資料１

プラットフォームサービスに関する研究会

主要論点（案）

２０１９年　月

目次

第１章　プラットフォームサービスの拡大に伴う利用者情報の取扱いの確保に係る検討の背景

○　近時のスマートフォンの普及やIoTの進展により、様々なヒト・モノ・組織がネットワークに繋がり、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 によるデータ解析等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本格的な「データ主導社会（Data Driven Society)」の実現が志向されている。

○　また、こうしたICTの進展は、従来の産業・ビジネスのバリューチェーンの各要素の分離（モジュール化)、ひいては市場のレイヤ構造化をもたらしており、これにより、多様なサービスを提供するサプライヤー及びそれらのサービスを享受するユーザの双方が利用する基盤としての機能を有するプラットフォームレイヤがビジネスの拡大に重要な役割を果たすようになり、同機能を提供する事業者（以下「プラットフォーム事業者」という。）が市場プレゼンスを増大させるようになっている。

○　このようなICTの進化と市場のレイヤ構造化を背景として、サイバー空間とフィジカル空間を跨いでデータを活用し、プラットフォームを通じて新たなサービスを提供する形態のビジネスモデルの創出が可能となっている。例えば、オンライン上におけるシェアリングエコノミー型のサービス、検索サービス、SNS、ショッピングモール、アプリストア、オークションやフリーマーケットなどの消費者参加型のｅコマース（電子商取引）等の新たなサービスやビジネスが普及・拡大しつつあるが、簡便な操作性とコストの低廉性を兼ね備えたこれらのサービスやビジネスは、ICTの進化と市場のレイヤ構造化に伴って実現したプラットフォーム機能が下支えすることにより初めて提供可能となるものであり、プラットフォームサービスはイノベーションを促進する存在として、また、社会基盤として今後さらに重要な役割を果たしていくことが見込まれる。

○　また、プラットフォームサービスの中には、ヒトやモノの間のコミュニケーションを可能とする機能を提供するものが多く、こうした電気通信サービス・機能とプラットフォームサービス・機能を一体的に提供する形態のビジネス・サービスは今後とも拡大・普及が進んでいくものと考えられる。

○　他方、プラットフォーム事業者がサービスを提供するに当たって取得・利用する大量のデータの中には多くの利用者情報が含まれているが、その利用メカニズムがわかりづらいとの声もあり（中には「ブラックボックス化している」との声も聞かれる。）、利用者の不安・懸念が高まっている。また、国内にサーバなどの設備を設置せずとも、メッセージサービスやSNSなど、電気通信事業者により提供される通信サービスと同様の、又は類似したサービスがプラットフォーム事業者により多様な形態で提供されている。こうした中、通信の秘密やプライバシー保護の観点から、現行の電気通信事業法における規律の趣旨が適切に確保されているか、確保されていないとすればどのような点が課題となるか検討することが必要となっている。

○　さらに、EU における「一般データ保護規則（GDPR：General Data Protection Regulation）」[1]の施行や「e プライバシー規則（ePrivacy Regulation）」[2]の提案等の動きに窺えるように、国際的なプライバシー保護の潮流との制度的調和の観点も勘案し、プラットフォームサービスの普及に伴うグローバルな市場環境に即した政策対応が求められるようになっている。

○　このほか、グローバルなプラットフォームサービスにおいて ID を活用して様々なサービスを利用できるようにする ID 連携が進展している中、通信の相手先となる人や組織の正当性の確認や認証にとどまらず、ネットワークにつながるモノの認証やネットワーク上を流れるデータの完全性（Data Integrity）の確保等を実現するため、我が国のトラストサービス（電子署名、利用者認証、タイムスタンプ等）の在り方について、EU における「eIDAS 規則」[3]の制定等の動きも踏まえ、相互運用性の確保の観点からも、包括的な政策対応が求められる。

○　加えて、EU では、オンライン上のフェイクニュースや偽情報対策が喫緊の課題であるとして、欧州委員会は「オンライン上の偽情報への対処：欧

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[2] Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

州のアプローチ（Tackling online disinformation：a European Approach)」[4]と題する政策文書（報告書）を公表（2018年４月）し、フェイクニュースや偽情報に対応するためのプラットフォーム事業者の行動規範（Code of Practice）の策定を求め、今後、当該行動規範をレビューすることとしており、我が国においても、プラットフォームサービスを通じて流布されるフェイクニュース等への対応の検討が必要になっている。

○　このため、今次「電気通信事業分野における競争ルール等の包括的検証」の一環として、プラットフォームサービスにおける利用者情報の適切な取扱いの確保の在り方等について、提案募集で寄せられた意見、ヒアリングにおける意見、これまでの会合における討議等に基づき、検討アジェンダを踏まえ、イノベーションの促進の観点及び通信の秘密やプライバシー保護の観点から政策対応を検討する上で必要となる主要論点の整理を行ったものである。

[4] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach

《参考1》プラットフォームの定義について

① これまでの政府文書等におけるプラットフォームの定義

○ 「複数のネットワーク・端末をシームレスにつなげ、様々なアプリケーションを提供しやすくするための共通基盤」
（ユビキタスネット社会におけるプラットフォーム機能の在り方に関する研究会（2005年））

○ 「物理的な電気通信設備と連携して多数の事業者間又は事業者と多数のユーザー間を仲介し、コンテンツ配信、電子商取引、公的サービス提供その他の情報の流通の円滑化及び安全性・利便性の向上を実現するサービス」
（通信・放送の総合的な法体系に関する研究会（2007年））

○ 「通信レイヤー上でコンテンツ・アプリケーションを円滑に流通させる機能」
（通信プラットフォーム研究会（2009年））

○ 「ICT ネットワーク、とりわけインターネットにおいて、多数の事業者間ないし多数の事業者とユーザー間を仲介し、電子商取引やアプリ・コンテンツ配信その他の財・サービスの提供に必要となる基盤的機能」（情報通信白書（2012年版））

② EU 文書（「欧州のためのオンライン・プラットフォーム及びデジタル単一市場の機会及び挑戦」）における定義

- 総括する定義をせず、オンライン・プラットフォームの例と共通する特徴のみを示している。

- 例示：
  オンライン広告、検索エンジン、ソーシャルメディア、アプリケーション配信プラットフォーム、通信サービスなど。

- 特徴：
  (1) 大規模なデータの収集、処理、編集により新たなビジネスを創出し、新たな市場を作り上げる能力を有する。
  (2) 多面市場で事業を行うが、各市場におけるコントロールの程度は様々である。
  (3) 「ネットワーク効果」による便益を受ける。
  (4) 情報通信技術を利用し、瞬時かつ容易に利用者に到達する。
  (5) データ収集等の重要価値の利用、戦略的依存の構築等で、デジタル分野の価値創出において重要な役割を担う。

第２章　電気通信分野における利用者情報の取扱いに係る現状

第１節　電気通信分野における利用者情報の取扱いに係る法制度等の現状

１．通信の秘密の保護

○　日本国憲法第21条は、基本的人権の一つとして表現の自由を保障するとともに（第１項）、通信の秘密の保護について規定している（第２項後段）。同条は、表現の自由の保障と通信の秘密の保護を併せて規定している点で我が国の憲法に特徴的なものである。すなわち、憲法において通信の秘密を保障する意義は、プライバシーの保護にとどまらず、国民の表現の自由や知る権利を保障すること、さらに、国家権力が自ら通信の秘密を侵害しないのみならず、私人による侵害から通信の秘密を保護すること、言い換えれば、国民が安全に安心して通信を利用できるよう通信制度を保障することにより、国民の通信の自由を確保することにあると考えられる。

○　電気通信事業法（昭和59年法律第86号）においては、通信の秘密の保護に関して「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」（第４条第１項）と定めている。同規定は、上記憲法上の要請を担保するために法律レベルで具体化したものであると考えることができる。つまり、同法の通信の秘密の保護規定は、これによって電気通信事業者を含めて何人からも通信がみだりに侵害されないよう利用者の通信を保護し、もって利用者が安心して通信を利用できるようにすることで、表現の自由や知る権利を保障するとともに、電気通信ネットワークや通信制度そのものへのユーザの信頼を確保し、インターネット上での多様なサービスやビジネス提供の拡大による電気通信の健全な発展と国民の利便の確保を図ることが、その意義であると考えられる。

○　こうした趣旨に鑑み、「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれると従来より整理がされている。

