

プラットフォームサービスに関する研究会（第2回）

1 日時 平成30年11月5日（月）10:00～11:30

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、宮内構成員、森構成員、山口構成員

（2）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

（3）オブザーバー

三原個人情報保護委員会参事官

4 議事

（1）トラストサービスに関する現状

（2）提案募集の結果等について

（3）意見交換

（4）その他

【宍戸座長】 本日は、皆様、朝早くからお忙しい中お集まりいただきましてまこと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2回会合を開催させていただきます。

冒頭、カメラ撮りがございますので、少々お待ちください。

【岡本消費者行政第二課企画官】 会議の冒頭、カメラ撮りの報道関係者が退出いたしますので、しばらくお待ちください。

(マスコミ退室)

【宍戸座長】 それでは、カメラ撮りはここまででございますので、早速本日の議事に入りたく存じます。

本日は、前回会合で示されました検討アジェンダ（案）にありましたトラストサービスについて、事務局からのご説明と、手塚構成員からのご発表を予定しております。その後、事務局から提案募集の結果などについてご説明をいただき、これを踏まえた意見交換をお願いしたいと考えております。

それでは、まず事務局から、トラストサービスに関する状況について、ご説明のほうをお願いいたします。

【赤阪サイバーセキュリティ統括官室参事官】 資料1をごらんください。本研究会の検討事項といたしましては、プラットフォーム事業者における利用者情報の取扱い等に加えまして、いわゆるトラストサービスの在り方につきましても位置づけられております。まず、事務局より、このトラストサービスに関する現状について、簡単に概要をご紹介させていただいた後、手塚構成員より、EUの動向も含めまして、より詳しいご説明をいただきたいと思っております。

資料1の、ページをめくっていただきまして、1ページ目をごらんください。サイバー空間と実空間の一体化が加速的に進展していきまして、実空間でのさまざまな活動がサイバー空間に置きかわっております。こうしたさまざまなサービスの利用に当たりましては、グローバルなプラットフォーム事業者が提供するIDと連携する形での利用というものが広がっているかと思えます。

他方で、オンラインでのやりとりにおきまして、通信の相手先となる組織や人の認証にとどまらず、ネットワークにつながるモノの認証であるとか、あるいはネットワーク上を流れるデータの完全性の確保、こういったものが求められているところかと存じております。

こうした中、EUにおきましては、eIDAS規則というものが制定をされておりました、絵の下の部分でございますけれども、電子署名、タイムスタンプ、ウェブサイトの認証、それから法人を認証するeシール、それから送受信の識別や送受信データの完全性を保証するeデリバリー、こういったサービスをトラストサービスとして包括的に規定するというを行っております。

こうした中で、我が国といたしましても、国際的なサービスの進展を視野に入れた相互

運用性の確保の観点から、こうしたトラストサービスの在り方について検討する必要があるものと考えております。

2 ページ目をごらんください。トラストサービスのうち、我が国におきましては電子署名につきまして、電子署名法という法律がございます。その内容でございますが、(1) にございますとおり、本人による一定の条件を満たす電子署名が付されている電子文書につきましては、真正な成立が推定されるということ。それから、(2) にございますとおり、電子署名を付すために必要となる電子証明書を発行する認証業務につきまして、一定の基準に適合するものを認定するスキームというものが規定されているところでございます。

3 ページ目をごらんください。上の部分でございますが、リアルの世界では、文書に本人の署名または押印があるときには、その文書は真正に成立したものであるということで推定をされており、下の部分でございますが、電磁的記録につきましても、電子署名法によりまして、本人による電子署名が行われているときは、真正に成立したものと推定するということが規定されているところでございます。

4 ページ目をごらんください。電子署名法に基づきまして、認定をされている認証事業者の一覧でございます。現在、8 事業者 11 業務が認定をされているところでございます。

5 ページ目は、電子証明書の発行枚数の推移でございます。ここ数年は三十数万枚ということで推移をしております。現在の主な用途は、国や地方公共団体への電子申請とか届け出といったものに使われているものかと承知しております。例えば、電子証明書につきましては、有効期間が1年で1万円とか1万数千円、有効期間5年の場合は5万数千円、こういった形で発行されているところでございます。

6 ページからは、タイムスタンプの概要でございます。タイムスタンプにつきましては、電子データにつきまして、その時刻にデータが存在したこと、それから、その時点から現在に至るまで、データが改ざんされていないことを証明するための仕組みでございます。

これにつきましては、その下にございますけれども、領収書等の国税関係書類の保存に当たりまして、紙ではなくてスキャナーとかカメラで撮影したデータを、タイムスタンプを付すということを要件として保存するということが認められております。こういったことによりまして、かなり利用が進んでおりまして、平成30年の1月から6月の発行件数でも1億枚を超えているという状況になっております。このタイムスタンプにつきましては、例えば1,000スタンプまで8,000円というような形でのサービス提供が行われ

ているところでございます。

7ページ目でございます。このタイムスタンプにつきましては、法律に基づく制度ということではございませんで、総務省による指針というものを踏まえまして、一般財団法人日本データ通信協会におきまして、タイムビジネス信頼・安心認定制度というものを運用しているところでございます。この民間の制度に基づきまして、一定の要件を満たすタイムビジネスの事業者につきまして、認定をされているというスキームとなっております。

8ページ目が、認定されている事業者の一覧でございまして、茶色く色を塗られているほうが、実際のタイムスタンプのサービスを提供している事業者でございまして、現在7つの事業者がございまして、上の青いほうが、その事業者に対して正確な時刻を配信したり、あるいは監査を行っている事業者でございまして、こちらが2事業者認定をされているところでございます。

それから、9ページ目でございますが、サーバ証明書につきましても資料をつけてございます。ウェブサーバにつきましては、ウェブサーバが正当なものであるかを判断するために、サーバ証明書というものが用いられてございます。よくブラウザで鍵のマークが表示されているのをごらんになったことがあるかと思いますが、この鍵のマークが表示されている場合には、相手のウェブサーバがきちんとサーバ証明書を使っているということが確認されているということになっております。

このサーバ証明書につきましては、10ページ目でございますけれども、米国の認証事業者ですとか、あるいはアップル、グーグル、マイクロソフト、Mozillaといったようなウェブブラウザのベンダー等から構成されるCA/Browser Forumというものがございまして、こちらのフォーラムにおきましてサーバ証明書を発行する認証局の要件について定めてございまして、この要件がデファクトスタンダードということになっております。したがって、例えば日本のウェブサーバにおきましても、このCA/Browser Forumが定める要件を満たす認証局が発行しているサーバ証明書を利用しているということになっております。

他方で、一番下の※に書いておりますけれども、EUでは、eIDAS規則に基づきまして、信頼できる認証局をトラストリストという形でリスト化してございまして、このリストに掲載されている認証局は、CA/Browser Forumにおいても要件を満たすものとして扱われるということになっております。こうした点につきましても、日本としても考えるべき点があるのではないかとということが論点になるかと思っております。今、電子署名

とタイムスタンプ、それからサーバ証明書についてのみ取り上げさせていただきましたけれども、EUのeIDAS規則と比べて、日本としてどういった点について考えていかなければいけないかというところにつきまして、ぜひご議論をいただきたいと思っております。

事務局からは以上でございます。

【宍戸座長】 ご説明ありがとうございました。

それでは、引き続きまして、資料2、「国際連携を踏まえたトラストサービスとトラスト基盤」につきまして、手塚構成員のほうからご報告をよろしくお願いいたします。

【手塚構成員】 ただいまご紹介にあずかりました、手塚でございます。それでは、資料2に基づきまして、ご説明をさせていただきます。

まずページをめくっていただきまして、先ほど事務局のほうからも、トラストサービスについての概要ということでお話いただいたわけでございますけれども、さらにちょっとそれを具体的に、もう少しかみ砕いてご説明させていただければと思っております。

まずページにつきましては、EUの状況ということで、3ページでございます。eIDAS規則というものがございまして、これは2014年9月から発効されているものでございます。eIDASという命名は、真ん中に書いております、Electronic Identification, Authentication and Signature Regulationということで、この赤い部分の頭文字を取ってきていると。最初のeIDは、まさにIDのエレクトロニック化、それとAuthenticationは認証、それとSignatureは署名、こういうものの規則ができ上がってきているということでございます。

