プラットフォームサービスに関する研究会（第３回）

１　日時　平成30年12月21日（金）13:00～15:00

２　場所　総務省講堂（地下２階）

３　出席者

（１）構成員

宍戸座長、新保座長代理、生貝構成員、大谷構成員、木村構成員、崎村構成員、手塚構成員、寺田構成員、松村構成員、宮内構成員、森構成員

（２）ゲストスピーカー

筑波大学大学院図書館メディア研究科　石井准教授

（３）総務省

谷脇総合通信基盤局長、竹内サイバーセキュリティ統括官、秋本電気通信事業部長、泉国際戦略審議官、竹村総合通信基盤局総務課長、山碕事業政策課長、中溝消費者行政第二課長、赤阪サイバーセキュリティ統括官室参事官、山路データ通信課長、大内事業政策課調査官、岡本消費者行政第二課企画官

（４）事務局

三菱総合研究所　西角主席研究員、安江チーフコンサルタント

（５）オブザーバー

三原個人情報保護委員会参事官

４　議事

（１）諸外国の状況等

（２）意見交換

（３）その他

【宍戸座長】　本日は、皆様、年末のお忙しいところ、お集まりいただきまして誠にありがとうございます。定刻となりましたので、「プラットフォームサービスに関する研究会」第３回会合を開始させていただきます。

冒頭、カメラ撮りがあると伺っておりますが、この関係で少々お待ちいただければと思います。

カメラ撮りのほうはよろしいですか。

（マスコミ退室）

【宍戸座長】　それでは、早速議事に入りたいと存じます。

本日は、まず事務局から、電気通信分野における競争ルール等の包括検証に関する特別委員会主査ヒアリングにおける主な意見、及び諸外国の状況等としてePrivacy規則（案）をめぐる議論の状況等についてご説明をいただきます。

次に、筑波大学大学院図書館メディア研究科石井准教授から、米国におけるプライバシー保護法制等の動向についてご発表いただきます。この時点で意見交換を行わせていただいた上で、その後、森構成員から、検討アジェンダ（案）に対する意見についてご発表いただきます。

なお、本研究会の検討アジェンダにつきましては、構成員の皆様からのご意見等を踏まえ、参考資料１とさせていただいております。ご確認をいただければと思います。

それでは、まず事務局から、電気通信分野における競争ルール等の包括検証に関する特別委員会主査ヒアリングにおける主な意見及びePrivacy規則（案）とパーソナルデータの提供に関する消費者の意識について、それぞれご説明をお願いいたします。

【岡本消費者行政第二課企画官】　主査ヒアリングにおける主な意見について、資料１に基づきご説明申し上げます。

本主査ヒアリングは、特別委員会、親会におきまして、関係事業者等からヒアリングを行ってきたもので、プラットフォームサービスに関する研究会の構成員の皆様にもご参画をお願いしてきたものでございますが、この主査ヒアリングは一通り終了しておりますので、本研究会に係るヒアリングの結果についておさらいをさせていただくものでございます。

１ページ目をご覧ください。本研究会の検討アジェンダの柱の１つとなっております利用者情報の取扱いについてでございます。

上段部の左上の曽我部教授からのものでございますが、１ポツ目で、プライバシーの問

題とプロファイリングの問題の結合等を課題として挙げていただいた上で、２ポツ目で、プロファイリングの進展は自律能力の展開の阻害や民主政の前提となる公論の場が脆弱となるおそれがあることから、３ポツ目で、適切な規律が求められるとのご意見でございます。

また、右上の１ポツ目で、ＳＮＳは多くの人々にとって表現活動の重要な場となっておりますことから、２ポツ目で、ユーザーの表現の自由の観点からは、民間事業者による管理権限は制限され得るのではないか、３ポツ目で、国家がプラットフォームを規制することも一般論としては否定されないとのご意見をいただいております。

次に、下段部をご覧ください。日本マイクロソフト社からのものでございますが、事業者のフリーハンドによる民営化されたコントロールとの概念で捉えた上で、有害コンテンツからの利用者の保護といったコンテンツ管理やセキュリティー上の脅威への対処に当たっての利用者情報の利用について、どのように適正化、透明化を図るかは事業者にとっても課題とのご意見でございました。

２ページへお進みください。上段部でＬＩＮＥ社からでございます。２ポツ目で、社として通信の秘密を遵守し、ユーザー間のトーク内容の閲覧は行っていないとした上で、４ポツ目でございますが、仮に事業者間でユーザーデータの取扱いに関し、法令適用に差異があるのであれば、公正競争の観点から是正すべきとのご意見でございました。

同様に、下段部でヤフー社からでございますが、２ポツ目で、さまざまなデータの利活用を進めているが、その際には利用目的等を平易明確にして利用者から同意を取得しているとした上で、３ポツ目で、データ利活用のルールにおいて海外事業者との間で差が生じ、国内事業者に不利益な競争環境が生じているおそれがあり、通信の秘密に関する規律についてイコールフッティングを図るべきとのご意見でございました。

３ページへお進みください。海外事業者の１つであります米国アップル社からのご意見でございます。１ポツ目で、顧客のプライバシー保護はかつてないほど重要となっているとし、２ポツ目及び３ポツ目で、さまざまなプライバシー保護に向けた取り組みが紹介され、４ポツ目で、デバイスの製品設計の初期段階で対策を組み込み、プライバシーへの影響を最小化することが重要とのご意見でございました。

４ページへお進みください。引き続き検討アジェンダにおける利用者情報の取扱いの一環でございますけれども、法のイコールフッティングについてでございます。曽我部教授からでございますが、１ポツ目で、グローバルなプラットフォームは個人を把握する巨大

な中間団体となりつつあり、プラットフォームがより全人格的に個人を把握する可能性があるとした上で、３ポツ目で、イコールフッティングの問題は、公正競争のみならず、個人の権利、自由の保障の観点からも重要とのご意見でございます。

右側につきましては、１ポツ目で、プラットフォームの濫用的振る舞いは競争環境下では抑制される可能性があり、それが奏功しない場合に、直接規制や直接規制及び間接規制の組合せなど、規制の在り方についてさまざまな手法が考えられるとした上で、最後のポツでございますが、共同規制の在り方を探るなど、行政の在り方もよりそれに適したものに転換を図る必要があるのではないかとのご意見でございました。

それ以下は、先ほどご紹介いたしましたとおり、事業者から、公正競争の観点からイコールフッティングの必要性についてのご意見を寄せられておりますので、再掲しているところでございます。

資料１については以上でございます。

【三菱総合研究所】　では、続きまして、資料２をご説明させていただきます。発表は三菱総研、西角が担当いたします。よろしくお願いいたします。

目次をご覧いただきますと、本日お題は３つございまして、初めの１５分ほどは欧州のePrivacy規則（案）について、最新の検討状況についてご説明をさせていただきます。その後、パーソナルデータの提供に関する国内の消費者の意識について簡単にご紹介し、最後、資料は構成員限りとさせていただいておりますけれども、主要なプラットフォーム事業者におけるデータの利活用状況につきまして簡単にご紹介したいと思っております。

では、３ページ目をご覧ください。ePrivacy規則の概要につきましては、第１回の会合でも生貝先生からご説明いただいたところでございますが、今回はその後の検討状況ということでご説明をしたいと考えております。

本規則につきましては、昨年１月に欧州委員会が当初の案を発表いたしまして、その後２年ぐらいたちますけれども、現在でも議論が行われているという状況でございます。その間、ステークホルダーであるところのＥＵの関係機関、業界団体等の意見提出がございまして、また昨年１０月には欧州議会で修正採択というものが行われました。この１年は、閣僚理事会において新たな規則案の検討が行われておりまして、最新の案が１０月に出ているというのが状況でございます。

欧州の立法プロセスについて、ちょっと複雑でございますので、４ページ目に簡単にご紹介しておりますけれども、本規則につきましては、通常の立法手続にのっとって進めら

れているところでございますけれども、下の図の中央左側、欧州委員会、こちらが法案を出しまして、右に書いてございます欧州議会、ＥＵ理事会、閣僚理事会、こちらが共同で採択をするという仕組みになってございます。

現状、本件につきましては、議会でこの法案に修正が必要であるという議決を行いまして、それを受けまして、右下にある閣僚理事会で修正案を検討しているという状況でございます。ですので、最終の修正案を議会が承認すれば、晴れて規則が成立するといった形になるわけでございます。

次に、５ページ目、現在、最新の案において規則の構成がどうなっているかというところを当初案との比較ということで一覧にしてございます。

当初案との比較で申しますと、第９条、１０条、１７条が削除されているというところと、４ａ条というものが追加されている。こういった変更がございますのと、それぞれの条文の中では個々で修正が加えられておりまして、こちらは後ほどまたご紹介をいたします。

６ページと７ページ目、先ほど申しましたとおり、ステークホルダーがさまざまな意見を提出しているということで、議論の過程で出てきた意見、概要をこちらでまとめてございます。詳細につきましては、各団体の意見、巻末の参考資料にまとめてございますので、ご関心ありましたらご覧いただければと思います。

まず、ＥＵ関係機関の意見の要点ということでございますけれども、基本的なスタンスとして、社会における通信の秘密の重要性というものが近年ますます増大しているということを指摘しておりまして、それを踏まえて、規則の内容につきましては、まず総論として、ＧＤＰＲで規定されているデータの保護レベル、これを下回らないようにという大原則。それから、現行のePrivacy指令、この指令の保護レベルについても守るべきだといったことを言っております。

それを踏まえた上で、具体の意見としては、例えば規制対象について、電気通信事業者だけではなくＯＴＴも含めて、あらゆる形式の電子通信について技術中立的に規制対象とするといった話、また、コンテンツとメタデータについて同等の保護を与えるべきである、あるいはトラッキング・ウォールと呼ばれるものについて明確に禁止をすべきであるといった意見が出ております。

このトラッキング・ウォールと申しますのは、クッキーウォールといった言い方もありますけれども、例えばウェブサイトを見るときに、広告目的でクッキーを使うことについ

てユーザーが同意をしない限り、そのサイトの中身が見られない、そういった機能を指しております。こちらについては、また後ほど論点としてご説明いたします。

次に、対抗する立場でございます業界団体等の意見ということで７ページ目にご紹介しておりますけれども、基本的には規則が厳しくなることによって、欧州全体のデジタル・トランスフォーメーションあるいはイノベーション、こういったものに対して悪影響が出るということで慎重な議論を求める意見が出ております。

中でも、インターネット広告業界の団体からは、現在普及しているデータを活用した広告のモデルというものがユーザーの利便性にも非常に貢献しているということで、これに仮に過剰な規制をかけてしまうと、例えばグローバルなプラットフォーマーがＥＵのマーケットから出て行ってしまう、あるいは機能の制限をするといったことでユーザーの利便性が損なわれるのではないかという問題提起をしております。

また、その他、製造業、金融業、モビリティ産業等々、各産業からは、やはり通信の秘密を保護するという目的に照らしたときに、今回のルールが過剰規制になっているのではないか、それによってデータ利活用による製品、サービスのイノベーションといったものが損なわれるのではないかといった懸念が提起されているという状況でございます。

