォームサービスに関する研究会　開催状況
参考３　誹謗中傷等への対策状況　ヒアリングシート（2021 年 2 月 25 日）回答における主な項目の比較
参考４　フェイクニュースや偽情報等への対策状況　ヒアリングシート（2021 年 3月 30 日）回答における主な項目の比較
参考５　違法・有害情報への取組に関する透明性・アカウンタビリティ確保に係る各国政策の比較

第２部　利用者情報の適切な取扱いの確保について

参考６　プラットフォームサービスに関する研究会　プラットフォームサービスに係る利用者情報の取扱いに関するＷＧ　構成員名簿
参考７　プラットフォームサービスに関する研究会　プラットフォームサービスに係る利用者情報の取扱いに関するＷＧ　審議経過
参考８　海外動向関連参考資料
参考９―１　移動通信事業者における利用者情報の取扱い状況
参考９－２　プラットフォーム事業者における利用者情報の取扱い状況

第１部　誹謗中傷や偽情報を含む違法・有害情報への対応について

参考 1

プラットフォームサービスに関する研究会
構成員名簿

（敬称略・五十音順）

【構成員】

	生貝　直人	一橋大学大学院　法学研究科　准教授
	大谷　和子	株式会社日本総合研究所　執行役員　法務部長
	木村　たま代	主婦連合会　事務局長
	崎村　夏彦	東京デジタルアイディアーズ　主席研究員
（座長）	宍戸　常寿	東京大学大学院　法学政治学研究科　教授
（座長代理）	新保　史生	慶應義塾大学　総合政策学部　教授
	手塚　悟	慶應義塾大学　環境情報学部　教授
	寺田　眞治	一般財団法人日本情報経済社会推進協会　主席研究員
	松村　敏弘	東京大学　社会科学研究所　教授
	宮内　宏	宮内・水町 IT 法律事務所　弁護士
	森　亮二	英知法律事務所　弁護士
	山口　いつ子	東京大学大学院　情報学環　教授
	山本　龍彦	慶應義塾大学大学院法務研究科教授

【オブザーバ】

個人情報保護委員会事務局

法務省人権擁護局

参考２

プラットフォームサービスに関する研究会　開催状況

	開催日程	議題
第 21 回	令和 2 年 11 月５日	（１）　今後の検討の進め方 （２）　利用者情報の適切な取扱いの確保に向けて
第 22 回	令和 2 年 12 月４日	（１）　利用者情報の適切な取扱いの確保に向けて
第 23 回	令和 2 年２月 25 日	（１）　誹謗中傷等への対策状況に関する事業者ヒアリング （ヤフー、Facebook、Google、LINE、Twitter） （２）　誹謗中傷等への対策状況に関する事業者団体ヒアリング （セーファーインターネット協会、ソーシャルメディア利用環境整備機構） （３）　政策パッケージの進捗状況について （４）　違法・有害情報相談センターに寄せられている相談状況および関連機関との連携について （５）　法務省の人権擁護機関による削除要請と削除対応率について
第 24 回	令和３年３月 17 日	（１）　インターネット上の違法・有害情報を巡る諸外国の動向について （２）　誹謗中傷等に対する取組の検証・評価について
第 25 回	令和３年３月 30 日	（１）　フェイクニュースや偽情報への対策状況に関する事業者ヒアリング（ヤフー、Facebook、Google、Twitter） （２）　フェイクニュースや偽情報への対策状況に関する事業者団体ヒアリング （セーファーインターネット協会） （３）　米国大統領選挙でのプラットフォーマーの取組について （４）　フェイクニュースや偽情報等に対する取組についてのフォローアップに関する主な視点
第 26 回	令和３年４月 12 日	（１）　「フェイクニュース」に関するアンケート調査結果について （２）　誹謗中傷やフェイクニュースの拡散メカニズムについて
第 27 回	令和３年５月 13 日	（１）　フェイクニュースや偽情報への対策状況に関する事業者ヒアリング（LINE） （２）　日本や海外におけるファクトチェックの取組について （３）　諸外国におけるファクトチェックの取組について （４）　フェイクニュース生成・拡散のメカニズム
第 28 回	令和３年６月 10 日	（１）　プラットフォームサービスに係る違法・有害情報（誹謗中傷、偽情報等）への対策に関する主な論点について （２）　プラットフォームサービスに係る利用者情報の取扱いに関する主な論点について

誹謗中傷等への対策状況　ヒアリングシート（2021年2月25日）回答における主な項目の比較

※総務省において要約したもの。詳細は各社の回答原本を参照。

社名			ヤフー株式会社	Facebook Japan株式会社		Google合同会社	LINE株式会社	Twitter Japan株式会社
1-①	対象サービス名		Yahoo!知恵袋、Yahoo!ニュース(コメント欄のみ)、Yahoo!ファイナンス	Facebook	Instagram	YouTube, Google 検索, Google マップ	LINE タイムライン、LINE Openchat、LINE LIVE、LINE BLOG、livedoor Blog	Twitter
1-②	加入者数、月間アクティブユーザ数又は書き込み数	【日本の数値】	2020年度の任意の1か月における書き込み総数 ■知恵袋 投稿数：約440万件 ■ヤフーニュース 総投稿数：約1,300万件 ■ファイナンス掲示板 総投稿数：約210万件	月間アクティブアカウント数：2,600万人（2019年7月）	月間アクティブアカウント数：3,300万（2019年3月）	回答なし	国内MAU 8,600万人（2020年9月末時点）	回答なし
		【グローバルの数値】		月間アクティブアカウント数：28億人（2020年6月）	月間アクティブアカウント数：10億（2018年6月）	YouTube: 毎月20億人以上のログインユーザー。毎日10億時間以上の動画視聴 Google 検索: 毎年何兆回もの検索回数 Google マップ: 10 億人以上	主要4か国（日本・台湾・タイ・インドネシア）MAU 1億6,700万人（2020年9月末時点）	回答なし
		【（質問に答えられない場合）参考となる数値】						収益化可能な日時平均アクティブユーザー数（mDAU）：1億9,200万（2020年第4四半期；グローバル）
2-①	誹謗中傷等に関する申告や削除要請の件数 (i)一般ユーザ、(ii)司法機関・行政機関	【日本の数値】	・各サービスにおいて、特定の一か月間の数値を算出。 ・また、サービスごとに利用している申告フォームの仕様や運用等が異なるため、集計できる数値に差異がある。 (i)(ii)合計値： ■知恵袋 「違反連絡リスト＞不適切な投稿」で申告された案件数：約6.6万件 ■ヤフーニュース 「不快」を理由とする違反申告数：不明（取得不可） ※総違反申告数：約16万件 ■ファイナンス掲示板 不快（アダルト・グロ・罵詈雑言）での違反申告数：約1.6万件	サービス全ての合計、誹謗中傷以外を含む (i)一般ユーザ 非公開 (ii)司法機関・行政機関 86 件（2019 年 6 月～2020 年 5 月） （行政機関および法執行機関からの情報開示請求）		(i)一般ユーザ [検索]： 名誉毀損問題の法的理由のためにコンテンツを報告するためにGoogle検索ウェブフォームを通じて提出されたURL：約7000件（2019年） (ii)司法機関・行政機関 2020年1月から6月までに日本政府（政府機関及び裁判所命令）から受けた名誉毀損に関する依頼は57件（アイテム数595件）。政府から受けた依頼全体の85%。	(i)一般ユーザ [タイムライン] 919件、[Openchat] 2,115件、[LIVE] 312件、[BLOG] 27件、[livedoor Blog] 2,479件 ※タイムライン／Opencaht／LIVEについては、迷惑行為全般に関する件数。BLOG／livedoor Blogについては、プライバシー権・名誉権侵害に関する件数。 (ii)司法機関・行政機関 [タイムライン] [Openchat] [LIVE] [BLOG] 0件 [livedoor Blog] 19件	(i)一般ユーザ 回答なし (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 裁判所命令：21 その他の法的要請：19,903
		【グローバルの数値】						(i)一般ユーザ（2020年上半期） 暴力をほのめかす脅迫：2,203,411 センシティブな内容のメディア：3,365,868 個人情報：1,115,655 合意のない裸体の描写：609,842 なりすまし：1,572,672 ヘイト行為：6,055,642 児童の性的搾取：92,485 攻撃的な行為、嫌がらせ：5,138,663 (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 裁判所命令：1,894 その他の法的要請：40,326
2-②	誹謗中傷等に関する申告や削除要請に対する削除件数 (i)一般ユーザ、(ii)司法機関・行政機関	【日本の数値】	(i)(ii)合計値： ■知恵袋 「違反連絡リスト＞不適切な投稿」で申告された案件の削除数：約1.9万件 ■ヤフーニュース 違反申告されて「不快」を理由に削除された件数：約1.8万件 ※誹謗中傷等に関する申告件数が取得できないことから、削除された理由が「不快となっている」もものについて集計。 ■ファイナンス掲示板 違反申告されて「不快（アダルト・グロ・罵詈雑言）」で削除された件数：約7千件	（誹謗中傷以外を含む） (i)一般ユーザ 0 件（2020 年 1 月～6 月） （利用者の申告に基づき、コミュニティ規定に違反していないコンテンツで、日本の法令違反だとみなされたコンテンツの制限） (ii)司法機関・行政機関 0 件（2020 年 1 月～6 月） （司法機関の命令に基づき、コミュニティ規定に違反していないコンテンツで、日本の法令違反だとみなされたコンテンツの制限） 全情報開示請求のうち 53%で何らかのデータを提供（2020 年 1 月～6 月）		(i)一般ユーザ [Youtube]：コミュニティガイドライン違反（ヘイトスピーチ、嫌がらせやネットいじめ以外も含む）で削除された動画の数：49,180 本（2020年10月から12月まで） ※ユーザーからの報告や機械によってフラグされたものを含む （参考）グローバルでは、削除された約1,000万本の動画のうち、ハラスメントやネットいじめが原因で削除された動画はそのうちの約0.8%。 [検索]：法律に基づく削除に関する問題を報告するためのウェブフォームを通じて一般ユーザー（もしくはその法的代理人）により名誉毀損を報告された推定7000件のURLのうち、法的理由で約1700件のURLを検索結果から非表示化（2019年）。 非表示化した報告：約24%。非表示化しなかった報告：約55%。 Googleから報告者に追加情報の提供を求める必要があった報告：約20%。 ※Google が追加情報を要求する理由としては、権利者が明確に特定されていない可能性がある、要求の法的根拠が明確に特定されていない可能性がある、などが挙げられる。 (ii)司法機関・行政機関 449件を削除（google全体、名誉毀損以外の請求などに関するものも含む。2020年1月から6月）	(i)一般ユーザ [タイムライン] 8件、[Openchat] 22件、[LIVE] 26件、[BLOG] 24件、[livedoor Blog] 約1,600件 (ii)司法機関・行政機関 [タイムライン] [Openchat] [LIVE] [BLOG] なし [livedoor Blog] 14件	(i)一般ユーザ 回答なし (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 表示制限されたアカウント：0 表示制限されたツイート：181 利用規約違反によるコンテンツ削除：7,148
		【グローバルの数値】		(i) 630万件（2020 年10 月～12 月） （コミュニティ規定に違反したコンテンツの削除件数）	(i)500 万件（2020 年10月～12 月） （コミュニティガイドラインに違反したコンテンツの削除件数）			(i)一般ユーザ（2020年上半期） 暴力をほのめかす脅迫：23,835 センシティブな内容のメディア：167,697 個人情報：25,756 合意のない裸体の描写：9,227 なりすまし：131,136 ヘイト 行 為：635,415 児童の性的搾取：444,781 攻撃的な行為、嫌がらせ：398,057 (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 表示制限されたアカウント：82 表示制限されたツイート：3,069 利用規約違反によるコンテンツ削除（裁判所命令）：407 利用規約違反によるコンテンツ削除（その他法的要請）：25,110

参考3

社名			ヤフー株式会社	Facebook Japan株式会社		Google合同会社	LINE株式会社	Twitter Japan株式会社
2-②	削除割合 (i)一般ユーザ、(ii)司法機関・行政機関	【日本の数値】	(i)(ii)合計値： ■知恵袋 誹謗中傷等に関する申告数における削除率：29.3% ■ヤフーニュース 総違反申告数に対する全ての申告削除率：17.5% ※誹謗中傷に限定されない ■ファイナンス掲示板 不快を理由とする違反申告数における削除率：44.5%	回答なし	回答なし	回答なし	(i)一般ユーザ [タイムライン] 1%、[Openchat] 1%、[LIVE] 8%、[BLOG] 89%、[livedoor Blog] 65% ※申告・要請件数に関しては前項2. ①の通り各サービスの態様/性質に応じて計上する一方、削除に当たってはポリシーに則って対応しておりサービス毎に削除割合の多寡が異なる。 (ii)司法機関・行政機関 [タイムライン] [Openchat] [LIVE] [BLOG] なし [livedoor Blog] 74%	(i)一般ユーザ 回答なし (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 裁判所命令：95% その他の法的要請：32%
		【グローバルの数値】		回答なし	回答なし	回答なし		(i)一般ユーザ 回答なし (ii)司法機関・行政機関（2020年上半期；誹謗中傷等に限定しない削除請求） 裁判所命令：19% その他の法的要請：31.7%
		【（質問に答えられない場合）参考となる数値】		回答なし	回答なし	（参考回答） リクエストに応じずコンテンツを削除しない理由は状況によって様々。政府やユーザーが求める削除対象が明確でない（たとえばリクエストにURL が記載されていない）場合や、コンテンツがすでに作成者によって削除されている場合などは、リクエストに応じることはできない。上記情報で一部は削除割合を示しているが、削除割合にとらわれることは全体像を理解する上で必ずしも得策ではないことに留意が必要。		
	削除までの平均時間 (i)一般ユーザ、(ii)司法機関・行政機関	【日本の数値】	回答なし	回答なし	回答なし	回答なし	(i)一般ユーザ 数日～10日前後 (ii)司法機関・行政機関 1週間程度～数ヶ月前後	回答なし
		【グローバルの数値】	回答なし	回答なし	回答なし	回答なし		回答なし
		【（質問に答えられない場合）参考となる数値】	申告窓口やパトロールの手法（人かAIか）、事案の軽重等により異なるため、一概に回答することは難しいが、AIや機械学習を用いた監視体制であれば投稿後、速やかに削除可否の判断が可能である。 また、人によるパトロールであっても、権利侵害性に疑義がない明確な投稿であれば一両日中に判断できるものもあれば、判断に悩ましい投稿については、一担当者のみの判断によらず、複数人での協議や、法的判断を行っている専門部署へのエスカレーション、投稿者への意見照会などを経て最終的な判断がなされるため、相当の期間をもって慎重に判断がなされる。	「表示頻度（prevalence）」 ※表示頻度指標は、違反コンテンツの総閲覧回数（分子）を、すべてのコンテンツの総閲覧回数（分母）に占める割合として推定。 例えば、2020年第4四半期のヘイトスピーチの表示頻度は0.07%～0.08%、つまり、コンテンツの1万ビューごとにヘイトスピーチのビューが7～8回。		「平均所要時間」に基づく評価は、いくつかの理由から問題があると考えている。①プラットフォームが展開した施策の有効性を評価するための最も効果的な指標ではない可能性がある。②プラットフォームに対して、迅速かつ慎重に作業するよりも、対処にかかる時間を早めることを奨励することとなる可能性がある。③平均的な所要時間を測定することは、例えば平均所要時間の中央値のようなデータと比較をするなど、不用意にデータを歪めることを誘導しかねない。		回答なし
2-③	②以外の誹謗中傷等に関する削除件数（AIを用いた自動検知機能の活用等）	【日本の数値】	・各サービスにおいて、特定の一か月間のパトロール数値を算出。 ・また、サービスごとに利用しているパトロールツールの仕様、運用、基準等が異なるため、集計できる数値に差異がある。 ・効率的なパトロールとなるよう、重点的に対応すべきパトロール対象、運用方法については柔軟に見直しを実施。本件数値については、集計対象期間によっては必ずしも同じ結果となることを示すものではない。 ■数値 ■知恵袋 約3万2千件 ※違反申告を除く、低品質対応・積極巡回による不快削除件数 ■ヤフーニュース 約5万8千件 違反申告以外で不快で削除された件数 AIによる投稿削除数：約25万件 ■ファイナンス掲示板 約5万4千件 ※違反申告以外での不快（アダルト・グロ・罵詈雑言など）で削除された件数	回答なし	回答なし	回答なし	[タイムライン] 78,962件、[Openchat] 78,770件、[LIVE] 3,780件、[BLOG] 6,358件 ※自動検知したうち一定の要件に合致した件数。	回答なし
		【グローバルの数値】		48.8%（2020 年 10月～12 月） 「How much did we find before users reported it」（事前対応率）	80.0%（2020 年10月～12月） 「How much did we find before users reported it」（事前対応率）	930万本以上の動画をコミュニティガイドライン違反を理由に削除（2020年10月から12月）。 これらの動画の94%に当たる8,800,082件は、人間ではなく機械によって最初にフラグ化。人工知能によって検出された動画のうち、35.9%は一度も視聴をされる前に、35.9%は1～10回以下の視聴回数のうちに削除。 9億件以上のコメントを削除（2020年10月から12月）。削除されたコメントの99.6%が自動的に検出。		回答なし
		【（質問に答えられない場合）参考となる数値】		回答なし	回答なし			・2019年4月時点で、強制執行措置の取られた攻撃的なコンテンツの38%は、利用者からの報告ではなく、テクノロジーを駆使しTwitterの専門のチームによって積極的に特定されたもの。 ・2020年上半期に児童の性的搾取に関連する違反を理由に凍結されたアカウントのうち、91%が、テクノロジー（PhotoDNA、社内の独自ツールなど）の組み合わせで明るみに出たもの。

社名			ヤフー株式会社	Facebook Japan株式会社		Google合同会社	LINE株式会社	Twitter Japan株式会社
2-⑤	不正な申告や削除要請への対策の方法・仕組み、対応件数	【具体的な方法・仕組み】	不正な申告や不正な削除要請への対応は、パトロール部隊や専門部署により人の目により確認が行われているため、不正か否かにかかわらず、一件一件、内容を確認している。	システムの悪用を防ぐための技術を導入しており、大量の報告がコミュニティ規定の実施方法に影響を与えることはない。報告されたレポートは、FacebookとInstagramの両方のプラットフォームを担当するさまざまなチームによって審査される。利用者からの重複報告を認識する技術を使用しており、1,000人があるコンテンツを報告しても、1,000人が同じコンテンツをレビューすることがないようになっている。 また、AIは、コンテンツレビュアーがレビューするケースに優先順位をつけて、最も有害で時間的な問題のあるコンテンツを最初に処理できるようにしている。		規定に違反するコンテンツについて、削除する前に多くの人に視聴されない、またはー切視聴されることがない方が望ましいため、YouTubeを含む様々なプロダクトで、ポリシーに違反する可能性のあるコンテンツの検出を支援する自動化されたシステムを導入している。 またYouTube は、コンテンツを迅速に削除するための最善の方法は、新たな性質の問題が大きくなる前に予測することと考えている。YouTube のIntelligent Desk チームでは、ニュース、ソーシャルメディア、ユーザーの報告を監視して不適切なコンテンツに関する新しい傾向を検出し、大きな問題に発展する前に対処できるようチームの体制を整えている。		回答なし
		【日本の数値】	何をもって「不正な申告や削除要請」であると判断するのかが難しく、数値は計測していない。	回答なし	回答なし		[livedoor Blog] 857件 ※主に違法性がないと思われる投稿等への濫用的な申告の件数。	回答なし
		【グローバルの数値】		回答なし	回答なし			回答なし
		【（質問に答えられない場合）参考となる数値】		回答なし	回答なし			回答なし
3-③	対応決定時における通知の内容、理由の記載の程度		問い合わせ方法により異なるが、プロバイダ責任制限法に基づく削除請求を受領した場合には、対応決定後、申立て者に対し回答書面の発送を行う。回答書面においては、一般的な理由の記載はあるが、理由の詳細については回答していない。※個々のガイドラインに抵触する旨の説明は容易であるが、ガイドラインに抵触しないことを説明するのは非常に難しい。 削除時に投稿者に対し通知がなされるか否かは、サービスにより異なる。 例えば、知恵袋においては、削除された質問・回答については、削除がなされてから2週間、My知恵袋のページにおいて削除理由を確認することができる。	Facebookでは、虐待や嫌がらせであると報告されたコンテンツを評価する際には、常に、その報告をした人にサポート受信箱でその人の言語で最新情報を提供している。報告者には、当社が報告を評価したことだけでなく、当社がいつ、どのような措置をとったかがわかる（報告されたコンテンツに対して措置をとったか、とらなかったかの理由、報告者が好まないコンテンツや当社のコミュニティ規定に反する可能性のあるコンテンツへの対処方法の提案を含む）。場合によっては、報告者はFacebookの決定の見直しを要求することも可能。 また、Facebookは、報告の対象となった投稿を行った利用者が、実際にコミュニティ規定に反するコンテンツを投稿したと判断した場合はいつでも、報告された利用者に通知。その利用者には、当社が禁止しているコンテンツや行動の種類に関するより明確な情報とともに、当社がそのコンテンツの一部を削除したという通知が届く。 場合によっては、（アダルトヌード等の画像といった）当社のコミュニティ規定に反する可能性のある、利用者が過去に投稿した類似のコンテンツを削除するよう、確認を利用者にお願いすることがある。 これは、プラットフォーム上でどのようなコンテンツや行動が許容されるかについて人々を啓発するための取り組みの一環であり、これ以上の違反は、利用者が特定のアカウント機能へのアクセスを失ったり、アカウントへのアクセスを完全に失ったりする可能性があることを説明するためのもの。また、自分が管理しているグループやページ、イベントを削除した際には、その旨をお知らせしている。		削除要請に関するお知らせをユーザーにする方法は様々である。例えば、名誉毀損を理由に検索結果からあるURLの削除を依頼したユーザーには、受領確認としてケース番号が記載されたメールが送信される。ユーザーが削除リクエストの際にURLの管理者に連絡を試みたかどうかの確認が取れなかった場合、メールには管理者への連絡が推奨される理由や、キャッシュされたURLのコピーの削除を迅速に行う方法、特定のGoogleポリシーの削除フォームに関する情報も含まれる。削除するかどうかの決定の結果についても、メールで伝えられる。濫用を防ぐために結果に至った理由は詳細には伝えられないが、Googleとしては削除できない場合であってもその他取り得る手段などを伝えている。	削除可否等について通知。	有（日本語） 対応内容および該当するルール／ポリシーを記載。異議申し立てについても案内。
3-④	一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数	【日本の数値】	全サービス共通の数値ではあるが、パトロール部隊には数百名在籍し、24時間365日、シフトを組んで対応にあたっている。プロバイダ責任制限法に基づく法的な判断をする部署については、7.8名程度で対応。そのほか、社外弁護士複数名に諮問して対応にあたっている。	回答なし	回答なし	回答なし	各サービスにつき、10名程度	回答なし
		【グローバルの数値】		コミュニティ運営チームには、日本語を含む50以上の言語でFacebookやInstagramのコンテンツをレビューするコンテンツレビュアーが存在。過去数年の間に、安全、セキュリティ、コンテンツレビューに特化したチームを35,000人以上に拡充し、そのうち約15,000人をコンテンツレビアーに充てている。 これにより、あらゆる時間帯をカバーし、日本語を含む50以上の言語に対応。例えば、日本の真夜中に誰かが日本語の投稿を報告した場合、日本語を話すレビュアーが常に存在し、迅速なレビューのためにレポートを転送することが可能。しかし、実際には言語サポートを必要としないレポート（ヌードなど）もあり、言語に関係なく世界中のレビュアーに割り振られる。言語能力に加えて、各投稿の文脈を理解しているかどうかを確認し、有害かどうか、ポリシーに違反していないかどうかを判断するために、文化を理解している人員の確保に努めている。		当社のチームは、製品の専門家、エンジニア、弁護士、データサイエンティスト、元法執行機関職員など、多様な専門性を有している。彼らは、専門家のネットワークと密に連携をとりながら仕事をしている。 現在では Google 全体で 10,000 人を超えるスタッフが、1 日 24 時間、週 7 日、1 年 365 日体制で、Google のプラットフォーム全体でコンテンツの確認と削除に取り組んでいる。		回答なし
3-⑤	④の部署・チームに関する日本国内の拠点の有無、日本における責任者の有無			当社の審査は、ドイツ、アイルランド、ラトビア、スペイン、リスボン、米国、フィリピンなどの国の世界20以上のサイトに拠点を置いている。 いくつかのレビューサイトの所在地は公表しているが、安全性とセキュリティ上の理由から、多くのサイトやそこで働く人々についての具体的な詳細は公開していない。 私たちの人の目による審査の担当者は、様々なバックグラウンドを持った人たちである。最も重要なのは、言語と文化的背景。当社のチームは、日本語を含む当社のコミュニティで最も広く使われている言語をカバーし、50以上の言語で当社のポリシーに照らし合わせてコンテンツを審査している。		具体的な人数などは非公開。 Google では、グローバルポリシーとコミュニティガイドラインに基づき、各国の文化的背景やトレンドを理解した上で実施。例えば YouTube では各国のコンテクストやトレンドも把握しながら対策を行っており、日本を含めた各国のコンテクストを理解できるスタッフも存在し、適切な体制（日本語のネイティブのレビュアー等）を整えてる。	日本国内に拠点があり。 日本における責任者を置いている。	回答なし
3-⑥	削除等への苦情や問い合わせに対する苦情受付態勢及び苦情処理プロセス		削除等への苦情や問い合わせについては、ご意見・ご要望フォームを通じてCS窓口にて受付を行い、回答に当たり法的な判断が必要なものであれば、専門部署へエスカレーションが行われ、回答指示を行う。 今後は、後述の社内有識者会議において、AIによる対策の拡大などが進んだ場合における誤削除されたユーザーの救済が重要である旨の提言がなされたことを踏まえ、削除されたユーザーからの専用窓口を設置するとともに、削除理由の開示フローなどについて検討を進める。	Facebookでは、いじめや嫌がらせ、ヘイトスピーチなどのコミュニティ規定違反で削除された決定に異議申し立てする機会を提供。コンテンツが誤って削除されたと判断された場合、削除されたコンテンツは復元される。		Google のサービス全体で、Google の利用規約やサービス固有の追加規約またはポリシーに違反していると思われる、または違反していると報告されたものに対して措置が取られることがある。ユーザーは再審査請求をすることで、その決定に不服を申し立てることが可能。 例えば、YouTube では再審査請求を認めている。動画が削除されたクリエイターには通知が発行され、再審査を請求するための手順が記載されたリンクも提供される。クリエイターが再審査請求を提出すると、その請求は審査担当者に送られたのち、判定が維持または破棄される。この再審査は、動画の削除について最初の判断を行った審査担当者とは異なる担当者によって行われる。クリエイターには、結果を知らせるフォローアップ メールが送られる。 また例えば、Google マップにおいて、自分の投稿の多くが削除された場合や、ローカルガイド プログラムから削除された場合は、このフォームから再審査請求することが可能。	[タイムライン][Openchat][LIVE] ユーザからの異議申し立てがあった場合は、その内容に応じて適宜対応。 [BLOG] [livedoor Blog] モニタリングの削除基準に該当しないものについては、プロバイダ責任制限法に則って対応。	違反者は、Twitterの判断が間違っていると思う場合は、異議を申し立てることが可能。異議申し立ては、Twitterプラットフォームのインターフェースまたはヘルプセンターから行うことが可能。Twitterは異議申し立てを受けても対応が妥当であると判断した場合、アカウントが違反しているポリシーについて説明することにより異議に対応。
4-①	発信者情報開示請求を受けた件数 (i)裁判上の開示請求件数、(ii)裁判外の開示請求件数	【日本の数値】	(i)裁判上の開示請求件数：30件 (ii)裁判外の開示請求件数：55件	回答なし	回答なし	回答なし	(i)裁判上の開示請求件数 6件（Openchat 1件、livedoor Blog 5件） （ⅱ）裁判外の開示請求件数 27件（タイムライン 1件、Openchat 1件、BLOG 1件、livedoor Blog 24件）	回答なし
		【グローバルの数値】		回答なし	回答なし	回答なし		回答なし
		【（質問に答えられない場合）参考となる数値】		回答なし	回答なし	透明性レポートでは、その目的に沿って裁判所を含む政府機関（民事訴訟を除く）におけるユーザー情報の開示についてのデータのみ提供。 日本におけるユーザー情報の開示リクエストは合計241件、アカウント数は464件、なんらかの情報の開示に至ったリクエストの割合は87%（2019年7月～2019年12月）。		回答なし
4-②	開示を行った件数 (i)裁判上の開示件数、(ii)裁判外の開示件数	【日本の数値】	(i)裁判上の開示件数：13件（うち一部開示が4件） (ii)裁判外の開示件数：5件（うち一部開示が4件）	回答なし	回答なし	回答なし	(i)裁判上の開示件数 5件（Openchat 1件、livedoor Blog 4件） （ⅱ）裁判外の開示件数 6件（BLOG 1件、livedoor Blog 5件）	回答なし
		【グローバルの数値】		回答なし	回答なし	回答なし		回答なし
		【（質問に答えられない場合）参考となる数値】		回答なし	回答なし	刑事（民事は含まない）87%		回答なし

社名			ヤフー株式会社	Facebook Japan株式会社		Google合同会社	LINE株式会社	Twitter Japan株式会社
5-②	その他の対策（警告表示・ミュート機能等）		■知恵袋 ・不適切投稿の非表示ルールについて 「利用規約」や「利用のルール」に書かれている禁止事項に該当する回答は、専門的なパトロールチームによる投稿の削除のみならず、アダルトや低品質な投稿については、不適切な投稿として機械的に判定し、質問詳細ページで非表示となる仕様が存する。 また、当該投稿については、知恵袋Topページの新着一覧やランキングにおける非掲出も実施。 ・いたずらや中傷などの不快な投稿を繰り返す利用者をブラックリストに登録可能。 ■ニュースコメント 特定のユーザーのコメントを閲覧したくない場合には、ユーザー単位で非表示に設定することが可能。また、記事を読む際、コメント自体を表示させたくない場合には、コメント欄を非表示に設定することも可能。 ■ファイナンス掲示板 不快な投稿を繰り返すなど、特定の利用者の投稿を見たくない場合は無視リストに登録すると、非表示にすることが可能。	(1)自分のプロフィールや投稿を誰が見たり共有したりできるかを細かく設定できる機能。 (2)コメントの非表示・削除機能。 (3)利用者をブロックする機能。 (4)利用者は、公開したくない写真が無断で共有されている場合、報告が可能。 Facebook上のプロフィール、ページ、グループ、投稿、コメント、その他のコンテンツを簡単に報告可能。また、専門家や利用者からのフィードバックに基づいて、プラットフォーム上での嫌がらせを防止するために、他の業界をリードするツールにも投資。 ・ブロックした人が新しいアカウントを作成したり、自分が管理している別のアカウントから連絡を取ろうとしたりしたときに、友達リクエストやメッセージなどの望まないやり取りを自動で検知し、防止することが可能。 ・送信者をブロックすることなく、Messenger に届いたメッセージを見ることがないように、自動的に受信トレイの外に移動するオプションを提供。 ・Facebook ページ上の不適切な言葉や任意の単語をブロックするフィルタを提供。 ・ページやグループの管理者にアカウントを禁止したり削除したりする機能を提供。 ・誰がFacebook Liveにコメントできるかを制御するオプションを提供。	一度に交流したくない複数の人をブロックしたり、ポジティブなコメントをトップにピン留めしてポジティブな交流を促したり、タグ付けや投稿へのコメント、メッセージを許可する人を選択可能。 「制限」機能により、あなたのアカウントを不要なやりとりから保護し、フォロワーがこれらを見ないように保護することが可能。 特定の人をブロックしたり、特定の人からのコメントをブロックすることが可能。	例えば YouTube 上では、コミュニティガイドライン違反に近いものの実際には違反していないため、削除されない場合がある（＝「ボーダーラインのコンテンツ」）。こうしたコンテンツは、米国のYouTubeで視聴されているコンテンツの1%にも満たない数。YouTube のおすすめ機能において、ボーダーライン上のコンテンツと有害な誤情報に関しても、ユーザーの 目に触れる機会をできるだけ減らす取り組みを実施。	・LINEでは友だちをブロックすることができるため、誹謗中傷を投げかける友だちがいた場合、それ以降のメッセージを受け取らない設定が可能。 ・見知らぬ人との出会いが思いがけぬトラブルに発展することがあることから、18歳未満はLINE ID検索ができないよう、機能制限が設けている。 ・LINEでは、文部科学省や長野県、大津市などといった行政府と協力していじめを始めとする子ども向けの悩み相談窓口を用意。 ・誹謗中傷やデマなどの有害コンテンツ有害コンテンツへの対応方針を発表し、パブリックコメントを募集（2020年8月3日～同月31日）し、その結果を公表。 ・一般財団法人全国SNSカウンセリング協議会、一般社団法人全国心理業連合会と連携し、インターネット上の誹謗中傷による精神的ダメージを受けた方を対象とした無料のLINE相談窓口「SNS誹謗中傷等の心のケア相談」を開設。 ・ガイドライン違反の可能性があるテキストを投稿する前に、ユーザに対して警告を通知する機能の開発を進めている。2021年上半期にタイムラインに実装し、2021年下半期 にOpenchat等の他サービスへ実装する予定。	・ミュート：他のアカウントをミュートすると、そのアカウントのツイートはタイムラインに表示されなくなる。また、見たくない特定のキーワードやハッシュタグを設定することでタイムラインに表示されなくなる。 ・ブロック：アカウントをブロックすると、そのアカウントとのやり取りを制限可能。かかわりたくないアカウントとの やり取りを避けるために効果的。 ・ツイートの公開または非公開設定：ツイートを非公開にすると、ツイートがフォロワーだけに表示され、他の人は見られなくなりる。ツイートを非公開にすることで、Twitterをより安全に活用可能。 ・通知フィルター：受け取る通知をフィルタリングすることで、管理をさらに強化可能。クオリティフィルター、ミュート、詳細フィルターを使ってフィルタリングが可能。 ・セーフサーチ：初期設定でセンシティブな内容が含まれている可能性があるツイートや、ブロックまたはミュートされているアカウントからのツイートを検索結果のページから除外。 ・センシティブなメディア：Twitterの初期設定では、センシティブな内容が含まれている可能性があるメディアには警告文が表示。設定で調整することが可能。 ・自分のツイートに返信ができる範囲を選択：ツイートする前に、1）全員が返信（Twitterでのデフォルト設定）、2）フォローしている人だけが返信、または、3）@アカウントで指定した人だけが返信、といった3つの選択肢から選択可能。
5-③	取組の効果分析		各種取り組みの効果分析を行いながら対策の改善を検討している。 外部へ公開している事例については、以下のリンクを参照。 ■ニュースコメント Yahoo!ニュースにおけるAIを活用した投稿時注意メッセージの掲出効果について （参照）https://about.yahoo.co.jp/pr/release/2021/02/16a/ （以下、抜粋） 不適切なコメントを繰り返し投稿するアカウントが13.5%減少 ヤフー株式会社が提供する日本最大級のインターネットニュース配信サービス「Yahoo!ニュース」が、2020年7月からAIを活用して取り組んでいる投稿時の注意メッセージ掲出の効果により、「Yahoo!ニュース コメント」（以下、コメント欄）に不適切なコメント を繰り返し投稿しているアカウントが、掲出直後と比較して13.5%減少しました。	四半期ごとにコミュニティ規定施行レポート(CSER)を発行し、ポリシーに違反するコンテンツの防止と対策の詳細を記載。 前回のCSER（2021年2月）によると、2020年10月から12月までの期間に、いじめや嫌がらせのポリシーに違反していたFacebook上の630万件のコンテンツに対して対策を講じた。 また、ヘイトスピーチのコンテンツに関しては、Facebook上の2,690万件のコンテンツに対処した。そのうち97.1%は利用者が報告を行う前に検出。これは、ヘイトスピーチの文脈に大きく依存する性質を考えると、長年の課題となっていたヘイトスピーチ対策の取り組みを大幅に改善したもの。2年前には340万件のヘイトスピーチコンテンツを削除したが、そのうち60.7%がAIを介して利用者が報告を行う前に識別された。	四半期ごとにコミュニティ規定施行レポートを発行し、ポリシーに違反するコンテンツの防止と対策の詳細を記載。 前回のCSER（2020年11月）によると、2020年10月から12月までの期間に、いじめや嫌がらせに関するポリシーに違反したInstagram上のコンテンツ500万件に対して対策を講じた。ヘイトスピーチのコンテンツに関しては、660万件に対して対策を講じた。そのうち95.1%は利用者が報告を行う前に検出。これは、ヘイトスピーチの文脈に大きく依存する性質を考えると、長年の課題となっていたヘイトスピーチ対策の取り組みを大幅に改善したもの。2年前には65万件のヘイトスピーチコンテンツを削除しましたが、そのうち44.6%がAIを介してユーザーが報告を行う前に識別された。	YouTube上のボーダーライン上のコンテンツなどが、登録をしていないチャンネルからおすすめされて視聴する動画の再生時間を70%削減（米国）。 2017年6月にYouTube上の過激なコンテンツを検出するために機械学習技術を導入。より正確に悪質なコンテンツを分類できる機械を訓練するために、200万本以上のコンテンツをレビュー。自動化されたフラグシステムの品質と有効性を継続的に向上させるための取り組みを下記の通り進めてきた。 ● 2017年第1四半期には、暴力的過激主義ポリシーに違反して削除された動画の8%は、削除時の再生回数が10回未満。 ● 2018年第1四半期には、この数字は50%以上に達した。 ● 2019年第4四半期には、暴力的過激主義ポリシーに違反したとして削除されたアップロードされた動画の 約90%が、再生回数が10回に満たないうちに削除された。 ● 2020年第４半期には、ハラスメントや嫌がらせなどのその他のコミュニティガイドライン違反も含む全体でYouTubeは9億件以上のコメントを削除した。削除されたコメントの99.6%が自動的に検出された。	・長野県　いじめ・自殺相談では、2017年9月10日から23日だけで、長野県内の中高 生390人から計547件の相談が寄せられ、前年度１年間の電話相談259件を大きく上回った。 ・文部科学省「SNS等を活用した相談体制の構築事業」では、都道府県19、指定都市8、市町村3の合計30自治体で、11,039件の相談が寄せられた。 ・「SNS誹謗中傷等の心のケア相談」では、告知を開始した2020年8月4日から相談終了 の同月19 日までの14日間で、164件の相談があった。	・フォローしていないアカウントからの攻撃的な行為による報告は16%減少。 ・新たにアプリ内で異議申し立てが可能になったことにより、対応時間がこれまでより60%減少。 ・報告を受領後24時間以内に凍結した悪質なアカウントの件数が、前年同期比で約3倍に増加。 ・簡単で新しくなった報告プロセスによって、2.5倍以上の個人情報を削除。（2019年4月時点）
6-③	透明性レポートの公開		有識者会議における提言書に基づき、2020年度の透明性レポートを本年夏頃を目処に作成予定。	コミュニティ規定施行レポートを日本語に翻訳し公表。 https://about.fb.com/ja/news/2020/08/community-standards-enforcement-report-aug-2020/。 https://about.fb.com/ja/news/2020/11/community-standards-enforcement-report-nov-2020/	コミュニティ規定施行レポートを日本語に翻訳し公表。 https://about.fb.com/ja/news/2020/08/community-standards-enforcement-report-aug-2020/。 https://about.fb.com/ja/news/2020/11/community-standards-enforcement-report-nov-2020/	日本語で公開 https://transparencyreport.google.com/?hl=ja	LINE Transparency Report （https://linecorp.com/ja/security/transparency/top)にて以下を公開： ・違反投稿への対応：当社におけるコンテンツモニタリングの仕組みと対応実績のレポート（全世界対象） ・ユーザからの削除申告への対応：名誉毀損やプライバシー侵害について当社が受領した削除申告の対応実績レポート（日本のみ対象） なお、本レポートは日本語で公開。	・2012年7月以来、年2回更新される「Twitter透明性センター」（https://transparency.twitter.com/ja.html）を通じて、Twitterに寄せられる法的請求、知的財産に関する異議申し立て、Twitterルールに基づく強制的対応、プラットフォームの操作の状況等を公表。 ・日本語訳も提供。最新版（2020年上半期）は2021年2月現在翻訳作業中。