○　また、通信の秘密の侵害行為には、「知得」（積極的に通信の秘密を知ろうとする意思のもとで知得しようとする行為）、「窃用」（発信者又は受信者の意思に反して利用すること）、「漏えい」（他人が知り得る状態に置くこと）の３類型がある。ただし、利用者の同意がある場合には、通信の秘密の侵害に当たらないほか、通信の秘密を侵害した場合であっても、正当行為（刑法（明治 40 年法律第 45 号）第 35 条）、正当防衛（同法第 36 条）、緊急避難（同法第 37 条）に当たる場合等違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容される、と解されている。

○　特に電気通信事業者には、通信の秘密の厳格な保護が求められており、通信の秘密の侵害罪について電気通信事業者にはより重い量刑が科されるとともに（電気通信事業法第 179 条第２項）、業務の方法に関し通信の秘密の保護に支障があるときには、総務大臣が業務の改善を命ずることができる旨が規定されているほか（同法第 29 条第１項第１号）、電気通信事業者による通信の秘密に属する事項の具体的な取扱いについての指針等が総務大臣により策定されており（例えば「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）など。）、これらによって、電気通信事業者による通信の秘密の厳格な保護が確保されている。また、登録・届出を要しない電気通信事業を営む者についても、「検閲の禁止」「通信の秘密」に関する規律が適用される（同法第 164 条第１項、第３項）。

○　なお、現行の電気通信事業法は、国外に拠点を置き、国内に電気通信設備を有さずにサービスを提供する者には、日本国内の利用者に向けてサービスを提供する場合であっても規律が及ばない、との運用がなされている。

２．電気通信事業における個人情報の保護

○　電気通信事業は、上記のとおり通信の秘密と直接関わる事業であり、また、通信の秘密に属さない情報であってもプライバシー保護を必要とする多くの情報を取り扱うことから、そこで取り扱われる個人情報を保護する必要性は大きい。電気通信サービスの高度化・多様化は国民に大きな利便をもたらしている反面、これらの電気通信サービスの提供に伴い取得される個人情報が不適正な取扱いをされると、個人に取り返しの

つかない被害を及ぼすおそれがある。

○　こうしたことを踏まえ、電気通信事業を行う者に対し、通信の秘密に属する事項その他の個人情報の適正な取扱いについてできるだけ具体的な指針を示すことにより、その範囲内での自由な流通を確保して電気通信役務の利便性の向上を図るとともに、利用者の権利利益を保護することを目的として、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び電気通信事業法の関連規定に基づく具体的な指針として、「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」（以下「ガイドライン」という。）が総務大臣により定められている。同ガイドラインは、「個人情報の保護に関する法律についてのガイドライン」（平成 28 年 11 月 30 日個人情報保護委員会）の規定に準拠しつつ、通信の秘密その他の電気通信事業に特有の事情等に鑑み必要となる規定も併せて、電気通信事業を行う者に適用される規律を一元的に示したものとなっている。

第２節　IoT 化・デジタル化の進展に伴う電気通信分野における変化の現状

１．利用者情報を始めとするデータの流通量の飛躍的増大

○　近年の AI や IoT 化、デジタル化の進展によるサイバー空間とフィジカル空間の融合の加速化に伴い、様々な事象のデータ化により大量かつ多様なデータが生成・集積され、データ流通がグローバル規模で飛躍的に増大している。スマートフォン、タブレット端末の急速な普及と利活用の拡大、HD（高精細）映像などの高品質・リッチコンテンツの流通がデータ流通量の増大に寄与し、さらに今後の超高速・広帯域の 5G の実現などブロードバンドネットワークの拡大により利用できるサービスが多様化することから、その利用者の更なる拡大が見込まれる[5]。

○　様々なヒト・モノ・組織がネットワークに繋がるようになれば、多くの分野や業種においてモノとモノとの間のデータのやりとり（いわゆる M2M（Machine-to-Machine）通信）が飛躍的に増加するのみならず、利用者情報の流通も増大することが想定される。

○　なお、特にプラットフォームサービスにおいては膨大な利用者情報が集積されるが、昨今、国外に拠点を置いてグローバルにプラットフォームサービスを提供する事業者による利用者情報の大量流出事案が相次いでいる。また、そうした状況において、我が国の利用者の利用者情報の取扱いや被害状況の詳細が必ずしも明らかにされない等により、ユーザの懸念が高まっている。また、サイバー攻撃に伴う利用者情報の漏えいリスクへの懸念も高まっている。

２．産業・ビジネスのレイヤ構造化を始めとする市場構造の変化

（１）レイヤ構造化によるプラットフォームのプレゼンスの増大

○　近時、デジタル化の急速な進展に伴ってもたらされる、モジュール

[5] IDC の調査レポート（2018 年 11 月）によると、世界のデータ量は 2018 年の 33ZB（ゼタ：10 の 21 乗）から 2025 年には 175ZB に達すると予測している。また同レポートによると、現在、世界で 50 億人以上の利用者が毎日データをやり取りしているが、それが 2025 年までに世界人口の 75%に相当する 60 億人まで増加し、インターネットに繋がる全ての人が 18 秒に 1 回以上のデータのやり取りを行うと予測している。データ量が加速的に増加する要因としては、世界中で繋がる数十億台の IoT デバイスが挙げられており、これにより 2025 年には 90ZB 以上のデータが生成されるとしている。

化、ソフトウェア化、ネットワーク化により、企画・調達・製造・販売といった各業務・工程が連鎖的に繋がり、最終的な価値を生み出す既存のバリューチェーン構造からバリューチェーンを構成する各要素の分離が進み、業種の垣根を越えた連携や統合の進展等によるレイヤ構造化を始め市場構造が変化している。

○　こうした状況の下、業種横断的なプラットフォーム領域を形成し、アプリケーション等の様々なサービスを提供するサプライヤー及びそれらのサービスを享受するユーザの双方が利用する基盤を提供するプラットフォーム事業者が市場プレゼンスを増大させるようになっている[6]。

○　プラットフォームサービス・ビジネスの例としては、オンライン上におけるシェアリングエコノミー型のサービス、検索サービス、SNS、動画配信、ショッピングモール、アプリストア、オークションやフリーマーケットなどの消費者参加型のｅコマース（電子商取引）等が挙げられる。

○　プラットフォームを通じたこれらのサービスの提供形態は、提供するサービスの内容等に応じて、水平統合、垂直統合若しくは垂直分離又はそれらの混合形態など、多様な形態が窺えるものとなっており、一律にプラットフォームサービスの提供形態を論じることはできないが、今後もICTの進化によってレイヤ構造化が進展すると考えられることから、プラットフォームサービスはイノベーションを促進する存在として、また、社会基盤として、今後さらに重要な役割を果たしていくと予想される。

（２）電気通信サービス・機能とプラットフォームサービス・機能の一体的な提供形態の普及・拡大

○　プラットフォーム事業者の提供するサービスを見ると、ヒトやモノの間のコミュニケーションを可能とする機能を提供するものが多くあり（電気通信事業法に根拠を持つ、従来からの電気通信役務と整理

6 PwCの調査レポートによれば、2018年３月末時点における世界の時価総額ランキングでは、アップル、グーグル（アルファベット）、マイクロソフト、フェイスブックの米国系５社、テンセント、アリババの中国系２社のグローバルプラットフォーム事業者がトップ10にランクインし、2009年３月末時点との比較で分かるように、著しいスピードで急成長を続けている。

できるサービスの場合や、電気通信事業として整理ができないものの、外形的には電気通信役務に類似したサービス又はそれらの混合形態の場合などがあり、複雑な態様となっていることが多い。)、こうした電気通信サービス・機能とプラットフォームサービス・機能を一体的に提供する形態のビジネス・サービスは今後とも拡大・普及が進んでいくものと考えられる。

○　また今後、電気通信分野において提供される通信サービス自体も、デジタル化の進展と相俟って AI や IoT などの最新技術を駆使したものに変遷・進化していくと考えられるとともに、通信ネットワークにおける仮想化技術の進展により、その提供形態についても、電気通信設備（ハード）と機能（ソフト）を分離した形でのビジネスモデルへと変化していくことが想定される。そして、それに伴い新たなスタイルを有するプレイヤが登場することも考えられる。すなわち、通信サービスの提供主体の質・量がともに変貌し、既存のスタイルに囚われない電気通信事業者の登場や電気通信事業者とプラットフォーム事業者との協業や連携・融合が進み、市場環境が一変することも想定される。