こういったそれぞれの意見をePrivacy規則の条文に則して整理したのが８ページ目でございまして、下の表に４つの論点ということで整理をしてございます。

１つ目、①と書いてあるところ、１０条関係でございますが、プライバシーの設定方法をどうするのかという議論でございます。ＥＵの関係機関では、オンラインサービスのプライバシー設定について、ブラウザ、ウェブブラウザが典型ですけれども、こういったソフトウェアで行って、なおかつデフォルト設定で追跡を拒否するという最も厳しい設定にすべきであるという主張を行っております。

これに対して業界団体等では、一々ユーザーの同意を求めるということでユーザー負担が非常に大きくなる、利便性が下がるということで、こういった条項については削除してほしいという要請をしているということでございます。

最新の閣僚理事会の案では、この第１０条というものが削除されておりますので、業界団体の意見が通っているという形になっております。

それから、２つ目の論点として、エンドユーザーの端末あるいは端末のソフトウェア、こちらの持っている情報のデータ処理をどうするか。例えばＭＡＣアドレスとかクッキーとかいったものが含まれますが、このデータ処理についての論点でございます。現状、第

８条というところでどういう規定になっているかというと、基本的にはエンドユーザーの同意を取得してくださいということですが、それ以外に同意を取得しなくても許される場合というものが例外条件という形で一つ一つ列挙されるということになっております。

これに対して業界団体の主張としては、一つ一つ列挙するという形ではなくて、正当な利益に基づくデータ処理であれば、一定の範囲内で認められるという包括的な規定にしてほしいということを言っています。これはＧＤＰＲにも類似の規定がございますので、それを参照する形でそういった主張をしているということでございます。

一方、ＥＵの関係機関では、そういった正当な利益といった形での包括的な例外規定は認めるべきではないという主張をしておりまして、現在、最新の規則案では、正当な利益に基づくという包括の規定というのは反映されていないという形になっております。

３点目に第５条の関係ですが、Ｍ２Ｍを含むかどうかという論点がございます。これについては、現行のePrivacy指令ではＭ２Ｍも含まれておるということもあり、ＥＵの関係機関としては、Ｍ２M通信のデータについても同じく規制対象にすべきだという立場でございます。

一方で、業界団体、産業界では、こちらは当然、例えば医療だとか自動運転だとかいったものにも含まれてまいりますので、デジタル経済全般に対して非常に大きな悪影響が出るということで、Ｍ２M全体を対象外にすべきだという議論をしております。

現状の案では、最終的には規制対象外、Ｍ２Ｍを含むという案が削除されているというのが現状でございます。

最後４つ目ですけれども、先ほどもご紹介したトラッキング・ウォールに関する論点でございます。こちらについてＥＵの関係機関では、ターゲティング広告を行うためのデータ処理というのは、本来のサービスのための必須要件ではないということで、これは認められないという意見でございます。

一方で広告業界としては、ターゲティング広告というものは、確かにサービスそのものに必須ではないけれども、もう少し視野を広げてビジネスモデルと考えたときには、広告というものがないとそもそもビジネスとして成立しないのではないかということで、これを認めてほしいという主張をしております。

現状は、トラッキング・ウォールを禁止する規定については、最新案では無くなっているという形になっているところでございます。

以上、主要な４論点について状況をご説明しました。詳細、９ページ目から１２ページ

目までは、今の４つの論点について条文等も記載しながら解説しておりますが、こちらは、今回は時間の関係もありますので割愛させていただきます。

１３ページ目まで飛んでいただいて、今の４論点以外にその他論点ということで２点ほどご紹介させていただこうと思います。

まず、１３ページ目、こちらは先ほどの第８条の論点に関連して、エンドユーザーの端末の情報をユーザーの同意なしにデータ処理を行うことが認められるのはどういう場合かという例外規定の中身についての修正の状況でございます。

欧州委員会の当初案では、ユーザー同意以外で、そちらの囲みの上に書いてございますａ、ｂという２つの条件です。接続の確立に必要な場合、取得方法・目的・責任者、エンドユーザーが収集を停止・最小化するために必要な方法等の情報が明確かつ目立つ形で通知される、こういった場合には端末情報の収集をして構わないとしておりました。しかし、現在公開されている最新の閣僚理事会の案では、これがまた変更されまして、エンドユーザーの明示的な同意以外では統計目的でのみ利用が可能であるということで、厳しい規制になっているというのが現状でございます。

それから次、１４ページと１５ページのところで、通信データの分類の規定についてご説明したいのですが、そもそもePrivacy規則というものは、電気通信データの提供利用に係る通信の秘密の保護ということが目的でございますが、この電子通信データの中には、１４ページの下の図にございますとおり、メタデータとコンテンツという２つの種類があるということでございます。

コンテンツは通信の中身そのものですが、メタデータというのは、コンテンツを送信等するために付随して処理されるデータということで、例えば通信元、通信先を表す電話番号とかアドレス、あるいは基地局の情報とかいったデバイスの位置情報だとか、通信の日付とか期間、こういったものがメタデータと定義されているわけでございます。これらについては、基本的には通信の秘密の保護対象になり、すなわちデータの処理については原則禁止ということでございますが、例外規定があって、こういう場合にはデータ処理を行って構わないということが記載されております。

この例外規定につきましてどういうふうに規定するかということが１５ページになりますけれども、議論されておりまして、作業部会で出ている意見として、ＡＩだとかＩｏＴといったデジタル化の進展を踏まえると、例外規定についてもある程度将来の発展を見越した形で少し解釈の余地を残すものにするべきだろうという議論がございました。

これを受けまして、最新の規則案においては、６条において２ａと２ａａという条項が追加されております。こちらは何を変更しているかというと、例えば取得したデータをディープラーニングにおけるデータとして利用したいといった場合、つまり、ユーザーが同意した取得時の目的と異なる目的で利用する場合にも、一定の条件を満たせば改めて再同意をしなくても利用できるということに道を開く規定が、ここで２ａということで追加されたという変更が加えられているということでございます。

ePrivacy規則につきましては以上でございます。

次に２点目でございます。パーソナルデータの提供に関する消費者の意識ということで、１７ページでございますけれども、消費者アンケートの結果に基づきまして簡単にご紹介をしたいと思っております。この元データにつきましては、総務省様で２０１７年に実施された国際アンケートに基づいているものでございます。

１８ページ目、こちらは、パーソナルデータの提供に関するユーザーの不安、こちらの国際比較になっております。上の図をご覧いただきますと、基本的に不安を感じるかどうかという質問については、日中韓、アジア諸国では８割程度と比較的不安を感じる人が多いという形になっておりまして、特に一番左、日本をご覧いただきますと、一番下の項目、「とても不安を感じる」という割合が２割超ということで非常に高くなっているのが特徴でございます。

それから、下の図、グラフが読みづらくて恐縮でございますけれども、比較的、日中韓では氏名とか住所といった基本情報の提供に対して警戒が強いということと、また日本については、ウェブサイトのアクセス履歴についても不安感が６カ国中で一番強いといった結果になってございます。

次、１９ページ、パーソナルデータの提供に関するユーザーの理解、確認の状況がどうなっているかということを問うたものでございます。上の図、日本における理解度につきましては、利用目的をちゃんと理解しているかということにつきましては８割程度の理解度ということで、これは国際的に大きな差はございません。

上の図と下の図を比較していただきますと、国別に見たときに、利用目的を確認しているかどうかということと目的をきちんと理解しているかどうか、こちらの２つの項目において一定の相関が見られる形になっているということでございました。

次、２０ページ目は、国内に限ってですが、属性別の分析というのも少ししております。性・年代別に見ますと、左の図にございますとおり、総じて男性よりも女性がパーソナル

データ提供に関する不安が高いといった傾向が出ております。また右の図では、特定のアプリケーション、例えばウェブメールとかゲームあるいは動画配信、こういったものを使う場合に、比較的不安を感じる人が多い、そういった結果が出ているということでございます。

最後、２１ページ目でございますけれども、パーソナルデータの提供について不安を感じないという人も一定数いるわけでございますけれども、この「不安を感じない」と答えている人が、では果たしてほんとうに利用の目的とか理解、確認を行っているのかということを分析したものでございますが、ご覧いただいたとおり、左の図では、「不安を感じない」という人でもかなりの割合が利用目的を理解していない、あるいは右の図では確認をしていないということになっているということでございます。

ですので、不安を感じないと言っている人の中にも、ちゃんと確認して理解したから不安を感じないという人もいますが、一方で、全く無関心であるがゆえに不安がないという層もいるということには留意する必要があるという結果になってございます。

アンケートにつきましては以上でございまして、最後、資料は構成員限りとさせていただいているんですけれども、こちらでオンラインプラットフォーム事業者のデータ収集と利活用の状況について調査を行っておりまして、そのざっくりとした経過のご紹介ということで出しております。

資料としては２３ページ目でございます。こちらの一覧にあります８社につきまして整理を行っております。

２４ページ目と２５ページ目、こちらに８社、２４ページ目が海外事業者、ＧＡＦＡについて。それから、２５ページ目で国内事業者について、レイヤごとの提供サービスの一覧ということで整理をしているところでございます。

こちら、それぞれのページの半分から下、下半分に注目していただきたいんですけれども、下半分を見ていただきますと、ＧＡＦＡ、海外勢のほうがプラットフォームレイヤの一番下にある汎用プラットフォームと呼ばれる部分、ここがブラウザとかＯＳとかいったものなんですけれども、この部分について非常に多くサービス、製品を有していて、それを踏まえ、さらに下のレイヤであるネットワークレイヤ、端末レイヤというところに進出しているという状況が見てとれるかと思います。国内事業者のほうは、どちらかというと、そこが若干脆弱であって、上位レイヤのサービスのほうが中心である、こういった傾向の違いがあるということでございます。

それから、２６ページ目以降は、今回ケーススタディーをした各社につきまして、プライバシーポリシーとかサービスのホームページ上の情報をもとに、どのようにデータを収集しているのか、またどんなデータを集めてどんな目的でそれを使っているのかということを整理したものでございます。

各社ごとのご紹介はいたしませんが、全体に共通する特徴について申しますと、データの収集方法につきましては、これはレイヤとかサービスによらず横断的に記載されているという形になっておりますが、一方で、実際に収集するデータ項目、収集したデータを何に使うか、これにつきましては、サービスごとに細分化された形で説明がされているとなっております。ですので、１つのサービス、あるサービスで収集したデータを別のサービスで横断的に使い回すとかいった形の説明にはなっていないというのが全体の傾向であるということでございます。

個別の会社につきましての説明は割愛いたしますので、構成員の皆様、資料がございますので、ご覧いただければと思います。

以降のページは参考資料となってございますので、ご説明としては以上でございまして、振り返りますと、本日、欧州のePrivacy規則について最新の動向ということと、それと関連して国内における消費者の意識、それからフラットフォーマにおけるデータ収集利活用実態、この３点についてご紹介いたしました。

駆け足でございましたが、以上でございます。

【宍戸座長】　ありがとうございました。

それでは、引き続きまして、資料３「米国におけるプライバシー保護法制等の動向：カリフォルニア州法を中心に」、こちらにつきまして、石井先生からのご発表をいただきたいと思います。どうぞよろしくお願いいたします。