フェイクニュースや偽情報等への対策状況　ヒアリングシート（2021年３月30日）回答における主な項目の比較

※総務省において要約したもの。詳細は各社の回答原本を参照。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
1．前提（サービス概要）						
1-①	対象サービス名 サービス分類		(i)コンテンツ共有サービス：Yahoo!知恵袋、Yahoo!ニュース（コメント機能） (ii)ニュース配信サービス：Yahoo!ニュース (iii)検索サービス：Yahoo!検索（ウェブ検索）	コンテンツ共有サービス：Facebook	動画共有サイト：YouTube 検索エンジン: Google 検索 広告：Google広告	コンテンツ共有サービス：Twitter
1-②	加入者数、月間アクティブユーザ数又は書き込み数	【日本の数値】		月間アクティブアカウント数：2,600万人（2019年7月）		
		【グローバルの数値】		月間アクティブアカウント数：28億人（2020年6月）	YouTube: 毎月20億人以上のログインユーザー、毎日10億時間以上の動画を視聴 Google 検索: 毎年、Google 検索では何兆回もの検索が行われている	
		【（質問に答えられない場合）参考となる数値】	YahooJAPAN全体の月間アクティブユーザー スマートフォン：6800万UU、PC：2100万UU			収益化可能な日時平均アクティブユーザー数（mDAU）：1億9,200万（2020年第4四半期；グローバル）
2．「我が国における実態の把握」関係						
2-①	偽情報等の発生・拡散状況を把握できる体制 分析・調査の有無		(i) Yahoo!知恵袋 パトロール部隊による違反投稿の監視などを通じて、偽情報の検知、調査、対応の検討を実施。 (ii) Yahoo!ニュース ・ニュース部門、政策企画部門、リスクマネジメント部門など部署間連携によるフェイクニュース対策PJを組成 ・海外でのフェイクニュース事例・諸問題など外部シンクタンクの協力を得て分析調査を実施		脅威分析グループ（Thread Analysis Group/TAG）をはじめとする当社の専門家チームが、監視、分析評価し、行動計画を策定。ポリシーの開発および施行を行うチームにインサイトとインテリジェンスを提供することで、悪質な行為を行う者たちを先回りして対策を講じることが可能。 また、各国で見られた新たな問題やトレンドをグローバルチームに随時共有し、グローバルに実施するポリシー開発や対策に活用。 日本は世界でも早くからYouTube が広く活用された国であり、多くのユーザー、クリエイターの方がいるため、日本で見られたトレンドがグローバルのオペレーション改善の参考になることは実際に多々ある	
2-②	日本における偽情報等の発生・拡散状況、結果公表	【①社会的混乱関係（災害等）】			◯透明性レポート 透明性レポートでは、政府からのコンテンツ削除リクエストを国別に見ることが可能。また、コンテンツ削除リクエストの理由も開示。リクエストの理由には、不正行為、なりすまし、プライバシーとセキュリティ等が含まれる。 ◯Ads Safety Report Google はAds Safety Report（英語）を毎年公開。本レポートでは、Google の広告プラットフォーム上での悪意ある利用を防止する取り組みをまとめている。広告エコシステムにおけるポリシー違反防止対策の透明化は、私たちの長年の優先事項であり、特に今年はこれまで以上に多くのデータを公開している。（レポートでは、グローバルのデータを公開。） レポートでは、奇跡的な治療薬や供給不足のN95 マスク、最近では偽装ワクチンといった新型コロナウイルス感染症に関連する虚偽の広告を9,900 万件以上ブロックしたことなどを公開。	
		【②健康・医療関係（コロナ関係等）】				
		【③選挙・政治関係（米国大統領選等）】				
		【④全般・その他】	(i) Yahoo!知恵袋 ①の調査結果は内部限りのものとし、外部への公表はない (ii) Yahoo!ニュース ヤフーが提供する情報は信頼性の高い既存メディアと契約の上で掲載しているため、偽情報等の発生・拡散は行われていない。弊社がニュートピックスなどにおいて間違った情報を掲載した場合は、適宜お詫び・訂正を公表			
2-③	研究者への情報提供、利用条件		(i) Yahoo!知恵袋 投稿者のYahoo! JAPAN IDを暗号化するなど、個人を特定することができない情報に処理したうえで投稿内容、投稿日時などの投稿に関する情報を大学、独立行政法人など研究機関へ無償提供 (ii) Yahoo!ニュース 偽情報の調査分析における情報提供について実施した実績はない。仮にご要望がある場合は、内容等を精査した上で都度、当該事業部・サービスで判断			無償の学術研究プロダクトトラックを提供。新しい学術研究プロダクトトラックにより、許可された研究者は過去にリリースされたすべてのバージョン2のエンドポイントへのアクセスと、以下のことが可能。 ・フルアーカイブサーチエンドポイントを介したオープンな会話のすべての履歴への無償アクセス ・Twitter開発者プラットフォームへのより高レベルの無償アクセス。月次のツイートボリュームの大幅なキャパシティ1,000万件（Standard APIで現在利用できる量の20倍）。 ・すべてのバージョン2エンドポイントを対象とした、よりきめ細やかなフィルタリング機能。 データ収集の対象を研究テーマに限定し、データクリーニング要件を最小限に。 ・研究の成功を最大化する、新しい技術的および方法論的ガイド。
3．「多様なステークホルダーによる協力関係の構築」関係						
3-①	産学官民の協力関係の構築		Zホールディングス株式会社においては、「デジタル時代における民主主義を考える有識者会議」を開催し、デジタルプラットフォームが民主主義に及ぼす影響やデジタルプラットフォーム事業者に期待される役割等について、フェイクニュースなどの例をもとに検討を進める有識者会議を開催。 構成員として、マスメディアの方から学者まで、幅広い分野の専門家を招いて検討を実施。 (ii) Yahoo!ニュース 一般社団法人セーファーインターネット協会主催の「Disinformation対策フォーラム」へ参加し、有効な対策について多様なプレイヤーと議論を実施。 フォーラムを通じて、プラットフォームサービスとして、弊社が行っている対策やノウハウなどを共有。サービス運営において、パートナーメディアや専門家との連携を深化。 ZHDグループであるLINE社ニュースサービスとの間で、Disinformationに関する情報共有や対策協議を目的とした合同会議を設置。	ここ数年、人々がプラットフォーム上で遭遇するネガティブな体験の影響を最小限に抑えるために、人材と技術への投資を増加。 ソーシャルメディアやソーシャルテクノロジーのプラットフォーム上における誤情報、分断・両極化、情報の質及び紛争に関する課題についての理解を深めることを目的とした研究提案に対して、総額200万ドルの資金を提供。 https://research.fb.com/blog/2020/08/announcing-the-winners-of-facebooks-request-for-proposals-on-misinformation-and-polarization/	＜日本での取組＞ 多様な情報源に基づく影響力のあるジャーナリズムは、社会にとって極めて重要であり、また、Google のミッションの核となるものであるため、Google では、ジャーナリスト向けのデジタルスキル習得にフォーカスした世界的なトレーニングプログラムを提供し、偽情報と戦うための業界団体と連携し、メディアリテラシープログラムに貢献し、より多様で包摂的なニュースエコシステムを支援するためのプログラムを実施。 例えば、Google は新型コロナウイルス感染症の世界的な拡大に対応し報道機関を支援する目的で、ジャーナリズム緊急救援基金（Journalism Emergency Relief Fund）を通じて助成金を提供。この活動を通じて、日本においては全国 28 の報道機関に経済的な支援を提供。 ・Disinformation 対策フォーラム Google は、総務省「プラットフォームサービスに関する研究会最終報告書」に基づき2020 年 6 月に設立されたDisifnformation 対策フォーラムのメンバー。Google は、フォーラムの第3回会合において、Google 及びYouTube における偽情報対策を紹介。今後もフォーラムでの議論に積極的に参加していく予定。 ・研究 Google は、国際大学GLOCOM の研究プロジェクトInnovation Nippon を支援。Innovation Nipponでは、2019年以降、日本におけるフェイクニュースの実態と対処策について研究を実施。 研究成果は、Disinformation 対策フォーラムやオンラインシンポジウム「情報社会の言論環境を考える～ フェイクニュース、誹謗中傷とどう向き合うか～」等でも紹介され、より活発な議論、研究、政策分析に貢献。 ・対話 Google は有識者との公式、非公式を問わず意見交換に積極的に参加し、製品やコンテンツモデレーションに関する情報提供を実施。直近では、マスコミ倫理懇談会全国協議会ともこの問題に関する意見交換を実施し、業界をリードする有識者との意見交換にも力を入れている。	Disinformation対策フォーラム（https://www.saferinternet.or.jp/anti-disinformation）に構成員として参加。