3.グローバルなプラットフォーム事業者の台頭に伴う、利用者情報のグローバルな流通の進展

○　プラットフォームは、ネットワークとコンテンツやアプリケーションとの間を繋ぐ共通的な機能を有することから、垂直統合する場合と比較してコンテンツやアプリケーションを機動的に提供できる。このため、ネットワーク効果（利用者が増加すればするほどサービスの価値が高まる経済原理）が働き、コンテンツやアプリケーションが多様となることに伴い利用者数が増加し、その結果、サービス価値がより増加するとのシナジーが生まれることとなる。

○　こうしたプラットフォーム機能の特徴から、プラットフォーム事業者は国境を越えてグローバルにビジネスを展開し、より多くのユーザを対象とすることで、より多くの成功を収めることが可能となっており、我が国においても、こうした国外のグローバルプラットフォーム事業者のプレゼンスが大きくなっている。

○　グローバルなプラットフォーム事業者は、グローバルな規模で利用者情報を始めとする大量のデータを取得・利用することが可能となることから、こうした国境を越えたデータ流通の拡大を背景にして、諸外国においても、利用者情報の適切な取扱いに係るルールの整備や議論が行われている。

４．利用者情報の取得・活用に対する、サービス提供者のニーズの高まり

（１）利用者情報の取得・活用のインセンティブ

○　ICT の進展と市場環境の変化により、斬新で革新的なサービスを利用者が享受できるようになる一方で、プラットフォーム事業者を含む電気通信分野におけるサービス提供者は、より付加価値の高いサービスを利用者に提供するために、利用者情報をより積極的に取得し、かつ、活用しようとするインセンティブが働くことが考えられる。

○　例えば、検索連動型広告に見られるように、プラットフォーム上では、利用者は無料でサービスを利用できる一方、企業は広告料を支払うことにより利用者に対し自社の商品を PR するといった両面市場（Two sided market）のモデルが適用されることにより、サービス提供者が利用者情報を取得し、かつ、活用するインセンティブが働きやすい。

（２）利用者情報の取得・活用に係る利用者保護の必要性

○　このような利用者情報の取得・活用が新たなサービスを生み出し、利用者に最適なサービスを提供するとのスパイラルの中で、利用者はサービスに魅力を感じ、サービス規約に同意し、併せてプラットフォーム事業者による利用者情報の取得・活用にも同意することとなるが、前述のとおりサービス提供者にはできるだけ利用者情報の取得・活用の同意を得ようとするインセンティブが働くことが考えられることから、利用者の保護の観点から、同意取得に当たっては、サービス提供者から利用者に対して、取得する利用者情報の種類や利用方法等についてわかりやすい説明が行われるよう確保することがより一層重要となる。

○　また、利用者情報を活用したビジネス・サービスの提供に当たっては、データの寡占化によるロックイン（囲い込み）により、利用者の選択肢が狭められる可能性も考えられる。すなわち、近時のブロードバンド化やスマートフォンの急速な普及等を背景に、クラウド上のサービスが進展し、クラウド上にデータが集約されやすい構造となり、また、AI の更なる進展により質の高いデータセットの確保が競争優位性を左右する状況が生じており、プラットフォーム機能と不可分となっている。さらに、サイバー空間とフィジカル空間が融合する中で、リアルの世界でも利用者情報等のデータを集約する能力を持つプラットフォーム事業者がサービス面でも優位になる市場構造が形成されつつある。

○　こうしたデータ寡占によるロックイン効果の結果、電気通信分野において適切な競争が行われない、利用者にとって質の高いサービスが中長期的に提供されない、又は質の高いサービスの選択肢が与えられないなどの懸念が生じ得る。その場合、適切なデータ流通・利活用によるイノベーションの促進が阻害されるおそれがあるほか、更なるデータの集中・データの支配などのデータ寡占が進展すれば、電気通信分野における市場環境にも影響が及ぶこととなる。

５．パーソナルデータ提供等に係る利用者意識の変化

（１）パーソナルデータ提供に関する利用者の不安感の高まり

○　総務省の「安全・安心なデータ流通・利活用に関する調査研究」（平成 29 年）によれば、パーソナルデータの提供について「不安を感じる」という回答の割合は、日本、中国及び韓国のアジア３か国で７割超となっているのに対し、米国、英国及び独国の欧米３ヶ国は６割程度で明確な差があり、我が国の利用者は「とても不安を感じる」割合が他国と比べて高い。

○　また、６か国共通で提供に強い不安感があるデータは、「口座情報」、「公的な個人識別番号」、「生体情報」、「位置情報、行動履歴」となっている。特に、アジア３か国では、基本情報である「氏名、住所」、「連絡先」及び「生年月日」が欧米３か国に比べて警戒心が強く、我

が国では、「Web サイトへのアクセス履歴」の提供に対する不安感が６か国の中で最も高い[7]。

（２）プラットフォーム事業者の情報管理態勢に対するユーザの懸念

○　利用者はプラットフォームを介して多様なサービスを享受することができる反面、プラットフォーム事業者は膨大な利用者情報を取得・利用しており、特に昨今、国外に拠点を置いてグローバルにプラットフォームサービスを提供する事業者による利用者情報の大量流出事案が相次いでいるが、そうした状況において、我が国の利用者の利用者情報の取扱いや被害状況の詳細が必ずしも明らかにされない等により、ユーザの懸念が高まっている。

○　こうした「ブラックボックス化している」とも言われる利用者情報の利用メカニズムや大量流出事案が相次いでいる現状に鑑みれば、プラットフォーム事業者の情報管理態勢への不信感は払拭されているとは言い難い。

（３）いわゆる「同意疲れ」

○　一方、利用者情報の取得が増えるにつれて、累次の同意が繰り返される結果、利用者情報取得の同意に対する利用者の抵抗感が希薄となっていく局面も想定される。通信の秘密に係る利用者情報の取扱いについて有効な同意と言えるためには、従来原則として「個別具体的かつ明確な同意」が必要とされているが、あまりに多くの同意取得手続きが繰り返されることで、かえって利用者が十分に理解しないままに同意をしてしまう、いわゆる「同意疲れ」の問題が今後大きくなっていくことが予想される。

○　なお、これに関連して、例えば、現下の市場では利用者情報が集積される場合には、その都度それを示すアイコンを表示する機能をデバイスに具備させることにより、利用者に明示的に注意喚起を行うプライバシー・バイ・デザインを志向する動きもある。

[7] このほか、本調査による他の項目の国際比較においても、我が国の利用者は利用者情報に対して概して敏感に不安感を感じていることが窺える。詳細は参考２を参照。

《参考2》 パーソナルデータ提供等に係る利用者意識の調査結果

① パーソナルデータ提供時の利用目的等の理解度（国際比較）

○ パーソナルデータ提供時の利用目的等の理解度について見ると、韓国を除く5か国の利用者の理解度は、「明確に理解」と「大体理解」とを合わせて8割を超えている。

○ また、パーソナルデータの利用目的等の確認状況について見ると、「必ず確認する」、「大体確認する」、「サービス・アプリケーションによっては確認する場合がある」とを合わせた結果と前述の理解度とは比例関係にあり、韓国を除く5か国では確認状況と理解度との間に一定の相関が見られる。

（以上、総務省「安全・安心なデータ流通・利活用に関する調査研究」（平成 29 年））

② パーソナルデータの提供時における理解度と不安感等

○ 我が国においては、パーソナルデータ提供時に不安を感じる者がその利用目的の理解度が高く、利用目的をよく確認する傾向にある。

○ 一方、パーソナルデータ提供時に不安を感じない者は、不安を感じる者と比べ、その利用目的を確認・理解していない割合が高い傾向にある。

（以上、総務省「パーソナルデータ提供等に係る消費者向け国際アンケート調査」（平成 29 年））

③ パーソナルデータ提供時の不安感とサービス利用状況との関係

○ 我が国におけるウェブメール、SNS、インターネットショッピング・オークション、情報検索・ニュース、動画視聴・音楽視聴、地図・ナビゲーションのサービス利用におけるパーソナルデータ提供時の不安割合は、いずれも5割を超えており、特にウェブメールと動画視聴・音楽視聴については、不安を感じる者の割合が不安を感じない者の割合を上回っている。

（総務省「パーソナルデータ提供等に係る消費者向け国際アンケート調査」（平成 29 年））

○ インターネット利用時に感じる不安の内容として、「個人情報やインターネット利用履歴の漏えい」が8割を超えており、「コンピュータウィルスへの感染」（約7割）、「架空請求やインターネットを利用した詐欺」（約5割）が続いている。