【石井准教授】　筑波大学図書館情報メディア系の石井と申します。どうぞよろしくお願いいたします。

「米国におけるプライバシー保護法制等の動向：カリフォルニア州法を中心に」というタイトルでご報告させていただきます。

本日の内容は、主にカリフォルニア州のプライバシー保護法の内容をご紹介させていただくということでありますけれども、まずはアメリカ全体におけるプライバシー保護法制の動きを簡単に取り上げたいと考えております。

プライバシー保護に関係する連邦法としましては、公的部門においては１９７４年のプ

ライバシー法がありまして、民間部門はセクトラル方式の法令が制定されてきました。カテゴリーに分けますと、金融分野、通信分野、児童の保護、医療分野などがあります。また、幾つかの法律についてＦＴＣ、連邦取引委員会が規則を制定する権限、執行権限を持っていたりします。

連邦レベルで消費者プライバシーを保護するための一般的な法律をつくろうという動きもありました。具体的には２０１２年２月２３日に消費者データプライバシーに関する政策文書が公表されまして、２０１５年２月２７日には、消費者プライバシー権利章典法案と言われる討議文書が公表されました。だ、連邦議会でも消費者プライバシー権利法に関する法案が複数提出されましたが、現在に至るも制定には至っておりません。

一般法の内容としましては、諸原則を定めてＦＴＣが執行をかけるという内容になっております。

諸原則については、スライドには書いておりませんが、個人がコントロール権を有するということ、透明性を重視するということ、個人データを収集、利用、開示するときの状況に適した方法で取り扱うということ、データの安全性、個人の自分のデータへのアクセス権、訂正権、個人データの収集、保有についての適切な制限を課すということ、企業が個人データの取扱いについて、消費者プライバシー保護を守っているということを証明する責任を負わせる、すなわち、遵守する責任は事業者側に負わせるといったことが書いてありまして、そうした諸原則を守らせることが一般法としての提案内容です。

ＦＴＣの年次報告書に基づきまして、プライバシー絡みの問題事例を幾つかご紹介させていただいております。例えば、少し古い事案ですが、一番下のjerk.comというのはわりと有名な事案です。フェイスブックからユーザーのプロフィールをつくり、利用者にjerkな人間かそうでないかという格付けをさせるようなサービスでした。その内容に不満がある、自分の評価に不満がある人については、修正してほしければ３０ドル払えという詐欺的な実務を行っていたサービスがありしました。

次に、借り入れ情報、これはpayday loanという給料を担保とした小口の借り入れについての事案もありました。借り入れ情報についてはうその情報である一方で、本人を識別する情報は本物の情報でした。そうした情報を購入し、個人に対して、あなた、借り入れあるでしょうということで督促をかけたりしたという、詐欺的な実務についての執行事案が紹介されていたりします。

スライドの下から説明しているような形になってしまっていますけれども、Upromiseと

いう事案もありました。上から４つ目ぐらいですか、ポイント還元アプリの説明不足の事案について、ＦＴＣが執行をかけたという事案も紹介されていたりしました。

プライバシーに関わる詐欺的な実務についてＦＴＣが執行をかけるというスタイルがＦＴＣ法５条を根拠に行われてきたというのがアメリカの実務になっております。

ＦＴＣ法５条という法律は、消費者プライバシー保護の場面でＦＴＣが執行を行うときの根拠規定となっております。アメリカには包括的なプライバシー保護法はありませんけれども、ＦＴＣ法５条がかなりさまざまな場面で活躍してきたというのがアメリカの状況だと言えます。

６ページの２点目、FTC5条は、「商取引における又は商取引に影響を及ぼす不公正若しくは欺瞞的な行為又は慣行」を違法と宣言すると定められています。

違反行為に関しては、排除措置命令、民事罰、これは刑事罰以外の制裁金、提訴の対象となるということになりまして、消費者をだます実務は先ほどの文言の中の欺瞞的、情報の大量漏洩の場合は不公正の文言を使って、それに関連付けて執行をかけるというスタイルになります。

ただ、実際は同意命令という一種の和解手続によって審判手続を行わずに解決することが多いと言われています。

民事罰の最高額は、インフレ調整によって、現在の時点で違反ごとに４万１，４８４ドルになっています。

こちらはプライバシーシールドについてです。ＥＵからの越境データ移転について、ＥＵとアメリカの間では、2016年7月12日、プライバシーシールドに関する十分性決定が下されています。。これはセーフハーバーが無効になったことで改めて協議をして取りまとめられたというものになっています。

また、２０１７年１月１２日には、スイスとアメリカの間でプライバシーシールドの協定が結ばれています。

プライバシーシールドは、アメリカの中では商務省国際防衛局というところが運営しています。

諸原則を遵守することについて、商務省に対して守っていますということを自分で宣言し、プライバシーポリシーを公表する、その宣言に対してＦＴＣが執行をかける、その３つの要素で動いているのがプライバシーシールドになります。

諸原則は、通知、選択、第三者への移転、安全性、データの完全性、目的による制限、

アクセス、救済・執行及び責任です。個人情報保護の世界でわりとおなじみのルールが定められています。

９ページをご覧いただけますでしょうか。プライバシーシールドリストを見てみますと、昨日の時点で４，２４１事業者が有効な事業者、３０１事業者は期限切れか手続が済んでいないか、あるいは無効の事業者になっております。ここでグーグルと検索をかけると、グーグルも出てきます。、４，２４１件をお示しすることができませんので、１つの例として挙げております。

１０ページをお願いいたします。ＦＴＣはプライバシーシールドに基づく法執行権限を持っています。つまり、FTCはＦＴＣ法５条に基づいて執行をかけるという実務を行っておりまして、２０１８年１１月１９日時点で誤認表示、誤解を与える表示行為について４社との間で同意命令が最終的に承認されているという状況です。

IDmission、これはプライバシーシールドの手続完了前にプライバシーポリシーを先んじて表示してしまっていた。ここに誤解を与える表示があった事案です。

SmartStart、VenPath、あともう１個、これは期限が切れた後にもプライバシーシールドの参加をポリシーの中で表示し続けたという事案です。

セーフハーバーのときも同じですが、プライバシーシールドを実際には有効な形で持っていないにもかかわらず、それを表示するというところに欺瞞的な実務があるとみなされるという理屈になります。

１１ページをお願いします。プラットフォーム事業者への共同規制的アプローチがあり得るのかどうかということを考えてみると、まず、諸原則を定めます、それを守りますと宣言します。宣言すると、宣言に拘束されますというのが執行をかける根拠となります。その場合、仕組みを動かしていく上で重要な点としては、違反への執行をきちんと実効的な形にすることに加えて、苦情救済、苦情があったときにそれを救済していく道筋をできるだけ幅広く用意してあげること、さらには、消費者に対する説明をきちんと行うことに加えて、情報が欺瞞的にならないようにアップデートしていくというあたりがポイントになってこようかと思います。

２点目に、プライバシーシールド的アプローチをとるのであれば、執行、救済、透明性の３点が重要になってくると考えられます。

１２ページをお願いします。同意判決と同意命令、間違えやすいので、内閣府の資料などをお借りしながらご用意してみました。

同意判決は民事訴訟手続の中で和解を行うというもので、同意命令は、ＦＴＣが事件処理を行うプロセスの中で事業者との間で合意をして、命令を発出して事件を集結させるというものです。上は裁判所の関与がありますが、下は裁判所の関与がないという手続になります。

１３ページをお願いします。プライバシーシールド・アップデートという、欧州議会の調査サービスが出している、シンクタンクが出しているレポートがあります。このレポートによりますと、ケンブリッジ・アナリティカ事件が起きまして、十分な保護レベルを保障しているかどうかについての懸念がありますという点に触れられています

オンブズパーソン、これはプライバシーシールドの十分性決定の文書の中で、政府機関による、諜報機関による情報の収集への懸念が示されていまして、その対応策１つとして、オンブズパーソンを作り、監視の仕組みを入れますということがうたわれています。しかし、正規のオンブズパーソンの指名が遅れているというところが問題点として指摘されています。

CLOUD Actに関しましては、アメリカ国内所在のプロバイダに対して、アメリカ国外にあるデータ提出等を求めるということ、それから、アメリカ国外に所在するプロバイダに対して、アメリカ国外のデータの提出を求めるということ、両方できるようになっています。

ただ、行政協定を締結した国の国内にあるデータについては、プロバイダが出しなさいと言われたときに異議申立てを行うことができるという仕組みもあります。

Schrems事件は、セーフハーバーを無効にした人物が、別途訴えを起こしている事案があります。ここでは、主に標準契約条項の有効性が争われています。アイルランドの裁判所から欧州司法裁判所に対して事案を付託することについてフェイスブックが不服を申し立ててしていまして、１２月１９日に付託するかどうかの審問が行われたようです。

長くなっていますけれども、カリフォルニア州のプライバシー保護への取り組みについてご紹介させていただきたいと思います。

カリフォルニア州というのは、憲法の明文でプライバシー保護をうたっている州です。カリフォルニア州は、これまでにもプライバシー保護に関する幾つかの法律を制定してきていまして、アメリカの中ではプライバシー保護に積極的に取り組む州だということで知られています。

例えばセキュリティー侵害通知法、これはコンピュータデータへの不正アクセスがあったときに、本人に対してシステムのセキュリティー侵害がありましたということを通知す

る義務を課すという法律です。

シャイン・ザ・ライト法というのは、マーケティング目的で企業がどのように情報を共有しているかということを消費者が把握しまして、オプトアウトできるようにするという法律です。

追跡防止法、これはカリフォルニア州の住民の個人情報を収集するウェブサイトやオンライン事業者に対して、プライバシーポリシーの中にDo Not Trackを定めるべきといったことを規定しています。

生徒のプライバシー保護法。これはインターネットウェブサイトやオンラインサービスなどの事業者に対して、幼稚園の年長から高等学校を卒業するまでの１３年間の情報を使ってターゲティング広告に使ってはならないことなどを定めている法律です。

１５ページをお願いします。カリフォルニア州プライバシー保護法の制定背景です。これは州民発案によるということで、やや変わった立法プロセスがとられました。州民発案は直接民主制的制度で、住民が州の法案や憲法改正案を提出しまして、州の住民の直接投票でその法律を制定させるというものです。憲法、憲法改正ないしはその法律を制定させるかどうかということの是非を問う制度、これを州民発案と呼んでいます。カリフォルニア州のプライバシー保護法は、一旦州民発案で提案されまして、ですが、最終的には州民発案の取り下げと引きかえに、議会で消費者プライバシー法が成立したというプロセスになりました。州民発案がなされた後に、その間に反対派が一生懸命反対していた時期もあったのですが、ケンブリッジ・アナリティカ事件によって風向きが変わってということで、最終的には議会で成立したという状況です。２０１８年９月に一部改正されていますが、そんなに大きな改正ではないと認識しています。

カリフォルニア州のプライバシー保護法の構成ですけれども、第１条法律の名称ということで、カリフォルニア州の民事法典の中にプライバシーに関する規定を追加しますということを定めている、これが第１条になります。