その目的としましては、やはりEU域内にございます28カ国に対するデジタルシングルマーケットというふうに呼ばれている、デジタル単一市場の発展、安心・安全、こういうことを実現していく基盤を位置づけてきているものようでございます。

続きまして、次のページでございますが、日本でも電子署名法というものができ、そこからタイムスタンプ、こういうものなどで、かなりデジタルな基盤の安全・安心は実現してきているということを思っておりますが、EUにおきましては、一方では電子署名法の指令、Directiveから、さらに厳しいRegulationということで、さらには署名、認証、タイムスタンプ、こういうものも一括して1つの法体系に入れて動いてきているというのが、4ページで示しているものでございます。

続きまして、5ページでございます。eIDAS規則とトラストサービスというふうに

呼んでいるものの関係でございます。ここの図にございますように、二重の輪になっておりますが、まず一重目の輪に、例えばでございますが、一番左斜めのところでeSignatureという文言。それと、それに相対側でeTime-stamp。さらには先ほど事務局のほうからお話がありました、ウェブサイトのAuthentication、eDelivery、さらにはeSeal、こういうものが基本的な構成としてトラストサービスというものを構成しています。その周りの輪、これがそれらを活用してでき上がったさまざまなサービスを表現している、アプリケーションを表現しているということで、こういうトラスト基盤の上にサービスを形成していくという考え方で、それも法体系のもとできちっと整備していくという考え方が出てきているということでございます。

続きまして、次のページでございますが、ヨーロッパというのは、監査関係が非常にしっかりしているということでございます。サーティフィケーションの世界です。それをこれは書いてございまして、EU委員会からeIDAS規則まで、縦列にずっと見ていきますと、そのもとで各国の国家監督機関があり、そこで適合性評価機関があつて、それでトラストサービス、プロバイダー、こういうところをサーティフィケーションしていくという縦列の関係。さらにそれを評価する体制というものがしっかりとでき上がってきているというところを示してございます。

では続きまして、一方、日本の状況がどうかという点でございますけれども、わかりやすく書いたつもりでございますが、日本の場合はEUのeIDAS規則と対峙して見ていきますと、マイナンバー制度があり、eIDASのところではマイナンバー、Aとして電子利用者証明、それとSとして電子署名ということで、EU側と基本的な機能群としては、もう日本側もそろってきているというところは言えるかと思えます。これを制度としてどういうふうに体系化していくかという点で、考えるべきところがまだあるのかなという認識をさせていただきます。

次のページにいきまして9ページですけれども、EUの場合はeIDAS規則ということで1本の法律体系で、こういう安心・安全な環境を整備してきておるわけですが、日本の場合は、公的個人認証サービスというものと電子署名法という2つの法律体系で、基本的なところは組まれてきていると思っております。特に電子署名法につきましては、署名というレベルで、電子認証については、まだ基本的に制度としてはない状況だというふうに、私として認識しておりまして、この辺を今後どうしていくかというのは、論点項目かなというふうに思っております。

それに対しまして、公的個人認証のほうは、両方ともしっかりとでき上がって、もう動いているというふうな認識でございます。

続きまして、eIDAS規則のほうでも、法人系の話がございますので、個人に対して、法人のほうはどうかという点でございますが、これにつきましては、まず商業登記に基づく電子認証制度ということでもう稼働しておりまして、それが10ページに書かれているような内容でございます。

その構成図でございますけれども、11ページのところにございまして、法人の代表者、取締役クラスでございますが、その方たちに対しての電子証明書というものを発行し、企業と政府、または企業間での電子情報の署名をつけたやりとりというところが実現できているところでございます。

続きまして、12ページでございますが、ここで1つ論点になるのかなと思って、当時書いたものでございますが、特にまず(A)のほうでは、公的個人認証サービスと電子署名法の違いという点で、ポツ1のところ、公的個人認証サービスは、電子署名と電子認証両方を既に実現している。それに対して、電子署名法のほうは、法律の名のとおり、認証については入っていないという状況でございます。

それに対しまして(B)のほうは、今度は法人に対してでございますが、それは下の図を見ていただきますと、ブルーの部分について、まだうまく対応していないというところがございまして、これにつきましては、次のページでございますが、総務省さんのほうで、電子委任状法というものをつくっていただきまして、これで青い部分もカバーするというところで、一応個人の自然人と法人に対する体系というのは、署名に関しては整ってきているのかなと思っております。

それを図で示したものが14ページでございますが、簡単に申し上げますと、左下の法人A社員が契約相手方の法人Bとの間で契約行為をするときに、例えば法人Aが署名をしてきた場合、法人Aの属性の中の資格が、ほんとうにこの契約でやる権利とございますか、その企業での資格を持っているのかというところでございます。それをその上の法人Aの社長が電子委任状ということで、法律で定められた電子委任状取扱事業者というところにこの情報をお送りしまして、それで下の法人Aと契約相手方法人Bがやりとりするときに来た証明書の資格を、電子委任状取扱事業者に聞くことにより確認をとるということで、正しくトラストチェーンがつながっているということがわかるという法律でございまして、これによって法人の取締役以外の一般社員でも、実現できる環境をつくってきているとこ

ろでございます。

15ページでございます。そういうことから、我が国とEUの比較をざくっとしております。細かい点ではいろいろご議論あるかと思いますが、鳥瞰的に見ますと、まず機能としては、電子署名（個人）、電子認証（個人）、タイムスタンプ、法人格、一般にLegal Entity。これはヨーロッパではeSealというものがございます。それと電子署名の法人、電子署名の認証というふうに分類をしてございますが、このときに丸のついたところが、各法律ないしは制度で満たしているところというふうに見えてきております。そういうことから、論点としてはeIDASに対する我が国のサイドの丸のあるなしについて、検討する必要があるのかなというふうに思っております。

そういうものが、実際どういうところで使われるんだろうというところで書いてございまして、今、政府のほうが中心になって、Society5.0というものが強く打ち出されている中で、プラットフォームのところで活用していくというのが考えられるのではないかと。特にデータベースドリブンのアーキテクチャでございますので、データに対するアクセス並びにデータのインテグリティというものをきちっと保証していかないといけないと。アクセスということは、個人でアクセスする、法人でアクセスするということが出てまいりますので、まさにそれと、それらのデータの完全性を保証するために署名等の行為をして、データをやりとり、データの流通を安心・安全に行うという環境が必要ではないかということでございます。

その次のページでございますけれども、これはセキュアデータ共有活用基盤ということを書かせていただいておりますが、APIインターフェースを提供するというお話は既に出ておるわけですが、APIにアクセスするアクセス制御のところ非常に重要になってくると。誰でもアクセスしていいというわけではなく、しかるべき人が資格を持ってアクセスすることが大事ですので、まさに今ご議論している基盤を活用して、その安心・安全な環境を実現していくということになるかと思っております。

19ページでございますが、それを簡単に示したものでございます。A社、B社とか、または個人でもよろしいわけですが、左側がエンドエンティティを表現してございます。まずはAuthenticationということで認証をします。さらにAuthorization、これは属性認証といいますか、属性の資格を確認するというレベルでございます。それが初めて通ってAPIにたどり着くという基盤の構成です。こういう機能群を、やはりSociety5.0の中にも埋め込んでいくと。そのために、まさに今回議論しているトラストサービスの考え方を

反映していく必要があるのではないかというふうに考えてございます。

続きまして、最後でございますが、21ページ、トラストサービスの国際連携構想ということで書かせていただいております。これは日本、我が国とEU、またさらには同じように経済圏として米国、こういうものと国際連携を図るということは、今後のEPA等を含めて考えていきますと、デジタルエコノミーの国際的なつながりという点で、非常に重要なテーマに今後なっていくだろうというふうに思っております。そのための先行的な活動として、民間側で、このEUとアメリカとの連携について、考え方、メソドロジーというものをしっかりと組み立てていこうということで、活動をこの10月にちょっと立ち上げたものがございまして、そのご紹介にもなっております。

最後のページでございますけれども、そのメンバー構成として、International Mutual Recognition Technical WGということで、通称IMRT-WGと呼んでおりますが、これを立ち上げまして、10月末のとき、ベルリンでEU、さらに米国側は電話会議で入っていただきまして、ここに書いてございますようなメンバーで動きを始めたというところでございます。

そういうことから、最後全体を通してでございますけれども、トラストサービスというのは、まさに今、非常に国際的にも重要なテーマとなってきておりますので、この研究会でぜひ論点整理をしていただいて、我が国の発展に貢献できればというふうに思っております。以上でございます。

