【座談会】

# 総務省「AI利活用原則案」の課題

## ――情報法制の可能性について(2) in 青森――

東京大学大学院法学政治学研究科教授
宍戸常寿
*SHISHIDO George*

中央大学総合政策学部教授
実積寿也
*JITSUZUMI Toshiya*

青森公立大学経営経済学部准教授
木暮祐一
*KOGURE Yuichi*

（司会）東京大学大学院工学系研究科准教授
鳥海不二夫
*TORIUMI Fujio*

1　AIネットワーク社会推進会議の報告書案
2　原則の構成
3　利用者の定義
4　AIに特化した問題と一般的な問題の切り分け
5　利用者の責任
6　透明性の原則
7　終わりに

### 1　AIネットワーク社会推進会議の報告書案

**一同**　よろしくお願いします。

**鳥海**　宍戸先生，実積先生，木暮先生，私，鳥海で，座談会ということで，青森まで来ました。本日は，AIネットワーク社会推進会議の報告書案（2018年5月22日公表）を題材にして，議論をしていきたいと思います。

**宍戸**　では，私のほうから全体像をご説明します。AIネットワーク社会推進会議では，2017年6月にAI開発ガイドライン案を公表しました。このガイドライン案については，確定前に，『情報法制研究』の1号に，実積先生，鳥海先生と議論した座談会を掲載しています。AIネットワーク社会推進会議では現在，「AI利活用の促進およびAIネットワーク化の健全な進展に向けて」という報告書を作成しており，6月中にパブリックコメントにかける予定です。現在は，親会の下の分科会で議論をしているところです。5月22日に，その報告書2018の案について事務局より報告があり，議論しました。今日はこちらの報告書案について，木暮先生，鳥海先生からもご議論をいただきたいと思っています。資料5-1では，これまでの検討の経緯が記されています。第1章では，AIネットワーク化を巡る最近の動向として，国内外の動向がよく整理されていると思います。

**鳥海**　宍戸先生が先日出版された『ロボット・AIと法』とも似ていますね。

**宍戸**　整理する作業は，みんな同じですから。第2章では，AIネットワーク化が社会・経済にもたらす影響について，シナリオ分析やエコシステムの展望についてまとめられています。今日の議論の本丸である第3章の部分が「AIの利活用において留意することが期待される事項」です。先ほどもお話ししたとおり，総務省の会議では，既に，AIの開発者が遵守すべき事項と思われる，AI開発ガイドライン案を策定して，国際的な会議の場に出しています。一方で，AIの開発者だけが縛られれば，全てのAIネットワーク化がもたらすことによって生ずるリスクが低減するわけではありません。むしろ，開発者だけではなくて利用者の側も，利活用において留意すべき事項があるということが，今回の報告書案の背景にはあります。開発者の側も利活用者の側でも気を付けて，全体でAIのリスクを低減し，AIのベネフィットを最大化していくということが望まれるのではないかという観点から，AIの利活用原則の議論をしています。

具体的には，「資料5-1　事務局説明資料（報告書2018（案）概要）[1)]」の6ページ（後掲図2）です。AIの利活用には，いろんな主体が考えられるという概念整理を行っています。報告書では，具体的なユースケースに応じて，利用者，間接利

とりうみ・ふじお 氏

用者等の区別を行っています。ステークホルダーが多様にあり得るということを前提にして，7ページ目で，AI利活用原則案が10個に分けて掲げられています（後掲図1）。このうち，適正利用の原則，適正学習の原則，連携の原則は，AIのネットワーク化の便益を増進させるために，利活用者が留意すべき事項です。これに対して，尊厳・自律の原則，公平性の原則，透明性の原則，アカウンタビリティーの原則は，AIネットワーク，あるいはAIシステム，あるいはAI運用に関連するサービスに対する，社会的な信頼を醸成するための原則です。これら10個は，いずれも国際的な議論にかけるためのもので，直ちに法制化とか，利活用者を縛るというようなことではありません。非規制・非拘束的な，いわゆるソフトローという形での取りまとめ作業を，現在進めています。

特に，8番目の公平性の原則は，大きな議論があるところだろうと思います。9番目の透明性の原則は，おそらく理系の技術に関わる方から見ると，疑問があるでしょう。また，適正利用や適正学習の原則が，利活用者に期待できるのかどうか。このあたりが，AI利活用原則を論ずる際に，特に焦点になり得るところだと思います。具体的な論点等は，スライド8ページに，AI利活用原則ごとに書かれていますので，こちらも参考に議論いただければと思います。