第２条は、議会がどうしてこの法律を制定するのかという認識事項の中に、ケンブリッジ・アナリティカ事件への言及があります。

第３条が具体的に民事法典に組み入れられる規定で、第４条は分離可能性、これは一部の規定が無効になったとしても、他の規定には影響がありませんよということを定めている規定です。

カリフォルニア州プライバシー保護法の要点としましては、消費者の権利がさまざまに

定められていまして、開示請求権、削除ないしは消去請求権、オプトアウト権、権利行使に伴う差別の禁止、消費者が権利を行使するために事業者が講じるべき措置、定義制裁の仕組みが挙げられます。

１８ページをお願いします。この法律には開示請求権が３種類あります。個人情報を収集する事業者に対する、個人情報の種類、個別の個人情報の開示請求権といった個人情報へのアクセス権が１つめです。。２つめが個人情報を収集する事業者に対して、小さい文字で書いてあるほうですけれども、共有先第三者の種類などの開示をしなさいと求める権利があります。それから３つ目、個人情報を販売し、又は事業目的で提供する事業者に対して、収集した個人情報の種類、販売した個人情報の種類、販売先第三者の種類などを開示しなさいという権利です。この３種類に分けることができます。

次は消去請求権です。これは消費者から直接情報を収集した場合の消去請求権になります。事業者に対しては、個人に消去請求権が存在する旨を通知するということ、それから、消去請求権の行使があれば、自分の会社の記録からデータを消去して、サービス提供者にも消去しなさいと指示するといった義務が定められています。

ただ、例外もいろいろとありまして、契約の履行のため、セキュリティーインシデントの検出などの幾つかの場合には例外が認められています。

２０ページをお願いします。オプトアウト権です。このあたりは有名なところかと思いますけれども、自分の個人情報を第三者に販売する事業者に対して、販売をやめてくださいという権利を行使することができます。１６歳未満の場合は、あらかじめ同意を得る必要があり、オプトインが義務付けられます。

そのために必要な措置として、事業者のインターネット上のホームページに、個人情報の販売お断りというタイトルをつけて、消費者またはその代理人が個人情報の販売をオプトアウトできるようなウェブページへのリンクを張りましょうということが定められていたりします。あるいは、カリフォルニア州のウェブサイトから飛べるようにもする、そのような方法もあるようです。

２１ページをお願いします。こちらはプロファイリング的な話にもなってきますが、消費者が権利を行使することを理由とした差別を禁止する規定です。消費者プライバシー保護の観点での差別禁止です。

具体的な差別の内容としては、商品またはサービスを提供しない、あるいは値引き、得点の活用、ペナルティーの徴収、そのような方法を通じて、商品、サービスに異なる価格、

料金を課すといったものです。４点ほど挙げておりますけれども、消費者が権利を行使したことを理由に、消費者の利益を害するような差別を行ってはならない、商品、サービスの提供の関係で差別を行ってはならないということが定められています。

２２ページをお願いします。そうはいっても、消費者のデータ自体が示す価値がありまして、それが差異をもたらすことを合理的に説明できる、関連づけられるような場合には、異なる商品のレベル、サービスのレベルで実務を行うことができるようになっています。

また、事業者側としては金銭的インセンティブを提供することができます。保証金を支払うことなどによって、個人情報の取扱いを認めてもらいましょうというポイント還元プログラム的な話になってきますが、そうした形でインセンティブを提供することも認められています。

この金銭的インセンティブプログラムは、消費者がオプトインで事前同意を与えて、そのオプトインをいつでも撤回できる場合に限って加入させられるということになっています。インセンティブプログラムには若干制約はありますけれども、ただ禁止されているわけではありません。

２３ページをお願いします。消費者が権利行使をするためにフリーダイヤルを用意しましょう、ウェブサイトを用意しましょう、プライバシーポリシーを用意しましょう、そのようなことが定められている条文があります。

定義は最後の方に出て来ます。２４ページあたりです。ここでは消費者集団情報や事業者などの定めがありまして、全ての定義を挙げているわけではありませんが、主なものをピックアップしてみました。

消費者プライバシー保護法の義務規定については、消費者集団情報や匿名化情報というのを収集したり、利用したり、保有したり、販売したり、提供したりする場合に、そうした事業者の能力を制限してはならないという規定があります。つまり、特定の消費者に結びつかない情報については、自由に使えるようにしましょうといったことが書いてあります。

事業者については、適用範囲が若干問題になりまして、営利目的事業者で、小さい字で３点書いてある部分のいずれかを満たすものが事業者になります。大事な言葉を忘れていたのですが、カリフォルニア州で事業を営んでいる、操業していることというのが要件となります。3点のどれかに当てはまるケースとして、年間総収益が２，５００万ドルを超えること、年間５万件を超える個人情報を取り扱うこと、消費者の個人情報の販売から年間

収益の５０％を超える利益を得ていること。どれかに当たれば対象になります。

カリフォルニア州で事業を営んでいれば対象となりますので、文言上は、州の外の事業者、外国の事業者も含まれ得るという解釈になるはずです。

２５ページをお願いします。カリフォルニア州法は事業目的と営利目的を使い分けています。事業目的は、事業者もしくはサービス提供者の営業目的、その他通知された目的での個人情報の使用をいいます。いわゆる営利目的とは違う目的となります。事業活動上の目的のうち、営利目的を除いたものと見ていただいたほうがいいかもしれません。

営利目的はCommercial purposeということで要件が定められています。

２６ページ、消費者です。カリフォルニア州民である自然人が、ここで言う消費者です。下の「推測する」ないしは「推測」というのは、カリフォルニア州法の中でプロファイリングと絡むような定義になってきています。事実、証拠、情報もしくはデータその他の入手もとから情報、データ、予測または結論を導き出すことということで、この推測も個人情報の定義に含まれます。　２７ページから個人情報の定義を挙げております。特定の消費者または世帯について、直接的または間接的に、識別し、関連づけ、説明し云々と定められております。個人情報には次のものが含まれるが、これに限定されないということで、さまざまな情報のカテゴリーが挙げられています。

２８ページをご覧いただきますと、推測という言葉が入ってきます。推測を含むものが個人情報として幅広く定義されているというのが１つの特徴になろうかと思います。

ただし、個人情報の中から除かれるものがあります。２８ページの下のほうに書いてありますが、一般公開されている情報、すなわち連邦政府、州政府、地方自治体の記録から適法に入手できる情報は含まれません。公的機関から入手された情報は含まれません。

２９ページは、処理、販売などの定義を挙げています。自動的手段、コンピュータ処理による手法によるかどうかを問わず、個人データ、一連のデータについて実行される単一、一連の作業、幅広いデータの処理が含まれます。

販売についても定義があります。金銭的、その他有価の対価と引きかえに個人情報を販売、貸与、開示、発信など行うことです。

３０ページ、民事訴訟です。セキュリティー違反による不正アクセス等に対する民事訴訟を提起することができるという規定があります。消費者１人、事案１件につき１００ドル以上７５０ドル以下の金額といった形で法定賠償が定められています。

ここから先は細かいので省略したいと思いますけれども、消費者が提訴するときの要件

が設けられていたりもします。

３１ページ、民事罰です。こちらは司法長官が科すものになります。あらゆる企業、または第三者は本編の規定の遵守方法に関する指針として司法長官の意見を求めることができます。司法長官に意見を求めたところ、違反が見つかると民事罰の対象になってくる可能性が出てきます。

民事罰の対象ですけれども、故意の違反１件につき７，５００ドル以下の民事罰です。和解して和解金を分配し、それを消費者プライバシー基金に入れるという規定もあります。

３２ページ、消費者プライバシー基金ですけれども、この法律の執行のために訴訟を提起して、裁判所が負担する費用、司法長官が負担する費用を補填するために、消費者プライバシー基金が用意されています。個人への賠償を補填するものではありません。

３３ページ、消費者プライバシー保護法の評価ですが、内容的にはＧＤＰＲとはかなり違うと見たほうが良いという印象です。

まず、この法律は、透明性の向上を図っているということ、次に、差別禁止の規定はありますが、例外は結構広いといえること、金銭的インセンティブをどのような場合に提供できるのかが明確ではないこと、公的機関による公開情報が除外されるために除外情報が多いのではないかということ、さらには、私的訴権、損害賠償請求を起こしたとしても、立証が結構難しいのではないかということ、消費者プライバシー基金は消費者保護には役に立たないこと、このようなコメントが専門家から寄せられていたます。

このカリフォルニア州法は、ＧＤＰＲの米国版とも言われますが、かなり性格が異なっていまして、消費者のプライバシーを保護するという観点で定められているものです。また、対象は、民間事業者だけですし、個人の権利を定めることが中心となっているというところでも違いがあります。

救済方法としては、法定賠償と民事罰という形で、これもＧＤＰＲとは違う種類の違反への制裁のスタイルになっています。

それから、金銭的インセンティブを認めるなど規定がカリフォルニア州法にはありますが、ＧＤＰＲにはありません。

では、アメリカはアメリカで包括的な連邦法を制定する動きがあるのかといいますと、３４ページ以下に可能な範囲で幾つかスライドをご用意してみました。

１０月のプライバシーコミッショナー会議でアップルとフェイスブックがＧＤＰＲ的な立法をすべきだという発言をしたことがフィナンシャルタイムズの１面で紹介されていま

す。こちらの３４ページのスライドのように、コミッショナー会議の中でＧＤＰＲを持ち上げるような発言は結構出てきたようです。

３５ページです。では、アメリカで消費者プライバシー法を制定する動きがどの程度実現可能なものとして動いているのかを見るために、Consumer Privacyで法案の検索をかけてみました。２２５の法案が出されていまして、ほとんど法案提出段階でとまっているというものになります。

３６ページをご覧いただけますでしょうか。ケンブリッジ・アナリティカ事件を受けて法案を提出することがニュースに載っていた法案を幾つか探してみますと、これも法案提出段階にとどまっているという状況です。

現在、トランプ政権ですけれども、大統領府に対して電気通信や情報政策に関する助言を行う行政機関としてＮＴＩＡがあります。ＮＴＩＡは、基本的には自主的なプライバシーの枠組みを検討するということで意見募集を行っていたのが２０１８年１０月ごろでした。自主的なプライバシー枠組みとしては、こちらに挙げておりますような７つの原則が掲げられているということで、立法化の動きは私の知る限りでは具体的にはなっていないであろうという印象ではあります。

長くなりましたが、以上で報告を終わらせていただきます。

【宍戸座長】　ありがとうございました。

それでは、ただいまの事務局及び石井先生からのご発表につきまして、ご質問、コメントがございましたら、どこからでもお願いいたします。いかがでございましょうか。

では、まず宮内先生。

【宮内構成員】　ご説明ありがとうございました。宮内でございます。

今の石井先生のご説明について１点質問させていただきたいと思います。

消費者が対象のプライバシー保護ということなんですけど、消費者の定義には単に自然人と書いてあって、全体として消費者というところを個人と読みかえても大丈夫なのかどうかというのを１つ知りたいことと、もしも消費者という限定があるとしたら、具体的にどういう人たちが排除されて、その人たちはどういうふうに扱われるんだろうかと。常に個人情報をプールされていても、消費者に当たらないようなケースもあり得るのか。このあたりの範囲について教えていただきたいと思います。お願いします。