（総務省「平成 29 年通信利用動向調査」）

第３節　欧米等における利用者情報の保護等を巡る動き

１．GDPR による利用者情報の保護

○　EU では、デジタルサービスやコンテンツが EU 域内の国境を越えて自由に流通する「デジタル単一市場（Digital Single Market)」の構築を政策目標として、GDPR（一般データ保護規則）が制定され、2018 年５月より施行されている。

○　GDPR は、主として個人データの取扱い（処理）と移転を規律するものである。具体的には、個人（データ主体）の権利保護を明確化するため、識別された又は識別され得る自然人に関するあらゆる情報（any information）を個人データと定義し、その取扱いは個人データに係る全ての操作に関して適法性、公正性及び透明性を求めている。

○　そのほか、地理的適用範囲（域外適用を含む。）については、①個人データの取扱いが欧州経済領域（EEA：European Economic Area）内における管理者・処理者の拠点（establishment）の活動に関連して行われるもの、また、EEA 内に管理者・処理者の拠点がない場合であっても②EEA 内のデータ主体に物品・サービスを提供するもの、③EEA 内における個人の行動の監視については、GDPR の適用対象とされる（②及び③では、EEA 内の代理人（representatives）を指定）。

○　さらに、GDPR において新たに法的位置付けを付与され、導入された規律のうち注目すべきものとして行動規範（Codes of Conduct）[8]がある。

２．e プライバシー規則(案)における利用者情報の保護

○　GDPR に引き続き、インターネットベースのサービスの進展に伴う通信分野におけるプライバシー等の保護を拡充するため、通信の秘密等の適用対象を従来の通信サービス（traditional electronic communication service)に加え、ウェブメールや SNS などの OTT の通信サービス(Over-the-Top communications services）に拡大する e プライバシー規則

[8] 個人データの管理者又は処理者を代表する業界団体が策定する自主的な規律を指し、監督当局の承認を経ることにより、透明性のある個人データの取扱い等 GDPR の趣旨を踏まえたものとして取り扱われることとなるもの。

（ePrivacy Regulation）（案）の策定作業が進められている。

○ GDPR は全ての個人データ（all personal data）を保護対象とし、個人データの権利（the right of personal data）を規定するのに対して、e プライバシー規則（案）の保護対象は個人データか否かを問わず、通信と端末機器の情報（electronic communications and the integrity of the information on one's device）であり、通信の秘密とプライバシーの権利（right to the privacy and confidentiality of communication）を規定しようとするものであるほか、地理的適用範囲については、事業者の拠点が EEA 内か外かを問わず、EEA 内でのサービス提供があれば規制対象となる（拠点がない場合は代理人を指定）。

３．米国における利用者情報の保護

○ EU に呼応するように、米国でも動きが見られる。現在連邦レベルでは事業分野・情報の分野ごとの規律が存在しているが、包括的な保護法制は存在しない。州法レベルにおいても包括的な保護法制はみとめられなかったものの、近時包括的な保護法制として、カルフォルニア州消費者プライバシー法（CaCPA：The California Consumer Privacy Act of 2018）が成立し、同法ではカリフォルニア州に拠点のない事業者も規制対象（域外適用）となる可能性がある。なお、直近では包括的な連邦法を志向する動きも見られる。

○ 米国と EU の間では、個人データ移転についての原則を規定した「セーフハーバー協定（Safe Harbor）」（2000 年）が締結され、EU のプライバシー保護基準に沿ったルールを適用することにより米 EU 間の個人データの移動が可能となるものとしていたが、これが「プライバシーシールド」（2016 年）として引き継がれた。これに基づいて、米国企業はプライバシーポリシーを公表し（自主規制）、商務省に対して自己認証を行うこととし、仮に当該プライバシーポリシーに反した場合には FTC 法（Federal Trade Commission Act）に基づき執行されること等により履行確保が担保されている。

４．韓国における利用者情報の保護

○ 韓国では、憲法及び電気通信事業法において、通信の秘密を保護する規

定があり、情報通信網の利用及び情報保護等に関する法律（以下「情報通信網法」という。）においても、情報通信サービス提供者を対象に情報通信網における他人の秘密を侵害等してはならないとして、利用者情報の保護を図っている。2018 年、国外における韓国国民の利用者情報の流通の安全を確保することを目的に情報通信網法が改正され、国内に住所又は営業所がない情報通信サービス提供者に対して、国内代理人の指定を義務付ける規定が新設された。

５．多国間における利用者情報の保護

○　OECD では、1980 年に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」が採択され、附属文書である「プライバシー保護と個人データの国際流通についてのガイドライン」に OECD8 原則と総称される基本原則が示されている。本勧告は 2013 年に改訂され（同原則については改訂されておらず、規定の追加等が行われたもの。）、2018 年からは、2013 年の改訂から５年を契機として加盟国における履行状況のレビューが行われている。

○　また、欧州評議会（Council of Europe）では、1980 年に「個人データの自動処理に関する個人の保護のための条約(ヨーロッパ第108号条約)」が採択された。現時点で我が国は適用を受けるものとはなっていないが、プライバシー等の保護を拡充する動きがあるなど、多国間においてもプライバシー等の保護を志向する動きが見られる。

６．オンライン上のフェイクニュースや偽情報対策

○　EU では、フェイクニュースや偽情報対策を喫緊の課題として、プラットフォーム事業者を巻き込んで政策対応している。これは、2015 年３月に欧州委員会が、ロシアが進めていた偽情報（disinformation）のキャンペーンに対処するための行動計画を策定するため代表者を招集し、「イースト・ストラトコム・タスクフォース（the East StratCom Task Force)」を立ち上げたことが端緒となっている。

○　その後、2018 年１月、ハイレベル専門家グループを欧州委員会に設置し、検閲的な措置ではなく、利害関係者が協力することで社会としての耐性を向上させるべきとする旨の答申を提出した。

○　これを受け、同年４月、欧州委員会は政策文書（報告書）を公表し、プラットフォーム事業者、広告事業者等を含むステークホルダーが集まり、フェイクニュースや偽情報に対応するため、プラットフォーム事業者に対して行動規範（Code of Practice）の策定を求め、同年９月に行動規範が公表された。今後、欧州委員会では、当該行動規範をレビューすることとなっている。

第３章　プラットフォームサービスに係る利用者情報の適切な取扱いの確保に係る政策対応上の主要論点と基本的方向性

第１節　基本的視点（利用者情報の利活用とプライバシー保護とのバランス）

○　前章で見たとおり、電気通信分野においては、技術の進歩と市場構造の変化を背景としたプラットフォーム事業者の台頭と、プラットフォーム機能を通じた多様で利便性の高いサービスの創出が相次ぐなど、提供する事業者、提供されるサービス、提供の形態（ビジネスモデル）が劇的に変化しつつある。

○　また、新たなサービスやビジネスにおいて取得・利用される利用者情報についても質・量ともに進展・拡大が著しく、これに伴って利用者情報に対する利用者の意識にも多くの変化がみられるようになっている。

○　これらの変化を踏まえて、電気通信分野における通信の秘密を含めて利用者情報の適切な取扱いの確保に係る政策についても、必要な見直しを検討する必要がある。

○　利用者情報の適切な取扱いの確保に係る政策対応の在り方の検討に当たっては、電気通信事業法の目的に鑑み、利用者が電気通信事業者や通信ネットワークを信頼し、安心してサービスを利用できるようにすることで、オンライン上での多様なサービスやビジネス提供の拡大による電気通信の健全な発展、ひいては国民の利便の確保を図るためにはいかなる対応が適当か、という観点で検討することが適当である。

○　すなわち、利用者情報の利活用により、利用者の嗜好やニーズに沿った様々なサービスがプラットフォームを介して提供され、利用者に新たな便益をもたらす。プラットフォームサービスは、技術革新の急速な進展とともに、より一層利便性に優れ、高品質で付加価値の高いサービスの創出を促し、イノベーションに繋がる側面があり、電気通信の健全な発展と国民の利便の確保を図るための社会基盤として今後ますます重要な役割を果たしていくと考えられる。

○　一方で、履歴情報や位置情報などの利用者個人に係る様々なデータが生成・集積され、これらのデータが他のデータと結合することにより、利

用者個人の人格も表す性格を帯びてくることとなれば、利用者個人のプライバシーが把握されることへの懸念・不安がより一層拡大し、利用者が安心してサービスを利用することが難しくなるおそれがある。

○　このため、プラットフォームサービスに関する利用者情報の適切な取扱いの確保の在り方等の検討に際しては、次の３点を基本的視点として政策対応を図っていくことが適当である。