報告書の第4章については，スライドの9ページに，今後議論が必要な点がまとめられています。まだ決着が付いてない論点はたくさんありますし，AIの普及に応じて優先順位が上がってくることが伝わるかと思います。とりわけ，教育，人材育成の問題は，この中で当然，重要なものであり，現段階では，ブレインストーミング的な内容が，第2章に書かれています。

以上が差し当たり全体の概要ですが，実積先生から何か補足をいただける点はありますか。

**実積**　去年の10月にOECDで開催されたカンファレンス“AI: Intelligent Machines, Smart Policies”の中で，日本側から開発原則の説明をしています。OECDでは，13カ国におけるAIに関するプリンシプルを取りまとめ，それらを参考にして，11月のOECDデジタル経済政策委員会でレコメンデーションにする作業を開始するという決議を採る方向で現在動いています。注意しなければいけないのは，わが国で現在議論されているのは利活用原則で，開発原則は議論が終わっているという段階ですが，OCEDでは，それらを区別していません。2つに分けているのは日本の都合なので，OECDから次に出てくるものは，利活用を含めた原則になります。今回提案されている利活用原則は，AIネットワーク化推進会議の本来のタイムスケジュールでは来年ぐらいに議論されるものだったのが，だいぶ前倒しになっています。

**宍戸**　各国政府が，それぞれのステークスホルダーの方にとって負荷がかかるような規制をかける方向にならないよう気を付けていただきたいですね。もう1点，今回の利活用原則案でも，例えば研究を促進すべき等，政府が本来何をすべきかという問題が入っていないことにも注意する必要があります。

## 2　原則の構成

**鳥海**　ではさっそく，AI利活用原則案（図1）に

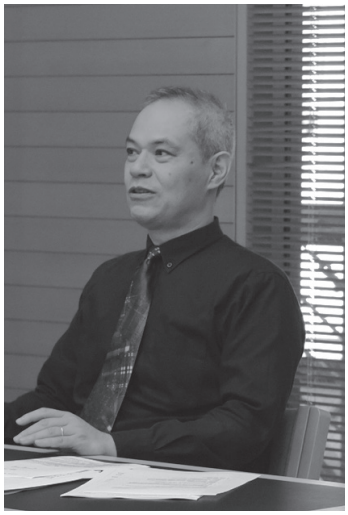
1）　http://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02iicp01_04000137.html

ついて突っ込みを入れていきましょうか。

**実積**　全部で10項目ありますが，それぞれの抽象度はだいぶ違うと思っています。1から4番目の利活用原則はそれ以降のものと比べてより上位の概念です。それ以降のものと同じ水準で並べてあるのには違和感がある。また，各原則は行動を定義するだけで，何のためかといった目的が書いてない。

**宍戸**　付け加えますと，開発ガイドラインは，基本理念の下で，いくつかの原則に構造化されています。本来であれば利活用原則案も，基本理念を立てて，それを各原則にブレークダウンしていくという，2層構造になるべきだと思います。実積先生がおっしゃるように，ハイレベルの内容が個別の原則の中に入ってたり，逆になっていたりする点を整理し直したほうがよいのではないかと思っています。