【宋戸座長】 手塚構成員、ありがとうございます。

それでは、事務局及び手塚構成員からのトラストサービスに関するご発表につきまして、ご質問、ご意見などございましたらどこからでもお願いしたいと思っておりますが、いかがでございでしょうか。森構成員、お願いいたします。

【森構成員】 ご説明をいただきましてありがとうございます。大変わかりやすくご説明いただきまして、私も知らないことが多かったんですけども、大変勉強になりました。

知らないことの延長ですけども、手塚先生のご説明で、資料2の12ページと14ページのところに、法人の社員の権限を委任状で認証するというものがあるんですけども、これがちょっとリアルに考えた場合に、あまり法人の従業員が委任状を持って契約をしに行くということがないかと思っておりますので、実態的におそらくこれは委任状のかわりではなく、何か別のもの、身分証明みたいなものなのかもしれないなと思っているんですけど

も、ちょっとリアルで委任状がないこととの何か整合性のご説明がもしありましたら、教えていただきたいと思います。よろしく申し上げます。

【手塚構成員】 ただいまのご質問の委任状の部分でございますけれども、ここの基本的な考え方は、例えばA社の社員がいて、その社員が一体契約がどこまでできるのかとか、契約範囲とか、そういうのが一般企業の中では当然でございます。つまり、わかりやすく言うと社長から委任を受けているという構成で、当然なるわけでございますけれども、そこをどういうふうに電子の世界で実際実現するかということになりまして、それを何々社員は契約金ここまで、こういう範囲のというスコープを明確にしたものを、企業側で書いていただいて、それに社長印を押して、確かにこれは社長が認めたものだということがそれでわかりますので、それを電子委任状取扱事業者のほうにお渡しするというのが一般的な考え方で構成しています。

これをさらにPKI (Public Key Infrastructure) の証明書の世界でも実現で自動化できるように検討もしております、そういう要素もこのところには入ってまして、基本的には電子のやりとりの中で、半オートマティックにできるような仕掛けになるというようなところでございます。

【宍戸座長】 宮内構成員、お願いします。

【宮内構成員】 まず1点、今の件についてコメントさせていただきたいと思います。電子委任状という名前なんですけれども、実現の方法としては、電子証明書に属性を書き込むような形で実現されている例が、今のところ行われています。これは要するに、権限を書くこともできますが、会社への所属ですとか、会社での肩書ですとか、そういうものをここに書くことができると。ですから、例えばいい例はあまりないんですけれども、資材部長という肩書があれば、資材の調達について一定の権限が、おそらく使用人の包括的代理権に基づいて認められるわけですね。こういうようなことを書いた電子証明書というのを出すことができると。そうすると、この電子証明書に基づいてサインをすれば、いわば本人印と名刺がセットになってついていくような形でB to Bに使っていけると、こういうことが大体考えられているんです。

ですから、もちろん今直接使われているのは、例えば入札のための権限が与えられた人が、それに基づいて入札書を入れるというのがありますけれども、将来的にはもっと広く、名刺プラスアルファみたいな形でこういった証明書を使っていくことができるのではないかとこのように考えています。これが1つ、使いでのあるものだと思っています。

あと、全然別の点でコメントしておきたいんですけども、まず手塚先生の資料の15ページで、ここに法人の電子署名と法人の電子認証という話がありましたけれども、基本的には法人の電子署名というのはどういう概念なのかという、若干難しいものがありますよね。法人そのものが意思表示をすることは、一応できないという建て付けに、我が国の法律はなっていると思いますので、署名というのは何のためにするのかというのを、少しよく考えておかないといけないと。意思表示は難しいんですけども、発信者の確認ですか、今通信している当事者の確認というのをどうするかという場合に、この法人から出てきたものだとか、そういうものは当然重要なポイントになってくるんですね。

例えばの例ですと、プログラムに署名をつけて出して、これは確かにこの会社が出したプログラムだとか、そういう信用性にかかわる問題にもなってくると。あと通信のためには、先ほど出てきましたTLSのときに使うと、こういうところで使いますので、法人の場合の署名の在り方というのは、多分自然人の意思表示等に考える署名とは、若干意味合いが違ってくるのかなというふうに思っています。これはコメントその2です。

手塚先生に教えていただきたいことが1つありまして、電子署名をやるときに、現在は自分でICカードを持っているとか、秘密鍵を自分のPCに入れておくとかして証明しているんですけども、リモート署名というのが最近よく取り沙汰されてきているんですね。つまり、例えば2,048ビットの鍵を覚えたり持っているというのは結構大変なので、覚えることはできないですけども。こういうものをサーバに預けておいて、そこにログインして証明してもらうという方法、リモート署名というのがありますけれども、これだと結構いろいろ使えると。例えば、認証、ID・パスワードだと簡易ですけども、例えばマイナンバーカードに基づいてログインして、その上で向こうで証明してもらうみたいなこともできると。そうすると、あとの署名は、例えば今の委任状法の署名でも構わない、こういうようなことができると思っっているんですが、このあたりについて、EUの状況と、今、日本での状況をもしご存じでしたら教えていただきたいと思っております。お願いします。

【手塚構成員】 どうもありがとうございます。リモート署名のことはあえてちょっと書かなかったんですが、今ご質問がありましたので言いますと、昨年7月のときにEUのETSIが日本に来て、日本の3つの機関プラス慶応と共同でワークショップを行いました。その3つの機関は、トラストサービス推進フォーラム(TSF)、JT2A(Japan Trust Technology Association)。それともう一つ、JIPDECの3つの機関

と、プラス私のところの慶応ということでやったんですが、そのときにEU側も既にリモート署名については検討しておりまして、そこで初めて意見交換したんですけども、日本と大体同じぐらいの足並みで、今、動いてきていると。

リモート署名というのは、まさにクラウドができたときに、クラウド上で全部本人の鍵も置いて、それでクラウドに入るところの電子認証、ここをしっかりと確実にやれば、あとはその延長で署名行為もしていいだろうということで考えがまとまってきているのがリモート署名でございます。これをやると、要するに秘密鍵のデリバリーという、非常に運用の大変なところがなくなるということで、結構今、ヨーロッパのほうでも広がってきていまして、クラウド署名コンソーシアムというのが立ち上がって動いてきています。これは署名の行為が入り、認証の行為も入ってくる。

認証のところはどうするかというと、フィンテック系でいうと大体2ファクターオーセンティケーションなどを使って入っていくと。でも、我が国においては、公的個人認証の認証がございますので、一発でぼんといけるということで、非常に今、日本はむしろいい立場にあるのではないかというふうに思っているところです。

このリモート署名については、ぜひこういう考え方の中で、日本もまさにそこをガイドラインとして、先ほどの3つの機関等とも相談しながら進めておりますので、状況としてはそんなところで、大体足並みがそろってきているところでございます。

【宍戸座長】 ありがとうございます。まだご質問、ご意見等あろうかと思いますが、時間の関係上、次の議事のほうに移らせていただきたいと思います。

前回会合で事務局よりご説明がありました、本研究会の検討アジェンダ（案）につきましては、第1回会合で構成員の皆様からいただきましたご意見を踏まえ、お手元資料3-1の形で提案募集を実施させていただきました。本日は事務局から、提案募集の結果などについてご説明のほうをお願いいたします。

【岡本消費者行政第二課企画官】 資料3-2についてご説明申し上げます。1ページをごらんください。本提案募集は、第1回研究会の翌々日、10月20日から31日までの12日間行ったものとなります。提案募集の対象及び結果はごらんとおりとなります。

2ページ目にお進みください。こちら以降は、資料3-1のアジェンダ（案）のほうに提出された意見を記載しているものとなります。その順で、提出された意見を記載しているものとなります。

まず、今般の検討を行う背景部分についてでございます。1ポツ目、通信の秘密やプラ

イバシー保護について、事業者の分類、設備の設置場所によらず、公平・公正な競争環境の検討を望む。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、同じように取り扱われることが必要。今後、IoT等のさまざまなビジネスモデルの検討を進めていく中で、利用者の立場から見てどこまでが実施可能で、どこまでが問題となり得るのか、線引きが必ずしも明確でないケースがあらわれると。これを踏まえ、健全なグローバル競争やイノベーション促進を達成するため、規制ありきではなく、事業者の自主的な取り組みを後押しするような検討が重要としております。