①　プラットフォームサービスは新たなサービスの創出を促し、イノベーションを促進するための社会基盤として今後更に重要な役割を果たしていくと考えられることから、利用者情報以外の情報も含めた自由なデータ流通の確保を図ることにより、プラットフォーム機能の最大化が図られること

②　一方で、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、利用者が安心してサービスを利用できるよう、利用者情報の適切な取扱いを確保すること

③　自由なビジネス環境の実現を通じたイノベーションの促進と利用者のプライバシー保護とのバランスを確保すること。

第２節　各検討項目に係る政策対応上の主要論点と基本的方向性

１．利用者情報のグローバルな流通の進展に対応するための規律の適用の在り方

（１）政策対応上の主要論点

○　第２章第２節のとおり、プラットフォーム事業者は国境を越えてグローバルにビジネスを展開するようになっており、我が国においても、こうした国外に拠点を置いてグローバルにプラットフォームサービスを提供する事業者のプレゼンスが大きくなっている。

○　我が国の電気通信分野においても、メッセージングサービスや SNS を始め電気通信事業者が提供する通信サービスと同様の、又は類似したサービスがプラットフォーム事業者によって多様なビジネスモデルにより提供されており、我が国の多くの利用者がこれらのサービスを利用している状況にある。

○　一方で昨今、国外のプラットフォーム事業者による利用者情報の大量流出事案が相次いでおり、これらの事業者による利用者情報の取扱いに対する利用者の懸念が高まっている。

○　利用者情報、特に通信の秘密に係る情報の取扱いの確保については、電気通信事業法に通信の秘密の保護規定（第４条ほか）を設けることによって、その適切な取扱いの確保を図っているところである。しかしながら、従来、電気通信設備を国外のみに設置する者であって、日本国内に拠点を置かない者に対しては、同規定による規律は及ばないものとして運用されてきたところ、上記の状況の変化に対応する観点から、国外に拠点を置き、国内に電気通信設備を有さずにサービスを提供する国外のプラットフォーム事業者に対する同規律の適用の在り方が論点として挙げられる。

（２）政策対応上の基本的方向性

○　第２章第１節において我が国憲法の特長として触れているように、通信の秘密の保護を基本的人権の一つとして表現の自由と併せて定

めていることに照らして、憲法上の通信の秘密を保護する意義が国民の表現の自由や知る権利の保障、プライバシーの保護、さらには、我が国の通信制度を保障して、国民による安心・安全かつ自由な通信の利用を確保することにある点に鑑みると、提供主体が国内か国外かを問わず国民の通信の秘密を保護することこそが上記憲法上の要請に適うものと考えられる。

○　すなわち、今日国外のプラットフォーム事業者のプレゼンスが増大し、多くの利用者がこれらの事業者が提供するプラットフォームサービスを利用している状況や国外のプラットフォーム事業者による利用者情報の大量流出事案が相次いでいる状況に鑑みると、国外のプラットフォーム事業者による利用者情報の適切な取扱いの確保がなされなければ、利用者が安心してサービスを利用することができなくなり、ひいてはプラットフォームサービスに対する利用者の信頼の確保が図られず、プラットフォームを通じた多様なサービスの普及による電気通信の健全な発展と国民の利便の確保に支障が生じ得ると考えられる。

○　したがって、我が国の利用者を対象にサービスを提供する場合には、提供主体が国内か国外かに関わらず等しく利用者情報及び通信の秘密・プライバシーの保護に係る規律を適用することにより、我が国の利用者の利用者情報の適切な取扱いが確保されるようにすることが適当である。

○　また、国内外の事業者間の公平性を確保し、イコールフッティングを図る観点からも、国内か国外かにより、利用者情報及び通信の秘密等に係る規律が等しく適用されることが適切であると考えられる。

○　具体的には、国外のプラットフォーム事業者が、我が国の利用者を対象として電気通信サービスと同様の、又は類似したサービスを提供する場合についても、電気通信事業法に定める通信の秘密の保護規定が適用されるよう、法整備を視野に入れた検討を行うとともに、併せてガイドラインの適用の在り方についても整理することが適当である。

２．電気通信サービス・機能とプラットフォームサービス・機能の連携・融

合等の進展に対応するための規律の適用の在り方

（１）政策対応上の主要論点

○　第２章第２節で見たように、今後、電気通信分野において提供される通信サービスは、デジタル化の進展と相俟って AI や IoT などの最新技術を駆使したものに変遷・進化し、ビジネスモデルも大きく変貌を遂げていくと考えられる。すなわち、電気通信サービス・機能とプラットフォームサービス・機能を一体的に提供する形態のビジネス・サービスの拡大・普及や、通信サービスの提供主体の質・量がともに変貌し、既存のスタイルに囚われない電気通信事業者の登場や電気通信事業者とプラットフォーム事業者との協業や連携・融合が進み、市場環境が一変することも想定される。

○　またこうした変化に伴い、より多様なサービスを通じてより多くの利用者情報が取得・活用されるなど、利用者情報の取扱いが質・量ともに深化・拡大することが想定される。したがって、電気通信サービス・機能とプラットフォームサービス・機能の一体化、連携・融合に伴う利用者情報の適切な取扱いの確保を図るため、現行のガイドラインの適用対象や適切な取扱いの在り方の見直しが論点として挙げられる。

○　また、ガイドラインの適用や該当条文が明確になっていないために、利用者情報のビジネス・サービスへの活用が十分に図られないケースなどもあり得ることから、法律やガイドラインの適用関係の明確化が論点として挙げられる。

○　具体的には、ウェブ上の行動履歴や位置情報について、とりわけ、スマートフォンやタブレット端末などのユーザ端末から発せられ又はユーザ端末に蓄積される端末 ID やクッキーなど端末を識別する情報等（以下「端末情報」という。）をターゲティング広告のために取得・利用する行為が通信の秘密・プライバシー保護との関係で如何に整理されるかが論点として挙げられる。

○　なお、電気通信サービス・機能とプラットフォームサービス・機能の一体化や連携・融合の進展は、通信ネットワークレイヤとプラット

フォームレイヤの両レイヤにおけるドミナント性を強めることとなり、結果として利用者に質の高いサービスの選択肢が与えられないなどの懸念が生じ得るのみならず、市場における公正競争が阻害されるなど電気通信分野の市場環境にも多大な影響が及ぶ可能性があり、これへの対応の在り方も論点となる。

（２）政策対応上の基本的方向性

○　電気通信サービス・機能とプラットフォームサービス・機能の一体化、連携・融合に伴う利用者情報の適切な取扱いの確保を図り、今後とも利用者が安心してプラットフォームサービスや電気通信サービスを利用できるようにする観点からは、こうした環境変化を踏まえたガイドラインの適用対象の見直しを進め、ガイドラインに定める規律をこれらのサービス・ビジネスに適用できるようにすることが適当である。

○　ガイドラインの適用関係等の明確化に関しては、端末情報をターゲティング広告のために取得・利用する行為について、通信の秘密に係るこれまでの整理に照らすと、現状では、主に広告事業者等がウェブ上の行動履歴を把握するために利用するサードパーティクッキー等の仕組みは電気通信事業者の取扱中に係らない行為と考えることができ、通信の秘密に含まれると整理することは適当ではない。

○　他方、第２章第１節のとおり、憲法における通信の秘密の趣旨が、ユーザによる安心で安全かつ自由な通信を保障することにあることに鑑みれば、利用者が端末情報の取扱いを適切にコントロールできることが重要と考えられる。利用者のコントロールが及ばないにも関わらず、OS 事業者、通信事業者、プラットフォーム事業者、アプリ事業者等が端末情報を取得しているとすると、プライバシー上の適切な保護を検討する余地が生じ得るところ、e プライバシー規則(案)の議論も参考にしつつ、今後具体的な規律の在り方について、引き続き検討が必要と考えられる[9]。なお、M2M（Machine-to-Machine）通信、すな

[9] 検討アジェンダ（案）の提案募集において「Web 等のターゲティング広告に係るアクセス履歴の取得に対する規制は、･･･（中略）･･･通信の端点で得られているだけの履歴を通信の秘密として拡大解釈することは避けるべき。通信の秘密侵害は直罰が科される重罪であり、単なる Web 等の履歴の取扱いにすぎないものには馴染まない。仮に辻褄合わせのために通信の秘密に係る規制を緩めた場合、厳格に捉えるべき本来の通信の秘密概念を形骸化させることになりかねない」との意見が寄せられており、こうした意