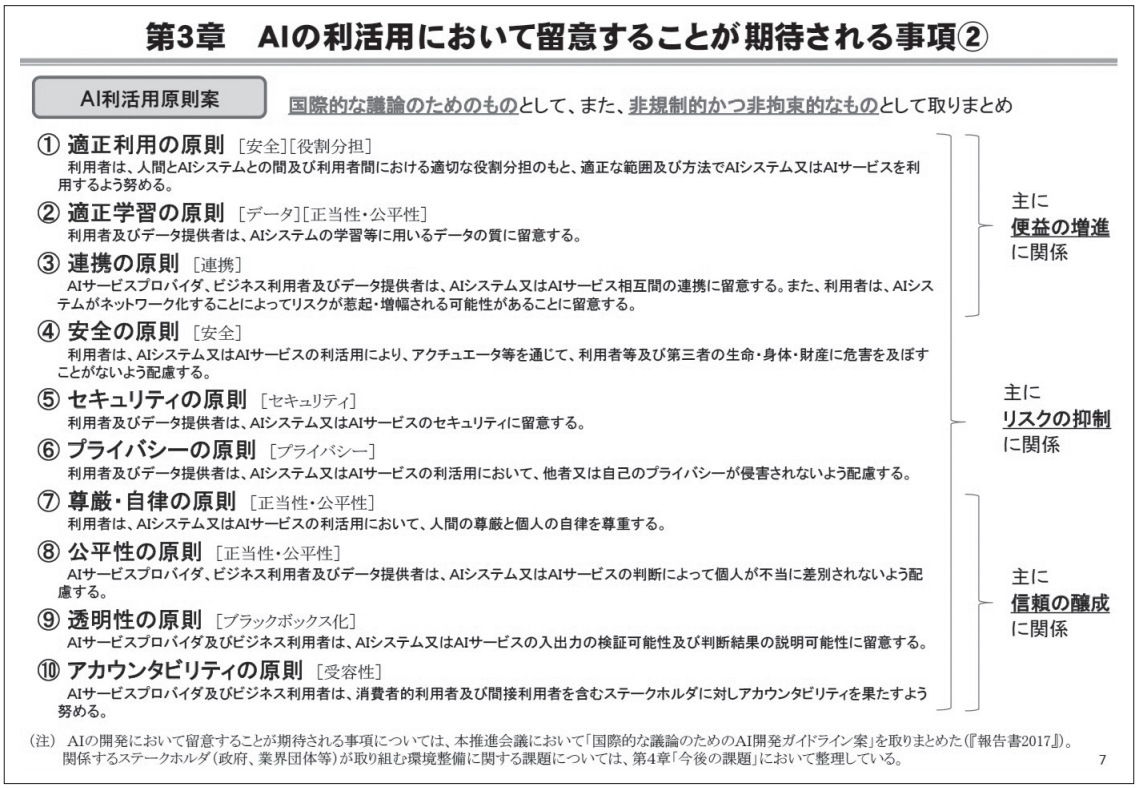
**鳥海**　例えば，適正利用の原則の中で，安全と役割分担ってありますけど，安全の原則も別にあるわけですよね。



じつづみ・としや 氏

**宍戸**　第2章でリスクシナリオ等を検討していった結果，安全や連携等が必要だということになり，第3章でそれに対応するものを書き出しています

図1　AI 利活用原則案（AI ネットワーク社会推進会議　第9回　配付資料・資料3-1　報告書2018（案）概要 PDF P.7）



**第3章　AIの利活用において留意することが期待される事項②**

AI利活用原則案　国際的な議論のためのものとして、また、非規制的かつ非拘束的なものとして取りまとめ

① **適正利用の原則**［安全］［役割分担］
利用者は、人間とAIシステムとの間及び利用者間における適切な役割分担のもと、適正な範囲及び方法でAIシステム又はAIサービスを利用するよう努める。

② **適正学習の原則**［データ］［正当性・公平性］
利用者及びデータ提供者は、AIシステムの学習等に用いるデータの質に留意する。

③ **連携の原則**［連携］
AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIシステム又はAIサービス相互間の連携に留意する。また、利用者は、AIシステムがネットワーク化することによってリスクが惹起・増幅される可能性があることに留意する。

④ **安全の原則**［安全］
利用者は、AIシステム又はAIサービスの利活用により、アクチュエータ等を通じて、利用者等及び第三者の生命・身体・財産に危害を及ぼすことがないよう配慮する。

⑤ **セキュリティの原則**［セキュリティ］
利用者及びデータ提供者は、AIシステム又はAIサービスのセキュリティに留意する。

⑥ **プライバシーの原則**［プライバシー］
利用者及びデータ提供者は、AIシステム又はAIサービスの利活用において、他者又は自己のプライバシーが侵害されないよう配慮する。

⑦ **尊厳・自律の原則**［正当性・公平性］
利用者は、AIシステム又はAIサービスの利活用において、人間の尊厳と個人の自律を尊重する。

⑧ **公平性の原則**［正当性・公平性］
AIサービスプロバイダ、ビジネス利用者及びデータ提供者は、AIシステム又はAIサービスの判断によって個人が不当に差別されないよう配慮する。

⑨ **透明性の原則**［ブラックボックス化］
AIサービスプロバイダ及びビジネス利用者は、AIシステム又はAIサービスの入出力の検証可能性及び判断結果の説明可能性に留意する。