2 ポツ目です。GAFMAとどう対峙していくべきかについて、状況によっては諸外国政府・民間機関などとの協調・連携の道を探ることも選択肢である。

3 ポツ目です。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、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。

4 ポツ目です。過剰規制とならないように配慮するとともに、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り扱い、その他制度面の扱いについて、イコールフットイングの確保を重視すべきとしております。3 ページにお進みください。

今般の検討を行う背景部分が続いております。Society5.0を実現するためには、流通するデータの信頼性を誰もが認識できる仕組みが必要。課題抽出・対応の在り方を国家レベルで検討することは有意義としております。4 ページにお進みください。

分析のための射程についてです。1 ポツ目、プラットフォームは多種多様であり、ひとくくりに議論することは難しいことから、個別のビジネスモデルの違いに配慮した議論が必要としております。

2 ポツ目。プラットフォーム事業者と電気通信事業者を比較して検討を行うことは、両者のサービスと適用規律の違いが明らかとなり、利用者及び事業者双方にとって有意義としております。5 ページにお進みください。

その他、範囲の捉え方として考慮すべき事項についてです。プラットフォームの利用者にとってのプラットフォームの役割や、事業者による利用者保護に対する自主的な取り組みについても十分理解した上で検討すべき。すなわち、各プラットフォーム事業者は利用者保護関連法令の遵守のみならず、独自の利用者保護対策に努めているとして、ごらんの対策例が挙げられております。6 ページにお進みください。

保護すべき利用者情報の分類や比較についてです。1ポツ目です。プラットフォーム事業者に対し、通信の秘密・プライバシー保護を求めることには反対。電気通信事業者に対して、ユーザーの選択と透明性を尊重しつつ、個別具体的にデータ利活用を認めることができないかを検討すべき。

2ポツ目です。利用者情報を分類することで、取得情報や規律の適用が整理され、周知されることにより、利用者が安心してサービスを利用できることは、事業者にとって望ましい。

3ポツ目です。通信の秘密の保護法益を、単なる利用者のプライバシー保護としてのみ捉えるのではなく、通信路上で恣意的に干渉・介入されないという意味で、電気通信に対する社会的信頼の確保として捉えるべき。

4ポツ目です。※、その下の部分に書いておりますけれども、この部分につきまして、事業者間の円滑な協調や公平・公正な競争が可能となるように、通信の秘密・プライバシー保護の在り方を検討するべきとしております。7ページにお進みください。

利用者情報の保護の対象範囲等についてです。ネットワーク効果により、利用者情報を収集・蓄積するインセンティブが働くとされているとはいえ、必ずしも利用者情報の収集・蓄積に走るわけではない。事業者自身によるプライバシー保護の具体的な取組をも念頭に置いた上で検討すべきとしております。8ページにお進みください。

利用者情報の分類及び範囲に関して、その他考慮すべき事項についてです。1ポツ目です。実質的に保護すべき利用者情報の範囲を検討すべき。一律に硬直的な規律を適用するのではなく、柔軟な規律の在り方が考慮されるべき。

2ポツ目です。利用者情報を取り扱う国内外事業者の活動において、利用者利益保護の実現が確保されるべき。

3ポツ目です。通信内容と通信の構成要素のいずれにも通信の秘密の保障が及ぶことに異論はないものの、それぞれの規制のレベルを同じとする必要はないとしております。9ページにお進みください。

国際的な制度的調和についてです。1ポツ目です。国内と国際と二重の対応を求められることは好ましくないが、日本の実情に合わせたルールとなることが望ましい。

2ポツ目です。単に国内法に比して厳格な各国法の規制に追従することの要否だけではなく、国内法と各国法の差分について、その合理性も含め議論することが望ましいとしております。10ページにお進みください。

法令の適用、運用・執行上の差異についてです。1ポツ目です。海外の事業者によるウェブメールなどに通信の秘密が適用されていないのは、消費者保護の観点から問題。

2ポツ目です。事業者間の公平性の観点から、同一のサービスに対して同一の規律が適用されるべき。仮に海外事業者に対し、国内法規の適用が困難な場合でも、そのサービスに適用される規律については、利用者が理解しやすい説明・表記を求める等とすることが必要としております。11ページにお進みください。

法令の適用、運用・執行の在り方における国際協調の在り方についてです。欧米で、クッキーなどデバイスやアプリケーションの識別子を保護対象とするかどうかの該当性を幅広く取り、処理や取引の対応によって規制の強弱を変えるアプローチが見られるが、我が国でもこのようなアプローチがとられれば、データの処理や移転の実態に即した対応が可能となることから、検討をお願いしたいとしております。12ページにお進みください。

法令の適用、運用・執行や国際協調のその他考慮すべき事項についてです。1ポツ目です。通信の秘密の取得等に当たる行為の主体が、電気通信事業者であるか否かによって、侵害の該当性の評価が変わらないように運用されるべき。

2ポツ目です。EU、米国ともに不適當な行為があった事業者等に対し、当局が大きなサンクションを課す一方、日本はデータ保護領域での当局からのサンクションは極めて限定的であることから、積極的な執行を行うべき。それを前提として、共同規制の枠組みを導入し、事業者団体のガイドラインを遵守する加盟事業者に対して、執行の猶予や緩和の措置をとることで、業界ごとの特性に合わせたルールを機能させられると期待としております。13ページにお進みください。

ここからはトラストサービス等の在り方ですけれども、1つ目といたしまして、ID連携・データ共有・活用の促進についてです。1ポツ目です。ID連携は重要なツールであることから、特定の事業者が市場支配力を濫用することがないようなルールが検討されることが望ましい。

2ポツ目です。送信者の意思表示の際には、電子署名のほうが手書き署名より信頼性が高く、行政、訴訟、医療サービスのオンライン提供の可能性を開く。

3ポツ目です。多様な事業者によるID連携、データ共有・活用の促進するための環境整備が必要としております。14ページにお進みください。

トラストサービスの在り方全般についてです。1ポツ目です。電子データを海外と取引するに当たり、同データの信頼性について、各国独自ではなく相互運用されるべきで、海

外との相互運用性を追求・整備する必要がある。

2 ポツ目です。国際的に通用する日本のトラストサービス創出のため、国際的視野による包括的な検討を行うことが必要。

3 ポツ目です。国際的サービスの進展を視野に入れ、相互運用性確保を目指さなければ、これは分野は異なりますが、GDPRに係る日・EU交渉のようなそういった交渉に不利益をもたらすとしております。

4 ポツ目です。正当性の確認や認証にとどまらず、完全性を担保する仕組みを検討することが必要。

5 ポツ目です。機微情報を取り扱う行政機関及び重要インフラ事業者並びに防衛産業について、情報システムの利用者認証と検証の仕組み等について、リスクに応じた技術基準に適合したトラストサービスの利用を義務づけることが必要。

6 ポツ目です。信頼性が確保されたトラストサービスを公開する仕組みが必要。すなわち、アプリケーションサービス自体の信頼性評価の仕組みの確立が重要。

7 ポツ目です。電子署名のみならず、利用者証明の信頼性を評価する仕組みを法的にオーソライズする規定を追加すべきとしております。15 ページ目にお進みください。

トラストサービスの利用者認証についてです。1 ポツ目です。国際的なサービスの進展を視野に入れた相互運用性確保に向けて、日本においても規律・ガイドラインの検討が必要。

2 ポツ目です。本人のみが知るID・パスワードなどによる認証、このリスクを正しくユーザーが理解して利用できるための仕組みを検討する必要がある。

3 ポツ目です。eIDASと同様、利用者認証を検討し、電子署名法の改正まで視野に入れるべき。16 ページにお進みください。

トラストサービスのタイムスタンプについてです。1 ポツ目です。日本でも、eIDASに相当するタイムスタンプを含むトラストサービスに関する法制化が必要。

2 ポツ目です。海外での法的根拠のあるタイムスタンプとの相互認証を今後認められるところ、現在の認定制度における信頼時刻を利用したタイムスタンプを法的に利用価値があるものと認めることを検討する必要がある。

3 ポツ目です。国内のみならず、国際でもタイムスタンプを信頼性・正当性あるものとして通用させる裏づけとして、法制化は必要。

4 ポツ目です。EUでは法体系として整備されているが、日本ではガイドラインどまり

であり、国際間データ取引で対等な関係とはなり得ないのではないかとしております。17ページにお進みください。

トラストサービスの法人認証についてです。1ポツ目です。どのようなシーンで、いかなる認証レベルで求められるか。それを国際的にどう担保するか、法人認証で何を行うか、そのためにどんな手段を、どんな技術基準に基づき実装するか。