参考4

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
4.「プラットフォーム事業者による適切な対応及び透明性・アカウンタビリティの確保」関係						
（1）偽情報等に関するポリシー						
4(1)-①	(i)禁止行為	【①社会的混乱関係（災害等）】		コミュニティ規定「暴力と扇動」: 「Facebookでは、Facebookのコンテンツに関連して起こりうるオフラインでの危害を防止するための取り組みを行っています。人は不満や他人との意見の相違を示すため、実行するつもりのない暴力の脅しや呼びかけを、深く考えずに行うことがあります。Facebookは、深刻な暴力行為を煽ったり、促したりする発言を削除します。人身に実際の危害を及ぼす、または公共の安全を直接脅かすおそれがあると思われる場合には、Facebookはコンテンツを削除し、アカウントを停止し、法執行機関に協力します。気軽な発言と、公共または個人の安全を実際に脅かすおそれがあると思われるコンテンツとを区別するために、Facebookでは言葉や文脈について考慮するように努めています。また、起こりうる脅威かどうかを判断する際に、Facebookは対象の個人の知名度や身の危険が及ぶリスクなどの追加情報を考慮することもあります。」	【④全般・その他】と同様	暴言や脅迫、差別的言動に対するTwitterのポリシー: Twitterでは、法的または社会的に守られるべき特定のカテゴリーに属する人々について、恐怖心を扇動したり、危険または非合法な活動に参加する傾向が強いと主張することを禁止。 特に社会的混乱の最中、例えば災害の直後などは、同様の主張は特定のカテゴリーに属する人々の深刻な身体的危害に繋がりかねないことを考慮し、Twitter 上で広めることは認められていない。
		【②健康・医療関係（コロナ関係等）】		コミュニティ規定 「世界中の人々が、前例のない公衆衛生上の緊急事態に直 面しています。このためFacebookでは、コミュニティ規定で、新型コロナウイルス感染症に関連した有害なコンテンツや新たな不正利用から利用者を守れるようにしたいと考えています。弊社は、現実世界での危害が生じるリスクを助長するコンテンツを削除するように取り組んでいます。例えば、危害を加えるための計画、医療用マスクと関連商品の販売、ヘイトスピーチ、いじめや嫌がらせ、差し迫った暴力または身体的危害のリスクにつながる偽情報を禁止するポリシーを設け、それに沿って対応しています。」	○YouTube 深刻な身体的危害や死亡のおそれがある危険行為または違法行為の助長を目的としたコンテンツ（一部の医療に関する偽情報を含む）を禁止。COVID-19（新型コロナウイルス感染症）の状況の進展に伴い、Google は、Google のポリシーの定義や執行が、深刻な被害をもたらす重大リスクのあるポリシー違反動画の削除に有効であることを確保するため、国際機関及び各国保健当局と緊密に連携。こうした取り組みを通じ、Google は、新型コロナウイルス感染症の医学的に誤った情報に関するポリシーを策定。 例えば、このポリシーは、新型コロナウイルスの存在を否定するコンテンツや、医療機関で治療を受ける代わりに家庭療法をすすめるコンテンツを禁止。また、新型コロナウイルス感染症の感染防止を目的とした社会的距離の確保または自己隔離措置に関する地域の公衆衛生当局や WHO のガイダンスの有効性に異議を唱えるコンテンツを禁止。 2020 年 10 月 14 日には、新型コロナウイルス感染症ワクチンに関して、地域の公衆衛生当局またはWHO の専門家間で広く合意されている内容と矛盾する主張を対象に追加。例えば、承認されたCOVID-19 ワクチンが死亡を引き起こすと主張するコンテンツを削除。 ○検索 新型コロナウイルス感染症に関する検索においては、医学的なトピックに関するポリシーをナレッジパネルで表示する情報に適用。医学的なトピックに関する情報を Google 検索 の対象にする際、Google は医学界の統一見解とエビデンスに基づくベスト プラクティスが反映された情報を質の高い情報とみなし、そうした情報をナレッジパネルで表示するよう努めている。そのため、検索対象となった情報が医学界の一般的な統一見解に反するものであるときは、Google はそうした情報を訂正または検索結果から除外する権利を有する。 ○Google Play 自然災害、残虐行為、健康危機、紛争、死、その他の悲劇的な事象に対する妥当な配慮を欠く、またはそのような事象を利用するアプリを禁止。Google のポリシーでは、従来から、誤解を招く又は潜在的に有害な健康に関係するコンテンツや機能を厳しく禁止してきており、これには新型コロナ感染症を含む。これらのポリシーに違反するアプリは削除。 ○Googleマップ 新型コロナウイルス感染症の防止、感染拡大、治療、ある特定の場所で個人が新型コロナウイルス感染症に感染したという主張等に関する偽情報を禁止し、これらに該当するコンテンツは削除。	COVID-19について誤解を招く情報に関するポリシー: Twitterのサービスを使って、損害をもたらす可能性のある、COVID-19についての誤った情報や誤解を招く情報を共有することは禁止。
		【③選挙・政治関係（米国大統領選等）】		コミュニティ規定「危害を加えるための計画および犯罪の宣伝」: 「オフラインでの危害と模倣行為を防止および阻止するため、Facebookでは、人、ビジネス、財産、動物を対象とする特定の犯罪行為や有害行為について、これらを助長、計画、宣伝すること、またはそのような行為を告白することを禁止しています。 （例） ・投票者または国勢調査への干渉 ・投票や有権者登録、国勢調査への参加に関する日付、場所、時間、方法に関する不実表示 ・投票できる人物、投票資格、投票の有効性、投票するために提供しなければならない情報や書類に関する不実表示 ・国勢調査への参加資格や、国勢調査へ参加するために提供しなければならない情報 や書類に関する不実表示 米国移民関税執行局(ICE)が投票所に待機していると主張しているコンテンツ ・投票プロセスに参加すると新型コロナウイルス感染症(または別の伝染病)に感染するとする明確な主張」	○広告 2018 年の米国大統領中間選挙以降、米国において選挙関係広告の購入者に対して追加的な認証を求めるとともに、広告主が米国市民又は合法永住者であることを確認することを求めている。	市民活動の阻害に関するポリシー: 選挙やその他の市民活動の操作や妨害を目的としてTwitterのサービスを利用することを禁止。市民活動への参加を抑圧するようなコンテンツや、市民活動に関する日時、場所、方法について誤解を招くコンテンツの投稿や共有が含まる。市民活動について誤った情報や誤解を招く情報が含まれるツイートには、背景情報を提供するために、ラベルを付けたり、拡散を抑制する場合がある。
		【④全般・その他】	(i) Yahoo!知恵袋 プラットフォーム事業者において、どのような情報が虚偽であるか否かを判別することは難しく、殊更「虚偽情報」のみを取り上げて禁止するものではないが、名誉毀損など真実に反する記載により、第三者の権利を侵害する場合には削除措置がなされるほか、総合考慮により、他人を不快にさせる投稿 や、不適切として削除措置がなされる場合がある。 (該当する利用ルール) 禁止事項1：過度な批判、誹謗中傷など他人を攻撃したり、傷つける内容の投稿や、他人を不快にさせる内容の投稿 禁止事項11：その他Yahoo! JAPANが不適切だと判断するもの (ii) Yahoo!ニュース ・Yahoo! JAPAN メディアステートメントでは、以下の通り定めている。 「社会規範や品位を守り、良質で信頼できる情報の提供を目 指します。不正確な情報や、過剰に扇動的な表現、誤解を招く情報を届けることのないよう、真摯に取り組みます。」 ・禁止事項 Yahoo!ニュースでは、契約している媒体社に対して、契約やガイドラインにて、次に該当する内容を含む配信を禁止している。（なお、直接的に偽情報等を禁止するものではない） -正確性に欠ける、名誉毀損等の権利侵害、公 平性に欠ける、利用者に不利益を与えるおそれのある医療・健康情報など。 なお、Yahoo!トップページなど情報掲載面においても、サービスごとに各 種ガイドラインを設けている。また、ニュース以外の各 種サービスが従う医療健康美容に関するガイドラインや、コンテンツ調達に関するガイドラインなどを運用し、掲載場所での情報の信頼性確保に努めている。	コミュニティ規定「フェイクニュース」: 「Facebook上のフェイクニュース（偽ニュース）の拡散防止は、Facebookが責 任を持って真摯に対策を講じている事項の1つです。Facebookはこれがセンシティブで難しい課題であることを認識しています。Facebookでは、人々の間の生産的な議論を妨げることなく、利用者が有益な情報を得ることができる環境を作りたいと考えています。フェイクニュースと風刺や意見との線引きも、また難しい問題です。このような理由により、Facebookではフェイクニュースをなくすのではなく、ニュースフィードでの表示回数を下げることでフェイクニュースの配信を大幅に減らす措置を取っています。」	○Googleニュース コンテンツポリシーにおいて、欺瞞的行為として以下を禁止: ● 他人や組織になりすましたサイトやアカウント ● 自らのオーナーや主な 目的を偽ったり隠したり偽っているサイトやアカウント ● ユーザーに誤解を与えるような偽りの行為や組織的な行為に携わるサイトやアカウント これらの 悪意のある行 為をアルゴリズムで検 知することに加え、Trust ＆Safety チームは、ユーザーからの報告や疑わしいアカウントの活動等に基づき調査を行い、組織的な行為に携わっていると確認されたサイトや関連するサイトに対し、適切な措置を講じる。 ○YouTube コミュニティガイドラインには、偽情報に関連し、直接適用可能ないくつかのポリシーが存在。 例えば、スパム、欺瞞行為、詐欺、なりすまし、ヘイトスピーチ、嫌がらせ等。 スパム、欺瞞行為、詐欺に関するポリシーでは、幾度も投稿されたり、むやみに繰り返したり、あるいは不特定 多数に向けたコンテンツ（ビデオ、コメント、プライベートメッセージ）で、視聴者に約束したものとは別のサイトに誘 導するといった行為 等を禁止 。同様に、視聴回数、高評価、コメントなどYouTube のエンゲージメント指標を販売するコンテンツも禁止。 また、民主的な手続きに対する妨害の扇動、例えば、投票手続きを邪魔したり干 渉したりするような妨害行為を他者に促すコンテンツを禁止。投票日に関する誤った内容のコンテンツはこれに該 当。チャンネルや個人のなりすましも禁止。 例えば、以下のようなコンテンツは禁止。 ● チャンネルの名前と画像は基本的に同じものを用いているが、名前にスペースが挿入されていたり、文字「O」がゼロに置き換えられていたりするところが唯一の違いであるもの。 ● 他人の本名、ユーザー名、画像、ブランド、ロゴ、その 他の個人情報を使用して、本人であるかのように見せかけているもの。 YouTube は、ヘイトスピーチやハラスメントを禁止する明確なポリシーを定 め ている。年齢、障がい、民族、性 同一性や性表現、国 籍、人種等の特性に基づいて個人 や集団に対する暴力や差別を助長するコンテンツは削除。また、本 来備わっている属性に基づいて長期に及ぶ中傷や悪意のある侮辱（人種差別的表現など）を行うコンテンツ、未成 年を辱める、欺く、または侮辱することを目 的にアップロードされたコンテンツを禁止 。	合成または操作されたメディアに関するポリシー: 何らかの損害につながる可 能性が高い、合成または操作されたメディアを、ユーザーを欺くことを意図してプロモーションすることは禁止 。 Twitterでは合 成されたメディアや操作されたメディアが 含まれるツイートをラベル付けし、ユーザーがツイートの信憑性や文脈を把握するのを支援する場合がある。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
4(1)-②	(ii)削除等の対応	【①社会的混乱関係（災害等）】		【①社会的混乱関係（災害等）】 コミュニティ規定に照らして違反する場合には削除等の措置を講じる。	法律に違反している場合と、その製品やサービス上の「ルール」に違反している場合に、コンテンツを削除。	暴言や脅迫、差別的言動に対するTwitterのポリシーに違反した場合： このポリシーの違反に対する処分を判断する際に、Twitterは、その違反の重大さや違反者の過去の違反歴など、さまざまな要因を考慮。 ・違反しているコンテンツの削除を要請し、再びツイートできるようになるまで、一定期間読み取り専用モードで利用するよう求める ・その後の違反については、読み取り専用モード期間が延長され、最終的にはアカウントが永久凍結 ・アカウントの活動が主に攻撃的な行為ばかりである場合、または強烈な身体的脅迫を共有したとみなされる場合、Twitterは最初の調査でアカウントを永久凍結
		【②健康・医療関係（コロナ関係等）】		【②健康・医療関係（コロナ関係等）】 例えば、危害を加えるための計画、医療用マスクと関連商品の販売、ヘイトスピーチ、いじめや嫌がらせ、差し迫った暴力または身体的危害のリスクにつながる偽情報を禁止するポリシーを設け、それに沿って対応。		COVID-19について誤解を招く情報に関するポリシーに違反した場合： COVID-19について誤解を招く情報に関するポリシーへの違反に対する措置は、その違反の程度や種類、違反者の過去の違反歴によって、「ストライク制」を適用して、さらなる強制的対応を適用すべきかどうか判断。 〇ツイートの削除 （1）COVID-19ウイルスの特性または治療に関して誤解を招く情報や、（2）悪意のある勢力や強い権力による意図的な陰謀を思い起こさせるパンデミックやCOVID-19ワクチンなど、このポリシーへの違反の程度が深刻な場合、Twitterは該当するコンテンツを削除するように要請。また、アカウントを一時的にロックしてツイートできないようにする。ツイートの削除は2ストライクとしてカウント。 〇ラベル付け このポリシーに違反するコンテンツを削除しない場合は、Twitter上に表示されているコンテンツを共有するツイートに背景情報を追加。具体的には、以下の措置を実施。 ・当該ツイートにラベルや警告メッセージを適用 ・当該ツイートの共有やいいねを行おうとするユーザーに警告を表示 ・ツイートの拡散を抑制、おすすめから除外 ・いいね、返信、リツイートを無効 ・まとめられたランディングページや関連するTwitterのポリシーなどに、補足説明のためのリンクを表示する 多くの場合、ラベル適用の対象となるツイートに対し、上記すべての措置を適用。Twitter上の誤解を招くコンテンツが大きな注目を集め、公衆に混乱が生じる場合には、優先的にTwitterモーメントを作成。有害と判断され、ラベル付けされたツイートは、1ストライクとしてカウント。 〇アカウントのロックと永久凍結 COVID-19について誤解を招く特定の説（または一連の説）をツイートしたり広めたりするためだけにアカウントが利用されているとTwitterが判断した場合も、凍結の根拠となる。 このポリシーへの違反が重大であったり、違反が繰り返されたりする場合、アカウントを永久に凍結。 このポリシーへの違反が繰り返された場合、その違反によって課された累積ストライク数に応じた強制的対応が取られます。 ・1ストライク: アカウントレベルでの対応なし ・2ストライク: 12時間にわたるアカウントのロック ・3ストライク: 12時間にわたるアカウントのロック ・4ストライク: 7日間にわたるアカウントのロック ・5ストライク以上: 永久凍結
		【④全般・その他】	投稿などの削除、サービスの利用停止、ID削除 (i) Yahoo!知恵袋 ガイドライン違反と判断した場合には、掲載・投稿の制限を行う可能性がある旨を規定。違反投稿が繰り返され、複数回にわたり削除措置がされたアカウントについては、それ以降の投稿ができなくなるよう「投稿停止処置」が行われることがある点についても規定。 (ii) Yahoo!ニュース Yahoo!ニュースでは、以下のとおり、偽情報等が入り込みにくい体制を構築している。 ・契約前の審査記事内容や制作体制などについて審査を行ったうえで媒体社と契約を行なっている（審査の結果、契約に至らない場合も多い）。 ・媒体社には、契約、ガイドラインに従った配信をお願いしており、契約後も適宜、媒体社様の審査を行っている。深刻なガイドライン違反があった場合などについては、契約を終了させていただく場合がある。 ・配信記事について申告をいただいた場合等、記事に問題があるおそれがある場合には、媒体社に確認を行い、必要に応じて修正、削除等の対応を行っていただいている。 (ii)検索サービス フェイクという観点ではなく、当該情報がプライバシー侵害や権利侵害に該当するものに対して削除や非表示措置を実施している。	【④全般・その他】 ・偽情報を広める利用者、ページ、ドメインに対する経済的なインセンティブの提供を断つ ・コミュニティからのフィードバックを含むさまざまなシグナルを利用して、どの記事がフェイクであるかを予測する機械学習モデルに通知する ・独立した第三者ファクトチェッカーによりフェイクと評価されたコンテンツの配信を減らす ・記事の背景を示し、利用者のニュースリテラシーを高めることで、何を読み、信じ、シェアするべきかを利用者自身で決められるようサポートする ・この困難な問題を解決するため、学術団体やその他の団体と協力する		合成または操作されたメディアに関するポリシーに違反した場合： ツイートで共有されているメディアが、ユーザーを欺くことを意図して、大幅に改ざんまたはねつ造されていると判断する根拠がある場合、Twitterは、Twitter上に表示される当該メディアを共有しているツイートに文脈を追加して表示。具体的には、以下の措置を実施。 ・Twitter商品に表示される当該コンテンツにラベルを適用 ・当該コンテンツの共有やいいねを行おうとするユーザーに警告を表示 ・ツイートの拡散を抑制、おすすめから除外 ・Twitterのモーメントやランディングページなどに、補足説明のためのリンクを表示 多くの場合、ラベル付けの対象となるツイートに対し、上記すべての措置が取られる。 合成または操作されていて、ユーザーを欺くことを意図した方法で共有されており、何らかの損害につながる可能性が高いものはTwitter上で共有することが禁止されており、削除の対象となる。当ポリシーの違反を繰り返したアカウントや、当ポリシーに対して重大な違反を行ったアカウントは永久凍結される場合がある。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
(2)削除等の対応						
4(2)-①	偽情報等に関する申告や削除要請の件数	【日本の数値】	「偽情報」という切り口から対応件数をカウントしているサービスはない			
		【グローバルの数値】				
		【(質問に答えられない場合)参考となる数値】				
4(2)-②	(i)偽情報等に関する申告や削除要請に対する削除件数	【日本の数値】	「偽情報」という切り口から対応件数をカウントしているサービスはない			
		【グローバルの数値】				(コンテンツ削除件数:2020年上半期) COVID-19について誤解を招く情報に関するポリシー:4,647 市民活動の阻害に関するポリシー:2,710 (アカウント凍結件数:2020年上半期) COVID-19について誤解を招く情報に関するポリシー:1,751 市民活動の阻害に関するポリシー:0
		【(質問に答えられない場合)参考となる数値】				
4(2)-③	偽情報等に関する主体的な削除件数(AIを用いた自動検知機能の活用等)	【日本の数値】	「偽情報」という切り口から対応件数をカウントしているサービスはない			
		【グローバルの数値】			○広告 2020 年に、Google は新型コロナウイルス感染症関係の広告を2 億7,500 万件以上ブロック又は削除。Ads Safety Report では、多くの関連するデータを開示。 ○YouTube 2020 年2 月から2021 年1 月の間、Google は、850,000 以上の動画を削除。これらの動画は、新型コロナウイルス感染症に関する危険又は誤った情報に関係していた。その96%は,YouTubeの自動フラッグシステムによってフラグされ、視聴回数が 100 回に至る前に削除された。	
		【(質問に答えられない場合)参考となる数値】				
4(2)-④	③についての削除の方法・仕組み(AIを用いた自動検知機能の活用等)			Facebookには、安全とセキュリティに取り組むスタッフが35,000人以上おり、24時間体制で60以上の言語のコンテンツをチェックし、またコミュニティからの報告に対応。 人の目に触れる前にフェイクニュースが拡散するのを抑え、Facebookのポリシーに違反している可能性のあるコンテンツを特定するためのテクノロジーに投資。	Google では、テクノロジーを使用してプラットフォーム上にホストされている問題のあるコンテンツを検出。以前は、ユーザーがコンテンツにフラグを立てる手法に頼っていたが、現在では Google 製品上で削除されるコンテンツの大部分は、テクノロジーによって自動的に識別。 例えばYouTube では、毎分500 時間もの動画が新たに投稿されているため、人間と機械学習を組み合わせて問題のあるコンテンツを大規模に検出。機械学習はパターンの検出に向いており、以前削除したコンテンツに似たコンテンツを視聴される前に見つけ出すことが可能。 ユーザーからのフラグも受け付けているが、有害なコンテンツのほとんどが機械によって一度も視聴されずに削除されている。	コンテンツがポリシーに違反していると担当チームが判断した場合、ツイートにラベルを付与。そのような判断は自動化ツールに反映されるとともに、サービス上の同様のコンテンツを自主的に発見しラベル付けする能力の向上にも利用される。自動化ツールと人間によるレビュー双方を活用し、COVID-19ワクチンについて誤解を招く情報に対処していくことを目指している。機械学習や言語処理の自動化が実行を示すまでには時間がかかるため、まず英語のコンテンツへの対応から開始し、その後他の言語や文化的コンテクストにも拡大させる予定。
4(2)-⑤	削除以外の取組 (i)警告表示			Facebookは、利用者がどのコンテンツを閲覧し、信頼してシェアできるのかを判断するために、より多くの情報を知らせる機能と製品に投資。 2018年、コンテキストボタンでニュースフィードの記事の背景情報を提供することを開始。このボタンにはパブリッシャーについてのウィキペディア記事、Webサイトの年数、Facebookで記事がシェアされた回数やシェアされた場所などが表示される。コミュニティ規定に違反して削除された投稿や、第三者ファクトチェッカーによって「虚偽」、「虚実混交」または「虚偽の見出し」と評価された投稿をページクオリティタブに示すことで、ページの所有者がコンテンツの質を改善することを支援。		ポリシーに違反するコンテンツを削除しない場合は、Twitter上に表示されているコンテンツを共有するツイートに背景情報を追加。具体的には、当該ツイートにラベルや警告メッセージを適用、当該ツイートの共有やいいねを行おうとするユーザーに警告を表示。
	(ii)表示順位の低下			偽情報やクリックベイトなど、問題のあるコンテンツであってもコミュニティ規定の削除基準を満たさないものについて、コンテンツの投稿を許可する一方で、拡散されないように措置。	○Google 検索 膨大な数のウェブページを分類し、ユーザーが探している情報を提供するよう設計されている。特に、噂や誤った情報の拡散が生じやすい文脈(例えば、ニュース速報等)においても、品質や信頼性の高い情報へのアクセスを意味する。それぞれのプロダクトやサービスはそれぞれ異なった運用がなされるが、Google のアルゴリズムはウェブサイトを公平に取り扱うことを確保するという重要な原則を共有。 ● 情報は、ランクアルゴリズムにより整理される。 ● アルゴリズムは、Google のサービスの有用性を確保するために設計されており、その有用性は、アルゴリズムを作成したり監査したりする個人のイデオロギーや見解ではなく、ユーザーテストによって計測される。 全てのスパムが偽情報ということではないが、偽情報を拡散しようとする多くの悪意のある者は、何らかの形のスパムを行っており、その戦略は他のスパムを行う者と類似している。それゆえ、スパムに対するGoogle の対応は、偽情報に対するGoogle の対応と密接に関連している。Google のアルゴリズムはスパムの大半を発見し、自動で降格又は削除することが可能。残りのスパムについては、Google のスパム削除チームが手動で対応。多くの場合ユーザーの報告に基づきページをレビューし、ウェブマスターガイドラインに違反している場合は、フラグを立てる。	ツイートの表示順位を下げたり、「おすすめ」から除外。
	(iii)その他の取組内容			フェイクニュースの拡散抑制の方法として、偽アカウントを削除したり、偽情報を発信する個人やページの経済的誘因を取り除いている。コミュニティからのフィードバックなどのシグナルを利用して、虚偽の可能性がある記事を特定。 Facebookが独立した第三者ファクトチェッカーと連携している国では、ファクトチェッカーが虚偽と評価した記事はニュースフィードの下のほうに表示される。 繰り返し偽情報を作成またはシェアするページやドメインに対しては、そこからのコンテンツ配信を大幅に削減したり、広告を出せなくしている。	○ YouTube コミュニティ ガイドライン違反に近いものの実際には違反していないため、削除される「ボーダーラインのコンテンツ」は、米国のYouTubeで視聴されているコンテンツの1%にも満たない数だが、YouTube ではそのようなボーダーライン上のコンテンツと有害な誤情報に関しても、ユーザーの目に触れる機会をできるだけ減らす取り組みを実施。	いいね、返信、リツイートを無効にしたり、まとめられたランディングページや関連するTwitterのポリシーなどに、補足説明のためのリンクを表示。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
（4）透明性・アカウンタビリティの確保						
4(4)-③	取組の効果分析				〇YouTube ボーダーライン上のコンテンツなどが、登録をしていないチャンネルからおすすめされて視聴する動画の再生時間を70% 削減（米国）することに成功。この様なシステムの拡充を進めていく中で、他の地域へのインパクトについても、より多くの情報を共有できるようにしていきたいと考えている。 2017 年6 月にYouTube 上の過激なコンテンツを検出するために機械学習技術を導入。より正確に悪質なコンテンツを分類できる機械を訓練するために、私たちのチームは200 万本以上のコンテンツをレビュー。自動化されたフラグシステムの品質と有効性を継続的に向上させるために取り組んでいる。 ● 2017 年第1 四半期には、暴力的過激主義ポリシーに違反して削除された動画の8% は、削除時の再生回数が 10 回未満。 ● 2018 年第 1 四半期には、この数字は 50% 以上に達した。 ● 2019 年第4 四半期には、暴力的過激主義ポリシーに違反したとして削除されたアップロードされた動画の約 90% が、再生回数が 10 回に満たないうちに削除された。 ● 2020 年第4 半期には、ハラスメントや嫌がらせなどのその他のコミュニティガイドライン違反も含む全体でYouTube は9 億件以上のコメントを削除。削除されたコメントの99.6% が自動的に検出された。	
＜5.「利用者情報を活用した情報配信への対応」関係＞						
5-①	広告表示先の制限		「①社会的混乱関係（災害等）」 「②健康・医療関係（コロナ関係等）」 「③選挙・政治関係（米国大統領選等）」 Yahoo! JAPAN広告配信ガイドラインにおいて、広告の配信先は、メディアとしての知名度・実績があることと、広告配信先サイト内の情報に信頼性があることを条件としており、偽情報等のあるようなサイトへの配信はお断りしている。		広告主とパブリッシャーのためのポリシーを設けており、これらのポリシーは、私たちの広告プラットフォームでの偽情報への対応において主要な手段となっている。 ● 悪意のある行為を行う者への対策：ポリシーを回避しようとする行為を検知し対応 ● ユーザーにコンテクストを与える：「広告の表示について」という機能を通じ、ユーザーはその広告が表示された理由を理解し、表示されるパーソナライズド広告の設定を変更したり、パーソナライズされた広告を完全にオプトアウトしたり、自分の興味関心を変更する方法を確認し簡単に変更することが可能。 Google の広告プラットフォームにおける偽情報への対応に関するポリシーでは、政治や時事問題に関する内容の正確性の判断は避け、広告主やパブリッシャーによる誤った表現や有害な行動に焦点を当てるアプローチを採用。偽情報キャンペーンに関連する多くの行為を含む、悪質な行為を摘発するためのいくつかのポリシーを策定。 また、コンテンツを「偽情報」として特別に分類をしていないが、Google のプラットフォーム上での詐欺的または低品質のコンテンツを防止することを目的に、長年にわたり多数のコンテンツポリシーを策定。これらのポリシーは、欺瞞的なコンテンツに対応するための行動的アプローチを反映。具体的な主張の真意を判断するのではなく、誤った表現や有害なコンテンツに関連する広告主 やパブリッシャーの行為に対してポリシーを適用。 Google では、各プロダクトごとにパブリッシャーポリシーを策定。例えば、「危険または中傷的なコンテンツ」、「虚偽のコンテンツ」というポリシーのもと、パブリッシャーは次のトピックを収益化不可。新型コロナウイルス感染症に関連する偽情報もこれに該当し、国民に有害な影響を与える可能性のある偽情報は「危険または中傷的なコンテンツ」として収益化されるべきではない。 Googleは、「偽情報」ポリシーを定める代わりに、「偽情報」を細分化し、個別の問題についてよりきめ細かいポリシーを適用。	誤解を招く情報のラベルがついたコンテンツは、Amplifyパブリッシャープログラムにより自動的に収益化を無効化。また、不適切なコンテンツのポリシーのもと、広告として配信不可。
5-②	広告出稿制限		Yahoo! JAPAN 広告掲載基準において、下記の様に規定している。 「①社会的混乱関係（災害等）」 事実と異なる内容の広告は掲載をお断りしている。 「②健康・医療関係（コロナ関係 等）」 薬機法等の広告規制に基づき、虚偽広告は掲載をお断りしている。 「③選挙・政治関係（米国大統領選等）」 選挙および政治に関する広告は、選挙管理委員会や政党、政治団体による広告のみ掲載を認めています。その他の団体や個人による政治に関する広告は、虚偽か否かに関わらず掲載をお断りしている。	広告ポリシー： 「Facebookでは、サードパーティファクトチェッカーによって虚偽であると証明された主張、また場合によっては特定の専門性を持つ組織によって虚偽であると証明された主張を含む広告を禁止しています。虚偽と判断された情報を繰り返し投稿する広告主は、Facebookでの広告掲載に制限がかけられる可能性があります。」	Google のスタンスは、いわゆる「偽情報」をより細分化し、個々の悪質な要素に対し、「偽情報」ポリシーではなく、その要素に特化したより細かいポリシーを適用するというもの。例えば、広告主は新型コロナウイルス感染症関連の誤った情報に基づいた広告は禁止。 更に、公衆衛生上の緊急事態など、社会的、文化的、政治的に大きな影響を与えるセンシティブな出来事から利益を得たり、それを悪用する可能性のある広告は禁止。 ユーザーがコロナ禍において、必要な情報にアクセスできるようにするために、一部の組織や機関は関連広告を掲載することが可能。 https://support.google.com/google-ads/answer/9811449 政治に関するコンテンツ：Google では、選挙活動の一部とみなされるウェブサイトを宣伝する広告を日本で表示することを禁止。	〇政治に関するコンテンツ Twitterでは、政治に関するコンテンツを広告に掲載することを全世界で禁止。この決定は、政治に関するメッセージのリーチは購入するものではなく獲得するものであるという信念に基づいている。 Twitterでは、政治に関するコンテンツとは、候補者、政党、選出または任命された政府関係者、選挙、国民投票、住民投票、法律、規制、指令、または裁判に関する結果に言及するコンテンツであると定義。 このポリシーでは、政治に関するコンテンツへの言及を含んだ投票の呼びかけ、財政支援の要請、または、上記の類の政治に関するコンテンツに対する賛成または反対意見などを含む広告を禁止。 また、候補者、政党、選出または任命された政府関係者によるいかなる種類の広告も禁止。 〇不適切なコンテンツ 不適切なコンテンツに関するポリシーは、危険または搾取的なコンテンツ、虚偽なコンテンツ、誤解を招く、合成または操作されたコンテンツを禁止。
5-③	ターゲティング技術の適用に関する規定		偽情報等に関する広告は掲載を認めていないので、ターゲティング技術の適用に関する規定は設けていない。 政治広告については、ターゲティング技術の適用に関する規定を設けていないが、今後何らかの規定を設けるべきかを検討している。 なお、これらの広告に限らず、弊社ではYahoo! JAPAN 広告データ利用基準を定めており、広告における不適切なデータの利用を防止している。	広告ポリシー： 「7. ターゲット設定 1. 利用者を差別、侮辱、挑発、攻撃する目的で、または略奪的な広告活動を行う目的でターゲット設定オプションを使用してはいけません。 2. カスタムオーディエンスを広告のターゲットにする場合は、オーディエンス作成時に利用規約に準拠する必要があります。」	Google のスタンスは、いわゆる「偽情報」をより細分化し、個々の悪質な要素に対し、「偽情報」ポリシーではなく、その要素に特化したより細かいポリシーを適用するというもの。 なお、違反広告には広告ポリシーが適用されるため、違反広告において「ターゲティング技術」というものは該当しない。	Twitter広告には、広告主のコンテンツに関心がありそうな利用者にリーチするためのさまざまなターゲティングオプションが用意されている。タイムラインでのキーワードターゲティングを使用する場合、利用者の信頼を損なわずにキャンペーンの目標を達成することが重要。広告主がタイムラインでのキーワードターゲティングを使用する場合、キーワードターゲティングに関するポリシーおよび他のすべてのTwitter広告ポリシーに従う必要がある。 Twitterはユーザーのプライバシーを尊重しているため、ユーザーはサポートされている端末で、Twitterの興味関心ターゲティングによる広告サービスをオプトアウト可能。
5-④	広告のアルゴリズムに関する透明性・アカウンタビリティ確保方策		広告のアルゴリズムの詳細は開示していないが、政治広告等に限らずターゲティング広告が表示された理由を、広告に付帯しているiアイコンからのリンク先のページで表示している。		違反広告は広告ポリシーで管理されているため、違反広告における「ターゲティング技術」は該当しない。 日本では、Google 広告ポリシーにおいて一般的な政治広告は許可されていますが、選挙広告は禁止。	
5-⑤	出稿者の情報や資金源の公開		広告出稿者の社名・団体名・個人名等および所在地、連絡先を広告サイト内に明示することをYahoo! JAPAN広告掲載基準に規定している。 特に政治広告の資金源の公開については、現状求めていないが、世情に合わせ今後必要があれば検討していきたいと考えている。	広告ライブラリでは、Facebook製品に掲載されている広告を検索することができ、表示された広告に関する情報を確認可能。 社会問題、選挙または政治に関連する広告の場合、アクティブではない広告（すでにFacebook製品に掲載されていない広告）も検索可能。選挙への介入を防ぐためには透明性が重要であるため、広告ライブラリには広告費用の出資者、広告費の金額範囲、広告がリーチした利用者層など広告についての追加情報も表示される。これらの広告は、ライブラリに7年間収録。	● Google 広告ポリシーは、日本での一般的な政治広告を許可しているが、日本における選挙広告を禁止。 ● 2020年には、Googleは、全ての広告主のアイデンティティ及びビジネスに関するより多くの情報を把握するため、新しく広告主認証プログラムを導入。プログラムでは、「この広告について」というメニューにおいて、それぞれの広告の広告主及びその所在を開示。世界で順次導入予定であり、年内にも日本で導入される見込み。 ● 米国を含むいくつかの国では、選挙に関する透明性レポートを公開。	Twitterは2019年11月に政治広告を全面的に禁止。2018年5月24日から2019年11月22日にかけて配信された政治広告と、2018年8月8日から2019年11月22日にかけて配信された社会問題広告については、以前開設していたTwitter広告の透明性センター（ATC）データのアーカイブ版を提供。
5-⑦	その他の透明性・アカウンタビリティ確保方策		広告審査および広告配信先の審査に関する透明性レポートを定期的に公開。実際にお断りした件数や内容の内訳をまとめている。		Google はGoogle、YouTube、その他のGoogle サービスにおける政治広告について極めて高い透明性を確保したいと考えている。 誰もがオンラインで見る広告を理解できるよう、選挙関連の広告主の認証済みの支出に関する情報を含む透明性レポートを公開。（日本では選挙広告が許可されていないため、Google は日本では選挙に関する透明性レポートを提供していない） ● Googeでの政治広告：https://transparencyreport.google.com/political-ads/home?hl=ja ● 広告が表示される理由：https://support.google.com/accounts/answer/1634057 ● 特定の広告のブロック：https://support.google.com/ads/answer/2662922 ● プライバシーヘルプセンター：https://support.google.com/policies/answer/9581826	Twitterの利用者は誰でもTwitter広告をアプリ内またはwebフォームから報告可能。 特定の広告を非表示にしたり、広告主をブロックすることも可能。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
6.「ファクトチェックの推進」関係						
6-①	ファクトチェック結果の表示具体的な仕組み・基準		(ⅰ)コンテンツ共有サービス 多くの一般ユーザーが投稿するCGMサービスにおいては、投稿内容もさまざまであって、真偽の確認も困難であることが多いため、ファクトチェック機能は導入していない。 (ⅱ) Yahoo!ニュース ・Yahoo!ニュースでは、信頼性の高いメディアと契約を締結し、コンテンツを調達・掲載している。また、Yahoo!ニューストピックスにおいては、誤情報・デマに対して正しい情報を積極的に掲載。 (例) トピックスに掲載された主なデマを打消すトピック(コロナ関連) 「バナナ食べると感染 デマ注意」 「新型肺炎めぐる世界のデマ 検証」 「新型コロナ お湯で予防はデマ」 など。 ・Yahoo!トップページを中心に、メディアサービス各所から誘導される「新型コロナ特設サイト」では、コロナ関連のデマへの注意喚起を行うコーナーを設置。 ・ファクトチェック団体FIJと情報共有連携を行い、メディアや専門家の記事を掲載。あわせて消費者庁や国民生活センターへのリンクも設置している。なお、各所への掲載にあたっては編集部が複眼的に確認をした上で掲載。	具体的なステップは下記のとおり: ①フェイクニュースを特定:Facebookの利用者からのフィードバックなどに基づいて偽情報の可能性のあるコンテンツを特定し、ファクトチェッカーに表示。また、ファクトチェッカー自身がコンテンツを特定したうえで審査する場合もある。 ②コンテンツを審査:ファクトチェッカーがコンテンツを審査し、事実を検証したうえでその正確性を評価。Facebook社からは独立して行われ、発信元や公開データを参照したり、動画と画像を認証したりなどの作業が含まれる。 ③偽情報を明確にラベル付けして利用者へ周知: ファクトチェックパートナーに審査されたコンテンツにラベル付けを行い、利用者が追加の背景情報を閲覧可能にする。また、ラベル付けされたコンテンツをシェアしようとする利用者や過去にシェアした利用者に通知。 ④偽情報を目にする利用者の数を抑制: ファクトチェッカーが「虚偽」、「改変」、「一部虚偽」と評価したコンテンツは、ニュースフィードでの表示順位が下がり、Instagramでの発見タブの表示対象から除外され、フィードやストーリーズで目立たないようになる。これにより、フェイクニュースを見る利用者の数を大幅に抑制。また、ファクトチェッカーによって評価されたコンテンツの広告は却下。 ⑤フェイクニュースを繰り返し配信する違反者への措置:「虚偽」または「改変」と評価された偽情報を繰り返し配信するページやウェブサイトに対して、配信数の抑制などの制限措置を実施。また、それらのページやウェブサイトは収益化や広告に関する機能へのアクセスやニュースページとしての登録が一定期間取り消される。 ファクトチェッカーによる評価の種類には、虚偽、改変、一部虚偽、背景の説明不足、風刺、事実があり、最終的にはファクトチェッカーが独自にコンテンツの審査と評価を実施。Facebook社が評価を変更することはない。	○Google 検索及び Google ニュース Google のファクトチェックにおいては、ユーザーに選択肢を与えるアプローチを採用。ファクトチェックのラベルは Google 検索及び Google ニュース結果に表示され、ユーザーがコンテンツのどの部分がポジティブにファクトとしてチェックされているかが確認でき、より詳細を調べたい場合も簡単により情報を探すことが可能。 Googleニュースにはファクトチェックボックスがあり、Google ニュースの新型コロナウイルス感染症用ニュースエクスピリエンスには専用のファクトチェック表示。 ○YouTube YouTubeには同様の仕組みがインド及びインドネシアのユーザーに提供されており、コーパスに関連記事がある場合ファクトチェック情報パネルが画像検索結果のトップに表示。 これらの機能は、第三者パブリッシャーのオープンなネットワークに依存。ファクトチェックはGoogleにより作られたものではなく、Google のサービスが IFCN を含む特定の 1 つのファクトチェックネットワークのみに依存するものでもない。 パブリッシャーのコンテンツがこのようなラベルの対象となるためには、下記のことを行う必要がある。 ● HTML マークアップとして知られるデザインツールを使い、ウェブサイト上の特定のページがファクトチェックであることを示すこと ● Google ニュースパブリッシャー向けファクトチェック基準を満たすこと 一定のアルゴリズム上のしきい値を満たすこと –Google の構造化されたデータガイドライン:"ファクトチェックが表示されることは保証されていません。Google 検索結果にファクトチェック要素を含めるかは構造化された形で決定されています。ファクトチェックの要素は、サイトの構造化されたランキングに基づいて評価されます。ページランキングと同様のプロセスでサイトは評価されます。サイトのランキングが十分高ければ、ファクトチェック要素はページと一緒に検索結果に表示されます。" デジタルやメディア・リテラシープログラムやユーザーだけでなく、ジャーナリスト及び研究者向けトレーニング等の活動を通して、Google はプロダクトを超えて健全なジャーナリズムのエコシステムをサポートし、市民団体や研究者とパートナーシップを組み、将来リスクの一歩先を行く。 しかし、上記記載のように、Google のファクトチェック機能は 1 つのネットワークのみに依存しない。むしろ関連する検索結果ページのファクトチェック作業を向上させ、Google のシステム上のサイトの品質の評価、中立的で公的に明文化されたポリシー及びプロセス(例えば、読者・インターネットユーザーにとって何がファクトチェックの一次情報なのか明確であること、ファクトチェックを行うもの身元、所有権の明確であることを保障すること)の基準を満たす。 Google はこれらのプロセスが公平な方法で、政治的なバイアスなく取り入れられ、実施されるよう特別の注意を払う。	
6-②	ファクトチェックを容易にするツールの開発及び提供				ファクトチェックエクスプローラー及びファクトチェックマークアップの 2 つのツールで構成されるファクトチェックツールを提供。 両方のツールはファクトチェックを行う人、ジャーナリスト及び研究者の仕事を調整することを目指している。例えば、ファクトチェックマークアップの目標は、記事そのものに何も加えず、シンプルなウェブフォームを通してマークアップに提出できるようにすることにより、クレームレビューマークアップを作る過程を容易にすること。 Google は、イメージの由来、偽情報対策のクリティカルなユースケースを確認するオープンソースでモバイル向けに最適化されたStoryful によるSource の発展をサポート。Google Cloud の技術を用いて、事実、言語を認識し、自動翻訳を提供して、Source はイメージの潜在的な履歴の迅速な分析を提供。	
6-③	ファクトチェックを実施する人材の育成					
6-④	ファクトチェック機関との連携		ファクトチェック団体FIJと情報共有連携を行い、メディアや専門家の記事を掲載。あわせて消費者庁や国民生活センターへのリンクも設置している。なお、各所への掲載にあたっては編集部が複眼的に確認をした上で掲載。(再掲) 連携相談や活動内容の共有などの定期的なMTGを実施。	Facebook社では、FacebookとInstagramにおける偽情報の拡散防止に真摯に取り組んでいる。多くの国と地域で、この種のコンテンツの識別、審査および措置の遂行のために、中立的な国際ファクトチェックネットワーク(IFCN)に認定された独立した第三者ファクトチェッカー団体と提携。	Google は、無党派組織で米国、ドイツ、ブラジル、アルゼンチン、南アフリカ、インドその他のファクトチェック組織を束ねる Poynter の国際的ファクトチェックネットワーク(IFCN)と提携。 ＜日本＞ Google はFIJ、InFact 及びBuzzFeed Japan 等に対し、Fact Check Tools の利用方法に関するワークショップを実施。Fact Check Tools にGoogle の定める要件を満たすファクトチェック記事を登録することで、検索結果にファクトチェック記事であることが明記されるようになり、また、ファクトチェック記事だけを網羅するFact Check Explorer にも表示されるようになる。メディアリテラシー教育の現場などで、誤った情報とその検証についての教材としての活用も期待。2021 年3 月、Buzz Feed Japanが、Google Fact Check Tools を使用開始。他メディアも採用を検討中。 YouTube は、ファクトチェックに関するクリエーターワークショップを2019 年11 月21 日に行い、20 のクリエーターが参加しました。Poynter Institution とのパートナーシップにより開催。 Google ニュースラボはジャーナリスト及び大学生に対し、偽情報を認識するスキル、検索の効果的な利用、マップ及びサテライト画像の利用を含む、ジャーナリズムにおけるデジタル技術提供及び活用ワークショップを提供しました。2015 年以来、1 万人以上がトレーニングに参加。	パンデミックの期間中、Twitterではパートナーシップ を構築し、公共の会話を保護し、利用者が信頼性の高い公衆衛生情報を見つけやすくするための取り組みを実施。 利用者が正しい情報源から正しい情報を得られるよう、広告枠の無償提供を実施(ファクトチェック機関に限定されない)。 世界保健機関、多数の政府機関や公共保健機関、世界中の当局者など、各国の関連するステークホルダーとオープンな対話を行っており、それらのステークホルダーがアカウントの問題をトラブルシューティングしたり、所属する専門家の認証を取得したり、損害を軽減するためにTwitterを活用する際に戦略的なアドバイスを求めたりできるようにしている。 これまでに実施してきた #StayHome(#ステイホーム)、#WashHands(#手を洗おう)、#WearAMask(#マスクをしよう)を呼びかける取り組みの成果を踏まえ、2021年1月にはTeam Halo、UNICEF、NHS、Vaccine Confidence Projectと合同でワクチン接種への指示を表明する #vaccinated(#ワクチン完了) 絵文字・ハッシュタグキャンペーンを立ち上げ。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
7.「ICTリテラシー向上の推進」関係						
7-①	普及啓発の取組・投資		FY21において教育現場（大学）において情報リテラシー教育を実施する予定。こうしたリテラシー教育の授業・研究を通じて、啓蒙コンテンツを作成しYahoo!を中心にグループで活用する予定。	アジア太平洋地域の専門家と協力して、いじめ防止やオンラインでの嫌がらせなどのリソースを提供するプログラム「みんなのデジタル教室」を立ち上げ。 日本の中学生・高校生を対象に、フェイクニュースが発信される動機や、情報を受け取る側の視点を考え、フェイクニュースを見分けるための様々なポイントについて、アクティビティを通じて学ぶ授業を展開。 また「みんなのデジタル教室」の授業のエッセンスをInstagram上で体験・学習できるコンテンツ『タグでたどる物語』を展開。専用のInstagramアカウント（@minnano_digital_kyoshitsu_1）を訪れ、物語を読み進めながら、プライバシー保護やフェイクニュースへの対応などについて理解を深めていただくことを目的としている。	Google は、「Google News Initiative」を筆頭に、数多くのメディア・リテラシープログラムを立ち上げ、支援してきた。また、Google.org（Google の慈善事業部門）は、イギリス、ブラジル、カナダ、インドネシアなどですでに支援してきたプログラムを拡充する形で、世界中のメディアリテラシーを支援するための1,000 万ドルのグローバルイニシアチブを 2018 年に立ち上げた。 ◯日本で実施してきた取り組み ● これまでに 10 万人以上の中学生・高校生にオンライン・リテラシー・カリキュラムを提供。このカリキュラムでは、ファクトチェックを含む主要なオンラインリテラシーのトピックを扱っている。 ● Grow with Google という私たちの無料のデジタルスキルトレーニングを提供するプログラムを通じて、ユーザーのインターネットリテラシー教育を強化するために、無料のオンライン講座を提供。家族で実践　安心・安全なインターネット利用のためにできることでは、家族を中心としたユーザーを対象に、情報の正確さを確認するためのヒントを含むオンライントレーニングを提供（あわせて個人で実践編も公開しています。） ● ウェブレンジャーと呼ばれる、10 代の若者にオンラインセーフティのためのプロジェクトを奨励するメディアリテラシープログラムを、2015 年、2016 年、2018 年に実施し、2000 人以上が参加。	・Twitterプラットフォーム上における公式アカウントからの情報提供 ・ヘルプセンターページでの情報や動画等の提供
7-②	他のステークホルダーとの連携・協力・投資		上記情報リテラシー教育において、企業と大学の連携により実施。 実施にあたっては有識者や伝統メディア関係者とも協力・連携していく予定。	上記プログラムでは、日本では特定非営利活動法人企業教育研究会の協力のもと、デジタルリテラシーに関する授業を提供。	◯研究活動 Google は、ニュースエコシステムの中で、リテラシー向上のために活動する多くの機関とパートナーシップを組んでいる。国際大学GLOCOM との共同研究であるInnovation Nippon では、プラットフォームや情報リテラシーに関する様々な研究を長年行ってきた。2019 年と 2020 年には、Innovation Nipponが「日本におけるフェイクニュースの実態と対処策」に関する調査を実施しました。これらの研究結果は、シンポジウムや報告書などで広く公開され、さらなる議論や研究、政策提言につながっている。 ◯トレーニング ● Google は、FIJ、InFact、BuzzFeed Japan に対して、ClaimReview の使い方のワークショップを行い、Google ファクトチェックツールの利用を支援している。 ● Google ニュースラボでは、ジャーナリストや大学生を対象に、デジタル技術をジャーナリズムに活用するためのトレーニングを実施し、誤情報の見分け方、Google 検索の効果的な使い方、Google マップやGoogle Earth の活用などのスキルを身につけてもらった。2015 年以降、10,000 人以上がトレーニングに参加。 またGoogle は有識者や新聞社など様々なステークホルダーと、リテラシー教育の効果やその推進方法について議論している。	・セーファーインターネットデーやその他国際的な記念日に際して、国際機関・各国政府・NPO等と連携し啓発キャンペーンをプラットフォーム上で実施。期間限定の絵文字や共通ハッシュタグを提供。 ・NPOに対する広告枠の無償提供プログラム「Ads for Good」の実施。 ・UNESCOとメディア情報リテラシーに関するパートナーシップを締結し、教育者向けの新しいハンドブック「Twitterを活用した教育と学習」を提供。 ・UNESCOならびに欧州委員会とのパートナーシップ による、COVID-19に焦点を当てたメディア情報リテラシーキャンペーンの実施。 ・SNS運営企業や学識経験者によって設立された業界団体であるソーシャルメディア利用環境整備機構（SMAJ）への参画。

社名			ヤフー株式会社	Facebook Japan株式会社	Google合同会社	Twitter Japan株式会社
9.「情報発信者側における信頼性確保方策の検討」関係						
9-①	信頼性の高い情報の表示		(ii) Yahoo!ニュース ・トピックスについて 公共性の高い情報をサービスの最も目立つ場所であるYahoo!ニュース トピックスやトピックス詳細ページに掲載。 ・オーサーコメントについて 特定分野の専門性を有するオーサーと契約を締結し、専門分野にかかる記事について、補足的な見解を示して、記事の内容についてのユーザーの理解を向上させることを狙いとする。 専門家の選定にあたっては、特定の分野における専門性、評判、知名度などを基準にした審査を行っており、また専門家による投稿は全件、担当者によるチェックを行うことで、一定の品質を保っている。 (iii)検索サービス ①社会的混乱関係(災害等) 大規模な災害が発生した際などは、関連するワードで検索した際に、各自治体や省庁などが発信している情報等をはじめ、信頼性が高い情報をまとめ、検索結果画面の上部に掲出する取組を実施。 ②健康・医療関係(コロナ関係等) 医療に関する信頼性の高い情報の提供を行うため、特定のワード(例えば「新型コロナウイルス」関連の主要なワードや、各種がんの病名等)で検索した際、公的機関が発信している情報等、信頼性が高い情報をまとめて、検索結果画面の上部に掲出する取組を実施。 同様にワクチンの情報を求めるようなワード(「ワクチン」「ワクチン反対」「ワクチン危険」等)においても、厚生労働省等と連携して、検索結果画面の上部で適切な案内や誤情報への注意喚起をするような施策を実施。 (iv)その他 Yahoo!トップページ(ニューストピックスおよびTOPタイムライン)の取り組み 新型コロナ等、国民の生命財産に関わる重大事項が発生している場合、Yahoo!トップページにおいて、メディアから提供を受けたコンテンツを誘導。首相会見や都知事会見等の動画のエンベッド(埋め込み)による提供や、特設サイトへの誘導など、ユーザーが認知しやすい場所に掲載。 災害においては、地震速報やユーザーのお住まいの地域ごとにアラート情報を掲出。 いずれの情報もメディアや公的機関の情報源とすることで信頼性の高い情報の提供に努めている。		● Google 検索の「ナレッジパネル」や、YouTube の「情報パネル」は、人物や物事についての重要な事実を提供。 ● Google 検索やGoogle News において、ファクトチェックの結果を見つけやすくすること:ラベルやスニペットを使うことにより、あるコンテンツがファクトチェックを受けたものであることがユーザーにすぐに分かるようにしている。 ● Google News の「Full Coverage」機能は、ユーザーがパーソナライズされていない、掘り下げたニュース記事へのアクセスを、ワンタップで可能。 ● ニュース速報やトップニュース、トップページのニュース速報には、重大なニュースがあった場合、Google ニュースのコンテンツポリシーに準拠しているニュース提供元から新着ニュースが提供されることがある。情報パネルはニュースウェブサイトに直接リンクしているため、ニュースの全文記事に簡単にアクセスして読むことが可能。 ● YouTube の情報パネルは、YouTube でニュースを視聴しているユーザーに対し、ニュースコンテンツの情報源をよりよく理解するための追加情報を提供。 ●「広告の表示について」ラベルは、ユーザーになぜその広告が表示されたのかを説明し、また、パーソナライズド広告を変えるために好みをどう管理すべきか、あるいは、パーソナライズド広告を停止する方法を案内。 検索、YouTube、広告等では、ユーザーは、フィードバックボタンを通じて、コンテンツがポリシー違反であることを Google に対して報告することが可能。	○#ThereIsHelp 特定分野のキーワードを検索すると、信頼性の高い公的機関やNPO等の連絡先が表示される #ThereIsHelp を提供。 COVID-19に関連するキーワードを検索すると、日本では厚生労働省の「新型コロナウイルス感染症について新型コロナウイルス感染症について」のページが案内。この取り組みは78カ国・地域で実施。 COVID-19以外では、自殺防止の #ThereIsHelp は日本を含む30カ国・地域で、ワクチン情報については39カ国・地域で、ジェンダーに基づく暴力対策では27カ国・地域で提供。 ○キュレーションによるTwitterモーメント テキスト、動画、GIF画像やライブ放送などの優れたツイートを見つけ、紹介。キュレーターは、オリジナルコンテンツを作ったり記事形式で紹介したりするのではなく、Twitterに既に存在する魅力的なコンテンツをまとめ、提示。こうしたコンテンツはモーメントや、トレンドの説明コンテンツ、リストなどに表示。 Twitterでは現在、5つの言語(英語、日本語、アラビア語、スペイン語、ポルトガル語)で16の市場に向けてキュレーションサービスを提供。キュレーターは正確性と公平性を期して、高品質のコンテンツを見つけるためのトレーニングを定期的に受けている。
9-②	ニュースの選別・編集に関する透明性・アカウンタビリティ確保方策		・トピ掲載基準の公開 Yahoo!ニュースでは、トピックスに掲載する記事の基準として、「公共性」と「社会的関心」を2つの大きな柱としており、その他の掲載基準についても公開。		Google は、膨大な量のコンテンツを分類するテクノロジーを通じて、ユーザーにとって関連性が高く重要かつ有用なニュースを提供。Google ニュースやYouTube で提示されるニュースコンテンツのランキングシステムには、Google 検索と同じウェブクロールとインデックス登録の技術が採用されています。これにより、ウェブ上のニュース記事を絶えず識別して分類し、キーワードやウェブサイトの鮮度といった主要な要因に注目して、検索インデックスにその情報をすべて記録。Google ニュースとYouTubeでは、ニュース メディアがコンテンツを直接 Google のシステムに追加することも可能。	○公平性、正確性、基準 Twitterでは、キュレーションの正確性、公平性、公正性について、高い基準を維持することを目指している。 モーメントでは、さまざまな内容の魅力的なオリジナルコンテンツを取り上げる。モーメントに掲載するツイートや動画の選定では、内容や画像/動画に加え、投稿者のプロフィール画像やユーザー名も検討の対象となる。 ○公平性: 議論を呼びそうな話題に関するツイートを選定する際には、データに基づいて決定を行い、すでにTwitterで大きな反応を呼んでいるツイートを見つける。公の議論に関するトピックの場合、可能な限り多様な視点を提示するように務める。キュレーターは、Twitterでのありのままの会話を客観的に映し出すことを目指し、公平性を期すためのトレーニングを継続的に受けている。 ○正確性: キュレーションの 目的は、正確な情報を提示する質の高いツイートを紹介すること。キュレーションチームは、ソーシャルメディアの検証方法に関して定期的にトレーニングを受けている。また、ほとんどのモーメントは、レビューのプロセスを経てから取り上げられる。 ○誤情報の訂正: 万が一、取り上げた情報が誤りだったことが判明した場合には、モーメントに目に見える形で訂正を加え、その旨をツイートで発表。ただし、稀に当該モーメントを削除し、関連する国のTwitterアカウントを使用して、誤情報を撤回する旨をツイートする場合がある。 ○基準: ニュース性の高い会話を紹介するために必要な場合を除いて、冒 涜、暴 力、裸体など、センシティブであるとみなされるコンテンツは選定の対象から外される。また違法行為を描写したり、助長したりするようなコンテンツは採用しない。センシティブであると受け取られる可能性のあるコンテンツがモーメントに含まれる場合、警告を表示。 ○利害関係の 対立の回避: Twitterのキュレーションチームは、収益を伸ばしたり、アカウント数を増やしたり、Twitterのパートナー関係を管理したりする責任は負わない。ツイートや動画の紹介 や、モーメントのトピックの選択は、Twitterのユーザーにとっての利益を最も重視して行われる。こうした決定が、広告主、パートナー、またはTwitterの事業関係者の 利益の影響を受けることはない。 キュレーションチームは基本的に、Twitterが属する業界 や自社、Twitterの競合企業を扱ったモーメントは作成しない。TwitterやTwitterの競合 企業がTwitter上の会話の中で重要な要素となった場合(たとえば、当該企業の何らかの問題がトレンドトピックになるなど)、Twitterのモーメント編集チームは、当該企業からのリアクションがあればそれも含め、事実に基づく概要をまとめることがある。
9-③	メディアとの連携体制構築具体的検討・取組		信頼できる質の高い情報を増やしていくため、伝統的メディアやネットメディア等と連携体制を構築。 ・適宜、媒体社の配信内容に関する審査を行なっており、ガイドライン等に照らして改善いただきたい点について伝達。 ・公共性・公益性が高いテーマ、社会課題について、媒体社とともに記事制作を実施。 ・公共性の高い情報をサービスの最も目立つ場所であるYahoo!ニュース トピックスやトピックス詳細ページに掲載。		ニュースエコシステムのパートナーと協働することは重要であり、Google は、Google News Initiative 等の多くの方法で協働を進めている。具体的な事例は、How Google Fights Disinformation のレポートを参照。	メディアパートナーは「話題を検索」タブに掲載されるモーメントを提出することが可能。このパートナーシップ は無償。