⑩ **アカウンタビリティの原則**［受容性］
AIサービスプロバイダ及びビジネス利用者は、消費者的利用者及び間接利用者を含むステークホルダに対しアカウンタビリティを果たすよう努める。

主に**便益の増進**に関係

主に**リスクの抑制**に関係

主に**信頼の醸成**に関係

（注）AIの開発において留意することが期待される事項については、本推進会議において「国際的な議論のためのAI開発ガイドライン案」を取りまとめた（『報告書2017』）。関係するステークホルダ（政府、業界団体等）が取り組む環境整備に関する課題については、第4章「今後の課題」において整理している。

7

ししど・じょうじ 氏

が，10 は多いですよね。

**実積**　本来であれば，利活用原則の最初の３つだけで良いと思います。

**宍戸**　漢の高祖が，長安に入ったときの法三章みたいですね。基本理念があって，また論点についてきちんと議論してから，原則を組み立てる議論が本来は必要だったと思います。先に原則を立てて，そこに論点を割り振ったからヘンに見えています。

**鳥海**　例えば，適正学習の原則ってあるんですけど，これは利活用原則に入ってる時点で，何かちょっと違う気がする。学習させるのは，どちらかというと開発側では。

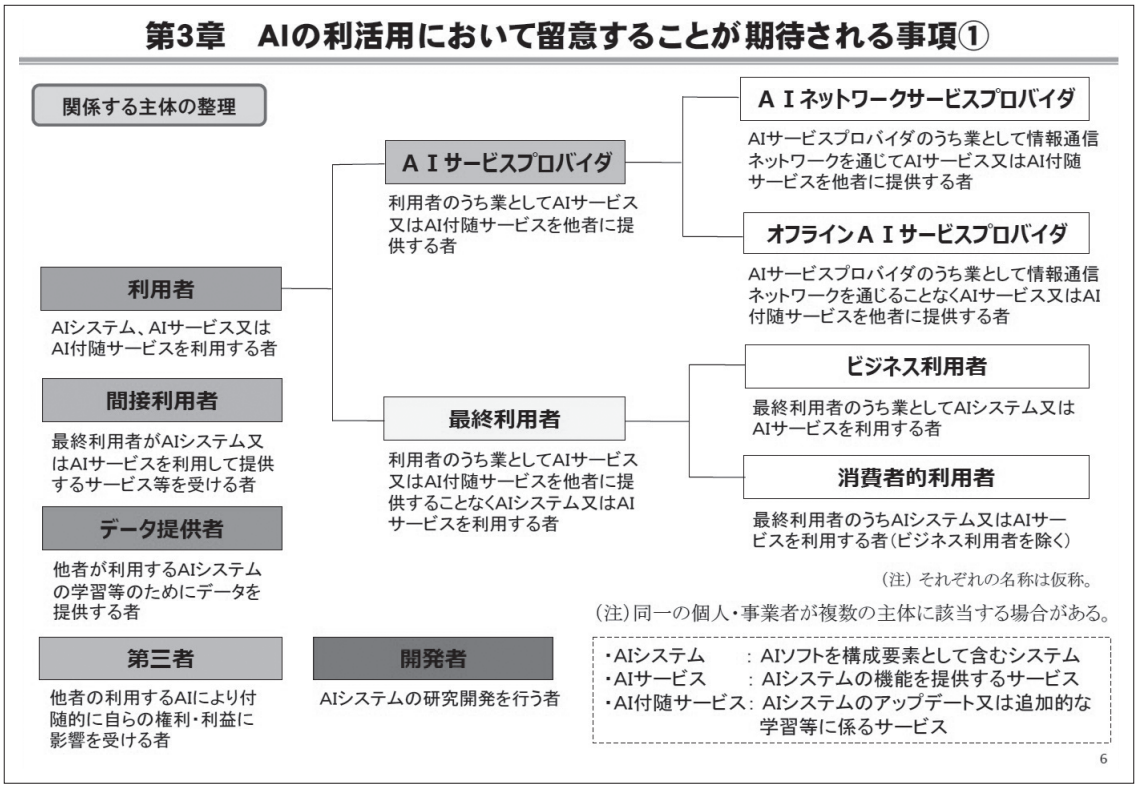
**実積**　学習させる主体は利活用原則でいうところの「利用者」の定義に該当します。