2ポツ目です。日本におけるトラストサービスとして、法人の意思表示ではない、電子角印としての定義、規定を検討する必要がある。

3ポツ目です。インターネットを通じた取引において、会社銀行印や角印（社印）に対応した、法人による電子署名の在り方を検討すべき。

4ポツ目です。ソフトウェアに対するコードサイン証明書を利用した、法人が作成した根源性を証明する場面が増加しており、これが検討されるべき。

次に、その下に移りまして、トラストサービスのサーバ証明書についてです。1ポツ目です。制度化の検討は有意義だけど、過度の負担、不便も強いることにならない制度となることを望む。

2つ目です。eIDASと異なり、日本では制度がなく、結果、政府認証基盤の発行するサーバ証明書が海外の任意団体から許容されないなど、影響が甚大であり、制度を検討すべきとしております。18ページにお進みください。

トラストサービスのその他についてです。1ポツ目です。トラストサービスについて知りたい、導入したいと思う人々がよりどころとなるポータルサイトの構築を検討いただきたい。

2つ目です。eIDASにおけるトラステッドリストの仕組みを構築し、EUのトラステッドリストとの相互認証ができる制度を早期に構築する必要がある。また、リモート署名をトラストサービスの1つとして要件定義を検討する必要がある。

3ポツ目です。IoT時代を迎え、機器認証に関しても検討すべきとしております。最後のページでございますが、19ページにお進みください。

その他として、オンライン上のフェイクニュースや偽情報への対応についてです。1ポツ目です。データローカライゼーション、規制撤廃、個人データ保護ルールの調和、日米の主導的役割を通じたグローバルな制度の構築と調和に取り組むべき。

2ポツ目です。フェイクニュースや偽情報への対応についての検討は有意義。利用者が意識してリテラシー向上に努めることについて、誰がどのように支援できるのか、または

すべきかといった検討が有効ではないか。

3 ポツ目です。ターゲティング広告に係る通信の利用は、通信の構成要素のみを利用するものであり、ソフトローにより適正化される余地がある。また、情報リスクの一翼を担うメディアの存否にかかわる点も考慮すべき。

4 ポツ目です。災害時のデマ拡散対策として、行政の把握している情報を即時に開示するプラットフォームがあれば、これを積極的に活用することで自浄作用が働くのではないか。

5 ポツ目、最後でございますが、プラットフォームによる利用者、加盟店、提携先への規約の押しつけ、顧客データの利用方法の不透明性、国外プラットフォームが国内で法人税を払っていないこと。プラットフォームとしての立場とプレイヤーとしての立場の二面性からくる利益相反についての検討が必要としております。

資料3-2は以上でございますが、資料3-3は、前回研究会で構成員の皆様からいただいたご意見をまとめたものとなります。ご説明は以上でございます。

【宋戸座長】 ありがとうございます。

それでは、提案募集に寄せられた意見をごらんいただきながら、また資料3-3もご確認いただきながらでございますが、お手元資料3-1、本研究会の検討アジェンダ（案）に反映すべき点などについて、ご意見をお寄せいただければと思います。どこからでもよろしいですが、いかがでございましょうか。新保先生。

【新保座長代理】 慶應義塾大学の新保です。今回の意見募集の結果を拝見いたしました。各項目、非常に細かくさまざまな意見が提出されています。とりわけ国内と国際的な取り組みについては、国内事業者と国外の事業者との執行の差も踏まえてさまざまな意見が提出されているところでありますけれども、少々意外に思ったのは、9ページの、提出された意見なしの国際的なプライバシー保護との潮流との制度的調和として考慮すべき事項。この点については、今回のまさにプラットフォームサービスに関する研究会という趣旨からしますと、非常に重要な論点である一方で、やはりこの点が、特に今回の意見募集の主な法人または団体として、事業者の方を中心に、一部団体などもございますけれども、制度的な観点からの問題については、特に意見がなかったのだと思いますので、私から2点、この点について、特に意見がないということでしたら、私から意見を述べさせていただきたいと思います。

2点何があるかといいますと、日本の現在の立ち位置から考えたときに、国際的な制度

的調和との関係で、今後、取組が必要、今まで取組をしてきておりますけれども、今後この観点から考えた場合に、プラットフォームサービスに関する事業者への対応という観点からすると2つあるかと思えます。1つは、2013年に改正されたOECDプライバシーガイドラインとの関係。もう一つは、欧州評議会の個人データ自動処理に係る個人の保護に関する、EU108号条約との関係における問題、この2つは避けて通ることができない問題であると考えております。

とりわけ2013年に改正されたOECDプライバシーガイドラインは、我が国の個人情報保護制度の基調となっている、1980年のガイドラインを改正したものでありますけれども、このガイドラインの本体には触れられておりませんが、私がこの改正過程では、OECDでは当時、SPDEの副議長を担当させていただいておりましたので、そのときのポイントとして、プラットフォームについての言及がございます。

ここでは、OECDプライバシーガイドラインの改正過程におけるポイントとして、マルチポイントかつ継続的なデータ流通を可能にする通信ネットワーク及びプラットフォームに支えられた個人データの国際的な利用可能性、これを基調として、OECDプライバシーガイドラインの改正を行うということが、副議長の集まりのビューロのミーティングで調整がなされた結果、最終的にはガイドラインの8原則を改正するということにはならなかったという経緯がございます。

つまり、各国、通信ネットワーク及びプラットフォームに支えられた個人データの国際的な自由な流通と保護を基調として、OECDのプライバシー8原則を基調とした制度が既にでき上がっているという観点からしますと、この点については、特に変更せずに、今後さらにさまざまな取り組みを行うことができるであろうということになったわけであります。

したがって、今後、2013年に改正されたOECDプライバシーガイドラインは、我が国におきましては、とりわけ総務省の検討会でも行われております、AIにおける研究開発及び利用における開発、あと開発原則と利用における原則なども踏まえて、もともとこういったOECDにおける取組。それから、今後はこの部分についてもOECDに提案をしていくという現状からいたしますと、1点目については、2013年のOECDプライバシーガイドラインという観点からの国際的な制度的調和というものは不可欠であろうと考えられます。

もう一つが、欧州評議会の108号条約です。こちらにつきましては、一見すると皆さ

んから誤解されがちなものであります。欧州評議会というEUの機関でありますけれども、我が国もオブザーバー参加をしております、EUの条約第108号諮問委員会につきましては、我が国も個人情報保護委員会がオブザーバーとして参加しております。これは昨年の5月から参加をしているわけでありまして、この点について、今後の動向としては、108号条約の改正というものが、GDPRが既に適用開始しておりますので、規則とかクッキー規制などもありますけれども、今後我が国に直接影響してくるものとしては、108号条約との関係における問題は避けては通れないだろうと。

OECDガイドラインと108号条約の違いは、ひとえにいうと法的拘束力であります。OECDガイドラインは、あくまでOECD加盟国が守るべきガイドラインとして提示されますけれども、108号条約は法的な拘束力を有する条約として締結されますので、今後、この点については非常に大きな点であると。とりわけ108号条約の特徴としては、諮問機関を通じた多国間の協力プラットフォームという、これは別の意味でのプラットフォームですけれども、その整備を目的としていることが、この108号条約の趣旨でありますので、今後、この2つの観点から、今回意見がなかった国際的なプライバシーと保護の潮流の制度的調和という観点からの取組が必要であると考えております。以上であります。

【宍戸座長】 ありがとうございました。

ほかにご意見等ございますでしょうか。いかがでしょうか。どこからでも結構ですが。森構成員、お願いします。

【森構成員】 感想のようなことでまことに申しわけないんですが、ほんとうにいろいろなご意見をいただいている、全く鋭くポイントを突いたものとか、全くそのとおりでと思うものと、共感できないものも若干あったということですが、私がこれと思ったものをちょっと申し上げておきますと、8ページ目の、特に個人の方の意見で大変これは鋭いなと思ったところが何点かございました。

8ページ目の一番下のポツですけれども、プラットフォーム事業者が収集・蓄積する利用者情報の保護の対象範囲ということについてのご意見ですけれども、通信内容と通信の構成要素のいずれも通信の秘密の保障が及ぶことに異論はないものの、それぞれの規制のレベルを同じとする必要はない。通信内容の秘密の侵害と通信の構成要素の秘密の侵害との間に差異があることを、市民も事業者も感覚として持っていることから、峻別して議論すべきというご意見がありまして、これは私も共感するところです。