【石井准教授】　ありがとうございます。

「消費者」の範囲に関しましては、消費者プライバシー法は別の法律に定義されている

ものを引っ張ってきています。結論としましては、固有の識別子などで識別されたカリフォルニア州の居住者である自然人が対象とますので、カリフォルニア州に住んでいる個人であれば基本的には消費者に該当すると見ていただいてよろしいのではないかと思います。

【宮内構成員】　つまり、そういった制限はないと考えてよろしいということですね。

【石井准教授】　別の法律の中に、どこまで制限があるかというのを見ないといけないのですが、細かい部分は確認が必要です。

【宮内構成員】　わざわざコンシューマーと書いてあるところが少し気になったというだけなんですけれども、とりあえずそんな大きな制限はなさそうだということですか。

【石井准教授】　そうですね。識別されるカリフォルニア州の居住者である自然人となると、文言上は広く捉えていただいてよろしいかと思います。

【宮内構成員】　つまり、コンシューマーであって、こういうものだという意味じゃなくて、文字どおりこの定義だと考えてよろしいということですか。

【石井准教授】　交渉力の格差ですとか情報の格差があってとか、そういう制限ですか。

【宮内構成員】　そうじゃなくて、コンシューマーとはと読めたから、コンシューマーであって、かつかくかくしかじかの自然人という意味ではなくて、文字どおりこのとおり読めばよいのですねという。

【石井准教授】　そうですね。コンシューマーとという文言にはなっている。

【宮内構成員】　そうですね。わかりました。ありがとうございます。

【宍戸座長】　それでは、森先生、お願いいたします。

【森構成員】　ありがとうございます。私も石井先生に。なかなか勉強する機会がありませんでしたので、大変勉強になりました。ありがとうございました。

２４枚目なんですけれども、事業者の定義のほうなのですが、規模の限定とかがあるんですけれども、最後の行に「消費者の個人情報の販売から自己の年間収益の５０％超を得ていること」ということが要件となっておりまして、これだと随分限定された事業者が対象になるといいますか、販売ということだと、場合によってはグーグルなんかも入ってこないということになるかもしれませんので、この条件、年間収益というのは、ぱっと見た感じでは売り上げのような感じもするんですけれども、実際にデータを販売することをなりわいにしている人ということになるのでしょうかということが質問でございます。よろしくお願いします。

【石井准教授】　ありがとうございます。２４ページの事業者の３点目は確かに個人情

報を販売することから収益を得るという読み方になりますが、要件としてはどれかに当てはまればいいということになりますので、他の２つのどちらかに当てはまると事業者として適用対象になるという理解になります。

【森構成員】　ありがとうございました。そうすると、一定の規模がある事業者か、または名簿屋のような小規模でもそういうものということですか。

【石井准教授】　小規模事業者も入るのではないかという意見もあったりしますけれども、法律が想定しているのは、一定規模以上の事業者と見ていただくのがよろしいかとは理解しているところです。

【森構成員】　ありがとうございました。

【石井准教授】　ついでにもう１点よろしいでしょうか。

ご説明には入れませんでしたけれども、２４ページの事業者の定義で続きがあります。支配または支配される事業者ということで、その事業者と共通のブランディングを持っている、名称や役務商標、商標などを持っている事業者で、支配関係にある事業者も対象になるという規定があったりします。

【宍戸座長】　ありがとうございました。ほかにいかがでございましょうか。

生貝構成員。

【生貝構成員】　非常に貴重なご説明ありがとうございました。

石井先生の１８ページのところで、カリフォルニアのプライバシー法について、１７９８．１１０のところで、個人情報、開示請求権と上のところに書いているところ、こちらはｄ項のところだと思うんですけれども、そのデータというものはアクセス可能にする、readily useable format that allows the consumer to transmit the information to another entity without hindranceという形で、いわゆるデータポータビリティーの権利というのが、しかもＧＤＰＲのように本人が提供したデータに限る条項もない、非常に広い権利として含まれているように見えるところでございまして、いろいろと情報についてはヨーロッパでもさまざま議論があったところかと思うんですけれども、このポータビリティーの部分というもの、事業者の側ですとか、あるいは消費者の側、この条項について何か反応といいますか、そういった部分がもしあれば教えていただきたいという質問でございます。

【石井准教授】　GDPRとカリフォルニア州法を比較対照しているものは幾つかありますけれども、全く同じものではないですよね。ただ、カリフォルニア州法、確かにおっしゃ

るように、規定ぶりとしては結構幅広く読めてしまうというところがあります。実際に消費者が権利を行使するときにどう働いてくるのかというところは、国外事業者も含まれるという話になると、実効性のところは問題になるだろうという印象はあります。あまりお役に立てないコメントですみません。

【生貝構成員】　ありがとうございました。

【宍戸座長】　よろしいですか。ほかにいかがでしょうか。

では、寺田さん、お願いします。

【寺田構成員】　ありがとうございます。特にアメリカ、なかなかばらばらになっていてわかりにくいところが多いので、こうしてまとまっていると非常に助かります。

もしご存じだったらなんですが、ＮＩＳＴさんがプライバシーフレームワークのＲＦＩの募集を今されていると。なぜＮＩＳＴなのかというところもよくわからないところがあるんですが、これと今回の特にＮＩＴＡさん、ネットの関係というのを何かご存じでしょうか。

【石井准教授】　そこのフォローはできておりませんので、また後日でもよろしいでしょうか。申し訳ありません。

【宍戸座長】　もし何か石井先生のほうで後で情報がありましたら、事務局を通じてご提供いただければと思います。

【石井准教授】　はい、わかりました。

【宍戸座長】　あるいは、事務局において調べていただくのかもしれませんが。

ほかにいかがでございましょうか。よろしいでしょうか。

それでは、次の議論に移りたいと思います。続きまして、お手元の資料４でございますけれども、検討アジェンダ案に対する意見についてということで、森構成員からのご発表をよろしくお願いいたします。

【森構成員】　資料４をご覧ください。検討アジェンダ案に対する意見についてということで発表させていただきます。

検討アジェンダ案に対していろいろご意見が出ておりまして、幾つかピックアップしてご意見を申し上げたいと思います。

おめくりいただきますと、資料４、２ページ目、クッキー等によるウェブアクセス履歴の取得についてということで、ご意見としては３ページ目、一般財団法人情報法制研究所、読ませていただきますと、「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、個人情報保護法制で対処すべきものであり、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」というご意見です。

このご意見について申し上げる前に、どういう状況を問題にされているのかということで図でご説明をさせていただきます。

ご案内のとおりのことですし、また私がよくわからないのに説明するのもはばかられますけれども、後のことと関係もありますので、ゆっくりお話をさせていただきます。

まず、おめくりいただいて４ページ目、クッキーとはということで、ブラウザがサーバにアクセスをすると、サーバからクッキー、識別子を送ってもらって、再度、ブラウザがサーバにアクセスするときにそれを送り返すということになりまして、サーバとしては、この識別子はブラウザごとに違いますので、同じ人がまた来たなということがわかる、そのような仕組みであるということです。

ウェブ閲覧履歴の追跡ということになりますと、次の５ページ目の広告事業者のサードパーティークッキーというところのご説明ですけれども、仮にユーザーが私だとしますと、左側にスポーツ新聞のウェブサイトを毎日のように見ておりまして、○×スポーツのウェブサイトを私が見に行きますと、ウェブサイトからこのピンク色の部分が返ってきて、それを読むわけですが、白い画像というところがあります。この○×スポーツのウェブサイトとは、もちろんクッキーのやりとりがあるということですけれども、これがファーストパーティークッキーということになります。

この画像のところについては、○×スポーツのウェブサイトとしては、ここに広告を表示するということで、広告事業者のサーバにアクセスをして、そこから広告をとってきなさいという指示、これを画像タグというもので指示をしておりまして、その指示を受けて、私のブラウザが広告事業者のサーバに画像をとりにいく。これが４番からの手順でして、①、②、③と順番に振っておりますけれども、③のところで画像タグを受け取って、私のブラウザが、それでは広告事業者のサーバから画像をもらいましょうということで、④で広告事業者のサーバにアクセスして、⑤で画像の部分の広告とクッキーをもらってくるということですけれども、同じようなブラウザとサーバのやりとりですが、私が見ようと思っているウェブサイトはファーストパーティー、ファーストパーティークッキーで、知ら

ないうちにタグでアクセスさせられているほうがサードパーティーで、そこからくるのがサードパーティークッキー、そういう分類になるだろうと思います。

おめくりいただきまして、サードパーティーとのやりとりをさらに詳細に書いたのが６ページ目でして、こちらは私としては知らないわけです。画像タグによってブラウザが勝手にアクセスをしているわけで、私としては知らないうちに広告事業者のサーバにアクセスしている。そこからクッキーをもらってきまして、クッキーですので、同じ広告事業者のサーバにアクセスするとやりとりが発生する。私のブラウザが一意の識別子であるサードパーティークッキーを広告事業者に返すということになります。

このとき、この⑥のところに書いていますけれども、私のブラウザが指示に従って広告事業者のサーバにアクセスをするときに、広告事業者サーバとしては、どこの指示を受けてきたのかということがわかるということのようです。リファラーというところを見ると、私のブラウザが○×スポーツのウェブサイトの指示できましたよということがわかるということのようですので、その結果として広告事業者サーバの中で、○×スポーツと広告事業者が発行したサードパーティークッキー、ここではＤＭＰ１２３としていますけれども、この組み合わせが広告事業者のサーバのところで完成するということになります。

おめくりいただきまして、この仕組みを使って広告事業者はいろんなウェブサイトに、○×スポーツのウェブサイトと同じように画像タグを張ってもらうということになります。

画像タグを張ってもらっておくと、消費者、私がそれらのサイトにアクセスするごとに、消費者のブラウザは広告事業者のサーバからもらったクッキー、ＤＭＰ１２３を送ってくるということです。実は、私はいろんなウェブサイトを見たいので、スポーツ新聞だけ見ているというわけにもいきませんのでいろんなものを見ますけれども、実は広告事業者側では、いろんなウェブサイトにネットワークを持っていますので、サードパーティークッキーのやりとりをする広告事業者のサーバは同じドメインであるために、同じサードパーティークッキーをやりとりする。ファーストパーティーだけが変わるということになっているということでございます。

先ほど申し上げましたように、広告事業者サーバとしてはどのファーストパーティーからアクセスを指示されたかということもわかりますので、結果的にこのサードパーティークッキーであるＤＭＰ１２３をキーにして、ウェブサイトの閲覧履歴を作成することができるということになります。

おめくりいただきますと、こんな感じでサードパーティークッキーをキーにして、アク

セスの日時とどんなファーストパーティーにアクセスしたかということがわかるということになっております。こんな感じで、なるほど、このスポーツ新聞をよく見ていて、どうも引っ越しのウェブサイトに行っているな、ランニングシューズの検索をしているなということがわかるという形になっております。