## ３　利用者の定義

**実積**　自分の手術の技を覚えさせるとかね。AI 自体のアルゴリズムは開発しないんだけれど，自分のデータを学習させて，利用するのは利用者ということになる。（図２参照）

**鳥海**　学習をさせる人は利用者であり，開発者でもあるっていう立場なんですか？

図２　関係する主体の整理（AI ネットワーク社会推進会議　第９回　配付資料・資料 3-1 報告書 2018（案）概要 PDF P.6）



こぐれ・ゆういち 氏

**実積**　AI の場合は，利用者が開発者から購入した後で，自分のデータを読み込ませて新しく学習させる可能性があるので。

**鳥海**　AI システムっていうのが，そういうイメージで作るものなのか。データを学習させて初めて AI になるので，それまでただのアルゴリズムでしかないんですよね，本当は。データ学習させて初めて，システムが開発されたことになります。

**実積**　推進会議ではいくつかの利用企業にヒアリングを行いました。例えば，銀行が顧客対応に AI を使いましょうという企画を進める場合，銀行が AI 開発することになるわけではないという自己認識でした。

**鳥海**　それを AI の開発ではないっていうふうに言い切るんですね。

**宍戸**　AI の「開発者」は，自らの開発した AI システムを用いて AI ネットワークサービスを他者に提供するプロバイダーを含め，AI システムの研究開発を行う者です。一方で，「利用者」は，最終利用者の他，他社が開発した AI システムを用いて，AI ネットワークサービスを第三者に提供する者を含みます。

**鳥海**　顧客対応している人たちは，データを学習させる人？　学習させない人？

**実積**　学習させない人。AI サービスを売ってるだけ。だから，真ん中の AI に関しては全く触っていない。

**鳥海**　その人たちは何て呼ぶんですか。

**宍戸**　この中だと「間接利用者」ですね。

**実積**　そういう意味では，利用者がすごく広い。

**鳥海**　本来はデータを学習させる人と，学習した後の AI にデータを入力して使う人は，分けて考えないといけないですね。学習させるのってそんなに簡単なこととは限らないんですよね。学習させる人なのか，学習済みの AI を使う人なのか，アルゴリズムだけを作った人なのか，アルゴリズムを作って，かつ学習もさせた人なのかとか，そこを全部きちっと分けて定義してあげないと混乱する。誰がそれぞれの対象なのかが分からなくなる。もっとも，アルゴリズムだけとなるとほとんどライブラということになるので，Google とか PFN とか限られた一部の企業になりそうですが。

**宍戸**　本当は，自分が AI との関わりで，AI に直接触れているのか，学習させているのか，何をやっているのかを理解するのが，まず大事です。AI の研究者は分かっておられると思いますが，サービスを提供してる人は，自分の立ち位置に気づくことも難しいのではないでしょうか。

**鳥海**　例えば，この会場でもカメラで撮影が行われています。そのカメラの中に AI が入ってるわけです。この場合，その写真を，例えば『情報法制研究』に載せますよね。その読者は最終利用者になるんですか。

**宍戸**　読者は間接利用者でしょうかね。

**鳥海**　すると利用者は写真を撮影した人？

**宍戸**　写真を撮影した人が利用者ですから，今の例であれば，『情報法制研究』を発行する主体が利用者ですね。

**鳥海**　例えば，カメラの中に入ってる AI は，カメラメーカーが開発した AI じゃないとしましょう。海外の会社（A 社）が作った AI を使って，顔認識は誰か別の人（B 社）が作りました。それをカメラメーカー（C 社）がキャリブレーションをし，カメラを作りました。それを撮影者（D）が使って，写真を撮りました。