参考５

違法・有害情報への取組に関する透明性・アカウンタビリティ確保に係る各国政策の比較

（第 24 回プラットフォームサービスに関する研究会　資料５より）

本資料では、日本の「緊急提言」及び事業者ヒアリングシート、EU の「デジタル・サービス・アクト（法案）」、英国の「Online Harms White Paper（OHWP）*」、ドイツ「ネットワーク執行法（SNS 法）」を対象に、それぞれにおける違法有害情報への取組に関する事業者の義務や透明性確保に関する規定について比較した。

国・地域	政策・法律等	性質・ステータス	対象とする情報(定義・範囲)
日本	**インターネット上の誹謗中傷への対応の在り方に関する緊急提言**[*1] **事業者ヒアリングシート**[*2]	自主的スキーム	誹謗中傷等(違法情報・有害情報)
EU	**デジタル・サービス・アクト (DSA)**[*3]	法律案	違法情報
英国	**Online Harms White Paper (政府の完全な対応)**[*4] **透明性レポートに関する政府報告書**[*5]	法律案の方向性	個人の身体的または心理的に重大な悪影響を及ぼす有害情報(違法情報／子供に有害な情報／合法だが成人に有害な情報)
ドイツ	**ネットワーク執行法 (SNS法)**	法律 (施行済)	違法情報(刑法に違反する情報)

【凡例】　次ページ以降の「比較結果」の記載は以下を表す
★：透明性レポート等で報告・公表義務あり
☆：報告・公表が求められるもの
〇：対応が求められるもの（透明性レポート等での報告・公表義務はなし）
△：上記に明確に該当するものではないが、類似する規定がある場合
×：現時点では明確に否定されている場合、または慎重な検討が必要と考えられる場合
※空欄は該当項目・規定なし

大項目	中項目	日本 緊急提言及び ヒアリングシート	EU DSA案	英国 ①OHWP(政府の完全な対応) ②透明性レポートに関する政府報告書	ドイツ SNS法
施策の性質・ステータス		自主的スキーム	法律案	法律案の方向性	法律施行済
対象となる情報の規定(定義・範囲)		誹謗中傷等 (違法情報・有害情報)	違法情報	個人の身体的または心理的に重大な悪影響を及ぼす有害情報 (違法情報／子供に有害な情報／合法だが成人に有害な情報)	違法情報 (刑法に違反する情報)
1．サービス概要とポリシー	1.1. 加入者数、月間アクティブユーザ数又は書込数	☆	★ 23条2項		
	1.2. 利用規約（記載内容等の要件）	☆	○ 12条1項	★ ②Category 1	
	1.3. 削除等の対応	☆	○ 12条2項	★ ②Category 1	★ 2条(2)項1, 2, 9
	1.4. サービスの設計・開発・更新の各段階で実施したリスク評価のプロセス・結果		○ 26条 ★ 33条2項	★ ①4.18節・Box 17	
2．削除等の対応	2.1. 一般ユーザからの申告や削除要請の件数	☆	★ 13条1項b	★ ②Category 2 (一般ユーザ/行政・司法機関の区別に言及はないが、行政・司法機関の関与・協力体制に関する情報を含める必要あり)	★ 2条(2)項3
	2.2. 行政・司法機関からの申告や削除要請の件数	☆	★ 13条1項a		★ 2条(2)項3
	2.3. 一般ユーザからの申告や削除要請に対する削除件数・削除割合	☆	★ 13条1項b	★ ②Category 2 (一般ユーザ/行政・司法機関の区別に言及はないが、行政・司法機関の関与・協力体制に関する情報を含める必要あり)	★ 2条(2)項7
	2.4. 行政・司法機関からの申告や削除要請に対する削除件数・削除割合	☆	★ 13条1項a		★ 2条(2)項7
	2.5. 一般ユーザからの申告や削除要請に対する削除までの平均時間	☆	★ 13条1項b		★ 2条(2)項8
	2.6. 行政・司法機関からの申告や削除要請に対する削除までの平均時間	☆	★ 13条1項a		★ 2条(2)項8

大項目	中項目	日本 緊急提言及び ヒアリングシート	EU DSA案	英国 ①OHWP(政府の完全な対応) ②透明性レポートに関する政府報告書	ドイツ SNS法
2．削除等の対応(つづき)	2.7. その他の主体的な削除件数（AIの活用等）	☆	★ 13条1項c	★ ②Category 3	
	2.8. その他の主体的な削除の方法・仕組み（AIの活用等）	☆	★ 23条1項c	★ ②Category 3	
	2.9. 自動化されたコンテンツモデレーションの透明性	(PF研最終報告書においてフェイクニュースや偽情報への対応の一環として記載)	★ 23条1項c	★ ②Category 3	
	2.10. 不正な申告や削除要請への対策の方法・仕組み	☆	○ 20条		
	2.11. 不正な申告や削除要請への対策の対応件数	☆	★ 23条1項b		
	2.12.削除義務	× (慎重な検討が必要)		○ ①2.19節 (違法コンテンツの削除も「注意義務」に含まれる)	○ 1条(3)項・3条(2)項2・3条(2)項3 (明らかに違法なコンテンツ：24時間以内に削除、違法なコンテンツ：7日以内に削除)
3．削除要請や苦情に関する受付態勢・プロセス	3.1 一般ユーザからの申告・削除要請への受付窓口・受付態勢、対応プロセス	☆	○ 14条	★ ②Category 4	○ 1条3項(1) ★ 2条(2)項1, 2, 4
	3.2 申立時における申立者や発信者への通知の有無	☆	○ 14条4項		○ 3条(2)項3 a) 2条(2)項9
	3.3. 対応決定時における通知の内容、理由の記載の程度	☆	○ 14条5項 15条	★ ②Category 4	★ 2条(2)項9
	3.4. 一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数	☆	△ 32条(コンプライアンスオフィサーが責任を持つ)	★ ②Category 4	★ 2条(2)項4
	3.5. 一般ユーザからの申告や削除要請に対応する部署・チームの規模・人数に関する日本国内の拠点の有無、日本における責任者の有無(*1)	☆	○ 32条(コンプライアンスオフィサー) 11条(法定代理人)		○ 5条(1)項(国内送達受取人)・(2)項(国内の刑事訴追官庁の情報提供要請に対して漏れなく回答する義務)

大項目	中項目	日本 緊急提言及び ヒアリングシート	EU DSA案	英国 ①OHWP(政府の完全な対応) ②透明性レポートに関する政府報告書	ドイツ SNS法
3．削除要請や苦情に関する受付態勢・プロセス(つづき)	3.6. 一般ユーザからの申告や削除要請に対応する部署・チームの人材が有するスキルや、教育の状況			★ ②Category 4	○ 3条(4)項 ★ 2条(2)項4
	3.7. 所管庁からの連絡窓口の設置		○ 10条	△ (①4.48節にて、連絡先を要求する可能性に言及)	○ 5条(1)項(国内送達受取人)・(2)項(国内の刑事訴追官庁の情報提供要請に対して漏れなく回答する義務)
	3.8. 国内拠点の設置		○ 11条(法定代理人)	× (当初記載されていたが、パブコメ後に削除)	○ 5条(1)項(国内送達受取人)・(2)項(国内の刑事訴追官庁の情報提供要請に対して漏れなく回答する義務)
	3.9. 削除等への苦情や問い合わせに対する苦情受付態勢及び苦情処理プロセス	☆	○ 17条	★ ②Category 4	★ 2条(2)項2
3．削除要請や苦情に関する受付態勢・プロセス(つづき)	3.10. 削除等への苦情・問い合わせを受け付けた件数	☆	★ 13条1項d	★ ②Category 4	★ 2条(2)項3
	3.11. 削除等への苦情・問い合わせに対応した件数	☆	★ 13条1項d	★ ②Category 4	★ 2条(2)項7
	3.12. 一般ユーザからの申告や削除要請に対応する部署・チームの人材が有するスキルや、教育の状況		★ 13条1項d		★ 2条(2)項8 (24時間以内、48時間以内、1週間以内又はそれ以上の期間での分類)
	3.13. 裁判外紛争解決機関の利用		○ 18条		○ 3条(2)項3 b) (認定自主機関)
	3.14. 法廷外紛争解決機関に提出した紛争の数、解決の結果、解決までの平均時間		★ 23条1項a		★ 2条(2)項6
	3.15. 信頼できる旗手		○ 19条		

大項目	中項目	日本 緊急提言及び ヒアリングシート	EU DSA案	英国 ①OHWP(政府の完全な対応) ②透明性レポートに関する政府報告書	ドイツ SNS法
4．発信者情報開示への対応	4.1. 発信者情報開示請求を受けた件数	☆	★ 13条1項a		
	4.2. 開示を行った件数	☆	★ 13条1項a		
5．その他の取組	5.1.普及啓発	☆		★ ②Category 6	
	5.2.削除・普及啓発以外の対策(警告表示・ミュート機能等)	☆	○ 27条 ★ 33条2項		
	5.3.取組の効果分析	☆	○ 27条 ★ 33条2項	★ ②Category 6	
6．情報分析・公開	6.1.誹謗中傷等の流通状況に関する分析・調査	☆	○ 26条 ★ 33条		
	6.2.研究者への情報提供・その利用条件	☆	○ 31条	○ ①4.29節	
	6.3.透明性レポートの公開	☆	★ 13条・23条・33条	○ ①4.15節	★ 1条・2条(1)項
7．行動規範の策定	7.1.行動規範の策定	△ (自主的スキームが達成されない場合又は効果がない場合に策定・遵守の求めを検討)	○ 35条	○ (執行機関が行動規範を策定し、企業はそれに則る)	
8．事業者間連携・ノウハウ共有	8.1.事業者間連携・ノウハウ共有	☆		★ ②Category 6	
9．広告	9.1.透明性レポートの公開	(PF研最終報告書においてフェイクニュースや偽情報への対応の一環とした透明性確保に関する記載)	○ 24条・30条		
	9.2.アルゴリズムの透明性	(PF研最終報告書においてフェイクニュースや偽情報への対応の一環として記載)	○ 24条(表示される個々の広告ごと)		
	9.3.行動規範の策定		○ 36条		
10．レコメンドシステムの透明性	10.1.レコメンドシステムの透明性	(PF研最終報告書においてフェイクニュースや偽情報への対応の一環として記載)	○ 29条		
11．モニタリング	11.1.モニタリング	△ (ヒアリングシートの提出を求めること等により把握)	○ 50条～58条	○ ①4.22節～4.28節 (Ofcomによる情報収集・立入調査・聴取調査の権限)	○ 3条(4)項
12．罰則	12.1.罰則	× (慎重な検討が必要)	○ 58条～62条	○ ①4.43節・Box 19	○ 4条

第２部　利用者情報の適切な取扱いの確保について

参考６

プラットフォームサービスに関する研究会
プラットフォームサービスに係る利用者情報の取扱いに関するＷＧ
構成員名簿

（敬称略・五十音順）

【構成員】

	生貝　直人	一橋大学大学院　法学研究科　准教授
	石井　夏生利	中央大学　国際情報学部　教授
	板倉　陽一郎	ひかり総合法律事務所　弁護士
	太田　祐一	株式会社 DataSign 代表取締役社長
	小林　慎太郎	株式会社野村総合研究所　上級コンサルタント
	佐藤　一郎	国立情報学研究所　情報社会相関研究系　教授
	沢田　登志子	一般社団法人 EC ネットワーク　理事
（主　査）	宍戸　常寿	東京大学大学院　法学政治学研究科　教授
	新保　史生	慶應義塾大学　総合政策学部　教授
	高橋　克巳	NTT 社会情報研究所　主席研究員
	寺田　眞治	一般財団法人日本情報経済社会推進協会　主席研究員
	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会　監事
	森　亮二	英知法律事務所　弁護士
（主査代理）	山本　龍彦	慶應義塾大学大学院　法務研究科教授

【オブザーバー】

デジタル市場競争本部事務局

個人情報保護委員会事務局

参考７

プラットフォームサービスに関する研究会
プラットフォームサービスに係る利用者情報の取扱いに関する WG　審議経過

会合	開催日	主な内容
第１回	令和３年３月 18 日	【事業者団体ヒアリング】 ・一般社団法人　日本インタラクティブ広告協会 「インターネット広告市場の動向と利用者情報の取扱い等に関する取り組みについて」 【事業者ヒアリング】利用者情報の取扱いについて ・株式会社 NTT ドコモ ・KDDI 株式会社 ・ソフトバンク株式会社 ・楽天モバイル株式会社 【構成員発表】 ・高橋構成員 「位置情報の取扱いの検討について」 【その他】 ・事務局 「利用者情報の適切な取扱いの確保に向けた検討課題」 「今後の検討の進め方（案）」
第２回	令和３年４月６日	【事業者ヒアリング】利用者情報の取扱いについて ・Apple Inc. ・ヤフー株式会社 【構成員発表等】 ・小林構成員 「実効性のある通知・同意取得方法の在り方に関する実証事業の報告」 ・株式会社インターネットイニシアティブ 「ePrivacy 規則　閣僚理事会案について」
第３回	令和３年４月 22 日	【構成員発表】 ・寺田構成員 「オンライン広告における利用者情報取扱いの動向」 【事業者ヒアリング】利用者情報の取扱いについて ・Facebook Japan 株式会社 ・Google 合同会社 ・株式会社 Agoop
第４回	令和３年５月 18 日	【事業者ヒアリング】利用者情報の取扱いについて ・LINE 株式会社

		【構成員等発表】 ・株式会社日本総合研究所 「スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る調査・分析」 ・森構成員 「利用者端末情報等に関する規制の方向性」 【その他】 ・事務局 「プラットフォームサービスに係る利用者情報の取扱いに関する主な論点」
第５回	令和３年６月４日	【その他】 ・個人情報保護委員会事務局 「令和２年度改正個人情報保護法ガイドライン（案）について」 ・事務局 「電気通信事業における個人情報保護に関するガイドライン改正に向けた考え方（案）」 ・事務局 「プラットフォームサービスに係る利用者情報の取扱いに関する主な論点」
第６回	令和３年７月９日	【その他】 ・事務局 「プラットフォームサービスに係る利用者情報の取扱いに関するWG　中間とりまとめ（案）」

参考 8

海外動向関連参考資料

【米国関係】

① CCPA（カリフォルニア州消費者プライバシー法）関係

② NIST Privacy Framework、NIST SP800-53 Revision 5関係

【EU】

① GDPR（一般データ保護規則）関係

・有効な同意について（GDPR4条関連）
・透明性確保について（GDPR12 条関連）
・ICO（英国データ保護機関）が推奨する通知・同意取得における工夫

② e プライバシー規則（案）

・e プライバシー規則制定に向けた動き
・クッキー設定に係る判例・e プライバシー規則検討に係る論点
・e プライバシー規則の動向（閣僚理事会最終案）
・同意の有効要件（e プライバシー規則（案）4a 条関連）
・クッキー等規制（e プライバシー規則（案）8条関連）

③ デジタル・サービス・アクト（DSA）（規則案）

【ISO/IEC】

・ISO/IEC 29184

CCPA（カリフォルニア州消費者プライバシー法）関係

1

CCPA執行開始　　CPRA施行予定

2020年１月　2020年７月　2020年11月　2023年１月

カリフォルニア州消費者プライバシー法　施行
（**CCPA**: California Consumer Privacy Act）

住民投票で改正法案であるカリフォルニア州プライバシー権法案可決
（**CPRA**: California Privacy Rights Act）→さらなるプライバシー保護強化へ

CCPA概要

○　カリフォルニア州居住者の個人情報を収集等する一定の事業者（州内拠点は不要）に適用されるプライバシー保護法。
○　「個人情報」は、特定の消費者又は世帯を識別等できる情報とされ、**オンライン識別子**も含まれる。
○　改正法案であるCPRAにより、監督当局であるCCPAの設立、オプトアウト権の拡張（販売に加えて共有が追加）、センシティブ個人情報の新設、訂正権の新設等、プライバシー保護がさらに強化された。

CCPA及びCCPA規則に基づくプライバシーポリシー・通知に関する義務

○　一般的なルールとして、**簡潔でわかりやすい表現**を用いること、**読みやすく、目立つ形式**を使用することなどが定められている。

プライバシーポリシー	通知	
記載内容		記載内容、通知方法等
①　**収集、開示、又は販売される個人情報について知る権利** ・消費者が、収集、利用、及び開示される個人情報について事業者に開示を求める権利を有すること ・直近12か月に当該事業者が収集した個人情報の類型　など ②　**削除請求権** ③　**販売からのオプトアウト権** ④　消費者プライバシー権を行使したことにより差別されない権利 ⑤　代理人による権利行使方法 ⑥　プライバシーポリシーの最終改定日　など	個人情報の収集時	・収集する個人情報の**類型**　・**利用目的** ・**"Do Not Sell My Personal Information"**リンク/URL ・**プライバシーポリシー**へのリンク/URL ・消費者が**想定しない目的**で消費者の**デバイス**から個人情報を収集しようとするときは**ジャストインタイム通知**（例：ポップアップ）を行う　など
	販売からのオプトアウト権	消費者が、ホームページやモバイルアプリのダウンロード/ランディングページ上の**"Do Not Sell My Personal Information"**リンクをクリックして飛ぶウェブページ等に、個人情報の販売からのオプトアウト権の説明やリクエストフォームを記載するなど
	金銭的インセンティブ	事業者が個人情報の収集等について金銭的インセンティブを提供している場合には、消費者がオプトインする前に金銭的インセンティブの概要、関連する個人情報の類型等を通知するなど

プライバシーポリシーの該当箇所へのリンクの記載をもって代えることも可能

NIST Privacy Framework、NIST SP800-53 Revision 5関係

2

概要

○　米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が2020年１月に、企業のリスクマネージメントを通じたプライバシー改善ツールとして、「NIST Privacy Framework」を公表（その前に公表された「NIST Cyber Security Framework」の姉妹編の位置付け。）。法的効果や強制力を持つものではない。
○　NISTは、「NIST Privacy Framework」と「NIST Cyber Security Framework」をシームレスに統合した文書として、「NIST Security and Privacy Controls for Information Systems and Organizations（SP800-53 Rev5）」を2020年９月に公表し、同意取得や通知を行う際の留意事項を提示。

Privacy Framework

Core（機能）	以下５つの機能ごとに、カテゴリー・サブカテゴリーを設けて細分化。
	Identify-P（特定）
	Govern-P（統治）
	Control-P（制御）
	Communicate-P（消費者やステークホルダーとの対話体制の整備）
	Protect-P（保護）
Profiles	Current state（現在の姿：CoreとTierで具現化）と Desired target state（めざすべき姿）のギャップを明確化
Implementation Tier（Coreに対する評価基準）	Tier1：Partial（部分的に対応できている）
	Tier2：Risk Informed（リスクが認識できている）
	Tier3：Repeatable（対応に再現性がある）
	Tier4：Adaptive（変化に適応できる）

SP800-53 Revision5

○　**同意取得**の管理（個人のインフォームド・ディシジョン促進のために、個人情報収集前に、個人が処理に同意するためのツールまたはメカニズムを実装）を強化する手法として、**Tailored Consent**、**ジャストインタイムの同意**、**撤回**を提示。
○　**通知**の管理（組織が定義した頻度での通知、平易な言語で明確かつ分かりやすい表現、処理を許可する権限の識別、処理目的の特定等）を強化する手法として、ジャストインタイムの通知等を提示。
○　**リスク評価**の管理として、システム、プログラム又はその他の活動について、**事前にプライバシー影響評価を実施**するとしている。

有効な同意について（GDPR４条関連）

GDPRにおける有効な同意

○ GDPR第４条により、有効な同意といえるには、①自由に与えられ、②特定され、③説明を受けた上での、④不明瞭ではない積極的な意思表示であるという４つの要素を充足しなければならないと定められている。

○ Guidelines on Consent under Regulation 2016/679（最終改定（Ver1.1採択）2020年5月4日）により、４要素の詳細・具体例が示されている。

①「自由に与えられる」（任意）

○ データ主体に選択権・支配権があること
- 強制されたと感じない
- 同意しなくてもネガティブな結果に直面すると感じない
- 同意が契約条件の交渉できない部分として まとめられて（抱き合わせになって）いない

○ Ver1.1で、同意がサービス提供の条件になってはいけないことが明記された。
- ユーザーが同意しなければ当該サービスを使えず、**他社の同等のサービス**を探すことになる場合は、任意の同意とはいえない
- **Cookieウォール**（同意を求めるポップアップに同意しないと、ウェブサイトが利用できない）による同意は任意とはいえない

②「特定されている」

○ 特定の目的に対し、同意するか否かをデータ主体が選択できる
- 同意の目的は明確に記述する
- 同意取得に関係した情報は、他の情報から明確に分離する
- 別目的に使う場合は同じデータでも追加の同意が必要である

○ 特定の目的に対し、特定の同意を与えられるよう、管理者は個別のオプトインを提供すべきである

③「説明を受けている」

○ 同意を取得する前に、データ主体に情報提供することが必要不可欠である

○ 最小限の内容として、管理者の身元、同意が求められる各取扱業務の目的、収集・利用されるデータ（そのタイプ）、同意を撤回する権利の存在等が挙げられている。

※本要素については、次ページのICOからの推奨事項も参照されたい。

④「不明瞭ではない積極的な意思表示」

○ 同意は、データ主体が積極的に行動・宣言して与えられるべきである
- 契約書への合意やサービス条件の承諾だけでは、積極的な同意とはみなされない
- あらかじめチェックの入ったオプトインのチェックボックスやオプトアウトの仕組みも無効（承諾「しない」ことに行動が必要）

○ Ver1.1で、**ウェブページのスクロールやスワイプ等は、明確で積極的な意思表示とはいえない**ことが明記された。

透明性確保について（GDPR12条関連）

GDPRにおける透明性確保

○ GDPR第12条では、「データ主体への情報提供」「権利行使に関するデータ主体との連絡」「データ侵害に関する連絡」について、透明性確保に関する一般ルールを定めている。

① **簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式**でなければならず
② 明瞭かつ平易な文言が使われなければならず
③ 子どもに情報を提供する際は、明瞭かつ平易な文言という要件が特に重要であり
④ 書面で、又は適切であるときは電子的な手段を含め、その他の方法によらなければならず
⑤ データ主体によって要求された場合は、口頭で提供することができ
⑥ 一般に無償で提供されなければならない

○ Guidelines on Transparency under Regulation 2016/679（最終改定2018年4月11日）により、透明性確保のために推奨される通知方法・工夫の例示が示されている。

	具体的な意味合い	推奨される通知方法・工夫の例
簡潔である	主体に情報疲労をさせない為に、情報管理者が情報／通知を効率的かつ簡潔に提示する	階層的なプライバシーステートメント／プライバシー通知により、大量のテキストスクロールを不要とする
透明性がある	• データ主体が使われ方を事前に知らなければならない • リスクを事前に評価し、正しくデータ主体に伝える	事前にリスクの有無を丁寧に評価する
理解しやすい	• ごく普通の人でも理解できるようにすることが必要である • 可能ならば対象者に理解してもらいやすい説明を行うべき	理解のしやすさや有効性が分からないときは、公開討論やテストで試行する
容易にアクセスできる	必要な情報がどうすれば確認できるかが一目瞭然である	• サイト上に、明瞭に視認できる形でプライバシーステートメント／プライバシーノーティスを公表する • アプリの場合は、ダウンロード前のオンラインストアや、アプリ内から情報に容易に（2タップ以内で）アクセスできるようにする • 個人データを収集する時点で、プライバシーステートメント／プライバシーノーティスへのリンク、又は個人データを収集するのと同じページにその情報を表示する

ICO（英国データ保護機関）が推奨する通知・同意取得における工夫

ICOが推奨する通知・同意取得における工夫

○ 英国のデータ保護機関であるThe Information Commissioner's Office（**ICO**）は、GDPR第４条の有効な同意の４要素のうち③「説明を受けている」について、公式サイト（※）で、スマートフォンに表示すると良い画面等の例を示しつつ、望ましい情報提供の在り方を解説している。

1	階層的アプローチ （Layered Approach）	重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。
2	ダッシュボード （Dashboards）	管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。
3	ジャストインタイム通知 （Just-in-time-notices）	個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。
4	アイコン （Icons）	特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。
5	モバイル及びスマートデバイスの機能性 （Mobile and smart device functionalities）	ポップアップ、音声アラート、モバイルデバイスのジェスチャーなど。

※ICOウェブサイト *"What methods can we use to provide privacy information?"*
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

eプライバシー規則制定に向けた動き

EUでは、オンラインサービス利用者の端末装置でのデータ処理に対する規制（クッキー規制）が行われている。
2017 年以来、EU 域内規制を統一するためePrivacy規則案がドラフトされていたが、
2021年2月10月、欧州連合理事会（閣僚理事会）が、加盟国がePrivacy規則案に合意したことを発表。

2002年	**ePrivacy指令施行**。クッキー設定について、 (1)情報提供、(2)拒否権（オプトアウト権）提供を義務づけ
2009年	**ePrivacy指令改正**。クッキー設定について、 **同意取得を義務づけ。** 同意有効要件は1995年旧EUデータ保護指令を引用：(1)任意、(2)対象特定、(3)情報提供
2018年	**GDPR施行、同意有効要件が厳格化**された。 (1)任意、(2)対象特定、(3)情報提供、(4)曖昧ではない陳述、または明確で肯定的な意思表示。

オプトアウト、暗黙の同意、みなし同意が許されなくなった。

ePrivacy指令の問題点

○ ePrivacy 指令を施行する EU 加盟国の国内法による規制内容は、国ごとにばらつきがある。
○ プライバシー侵襲の程度が低い類型のクッキーを同意なく利用できる範囲を明らかにする必要。

ePrivacy規則制定への動き

クッキー設定に係る判例・eプライバシー規則検討に係る論点

欧州司法裁判所(CJEU)の裁判例により、同意有効要件、クッキー設定に複数主体が関与する場合の責任範囲等に関する判例法が確立されつつある。

あらかじめチェックされたチェックボックスによる同意取得の有効性（Planet49判決）

GDPR が規定する同意は、能動的な意思表示でなければならない。
あらかじめチェックが入れられたチェックボックスを示し、利用者が同意を拒否するためにはこのチェックを外さなければならない状況では、**有効な同意は取得し得ない。**

クッキーを設定する第三者の責任（Fashion ID判決）

広告最適化の目的でサードパーティークッキーをウェブサイトに設置するなど、第三者による端末装置におけるデータの読み書きを許容する**ウェブサイト管理者**は、クッキー設定元の第三者であるネット広告エージェンシー、ソーシャルメディア等とともに、**GDPR 上の共同管理者の立場**に立ち、端末識別子、閲覧・行動履歴など取得される**個人データの利用目的について利用者に情報提供し、利用者から同意を取得する義務**を負う。

2019年11月以来、閣僚理事会輪番議長国がePrivacy規則案のドラフトを提出。端末装置におけるデータ処理に関する適法根拠として、サービス提供に必須な場合**（必須クッキー）の他、何を含めるかが論点**となった。

・広範
・GDPR第6条1(f)の適法根拠を採用

利用者の権利・利益に優越するサービス提供者の**「正当な利益」**

利用者への情報提供、オプトアウト提供などの条件の下での、**セキュリティ維持**

限定的

eプライバシー規則の動向（閣僚理事会最終案）

閣僚理事会最終案 2021/2/10

- **クッキー規制**：端末装置におけるデータ処理は、以下の場合等に許される。
  - 電子通信サービス提供のために**必要**な場合
  - 利用者の**同意**がある場合
  - 利用者が個別に求めるサービスの提供に**必須**の場合
  - サービス提供者がもっぱら**オーディエンス測定**のために必要とする場合
  - オンラインサービスの**セキュリティ維持**等のために必要な場合
  - **セキュリティ**のためのソフトウェアアップデートに 必要な場合
  - 緊急通報
  - 他目的への**二次利用**は、以下の判断要素に照らして当該他目的が当初の処理目的と相容れるものである(**compatible**)場合のみ許される。
    - ✓ 当初の目的と当該他目的との関係
    - ✓ 当該他目的処理を行うに至った状況
    - ✓ 対象データがセンシティブなデータを含むものかどうかなど処理の性質
    - ✓ 当該多目的処理が利用者に及ぼす影響
    - ✓ 暗号化・仮名化などの安全措置の有無
- **クッキー利用の同意をサービスの提供条件**とするには、**当該事業者が、同意を提供条件としない同等のサービスを提供している（利用者から選択権を奪わない）**ことが必要。
- 利用者氏名等不詳でも、端末識別子による特定によりクッキー同意証明を認める。
- 毎年１回以上、**同意撤回権**があることを通知する義務
- **域外適用**：利用者がEU内に所在する場合、域外事業者にも適用。
  EU代理人の選任が必要となる。
- 規則違反に私的訴権、非営利団体による代理訴訟、非金銭的損害の賠償を認める。
- 電子通信データの違法利用について、 €20M または世界売上 4% の行政制裁金

- ➢ 適法根拠に**「正当な利益」**は採用せず、限定列挙のみ
- ➢ 従来からの判例の蓄積などを取り込んだ内容
- ➢ オーディエンス測定、compatibleな場合の二次利用等、今後解釈の検討が必要な適法要件もある

閣僚理事会・欧州議会による正式な立法手続へ
※今後、内容の修正もあり得る

同意の有効用件（eプライバシー規則（案）4a条関連）

EUでは、オンラインサービス利用者の端末装置でのデータ処理に対する規制（クッキー等規制）が行われている。2021年2月10月、欧州連合理事会（閣僚理事会）が、EU 域内規制を統一するためのePrivacy規則案に加盟国が合意したことを発表した。

同意の有効要件等（4a条、前文）

○ ePrivacy規則における同意の定義は、GDPRによる同意の定義に従う。
→①**自由**に与えられたこと、②**特定**されていること、③**事前に説明を受けた**こと、④**不明瞭ではない**積極的な意思表示であることが必要（**オプトアウト、暗黙の同意、みなし同意は不可**）。

○ 端末装置の処理・蓄積機能を利用する者、又は端末装置からデータを収集する者が同意を取得する責任を負うが、同意取得を第三者に代行させることも可能。

○ **ブラウザ／アプリのソフトウェア設定**によるクッキー設定等への同意も、有効な同意と認められる。
※ただし、同意の対象は特定されていなければならないので（GDPRの同意有効要件）、ブラウザ／アプリの仕様が、広告・アクセス解析等の目的ごとの同意管理に対応する必要がある。

○ ユーザーが直接表明した同意の意思表示（※）は、上記のソフトウェア設定に優先する。
※例えば、クッキーバナーに表示されるボタンのクリック等。

○ サービス提供者がデータ主体を（氏名などにより）特定できない場合、**当該端末装置から同意が与えられたことを示す技術プロトコル**をもって、クッキー設定等に関する同意を取得することができる。

○ 同意したユーザーに対しては、**12か月を超えない間隔**で定期的に、当該**同意を撤回**できることを**リマインド**しなければならない。ただし、当該ユーザーがこのようなリマインドの受領を受け取らないことを希望する場合は、この限りではない。

○ クッキー設定等に対する同意をサービス提供の条件としても、①クッキー設定等の目的に関する**明瞭で正確な理解しやすい情報提供**がされ、かつ②**同じサービス提供者による同等のサービスでクッキー設定等に対する同意をサービス提供の条件としないもの**を利用者が選べる場合には、**利用者から選択権が奪われたとはみなされない**（＝同意の任意性がある）。

クッキー等規制（eプライバシー規則（案）８条関連）

クッキー等規制（8条）

○ 端末装置の処理・蓄積機能の利用、端末装置からの情報の取得（クッキーの利用等）は一般的に禁止され、以下の場合に限り許される。

許される場合	想定される適用例
もっぱら電子通信サービス提供に必要な場合	メッセージサービスのHTTPセッション維持
利用者が**同意**した場合	ターゲティング広告、コンテンツのパーソナライズ
利用者が個別に求める**サービスの提供に必須**な（strictly necessary）場合	ユーザー入力、ログイン認証状態、表示言語の記憶
もっぱら**オーディエンス測定**に必要な場合	閲覧者のWebページ滞在時間等の解析
オンラインサービス、端末装置の**セキュリティ維持・復旧、不正利用防止、障害検知・防止**に必要な場合	当該ユーザーが通常利用しているブラウザとは別のブラウザからのログイン試行の検知、これに対する警告
ソフトウェア・アップデートに必要な場合 ただし以下の３つの条件を満たす必要がある。 ① セキュリティ上の必要によるものであり、ユーザーの選択したプライバシー設定を変更しないこと ② 個別アップデートごとに事前にユーザーに情報提供すること ③ 利用者が自動アップデートを延期又は中止できること	ブラウザが最新のセキュリティアップデートをインストールしているか否かの確認
緊急通報において端末装置の位置を特定するために必要な場合	同左
同意又は一定の公益保護を目的とする法令上の根拠がある場合、及び二次利用の目的が当初の処理目的と相容れる(compatible)場合は、二次利用が可能	不正ログイン検知情報を捜査協力目的で捜査機関に提供

EUにおけるデジタルサービスアクト（DSA）の概要

- 2020年12月15日、欧州委員会はDigital Service Act（DSA）の法律案を公表。DSAは全ての仲介サービス提供者（プラットフォーム事業者等）に対して、違法コンテンツの流通に関する責任を規定するとともに、事業者の規模に応じたユーザ保護のための義務を規定。

1.対象事業者

仲介サービス（ISP等）、**ホスティングサービス**、**オンライン・プラットフォーム**（オンラインマーケットプレイス、アプリストア、SNS等）、**超大規模オンラインプラットフォーム**を提供する事業者

2. 仲介サービス提供者の違法コンテンツに対する責任【第Ⅱ章】

・「単なる導管」、「キャッシング」、「ホスティング」の3類型に分けて**違法コンテンツに対する免責条件を規定**。

・一般的モニタリング義務は無いものの、司法及び行政**当局からの削除等の措置命令・情報提供命令**への**報告義務**を規定

3. 透明で安全なオンライン環境のための義務【第Ⅲ章】

(1)全ての仲介サービス提供者に対する義務【第1節】

コンテンツモデレーション措置を定めた利用規約の公開、**透明性報告義務**（※1）、連絡窓口・国内法定代理人の設置 等

※1　違法コンテンツの通知件数・削除件数、自発的なコンテンツモデレーションの内容、対応に関する苦情の件数等。事業者の規模に応じ、透明性義務の内容を追加

(2)ホスティングサービス提供者の義務【第2節】

違法コンテンツの通知受付体制整備、**違法コンテンツへの対応に関する理由の通知**　等

(3)オンライン・プラットフォームの義務【第3節】

違法コンテンツへの対応に関する苦情受付体制整備、裁判外紛争解決機関の利用、信頼された旗手、不正な通知・反論に対する対策、**オンライン広告の透明性確保**（※2）　等　※2　広告であること、広告主及び広告表示決定に用いられた主なパラメータ等を表示

(4)超大規模オンライン・プラットフォームの義務【第4節・第5節】

サービスのリスク評価実施・リスク軽減措置の実施、外部監査の実施・公表、レコメンダー・システム、**オンライン広告の透明性の追加**（※3）、規制当局及び研究者のデータアクセス、コンプライアンス・オフィサー設置、**行動規範**、危機対応　等

※3　広告表示から1年後まで、広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂・APIを介して一般に利用可能とする。

4. モニタリング及びエンフォースメント

・各加盟国はDSAの執行責任者であり調査権限等を持つ**デジタルサービス調整官**を設置。

・欧州委員会は超大規模オンライン・プラットフォームをモニタリング。義務違反の場合、**前年度の総売上高の最大6%の罰金**等を科すことが可能。

対象事業者の分類

- DSAの対象は、情報社会サービスのうちの「仲介サービス」「ホスティングサービス」「オンライン・プラットフォーム」「超大規模オンライン・プラットフォーム」であり、第2条(f) (h)、第16条、第25条にて規定されている。