おめくりいただきまして、このようにサードパーティークッキーをベースにして、この人は大体こういうところに関心があるということがわかりますので、広告を表示するときに、このスポーツ新聞のコンテンツの広告の部分、これが広告枠ですけれども、この枠にどんな広告を表示しましょうかということを決める手続がありまして、この枠はこんな人ですよ、５０代の男性です、どうも港区にいるようです、ランニングシューズを検索しています、引っ越しの予定があるようだということで、広告主側が、そうですか、それなら幾ら払いましょうということで競りをしまして、一番高いお金をつけた人が、何とか引っ越しセンターがこの広告枠を買いますと、そこに引っ越しの広告が表示されるということになります。これが、その広告を表示されるまでの短い間に起こるということです。９枚目のスライドはイメージでして、実際には全て機械的に行われていますし、基本的には広告主側代理人側のところで一元的にこういう手続が行われているということですが、イメージとしてはこんな感じのことが起こっているということです。

そうだとしますと、スライドをお戻りいただきまして、５枚目のスライドをご覧いただきますと、結局、左側の私のブラウザと○×スポーツの間の通信を広告事業者のサーバが観察することができるという状態にあるということになります。それの評価が先ほどの冒頭のご意見であったということです。

１０ページ目のスライドをご覧いただきまして、ご意見の評価ということになっていますけれども、サードパーティークッキーによるウェブ閲覧の観察、○×スポーツとブラウザの間の通信の観察行為は、直感的に見れば通信の秘密の侵害に該当し得るであろう。ただ、一方当事者の同意があるという整理は可能かなと思います。というのは、○×スポーツの協力がなければ、広告サーバは観察ができないわけですので、○×スポーツ側ではそれを教えてあげようと思っているわけです。それはそうなんですけれども、ただ、それによって直ちに通信の秘密の侵害でなくなるわけではないという考え方もあるということを主査の宍戸先生の文献で、ご論考で学びまして引用させていただいております。もしかしたら誤解しているかもしれませんので、ご指摘をいただければと思います。

そうなんですけれども、しかしながら、こういうことはかなり以前から、しかも日常的

に広範に行われてきた実態があるということですので、これを通信の秘密の侵害として統制することは、通信の秘密の形骸化、希薄化につながるというご意見はもっともだろうと思います。

他方で、こういった収集行為が個人のプライバシーを侵害するおそれがあることは否定しがたいというところでもありますので、これを放置することは妥当でないとも言えるかなと思います。

これにつきまして、ちょっと話は変わりますけれども、一番下の行に、クッキーにひもづく閲覧履歴、先ほどの表のようなものをユーザーの個人情報と結合することは、場合によっては個人情報保護法上の問題を生じるということになります。これは通信のこととは別の話です。

おめくりいただきまして、通信のお話に戻りまして、先ほど三菱総研さんからご紹介のありましたePrivacy規則案による規制というものがこれと同じ場面を取り扱っているので、参考になるかなと思ってここに書いてまいりました。基本的には、先ほどご説明があったとおりですけれども、前文の２１というところで、トラッキング用のクッキーなどが利用者の知らないうちに、利用者の端末機器に入れられることがある、そういう事実を指摘していまして、その上でクッキー等を利用した利用者のオンラインでの行動、それから端末機器の位置をひそかに監視する技術は、利用者のプライバシーにとって深刻な脅威である。前半と後半で違うことを言っておりますけれども、少なくとも前半、利用者のオンラインでの行動。

それから、３番目ですが、したがって、このような端末機器への干渉は、利用者の同意があり、かつ特定された透明な目的のためにのみ許容されるとしております。

これを受けて、おめくりいただきまして、条文としては８条というところになりますけれども、ユーザーの端末機器の情報を収集することを原則として禁止していて、電気通信の送受信に必要な場合や利用者の同意がある場合等の例外的場合にのみこれを可能とする、そういう規則案になっているということです。

許容される場合、これが限定列挙なのか、それとも例示列挙なのかというのが先ほどの三菱総研さんのご説明であったということです。限定されたものの場合だけ許されるのか、それともその他正当な利益がある場合という許容の仕方をするかということについて議論があるということでした。こういったことを参考にできるのではないかと思います。

以上が閲覧履歴の問題でしたけれども、その次に位置情報についてお話をしたいと思い

ます。これはご意見ということではないんですが、先ほどのePrivacy規則の前文で、１１ページをご覧いただきますと、２番目のポツのところですが、「Cookie等を利用した、利用者のオンラインでの行動」、これが先ほどのお話ですが、それともう一つ、「端末機器の位置を密かに監視する技術」ということになっておりまして、こちらも懸念があるということがePrivacy規則の前文で語られているということです。

１４ページにお戻りいただきますと、この位置情報、位置の観察について、前記のとおり、これこれは利用者のオンラインでの行動のみならず、端末機器の位置をひそかに監視する技術について懸念しているということですが、これについては、我が国の電気通信事業者については、位置情報プライバシーレポート、それから電気通信事業者向け個人情報保護法ガイドラインによって厳格な制約が課せられているというところかなと思います。この部分については対応があるということです。

ただ、これは電気通信事業者に対するものですので、そうでない場合であっても、同じような監視が可能、ひそかに監視することが可能である場合には、何らかの制約、電気通信事業者と同等の制約が必要ではないかと考えられるのではないかと思います。

位置情報プライバシーレポートは、対象が電気通信事業者に限られているということ、それから、時期的な問題もあって用語が古いというところがあります。特定性低減データという、現在では匿名加工情報という正式名のものですけれども、そういったことがありますので、改定の必要性があるのではないかと書かせていただいております。

次が３番目で、こちらが最後となりますが、電気通信事業法の域外適用についてということです。

おめくりいただいて１６ページ目ですけれども、これも検討アジェンダに対する意見ということで、株式会社ＮＴＴドコモからのご意見です。下線部分を読みますが、「通信の秘密やプライバシー保護について、事業者の分類（電気通信事業者／プラットフォーム事業者等）によらず、また電気通信設備の設置場所（国内／国外等）によらず、公平・公正な競争環境を実現できる規律の在り方が検討されることを望む。また、利用者から見たときに同一の意味を持つ情報については、利用者情報の分類によらず、通信の秘密やプライバシー保護の在り方も同じように取り扱われることが必要」とされています。

おめくりいただきまして１７ページ、ソフトバンク株式会社のご意見です。下線部のみ読みますが、「プラットフォームサービス（電気通信役務を含む）に関する検討を行う際には、公正な競争環境が整備されるよう、プラットフォーム事業者が保有する利用者情報

の取扱いやその他制度面の扱い等においてイコールフッティングの確保を重視すべき」というご意見になっております。

これは、日本の電気通信事業法の規制が同じようなサービスを行う外国事業者に対しても適用されるべきであるというご意見であろうかと思いますけれども、この問題、つまり国内の規制が、日本の規制が国内事業者に適用されるけれども、国外事業者に適用されないという問題は、最近では一国二制度と言われておりまして、非常に大きな課題であるということで、いろんなところで検討されております。特に他のプラットフォームに関する政府の検討、こういったところで取り上げられておりまして、多く報道されているデジタル・プラットフォーマーを巡る取引環境整備に関する検討会、総務省、経産省、公正取引委員会の検討ですけれども、こちらの報告書にも記載があるところです。

これはどちらかというと、競争を中心に検討されていることなので、イコールフッティングというところが前面に出ていますけれども、まず規制について考えるべきことは、その趣旨は、国内の消費者の保護ということですので、２ポツのところですが、我が国の利用者に電気通信サービスを提供する事業者に対して、等しく電気通信事業法が適用されないことは、我が国の利用者の保護に欠けるということ、これが重要ではないかと思います。もちろん、公正競争という観点からは、このイコールフッティングも重要であるということになりますが、まずは利用者が守られない場面が出てくるということが、国内法が同じサービスを提供する外国事業者に適用されないことの直接的な問題ではないかなと思います。

このようなことから、域外適用を可能にするような規定を電気通信事業法に設けるべきではないかと書かせていただきました。

また、共同規制という考え方もありまして、自主規制、共同規制、ソフトローの考え方もありまして、内外のプラットフォーマーが同じ行動規範に服する自主的な取り組みが考えられる、そういったご意見もさまざまなところで伺うところですけれども、ただ私は個人的には、日本の場合は皆さんで自主的な取組みというと、わりと皆さんでということになるわけですけれども、なかなか外国の事業者さんですと、何で入らないといけないんですか、どういう利益があるのか、どういう不利益があるのか、最終的には間に入った日本のご担当の方が説明にお困りになるということもありますので、実効性には疑問があるのかなと思っているところです。

長い間お時間をいただきました。私のご説明は以上です。

【宍戸座長】　ありがとうございました。

お手元、参考資料１をご覧いただきたいと思います。プラットフォームサービスに関する研究会の検討アジェンダというので、先ほどもご紹介がありましたように、これまでの議論を踏まえて、この研究会としてのアジェンダとしてまとめられているものですけれども、先ほどの森先生のご指摘、ご意見は、この前の第２回のときにご提出いただいた資料ということで、検討アジェンダ案に対して出されたご意見に即しながらいろいろご意見をいただいたものと思います。参考資料１とそのまま通じるところがあろうかと思います。

具体的に申しますと、先ほどお話のあったクッキー、位置情報は、参考資料１で申しますと７ページ、８ページの利用者情報の保護の範囲の問題。それから、今のイコールフッティングといいますか、域外適用関係のお話は、参考資料１で言いますと５ページの射程であったり、１２ページの運用・執行の在り方の問題についてご意見をいただいたということで森先生、よろしゅうございますか。

【森構成員】　はい、結構です。

【宍戸座長】　ありがとうございます。

それでは、今の森先生からのご発表を前提にしてご議論をいただければと思いますが、いかがでございましょうか。

では、生貝先生、お願いします。

【生貝構成員】　ありがとうございます。今、森先生がご説明をいただいたこと、私としても全体としてePrivacyを見ながら考えていること、およそ同意見でございます。

特に２つございまして、１点目は特にクッキーですとか位置情報等の問題に関して、確かに日本法上、通信の秘密に位置づけるということはさまざまな議論があるんだろうと思います。ですが、前も申し上げましたとおり、ヨーロッパのほう、ePrivacyはDirectiveの時代から、このことをconfidentiality of communicationを実現するという大きな枠の中で具体的に緻密にどうするかということを考えてきたと。だから、僕は、confidentiality of communicationを日本語に、通信の秘密と訳すことにすごく躊躇があるのはそこにあって、同じことを目的にしているんですけど、やっぱり違うんですよねといったこと。

そういう中で、広く通信のプライバシー、通信に関連するプライバシーをどう守るのか、通信の信頼性、あるいはそれに根差す表現の自由というものをどうやって守っていくのか、これはＥＵも全て共通するところでございますので、そういう観点からおそらく枠組みと

いうものを、今までの通信の秘密というところとまた並行しながら広い意味で考えていく必要があるんだろうということが、最近改めてヒアリング等を聞いていても感じるところであります。