**宍戸**　その場合だと，開発者が A 社で，B 社と C 社は AI サービスプロバイダーになります。

**実積**　AI のキャリブレーションをどう捉えるかだろうね。キャリブレーションの前のシステムをいじる主体は，明らかに開発者だと思うんだけど，キャリブレーションをどう考えるか。実際のデー

タを入れれば適切な答えが出るようパラメータ調整をするっていうのが開発だと僕は思ってる。実際にデータを入れるのは開発じゃないんじゃないかな。

**鳥海**　となると，データを入力して出力を見る，以上のことをやる人は開発者側とするべきな気がしますが，ここはまだ議論が不十分に見えますね。

**宍戸**　自動運転タクシーの例（図３・例③）ではどうでしょうか。メインは真ん中にいる自動運転タクシー業者になる。

**実積**　お金を払っている乗客はサービスの受益者（最終利用者）になる。このサービスを提供するのがタクシー会社になる。その車を造ってる人がいる。

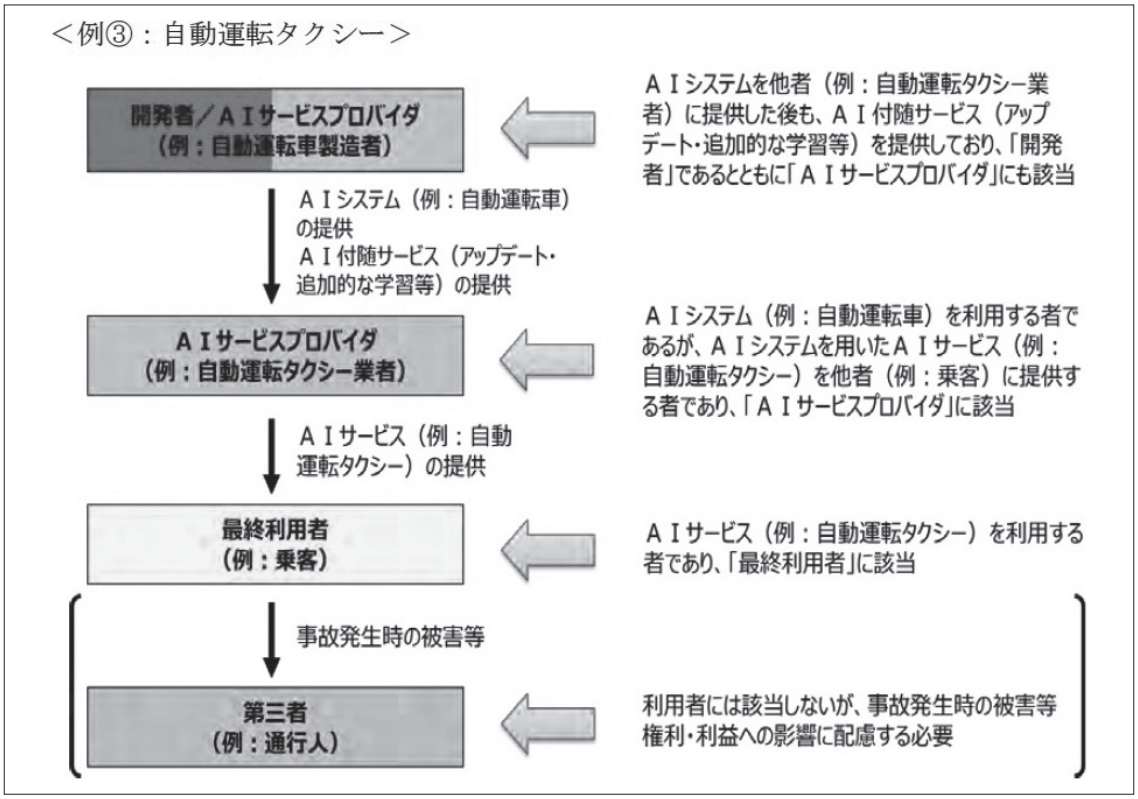
**鳥海**　車を造っている人と言うと範囲が広いですね。自動車の車体を作っている場合もあれば，組み込みのコンピュータを作っている会社や，ナビを作っている会社もある。そもそも，この場合は，自動運転タクシー業者は，AI サービスプロバイダなんですか？

**宍戸**　AI 自動運転タクシー業者は当然，街中に車を走らせてるので，データを収集して，自分たちが使っている AI に入力していることは間違いない。

**鳥海**　本当は，自動運転で一番重要な AI って画像認識なんですよね。でも，ここでの議論は，交通網や渋滞状況等を考慮してルートを決定する AI のイメージなんですね。ルートの話であれば，カーナビ会社が開発者かな。しかし，個々の会社ごとに最適ルートを学習させるとなると，タクシー事業者も開発者になるべきですかね。ルート学習アルゴリズムがすでに開発されているなら，利用者になるのかな。学習していると意識して使っていたら開発者ですかね。