出典:　https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

仲介サービス　【第2条(f)】

ネットワークインフラを提供する仲介サービス。ISP、ドメイン名レジストラの他、以下のホスティングサービスも含む。

※　第Ⅱ章では、「単なる導管」、「キャッシング」、ホスティングに分類してそれぞれの免責条件を規定。

ホスティングサービス　【第2条(f)】

クラウドやウェブホスティングなどのホスティングサービスの他、以下のオンライン・プラットフォームを含む。

オンライン・プラットフォーム　【第2条(h)：第16条※】

オンライン・マーケットプレイス、アプリストア、コラボレーション・エコノミー・プラットフォーム、ソーシャルメディア・プラットフォームなど、売り手と消費者を結びつけるオンライン・プラットフォーム。

※規制対象から除外する小規模オンラインプラットフォームを規定

超大規模オンライン・プラットフォーム　【第25条】

非常に大規模なオンライン・プラットフォームは、違法コンテンツの流布や社会的危害において特にリスクがある。**欧州の4億5000万人の消費者のうち10%以上の消費者にリーチするプラットフォーム**については、特定のルールが想定されている。

対象事業者に応じた義務の一覧

- それぞれの対象ごとに規定されている義務は以下のとおり。

		仲介サービス	ホスティングサービス	オンライン・プラットフォーム	超大規模プラットフォーム
命令を受けて国の機関と連携	第8条・第9条	●	●	●	●
連絡先、必要な場合には法定代理人	第10条・第11条	●	●	●	●
基本権を考慮した利用規約の要件	第12条	●	●	●	●
透明性の報告	第13条	●	●	●（第23条も追加）	●（第23条及び第33条も追加）
利用者への通知・行動と情報提供義務	第14条・第15条		●	●	●
苦情・救済の仕組みと裁判外紛争解決	第17条・第18条			●	●
信頼された旗手	第19条			●	●
不正な通知・反論に対する対策	第20条			●	●
犯罪行為の通報	第21条			●	●
サードパーティサプライヤーの信用証明書の審査(KYBC)	第22条			●	●
オンライン広告のユーザ視点の透明性	第24条			●	●
リスク管理義務とコンプライアンス・オフィサー	第26条・第27条・第32条				●
外部リスク監査と公的説明責任	第28条				●
レコメンドシステムの透明性と情報へのアクセスのためのユーザーの選択	第29条・第30条				●
当局・研究者とのデータ共有	第31条				●
行動規範	第35条・第36条				●
危機対応への協力	第37条				●

（参考）DSA法案の条文構成(1/2)

- 詳細な条文構成は以下のとおり。

第Ⅰ章　総則

第1条　主題と範囲
第2条　定義

第Ⅱ章　仲介サービス提供者の責任

第3条　「導管」
第4条　「キャッシング」
第5条　ホスティング
第6条　自主調査と法令遵守
第7条　一般的なモニタリング及び積極的な事実調査の義務なし
第8条　違法コンテンツに対する措置命令
第9条　情報提供の命令

第Ⅲ章　透明で安全なオンライン環境のためのデューデリジェンス義務

第1節　すべての仲介サービス提供者に適用される規定

第10条　連絡先
第11条　法定代理人
第12条　利用規約
第13条　仲介サービス提供者に対する透明性報告義務

第2節　オンライン・プラットフォームを含むホストサービスの提供者に適用される追加規定

第14条　通知と行動の仕組み
第15条　理由の記載

第3節　オンライン・プラットフォームに適用される追加規定

第16条　零細企業及び中小企業の排除
第17条　内部通報制度
第18条　法廷外紛争解決
第19条　信頼された旗手
第20条　不正使用に対する措置及び保護
第21条　犯罪行為の疑いの届出
第22条　トレーダーのトレーサビリティ
第23条　オンラインプラットフォームの提供者に対する透明性報告義務
第24条　オンライン広告の透明性

第Ⅲ章　透明で安全なオンライン環境のためのデューデリジェンス義務

第4節　システムリスクを管理するための超大規模オンライン・プラットフォームの追加義務

第25条　超大規模オンライン・プラットフォーム
第26条　リスク評価
第27条　リスクの軽減
第28条　独立監査
第29条　レコメンダー・システム
第30条　オンライン広告の透明性の追加
第31条　データへのアクセスと精査
第32条　コンプライアンス・オフィサー
第33条　超大規模オンライン・プラットフォームの透明性報告義務

第5節　デューデリジェンス義務に関するその他の規定

第34条　標準
第35条　行動規範
第36条　オンライン広告の行動規範
第37条　危機のプロトコル

（参考）DSA法案の条文構成(2/2)

第Ⅳ章　実施、協力、制裁及び執行
第1節　主務官庁及び各国デジタルサービス調整官
第38条　主務官庁及びデジタルサービス調整官 第39条　デジタルサービス調整官の要件 第40条　管轄 第41条　デジタルサービス調整官の権限 第42条　罰則 第43条　苦情を申し立てる権利 第44条　活動報告 第45条　デジタルサービス調整官の国境を越えた連携 第46条　共同調査及び欧州委員会の介入要請
第2節　欧州デジタルサービス会議
第47条　欧州デジタルサービス会議 第48条　会議の構成 第49条　会議の任務
第3節　超大規模オンライン・プラットフォームに関する監視、調査、遵守及びモニタリング
第50条　超大規模オンラインプラットフォームの監督強化 第51条　委員会の介入及び手続開始 第52条　情報の要求 第53条　聴取り・陳述を行う権限 第54条　立入検査の権限 第55条　暫定措置 第56条　約束 第57条　モニタリング行為 (右上につづく)

第Ⅳ章　実施、協力、制裁及び執行
第3節　超大規模オンライン・プラットフォームに関する監視、調査、遵守及びモニタリング
(左下からのつづき) 第58条　不遵守 第59条　罰金 第60条　定期的な違約金の支払い 第61条　刑罰の制限期間 第62条　刑罰の執行の制限期間 第63条　聴取及びファイルにアクセスする権利 第64条　決定の公表 第65条　アクセス制限の請求と国内裁判所との連携 第66条　欧州委員会の介入に関する実施法
第4節　遵守に関する共通規定
第67条　情報共有システム 第68条　代理
第5節　委任された行為
第69条　委任の行使 第70条　委員会
第Ⅴ章　最終条項
第71条　指令2000/31/ECの特定の規定の削除 第72条　消費者の集団的利益の保護のための代表者行動に関する指令2020/XX/ECの改正 第73条　評価 第74条　効力の発生及び適用

ISO/IEC 29184

概要

○　国際標準化機構（ISO：International Organization for Standardization）が「Information technology – Online privacy notices and consent（消費者向けオンラインサービスにおける通知と同意・選択）」と題する規格を、2020年６月に出版。

○　通知及び同意について、組織の義務として、次の点が記載されている。

通知	
通知の義務	通知が必要な状況を特定し、必要な場合はいつでも本人に通知。
適切な表現	本人に対し、明確かつわかりやすい方法で通知。
多言語	本人が使用すると想定される言語で通知。
適切なタイミング	本人に通知する適切なタイミングを決め、文書化。
適切な場所	オンラインの場合も含め、本人が簡単に見つけてアクセスできるようにする。
適切な形態	どのように通知を提供し、アクセスできるようにするかを決める。
継続的な参照	同意した際の通知の最新版などを本人が容易に参照できるよう、保管。
アクセシビリティ	オンラインサービスの技術に適した、本人がアクセス可能な方法で通知を提供。

同意	
同意の適切さの識別	同意または明示的な同意が適切な状況かを特定した上で同意を求める。
フリー/インフォームドコンセント	本人が強制や強要を受けず、意図的な行為（チェックボックスのクリック、ボタン押下、スライドバーのスライド等）で得られた同意であること。 十分な情報が提供され、変更や撤回が簡単に行うことができること。
対象アカウントの明示	アカウントに紐付いた同意収集の場合、どのアカウントか明示。
他の同意からの独立性	プライバシーに関する同意は、他の事項に関する同意と明確に区別して取得。
必須/任意の個別同意	必須要素と任意要素のそれぞれについて、本人が個別に同意を提供できる仕組みとする。
頻度	適切な間隔を置いて、既存の同意の確認、あるいは新規の同意取得を行う。
適時性	適切なタイミングで同意を取得。

○　他、Annexとして、PCやスマホで同意を取得する際のユーザーインターフェース例、同意の証跡例が添付されている。

移動通信事業者における利用者情報の取扱い状況　ヒアリングシート回答における主な項目の比較

社名		株式会社NTTドコモ	KDDI株式会社	ソフトバンク株式会社	楽天モバイル株式会社
１．利用者情報の取扱いの状況、位置情報の取得・分析					
1-1.	利用者情報取得の場面・取得する情報の内容	・別紙にて回答	・主にWebサービスやアプリの利用時に、サービスの利用履歴や登録いただいた情報を利用者情報として取得。利用履歴には閲覧履歴・決済履歴・購買履歴等が含まれる。	＜取得の場面＞ ・サービスのお申込時、ご利用時、お問い合わせ対応時等に、取得。なお、取得時の同意については 2-2.を参照。 ＜情報の内容＞ ・氏名、住所、生年月日、性別、電話番号、職業、勤務先、メールアドレスなど。なお、個人情報の取得全般については、プライバシーポリシーに公表している。 https://www.softbank.jp/corp/privacy/telecom/	・サービス（回線、オプション、その他楽天モバイルから提供しているアプリ等のサービス）利用時。利用者の氏名、年齢、住所、電話番号等の情報。
1-2.	位置情報取得の場面・取得する情報の内容	・別紙にて回答	・auカーナビ・My au・au PAY等のアプリケーションにてGPS位置情報を取得。また、アプリ利用時に取得するGPS位置情報以外に、基地局側で取得する位置登録情報も取得。	＜取得の場面＞ ・契約時の通信サービスの約款等により、同意を取得し、通信サービス提供に必要な範囲で取得。 ●基地局に係る位置情報＊： ・電源をONにしたタイミングや個々の通信時以外に移動体端末の所持者がエリアを移動するごとタイミングなど。 （＊位置登録情報：通話やメール等の通信を成立させる前提として取得している情報） ●Wi-Fi位置情報＊： ・端末がアクセスポイントと接続し、外部と通信を行う前提として、端末がMACアドレス等をアクセスポイントに送信するタイミングなど。 （＊Wi-Fiのアクセスポイントと移動体端末間の通信を位置情報の測位に応用することによって、利用者によるインターネット接続の前後を問わず取得される位置情報） ＜情報の内容＞ ●基地局に係る位置情報： ・基地局の識別番号、端末の識別番号、取得日時など ●Wi-Fi位置情報： ・日時、端末MACアドレスなど	・回線サービス提供に伴う取得（基地局位置情報など） ・アプリ等で GPS 取得を許可されている場合の取得（GPS 位置情報）
1-3.	アプリやサイト（ブラウザ）経由の取得の状況・今後の予定	・別紙にて回答	・弊社提供サービスをご利用いただくことに伴うサービスの利用情報等を取得。	＜取得の状況＞ ・各サービスごとに、サービス提供に必要な範囲で、取得。 例えば、弊社WebサイトではGoogle Analyticsを利用してサイト訪問者の行動履歴（ページ遷移、離脱等）を取得。 ＜今後の予定＞ ・お客さまへの説明についてより一層わかりやすくする取り組みを検討中。	・Rakuten Link、My 楽天モバイルなどアプリによる取得あり。今後もアプリやブラウザによる取得の予定あり。
1-4.	端末からの取得情報（センサー情報等）	・別紙にて回答	・弊社スマートホームサービスであるau HOMEでは、各種デバイスのセンサーにより、以下のような情報を取得。 ・開閉センサーによるドアや窓の開閉情報 ・マルチセンサーによる人/動物の検知情報 ・スマートロックによる鍵開閉情報 ・睡眠センサーによる心拍・呼吸・体動情報 ・スマートプラグによる電気使用量情報　等	＜GPS、位置センサー等の取得情報＞ ・日時、IDFAもしくはAdvertisingID、端末IPアドレス、GPS緯度経度情報など、アプリケーションに依存。	・端末識別 ID(IMEI)、端末機種名、OS 情報、端末に紐づく広告 ID（IDFA、Advertising ID）、位置情報(WiFi, Bluetooth)。
1-5.	取得情報の加工・分析・利用状況	・別紙にて回答	・取得した情報は、サービス毎に利用実態の分析やレコメンデーションに利用するほか、当社が付与した識別子をキーとして様々なサービスで取得した利用者情報を集約し、サービス横断での利用実態の分析を実施し、自社サービスのマーケティング活動を目的にサービス利用者のプロファイリングやターゲティング広告に利用。	＜利用・分析状況＞ ・取得時の利用目的の範囲でサービス提供やお問い合わせ対応などのために利用、また、商品開発などを目的とした経営分析などに利用。 ・利用の目的の詳細については、プライバシーポリシーを参照。 https://www.softbank.jp/corp/privacy/ ＜匿名加工情報への加工＞ ・広告ビジネスを目的とし、個人情報保護法に則り、匿名加工情報としてHPに公表の上、加工、利用している。 ・詳細は、「お客さま情報の利活用にあたってのプライバシー保護の取り組み」を参照。 https://www.softbank.jp/corp/privacy/utilization/ ＜統計情報への加工＞ ・公共計画などを目的とし、匿名化、統計処理、秘匿化の加工を行い、統計データとして利用。	構成員限り

参考９－１

社名		株式会社NTTドコモ	KDDI株式会社	ソフトバンク株式会社	楽天モバイル株式会社
1-6.	位置情報と位置情報以外の情報（加入者情報等）を組み合わせた分析・利用状況	・別紙にて回答	・各サービスの改善の分析等の他、位置情報に性別・年代の属性情報を付与してエリアの人口動態が分析できるサービスを官公庁や自治体、その他民間企業に対し提供。 （https://k-locationanalyzer.com/）	・位置情報と位置情報以外を組み合わせた分析・利用を行っています。例として、位置情報を統計化したデータと年代などを組み合わせることで、各地域ごとの年代別の人流の変化を分析することで、新型コロナウィルスへの対策検討や、災害時の避難状況の把握などに利用。 ・詳細は、「お客さま情報の利活用にあたってのプライバシー保護の取り組み」を参照。 https://www.softbank.jp/corp/privacy/utilization/	構成員限り
1-7.	利用者情報の第三者提供の状況	・別紙にて回答	・各サービスの提供に必要な範囲で利用者情報の第三者提供をしている。例えば、弊社グループ会社と連携した割引や特典の付与等のために利用者情報を提供する場合がある。	・個人データの第三者提供は、お客さまの同意に基づき、実施。 例として、スマートフォン決済の新規ユーザー登録を簡便化するために、お客さまの同意に基づき、情報連携を行うことで、快適なユーザー体験とお得な特典を実現。	・楽天グループへの共有（キャンペーンのポイント付与、広告）。 ・公的機関等による開示命令への対応。
1-8.	広告ビジネスモデルへの利用者情報の活用状況	・別紙にて回答	・cookie等を利用し、広告配信事業者を介してインターネット上のさまざまなサイトやアプリにおいて、弊社の広告を掲載。	・広告ビジネスに、利用者情報を利用。 ・詳細は、「お客さま情報の利活用にあたってのプライバシー保護の取り組み」を参照。 https://www.softbank.jp/corp/privacy/utilization/	・利用者情報を利用した当該サービスに関する広告の提供。
1-9.	利用者のプロファイリング・セグメント化状況	・広告ビジネスにおいて、cookieや位置情報等を用いたプロファイリング・セグメント化を行う等の取組をしている。	・お客様に入力いただいた属性情報（性別・年齢・子供の有無など）をターゲティングセグメントとして用いるほか、各サービスの利用頻度や各種利用情報を分析・利用。	・年齢、性別、位置情報に基づいたセグメントを作成し、広告ビジネスに活用。 ・詳細は、「統計サービス・推奨型広告について」を参照。 https://www.softbank.jp/corp/privacy/utilization/ads/”	・特になし
1-10.	利用者情報、位置情報取得との関係での留意事項、参照している GL 等	・cookieの取得や利用にあたっての留意事項として、Webサイト等の利用者の導線上にて、パーソナルデータを利用している外部サービス（3rdパーティの情報収集モジュール等）を自動検出し通知する。（https://www.nttdocomo.co.jp/utility/term/） ・利用者情報、位置情報の取得及び利用においては、「電気通信事業における個人情報保護に関するガイドライン」、「位置情報プライバシーレポート」、「SPI」を遵守する。	▪お客様に対して取得データ・利用目的を明確に提示し、必要最低限かつ具体的なデータの取得・目的を提示して同意を取得。 ・位置情報のマーケティング利用・グループ会社へのマーケティング目的での第三者提供については、同意をいただいた後も撤回できるオプトアウト機能を提供。 ・「電気通信事業における個人情報保護に関するガイドライン」をはじめとした特定分野ガイドラインや、SPI、位置情報プライバシーレポート等を参照。	＜留意事項＞ ・法令やガイドラインの遵守に加え、（設問６のPIAに関連し）利用者情報や位置情報の利活用案件ごとに、プライバシーへの影響を、社内の専門組織が評価するとともに、必要に応じて、社外有識者への確認。 ・PIAでは、リスクの評価結果に応じて、リスクの低減を行い、また、お客さまに対しては、わかりやすさと詳細さのバランスを考慮した説明を行う等の取り組みを行っている。 ＜参照しているGL等＞ ・個人情報保護法関連の各種ガイドライン、電気通信事業法関連のガイドライン、位置情報プライバシーレポート、スマートフォンプライバシーイニシアティブ、カメラ画像利活用ガイドブック、AI・データの利用に関する契約ガイドライン、DX時代の企業のプライバシーガバナンスガイドブック等、政府の文書。 認定個人情報保護団体の指針や各種業界団体等のガイドブック、および、社内規定類。	・電気通信事業における個人情報保護に関するガイドライン ・電気通信事業における 「十分な匿名化」に関するガイドライン ・SPI ・位置情報プライバシーレポート ・同意取得の在り方に関する参照文書
２．利用規約・プライバシーポリシー					
プライバシーポリシー等					
2-1.	利用者情報の取扱いに係るプライバシーポリシーの内容	・「NTTドコモ　プライバシーポリシー」は、「NTTドコモ パーソナルデータ憲章」に基づき、パーソナルデータの取扱いに関する方針として「当社がパーソナルデータをどのように取扱っているのか」「お客さまが自分のパーソナルデータをどのように管理することができるのか」などを明らかにしている。具体的には、パーソナルデータの取得、利用目的、安全管理及びお客様問い合わせ窓口等を公表。 ・あわせて、お客様が各種サービスを利用される際のパーソナルデータの第三者提供について「パーソナルデータの取扱いに関する同意事項」として公表。	・1-10で記載しているガイドライン等を踏まえ、利用する情報や目的、その他必要事項を弊社方針として記載した「プライバシーポリシー」を制定・公開。また、アプリ毎に「アプリプライバシーポリシー」を制定し、アプリ特有の利用目的等を記載。 ＜参考＞ ・KDDI プライバシーポリシー (https://www.kddi.com/corporate/kddi/public/privacy/) ・アプリプライバシーポリシー（例： My auアプリ【iOS】） (https://www.kddi.com/app-policy/ios/app-policy-Myau-1.2.html)	・個人情報の取り扱いについては、個々のサービスでお客さまへのご説明が必要な場合は、各サービス約款・利用規約等に記載。また、個人情報の取り扱い全般をプライバシーポリシーに記載し、当社ホームページに公開。 プライバシーポリシー https://www.softbank.jp/corp/privacy/telecom/	・下記ページに集約。 https://corp.mobile.rakuten.co.jp/guide/privacy/
2-2.	サービス利用開始前の利用者への示し方、通知/同意取得の方法（導線及び掲載場所）	・「NTTドコモ　プライバシーポリシー」は、コーポレートサイトのトップページから1クリックで辿り着ける場所に配置。 ・個別のサービス利用申込みの際には、利用規約等にパーソナルデータの取扱いについて「NTTドコモ　プライバシーポリシー」にて公表している旨を定めている。	・各種サービスの契約・申込時にプライバシーポリシーを掲示しています。具体的には、WEB画面では申し込み動線の中で表示をしています。対面でのご案内の際は、重要事項説明書に利用目的を明示し、口頭でご案内している。	・プライバシーポリシーは、当社ホームページに公表し、また各サービス約款・利用規約は、必要に応じて当社ホームページ等に公表。お客さまがサービスをお申し込みされる際は、各サービス約款・利用規約及びプライバシーポリシーを通知し、同意を取得。例として、携帯電話の契約締結時には、ショップなどでお客さまに利用規約の説明を行い、同意を取得。	・上記の通り当社 Web サイト上に掲載し、いつでも誰でも閲覧可能な状態としている。また、アプリに関してはアプリからプライバシーポリシーにリンク可能な状態としている。 ・回線契約時やアプリ利用開始時にリンクを掲載し同意した上での申し込みを受けている。 ・位置情報等に関する情報に関しては、契約の申込みやアプリ利用開始時に別の利用の同意に関する文言を個別に明確に表示した上で承諾を取得している。（承諾をしないことも可能であり、また、同意しているユーザも事後のオプトアウトも可能としている。
2-3.	変更に際しての通知/同意取得の方法	・2019年12月の「NTTドコモ　プライバシーポリシー」再編の際に、３か月以上の周知期間を設けてdポイントクラブ会員向けにSMSやメール等によるプッシュ通知、郵送等による周知を徹底した。	・各サービスの利用規約等で情報の取り扱いについても規定しており、利用目的等を変更した際には都度同意をしていただく。また KDDIプライバシーポリシーについては、最新版を弊社HP上にて公表しているほか、通信サービスを含む各種サービスの契約タイミングで最新版のプライバシーポリシーを参照し同意をしていただく。	・軽微な修正の場合＊は、HPでお知らせを行っている。 ＊変更前の利用目的と関連性を有すると合理的に認められる範囲 重要な変更の場合には、一斉メール送付、サービス利用時等に同意取得を予定。	・目的の範囲内の変更についてはウェブサイト上で公開。 ・目的の範囲を超えた変更については現状実績なし。
2-4.	利用開始後（最初の同意・通知後）における、定期的な通知等の工夫	・定期的な通知はしていないが、利用者が同意した内容について容易に確認可能とする「パーソナルデータダッシュボード」のしくみを用意している。	・プライバシーポリシーの他、各サービスの利用規約および各アプリプライバシーポリシーに関しては、弊社HP上で最新版及び過去版を公表しているほか、特定のサービスについては、お客様のau ID アカウント管理画面上で、お客様が同意した規約バージョンの内容と最新バージョンの確認ができるようにしている。	・現在、利用開始後の定期的な通知は行っている。	・上記の通り当社 Web サイト上に掲載し、いつでも誰でも閲覧可能な状態としている。アプリに関してはアプリからプライバシーポリシーにリンク可能な状態としている。また、変更が生じる場合は、上記の通りウェブサイト上で公開。アプリに関しては再度ログインする場合等に同意を取得している。

社名		株式会社NTTドコモ	KDDI株式会社	ソフトバンク株式会社	楽天モバイル株式会社
透明性確保のための工夫					
2-5.	利用者情報の取扱いを分かりやすくするための考え方、工夫や対処 （利用者への働きかけや情報提供、ユーザーテストの実施等）	・「NTTドコモ　プライバシーポリシー」および関連コンテンツ「知ってナットク！ドコモのパーソナルデータ活用」「パーソナルデータダッシュボード」を公表している他、利用者の認知度・満足度等のアンケート調査を実施。 ・コロナ禍による位置情報への関心の高まりを受けて、「知ってナットク！ドコモのパーソナルデータ活用」のコンテンツを拡充（「ナットク！位置情報のトリセツ」）する等、継続的改善を実施。	▪プライバシーポリシーや各種利用規約の中で説明しきれない詳細な内容についてはプライバシーポータル （https://www.kddi.com/corporate/kddi/public/privacy-portal/）にて補足説明。 ・位置情報のマーケティング利用等、特定の同意事項に関してはオプトアウト機能を提供し、プライバシーポータルからオプトアウト機能へリンクするなどして、お客様のプライバシーに関わる情報をプライバシーポータルに集約。 ・プライバシーポータルの制作にあたってはユーザーテストを実施しており、今後もお客様のご意見や第三者の評価を踏まえたアップデートを継続的に実施予定。	＜考え方＞ ・利用者情報の取扱いを分かりやすくするため、以下のような考え方、世界観をもって、取り組んでいる。 ・重要なポイントをわかりやすく、Web等でコミュニケーションすることで ・手続きの負担感やわかりにくさを解消し ・お客さまが、いつでも確認して安心でき ・その時その時で、意思を反映・変更、開示請求もできる ＜利用者への働きかけ等＞ ・現在、さらに透明性を確保する具体的な工夫や対処を検討中。	・下記ページのようなイラストを用い概要説明する等の方法による情報提供。 https://corp.mobile.rakuten.co.jp/guide/privacy/
2-6.	同意取得/通知に際しての、利用規約やプライバシーポリシーを理解しやすくするための工夫 （階層的アプローチ、ダッシュボード、ジャストインタイム、アイコン、モバイル及びスマートデバイスの特徴の利用等）	・利用者が同意事項を確認できる「パーソナルデータダッシュボード」やパーソナルデータの活用例を例示する「知ってナットク！ドコモのパーソナルデータ活用」を公表。 ・アプリケーションプライバシーポリシー（以下「APP」）では、利用者にとって分かりやすい表示方法として、概要版の表示及び詳細版閲覧用のリンクを設けているほか、項目毎に開閉可能な階層型で作成する運用としている。	・2-5に記載しているとおり、プライバシーポータルでよりわかりやすい説明に努めている。同意画面や規約文章等についても、お客様のご意見や第三者の評価を踏まえ、継続的に改善を実施予定。	・お客さまが、利用規約やプライバシーポリシーを理解しやすくするため、現在、さらに透明性を確保する具体的な工夫を検討中。	・上記ページのとおり、個別のプライバシーポリシー以外にイラストを用いた全体のプライバシーポリシーの概要を設け、その下に個別の事業・アプリに応じたプライバシーポリシーを設ける階層的なアプローチをとっている。また、アプリに関しては、アプリからプライバシーポリシーにリンク可能な状態としている。
オプトアウト					
2-7.	利用者情報の提供を希望しない意思を示すオプトアウトの設置状況（方法、対象範囲等含む）	・利用者が自身のパーソナルデータの取扱いについて意思表示できる項目は、原則全て「パーソナルデータダッシュボード」から選択できるようにしている。 ・パートナーへの第三者提供については、提供情報（基本情報／利用情報／位置情報／医療健康情報）×提供先（ドコモグループ／dポイント加盟店／その他提携先）ごとに停止できるオプトアウトを用意。 ・位置情報の利用については、ドコモが利用しないように意思表示することができる設定変更画面を用意。	・位置情報のマーケティング利用・マーケティング利用目的でのグループ会社への第三者提供等の同意事項については、各同意の取得時、及び、au IDのアカウント管理画面にて、お客様がオプトアウトできる。また、GPS情報の取得についても、各取得アプリで取得の停止を行う事ができる。	・プライバシー保護の取り組みにおいて、公式アプリやMySoftBank（お客様向けの契約等を管理できるサイト）などで、統計サービス、推奨型広告、DM送付のオプトアウトを用意し、お客さま自らがこれらを利用停止できる手段を設けている。	・利用者情報に関してはプライバシーポリシーに基づき削除、停止等を認めている。 ・位置情報等に関する情報については、オプトアウトを認めている。
2-8.	オプトアウトをした場合のサービス利用継続の可否	・利用者が自身のパーソナルデータの取扱いについて意思表示できる項目は、原則全て「パーソナルデータダッシュボード」から選択できるようにしている。 ・利用者はオプトアウト後も継続してサービスを利用できるようにしている。	・2-7に記載のオプトアウトを行った場合でも、各サービスの利用は継続可能。	・利用継続は可能。	・利用者情報に関しては、サービスを継続したままオプトアウトできる範囲はプライバシーポリシーで認められた範囲のみ。 ・位置情報等に関する情報についてはオプトアウトしたままでサービス利用継続可能。
2-9.	利用者情報の提供について個別に選択できるダッシュボード等の設置状況（方法、対象範囲等含む）	・利用者が自身のパーソナルデータの取扱いについて意思表示できる項目は、原則全て「パーソナルデータダッシュボード」から選択できるようにしている。 ・「パーソナルデータダッシュボード」では、「第三者提供の管理」「位置情報利用の管理」「お知らせ配信の設定」「dアカウント連携サービスの変更」が可能。	・2-7に記載のオプトアウトやメールマガジンの停止等の手続きについて、プライバシーポータルに動線を設置。	・現在、個別に選択できるダッシュボード等を検討中。	・2－5、2－6 記載のもの。
データポータビリティ					
2-10.	データポータビリティに関する取組 （データポーテビリティーを求める方法、対象範囲）	・現時点ではデータポータビリティに対応していない。	・ユーザニーズや事業分野ごとの必要性に応じて実施を検討する。	・現在は対応していない。	・なし
2-11.	データポータビリティが可能である場合 ・提供されるデータのフォーマット ・提供先の要件 ・インターオペラビリティ確保に関する考慮状況	・現時点ではデータポータビリティに対応していない。	回答なし	・N/A	回答なし
2-12.	個人情報保護法に基づく開示請求への対応状況 （電磁的な開示の実施状況、開示請求の方法、提供フォーマット等）	・開示請求方法は、「個人情報開示申請書」と本人確認書類を弊社宛に郵送し、契約者本人宛に回答を送付する形。 ・紙面による開示を行っており、電磁的方法による開示は行っていない。 ・開示請求手続方法は、「NTTドコモ　プライバシーポリシー」にて公表。 （https://www.nttdocomo.co.jp/utility/personal_data/request/?icid=CRP_UTI_privacy_to_CRP_UTI_personal_data_request）	・現状は、申請書を書面にて送付いただく形で受け付け、書面にて開示をしている。 ・また電磁的な開示については、個人情報保護法の改正に従い、対応を実施する予定。	＜現行法での対応状況＞ ・コールセンターに「個人情報専用窓口」を設け、専門スタッフが個人情報責任部署や関係部門と連携し、お客さまへの開示等請求対応を行っている。現在の提供フォーマットは文書。 ＜改正法での電磁的な開示＞ ・本年5月頃に予定されている個人情報保護委員会のガイドライン案の公表を確認の上、電磁的なフォーマットでの提供を検討する。	・下記 https://corp.mobile.rakuten.co.jp/guide/privacy/request/index.html
３．他アプリやサイトを経由した情報収集の状況					
3-1.	他アプリやサイトを経由した情報収集の状況	・パートナーのWebサイトで、ドコモの情報収集モジュールによりcookie等の情報を取得する場合がある。	・実施していない。	・まもなくサービス終了予定だが、以下の収集を行っている。 ・自社広告タグとして「SB AdsPlatforrm」タグをサービス提供 ・他社広告のインプレッション計測に当社1stPartyタグを使用 ・なお、他社にSBタグを置いて、SBがデータを吸い上げている事例はない。	・特になし
3-2.	他アプリ提供者やサイト運営者に対し、どのような同意取得や通知を促しているか	・Webサイト運営者がドコモの情報収集モジュールを導入する際の契約において、所定のWebページへのリンクを表示する等、Webサイト訪問者への説明を行うことを定めている。 （https://www.nttdocomo.co.jp/utility/term/handling_information.html）	回答なし	・まもなくサービス終了予定だが、「SB AdsPlatform」のタグ提供時に、ユーザー向けのオプトアウト画面のURLを提供。	回答なし
3-3.	JavaScript の取扱状況 （後から情報取得内容が変更されることについて、他アプリ提供者やサイト運営者にどのように伝えているか等）	・JavaScript自体の詳細仕様は開示していないが、取得している情報やオプトアウト方法は公表。 （https://www.nttdocomo.co.jp/utility/term/handling_information.html）	回答なし	・過去に仕様変更を実施していないが、変更する際はサイト運営者に都度案内を実施する運用ルールとなっている。	回答なし
3-4.	複数の他アプリやサイトから収集している場合の、情報管理状況	・複数のサイトから収集した情報について、dアカウントで認証されたユーザのデータを統合管理している。	回答なし	・現在他アプリや、他サイトから個人情報を収集していませんが、今後行う場合は自社が取得した情報と混在しないよう情報管理し、安全管理を行う。	回答なし