わちモノとモノとの間のデータのやりとりも今後飛躍的に増大すると想定されるが、これら M2M 通信の中には利用者のプライバシーに直接に関わらないものもあり得るところ、M2M 通信への通信の秘密に係る規律の適用の在り方についても検討することが適当である。

○　このほか、ガイドラインの適用関係等の明確化に関連して、通信の秘密の保護に関しては、電気通信事業法第４条第１項において「電気通信事業者の取扱中に係る通信は侵してはならない」旨が規定されており、また、通信の秘密に属する事項の一部についてはガイドラインに定めるとともに、解説を示すことにより明確化を図っているところであるが、より一層の明確化を図る観点から、例えば、通信の秘密に係る情報の取得・活用・外部提供が許容されるケースを法律に明記するなどすべきとの意見が聞かれる。

○　また、ガイドラインにおける通信の秘密に係る情報等の適切な取扱いに係る規定に関して、情報の種別に着目して定めるのではなく、今後は具体的な要件や態様（取得・活用・外部提供が許容されるケース）に着目した規定振りや考え方を取り入れていくことが必要になるとの意見も聞かれる。

○　さらに、通信の秘密に係る情報の活用に当たっては、従来原則として利用者の「個別具体的かつ明確な同意」の取得が求められるとの整理がなされているところ、利用者情報の取得が増えるにつれて、累次の同意が繰り返される結果、かえって利用者が十分に理解しないままに同意をしてしまう、いわゆる「同意疲れ」が課題となっていることから、同意取得の在り方についても見直しが必要との意見も聞かれる。

○　これらの課題については、いずれも利用者情報の取得・活用によるイノベーションの促進と、利用者情報の適切な取扱いを確保するための枠組みとのバランスをいかに確保するかという基本的な方向性を踏まえつつ、新たなサービス・ビジネスの創出を巡る市場動向、さらには諸外国のプライバシー保護に係る制度の動向も参考にしながら、今後引き続き検討していくことが適当である。

見にも留意することが望ましい。

○　なお、電気通信サービス・機能とプラットフォームサービス・機能の一体化や連携・融合の進展に伴うドミナント性の高まりへの対応に関しては、今後の通信ネットワークの仮想化に伴う電気通信設備（ハード）と機能（ソフト）の分離の進展も見据えつつ、従来ドミナント規制が主として対象としてきた通信ネットワークレイヤに限定することなく、レイヤを超えた支配力の行使に適切に対応できる規律の在り方について、電気通信分野の市場環境の変化に応じた適切な規律を確保する観点から、今後引き続き検討することが適当である。

３．プラットフォーム事業者による、規律に従った適切な取扱いを確保するための方策の在り方

（１）政策対応上の主要論点

○　前述１．及び２．で検討したように、プラットフォーム事業者に対して利用者情報及び通信の秘密等に係る規律を適用したとしても、当該規律に従った適切な取扱いがこれら事業者によって実際になされなければ、我が国の利用者の保護が十分に図られないこととなる。

○　国外のプラットフォーム事業者による適切な取扱いを確保するための方策としては、例えば国際的な執行協力やGDPRに見られるように域内に代理人を設置する方法などが考えられ、また、事業者による自主的な取組と合わせた共同規制的なアプローチも考えられるところ、履行を確保するためどのような方策が望ましいかが論点となる。

○　また、最近相次いだ国外のグローバルプラットフォーム事業者による利用者情報の大量流出事案においても、我が国の利用者の利用者情報の取扱いや被害状況の詳細が明らかにされないなどのケースが見受けられたところであるが、我が国の利用者が、事業者がどのように利用者情報を取り扱っているか等について的確に理解・把握して、安心してサービスを利用できるようにするため、これら事業者による利用者情報の取扱いに係る透明性をいかに確保するかについても論点となる。

○　さらに、国外のプラットフォーム事業者が提供するサービスに係る利用者情報の取扱いに関し、我が国の利用者からの問合せに応じ

る窓口が分かりづらい、日本語では対応しないなどの事例もあり、我が国の利用者が不便を強いられるのみならず、利用者情報が漏えいした場合等に適切な利用者への対応がなされず、通信の秘密やプライバシー保護の観点から看過できないケースが生じ得るおそれもあることから、こうした利用者情報の管理態勢・苦情相談態勢の在り方も論点として挙げられる。

（２）政策対応上の基本的方向性

○　国外のプラットフォーム事業者による規律に従った適切な取扱いを確保するための方策は、上記（１）において言及したEUの事例をはじめとして多様な選択肢が考えられるところ、我が国の法律の執行力の確保の在り方については、eプライバシー規則(案)の議論の動向等を踏まえて、引き続き検討していくこととするのが適当である。

○　なお、今後の検討に当たってまず留意すべきことは、個々のプラットフォームサービスによってビジネスモデルが異なり、取り扱う利用者情報も、また、利用者情報の活用の仕方もまちまちであるという点である。

○　また、各プラットフォーム事業者は、自らが提供するサービスができるだけ多くの利用者に受け入れられるよう、サービスの魅力を高めるのみならず、利用者からの信頼を得るために、自ら利用者情報の適切な取扱いを図ろうとするインセンティブが働くという面もある。

○　したがって、各プラットフォーム事業者による自主的な取組を尊重しつつ、その取組を後押しするための方策を講じるとともに、適切な取扱いの確保を担保するための法的基盤を整備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望ましく、今後その具体的な方策について検討を深めることが適当である。

○　また、国外のプラットフォーム事業者による自主的な取組として期待される具体的な事項としては、例えば、利用者情報の取扱いについて利用者が的確に把握・理解できるよう確保することが重要であるところ、利用者情報の取扱い方策の透明性の確保・向上や、我が国の利用者からの問合せに応じる窓口を始めとする苦情相談態勢につ

いても、我が国の利用者の通信の秘密及びプライバシー保護の観点から充実した対応が求められるところであり、こうした共同規制的なアプローチの具体化を検討するに当たっては、これらの自主的な取組が適切に機能するよう留意することが適当である。

４．欧米におけるプライバシー保護法制を始めとする国際的なプライバシー保護の潮流との制度的調和に係る政策対応

（１）政策対応上の主要論点

○　第２章第３節で見たように、EU では、新たなインターネットベースのサービスの進展に伴う通信分野でのプライバシー・個人情報の保護を拡充するため、通信の秘密等の適用対象を従来の通信サービス（traditional electronic communication service）に加え、ウェブメールや SNS などの OTT の通信サービス（Over-the-Top communications services）に適用を拡大する e プライバシー規則(案)の策定作業が進められ、米国においても、カリフォルニア州では CaCPA が成立し、また、包括的な連邦法を指向する動きが見られる。こうした諸外国のプライバシー保護の潮流との制度的調和の確保が論点となる。

（２）政策対応上の基本的方向性

○　諸外国においても通信の秘密を含むプライバシー保護に関する制度の見直し等が進められている中で、国際的なプライバシー保護の潮流との制度的調和を図ることなく、我が国の規律に従った取扱いを確保するための方策を推し進めれば、一国マルチ制度のような状況を招き、プラットフォーム事業者やその提供するプラットフォームサービスの利用者に混乱を来たすおそれがある。

○　したがって、これら諸外国の動向を引き続きフォローし、電気通信分野におけるプライバシー保護に係る規律についての国際的な調和（ハーモナイゼーション）を図っていくことが適当である。

また、国外のプラットフォーム事業者が我が国の利用者に対して通信サービスを提供する過程で取得した利用者情報への外国政府等からのアクセスについても、併せて論点や考え方を整理していくことが

必要と考えられる。

○　このほか、国外の事業者に対して、規律に従った適切な取扱いを確保するための方策についても、グローバルな相互運用の可能性も展望しつつ、国際的な調和（ハーモナイゼーション）を図っていくことが適当である。

第４章　トラストサービスに関する主な検討事項

第１節　トラストサービスの必要性

１．サービスに応じたIDの利用

○　プラットフォーム事業者の提供するサービスの規模が拡大する中、当該事業者の発行するIDを利用して当該事業者以外の事業者が提供するサービスにもログインすることが可能になるなど、IDを利用した様々なサービス間の連携が進展している。ただし、当該IDの発行に際して行われる本人確認のレベルは様々であり、必ずしも厳格な本人確認が行われていないものも存在している状況にある。