一方で、さはさりながらということなんですけれども、同種の意見が、失礼しました、ちょっと同種の意見ということではないですが、12ページをごらんいただきまして、こちらは法令の執行・運用の在り方というところなんですけれども、これも全く同じような通秘に関するのですが、意見が2つありますけれども、2つとも大変重要なご意見かなと思っ
ていまして、前半部分は、下線部ですけれども、通信の秘密の知得等に当たる行為の主体が電気通信事業者であるか否かによって「通信の秘密の侵害」の該当性の評価が変わらないように運用されるべきと。これは法文上当たり前のことではあるんですけれども、法文上全くそのように書かれているのでそうであるべきなんです、やはりそれがほんとうにきちんと実現されていないとだめであると。通信の秘密を侵害するのは、通信事業者だけではなくて、何人も侵害してはいけませんということになっていますので、そのように運用されなければいけないと思います。

2ポツ目ですけれども、こちらも個人のご意見ですが、法執行のことです。下線部ですが、EU、米国ともに不適當な行為があった事業者等に対し、当局が大きなサンクションを課すことで、事業者における事前の対応を促進している。一方、日本においてはデータ保護領域での当局からのサンクションは極めて限定的であり、より積極的な執行を行うべきであるということなんですけれども、以前はそうだったかもしれませんが、先々週、フェイスブックに対する個人情報保護委員会の行政指導ということが広く報道されていました。これは全くの快挙だと思いますし、このようにしっかりと法執行を進めていただきたいなと思います。

そういったしっかりした法執行前提での後半部分の、積極的な法執行を前提として、共同規制の枠組みを導入する。そして、様子を見るということもイノベーションとの関係では重要だなと思いますので、この2番目のご意見は大変重要なご意見だろうと思いました。以上です。

【宍戸座長】 森構成員、ありがとうございます。

ほかにご意見いかがでございましょうか。木村構成員、お願いいたします。

【木村構成員】 ご説明ありがとうございます。全体を通して思ったのは、利活用はいろいろと考えるべきではないという意見がいっぱいありましたが、利用者として不安になるのは、データの管理ですとか保存についてどういうふうに日本はしていくのかというところまで、私は検討が必要だと思います。

あともう1点は、事務局の資料の10ページの提出された意見のところなんですけれども、

上の海外の事業者が日本の消費者に対してサービスを提供する場合に、通信の秘密が適用されていないという点について、もう少し詳しく説明をしていただけるとありがたいです。ちょっとよくわからなかったのです。

【宍戸座長】 この点は、まず資料の10ページの1ポツ目の、KDDI株式会社さんから出てきたご意見の部分ですよね。これについて、事務局から少し補足説明をお願いできますか。

【岡本消費者行政第二課企画官】 こちらのほうは、前回の研究会でも少しだけ言及させていただいたと思うんですけども、現在のところ、まず電気通信事業法というものについて、域外適用の規定はございませんということです。ただ、電気通信事業法の考え方として、設備を根拠として規律をするということでもありますので、現在の運用といたしましては、例えば外国に設備があるとして、ただ、日本の会社の機関のほうから実質的に設備を支配、管理するというふうな場面であれば、実際には適用は考えられるというふうにしておりますけれども、ただ、完全に設備が外国にあって、そこに対して支配、管理というものをするような者が日本にいないとなりますと、現在のところは電気通信事業法の規定の適用がないというふうなことをご説明申し上げたものでございます。それをおそらく念頭に置いたご意見であると理解しております。

【宍戸座長】 木村構成員、それでいかがですか。

【木村構成員】 そのことは理解しているのですが、例えばウェブメールなどと書いてあるんですけども、海外の事業者さんを利用してかなりの量のウェブメールが利用されていると思うのですが、それもやはり適用されていないと考えてよろしいのですか。

【岡本消費者行政第二課企画官】 そのような理解でおります。

【宍戸座長】 確認ですけれども、海外事業者が日本の利用者に提供するウェブメールであって、電気通信設備が日本国内にない。そして、日本の側から電気通信設備についてコントロールする、そういう事業者の拠点のようなものが日本国内にない。まず基本的にそういう場合ですけれども、海外事業者の提供するサービス一般にそうで、通信の秘密の保障が及んでいないというわけではないんですけども、今のような条件がかかっているもの、そして特定のサービス名は申し上げませんが、広く使われているサービスの中には、まさに通信の秘密の規律が電気通信事業法上、及んでいないものがあると、そういう整理だと思います。

【木村構成員】 わかりました。ありがとうございます。

【宍戸座長】 ほかにいかがでございますか。大谷構成員、お願いします。

【大谷構成員】 ありがとうございます。さまざまな角度からのご意見をいただきましたので、日ごろあまり考えていないことも含めて、いろいろヒントをいただけたと思っております。

もともと事務局のほうでご用意していただいた資料3-1の一番最後に、オンライン上のフェイクニュース等への対応についてどうするかが述べられていました。もともと盛りだくさんのテーマなので、そこまで対応できるのか若干疑問ではありましたが、いただいた意見の中で、資料3-2の19ページにまとめていただいている中に触れられておりましたように、フェイクニュースや偽情報への対応についても、直接それらを規制するというような表現等への規制ではなく、利用者への支援の在り方についての検討ということで、表現の自由などについての謙抑的な姿勢を示していただいたことに、非常に共感を覚えています。そのような視点で、可能な範囲でこのテーマについても議論する必要があるのではないかと感じました。ちょっと感想めいておりますが、それが1点です。

それから、今日の前半でご説明していただいたトラストサービスについてもコメントしたいと思います。実は時間があればご質問したいと思っていたのですが、いわゆるGAF Aと言われているプラットフォーム事業者が、EUのeIDASなどのレギュレーションでどのように規制されていて、それがこういったプラットフォームによる競争力に対して、どのような効果をもたらしているのかということです。どちらかというところ、そういったレギュレーションというよりは、デファクトスタンダードをどんどん構築しながら、可能な範囲で競争力を伸ばしているというふうに見受けられる中で、このような規制というのにどのような効果が発生しているのかといったことについて教えていただきまして、その観点もやはり検討の項目に入れるべきかではないかとも思っております。

もともとトラストサービスについては、日本の海外も含めた取引のインフラとして、きっちり整備していく必要があるテーマだと思いますので、現在足りない点も含めて、体系的に構築し、利用しやすいようにしていくことを期待するものですが、プラットフォーム事業との兼ね合いということでは、どのように見ていくべきなのかということについて、今日ご説明くださった手塚先生等からコメントいただければと思っております。

【手塚構成員】 よろしいですか、今ご指名いただきましたので。あくまでもこれ、私の私的な意見というふうに聞いていただきたいんですけども。

やはりまず、ネットワークの中で使われて、サービスという視点で捉えたときに、サー

ビスという民間企業ばかりというそんなことはなく、公的なこともございますし、もつというさまざまなやりとりがされるわけですね。一番ハイエンドなデータという、やっぱりナショナルセキュリティのほうになっていくと思うんですけども、そこは今、ちょっと置いて。そうなりますと、今後は公共系の高い、一般的な行政的なもの。これも日本の中では14分野の中の1つ、14インフラ産業という位置づけにもなっているわけですけども、そういう重要インフラ産業のデータというものの取扱い、これが1つ大きくあると思うんです。

さらにいろいろな機軸があるので、きれいに縦方向で全部は言えないと思うんですが、あと個人情報のようなものがあると思います。そういう中で、GAF Aの分野が広がってきて、これは悪いことじゃないんですけども、サービスもよくなるのでいいんですが、その中でEUの視点からこれを見た場合に、EU市民の情報が国外に流れていくということに対してどういうふうに考えるかという点で、どうもEUは、GAF Aのサービスの上位レイヤにトラストサービスという概念を持ち込んだのではないかと。それがまさにレギュレーションを持ってきて、きちっとEUの28カ国でそれなりにコントロールができる世界。そうすると、一番大事なものは、本人確認とか、本人の属性情報とか、サービスを使いますから、そういう情報がみんな必要になるわけですね。そうすると、必ずそれはサービスをやるということは登録をするということにつながりますから、その情報がまさにサービサーのところに登録されていく。そこをトラストサービスというものの世界に持っていくことによって、EU域内で彼らとしてはサービスを完結するというのが、まず大きな1点としてあるのではないかと。それがeIDASのような、きちっとしたEUのレギュレーションのもとででき上がった環境、これが1つ言えると思っています。