社名		株式会社NTTドコモ	KDDI株式会社	ソフトバンク株式会社	楽天モバイル株式会社
４．他社へのデータ提供、他社との連携の状況					
4-1.	他社に対する、取得した利用者情報・位置情報に基づくデータ提供の内容、提供に関する留意点（ユーザーへの説明、他社の監督、安全管理など）	・「基本情報」「利用情報」「位置情報」「医療健康情報」について同意を得たものについて、パートナーとの協業等のために必要最小限のデータを第三者提供している。 ・第三者提供にあたっては、提供情報、提供先、提供先の利用目的を定めた上で利用者の同意を得るようにしている。 ・提供先における利用目的は、利用者から同意を得た範囲から逸脱しないよう、提供先との二者間の契約等においても定めている。 ・業務委託に伴う提供においては、個人データの安全管理について委託先の監督を行っている。	・お客様から第三者提供の同意をいただいた範囲内のデータ・利用目的で他社に対してデータ提供を行う事がある。 ・利用者情報、位置情報の提供に際しては、目的に応じて集計・セグメント化等を行い、必要最低限の情報の提供を行うように留意。 ・第三者提供先に対しては、記録義務等の法律で求められる事項の他、社間での契約を締結し、目的外利用を禁止。また、弊社からの第三者提供先の大半を占めるグループ会社に対しては、コンプライアンス・情報セキュリティ等の観点でガバナンスを徹底し、お客様データを適正に取り扱っている。 ・第三者提供に際し、au IDアカウント管理画面内で同意の撤回（オプトアウト）を行うようなことができるようにしている。	＜お客さまへの説明＞ ・他社への提供は、個々のサービス約款・利用規約等及びプライバシーポリシーに、第三者提供を明記のうえ、お客さまに通知し、同意を取得している。また、提供を望まないお客さま向けにオプトアウトを用意。 ＜他社の監督・安全管理＞ ・委託先： 契約時に、安全管理措置についての契約条項を盛り込むと共に、締結後もデータ取り扱いの実地監査など、適切な安全管理措置が行われているか、監督を行っている。 ・第三者提供先： 契約時に、再提供、派生データの作成、公表、利用終了後の削除、などの禁止または報告義務などを取り決めている。 また、利用終了後の削除などの確認、安全管理を行っている。”	・楽天グループ内でのデータ提供あり。2−5、2−6のとおり、イラストを用い概要説明する等の方法による分かりやすい説明を実施。第三者提供にあたっては、ガイドラインに従った安全管理を実施。
4-2.	利用者情報・位置情報の取得・活用に関する、他社との連携状況、連携に関する留意点（ユーザーへの説明、他社の監督、安全管理等）	・ID連携、ポイント連携、決済連携、サービスの共同開発、その他付加価値創出を行う。 ・他社との連携においてはそれぞれが独立した取扱い主体として利用者への説明責任を果たし、提供されたデータの目的外利用の禁止等を明確化。	・グループ会社とサービスの提供や各種特典・割引サービスの提供等のため情報の連携を行っている。提供にあたっての留意点は4-1に記載の内容と同様。また、お客様への最適な情報提供のためにも連携をおこなっているが、au IDアカウント管理画面内で同意の撤回（オプトアウト）を行うことができる。	・個々のサービス利用前にサービスの約款・利用規約等で説明を行い、法令の必要に応じた同意取得を行っている。 なお、位置情報の利活用については、HPで図を交えた説明を行っている。 ●お客さま情報の利活用にあたってのプライバシー保護の取り組み https://www.softbank.jp/corp/privacy/utilization/ ●推奨型広告・統計サービス https://www.softbank.jp/corp/privacy/utilization/ads/ （具体例は、スライドを参照）	・楽天グループからの提供。プライバシーポリシーにおいて説明。ガイドラインに従った安全管理を実施。
５．アプリ提供マーケット					
5-1.	SPI に関する取組状況	・当社が開発するアプリケーションについては、スマートフォンプライバシーイニシアティブ（以下「SPI」）を参照し、APPの概要版・詳細版にて規定すべき項目、画面デザインや画面遷移等に関する社内マニュアルを策定し、マニュアル策定部門や関連部門の照会を経てAPPを策定しアプリケーションへ組み込む運用をしている。	・社内規程を作成し、弊社のお客さま向けに提供しているアプリについてはアプリプラバシーポリシー作成の義務化に加え、SPI Ⅱで推奨される監査まで実施している。また、KDDIが提供するお客様向けアプリすべてにおいて、全社ガイドラインをもとに、プライバシーポリシーに即した挙動となっているか審査を行っている。	・アプリマーケットの運営は行っておらず、アプリケーション提供者の立場のみとなる。 ・アプリによる情報収集は、アプリに組み込むSDKを含め、アプリ毎に収集する情報と提供先をレビューした上で、アプリ利用者へのコミュニケーションの在り方を指導している。	・アプリ提供マーケットの運営は現状なし。
5-2.	アプリケーションプライバシーポリシーの作成や利用者情報取扱いの透明性確保の観点からのアプリ提供者に対する働きかけや情報提供	・当社が開発するアプリケーションについては、SPIを参照して社内マニュアルを整備し、アプリ提供主管部門はマニュアル策定部門への照会を必須とする運用フローを実施している。 ・同意画面は、利用者にとって分かりやすい表示方法として、アプリケーションプライバシーポリシー概要版の表示及び詳細版閲覧用のリンクを設けているほか、項目毎に開閉可能な階層型で作成する運用としている。	・弊社アプリ提供PF上で提供するアプリに対して、SPI提唱項目に準拠したアプリプライバシーポリシーの開示を必須化し、利用者情報の送信に関する透明性の確保に努めている。	・アプリマーケットの運営は行っていない。	回答なし
６．PIA・アウトカムについての考え方					
6-1.	PIA の導入状況 （GDPR の DPIA の具体的なに実施方法や、その他の実施事例）	・パーソナルデータの取り扱いにおける理念を明確化し、自らを規律するものとして、「NTTドコモ　パーソナルデータ憲章」を制定。 ・パーソナルデータを利用する際に憲章に沿った実行性を担保するために、プライバシー影響評価制度（PIA制度）を導入。 ・PIA制度の仕組みとして、まず、パーソナルデータを活用した施策・サービスを実施するにあたっては、必ずデータ活用部門自らがプライバシー観点での懸念点の有無などについて自己評価し、必要なプライバシー保護施策を検討するとともに、評価結果に基づき施策・サービスの実施是非を判断することとしている。 ・さらに、一定の基準に該当するパーソナルデータ活用事案については、社内のPIA会議でプライバシーへの影響を評価している（詳細は6-2のとおり）。	・GDPRの規制対象の範囲内では実施の体制を整備。今後、GDPRの規制対象以外についても社内制度を現在検討中。	・CDO（Chief Data Officer)を責任者とし、社長をレポートラインとする全社横断の専門組織にて、プライバシー・バイ・デザインの考え方で、データ利活用前に案件ごと＊のPIA（リスクの評価）を行っている。 ＊通信の秘密、個人情報、その他プライバシー情報を扱う案件は全件確認している。	構成員限り
6-2.	利用者情報の取扱いに関するアウトカムについての検討状況 （検討している場合、どのような考え方に基づき判断しているか）	・社内にプライバシー影響評価に関する諮問機関であるPIA会議を設置し、活用するパーソナルデータの性質や利用態様に応じた付議基準を設け、一定のパーソナルデータ活用事案については、データ活用部門による自己評価に加え、PIA会議において多角的な視点からプライバシーへの影響を評価する仕組みを設けている。 ・自己評価のみの場合もPIA会議で議論する場合も、パーソナルデータ憲章に反していないか、お客様や社会から受容していただけるかどうかという観点で、リスク評価を実施している。	・6-1とあわせ、必要な対応を検討している。	・PIA時、アウトカムについて、検討を行っている。 ＜判断にあたっての考え方＞ ・さまざまな関係者にとって 利益・便益というプラスの側面と、不利益や気持ち悪さなどネガティブな側面、双方から確認している。 具体的には、 ・お客さまにとって： 　便益につながる利用か？、不利益は生じないか？、プライバシー侵害にあたらないか？、気持ち悪さはないか？など ・事業者にとって： 　利用目的の範囲か？、必要な利用か？、価値を生む利用か？、利用環境、利用者、廃棄など安全管理に問題はないか？など ・社会にとって： 　社会的に価値ある利用か？、漏えいした場合のリスクの程度は大きいか？など	構成員限り

社名		株式会社NTTドコモ	KDDI株式会社	ソフトバンク株式会社	楽天モバイル株式会社
6-3.	利用者に対する、PIA の結果やアウトカムの説明の取組状況	・PIAの結果については、現状お客様に説明する取り組みは行っていない。 なお、当社としては、お客様にとって重要なのは、事業者がどのようにプライバシー影響を評価しているかではなく、実際に「どのような情報がどのような目的で利用されるのか」、「どのようなメリットがあるのか」、「取得・利用等を停止・拒否する手段はあるのか」という点だと考えており、それらの内容を含む施策・サービス等に係る報道発表やホームページ、同意取得時の説明ページなどにおいてご案内をするよう努めている。	・6-1とあわせ、必要な対応を検討している。	サービスの案内時や、ご利用開始前に、特にお客さまが気にされるだろうポイントに留意して説明を行っています。 なお、その説明の程度は、わかりやすさと透明性のバランスをはかるため、PIAの結果やアウトカムに応じて、説明の詳しさを変える取り組みを行っています。	構成員限り

別紙

利用者情報・位置情報の取得・分析・活用の例示

<table>
<tr><th colspan="2">項目</th><th>取得内容</th><th>同意取得場面</th><th>利用者情報・位置情報の取得場面</th><th>活用・分析・利用状況</th><th>第三者提供</th><th>統計加工利用</th></tr>
<tr><td rowspan="5">利用者情報</td><td>契約者情報</td><td>・氏名、住所、性別、生年月日、電話番号等</td><td>・携帯電話サービス契約時</td><td>・携帯電話サービス契約時</td><td rowspan="6">・ご契約内容に基づく各種サービス・機能の提供
・自社サービスの品質維持・向上
・自社サービス・アプリ・システム等の保全
・新商品や新サービスの企画、アンケート分析
・キャンペーン提案等、広告ビジネス活用</td><td rowspan="6">・パートナーとの協業に必要とする 同意の範囲内でパートナー企業へ提供</td><td rowspan="5">・自社サービスの品質維持・向上
・自社サービス・アプリ・システム等の保全
・新商品や新サービスの企画、アンケート分析</td></tr>
<tr><td>会員情報</td><td>・氏名、住所、性別、生年月日、職業、メールアドレス、ｄアカウントID、ｄポイントクラブ会員番号、端末識別子等</td><td>・ｄポイントクラブ会員加入時</td><td>・ｄポイントクラブ会員加入時</td></tr>
<tr><td>WEB・アプリ利用情報
ｄメニュー利用履歴</td><td>・訪問したWEBサイトの閲覧履歴、 cookie情報等
・アプリ起動回数等のアプリ利用ログ</td><td>・ｄポイントクラブ会員加入時
・アプリケーション利用開始時</td><td>・WEBサイトやアプリ利用等、当社サービス又は当社以外のサービス利用時</td></tr>
<tr><td>購買・決済情報</td><td>・ｄカー ド、ｄ払い等の決済利用情報等
・ｄポイントカード等の利用履歴等情報
・ケータイ払い購入商品、金額等</td><td>・ｄポイントクラブ会員加入時
・ｄカード契約時</td><td>・ｄカード、ｄ払い、、ケータイ払い ｄポイントカード等、当社サービス利用時</td></tr>
<tr><td>趣味・嗜好</td><td>・dポイントクラブアンケートにより取得した情報</td><td>・ｄポイントクラブ会員加入時</td><td>・ｄポイントクラブアンケート回答時</td></tr>
<tr><td colspan="2">位置情報</td><td>・アプリによる端末上の位置情報へのアクセスを許可設定した端末から取得するGPS位置情報
・端末の在圏情報（基地局位置情報）、 Wi-Fi 位置情報（アクセスポイントに関する情報）等</td><td>・ｄポイントクラブ会員加入時
・アプリケーション利用開始時</td><td>・端末の在圏登録時、dWi-Fiアクセスポイント通信時、当社サービス利用時等</td><td>・端末の在圏情報（基地局位置情報）について、非識別化処理・集計処理・秘匿処理による個人識別性の除去等を行ったうえで人口統計情報化し、「モバイル空間統計」としてサービス提供</td></tr>
</table>