○　例えば、無料動画視聴サービスや写真共有サービスのように、利用にあたって必ずしも高いレベルでの厳格な本人確認を必要としないものが存在する。一方、フィンテックを活用したオンラインでクレジットカード番号などの機微な情報をやりとりする金融サービスや企業の重要情報を取り扱う電子契約のように、利用にあたって高いレベルの本人確認を必要とするオンラインサービスも存在する。

○　求められる本人確認のレベルが様々である状況を踏まえると、利用者や利用可能なサービスの多寡を基準にIDを選ぶのではなく、利用するサービスに求められる本人確認のレベルに応じたポリシーに基づいて発行されたIDを選ぶことができ、同等のポリシーに基づくID同士での連携も可能な環境を整えることが必要である。

○　これにより、多種様々なオンラインサービスについて、それらの内容・重要度に応じてID情報の信頼度をレベル分けするLoA（Level of Assurance）の考え方に基づいた利用・提供の実現が可能となる。

２．Society5.0を支えるトラストサービス

○　サイバー空間と実空間を高度に融合させたシステムより、経済発展と社会的課題の解決を両立するSociety5.0の時代が到来しつつある。Society5.0においては、実空間にあるセンサーなどから大量のデータがビックデータとしてサイバー空間に収集され、収集されたビックデータ

を人工知能（AI）により解析し、実空間に高付加価値をフィードバックすることで、生活の利便性の向上や産業の高度化を実現することが期待されている。近年のIoTの爆発的な普及等に伴い、サイバー空間と実空間の一体化が加速的に進展しており、実空間での様々な活動がサイバー空間に置き換わる中、その有効性を担保するためには、サイバー空間の安全性や信頼性の確保が重要である。

○　サイバー空間の安全性や信頼性の確保のためには、センサーを始めとする様々なモノがネットワークにつながる中、正当でないモノがネットワークにつながったり、企業のサーバやセンサー等から大量のデータが送られるようになる際、誤ったデータや改ざんされたデータが紛れ込まないようにすることが重要である。したがって、人だけでなく、組織やモノも認証するとともに、データの完全性を確保するためのトラストサービスの実現が必要である。

○　Society5.0に向けて、トラストサービスの基盤を活用することが考えられる例として、他国に先行する我が国における取組である情報銀行が挙げられる。情報銀行は、個人とのデータ活用に関する契約等に基づき、個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき、データを第三者（他の事業者）に提供する事業であり、その普及が期待されている。当該事業においては、情報銀行を利用する利用者、情報銀行、データ提供先の第三者等、多種多様な関係者によってデータが取り扱われることが想定され、情報銀行による個人に向けたサービスが適切に行われるには、各関係者の正当性の確認や、データ流通の過程において改ざん等が行われていないかを担保する完全性の確保が重要となることから、その基盤として、トラストサービスを活用することが考えられる。

第２節　欧州におけるトラストサービスの動向

○　EUは、eIDAS(electronic Identification and Authentication Services)規則を 2016 年 7 月に発効した。eIDAS 規則では、一定の要件を満たすトラストサービスの提供者を適格トラスト・プロバイダーとして規定し、EU 各国はトラストリスト(適格トラスト・プロバイダーのリスト)を公開し、維持しなければならないとされている。

○　eIDAS 規則には、具体的に、①電子署名（自然人が電磁的に記録された情報について、その自然人が作成したことを示すもの)、②タイムスタンプ（電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの)、③ウェブサイト認証（ウェブサイトが真正で正当な主体により管理されていることが保証できることを示すもの)、④e シール（文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの)、⑤e デリバリー（データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの）等の法的枠組みが規定されている。

○　他方、我が国には、eIDAS 規則に相当するトラストサービスを包括的に規定する法令が存在しない。今後、Society5.0 に向けて、国際的なデータ流通が加速することから、国際的な相互運用性の確保の観点からも、トラストリストの構築を含め、我が国としてのトラストサービスの在り方について検討が必要である。

○　なお、データを国外とやり取りする国民や企業等が、国外での訴訟等においてその真正性や完全性を主張する場合など、国民や企業等が国外での権利実現を図る基盤としても、我が国における法制度に基づくトラストサービスの構築が期待されている。

第３節　トラストサービスの在り方の検討における基本的視点

１．ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保（Identification / Authentication）

○　プラットフォーム事業者が提供する ID による認証は、必ずしも厳密な本人確認が行われていない場合があり、本人確認に限界があることから、金融サービスや企業の重要情報を取り扱う電子契約のような利用にあたって高いレベルの本人確認が求められるオンラインサービスにおいては、プラットフォーム事業者が提供する ID の活用が十分に進んでいない現状がある。

○　信頼性の高いサービスを実現するためには、人やモノの真正性を適切に確認して ID が発行される（Identification）とともに、誰からの／何からのデータであるかを確認する仕組みとして PKI（Public Key Infrastructure）等を活用した、よりハイレベルで、より厳格なオブジェクト認証（Authentication）の仕組みが必要である。

○　具体的には、Society5.0 の実現に際しては、（１）誰からのデータであるかを保証する利用者認証、（２）組織が発行したデータであることを保証する組織による認証、（３）ネットワークにつながる IoT 機器等のモノからのデータであることを保証するモノの認証の在り方についての検討が必要である。

○　こうした認証を行うことは、認証された利用者、組織やモノがどのようなデータにアクセス可能か、データへの認可（Authorization）をサービスごとに柔軟に変えることができる仕組みの実現に寄与する。

２．データの完全性の確保（Data Integrity）

○　大量のデータが流通する Society5.0 において、データの利用価値を高めるためには、Integrity（完全性）の観点も重要であり、具体的な仕組みとしてトラストサービスは有効である。

○　データの信頼性を保証するためには、データの完全性（改ざんされていないか）を確保することが必要であり、（１）データの存在証明・非改

ざん証明の仕組みや、（２）データの完全性と送受信の正当性の確認を組み合わせた仕組みについての検討が必要である。また、トラストサービスが長期的に確保できる検証サービスについての検討も必要である。

３．トラストサービスの実現にあたって配慮すべき事項

○　Society5.0 において、サイバー空間におけるサイバーセキュリティの確保は重要であり、トラストサービスの実現にあたっては、サイバーセキュリティの三要素である機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を確保することが求められるとともに、トラストサービスの実現にあたっては、技術革新のスピードに鑑み、最新の技術動向を踏まえつつも、特定の技術に依拠することなく、要件志向で検討する必要がある。

○　また、トラストサービスの実現にあたっては、技術的な堅牢さや強度だけを追求するのではなく、利用者にとって使いやすいインターフェースであることや、ID 登録の際に取得する情報について必要最小限のものに留めるなどプライバシー・バイ・デザインにも配慮が必要である。さらに、トラストサービスを提供する事業者や利用者にとって過度なコスト負担や不便を強いることが無いよう、検討することが必要である。

第４節　トラストサービスの在り方の検討事項

１．人の正当性を確認できる仕組み

（１）利用者認証

○　プラットフォーム事業者が発行する ID について、当該事業者が提供するもの以外も含めて、様々なオンラインサービスのログインに利用が拡大している。しかしながら、当該 ID の発行に際しては、必ずしも厳格な本人確認が行われていない場合もあり、より高いレベルでの本人確認が求められるサービスへの利用については限界がある。

○　例えば、近年、金融サービスにおいて、スマートフォンを用いたモバイル決済等を実現するフィンテックの活用が進展している。金融サービスでは、クレジットカード番号など機微な情報も扱うことから、なりすましを防ぐためにも、オンラインでのやりとりにおいて、高いレベルでの厳格な本人確認が求められる。このような高いレベルでの厳格な本人確認が求められる新たなサービスの創出も見据え、その基盤となる利便性と信頼性を合わせ持った利用者認証のためのトラストサービスが期待されている。

○　トラストサービスの起点として、PKI ベースの電子証明書の活用が有力な方策となり得るが、これについては、公的個人認証制度[10]において、電子署名のための電子証明書に加え、マイナポータルに接続する際の本人確認等に用いる利用者認証のための電子証明書も発行されている一方、電子署名のための電子証明書を発行する民間の認証局に係る規律（電子署名法）はあるものの、利用者認証のための電子証明書を発行する民間の認証局については規律されておらず、官民で制度上の非対称が存在している。

○　こうした状況を踏まえ、民間の認証局が発行する電子証明書を利用するサービスの具体的なニーズと、当該認証局への規律の必要性について検討する必要があると考えられる。