その上で、少しだけ話題を広げてしまうんですけれども、やはり僕もここしばらく通信の秘密等を勉強することになって改めて感じるのは、やはり日本の場合、電気通信事業法４条の非常に短い条文のさまざまな一般法的な解釈の中で、緊急避難ですとか、正当業務行為ですとか、解釈ですとか、ガイドラインですとか、何々レポートですとか、そういう中で非常にクラフトを積み重ねてきていらっしゃるなと。それはそれで非常に頑健な方法ではあるのだと思うのですけれども、やはりこれから特に通秘というのが事実上、社会全体で非常に重要になるときに、そろそろePrivacy指令や最近のさまざまな事業者さんの状況、ご要望などを見ていても、そろそろePrivacy指令のように書き下していくことというのも具体的に考え始めてもいいのではないかということを、常に思いを強くするところがあるわけでございます。

例えばセキュリティーの目的、もしかするとそういった中身、メタデータの部分を利用したある程度消費者に便利なサービスですとか、そういったものというのが、本当に解釈の枠組みの中だけでどのぐらい適切に、かつ消費者を守りながら実現できるのか。

なおかつ、同意をどうやってとるのかということに関しても、少し三菱様のほうから、先ほど１０条のブラウザセッティングのところが取り除かれたというご説明をいただきましたけれども、ただ、あれもクッキーのドメインに関して、プライバシーのセッティングはブラウザ等のソフトでできるという規定そのものは引き続き残されておりますので、実質的にそうは変わっていない。個人情報を含めた議論というものをやはり電通通信も含めてやると、どうやって同意をとるのかといった難しくなるところ、やはりそれに独特の同意のとり方というところも含めて非常に丁寧に法のつくり方をやっていると。

これはあくまで、すぐに対応できる問題だと思ってしゃべってはいないんですけれども、ただ、この検討会自体、２０３０年というタイムラインをめどに置いて議論されていると思いますので、そういった中で、ePrivacy規則というのは、具体的には日本の電気通信事業法の４条と、電気通信事業における個人情報保護ガイドラインと、特定電気通信役務提供法などを１個にくくり出して、具体的な法律、電気通信分野のプライバシー法としてクオリファイしたものであります。そこまで大がかりなことにするのかといったことはともかくとして、やはりその点というのは、特にこれからＯＴＴ全体に通信の秘密をどうする

かという議論をしていくときに、果たしてそれがどこまで可能なのかというところを含めて考える必要があるのかなということが１つでございます。

１つで大分長くなりましたので、一旦ここで切ります。

【宍戸座長】　今、生貝構成員からご指摘あったのは、資料１で言いますと４ページ目の主査ヒアリングでの曽我部先生の右の法律の規律密度をもうちょっと向上させたほうがいいんじゃないかといったご指摘にも通じるところがあろうかと思います。どうもありがとうございます。

続きでやりますか。それとも、一旦よろしいですか。

【生貝構成員】　それからもう一つ、域外適用のところに関しても、森先生のおっしゃるとおりだと思っていまして、今イコールフッティングという言葉を強調されるんですけれども、半分以上に重要なのは、我が国の利用者の情報をどうやって守るか、安心して使えるようにしていくかということ、むしろこちらのほうが本丸の議論だと思います。

といいますのも、どうしてもこのプラットフォームの議論、この検討会に限らず、いろいろ参加しておりますと、どうもアンチＧＡＦＡなのか、海外プラットフォームをどうしたいのかといったこと、僕自身もいろいろ言われることが間々あるんですけれども、少なくともそんなことは僕自身は全くありません。

何かと言うと、やはり一消費者として考えたときに、一番便利なプラットフォームを国内外問わず、それはアメリカであったって、これからは中国であったって安心して使いたいし、自分たちの子供にも使わせたいという環境というのを果たして通信の時代にどうやって実現していくか。むしろ、国境なく、海外のサービスを安心して使えるようにするために、海外の事業者さんに対しても、日本の法をちゃんと守っていく方法というものをどうやって考えるかということがこの問題で、それに限らず、今いろいろ議論されているプラットフォームの議論の根底にあるべきものだし、あるんだと僕自身理解しております。

そういった観点から、まさに実際の事業者さんが無理のない形で、自主的な取り組みを尊重しつつ、しかし、法的基盤はしっかり整えていくといった本来の意味での共同規制的なアプローチを含めて、そういったことを実現する方法を考えていただきたいなという意味で、まさしく森先生の議論に非常に同調するところでございました。

長くなりまして恐れ入ります。

【宍戸座長】　ご意見ありがとうございました。ほかにご意見あるいはご質問等いかがでございましょうか。

寺田さん、お願いします。

【寺田構成員】　ありがとうございます。生貝さんのお話に続けてという形になるんですけれども、通信の秘密のほうでいくと、例外の積み重ねというのがこれまでずっと続いてきました。そろそろ例外のほうが多い、正当行為の例外のほうが多いようなおかしな状態になりつつあるんじゃないかなということで、ここは多分、もう一度見方をひっくり返さないといけないんだろうなと。何がだめで、何がいいのかというところをもう一度考え直す必要があるんだろうなと思っています。

もう一つ、今回、ePrivacyなんかでもそうですけれども、クッキーというところへすごく視点が行ってしまっていて、現実的にはここは端末のＩＤ全てにかかわってくる話だと思います。ＥＵの場合は、今回、コンテンツというのとメタデータというものに分けて、メタデータそのもの、全体をもう一度見直す仕組みになっているかと思いますけれども、このあたりも、アメリカでは全く違う、メタデータという考え方ではなくて、何をしてはいけないかという形の見方で考えているというところもあって、ここは整合性をとらないとしんどいことになるのかなと思っています。

というのが、端末のほうは、例えばスマートフォンのプライバシーというのであれば、ＭＡＣアドレスだとか、グローバルＩＤと言われるものとクッキーと言われるもの。最近ではそれ以外に、フィンガープリントであったりとか、ＩＤとして使えるものというのは幾らでも組合せでもつくっていけるというところもあって、こういったＩＤそのものを区分していく考え方というのはそろそろ限界だろうと。それを使ってやりたいことというのは基本的に同じようなことばかり考えていますので、そちらのほうから、いわゆる行為規制とかいったところから考えていかないともう追いつかないだろうと思っています。

これは実は位置情報も同じで、位置情報といった場合に、イメージとして基地局、ＧＰＳといった直接位置を把握するものを検討している部分が強いんですけれども、実際には最近は、例えば一番単純なところでいくとＱＲコード、これを取得するだけでそのＩＤがとれます。そのＩＤはどこにあるのかというのは、裏のデータベースにあって、そこから引っ張ってくることができますといったときに、これを位置情報の現在の考え方でいくと、規制というのは非常に難しい状態になると。これもやっていいことと悪いこと、そういった部分からもう一度見直さないとさすがに難しいなと感じています。

感想みたいなものですけれども、以上です。

【宍戸座長】　貴重なご指摘ありがとうございました。

ほかにいかがでございましょうか。

崎村さん、お願いします。

【崎村構成員】　寺田構成員のご意見に全く同意なんですけれども、個別のデータの項目に対してかけるというのは完全に限界にきていると思うんですね。こういうものを取得しますといっても、消費者は多分わからないです。今週のニュースだと例えばフェイスブックが端末の位置情報は取得しませんと言っていながら、ＩＰアドレスからどこかというのを検出して、それでターゲティング広告をやっていたというのがありますけれども、ユーザーはＩＰアドレスはとりますと言われているんですが、ＩＰアドレスと位置情報の一致性というのは多分想像の概念です。だから、ユーザーに対してプレゼンテーションする場合には、各項目じゃなくて、何をするんです、何をすることを許してください、目的のほうを許してもらうような格好に持っていかないとつらいんじゃないかなと思っています。

例えばブラウザに関して言うならば、今グーグルだとかフェイスブックだとか、大概のプロバイダは認証目的のためには１００種類以上の情報をとっています。それによって得られる一意特定性というのは、ユーザー名、パスワードよりも高いくらいになっているという状態です。ただ、本人を保護するために使うのはすごく正当な話なんですよね。逆に、それを使ってターゲティング広告を出すというのは許されないようなことだと思うので、やはり同じ情報でも目的によって違うので、情報の種類で規制をかけていくというよりも、目的で編さんするということのほうが、説明していくということのほうが重要なんじゃないかなと思っております。

【宍戸座長】　ありがとうございました。これも貴重なご指摘だと思いますが、さらにほかにいかがでございましょうか。

木村さん、お願いします。

【木村構成員】　いろいろとありがとうございます。本当にこういうことだというのをよくわかるご説明で、森先生、ありがとうございます。

私もいろいろ話を聞いていて、幾らどうだこうだといっても、ＳＮＳでも何でもそうですけど、利用者は使いやすいもののほうに流れてしまう。どんなに危険だと言われても、やっぱり使ってしまうというのはありがちなことだと思いますし、そういうことを踏まえますと、安心して利用できるように、森先生のご説明にあったように、域外適用を可能にするということはきちんと検討していかなければいけないと思いますし、一番最初の資料で三菱総研の利用者の意識というところで、不安感掛ける理解度というところがありまし

たけれども、利用者が不安感を感じなくて済むように検討していかなければいけないと思っています。

そして、今崎村先生からありましたように、同意についての考え方ですとか、今のままでは利用者もわからない。自分が使っている端末のことを本当に理解して使っている人なんて一握りで、みんな何となくわからないけれども、何となく便利だから使っているんだよねというところで、きちんと不安を感じないようにしていくことが必要ではないかと思います。雑駁な感想になってしまいましたけれども。

【宍戸座長】　ありがとうございました。消費者を代表して貴重なご意見をいただきました。さらにいかがでございましょうか。

もしなければ、私からも少し、一構成員としてご意見を申し上げたいと思います。

３つあるのですが、１つは、これまで、この研究会でもそうですし、森先生、生貝先生からも、域外適用という言葉でこの問題をご議論いただいている部分があり、またメディアにおいてもそうだと思うのですが、少し言葉遣いを整理したほうがいいのかなと思っております。つまり、例えば日本国民の通信の秘密を守る、しかもそれを域外適用として守るというときに、一番典型的な域外適用は、日本国民が例えばアメリカに行って、アメリカで電話をかけるといったときに、アメリカの通信サービスをまさにアメリカの場にいて利用しているといったものに対して、日本の電気通信事業法を適用する。域外適用という場合、これが基本的な典型的な場面だと思うのですが、今我々が議論しているのはそういうことではないわけであります。

日本国民がとりわけ日本国内で電気通信を利用する、そのときにキャリアさんが通信サービスを提供している場合には、我が国では電気通信事業者の提供する電気通信事業であるということで通信の秘密がかかっていた。そうではなくて、例えば日本国内で日本国民が他の日本国民とプラットフォーム事業者が提供する何らかのメールサービスなどを利用しているというものは、ある意味では日本国内で行われている通信であり、それにかかわる設備であったり、機能の一部、あるいはかなりの部分がもしかすると海外にあるかもしれない。しかし、利用者の行っている通信は、ある意味では国内で起きているというものであるわけです。そうだといたしますと、電気通信設備の問題はちょっと外しておきますと、域外適用と今のような自体を言うべきなのか。言うこと自体が１つ、本来整理が必要なのではないかと思っております。