そういうことによって構築されていくサービスというのは、やはりGAF Aの世界とは違う本人確認も、ある意味オレオレ確認ではなくて、きちっと国の公的なもので本人を特定した情報に基づいてできる世界という、そういうものがやはり定義上出てきたのではないかとこのように捉えています。ですから、個人情報の視点でいうと、個人情報を安全なコンベイする環境をつくってきていると。通信環境として安全な環境を提供して、その上にEU市民情報も乗っけていくというのが、今度は運用上も出てくるという、そういう捉え方ではないかと。これはあくまでも私の私的な意見ですが、そういうふうに捉えております。

【宍戸座長】 よろしいですか。ありがとうございます。

ほかにご意見、ご質問いかがでしょうか。寺田構成員。

【寺田構成員】 皆さん非常にいろんな、細部まで入った問題意識を持っていらっしゃるようで、これを全部解決していくのは大変だと思うんですが、全般的な感想めいたものにはなるんですけども、基本的にプラットフォームの中で、どうも日本は不公平な扱いを受けているのではないかと。それから、国際調和というのも、現行の法制度であったりとか、そういったところではできないのではないかと。それに対して改善していただきたいといった内容が多いのかなと思っています。

これに対して、当然意見の中でもちらっと見えてくるのは、だからといって独自の規制になるのは避けてほしいと。規制というよりは、やはりイメージとしてはまだ自主規制的なもの。ただし、この裏に必ず法的な何らかの裏づけがあってほしいなという、そういったイメージを非常に感じています。

EUの場合は、eプライバシー法という形で、データに関してきちんと分類をして、何をすべきかということを確認に定義し始めていると。こういった流れと、日本のほうでは、独禁法や、個人情報保護法や、今回の電気通信事業法、それ以外に業法といった形で非常にばらばらに分かれていて、こういった部分の統一的なものができていないというのを非常に感じますので、こういったところというのを一度まとめていくというのが重要じゃないかなと感じました。

感想めいたものになってしまいますが、以上になります。

【宍戸座長】 ありがとうございます。貴重なご意見だと思います。

ほかにかがでしょうか。宮内先生、お願いします。

【宮内構成員】 資料3-2の18ページ、トラストサービスの在り方のところについてです。これと、先ほど手塚先生がご説明されました資料2の6ページにちょっと関係あるんで、そちらも開いていただきたいんですが。ここでトラステッドリストという話が出てくるんですね。手塚先生の資料の6ページですと、青い枠の中で左端のほうにトラステッドリストとありまして、どのサービスが安全なのかというのを、国が何らかの形で確認した、そういうもののリストがここに上がってきて、これが法的な裏づけをもってつくっているということになります。

これと日本でつくったものが相互認証できれば、これは一番ベストな解だと思っておりまして、それに向けて日本がトラストサービスというものを認定ないし確認になりますかね、やっていく枠組みというのが必要になってくると思っています。ただし、日本でトラ

ステッドリストというのをつくるのは、まだ少し時間がかかりそうだというふうに私は、一応現状は見ているわけです。

資料3-2の18ページのほうでは、最初のグローバルサインさんのほうが、ポータルサイトの構築を検討しろということをしていて、セイコーソリューションズさんのほうが、トラステッドリストと相互認証できる制度を早期に構築する。これはどちらも正しいと思っているんですけども、トラステッドリストが仮に早期にできないとしたら、こういったポータルサイトを何らかの形で公的機関でつくっていくということも非常に重要なポイントになってくると思いますので、この点についても検討を進めていただきたいなと思っております。私からは以上です。

【宍戸座長】 ありがとうございました。

ほかにいかがでしょうか。崎村構成員、お願いいたします。

【崎村構成員】 崎村でございます。これも手塚先生へのご質問になるんですけども、たしかeIDASだと、政府機関は受け入れを強制されていたと思うんですね。この手のサービスというのは、受け入れを要求されて、それによって使うことができるようになるということが非常に重要なんですけども、この民間の対するものというのは、どういう状況でしょうかというのが1点目のご質問です。

2点目は、先生の資料の14ページで、属性認証の話があったんですけども。これで最近、実は、これは多分X.509を使ってという感じだと思うんですけども、むしろ属性の中で、この会社のどういう役職の方だというだけじゃなくて、位置情報とかそういったものもすごく重要になってくることがありまして。位置情報ですね、どのネットワークからアクセスできているとか、どのGPS、例えば海外から来ているのかどうかとか、その国の中からとか、そういうのは結構使われるようになってきておりまして、そうすると、より動的にやる必要が出てきています。そういった意味で、トークン化の話が出てきているんですね。だから、X.509にしてやるんじゃないなくても、JSONに署名したようなトークンを動的に出してやってやるというような形のもが出てきていて、実はその話で、ヨーロッパンコミッションにもこの間呼ばれて行って来たんですけども、そのあたりについても何か情報がありましたら、ぜひお伺いしたいと思います。

【宍戸座長】 今の崎村構成員からのご質問、2点ですね。

【崎村構成員】 はい。

【宍戸座長】 手塚先生、お願いいたします。

【手塚構成員】 1点目は、民間のほうは特に強制というわけではなくて、サービスとしてどうしていくかと。トラストサービスに乗っかってくれば、当然トラストリストに反映されてくる世界になりますので、そちらのほうでいくということだと思います。ですから、考え方は、同じ機能を提供したときに、保証レベルがどれだけ違うかというところに、多分最後はいくと思っています。ですから、あとは使われるほうのマシンといいますか、EU市民の人がどちらを選択するかということかなという考え方です。

【崎村構成員】 質問の趣旨がちょっと違うので。質問の趣旨が、市民が使わなければならないかとかそういう意味の強制ではなくて、例えばこのトラストリストに載っているプロバイダーで、例えば電子署名を打ってきたとしますよね、どこかの企業なり何なりが、eシールを打ってきたとして、そのときに受け取り側の企業が、いやいや、うちはeシールは嫌なんだと、紙じゃなきゃ嫌なんだとかいったりすると、なかなか進まないと思うんですね。そういう話なんです。

【手塚構成員】 まず、トラストサービスにおいては、クオリファイド証明書、QCと呼んでいます。この証明書が基本的な大前提になります。この証明書は、既に前のEUの中でも、電子署名法のディテクティブのほうで規定されていて、各国法で当然日本の電子署名法と同じように法制化してきた、その上での証明書です。それが前提になっています。

それを受け入れる、受け入れない、今度はオペレーションの話ですので、どちらかというところの話ですね。そこはちょっと私もまだ明確には受け入れられないか、られるかというところの強制力まではちょっと聞いてません。済みません。1個目はそういうことです。

2個目の属性認証については、私のほうでは、まだJSONのような話までは聞いてないですけども、今、崎村構成員がおっしゃったようなことは、今後出てきてもおかしくないと思います。ですから、あくまでも電子委任状法はもっと柔軟に、どんな環境にも適用できるように私はなっていると思うので、PKIはあくまでもその1つ。ですから、今言ったのが、むしろありがたいことで、位置情報等の。そういうもののクレデンシャル的な発想というのは大事かなと思います。以上でございます。

【宍戸座長】 ありがとうございます。

まだお時間ございますが、ほかにいかがでございましょうか。山口先生、お願いします。

【山口構成員】 ありがとうございます。今日の最初のトピックであるトラストサービスに関して、資料3-2の提案募集の結果も踏まえつつ、事務局の皆様ないしは省として

のお考えにつきまして、ご質問とコメントをさせていただければと思います。内容的には、端的に言いますと、コストの話です。

まず、ここでいうトラストを「価値」として捉えると、オンラインやネットの情報環境におけるこの価値の実現には、それを担保するための制度が必要であり、また、そこでの制度整備においては、今回の提案募集の結果を拝見させていただいても、＜国際的な相互運用＞が鍵になってくると思います。EUのeIDAS規則を見ても、そのサービスを提供する事業者のリストがネット上で容易に閲覧可能ですので、そうした相互運用に向けた日本での制度整備が急務になると考えています。

そこで、ご質問として、こうした国際的な相互運用に向けた事業者—特に国内における大手事業者のみならず中小事業者も含む—にとってのコストないし負担が、どの程度かかるのかといった事実状況について、ご教示いただければと思います。