[10] 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律

（２）リモート署名

○　近年、クラウドの急速な普及に伴い、様々なオンラインサービスにおいて、データやアプリケーション等をクラウド上に保管し、ネットワークを通じて必要なときに必要なデータやアプリケーション等を利用することができるクラウドサービスが進展している。

○　こうした利便性が高いサービスが進展する一方、現行の電子署名法においては、電子証明書（鍵）を IC カード等に収納し、ユーザーが当該カードを用いてパソコン等から電子署名を付すことを前提としている。

○　そのため、電子署名に関しても、クラウド上に電子証明書（鍵）を保存して署名を付すリモート署名について、一定のネットワーク環境があれば、端末を選ばずに電子署名を利用できるようになり、利便性が大幅に向上する、IC カードの紛失等のリスクが無くなるといったメリットから、ニーズが見込まれている。

○　こうした状況を踏まえ、リモート署名を実現する上での技術的課題や制度的課題について検討する必要があると考えられる。

２．組織の正当性を確認できる仕組み

（１）組織による認証

○　商業登記に基づく電子認証制度[11]においては、法人の代表者に対する電子証明書が発行されている。また、企業による行政への電子申請等、代表者の委任を受けて行う行為については、社員個人に発行された電子証明書を用い、代理権等については電子委任状による確認をすることで一定の措置がなされている[12]。

○　一方、例えば、企業がソフトウェアアップデートプログラムを配布する場合やプレスリリースを行うような場合には、組織として情報やデータを発行するものであり、企業の社員の意思に基づくものではな

[11] 商業登記法
[12] 電子委任状の普及の促進に関する法律

いため、社員個人による署名はなじまず、企業名による署名により発行するニーズが存在している。

○　受信者から見ても、組織のなりすましの防止により、安心してさまざまなサービスを利用できる基盤となりうる。EU では、eIDAS 規則において、文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すものとして e シールが規定されている。

○　こうした状況を踏まえ、我が国における組織による認証のユースケースの具体化や制度的課題について検討する必要があると考えられる。

（２）ウェブサイト認証

○　利用者がウェブサイトを閲覧する際、ウェブブラウザでサーバ証明書を確認することにより、そのウェブサイトが正当な企業等により開設されたものであるかどうかを確認することができるウェブサイト認証という仕組みが利用されている。

○　ウェブサイト認証のための電子証明書を発行する認証局に求められる監査の基準については、認証局事業者とウェブブラウザベンダ等からなる団体である CA／ブラウザフォーラムが定める要件がデファクトスタンダード化されており、当該要件を満たすと認められなくなると、必ずしもセキュリティ上問題がない場合であっても、ウェブブラウザ上、安全ではないサイトと表示されるおそれがある。

○　EU では、eIDAS 規則に基づき適格な認証局を公的にリスト化しており、当該認証局については、CA／ブラウザフォーラムにおいても安全なものと認定されている。

○　こうした状況を踏まえ、現行のデファクトスタンダード化の状況における問題点を具体化した上で、認証局に係る我が国として適切な要件を設定することの必要性を検討する必要があると考えられる。

３．モノの正当性を確認できる仕組み

○　IoT 時代において、例えば、各種センサーから送信される環境情報（気温や雨量等）や生体情報（体温や心拍数等）、自動走行する車の部品から送信されるプローブ情報（走行位置や速度等）等を活用する際、モノの正当性を確認することで、データのなりすまし等を防止する仕組みが求められる。

○　また、API（Application Programming Interface）を活用したさまざまなプログラムが機械的にサーバ等と情報を送受するようになり、AI（Artificial Intelligence）の活用が進展する中、モノがサーバ認証を行うケースが増えることが見込まれる。

○　利用者認証や組織認証と同様に、モノの認証においても例えば PKI による認証の仕組みが考えられるが、センサーなどの IoT 機器に PKI の仕組みを導入することには、機能的な制約もある。

○　モノの認証においてどのような認証の在り方があるか、技術的課題や制度的課題について検討する必要があると考えられる。

４．データの存在証明・非改ざん証明の仕組み

○　電子データと時刻情報を結合することで、その時刻にそのデータが存在したこと（存在証明）と、その時点から現在に至るまでデータが変更・改ざんされていないこと（非改ざん証明）を証明することができる仕組みとして、タイムスタンプが利用されている。

○　現在は、総務省指針「タイムビジネスに係る指針」（2004 年 11 月５日）に基づき、日本データ通信協会による民間の認定スキーム（タイムビジネス信頼・安心認定制度）により、タイムスタンプ事業者がサービスを提供しており、国税関係の帳簿保存への利用をはじめ、着実に利用が拡大している。法律上の位置付けがあれば、一層の利用拡大が見込まれることが期待される。

○　今後、タイムスタンプを付した電子文書を国際的にやりとりする機会が拡大することが見込まれている。EU においては、eIDAS 規則に基

づき一定の基準を満たすタイムスタンプ事業者が適格なサービス提供者として認められているところ、今後、我が国の事業者が発行するタイムスタンプが EU において有効とみなされない事態や、我が国のタイムスタンプビジネスが EU の事業者に席巻されるような事態を招くおそれがある。

○ EU との政策対話において、タイムスタンプを含むトラストサービスに関して、具体的なユースケースに基づいて相互の制度を比較するマッピングを進めることを合意している。その交渉状況を踏まえ、国際的な相互運用性の確保等の観点から、タイムスタンプの制度的手当ての必要性について検討する必要があると考えられる。また、トラストサービスが長期的に確保できる検証サービスについても検討する必要があると考えられる。

５．データの完全性と送受信の正当性の確認を組み合わせた仕組み

○ 送信・受信の正当性や送受信されるデータの完全性の確保を実現するサービスとして、eIDAS 規則においては e デリバリーが規定されている。

○ 例えば、ドイツでは、暗号化されたメッセージの送受信の証拠を保証する「De-Mail」サービスが提供されている。送受信されるデータは、end to end 間での暗号化がされているとともに、郵便における書留のように、データの送達確認等ができるものである。

○ こうした状況を踏まえ、送信・受信の正当性を確認するとともに送受されるデータの完全性の確保を実現するサービスに対するニーズの具体化について検討する必要があると考えられる。

第５章　オンライン上のフェイクニュースや偽情報への対応

（１）政策対応上の主要論点

○　フェイクニュースや偽情報の問題は、特に欧米諸国等において、プラットフォーム事業者が、利用者情報を分析して閲覧者の嗜好に働きかけるコンテンツ表示技術を通じて拡散することにより年々深刻化しており、今後、我が国においても同様な事象が社会問題となる可能性があるため、これらフェイクニュース等への対応が論点として挙げられる。

○　第２章第３節で見たように、フェイクニュースや偽情報の対応に関し、EU では、2018 年４月に欧州委員会が公表した政策文書の中で、今後の活動計画として、プラットフォーム事業者などが参照できる行動規範（Code of Practice）の策定を求め、その後、行動規範の効果測定（レビュー）などの検証を行い、その検証結果が不十分な場合には規制の導入を含む更なる行動を採ることとしている。

○　同時に、EU では、オンライン上のスポンサー付コンテンツが容易に識別できる仕組みづくりを検討するとしているほか、AI やブロックチェーン等を活用したフェイクニュースや偽情報対策のための研究開発の支援、ファクトチェックを行う組織を支援するためのデータやツールを提供するための公的プラットフォームの構築、メディアリテラシー教育の充実等に取り組むとしている。

○　なお、我が国の放送分野については、放送法において、放送番組編集の自由の保障の下（第３条）、「報道は事実をまげないですること」といった番組準則（第４条）が定められており、放送事業者は、自ら番組基準を定め、これに従って放送番組を編集し（第５条）、放送番組の適正を図るために放送番組審議機関を設置することとされている（第６条）。また、放送の質の向上等を図るため、放送事業者による自主的な運営組織である放送倫理・番組向上機構（BPO）が設置されている。

（２）政策対応上の基本的方向性

○　正しい情報を伝え、適切かつ信頼し得るインターネット利用環境となるよう、ユーザリテラシー向上及びその支援方策、また、ファクトチェックを行う機関の役割やプラットフォーム事業者との連携などの自浄メカニズム等について検討を深めることが適当である。なお、その際、表現の自由に配慮し、EU における対策を始めとする諸外国の動きを念頭に置くとともに、今後とも通信と放送の融合・連携の更なる進展が予想されるところ、上記の放送分野における取組みも参考にしつつ、プラットフォームサービスを通じて流布されるフェイクニュース等に対して求められるプラットフォーム事業者の役割の在り方に留意して検討することが適当である。