参考９－２

プラットフォーム事業者における利用者情報の取扱い状況　ヒアリングシートにおける主な項目の比較

	社名	Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
	最新の情報	https://www.apple.com/jp/privacy/	https://ja-jp.facebook.com/policy.php	https://policies.google.com/privacy?hl=ja	https://line.me/ja/terms/policy/	https://privacy.yahoo.co.jp/
	事業領域	IT機器の製造・販売、ソフトウェア、各種サービスの提供	オンライン・ソーシャル・ネットワーキング・ウェブサイト及びこれに関連するサービス等	・検索エンジン提供 ・広告事業　等	・SNSサービス ・広告事業 ・コンテンツ販売　等	・検索エンジン提供 ・広告事業（メディア事業） ・EC事業　等
1. 利用者情報の取扱いの状況						
1-1.	利用者情報取得の場面・取得する情報の内容	**「プライバシーは基本的人権である」として、消費者のプライバシー保護に責任をもって取り組んでいる。Appleのプライバシーへのアプローチは、4つのプライバシーの柱があり（「データの最小化」「デバイス上の知能」「透明性とコントロール」「セキュリティ保護」）、これらは、プライバシーについてAppleが行っていることすべての基礎となっている。** **・Appleは、革新的なテクノロジーと技術を利用して、Apple、そして他の人がアクセスできる個人情報を最小限（「データの最小化」）にしており、取得するデータが最小限になるように取り組んでいる。** 【取得の場面】 ・Apple ID の作成 ・デバイスの購入、アクティベーション ・ソフトウェアアップデート ・Apple のサービスへの接続 等 【情報の内容】 ・アカウント情報：Eメールアドレス、登録されているデバイス、アカウントのステータス、年齢など、Apple ID など ・デバイス情報：デバイスを特定できるデータ（デバイスのシリアル番号など）、デバイスに関するデータ（ブラウザのタイプなど） ・連絡先情報：名前、Eメールアドレス、住所、電話番号など ・支払い情報：銀行口座の詳細、請求先住所、クレジットカード情報などの支払い方法など ・取引情報：Apple の製品とサービスの購入に関するデータ、Appleのプラットフォームでの購入に関するデータなど ・不正防止情報：デバイストラストスコアなど ・使用状況データ：Apple の製品やサービスの使用に関するデータ（閲覧履歴、検索履歴、製品の操作、クラッシュデータ、パフォーマンスなどの診断データなど） ・位置情報：「探す」のサポートのみを目的とした詳細な位置情報と、おおよその位置情報。※ユーザーは位置情報の提供を拒否設定できる。 ・健康に関する情報：個人の健康状態に関するデータ ・フィットネス情報：ユーザーが共有することを選択したフィットネスとエクササイズの情報 ・財務情報：給与、所得、資産について収集された情報、Apple のブランドの金融サービスに関する情報 ・政府発行のIDデータ：特定の地域で、ワイヤレスアカウントの設定やデバイスのアクティベーションをする場合など限られた状況において、政府発行のID を要求 ・ユーザーから提供されるその他の情報：カスタマーサポートとのやり取り等、Apple とのコミュニケーションの内容などの詳細 （Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/））	・利用者の興味・関心に合わせたサービスを提供するために、個人データを使用する。 ・Facebook、Instagram及びMessengerの各サービスを提供する際に、利用者に関する情報を(i)利用者等が実行および提供するもの、(ii)デバイス情報及び(iii)パートナーからの情報という3つの基本カテゴリで受領する。 ・Facebook社が提供するサービスへの参加を希望する利用者が提供を求められる情報は、氏名、メールアドレス又は電話番号、性別、生年月日。 ・Instagramへの参加を希望する利用者が提供を求められる情報は、メールアドレス又は電話番号及び生年月日。 ・利用者は、自らの選択により、自身の住所、言語、学歴、仕事、趣味及び好きな映画や本、音楽に関する情報等、プロフィールの追加情報を当社に提供することもできる。 ・利用者の当社サービスとのエンゲージメントに関する情報も収集される。この利用者のエンゲージメントに関する情報には、例えば、利用者が「いいね！」ボタンを押したFacebookページ、利用者が参加しているFacebookグループ、利用者が使用している他のアカウント、利用者が閲覧するコンテンツ、プラットフォームにアップロードするコンテンツ（投稿、写真、動画、ストーリー等）及び任意で行うフィードバック（広告が不適切であり又は関連性がないこと等）が含まれる。 ・以下のような、自社のサービスと統合された、利用者が利用するデバイスからの情報、及び当該デバイスに関する情報を収集する。 　－ デバイスの特質: オペレーティングシステム、ハードウェアとソフトウェアのバージョン、電池レベル、信号強度、ストレージの空き容量、ブラウザーの種類、アプリとファイルの名称と種類、プラグインなどの情報。 　－ デバイスの操作: デバイス上で行われる操作と行動、ウィンドウが前景か背景であるか、マウスの動き(ボットの識別に役立てることが可能)などの情報。 　－ 識別情報: 利用者が利用するゲーム、アプリ、アカウントからの固有の識別情報、デバイスID、その他の識別情報、およびFamily Device ID(または、同じデバイスやアカウントに関連付けられているFacebookグループ企業の製品に固有の他の識別情報)。 　－ デバイスの信号:Bluetoothシグナル、および近くのWi-Fiアクセスポイント、ビーコン、セルタワーに関する情報。 　－ デバイス設定データ: GPSの位置情報、カメラ、写真など、デバイス設定で有効にすることにより利用者が弊社のアクセスを認めている情報。 　－ ネットワークおよび接続: 携帯電話会社名、インターネットサービスプロバイダー名、言語、タイムゾーン、携帯電話番号、IPアドレス、接続速度、場合によっては近くにあるまたはネットワーク上にある他のデバイスに関する情報など、当社が利用者の利用を手助けするための情報(動画を携帯電話からテレビにストリーミングするなど)。 　－ Cookieデータ: 使用デバイスに保存されたCookieデータ(CookieのIDや設定など)。	・Google は、すべてのユーザーによりよいサービスを提供するために情報を収集する。ユーザーの使用言語といった基本的な事項を理解することや、ユーザーにとって最も役に立つ広告はどの広告か（https://policies.google.com/privacy?hl=ja#footnote-useful-ads）、おすすめの YouTube 動画はどれか、などの複雑な事項を推定することが含まれる。 ・Google がどの情報を収集するか、その情報がどのように使用されるかは、ユーザーがどのように Google のサービスを利用するか、またプライバシー設定をどのように管理するかによって変わる。Googleはユーザーが作成し、提供する情報（例えばGoogleアカウント）、Googleのサービスにアクセスするために利用するアプリやブラウザ及びデバイスに関する情報を収集し、おすすめのYouTube動画を提示するなどユーザーにより役立つ情報を提供するために活用している。また、Google サービス利用時の位置情報も収集するが、ユーザーは Googleアカウントにアクセスして、Googleに共有する情報や位置情報のような情報をいつ削除するかを確認、管理することができる。Googleは、包括的なプライバシーポリシー（https://policies.google.com/privacy?hl=ja#infochoices）により、ユーザーがどのように自らのデータを管理できるのかを分かりやすく示している。	・主にユーザーのアカウント開設やサービス利用の場面において、電話番号、プロフィールネーム、プロフィール画像、 氏名、住所、生年月日、メールアドレス、サービス利用履歴等の情報を取得している。 ・利用者情報取得の場面及び取得する情報の詳細は、プライバシーポリシーに記載し、公表している。https://line.me/ja/terms/policy/	・ユーザーのパーソナルデータについては、プライバシーポリシーに基づき取得している。パーソナルデータの取得場面および取得する情報の内容は、次のとおり。 ①端末操作を通じてユーザーが入力する場合 　－ Yahoo! JAPAN IDを取得する際に入力される氏名、住所、電話番号等の登録情報 ②ユーザーから直接または書面等の媒体を通じて提供される場合 　－ ユーザーから送付される本人確認書類等に記載されたパーソナルデータ ③ユーザーによるサービス等の利用・閲覧に伴って自動的に送信される場合 　－ Yahoo! JAPANのウェブページへのアクセスに伴って送信されたIPアドレス 　－ Yahoo! JAPANのウェブページの閲覧履歴 　－ Yahoo! JAPANの検索機能を利用する際に入力された検索キーワード 　－ Yahoo! JAPANのショッピングサービスでの購買履歴 　－ Yahoo!防災速報、Yahoo!天気、Yahoo! MAP等をインストールされている端末の位置情報（ユーザーの利用端末の設定が有効になっている場合） 　－ Yahoo! JAPANの広告主や広告配信先等のウェブページやアプリに設置されたウェブビーコン等により取得するユーザーの利用端末を識別するための情報等 ④第三者から情報の提供を受ける場合 　－ Yahoo! JAPAN以外の第三者が取得した情報の提供を受けることで、パーソナルデータとして取得する場合がある。 ・上記は当社のプライバシーセンター（https://privacy.yahoo.co.jp/）の「パーソナルデータの取得」においてユーザーに対して詳細を説明している。 ※「サービス等」とは、サービス、商品、広告、コンテンツを指します。なお、サービス等は、パートナー向けおよびご本人以外のお客様向けのサービス、商品、広告、コンテンツを含む。
1-2.	取得情報の加工・分析・利用状況	・Appleがユーザーの個人データを使用するのは、個人データを使用する正当な法的根拠がある場合のみである。Appleは状況に応じて、ユーザーの同意に基づいて、またはユーザーとの契約を履行するため、ユーザーや他者の重大な利益を保護するため、もしくは法令を遵守するために個人データの処理が必要であるという事実に基づいて、個人データを使用することがある。また、Appleは、ユーザーの利益、権利および期待を考慮して、個人データを処理することがAppleまたは他者の正当な利益にかなうと考える場合、個人データを処理することがある。 ・サービスの強化：製品やサービスのパーソナライズ・改善。また、監査やデータ分析、トラブルシューティングなど。 ・取引の処理：ユーザーとの取引の処理 ・ユーザーとのコミュニケーション：取引やアカウントについての連絡、製品やサービスのマーケティングのための関連情報の提供等。 ・セキュリティおよび不正防止：損失防止、不正防止。児童ポルノ排除のための事前スクリーニング・スキャニングを含む。 ・法令遵守：適用法令の遵守のための利用 （Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/））	・利用者のための当社の製品及びサービスの提供、パーソナライズ化及び改善 　（i）機能及びコンテンツ（ニュースフィード及び広告など）のパーソナライズ化並びに、利用者に合わせたコンテンツを推奨し、（ii）よりパーソナライズ化され、広告支援サービス（Facebookのサービス、Instagram及びMessengerを含む。）において整合的な体験を提供するために情報の連結し、（iii）それらのサービスの開発、検証及び改善といった弊社のサービスを提供及び改善するために受領した情報を利用する。 ・測定、分析及びその他のビジネスサービスの提供 　保有する情報(訪問したウェブサイトや閲覧した広告など、利用者の当社製品外におけるアクティビティを含む)を、広告主などのパートナーが広告効果やサービス利用状況を測定し、そのパートナーのウェブサイト、アプリ、サービスをどのようなタイプの人々が利用し、どのように反応しているかを分析できるようにする目的で使用する。これにより、広告主は、高度な透明性及び測定にかかる知見を得られるとともに、より効果的な広告予算の活用方法に関する十分な情報に基づく意思決定が可能となる。 ・安全性、健全性及びセキュリティの促進 　保有する情報を、アカウントとアクティビティの認証、悪質な行為への対処、スパムなどの問題の検知と防止、当社製品の保全維持、当社製品の内外における安全とセキュリティの推進のために利用する。 ・公益目的のための研究及びイノベーション 　一般社会福祉、技術進歩、公共の利益及び健康と福祉といったトピックに関する研究及びイノベーションの実施及び支援を目的として、受領した情報（当社と協働する選び抜かれた研究パートナーからの情報など）を利用する。例えば、弊社は救助活動を支援するために、災害発生時の避難行動パターンに関する情報を分析する。	・サービスの提供 　ユーザーの情報を、サービスを提供するために使用する。たとえば、検索キーワードを処理して結果を表示するため、ユーザーの連絡先から共有相手の候補を表示してコンテンツを共有しやすくするためなどに使用する。 ・サービスの維持、向上 　ユーザーの情報を、サービスを意図したとおりに稼動させるために使用する。たとえば、障害事例を追跡するため、あるいは報告をいただいた問題の解決に取り組むためなどに使用する。また、ユーザーの情報を、Google のサービスを向上させるために使用する。たとえば、特にスペルミスの多い検索キーワードを把握し、各種サービスでのスペルチェック機能の向上に役立てる。 ・新しいサービスの開発 　既存のサービスで収集した情報を、新しいサービスの開発に役立てる。たとえば、Picasa（Google の最初の写真アプリ）でユーザーがどのように写真を整理するかを把握したことが、Google フォトの設計とサービス開始に役立った。 ・コンテンツや広告など、カスタマイズしたサービス提供 　Googleのサービスを個々のユーザーに合わせてカスタマイズするために、収集した情報を使用する。たとえば、おすすめ情報を表示する、カスタマイズしたコンテンツを表示する、カスタマイズした検索結果（https://policies.google.com/privacy?hl=ja#footnote-customized-search）を表示するなどの目的で使用する。 ・パフォーマンス測定 　Google のサービスがどのように利用されているのかを把握するために、分析や測定のためのデータを使用する。たとえば、Google のサイトへのユーザーのアクセスに関するデータを分析して、サービス デザインの最適化などに役立てる。また、広告主が広告キャンペーンの効果を把握できるよう支援するために、ユーザーが操作した広告に関するデータを使用する。 ・ユーザーの皆さまとのコミュニケーション ・Google、Google のユーザー、一般の人々の保護 　Googleは、収集した情報をGoogleのサービスの安全性と信頼性（https://policies.google.com/privacy?hl=ja#footnote-safety-reliability）を向上させる取り組みに使用する。こうした取り組みには、Google、Google のユーザー、もしくは一般の人々に害を及ぼすおそれのある不正行為、不正使用、セキュリティ リスク、または技術的な問題の検知、防止、対応などがある。	取得した情報は、必要に応じて加工・分析した上、以下のような目的で利用している。 ①サービスの提供・維持 ・ ログイン時の認証 ・ メッセージの送信 ・ ユーザーへの連絡 等 ②当社サービスやコンテンツの開発・改善 ・ サ ービス利用に関する統計の作成 ・ ユーザーの購入履歴からトレンドを把握して新規サービスの開発を行う ・ サ ービスの利用状況を基に画面デザインの改善を行う 等 ③セキュリティ・ 不正利用の防止 ・ 利用規約違反、不正アクセスなど、不正利用の有無の確認 ・ 不正利用が発生した場合のユーザーへの連絡 等 ④ユーザーに最適化されたコンテンツの提供 ・ ユーザーが購入したスタンプと関連する他のスタンプを推薦する ・ ユーザーのサービス利用状況等を基に広告を配信する 等 取得情報の利用状況の詳細は、プライバシーポリシーに記載し、公表している。https://line.me/ja/terms/policy/	・取得したパーソナルデータをサービス等の提供（ユーザーからの問い合わせへの対応、ユーザーへのお知らせ、適切かつ安全なサービス等の提供のための不正対策を含む）、改善や新たなサービス等の検討、サービス等のご利用状況等の調査、分析に利用する。具体的には次のとおり。 ①ログインの際の認証 ②パーソナライズ 　個々のユーザーに最適なコンテンツをはじめとするサービス等を提供する場合（おすすめの商品やサービス等を表示したり、案内したりする場合を含む）に、ユーザーの居住地域、性別、生年月等の情報や、ユーザーのサービス等の利用履歴（検索キーワード、閲覧されたウェブページ、利用されたアプリ、購入された商品等）を分析して、Yahoo! JAPAN独自の基準で推定したユーザーの興味関心に関する情報を利用する。 ③サービス等の改善・新たなサービス等の検討 　ユーザーが、どのような場所から、どのようにサービス等を利用したのかという情報をもとにユーザーのサービス等に対するニーズを分析して、サービス等の改善や新たなサービス等の検討をするために、ユーザーの居住地域、性別、生年月等の情報や、ユーザーのサービス等のご利用履歴（検索キーワード、閲覧されたウェブページ、ご利用になったアプリ、購入された商品等）を利用する。 ④広告の表示 　個々のユーザーのニーズに即した、より適切な広告が表示されるように、ユーザーの居住地域、性別、生年月等の情報を利用し、また、ユーザーのサービス等の利用履歴（検索キーワード、閲覧されたウェブページ、利用されたアプリ、購入された商品、位置情報等）や提供を受けた情報を分析してYahoo! JAPAN独自の基準で推定したユーザーの興味関心に関する情報を利用する。※複数の環境（端末、アプリ、ブラウザー等）の情報を利用する場合がある。 ⑤入力補助等 ⑥本人確認等 ⑦問合せ対応 ⑧代金請求 ⑨お知らせ等の連絡や送付 ⑩位置情報と連動したサービス等の提供 　Yahoo!カーナビでルート案内をしたり、Yahoo! MAPでユーザーの現在地を表示したりする場合に利用する。また、ユーザーが現在いる地域の災害に関する情報をタイムリーに提供する等、サービス等の提供に不可欠な場合のほか、ユーザーにより一層快適にサービス等を利用いただくために利用する。 ⑪メールの解析による便利機能の提供、広告の最適化 　Yahoo!メールで送受信されるメールを機械的に解析した結果を利用し、より便利にYahoo!メールを使うための機能を提供したり、ユーザーの関心と関連性が高いと判定された広告やお知らせを配信したりしている。 ⑫迷惑行為・不正利用の対策 ⑬企業や自治体での統計データの活用 ⑭通信環境改善 ⑮利用状況等の調査・分析 　サービス等の利用者数やYahoo! JAPANやパートナーが配信する広告の閲覧数、クリック数等を調査・分析するために、ユーザーによるサービス等の利用履歴を利用する。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
1-3.	**利用者情報の第三者提供の状況**	・Appleは、Appleを代理して行動するサービスプロバイダと、当社のパートナーと、またはお客様の指示を受けてその他の第三者と、 個人データを共有することがある。また、Appleは第三者自身のマーケティングを目的として第三者と個人データを共有することはない。 ・サービスプロバイダ：サービスプロバイダとして特定のタスク（製品の顧客への配達など）を行う契約を結んだ第三者。本プライバシーポリシーに準拠し、Apple の指示に従って個人データを取り扱う義務を負う。Apple が提供する個人データを自らの目的のために使用することはできず、Apple の要請実行後は個人データを削除または返却する。 ・パートナー：サービス・製品を提供するための連携先。 ・アフィリエイト：パフォーマンスCookie が、ユーザーがアフィリエイトサイトからApple のウェブサイトにアクセスし、製品を購入したりサービスを利用したことを、その詳細含めのアフィリエイトに知らせる。個人を特定できる情報は収集せず、収集した情報は集計するため、匿名性が保たれている。 ・その他：ユーザーの同意を取得した場合など （Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/）、 AppleによるCookieの使用について （https://www.apple.com/jp/legal/privacy/jp/cookies/）） ・Appleの広告プラットフォームはユーザーを追跡しない。 ・AppleのAppから収集したユーザーやデバイスのデータを、他社製Appから収集されたユーザーやデバイスのデータと組み合わせてターゲティング広告または広告測定のために使用しない。 ・AppleのAppから収集したユーザーやデバイスのデータをデータブローカーと共有しない。 ・コンテクスト情報：広告を提供するために、以下のコンテクスト情報を使用する。広告は、複数のユーザーから集約して作成するセグメント情報に基づき提供し、個人を特定して提供しない。 　－ デバイスの情報 　－ デバイスの場所 　－ App Storeでの検索 　－ Apple Newsと“株価” ・Apple は、個人を特定できる情報は他社と共有しない。Appleは、Apple と連携してAppleの製品およびサービスを提供したり、マーケティングに協力したり、Appleの代わりに広告を販売したりする戦略的パートナーに、個人を特定しない情報を提供する義務を負っている。 ・Apple Payの取引や「ヘルスケア」App のデータに、Apple の広告プラットフォームがアクセスしたり広告目的に使用したりすることはない。 ・Apple は、ユーザーの性的指向、宗教的信条、または支持政党に関する情報には関知せず、広告主にも提供しない。 ・App StoreまたはApple Newsにデバイスの位置情報へのアクセスを許可した場合、Apple の広告プラットフォームは、App Store とApple Newsで地理的にターゲットされた広告を表示するためにデバイスの現在地を使用することがある。※ユーザーは位置情報の提供を拒否設定できる。 ・Apple の広告プラットフォームは、個人情報を使用して、パーソナライズされた広告を配信する。※ユーザーは「パーソナライズされた広告」をオフにして、Apple に個人情報を広告ターゲティングに使用させないことができる。 （Appleの広告とプライバシー（https://support.apple.com/ja-jp/HT205223）	利用者の情報を他者に販売しておらず、今後も販売しない。また、パートナーに対しては、当社が提供するデータの利用と開示方法について厳しい制約を課している。情報を共有する外部パートナーの種類は次のとおり。 ・当社の分析サービスを利用するパートナー 　個人または事業者が自身の投稿、リスティング、ページ、動画、その他Facebook製品内外のコンテンツに対する人々の反応を把握できるように、集約した統計やインサイトを提供する。 ・広告主 　広告を見た人のタイプや広告の効果についてのレポートを広告主に提供しているが、利用者が許可する場合を除き、利用者を特定する情報（利用者への連絡や特定につながる利用者名やメールアドレスなど）は共有しない。例えば、利用者のデモグラフィック情報や趣味・関心に関する一般的な情報（例えば、広告を見た利用者は、マドリッドに住んでいる25～34歳の女性で、ソフトウェアエンジニアリングに関心があるといった情報）を、ターゲット層を把握するために役立たせる目的で広告主に提供している。また、どのFacebook広告が購入やアクションにつながったかを確認し、広告主に知らせる。 ・効果測定を行うパートナー企業 　利用者に関する情報を、当社パートナーに分析や測定のレポートを提供する目的で、データ集計を行う企業と共有する。 ・当社製品で商品およびサービスを販売するパートナー 　利用者が有料コンテンツの受信を申し込むか、当社製品内で販売されるものを購入する場合、当該コンテンツのクリエイターや販売者は、利用者の公開情報や他の共有情報、および取引完了に必要な情報（配送先や連絡先情報など）を受信する。 ・ベンダーとサービスプロバイダー 　当社は、技術インフラサービスの提供、当社製品の利用状況の分析、カスタマーサービスの提供、決済の代行、アンケートの実施などにより当社の事業を補助するベンダーとサービスプロバイダーに、情報とコンテンツを提供する。 ・研究機関や教育機関 ・法執行機関や法的要請	ユーザーは、Googleのサービスを利用するときに、下記の内容が明記されたプライバシーポリシーに同意の上で、利用を開始する。下記プライバシーポリシー該当箇所を参照。 Googleは、以下の場合を除いて、ユーザーの個人情報を Google 以外の企業、組織、個人と共有することはない。 ・ユーザーの同意を得た場合 　ユーザーの同意を得た場合に、Google 以外の者と個人情報を共有する。 機密性の高い個人情報 （https://policies.google.com/privacy?hl=ja#footnote-sensitive-info）を共有する場合は、ユーザーに明示的な同意を求める。 ・外部処理の場合 　Google の関連会社およびその他の信頼できる企業または個人に対し、個人情報を Google のために処理させる目的で当該個人情報を提供する。その場合、当該関連会社、企業、または個人は、Google の指示に基づき Google のプライバシー ポリシーならびにその他の適切な機密保持およびセキュリティの方策に従って当該処理を行う。たとえば、Google ではカスタマーサポートの提供をサービス プロバイダーに委託することがある。 ・法律上の理由の場合 ・個人を特定できない情報 （https://policies.google.com/privacy?hl=ja#footnote-info）を公開する。または Google のパートナー（サイト運営者、広告主、デベロッパー、権利者など）と共有することがある。たとえば、Google サービスの一般的な利用傾向がわかる （https://policies.google.com/privacy?hl=ja#footnote-trends）情報を公開する。また、特定のパートナー （https://policies.google.com/privacy?hl=ja#footnote-specific-partners）に、広告および測定の目的でパートナー自身の Cookie や類似の技術を使用してユーザーのブラウザまたはデバイスから情報を収集することを許可している。 ・Google が合併、買収、または資産譲渡の対象となった場合、引き続きユーザーの個人情報の機密性が保持されるよう取り計らい、個人情報が譲渡される前、または別のプライバシーポリシーの適用を受けるようになる前に、対象のユーザーに通知する。	・ユーザーから同意を取得して利用者情報を第三者提供する場合がある。 例えば、他社のアプリで ユーザーがLINEアプリ内で設定したプロフィール情報を利用する必要がある場合、ユーザーの同意を取得した上、当該情報を提供している。	・ユーザーの同意を得て提供する場合がある。 ・また、プライバシーポリシーに定める範囲に限定して、パーソナルデータを第三者に提供させていただくことがあるが、実際にパーソナルデータを第三者に提供する際には、法令に基づく場合または別途ユーザーの同意を得る場合を除き、氏名や住所等の直接特定の個人を識別できる情報や、要配慮個人情報を除外した上で提供する。
1-4.	**広告ビジネスモデルへの利用者情報の活用状況**	・Appleの広告プラットフォームはユーザーを追跡しない。 ・AppleのAppから収集したユーザーやデバイスのデータを、他社製Appから収集されたユーザーやデバイスのデータと組み合わせてターゲティング広告または広告測定のために使用しない。 ・AppleのAppから収集したユーザーやデバイスのデータをデータブローカーと共有しない。 ・コンテクスト情報：広告を提供するために、以下のコンテクスト情報を使用する。広告は、複数のユーザーから集約して作成するセグメント情報に基づき提供し、個人を特定して提供しない。 　－ デバイスの情報 　－ デバイスの場所 　－ App Storeでの検索 　－ Apple Newsと“株価” ・Apple は、個人を特定できる情報は他社と共有しない。Appleは、Apple と連携してAppleの製品およびサービスを提供したり、マーケティングに協力したり、Appleの代わりに広告を販売したりする戦略的パートナーに、個人を特定しない情報を提供する義務を負っている。 ・Apple Payの取引や「ヘルスケア」App のデータに、Apple の広告プラットフォームがアクセスしたり広告目的に使用したりすることはない。 ・Apple は、ユーザーの性的指向、宗教的信条、または支持政党に関する情報には関知せず、広告主にも提供しない。 ・App StoreまたはApple Newsにデバイスの位置情報へのアクセスを許可した場合、Apple の広告プラットフォームは、App Store とApple Newsで地理的にターゲットされた広告を表示するためにデバイスの現在地を使用することがある。※ユーザーは位置情報の提供を拒否設定できる。 ・Apple の広告プラットフォームは、個人情報を使用して、パーソナライズされた広告を配信する。※ユーザーは「パーソナライズされた広告」をオフにして、Apple に個人情報を広告ターゲティングに使用させないことができる。 （Appleの広告とプライバシー（https://support.apple.com/ja-jp/HT205223）	・広告やクーポンなどの利用者に表示するスポンサーコンテンツを選定およびパーソナライズする目的で、利用者に関して当社が保有する、利用者の趣味・関心、アクション、つながりなどの情報を利用する。 ・利用者の個人データを広告主に販売することはない。また、利用者の明確な許可を得ずに、利用者を直接特定できる情報（氏名、メールアドレスまたは他の連絡先情報など）を広告主と共有することもない。その代わり、広告主は自社の広告の配信を希望するオーディエンスの類型などを当社に知らせることができ、当社は興味を持ちそうな人にその広告を配信する。	Google はユーザーから共有されたデータをもとにGoogleのサービスを提供、維持、改善し、新しいサービスを開発している。ユーザー自身によるプライバシー管理によって、パーソナライズされたコンテンツ、広告を含めたサービスの提供に利用することができるようになる。Googleアカウントにサインインし、アクティビティ管理のページから、ウェブとアプリのアクティビティをオンにすると、Googleはユーザーに対しパーソナライズされた広告をユーザーの関心に基づき示すことがある。例えば、「マウンテンバイク」と検索すると、ユーザーはGoogleから提供された広告を表示するサイトを見るとスポーツ用品の広告を目にするかもしれない。Googleがユーザーに広告を出すために利用する情報は、広告設定 （https://adssettings.google.com/authenticated）からユーザー自身で管理することができる。また、ユーザーは広告主からの情報に基づいてパーソナライズ広告を目にすることがあるかもしれない。例えば、広告主のサイトで商品を購入したのであれば、広告主はサイトを訪問した情報を利用し広告を表示することができる。 データが広告においてどのように収集、利用されるのかについては下記のリンク参照。 プライバシーポリシー （https://policies.google.com/privacy?hl=ja#whycollect） パーソナライズド広告 （https://support.google.com/adspolicy/answer/143465?p=privpol_p13nad&visit_id=637545784792993386-2692730420&rd=1） 広告が表示される理由 （https://support.google.com/ads/answer/1634057?p=privpol_whyad&hl=ja&visit_id=637545784792993386-2692730420&rd=1）	・ユーザーにより最適化した広告を配信するために利用者情報を利用している。例えば、ユーザーのスタンプ等の購入履歴、よく利用する当社サービス、検索履歴等の情報を利用して広告を配信することがある。	ユーザーにより適切な広告を表示するために、ユーザーから取得した以下のようなパーソナルデータを利用して広告などを配信している。 ・Yahoo! JAPAN IDの登録情報 　生年月、性別など ・広告配信時に取得する情報 　時間帯、おおまかな現在地、広告が表示されるページ、広告表示時に検索していたキーワードなど ・広告配信前に取得した過去の履歴 ① Yahoo! JAPANサービスの利用履歴 　過去に検索したキーワード、閲覧したウェブページや広告、利用したアプリ、購入した商品、利用時間帯、地域、デバイスなど ② 広告主やパートナーサイトの利用履歴 ※人種、宗教、性的指向、健康状態など、慎重に扱うべき個人に関するデータは利用しない。
1-5.	**利用者情報のプロファイリング・セグメント化状況**	・Appleが提供する広告は、ユーザのプライバシーを尊重しながら、App、製品、サービスに出会うお手伝いをする。Appleの広告プラットフォームは個人情報を保護するように設計されており、Appleがどのように個人情報を使うかをユーザが決定できる。Appleの広告プラットフォームは、個人を特定できる情報は他社と共有しない。 （Appleの広告とプライバシー（https://support.apple.com/ja-jp/HT205223） ・似たような特徴を持つユーザーをグループにまとめてセグメントを作成し、これらのグループを使用してターゲット広告を配信する。ユーザーの利用者情報は、割り当てるセグメントおよび配信する広告を決定するために使用される場合がある。プライバシーを保護するため、ターゲット広告は5,000人以上のユーザーがターゲット基準に該当する場合のみ配信される。セグメントに割り当てるために、以下のような情報が使用される場合がある。 　－ アカウントの情報：Apple IDアカウントに登録された名前、住所、年齢、デバイス。名前や敬称などの情報を、性別を推測するために使用する場合がある。 　－ ダウンロードまたは購入した項目とサブスクリプション：ダウンロードした音楽、映画、ブック、テレビ番組、App と、App 内の課金およびサブスクリプション。App Storeから特定のAppをダウンロードしたことや、App Storeからの特定のApp 内での課金（サブスクリプションを含む）に基づくターゲティングは、当該App のデベロッパによる場合のみ許可される。 　－ Apple Newsと“株価”：閲覧した記事のトピックやカテゴリのほか、フォロー、登録、または通知するように設定している出版物。 　－ 広告：Appleの広告プラットフォームによって配信された広告に対する操作。 ・ユーザーは、自身のセグメント情報を確認可能。	・保有する情報を、機能とコンテンツのパーソナライズ、当社製品の内外における利用者へのおすすめの表示を含め、当社製品を提供するために利用する。 ・利用者に合わせて関連性の高いパーソナライズ製品を作成するために、利用者などから取得および認識したデータに基づく利用者のつながり、嗜好、関心、およびアクティビティを利用する。また、利用者の当社製品の利用状況ならびに当社製品に対する反応、および利用者が当社製品の内外でつながりを持ち関心を抱いている人、場所、物についても同様に利用する。	・Googleは収集した情報を、パーソナライズド広告に同意するユーザーにおいて、おすすめの提供、コンテンツのパーソナライズ化、検索結果のカスタマイズを含めた Googleのユーザーのためのサービスをカスタマイズするために利用する。セキュリティ診断のツールでは、利用する Googleの製品ごとにセキュリティ設定のヒントを提供している。 ・ユーザーの設定によって、ユーザーは関心に基づいたパーソナライズド広告を目にすることがある。例えば、「マウンテンバイク」と検索すると、ユーザーはGoogleから提供された広告を示すサイトを見るとスポーツ用品の広告を目にするかもしれない。ユーザーは広告設定 （https://adssettings.google.com/authenticated）より管理することが可能。広告設定のページにおいて、ユーザーには以下の点が通知されている。「広告は、Googleアカウントに追加された個人情報、Googl のサービスを利用している広告主から提供されるデータ、Googl が推定した興味 / 関心に基づいて表示されます。」 ・ユーザーは、人種、宗教、性的指向、健康のようなセンシティブな情報に基づいてパーソナライズド広告が示されることはない。また、名前やメールアドレスのようなユーザーを個人的に特定する情報をユーザー本人の求めがない限り広告主に共有しない。 詳細については、下記参照。 プライバシーポリシー （https://policies.google.com/privacy#whycollect） パーソナライズド広告 （https://support.google.com/adspolicy/answer/143465?p=privpol_p13nad&visit_id=637545784792993386-2692730420&rd=1）	・ユーザーの登録情報やサービス利用履歴等の情報 を基に、ユーザーの興味関心や属性を推定・分類した上、コンテンツの推薦や広告配信に利用している。	・個々のユーザーに最適なコンテンツをはじめとするサービス等を提供する場合（おすすめの商品やサービス等を表示したり、ご案内したりする場合を含む）に、ユーザーの居住地域、性別、生年月等の情報や、ユーザーのサービス等のご利用履歴（検索キーワード、閲覧されたウェブページ、ご利用になったアプリ、購入された商品等）を分析して、Yahoo! JAPAN独自の基準で推定したユーザーの興味関心に関する情報を利用する。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
２．利用規約・プライバシーポリシー						
(1)プライバシーポリシー等						
2-1.	**利用者情報の取扱いに係るプライバシーポリシーの内容**	・Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/） 　－ 階層構造 　－ PDF版もあり （https://www.apple.com/legal/privacy/pdfs/appleprivacy-policy-jp.pdf） ・Data & Privacy（https://www.apple.com/jp/legal/privacy/data/） 　－ 個々のサービスで取り扱う個人データの説明 　－ 上記「Apple プライバシーポリシー」の「Appleがお客様から収集する個人データ」で引用。 ・プライバシー概要（https://www.apple.com/jp/privacy/） 　－ ユーザー向けの簡略版。アイコンを使用してわかりやすくしている。 ・プライバシー機能（https://www.apple.com/jp/privacy/features/） 　－ Safari やマップ等のApple のサービスが備えている、プライバシー保護機能を説明。 ・プライバシーコントロール（https://www.apple.com/jp/privacy/control/） 　－ プライバシー設定の方法を説明	データポリシーにおいて、「弊社が取得する情報の種類」、「弊社が取得した情報の利用目的」、「情報の共有方法」、「ポリシー変更の際の通知方法」等の項目について説明している。 詳しくは、https://www.facebook.com/privacy/explanation参照。	・プライバシー ポリシーについて、できるだけわかりやすく伝えられるよう、具体例、説明動画、主な用語の定義を提示している。	・利用者情報の取扱いを定めたプライバシーポリシーを策定・公表している。 ・プライバシーポリシーには、取得する情報、利用目的、情報を第三者提供する場面及びユーザーの権利等を規定している。 https://line.me/ja/terms/policy/ ・プライバシーポリシーの内容などをわかりやすく説明するための「プライバシーセンター」を開設・公表している。 https://linecorp.com/ja/privacy/ ・個別サービス・機能等において別途のポリシー・規約を策定・公表している場合もある。	・当社においては、ユーザーとの契約の具体的内容となる文書である利用規約の中で、プライバシーポリシーを規定している。これは、プライバシーポリシーがユーザーとの約束であり、その内容が当社の債務になるとの位置づけを明確にするものである。内容は「第２章　プライバシーポリシー」（https://about.yahoo.co.jp/common/terms/chapter1/#cf2nd）のとおり。 ※なお、このプライバシーポリシーについて、ユーザーにとってより分かりやすく情報提供することを目的として、当社ではプライバシーセンターというページを用意しており、同センターにおいて、パーソナルデータの取得、パーソナルデータの活用、およびパーソナルデータの連携について、それぞれ詳細を説明している。
2-2.	**サービス利用開始前の利用者への示し方、通知/同意取得の方法（等級及び掲載場所）**	・プライバシーポリシーに加えて、ユーザーの個人情報の使用を必要とする製品および特定の機能について は、データとプライバシー情報を埋め込む形で提供している。この製品固有の情報は、データとプライバシーのアイコンと一緒に表示される。該当の機能を有効にする前には、こうした製品固有の情報を確認する機会が設けられる。また、この情報は、該当の機能に関連する「設定」や、オンライン(apple.com/jp/legal/privacy)でいつでも確認することができる。	・サービスの利用者が自らの個人データがどのように利用されているかに関する十分な情報を確実に受領し、また、当社と共有する情報を積極及び管理するための権限を確実に付与されるようにするための多くの方法を利用している。これにより、利用者は、当社のサービスへの登録及びエンゲージメントの選択において、十分な情報に基づいた意思決定が可能となる。 ・当社による個人データの収集及び利用に関するすべての利用者への十分な通知を担保するために、すべての見込利用者には最初の登録前に当社のデータに関するポリシーが提示される。利用者は、登録時に、関連するサービス利用規約、データに関するポリシー及びCookieに関するポリシーを確認及び同意するよう求められる。登録が完了した利用者は、ほぼすべてのFacebookのサービスウェブページから、Instagramウェブサイト並びにFacebookのサービス及びInstagram上のアプリ内メニュー経由で、データに関するポリシーへ容易にアクセス可能となる。	・ユーザーがGoogleアカウントを作成する際、プライバシーポリシーへのリンクとプライバシーに関する選択肢、及びアカウント作成の流れ自体に関する明確な説明が示される。ユーザーはアカウント作成後いつでもプライバシーポリシーにアクセスしたり、設定を変更することができる。 ・アカウント設定の流れには、プライバシーポリシーの概要も含まれる。したがって、新たなアカウントを作成するすべてのユーザーがプライバシーポリシーの概要を閲覧することとなる。この方法は、プライバシー監視機関（ICO）を含むデータ保護当局との協議を経て採用された。 ・アカウント作成の流れの最後に、ユーザーは、利用規約への同意を示すボックスとは別の、「上述の［すなわち、ユーザーが選択した設定による］ユーザー情報の処理」に対する同意を示すチェックボックスにチェックすることを求められ、アカウント作成プロセス終了前にさらにプライバシーポリシーの説明が示される。 ・アカウント作成時には、ユーザーにいくつかのプライバシー設定が提示され、特定の処理について説明されるとともに、パーソナライズド広告への同意など、ユーザーが選択をおこなう機会が提供される。	・LINEアカウント開設時に利用規約とプライバシーポリシーを掲載し、ユーザーの同意の上、アカウントを開設することとしている。 ・当社Webサイト又はLINEアプリ内からプライバシーポリシーの内容を確認することができる。	・Yahoo! JAPAN ID取得時の導線 　Yahoo! JAPAN ID取得時に掲出される約款に利用規約（プライバシーポリシーを含む）が含まれており、これらに承諾いただいた上でID登録いただいている。 ・サービス利用時の導線 　約款としてサービスご利用時に同意いただいている。掲出場所はサービスにより異なるが、サイト下部（フッタ部分）やアプリ設定において利用規約（プライバシーポリシーを含む）およびプライバシーセンターへのリンクを掲出している。
2-3.	**変更に際しての通知/同意取得の方法**	・重大な変更があった場合、変更の少なくとも1 週間前までにプライバシーポリシーが掲載されているサイトに通知を公開し、ユーザーのデータをAppleが保有している場合は変更について直接連絡する。 （Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/）の「プライバシーに関するご質問」）	・データポリシーに変更を加える場合、事前に利用者へ通知し、利用者が改訂後のポリシーを確認し、今後製品の利用を続けるかどうかを検討できる機会を設ける。 ・当社のプライバシー・プラクティスに関してフィードバックを行う機会を利用者に提供する取り組みを行っており、これは、2018年に行われた当社のデータに関するポリシーの大幅な更新の際に講じたプロセスからも明らかである。当時、データに関するポリシーの更新版を世界中の利用者に向けてリリースし、更新が確定されて利用者が更新後のポリシーへの同意を求められる前に、フィードバックを行う機会を提供した。	・最終更新日時を常に表示し、旧バージョンもユーザーが参照できるようにアーカイブに保存している。 ・一部のサービスについてはメールで知らせるなど、重要な変更についてはより明確な方法で告知している。 ・ユーザーによる明示的な同意なくポリシーに基づくユーザーの権利を縮小することはない。	・重要な変更に当たっては、アプリ内のバナー等に表示して周知を図っている。 ・必要に応じてアプリ起動時にポップアップ表示をしてユーザーから変更したプライバシーポリシーへの同意を取得する場合がある。	・重要なプライバシーポリシー等の改定にあたっては、アプリにおけるプッシュ通知に加え、全ユーザーへのメール送信など、確実に本人に通知できる方法を採用している。
2-4.	**利用開始後（最初の同意・通知後）における、定期的な通知等の工夫**	・該当の機能を有効にする前には、こうした製品固有の情報を確認する機会が設けられる。また、この情報は、該当の機能に関連する「設定」や、オンライン(apple.com/jp/legal/privacy)でいつでも確認することができる。	・プライバシーツアー： 新規及び既存利用者は、自らの情報がどのように共有されるかを管理するために、自らが使用することのできる機能及び設定を段階的に学べるツアーに参加することができる。新たな利用者は全員、プライバシーツアーに参加するよう促される。 ・プライバシーセンター：Facebookのサービスのほぼすべてのページの上部からアクセスできるプライバシーセンターというメニュー画面を提供している。プライバシーセンターでは、利用者はわずか数回のタップで自身のデータを管理できる。このメニュー画面上では、個人情報の管理方法（例：利用者は共有している内容の確認及び必要な場合の削除が可能）や閲覧する広告の管理、自身の投稿及びプロフィール情報を閲覧可能な相手の管理についてより深く学べるわかりやすい説明を表示している。 https://www.facebook.com/help/395495000532167/?ref=share https://www.facebook.com/ads/about/?entry_product=privacy_shortcuts ・プライバシー基本ガイド： 教育ツールのプライバシー基本ガイドは、プライバシーに関するさらなる情報を利用者に提供しており、FAQ機能の人気のトピックも含まれている。 ・ヘルプセンター： 当社は、広範囲にわたるトピックを検索可能なヘルプセンターを公開している。ここでは、当社のサービスの流れや利用者による管理に関する詳細情報が提供されています。 ・ アカウント設定： 全ての利用者は、自身のアカウント設定内でプライバシー関連の設定及び管理に容易にアクセスすることができる。 ・プライバシー設定の確認： プライバシー設定の確認ツールでは、利用者はデータ共有範囲に関する自身の選択を確認することができる。このツールは利用者の重要なプライバシー関連の設定に関するリマインダーの役割を果たし、利用者に自身が選択した内容を維持するか又は更新するかについて評価するよう促す。 ・全体公開投稿リマインダー：利用者が友達のみとの共有ではなくコンテンツを一般公開する意図があるかを確認するために、当社は、利用者がンテンツを一般公開するという選択を行う前に、短い通知を利用者に送る。 ・Facebookヒント：さらに、利用者に対して、ヒントを通じてFacebookのサービス上での管理の活用や個人情報の保護に関する啓発を定期的に行っている。ヒントは利用者のニュースフィードに表示され、世界中の利用者が自身に合ったかたちでFacebookのサービスを利用できるようにするためにパーソナライズされるものとして製品内に組み込まれているものである。ヒントは利用者のアカウントを安全に保つ方法からFacebookのサービス上での個人情報の管理及び保護、そして友達との交流の新たな方法まで広範なトピックを扱っている。	・Googleアカウントに保存される情報を管理し、プライバシーとセキュリティの設定を見直し、かつ、自身の意向に合わせて調整することを、ユーザーに推奨している。アカウントの作成の最後の段階において、ユーザーは、アカウントのカスタム設定に関する通知を受け取りたいかどうかに関して、チェックボックスで選択することができる。 ・ヘルプページや、サイバーセキュリティ月間やセーファーインターネットデー等に合わせた取り組みなどを通じて、ユーザーへの周知を行っている。	・2-3のとおり、重要な変更があった場合にはユーザーにわかりやすい方法での周知を図っている。 ・今後もよりユーザーにわかりやすい形で変更を知らせるよう、努めていく。	・直近では2020年7月、株式会社ZOZOがグループ企業とのデータ連携の対象として追加されることを知らせる電子メールにおいて、当該データ連携に関する設定に関して現在のユーザーの設定の確認のお願いを実施している。今後については、ユーザーのデータの取り扱いに関する設定について、確認をお願いするための電子メールを定期的に送信することなどの取り組みを拡大していく予定。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
(2)透明性確保のための工夫						
2-5.	利用者情報の取扱いを分かりやすくするための考え方、工夫や対処 （利用者への働きかけや情報提供、ユーザーテストの実施等）	・2-1 のとおり、Appleプライバシーポリシーに加えて、「プライバシー概要」「プライバシー 機能」「プライバシーコントロール」等を掲載。 ・データとプライバシーのアイコンについては、2-2 参照。	・2020年7月にホワイトペーパー「Communicating About Privacy」を発表して以来、消費者にプライバシーに関する情報を提示するためのより良いアプローチを模索するために、世界中のステークホルダーと協議を重ねながら、この課題を深く追求してきた。ホワイトペーパーでは、自分の情報がどのように使用されているかを人々に知らせるための、最良と思われるデザイン手法を幅広く紹介している。その中で明らかになったのは、すべての消費者にとって有効な、唯一の「正しい」プライバシー通知の方法はないということである。 ・他の多くの事業者と同様に、消費者がより詳細な情報を見つけられるようにリンクを張ったり、階層状のプライバシー通知を採用している。 ・ホワイトペーパーでは、より質の高い通知の開発を促進するために、業界と規制当局が協力して通知の基準を策定することや、説明責任の手段を再設計して、単に結果だけではなく、適切なプライバシー設計プロセスの遵守を求めることなどの提案も行っている。	・ユーザーの理解を高めるため、Google のプライバシー ポリシーでは、画像やアニメーション動画及び主要なコンセプトをわかりやすくハイライトした説明を行っている。 ・プライバシーとセキュリティの設定を確認及び調整し、自動削除などのツールを利用することなど、ユーザー自身が Google アカウントに保存されている情報を管理されることを推奨している。 ・ユーザーに対してヘルプページやセーファーインターネットデーなどに合わせた取り組みを通じて、これらを伝えている。	・ユーザーに対してプライバシーに関する意識調査を実施した上、利用者情報の取扱いについての懸念を把握し、プライバシーポリシーを読みづらいと感じる理由等を把握することで、データに基づいた効果的な対策を実施できるように努めている。	・プライバシーポリシーにおいてユーザーに当社のパーソナルデータの取り扱いについてのすべてを分かりやすく説明することは困難であることから、図表等を用いてその詳細を分かりやすく説明した「プライバシーセンター」をご用意し、パーソナルデータの取得、パーソナルデータの活用、パーソナルデータの連携について、それぞれ詳細を説明している。 ・利用目的については、プライバシーポリシーおよびプライバシーセンターのトップページに利用目的を掲げた上で、その利用目的の詳細については、プライバシーセンター内の「パーソナルデータの活用」のページにおいて説明している。さらに、パーソナルデータの活用のページでは、「広告の表示」等、利用の具体例として 15 の項目を掲げ、その項目ごとにどのようなデータを利用しているのか説明している。 ・このようなプライバシーポリシーおよびプライバシーセンターの内容や、同意取得にあたってのユーザーへの情報提供の在り方については、法務部門が事業部門と調整の上判断し、ユーザーのプライバシーに与え得る影響等に応じて、さらにデータ・ディレクター（DD）会で検討した上で、チーフ・データ・オフィサー（CDO）が責任者として決裁する仕組みを導入している。 ・これらのガバナンスシステムが適切に機能していることを第三者から監視・評価を受けるための仕組みとして、外部の多様な専門家により構成されるアドバイザリーボードを組織するだけでなく、加えて社内のデータ利用等に通じた者が同様に第三者的な立場から監視・評価するための仕組みとして、データ・プロテクション・オフィサー（DPO）を設置している。 ・上記のガバナンスシステムが適切に機能することを担保するための取り組みとして、プライバシー影響評価（PIA）の試験運用を始めており、本格運用を目指して取り組みを進めている。 ・2021年上半期にユーザーアンケートの実施を計画している。
2-6.	同意取得/通知に頼っての、利用規約やプライバシーポリシーを理解しやすくするための工夫 （階層的アプローチ、ダッシュボード、ジャストインタイム、アイコン、モバイル及びスマートデバイスの特徴の利用等）	・2-1 のとおり、Appleプライバシーポリシーで階層的アプローチ、2-2 のとおりデータとプライバシーのアイコンを採用。 ・2-1 のとおり、「プライバシーコントロール」でプライバシー設定の方法を説明。 ・データとプライバシーのページ（https://privacy.apple.com/）を用意（「プライバシーコントロール」のページにもリンクあり）。以下のことが可能。 － Apple ID に紐付けてApple に保管されているデータのコピーの取得 － ユーザー自身のApple ID を一時的に無効化する。 － ユーザー自身のApple ID を削除し、当該ID に関連づけられているデータを削除する。 － 個人データの訂正を申請する。 ・ユーザーは、「iPhone解析を共有」するか否かを選べる。ON にすると、を毎日自動的に送信するようになる。 （Appleに保管する個人情報の把握と管理（https://support.apple.com/ja-jp/HT208501））（デバイス解析とプライバシー （https://support.apple.com/ja-jp/HT210682））	・2-5のとおり、2020年7月、事業者はプライバシー設計の決定において「人」を中心に据えることで、プライバシー情報をよりよく伝える必要性を強調したホワイトペーパーを発表した。ホワイトペーパーでは、事業者、政策立案者、その他の専門家が協力し合うことの重要性も強調している。 ・当社が設立し支援する業界横断的な取り組みであるTTCラボを通じて、当社はさまざまな専門家や企業と協力し、データやプライバシーの選択について人々によりよく知らせるためのクリエイティブなデザインソリューションを開発している。 ・データポリシーのデザインを変更し、より読みやすく、適切なものにしたり、「プライバシー設定の確認」のような製品内プロンプトの追加を行ったり、さらには「この広告が表示されている理由」や「Facebook外のアクティビティ」などの機能を展開している。	ユーザーのエンゲージメントに影響を与えるGoogleのプライバシーポリシーの項目のうち、2018年のプライバシーポリシーの最新版を設計する際に考慮した要素は以下の通り。 ・ナビゲーションのしやすさ：明確な見出し、簡単なナビゲーション、オーバーレイなど、ユーザーが探しているものを見つけやすくするために、プライバシーポリシーを再設計・再編成した。 ・わかりやすさ：プライバシー ポリシーに、より明確な表現と詳細な説明を導入した。また、説明用の動画や図を追加し、文字による説明に加えて、よりわかりやすい視覚的な情報を提供している。 ・透明性と管理：ユーザーがプライバシー ポリシーを読んだ際に、すぐユーザーがプライバシー設定を変更できるように設定に直接アクセスできるリンクを提供することで、設定変更を容易にした。	・プライバシーポリシーの内容などをわかりやすく説明するための「プライバシーセンター」を開設・公表している。 ・プライバシーポリシーについては、できる限り各項目の冒頭に当該項目の概要を記載するようにしている。例えば、プライバシーポリシーの「取得するパーソナルデータ」や「パーソナルデータの利用目的」の冒頭に当該項目の概要を説明した後、詳細内容を説明するようにしている。 ・個別機能・サービスにおいて別途ポップアップで説明等を行う場合もある。	・2-5のとおり、プライバシーポリシーにおいてユーザーに当社のパーソナルデータの取り扱いについてのすべてを分かりやすく説明することは困難であることから、図表等を用いてその詳細を分かりやすく説明した「プライバシーセンター」を用意し、パーソナルデータの取得、パーソナルデータの活用、パーソナルデータの連携について、それぞれ詳細を説明している。 ・お客様の情報に関する設定を一ヶ所に集約し、「プライバシー・メール配信設定」としてご提供している。 ・同意取得や重要な通知に際してはポップアップを利用するなどしてユーザーが必ず目にするよう工夫している。
(3)オプトアウト						
2-7.	利用者情報の提供を希望しない意思を示すオプトアウトの設置状況（方法、対象範囲等含む）	・1-1、1-4 のとおり、ユーザーは位置情報の提供を拒否設定することができる。 ・1-4 のとおり、ユーザーはパーソナライズされた広告への個人情報の利用について拒否設定することができる。 ・ユーザーは、iPhone解析情報（ハードウェアおよびオペレーションシステムの仕様に関する詳細、パフォーマンスの統計情報、および各デバイスとApp の使用状況（個人が特定されることはありません））の提供を拒否設定できる。 （デバイス解析とプライバシー（https://support.apple.com/ja-jp/HT210682））	・当社のサービスは広告収入により支えられているため、パーソナライズ広告のすべてをオプトアウトする選択肢は利用者に付与していない。 一方で、利用者がFacebookのサービス上で閲覧する広告をカスタマイズ及び管理できる各種のツール及び機能を提供している。	・ユーザーは、Googleアカウントを作成する際に、Googleと共有する情報を選択することができる。同時に、アカウント、プライバシー、セキュリティに関するいくつかの重要な設定管理項目が提示される。アカウント作成後も、ユーザーは、https://myaccount.google.com/にある Googleアカウントの一括管理用ダッシュボードを通じて、いつでも Googleアカウント設定を確認し変更することができる。このツールは、デスクトップおよびモバイルのデバイス上のあらゆるブラウザを通じて使用できる。 ・ユーザーはアカウント ダッシュボードにアクセスして、特定の設定ボタンを ON または OFF にすることができる（オプトアウトとオプトイン）。例えば、ロケーション履歴は、ユーザーがサインインしたデバイスを持って訪れた場所に関する情報をGoogleアカウント上に保存する。これは、位置情報を収集し保存する特定の方法であり、位置情報は、Googleマップ、フォト、検索を含む、Google の製品とサービスを使うにあたってユーザーに様々な利点をもたらす。	・利用者情報の第三者提供（連携）や位置情報の取得等についてオプトアウトの機能を用意し、ユーザーが連携や情報提供を停止できる手段を提供している。	・Yahoo! JAPAN IDの「登録情報」において、プライバシー・メール配信設定画面を設置している。ここでは、「各アプリケーションでのデータ利用において、外部アプリケーションのデータ利用について、「グループ企業へのデータ連携設定」において、グループ企業へのデータ連携について、「外部企業へのデータ提供設定」において、個別の外部企業へのデータ提供について、それぞれオプトアウトが可能。当該設定については、プライバシーセンターの「プライバシー設定」においても案内している。
2-8.	オプトアウトをした場合のサービス利用継続の可否	・2-7のオプトアウトを行ってもサービス利用継続可。	・2-7参照。	・ユーザーは、これらをいつでも無効にでき（オプトアウト）、無効にした後も、Google マップ、フォト、検索を含む Google の製品やサービスを使い続けることができる。	・ユーザーが他社のアプリとの連携を解除した場合や位置情報をオプトアウトした場合であっても LINE アプリの利用は継続できる。	・ユーザーがオプトアウトした場合であっても各サービスの利用継続は可能。 ・行動ターゲティング広告を拒否した場合でも、広告の精度が悪くなる以外にユーザーに不利益が生じることはない。
2-9.	利用者情報の提供について個別に選択できるダッシュボード等の設置状況（方法、対象範囲等含む）	・2-6 のとおり、データとプライバシーのページがある。 ・2-7 のオプトアウトを、iPhoneやMacなどデバイスから設定できる。 － iPhone等：「設定」＞「プライバシー」 － Mac：「システム環境設定」＞「セキュリティとプライバシー」＞「プライバシー」	・「広告表示の設定」において、広告のターゲット設定に使用されるプロフィール情報、興味・関心のカテゴリ等を設定・管理することができる。 ・「この広告が表示されている理由」は、利用者が特定の広告が表示される理由の説明を確認することができる。 ・「Facebook外のアクティビティ」機能により、利用者は事業者や組織が自社アプリ又はウェブサイトの訪問、コンテンツの閲覧、及びショッピングカートへのアイテムの追加などの利用者のインタラクションに関して当社と共有しているアクティビティの概要の確認や、各自のFacebookのアカウントからの当該アクティビティの関連付けを解除することができる。	・2-7参照。	・ユーザーがLINEアプリにおける利用者情報を連携している他社のアプリについては、LINEアプリ内で連携中の他社アプリが一覧表示される画面を提供しており、当該画面内から連携解除が可能となっている。	・2-7のとおり、Yahoo! JAPAN IDの「登録情報」において、プライバシー・メール配信設定画面を設置しており、ユーザーはいつでも設定変更が可能となっている。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
(4)データポータビリティ						
2-10.	**データポータビリティに関する取組 （データポータビリティーを求める方法、対象範囲）**	・データとプライバシーのページで、「データのコピーをリクエスト」をクリックすると、当該ユーザーがApple に保存しているデータのコピーをリクエストすることができる。	・「個人データをダウンロード(DYI)」では、以下の2種類のデータセットが対象になっている。 －「あなたの情報（your information）」：プロフィール情報、投稿、「いいね！」、コメントなど、リクエストした個人がFacebook上で入力、アップロード、共有した情報。 －「あなたについての情報(information about you)」：Facebookへのログイン、使用しているデバイス、ニュースフィード、ウォッチ、ニュースでの推奨を行うための情報など、リクエストした個人のFacebookアカウントに関連する情報を含む。 利用者は、「設定」→「あなたのFacebook情報」を開き、「個人データをダウンロード」を選択することでリクエストを開始できる。このページでは、リクエストの対象となるデータのカテゴリの追加や削除、ダウンロードリクエストのフォーマットの選択、写真、ビデオ、その他のメディアの画質の調整、情報の特定の日付範囲の指定などを行うことができる。利用者がFacebookに参加した時期に応じて、100以上のデータカテゴリーから選択することができる。 ・「データをダウンロード（Download Your Data:DYD）」には、Instagramの利用者向けに同様のカテゴリーの情報が含まれている。ユーザーは、Instagramの「設定」→「セキュリティ」にアクセスし、「データをダウンロード」ツールを選択することで、Instagramデータのダウンロード要求を開始することができる。 ・2020年には、Facebookの写真や動画をGoogleフォト、Dropbox、Koofr、またはBackblazeに転送することができる「写真または動画の転送」ツールを開始した。ユーザーは、「設定」→「あなたのFacebook情報」を開き、「あなたのFacebook情報コピーを転送」を選択することで、写真やビデオの転送を要求することができる。そこから、フォトライブラリ全体または特定のアルバムを選択し、転送先を選ぶことができる。今後、新しいデータタイプや転送先の追加を予定している。	・Google Takeoutは、ユーザーにデータポータビリティに関する管理権限を提供している。ユーザーは、Google に保存した自身のデータの最新版コピーを自身のコンピューターにダウンロードしたり、サードパーティのプロバイダーのサイトに直接ポーティングすることができる。	・いわゆるデータポータビリティには対応していないが、「トーク履歴の送信」機能を利用してTextファイルでトーク履歴をダウンロード・送信することはできる。	・まずは電子的な手法による個人データの開示請求への対応をできるだけ早期に実現できるよう、対応を進めているところ。
2-11.	**データポータビリティが可能である場合 ・提供されるデータのフォーマット ・提供先の要件 ・インターオペラビリティ確保に関する考慮状況**	・2-10 のとおり、ユーザーは自身のデータのコピーをダウンロードすることが可能であり、それらには以下が含まれる。 － JSON、CSV、XML またはPDF形式のスプレッドシートまたはファイルでのApp 利用やアクティビティ情報 － それぞれの原フォーマットによる文書、写真及びビデオ － VCF、ICS 及びHTML フォーマットによる連絡先、カレンダー、ブックマーク	・利用者はいつでもデータファイルを要求することができ、HTMLファイル（DYI）またはJSON（DYIおよびDYD）で受け取ることを選択することができる。HTMLは、Facebookで一般的に使用されている、見やすいデータ形式である。受信者はZIPファイルで受け取る。ZIPファイルを開いて解凍すると、「index」という名前のHTMLファイルが含まれており、Webブラウザでwebページのように開くことができる。この.ZIPファイルには、リクエストされた画像や動画などのファイルが入ったフォルダが含まれている。JSONは機械的に読み取り可能なデータ形式で、他のサービスに情報をアップロードする際に、より簡単に情報を転送できる可能性がある。 ・セキュリティ対策のため、情報のコピーのダウンロードを開始する前に、パスワードの再入力を求めている。また、ダウンロードの開始を許可する前に、追加の確認ステップの完了を求めることがある。アカウント保護のため、ダウンロードリクエストは数日後に失効するが、いつでも新しいリクエストをすることができる。 ・2018年には、Apple、Google、Microsoft、Twitterと共同で、オンラインサービス間でデータを転送するための共通の方法を構築する「Data Transfer Project」への参加を発表した。このプロジェクトでは、どのようなサービスでも利用者に代わって直接転送を実行・管理することができるためオープンソースのライブラリを提供している。	・ユーザーは、製品、データの種類、用途に応じて選択できるさまざまな業界基準のフォーマットで、自身のデータをエクスポートできる。例えばGoogleドライブから、Googleドキュメントの文書を .docxファイルとしてエクスポートし、Microsoft Officeで簡単に使うことができる。データを複数のフォーマットでダウンロードできるようにすることで、フレキシビリティを最大化し、利用者自身のデータ活用方法の選択肢を広げている。 ・Data Transfer Project(DTP)は、プロバイダー間における直接のデータ転送を可能にする。DTPは、データポータビリティへのユーザーのアクセスを拡大するために、業界のパートナーと協力し立ち上げたイニシアチブで、どの企業も安全で拡張性のある直接データポータビリティソリューションを構築できるようにするものである。このプロジェクトは、2 つの製品インターフェース間で、データを直接インポートおよびエクスポートする接続を可能にする。	・2-10参照。	・2-10のとおり、電子的な手法による個人データの開示請求への対応をできるだけ早期に実現できるよう、対応を進めているところ。
2-12.	**個人情報保護法に基づく開示請求への対応状況（電磁的な開示の実施状況、開示請求の方法、提供フォーマット等）**	・電磁的な開示を行っている。2-6 のデータとプライバシーのページで、「データのコピーをリクエスト」をクリックすると、当該ユーザーがApple に保存しているデータのコピーをリクエストするページに行くことができる。	・消費者がプライバシーに関する質問又は当社のプライバシー慣行に関する質問を行えるように様々な連絡窓口を提供している。 ・例えば、Facebook社のサービスについては、利用者及び利用者以外も専用の問い合わせ用フォームを使用してFacebook社のデータに関するポリシーについて当社まで問い合わせることができる。また、当社のデータに関するポリシーの末尾にあるTRUSTe（外部の第三者紛争解決プロバイダー）のウェブサイトへのリンクを通じて、同社と連携することもできる。当社のデータに関するポリシーには、当社にメールで連絡することを希望する利用者向けの宛名及び住所も記載されている。 ・利用者は、Facebook社のサービスに投稿されたコンテンツについて肖像に係るプライバシーに関する苦情を申し立てることもできる。当社のプライバシーに関する運営の専門家チームによって受領された質問に対しては、速やかに回答がなされる。また、当社は、当社のヘルプセンターにおいて、プライバシー設定とツールに関する分かり易い説明、問い合わせ用フォームへのリンク、及びよくある質問への回答を提供している。	・Googleアカウントには、使用しているGoogleのサービス、メールや写真などの保存データの概要を確認できるダッシュボードがある。また、Googleアカウントには、Googleのサービス全般を通じて検索、閲覧、視聴するなどのアクティビティから収集されたデータを簡単に確認し、削除できるツールであるマイアクティビティも提供してる。 ・過去のオンライン上のアクティビティを簡単に振り返ることができるよう、トピック、日付、サービスで検索できるツールが用意しており、ユーザーは「データをダウンロード」からアカウントに保存されたデータのコピーにアクセスするか、プライバシーに関するトラブルシューティングまたは Googleプライバシー ヘルプセンターからアクセス可能な「データへのアクセス権をリクエスト」のフォームを送信することができる。 ・また（上記のツールで対応できない場合で）、適用されるプライバシー関連法に基づいて利用者からの要求があった場合、デジタルフォーマットで情報を開示する。	【開示請求の方法】 当社Webサイト内の問い合わせフォーム又は郵送にて開示請求を受け付けている。 【開示方法】 基本的にはユーザーへPDFを送信する方法で開示している。ユーザーが希望した場合には郵送での開示も実施している。	・2-10のとおり、電子的な手法による個人データの開示請求への対応をできるだけ早期に実現できるよう、対応を進めているところ。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
３．他アプリやサイトを経由した情報収集の状況						
3-1.	**他アプリやサイトを経由した情報収集の状況**	【Appleが他のソースから受け取る個人データ】 ・個人：他の個人から他のユーザーに関するデータを収集することがある（例：他の個人からユーザーに製品やギフトカードを送付、Apple のサービスやフォーラムへの参加への招待等）。 ・ユーザーの指示がある場合： － ユーザーが、モバイル通信事業者に対し、アカウントのアクティベーションのためにユーザーの通信事業者アカウントに関するデータをAppleと共有するように指示する場合 － Appleでの購入に対するリワードを獲得できるようにロイヤルティプログラムへの参加に関する情報を共有するようにユーザーが指示したりする場合　など ・Appleのパートナー：セキュリティおよび不正防止の目的で、ユーザーがApple IDの作成時に提供する情報を第三者からの情報を利用して検証することがある。 （Appleプライバシーポリシー （https://www.apple.com/legal/privacy/jp/）	・広告主、アプリ開発者およびパブリッシャーは、利用しているFacebookビジネスツール(ソーシャルプラグイン（「いいね！」ボタンなど）、FacebookログインFacebook、当社のAPIとSDK、Facebookピクセルなど)を通して、当社に情報を送信することができる。 ・上記パートナーが提供する情報には、利用者のFacebook外におけるアクティビティに関するものが含まれる。これには利用者のデバイス、訪問したウェブサイト、購入履歴、閲覧した広告、パートナーのサービスの利用状況が含まれ、利用者がFacebookアカウントを保持しているかどうか、またはFacebookにログインしているかどうかに関わらず提供される。 ・利用者のオンライン・オフラインアクションについて、および利用者の情報を当社に提供する権利を有するサードパーティデータプロバイダーからの購入についての情報が当社に提供される。	・ユーザーが同意した場合、Googleのサービスへのアクセスに使用したアプリ、ブラウザ、およびデバイスに関する情報を収集する。収集する情報には、固有 ID（https://policies.google.com/privacy?hl=ja#footnote-unique-id）、ブラウザの種類および設定、デバイスの種類および設定、オペレーティング システム、モバイル ネットワークに関する情報（携帯通信事業者名や電話番号など）、アプリケーションのバージョン番号などが含まれる。また、Googleのサービスとユーザーのアプリ、ブラウザ、およびデバイスの間の通信についての情報も収集する。たとえば、IPアドレス（https://policies.google.com/privacy?hl=ja#footnote-ip）、障害レポート、システム アクティビティ、リクエストの日時と参照 URLなど。 ・信頼できるパートナーからユーザーに関する情報の提供を受けることもある。たとえば、マーケティング パートナーから Googleのビジネス サービスのマーケットインサイトに関する情報の提供を受けたり、セキュリティ パートナーから不正使用防止 （https://policies.google.com/privacy?hl=ja#footnote-against-abuse）のための情報の提供を受けることがある。また、広告主から、広告やリサーチのサービスをその広告主に提供するための （https://policies.google.com/privacy?hl=ja#footnote-ad-services）情報の提供を受けることがある。 これらはすべて、プライバシーポリシーに明記している。	・当社の提携事業者が運営する他アプリやWebサイトに当社の広告配信等のためのツールが設置された場合、当該アプリ・サイトを訪問したユーザーに関する情報を取得する場合がある。	・Yahoo! JAPANの広告主や広告配信先等のウェブページやアプリを利用した場合に、当該パートナーのウェブページやアプリにYahoo! JAPANの「ウェブビーコン」等を設置してクッキーや端末情報を参照することで、ユーザーの利用端末を識別するための情報等を取得する場合がある。
3-2.	**他アプリ提供者やサイト運営者に対し、どのような同意取得や通知を促しているか**	・「6．アプリ提供マーケット」参照。	・利用者がパートナーのサービスを訪問、利用した場合、またはパートナーが連携する外部パートナーを通して、パートナーは利用者のデータを受け取る。これらのパートナーが当社にデータを提供する前に、パートナーが利用者のデータを取得、利用、共有する正当な権利を有していることを当社は当該パートナーに要求する。	・例えばGoogle Playでは、アプリとゲームがユーザーのデバイス上でアクセスしようとするデータについて、ユーザーが十分な情報を得た上で判断できるよう支援している。その一環として、以前から、デベロッパーへ、Google Playストアのアプリ一覧で、どのように個人情報を収集し使用しているかを開示することを義務付けてきた。2015 年にAndroid Marshmallowを公開した時には、ユーザーがいつでも、自身のデバイスでこまめに許可を確認、付与、拒否できるランタイム権限を導入した。	・他アプリやWebサイトにおいて、当社がCookie等により訪問履歴等の広告関連情報を収集し、広告の効果測定等に利用すること、およびオプトアウトの方法について通知を行うとともにユーザーから必要な同意を取得することを規約で義務づける等の対応を行っている。	・広告主のウェブサイト、アプリケーション等におけるユーザーの訪問・行動履歴情報を利用する広告商品利用時の遵守事項として、ユーザーの訪問・行動履歴情報を取得させる自身のウェブサイト、アプリケーション等において、記載項目を定め、この記載は、対象ウェブサイト等のトップ画面から1～2回の操作で到達できる場所に記載することを求めている。 記載を求める事項の詳細は次のとおり。 （1）ヤフー株式会社を始めとする第三者の提供する広告配信サービスを利用する場合があり、その場合において、クッキー等によって当該第三者がユーザーの対象ウェブサイト等の訪問・行動履歴情報を取得、利用する場合がある旨 （2）広告配信サービスを提供する第三者によって収集された対象ウェブサイト等におけるユーザーの訪問・行動履歴情報が、当該第三者のプライバシーポリシーに従って利用される旨 （3）広告配信サービスを提供する第三者の提供するオプトアウト手段により、当該第三者による対象ウェブサイト等において収集されたユーザーの訪問・行動履歴情報の広告配信への利用を停止させることができる旨 （4）ユーザーがクッキー等の設定を行うことにより、訪問・行動履歴情報が収集されることの可否を定めることが可能である旨
3-3.	**JavaScriptの取扱状況（後から情報取得内容が変更されることについて、他アプリ提供者やサイト運営者にどのように伝えているか等）**	・Safariは追跡者からユーザーを保護する。インテリジェント・トラッキング防止機能が、インターネット広告から追いかけられないようにする。ウェブサイトの中には、サイトを閲覧するあなたの行動を何百ものデータ収集会社に監視させ、ユーザーのプロファイルを作成して広告を表示するものがある。Safari のインテリジェント・トラッキング防止機能がデバイス上の機械学習を使って、追跡型広告をブロックできるようにする。 （プライバシー 概要（https://www.apple.com/jp/privacy/））	（回答なし）	・ データに関してパートナーとどのようにやり取りしているのかについては、プライバシーポリシーに規定。	・ガイドラインや媒体資料を用いて提携事業者に案内する運用をしている。	情報の取得内容が変更されることはない。
3-4.	**複数の他アプリやサイトから収集している場合の、情報管理状況**	N/A	・Facebookグループ企業内だけでなく、当社のパートナーや利用者が世界中でつながる共有者などの外部者とも、当社のデータポリシーに従って情報を世界規模で共有している。利用者の情報は、当社のデータポリシーに記載される目的で、米国やその他利用者の居住地以外の国に移転、転送、保存、処理される場合がある。 このようなデータの移転は、Facebook利用規約およびInstagram利用規約に明記されるサービスの提供や、当社製品のグローバルな運用と利用者への提供のために必要である。標準契約条項を活用するほか、該当する場合には特定国に関する欧州委員会の十分性認定に依拠し、米国や米国以外の国へのこのようなデータの移転について利用者の同意を取得している。	収集したデータを、データの内容、データの用途、ユーザーの設定内容に応じてそれぞれ異なる一定期間保持する。 ・収集するデータには、ユーザーがいつでも削除できるもの（ユーザーが作成またはアップロードしたコンテンツなど）がある。ユーザーは、アカウントに保存されているアクティビティ情報も削除できる。また、一定期間後に自動的に削除されるよう設定することもできる。 ・その他のデータ（サーバーログ内の広告データ （https://policies.google.com/technologies/ads?hl=ja）など）は、一定期間後に自動的に削除されるか、匿名化される。 ・サービスの使用頻度に関する情報など一部のデータは、ユーザーがGoogleアカウントを削除するまで Google が保持する。 ・セキュリティ、詐欺および濫用の防止、取引記録の保持など、正当な業務上または法律上の目的のために必要に応じて他のデータよりも長期間保持するデータもある。	・当社が付与したユーザーの内部識別子と関連づけて管理する場合がある。	・当社が取り扱うユーザー等のYahoo! JAPAN ID、パートナーのID、広告ID（Advertising Identifier(IDFA)およびGoogle Advertising Identifier(AAID)を含むがこれに限らない）、クッキーその他の各種識別子を紐づけて管理し、プライバシーポリシー記載の利用目的に利用する場合がある。