次に、コメントとして、この分野ではデファクトスタンダードも含めた「標準化」が急速に進んでいるところ、すでに走り出している国際的な相互運用のルールに、日本の国内の事業者が後から従うとなると、コストや負担も予想以上にかかってくると思いますので、今後は、初期の標準化の段階から先手を打ってその交渉の場に積極的に関与していくことも重要と思います。さらに、日本政府においてSociety5.0に向けた研究開発等のために相応の予算が手当される余地もあると思いますので、標準化も含めた国際的なルール形成に向けて、関係する省として、そうしたファンドの配分の在り方にも、先んじて見通しをつけて関与していくことも、将来的には、より包括的な視点での検討として必要になるかと思えます。

【宍戸座長】 ありがとうございます。事務局のほうから、今のコストを含めたトラストサービスの展開について、何か現時点でございますか。

【赤坂サイバーセキュリティ統括官室参事官】 まだ現時点で、具体的なコストとか、あるいはその負担をどうしていくかというところまで十分検討が及んでいないところではございますけれども、先ほどの資料3-2の17ページのサーバ証明書、(4)の下のほうにいただいたご意見についても、サーバ証明書について、より安全・安心な活用に結びつくものであれば、制度化の検討は有意義だけれども、その一方で、ユーザーであるとか、その事業者に過度の負担、不便を強いるものにならないことを望むというようなご意見もいただいております。

実際、先ほども少しご説明いたしましたけれども、こういった電子証明書を取得する際

には、当然コストもかかってまいりますので、そういう意味では、我々としても全ての取引に何らかこういったトラストサービスを強いるということではなくて、あくまでも必要なサービスについて、国際的にきちんと相互運用可能なような制度的な建て付けをどうしていくかと。その中で、必要なものについてはトラストサービスを利用できるような枠組みをつくっていくというようなことを目指してまいりたいと考えております。

【宋戸座長】 ありがとうございます。現時点では確となかなか言いにくいかもしれませんが、しかし、今後のトラストサービスの在り方を考える上で、非常に重要な指摘、将来的な観点ということをお願いいたします。

まだお時間ございますが。じゃあ生貝構成員、お願いします。

【生貝構成員】 私のほうから、全体を拝見させていただいての感想というところに近いところで今まで触れられていなかったところ、今まで少し議論もあったところでありませけれども、特に資料3-2の5ページ等でも触れられているような、事業者等における自主的な取り組みに対して十分理解した上で検討するべきというのは、非常にそのとおりなのかなと思っておりまして、まさにプラットフォーム、さまざま既に法令を超えたレベルでこういった利用者保護といったようなところ、外国のほうに対応して、実質的に日本のユーザーに対しても、そういう保護が及んでいるといったところも含めて、大変実質的にここでルールといいますか、利用者保護というのが実施されていると。

まずそれをしっかり理解して、それを尊重するというところはもちろんでありながら、ただ、やはりこういった自主的な取り組みというの、それが実行される背景にはいろいろなものがあるかというふうには思うのですけれども、やはりそこにハードローが及ぶ可能性や余地がないといったようなところで、なかなか安定的なソフトローというのが成り立ち難い場合もあるということは、1つ前提としてはあると思います。まさしく例えば電気通信事業法の海外に対する適用の在り方等を含めまして、こういったような自主的な取り組みをいかに促していくためのハードローの、外国に対する適用というものをいかに考えていくかということ、ぜひ念頭においていただけるとよいのではないかなというのが1つでございます。

それから、2つ目に関しましては、今、山口先生のほうからもおっしゃっていただいたことに近いと思うんですけれども、実際この分野はどのように法をつくっても、完全に細かいところまで決めてしまうわけにはいきませんので、前回も少し言及しましたように、例えば少し言及されたディスインフォメーションの部分ですとか、あるいはさまざまなデ

一タのポータビリティを含めて、コード・オブ・コンタクトの形成というものが、まさにヨーロッパの1つは外国法の後押しというところでもって、今まさにライブで業界標準というものが、業界標準という形で実質的な利用者保護のルールというものがつくられていようとしているというところに対して、まさにそういう国際的にデファクトとして形成されつつあるルールづくりというところに、いかにコミットしていくかという観点も、この分野でも必要になってくるのだろうと考えております。簡単ですが、以上です。

【宍戸座長】 ありがとうございます。本日、構成員の皆様から、一通りご意見を伺いましたが、私からも簡単に申し上げたいと思います。

まず、今回非常に短期間でございましたけれども、検討アジェンダ（案）について非常に多くの、しかも中身の濃い意見をお寄せいただいたということに、私からも御礼を申し上げます。

その上で、今回アジェンダ（案）で挙げてあるのは、大きく3つの論点でございましたけれども、その第1の利用者情報の取り扱いについては、やはり通信の秘密との関係をどのように考えるかということが焦点になろうかと思えます。つまり、現在の電気通信事業法上の通信の秘密の規律の適用範囲というものを、一面において広げるべきではないか。また他方で、そこで問題となる情報の内容、あるいは文脈に応じて、規律の密度と申すか、許される正当化も含めて、ある種の類型化をしたり、規律の柔軟化を図って、過剰規制を避けるべきではないか。例えばこういったご意見が、通信の秘密についてさまざまあつたらうと思えます。

また、この裏側で、プラットフォームサービスの実態ですね。つまり、現実の利用者情報の保護の在り方ということについて、正確な認識のないまま、まさに過剰規制になるようなことは避けなければいけないということもお寄せいただいた意見の中から見えてくるころだろうと思えます。

私としては、やはり電気通信事業法上の通信の秘密というのが、本来何を守っているのか。そして、このプラットフォームサービスが電気通信事業の上で大きく成長して、国民の生活、あるいは自由な情報流通というのを支えている現在の中で、日本国民の今後の社会基盤としてのプラットフォームサービスについて、先ほど申し上げた、本来通信の秘密で守ろうとしてきたものが、ここでどのように守られるべきなのか。共同規制等の手法も含めて、改めて深掘りをしていく必要があるのではないかと申すのが、1点目の利用者情報についての感想でございます。

それから、2点目のトラストサービスにつきましては、本日手塚先生のほうから、極めて重要なインプットをいただきました。今後の日本の社会において、極めて有用なトラストサービスを確保し、その上でさらにトラストアプリケーションサービスが成長していくということが非常に有用だと。そして、それには将来的にはリモート認証といったような、より簡便に国民がトラストサービスを利用できるといったような方向もあれば、また山口先生がご指摘いただいたようなコストの問題、こういったものも全体を踏まえながら、トラストサービスの健全な発展を考えていかなければいけないということ。そして、国際連携ということですね、EU等との、あるいは民間の団体との連携に整合性があるような規律を考えていくべきだ、こういうお話だろうと思います。

それから、3点目のフェイクニュースについて、いただいたご意見では、基本的にはやはり表現の自由ということへの観点からの慎重な考え方を幾つかいただいたところでございます。基本的にはスピーチにはモアスピーチでという、表現の自由の基本的な考え方からは適切なものと思いますけれども、他方で現在のプラットフォーム上の情報流通のアーキテクチャの構造上、ディスインフォメーション、あるいはフェイクニュースが流通しやすい仕組みになってはいないかどうか。そういったことに利用者、あるいは健全な世論形成を支えるためのリテラシーであるとか、アーキテクチャの組み方といったようなことについても、今後この場で時間があれば議論を深めることができるといふように、これは私個人の意見ですが、考えております。

以上、私のほうで、皆様からいただいたご意見、あるいは今回の構成員の皆様からのご意見への感想でございましたけれども、座長役に戻りまして、本日、いろいろさまざまなご意見をいただきましたので、それも踏まえまして、検討アジェンダ（案）を修正したいと思いますが、こちらの具体的な文言については、座長である私に一任とさせていただきます、後日、事務局から構成員の皆様にもメールにてお示しをしたいと思いますが、そのように進めるということでご承認いただけますでしょうか。

（「はい」の声あり）

【宍戸座長】 ありがとうございます。

その他、事務局から連絡事項があればお願いをいたします。

【岡本消費者行政第二課企画官】 次回会合は、12月21日で調整しております。また、それに先立ち、ヒアリングを調整しておりますので、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す。これにて本日予定した議事は全て終了となります。

以上で、「プラットフォームサービスに関する研究会」第2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をいただき、まことにありがとうございました。