つまり、他の分野で、法務省が所管するような法領域で議論されるときの域外適用とい

う言葉との整理が少しこの辺が必要ではないかと思っております。これが１点目です。

それから２点目は、そこで今のいわゆる日本国法上の電気通信事業者とＯＴＴ事業者の間の関係に関しましては、先ほど森先生から事業者間の公正競争でありますとか、あるいは電気通信事業者でない類似のサービスについて、通信の秘密を規定する電気通信事業法が適用されないと我が国の利用者の保護に欠けることとなる、こういったご指摘がありました。

もう１点考え合わせるべきは、サービスないしレイヤレベルで見ますと、電気通信事業あるいはネットワークで通信を扱っている部分、それからその上の部分。例えばプラットフォームレイヤあるいはコンテンツのレイヤがあり、ネットワークレイヤで行われている我々が通信の秘密としてこれまで保護してきたもの、その情報とＯＴＴのレベルでの情報というものをくっつけることによって、今までの通信の秘密は通信の秘密、コンテンツレベルあるいはＯＴＴレベルでの保護は個人情報保護といって、それぞれを別に分けてきたというものが、事業者の両方のレイヤをまたいだくっつけ方によっては、新たな質的に異なるプライバシーリスクを利用者の側に発生させているのではないか。

同じことは逆にも言えまして、プラットフォーム事業者がネットワークサービスを提供する。そして、プラットフォームサービスのレベルで集約してきたデータを通信領域でのネットワークレベルでの通信の秘密として問題になるものとくっつけることによって、何か新しい問題が起きるのではないか。つまり、このようなレイヤをまたいだ利用者情報の取扱いが一体的になされるといったことについての問題を少し考えておく必要があるのではないか。これが２点目でございます。

３点目は、森先生から先ほど私が随分前に書いた論文に触れていただきましたので、同意関係の問題、あるいはこれまでご指摘のあった、寺田さんとか崎村さんからご指摘のあったことについて考え申し上げますと、通信の秘密が結局何を本当は守ろうとしているのかということについて、前も私の理解ということで、安全、安心な通信サービスの供給、あるいは客観的な通信制度、主観的には利用者の通信の利用を保護する、通信の権利を保護するといった部分があるということと、それから表現の自由であったり、プライバシーを守るといった側面があるということを申し上げたことがあるかと思います。

その観点から見ますと、通信の秘密を通信を成立させるために使うというのは、もともと通信の秘密の窃用にならないとか、あるいはなるとしても、正当業務行為になると考えてきた。その延長線上で言いますと、安全、安心な通信サービスを確保するということも

似たような通信の秘密を保障する第一の根拠という観点から見ると飲み込めるかもしれない。また、通信の秘密に触れる、あるいは事業者以外の人が触れるということが利用者の自由な情報流通に対して何らかの萎縮をもたらすということがある。

例えば先ほど崎村さんとかがおっしゃった例にかかわるかと思いますけれども、携帯を持っているということで、しかし、それが実際にはよくわからない形で自分の位置情報とが把握されてしまうということは、この延長線上で自由な情報流通でありますとか、その人の生き方、行動を制約する、萎縮させることになり得るかもしれない。そうであれば、それがここで問題になっている、データの項目が何かどうかということとはかかわりなく、またそれを通信の秘密と言えるかどうかにかかわりなく規律をするということが正当化されるべきではないか。例えばこういうふうにも考えられる。

最後３点目で、プライバシーが通信の秘密の保障の根拠にあるということとの関係で言いますと、一般的には、森先生が挙げていただいたお話で言いますと、当事者間でいろいろ通信をしているときには、とりわけメッセージの部分については、両当事者がお互いに共有しているものであり、片側が裏切ってプライバシーを暴露したというときにはしようがないものだということでもともとメッセージの部分についてはやっているところがあるんだろうと思います。

しかし、ここでよく典型的に問題にされてきたのは逆探知の例だと思いますけれども、片方、メッセージの内容だけを逆探知における誘拐された児童等の保護者で、電話かかってきた人が警察に対して同意をするということで情報を提供するというときに、必ずしもこれはメッセージの部分だけではなかったわけです。居場所とかを特定しようとする。今のような場合ですと、誘拐犯にとってはそれは不意打ちになる。しかしながら、この場合、誘拐犯のそのような位置情報についての期待は別に保護すべきものではない。こうやってぐるぐる考えていきますと、逆探知のような場合に、一方当事者の同意によって通信の秘密の利益を侵害するということが、今のような全体の事情の中で許されるといった議論をしてきたんだと思います。

随分長々と私のほうからお話しさせていただきましたけれども、これまで通信の秘密の問題として議論されてきた、先ほどのお言葉をかりればデータ項目であったり、利用の在り方、利用の目的、あるいは規制すべき行為を少し整理し直して、とりわけプラットフォーム事業者についても通信の秘密、あるいはそれに類似する保護を求めるという場合に、今までの事例とかを含めて一定の整理をし直す。そして、整理をし直した上で、それを現

行法の解釈としていける部分があるのか。あるいは、明確な法的規定を置くか。それも、置き切れる部分と置き切れず、ある程度は解釈に残さざるを得ない部分も出てくるかもしれないけれども、そういった議論の整理を少ししていく必要があるのではないかということを今までお話を伺って、私の意見として思うところでございます。

誰からも手が挙がらなかったので、少し私のほうでしゃべらせていただきました。ほかにいかがでございましょうか。

森先生、お願いします。

【森構成員】　ありがとうございます。私もあまり自分でまとまってたわけではなかったんですけれども、先生方のご意見を伺ってだんだんはっきりしてきましたので、意を強くして申し上げますと、私もそうですし、先生方のご意見もそうでしたが、通信の秘密の規制を大きく変えようというご意見ではなかったんだろうと思います。

基本的には、従来の通信の秘密の考え方はそのまま維持されるべきであって、ただ、特に２つの点ですよね。メタデータの問題と、もう一つは違法性阻却事由、特に正当業務行為の問題を具体化する、それは現代に合わせた形だと思うんですけれども、例えば電気通信事業法の逐条解説を見ても、メタデータも保護の対象であるというところに、通信の相手方ですとか、通信の時刻ですとか、そういったものは通信の意味内容を推知させるものであるから保護されるべきであると書いてあります。確かに相手方はそうでしょうし、通信の時刻もそうだと思いますけれども、通話時間というものがありますが、通話時間というのは、もしもし、はいはいの世界ではそうかもしれませんけれども、例えばウェブサイトを見るときに、通話時間に相当するものは何なのかという気もいたしますし、さらに言いますと、データの場合はポート番号のようなものもありますが、ポート番号が果たして通信の意味、内容を推知させるのかというと、どうもそうではないような気もいたしますので、そういった形での洗い直し、私が今ここで、これは入ります、これは入りません、とても全然申し上げられるだけの見識がありませんけれども、現代化と具体化というのが求められているのかなと思いました。

【宍戸座長】　ありがとうございました。ほかにいかがでございましょうか。

では、大谷構成員、お願いします。

【大谷構成員】　どうもありがとうございます。森先生のご説明は、基本的に私も、基本的な方向については賛同するところですし、皆様からその後、相次いで寄せられた意見についても、なるほどと伺わせていただいたところです。

個人的に関心がありますのが、通信の秘密そのものについてもさることながら、やはりＭ２Ｍのように人が通信の当事者になっていないものが実は本当に多岐にわたっていて、人が実際使っているものでも、端末そのものに付与されているアドレスであったり、端末のコードといったものが収集されていて、特に個人と紐づけられることなく、広告などに活用されているという実態があるわけですので、実際にePrivacy規則案の中でも、Ｍ２Ｍの通信の取扱いなどについて議論が、まだ揺らぎがあるところだと思いますけれども、人が関わるもの、そして人の行動などを監視、推測するために使われている通信と、それではなく、どちらかというと産業目的に使われているものなどの役割をちゃんと整理していかなければいけないかなとも思っておりまして、それについては三菱総研さんのご紹介にもありましたけれども、現在、ヨーロッパで行われている議論の動向、特に産業界からのご意見などについても、引き続き情報収集をしたほうがよいのではないかと思って見ております。

また他方、人が関わるもの、実際には端末に付与されているＩＤですとか、それにかかわる位置情報などの場合は、どうしても個人がそれに対して同意を与えるか、あるいは許容しているかという観点で、同意がなされている場合には、それは使っていい情報だという整理をなされるものなんですが、通信の秘密と同意の関係については、今宍戸先生からもお話があったところで、ちょっと複雑な部分もあるとは思いますけれども、同意というものにあまりにも依拠した仕組みというのは、いずれ限界があり得るのではないかとも思っております。

同意という逃げ道がある制度というのは、他の行為規制などをある程度厳しくしたとしても、最終的には同意が得られているという形で規制をくぐり抜ける行動が、事業者としてはそういう行動にどうしても誘導される側面があると思いますので、同意という仕組みがあるとしても、それ以外にどんな可能性があるか。つまり、例外規定をつくるときの考え方というのをこれから十分に整理していく必要があるのではないかと思いました。

その点で非常に示唆をいただいたのは、三菱総研さんの取りまとめてくださった利用目的の確認の状況についての差異なんですけれども、もう少し詳しい情報、例えば年代別の利用目的の確認の実態などについてわかるようでしたら、そういうデータを後ほどいただければ議論の素材としても役に立つのではないかと思っております。

以上でございます。

【宍戸座長】　ありがとうございました。今後の調査についてもご意見をいただきまし

た。

予定した時間でございますが、ほかに何かこれはということはございますでしょうか。

では、お願いします。

【手塚構成員】　まさに今のＭ２Ｍ系の話は今後かなり環境としても出てくると思っております。そういう中で、今までの、特に私の見ている分野で言うと、署名とか電子署名なんかは、必ず日本の場合は自然人にリーチした形で全てが成立されている。これがＭ２Ｍになったときに一体どういうふうにこういう世界を考えていくのか。例えばサーバがばんばん打ったときに、これは誰の責任になるのかとか、そういう機器系のものと今あるヒューマン系との連携のところを今後法体系の中でどういうふうに考えていくのかというのは、ＩｏＴが出てくれば出てくるほどそこは重要なテーマになると思っていまして、ぜひその辺もこういう場でしっかりと検討いただけるとありがたいと思います。

【宍戸座長】　今手塚先生ご指摘いただいたのは、この研究会の第１アジェンダである利用者情報と、第２のアジェンダであるトラストサービスとまさに両方またぐお話だろうと思います。ありがとうございました。

まだいろいろご意見はあろうかと思いますが、時間でございますので、本日の質疑応答はここまでとさせていただきます。ありがとうございました。

その他事務局から連絡事項からございましたら、よろしくお願いいたします。

【岡本消費者行政第二課企画官】　次回会合につきましては、別途事務局からご案内をいたします。

事務局からは以上でございます。

【宍戸座長】　ありがとうございました。これにて本日の議事は全て終了とさせていただきます。

以上で、「プラットフォームサービスに関する研究会」第３回会合を終了とさせていただきます。本日は、皆様お忙しい中ご出席いただき、ありがとうございました。また、多くの方にとりましてはということですが、どうぞよいお年をお迎えいただければと思います。