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
４．他社へのデータ提供、他社との連携の状況						
4-1.	他社に対する、取得した利用者情報・位置情報に基づくデータ提供の内容、提供に関する留意点（ユーザーへの説明、他社の監督、安全管理など）	・3-1参照。	・1-3参照。	Google 以外の者との個人情報共有に関する Google のポリシーは、Google のプライバシーポリシーの「ご自分の情報の共有」の項に記載されている。Google のプライバシー ポリシーは、あらゆる種類の個人情報並びに第三者にグローバルに適用される。 以下の場合を除いて、ユーザーの個人情報を Google以外の企業、組織、個人と共有することはない。 ・ユーザーの同意を得た場合 1-3参照。 ・ドメイン管理者の場合 Googleサービスを使用する組織の従業員または学生の場合、使用している Googleアカウントには、アカウントを管理するドメイン管理者および販売パートナーがアクセスできる。ドメイン管理者および当該販売パートナーは次のことを行うことができる。 － ユーザーのアカウントに保存された情報（メールなど）にアクセスし、その情報を保持すること。 － ユーザーのアカウントに関する統計情報（ユーザーがインストールしたアプリの数など）を表示すること。 － ユーザーのアカウントのパスワードを変更すること。 － ユーザーのアカウントのアクセス権を一時停止または停止すること。 － 適用される法律、規制、法的手続き、または強制力のある政府機関の要請に応じるために、ユーザーのアカウント情報を受け取ること。 － 自分の情報またはプライバシー設定の削除や編集を行うユーザーの権限を制限すること。 ・外部処理の場合 1-3参照。Googleは、個人情報にアクセスできる担当者を、その情報の処理のためにその情報を必要とする Google の社員、請負業者または業務委託先、および代理人に限定している。内部ツールへのアクセスは厳重に管理されており、システムの悪用に対してはゼロ・トレランス・ポリシーを採用している。従業員であるか否かを問わず、当該担当者はいずれも、厳格な契約上の守秘義務を負っており、当該義務を履行しなかった場合は懲戒処分または契約解除の対象となることがある。 ・法律上の理由の場合	・他社に利用者情報を提供する場合、提供する情報をわかりやすく表示した上、ユーザーから同意を取得するようにしている。また、他社にユーザーの識別子を提供する場合、安全管理の観点から、提供先の企業ごとに異なる識別子を提供するよう努めている。 ・他社に利用者情報を提供する場合、当社と他社との間で、利用者情報を保護するための契約を締結し、利用者情報が安全に管理されるよう努めるとともに、ユーザーに対して事後のオプトアウト機能を提供する等している。	・ユーザーが同意した場合に限り、ユーザーへよりよいサービスを提供するために、プライバシーポリシーの範囲内でグループ企業、パートナー企業へのデータ連携を行うことについて、連携するデータの範囲、連携先に範囲等についてプライバシーセンターの「パーソナルデータの連携」の項目で説明している。 ・当社は、当社が定める基準を満たす安全管理措置を講じている第三者にのみパーソナルデータを提供する。 ・位置情報については、プライバシーセンターの「位置情報の利用について」の項目で、取得したユーザーの位置情報（端末から取得可能なGPS位置情報、Wi-Fi情報、Bluetooth情報等）をサービス等の提供（ユーザーからの問い合わせへの対応、ユーザーへのお知らせ、適切かつ安全なサービス等の提供のための不正対策を含む）、改善や新たなサービス等の検討、サービス等の利用状況等の調査、分析に利用する旨を説明している。
4-2.	利用者情報・位置情報の取得・活用に関する、他社との連携状況、連携に関する留意点（ユーザーへの説明、他社の監督、安全管理等）	・3-1参照。	・ここ数年間、データの扱い方を変更し、データへのアクセスとデータの管理に関するパートナーの責任の持ち方を変えてきた。APIへのアクセスを制限し、アプリレビューを拡張し、アプリ開発者の調査を開始した。開発者がFacebookのプラットフォームを責任を持って使用し続けるために必要なツールと情報を確実に持てるようにするため、次の4つの分野で改善を図ってきた。 － 開発者にデータの使用とシェアに関するさらに明確になったガイダンスを提供する。 － 開発者に責任を持たせるための新しいツールとコントロールをビルドする。その中には、年ごとのデータの使用状況の確認プロセスがある。このプロセスでは、開発者はFacebookプラットフォームAPI経由で自分たちがアクセスするデータのタイプをレビューし、データの利用方法がFacebookの規約とポリシーに準拠していることを確認できる。 － 開発者のエクスペリエンスを改善する。開発プロセスとアプリレビュープロセスをカスタマイズして多種多様な開発者をより良くサポートできるようにし、アプリダッシュボードを更新して必要なすべてのアクションをさらに容易に確認できるようにしてきた。 － 利用者のエクスペリエンスを改善する。アプリで利用者にポジティブなエクスペリエンスを提供するための追加のポリシーガイダンスを提供している。 ・最初の分野での取り組みの一環として、Facebook社のプラットフォームとツールを使用する際、データを保護し、利用者のプライバシーを尊重するという自分たちの責任を確実に事業者と開発者が明確に理解できるよう、新しいプラットフォーム規約と開発者ポリシーを導入する。新たなプラットフォーム規約と開発者ポリシーは、既存のFacebookプラットフォームポリシー(Messengerプラットフォームを含む)、Instagramプラットフォームポリシー、拡張プラットフォーム製品に関する補足規約、技術提供者修正条項を簡素化し置き換えるものである。 プラットフォーム規約：プラットフォーム規約は更新され、データ利用の制限、データセキュリティ要件、規定の実施、利用規約と保証(知的財産権など)に焦点が当てられている。これは、Facebookプラットフォームで製品とソリューションをビルドする際の、開発者の権利と責任をより良く概説するのに役立つ。 － プラットフォームデータの利用とシェア：更新されたプラットフォーム規約では、Facebookのプラットフォームから開発者が受け取るデータの2層構造を定義し、各層のデータをどのように利用しシェアするかに関する明確なガイダンスが提供されている。プラットフォームデータと制限プラットフォームデータというこの新しい区分は、情報開発者が利用者の明示的な同意なしに第三者とシェアできるものを制限し、利用者データのセキュリティ保護を強化する。 － データの削除：データ削除に関するポリシーの要件も明確化している。開発者は、正当なビジネス上の目的のためのデータ利用の必要がなくなったらデータを削除することが求められる。開発者が製品やサービスの運営を中止した場合、Facebook社が削除を要請するか、開発者がデータを受け取るとエラーになる。 － 施行＆監督：更新された規約では、開発者に対するFacebook社のデータセキュリティ要件の規定が強化されている。データ漏えいが発生した場合には、Facebook社に通知し、すぐに問題の修復を始め、妥当な範囲でFacebook社と協働することが求められている。また、監査、停止、施行に関するFacebook社の規定も明確化している。 － 開発者ポリシー：統合、品質コントロール、ユーザーエクスペリエンス、コンテンツ、美的、機能に関する要件をそれぞれ分け、開発者ポリシーという単一のドキュメントにまとめた。 ・1-4及び3-1参照。	・グループ会社との間で、ユーザーにより良いサービスを提供するために取得した利用者情報を連携する場合がある。 ・利用者情報を連携するグループ会社の範囲は、プライバシーポリシーに記載することによってユーザーに説明している。	・同意取得にあたってのユーザーへの情報提供の在り方を判断するガバナンスシステム、及び当該ガバナンスシステムが適切に機能していることを第三者から監視・評価を受けるための仕組みについては、2-5のとおり。 ・4-1のとおり、当社は、当社が定める基準を満たす安全管理措置を講じている第三者にのみパーソナルデータを提供する。 ・位置情報については、4-1のとおり。

	社名	Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
5．サードパーティによる情報取得への対応方針						
5-1.	**ウェブブラウザやアプリ経由等でサードパーティが情報取得することについての方針（Third Party Cookieや広告ID等の取扱い）ウェブとアプリで方針は同じか異なるか。**	・一部のWebサイトでは、第三者コンテンツ提供者を使用している。第三者コンテンツ提供者は、製品やサービスの広告を出すためにWebサイト間でユーザをトラッキングする可能性がある。Safariでは、「サイト越えトラッキングを防ぐ」の設定を有効にすることで、ユーザが第三者コンテンツ提供者のWeb サイトを閲覧しない限り、トラッキングデータは定期的に削除される。（Safariとプライバシー：https://support.apple.com/ja-jp/HT210675） ・Cookie は、サイト側が同じ人が再訪してきたときにわかるように、訪問者のデバイスに残していくデータである。Safariで「すべてのCookie をブロック」の設定ができる。（iPhone、iPad、iPod touch で Safari から閲覧履歴と Cookie を消去する） ・Appで収集した情報をサードパーティーと共有することについて、App Store Reviewガイドライン（https://developer.apple.com/jp/appstore/review/guidelines/#legal）「5.1.2 データの使用と共有」に規定するとともに、App Storeでは、すべてのAppleプラットフォームを対象に、ユーザーがApp をダウンロードする前にAppのプライバシー方針を確認できるようになった（https://developer.apple.com/jp/appstore/app-privacy-details/）。Appのユーザーデータをサードパーティと共有する場合は、そのサードパーティがAppのプライバシーポリシーやApp Store Reviewガイドラインで求められているものと同等のData protectionをユーザーに提供していることを確認する必要がある。 ・法律で許可されているものでない限り、事前にユーザーの許可を取らずに、ユーザーの個人データを使用、送信、共有することはできない。 ・Appで収集したデータは、Appの改善や広告の提示といった目的でのみサードパーティと共有することができる。 ・ユーザアクティビティをトラッキング（*）するには、App TrackingTransparency APIを介して、ユーザーの明示的な許可を得る必要がある。トラッキングについて詳しくは「ユーザーのプライバシーとデータの使用」（https://developer.apple.com/jp/app-store/user-privacy-anddata-use/）に記載。（*）トラッキングとは、ディベロッパーが自身のApp で収集したユーザーやデバイスに関するデータを、ターゲット広告や広告効果測定を目的として、他社のApp、Webサイト、またはオフラインのプロパティから収集されたユーザーやデバイスに関するデータに紐付ける行為を指す。また、ユーザーやデバイスに関するデータをデータブローカーに共有することもトラッキングに該当する。	・利用者がパートナーのサービスを訪問、利用した場合、またはパートナーが連携する外部パートナーを通して、パートナーは利用者のデータを受け取る。これらのパートナーが当社にデータを提供する前に、パートナーが利用者のデータを取得、利用、共有する正当な権利を有していることを当社は当該パートナーに要求する。	・第三者とのユーザーの情報共有に関するポリシーは、プライバシーポリシーの「ご自分の情報の共有」に規定されている。プライバシーポリシーはすべてのユーザデータ及び第三者についてグローバルに適用される。詳細は 1-3参照。 ・ユーザーのデータを匿名化、統計化し個人が特定できない形で第三者と共有することがある。	・LINEアプリにサードパーティが情報を取得するモジュールを設置する場合、情報を取得する事業者の名称、取得される情報の項目、利用目的等について、ユーザーへ情報提供を行っている。	・Yahoo! JAPANのサイトでは、提携先が、ユーザーのコンピュータにクッキーを送信・保存し、これを利用してYahoo! JAPANのサイトを訪れたユーザーの情報を蓄積・利用している場合があり、プライバシーセンターの「第三者の配信する行動ターゲティング広告（第三者によるクッキーの利用）について」において連携先を公表している。 ・Yahoo! JAPANのサービス等の利用状況を調査するために市場調査会社やサービスの利用状況分析ツール提供会社に対して、Yahoo! JAPANのサービス等に掲載された広告の効果を測定するためや、より適切な広告を配信したりするために広告効果測定ツール提供会社や広告主・広告代理店に対して、よりユーザーに合ったコンテンツを提供するために、パートナー企業に対して、クッキーの設置やアプリ開発キットの組み込みなどによる情報の直接取得を認めており、プライバシーセンターの「パーソナルデータの取得」の「パーソナルデータを第三者が直接取得する場合」において説明している。
5-2.	**フィンガープリント、Unified ID 2.0 等のクッキーの代替手段での代替取得の動きについての考え方**	・2-1 の「プライバシー 機能」の「『フィンガープリント』作成の防止」記載のとおり、Safari は、広告主やウェブサイトが個々のデバイスが持つ特性のユニークな組み合わせを使って「フィンガープリント」を作成し、ユーザーを追跡するのを防ぐ。簡略化されたシステム構成を提示し、トラッカーの目に多数のデバイスが同一に見えるようにすることで、各ユーザーのデバイスを特定しにくくしている。	・ここ数年、当社が取り組んできた方法のひとつであり、今後も優先的に取り組んでいくものが、プライバシー保護技術（PET）への投資である。これは、より少ない個人データを処理しながらパーソナライズされた広告を提供することを目的としている。例えば、人々のデバイスに残っているデータを使ってアルゴリズムを学習する方法を検討している。また、プライバシーに配慮した広告測定システムの構築に向けた業界の取り組みをリードしており、いくつかの技術をオープンソース化して他社が利用できるようにしている。 ・World Federation of Advertisers（世界広告主連盟）のクロスメディア測定イニシアチブなど、業界のイニシアチブに参加し、高度な広告ユースケースを可能にするプライバシー重視の測定システムの構築を支援している。	・プライバシーサンドボックスの重要な目的は、個別ユーザーに関するデータを共有したり秘密裏に追跡したりする、不透明もしくはユーザーから見えない技術から、人々を保護する技術を開発することである。（これはフィンガープリントとして広く知られている。） ・一例としては、端末のIPアドレスを悪用して、オプトアウトの知識がない利用者やオプトアウトの選択肢がない利用者を特定しようとするといった手法があげられる。Chromeは、ウェブサイトの通常の動作を妨げることなく利用者の アイデンティティ を保護するために、IPアドレスをマスクする方法の新たな仕様提案として Gnatcatcher（https://github.com/bslassey/ip-blindness）を公開した。他の提案仕様と同様に、ウェブコミュニティからのフィードバックに基づき今後も改良を続けていく。 この点に関するGoogleの考えに関する詳細は https://japan.googleblog.com/2021/02/2021-privacy-sandbox.html参照。	・当社の広告事業では、フィンガープリント、Unified ID 2.0といったクッキーの代替手段を導入する予定は今のところない。	・広告事業において、現在の3rd Party Cookieによる場合よりもユーザーのプライバシー保護を担保できる代替手段があれば導入を検討する可能性はあるが、現時点で代替手段による情報取得の予定はない。
6．アプリ提供マーケット						
6-1.	**SPI に関する取組状況**	・SPIを、参照すべき政府ガイドラインの１つとして強調している。（ドキュメント ユーザーのプライバシーを保護する（https://developer.apple.com/jp/documentation/uikit/protecting_the_user_s_privacy/）） ・App のディベロッパーに対し、App Store Reviewガイドライン（https://developer.apple.com/jp/app-store/review/guidelines/#legal）「5.1.2 データの使用と共有」と、App Store でのApp のプライバシーに関する詳細情報の表示（https://developer.apple.com/jp/app-store/appprivacy-details/）で、プライバシーポリシーの記載、利用者情報の取扱等について詳細に規定。例えば： －すべてのAppには、App Store Connectのメタデータフィールドと各App内にアクセスしやすい形で、プライバシーポリシーへのリンクを必ず含める必要がある。プライバシーポリシーはわかりやすく明確なものである必要がある。 －ユーザーや使用状況に関するデータを収集するAppでは、収集するデータが収集の時点またはその直後の時点で匿名であると考えられる場合でも、そのデータ収集に関してユーザーから同意を得る必要がある。 －有料の機能は、ユーザーデータへのアクセスをユーザーが許可することを条件とすることはできない。 －Appでは、簡単にアクセスできるわかりやすい方法でユーザーが同意を撤回できるようにする必要がある。 －必ず、「目的」でデータの用途を明確かつ十分に説明する必要がある。 －Appでは、ユーザーのアクセス許可設定を尊重する必要がある。 －不要なデータアクセスに同意するようユーザーを誘導したり、だましたり、強制したりすることは許されない。可能であれば、アクセスに同意しないユーザー向けに別の方法を用意してすることが推奨される（たとえば、位置情報の共有に同意しないユーザーには、住所を手動で入力できる機能を用意することができる、など）。 －ユーザーに情報を視覚的に提示する際は、必ずSafariViewControllerを使用する必要がある。SafariViewControllerを非表示にしたり、別のビューやレイヤーで隠したりすることは許されない。また、SafariViewControllerを使用して、ユーザーの認知や同意なしにAppでユーザーのトラッキングを行うことは許されない。		・Google Playは、アプリやゲームがユーザーのデバイス上でアクセスしようとしているデータについて、ユーザーが十分な情報を得た上で、判断できるような支援に努めている。その取り組みの一環として、Google Playストアのアプリの掲載情報に個人情報の収集と使用の方法を開示するよう、デベロッパーの皆様に義務付けている。詳細については、「How Play works」のウェブサイト（https://play.google.com/intl/ja_jp/about/howplayworks/）を参照。		
6-2.	**アプリケーションプライバシーポリシーの作成や利用者情報取扱いの透明性確保の観点からのアプリ提供者に対する働きかけや情報提供**			・セキュリティに投資しており、デベロッパーによる悪用や不正を検出する、いくつものシステムを導入している。例えば、デベロッパーによるユーザーの情報へのアクセスについて定めた Google API利用規約は、デベロッパーが収集、使用、他者と共有する利用者情報について明確かつ正確に定めたプライバシーポリシーを提供し遵守することを義務付けている。また、デベロッパーが明示的な「オプトイン」の同意なく、利用者の非公開データを他の利用者やサードパーティに開示することや、スクレイピング、データベース構築、その他利用者データの恒久的コピーを作成することも禁止している。 ・Googleの APIサービス利用者データポリシーは、デベロッパーがユーザーのGoogleアカウント データにアクセスするための許可を求めることを義務付けている。それらのアクセス許可の要求は、ユーザーにとって合理的なものでなければならず、アプリ実装に必要な情報に限定される必要がある。デベロッパーは、アプリの既存機能やサービス実装に必要な Google ユーザーのデータへのみ、ユーザーへアクセスを求めることができる。 ・Google Playでは、アプリとゲームがデバイス内のどのようなデータにアクセスを求めるかについてユーザーが十分な情報を得た上で判断できるよう支援している。この取り組みの一環として、以前から、デベロッパーがGoogle Playストアのアプリリストで、どのようにユーザーの情報を収集し使用しているかを開示することを義務付けてきた。2015年にAndroid Marshmallowを発売した時には、利用者がいつでも、自身のデバイスでこまめに許可を確認、付与、拒否できるランタイム権限を導入した。		

社名		Apple Inc.	Facebook Japan株式会社	Google LLC	LINE株式会社	ヤフー株式会社
7．PIA・アウトカムについての考え方						
7-1.	**PIA の導入状況 （GDPR の DPIA の具体的なに実施方法や、その他の実施事例）**	・GDPR 及び人権活動の一環として、主な製品やサービスについてPIAを行うとともに、新たな製品やサービスを開発するにあたってPIAを統合している。レビューは、アルゴリズムシステムに依拠した意思決定があるか否か、当該意思決定による個人や人権への影響を評価することを含む。リスクレベルが、識別されたリスクによって1年から2年にわたる再評価期間とともに全てのデータ利用に割り当てられる。もしもアルゴリズムシステムの開発に個人データが利用されている場合には、ユーザーのために、Appleの業界を牽引するコントロールに合わせて、ユーザーがそれらのデータ利用に同意しコントロールする手段を提供する。また、当社のPIAプロセスの一環として、全ての企業買収でプライバシー慣行を十分に評価することもしている。PIAでは、当社がビジネスを行う関連法域において法律がどのようにプライバシーに影響を与え、関連するプライバシー リスクをどのように評価するのかを考慮する。 （プライバシー・ガバナンス（https://www.apple.com/legal/privacy/en-ww/governance/））	・プライバシー・レビュー・プロセス（以下、「プライバシー・レビュー」）を導入している。プライバシー・レビューは、人々の情報の収集、使用、または共有及び、当社のプライバシーおよびセキュリティ慣行に関する外部への説明に係るプライバシー・リスクを評価するプロセスである。また、このプライバシー・レビューは、当社が特定したプライバシーリスクを識別し、軽減するためのものでもある。 プロダクトや機能の開発、新規または慣行の見直しは、プライバシーに関する以下のような観点から行われる。 － 目的の限定：人々に価値を提供する、限定された明確な目的のためにのみデータを処理する。 － データの最小化：明確な目的を達成するために必要な最小限のデータを収集・作成する。 － データの保持：明確に示された目的を遂行するために実際に必要とされる期間のみ、データを保持する。 － 外部からのデータ誤用：データの乱用、偶発的な損失、および権限のない第三者によるアクセスからデータを保護する。 － 透明性と管理：プロダクトの動作やデータの取り扱いについて、積極的に、明確に、正直に伝える。可能な限り、また適切な場合には、人々が管理できるようにする。 － データへのアクセスと管理：弊社が収集または作成したデータに人々がアクセスし、管理できるようにする。 － 公正さ：弱い立場にある人々のリスクを特定して軽減し、人々のために価値が創造されるようなプロダクトを構築する。 － 説明責任：当社の意思決定、プロダクト、業務に関わる内部プロセスおよび技術のコントロールを維持する。 ・プライバシー・レビューは、当社のコンプライアンス義務を評価して遵守し、法的要件を超えた広範なプライバシーリスクを特定して軽減するために使用される、深く協力的で部門横断的なプロセスである。プライバシー・レビューは、プライバシーチームが主導し、プロダクト、エンジニアリング、法的規制、セキュリティ、ポリシーなどのバックグラウンドを持つ、法務、ポリシー、その他を含めた横断的なチームに所属する社内のプライバシー専門家の専門家グループが実施している。このグループは、プライバシー審査の決定と提案を行う役割を担っている。 ・プライバシー・レビューの一環として、 横断的なチームは、プロジェクトに関連するプライバシーリスクを評価し、それらのリスクをコントロールするために発売前に行う必要のある変更があるかどうかを判断する。横断的なチームのメンバー間で何をすべきかの合意が得られない場合、チームはより上層のリーダーシップに諮り、解決のために必要であればさらにCEOに諮る。	・プライバシーとセキュリティに対する Googleの投資は、すべてのプロダクトにおいて一貫している。Googleの製品や機能は、Google社内全体からの意見に加えて、世界中のユーザーや専門家から定期的に意見を募る。Googleのプライバシーとデータ保護オフィスの専門家の承諾を得るまで提供を開始することはない。	・当社では、PIAを導入している。具体的には、新規サービス・機能のリリース時等にPIAを実施し、プライバシーへの影響を評価している。	・2-5のとおり、当社のガバナンスシステムが適切に機能することを担保するための取り組みとして、プライバシー影響評価（PIA）の試験運用を始めており、本格運用を目指して取り組みを進めている。
7-2.	**利用者情報の取扱いに関するアウトカムについての検討状況 （検討している場合、どのような考え方に基づき判断しているか）**	7-1参照。	・全社的なプライバシーリスクを特定、評価、対処するための年次評価を行うとともに、事故発生後にプライバシーリスクを評価するプロセスを実施するプライバシーリスク評価プログラムを設計している。今後、時間をかけて評価しながら、プライバシーリスク評価プロセスを進化・成熟させていく。 ・新しいプロダクトや機能にプライバシー・バイ・デザインを確実に組み込むための説明責任プロセス、セーフガード、技術的メカニズムを構築した。		・PIAを実施する際、プライバシーの観点における影響の有無・程度、利用者への不利益の有無、利用者の予想に反して情報が外部に公開されないか、利用者が気持ち悪いと感じないかなどといった点を考慮している。	・2-5のとおり、当社のガバナンスシステムが適切に機能することを担保するための取り組みとして、プライバシー影響評価（PIA）の試験運用を始めており、本格運用を目指して取り組みを進めているが、この中でユーザーに提供する便益とデータの利用によるユーザーへの影響のバランスが取れているか考慮される予定。
7-3.	**利用者に対する、PIA の結果やアウトカムの説明の取組状況**	プライバシー・ガバナンスについて以下を参照。 https://www.apple.com/legal/privacy/en-ww/governance/	・ニュースルームの投稿（「データを安全に転送するための手順」など）、データポリシー、透明性レポート、利用者へのグローバルな通知と更新、Facebookヘルプセンター（利用者がプライバシーや共有の設定を行う際に利用できる「プライバシーチェックアップ」など）を通じて、プライバシーに関する決定事項を明らかにしている。		・PIAの結果を踏まえて、サービス・機能の実装の際に説明やチュートリアルを追加する等の対応を行っている。	・PIAの本格運用にあたって検討予定。