**実積**　研究者からユーザーまでみんな AI に絡んでくるので，そこを統一するようなガイドラインを作らないと意味がないという考え方はありえたと思います。ただ，われわれは開発ガイドライン

図３　例③自動運転タクシー（AI ネットワーク社会推進会議　第９回　配付資料・資料 3-2　報告書 2018（案）本体 PDF P.49）



をすでに作っちゃったから，それを今更無しにできない。とすると，利用ガイドラインの対象について，開発者と利用者の線引きをきちんとしないと混乱する。今回は，AIが世の中に入るときに，何を気を付けましょうか，どこを政府として，規制庁として注意すべきかについて全体をまとめている。そのため，現実社会において，開発者と利用者の区別がつかないということになると，開発者も含めてガイドラインを作らないと，実効性がないものになってしまう可能性がある。

**宍戸**　ガイドラインは，適用対象を決めなければいけない。そこで，開発者か利用者かを分けられなかった場合は，開発も利用もひっくるめて「AIについて透明性を確保しましょう」という，中途半端で何を書いているのか分からなくなってしまいます。一方で，概念的には開発者と利用者を区別できるということと，実際の個別の事案がどちらに当たるのかは別で，実際には両方に当たる場合もあります。

**実積**　常に両方の属性を持ってますって言われる可能性はある。タクシーの運転手，雇われてる運転手以外は，両方に属する可能性が高い。

**宍戸**　ただ，個々の論点を見ていけば，議論を具体的に落とし込もうとしている部分もある。例えば，適正利用の原則では，一番最初の論点で，「利用者は，AIの性質，利用の態様等に応じて，利用する前に，リスクを認識し，正しい用途を理解するとともに，必要な知識・技能を習得すること等が期待されるのではないか。」と言っています。これは開発者等と比較して，知識に非対称性があるということを念頭に置いています。

**鳥海**　というと？

**宍戸**　利用者は開発者よりもAIシステムないしAIサービスについての理解が下がることを前提に置いた上で，より理解をしている者の情報提供や説明を踏まえて行動しましょう，という趣旨のことだと思います。

## 4　AIに特化した問題と一般的な問題の切り分け

**実積**　これを「AI利活用原則」とすることに僕は賛同できない。ここに列挙されている原則は，物やサービスを売るときには必ず満たさなくていけない当たり前のルールに過ぎないわけです。なので，「利活用原則」としてわざわざ新しく定義する必要はないと考えています。

**鳥海**　つまり，AIに特化した話ではないと言うことですよね。AI利活用ガイドラインなのにAIに特化してない話まで書くのかとは思いますね。

**宍戸**　AIに特化してない話も入っていますね。

**鳥海**　一般的な話を入れると混乱するので，やめたほうがいいのではないでしょうか。例えば，プライバシーに関してAIだから対応しなければということはなんなんでしょうか。

**宍戸**　プライバシーだとプロファイリングですね。

**鳥海**　AIを使わなくても，プロファイリングってできますよね。コンピューターを使えば大量のデータは処理できるわけですから，昔からできました。つまりAIがじゃなくて，ただのIT技術です。そう考えればAIを取り締まっても意味のない問題では。

**宍戸**　AI開発ガイドラインにしてもAI利活用原則にしても，AIが出てくるまでは人類社会に出てこなかった問題だけしか扱わない，というものではないです。

**実積**　開発原則の場合は，新しいもの作るって話だから，こういうの作るなとか，こう作れっていう制約をかける意味があった。今回はすでに存在しているAIをどう使うかという話。そのときに，AIを使う場合，ここを特に気を付けろっていう話になるか否かがルール作りの必要性を決める。AIによる自動運転車と，人が運転する車で，前者に対して余分な制約を与える必要がない限り，ガイドラインに書く必要はないと思う。

**木暮**　AIの応用は私たちの生活の中で意識さえしていないようなシーンにも広がろうとしています。「こういったシチュエーションにおけるAI」というふうに事例で記せないところまで広がっていきますね。

**宍戸**　AIが普及する社会では，われわれの生活やサービスが全部AIに関わってくるという前提で，新しい社会をデザインするイメージだと思います。

**実積**　そうすると，AIシステム，AIサービスっていうのに特に焦点をしぼってルールを書くべきではない。新しい時代にも非AIサービスはあるのだから，それらを包括した書き方にしないと。

**宍戸**　もう一つ，開発原則と利活用原則では状況が違ってくると思っています。開発者は，AIの利活用者に比べればですが，まだある程度均質的です。それに対してAIの利活用者は多分，何も分かっていないことが多い。

**実積**　このAIは，こういう性質を持ってる，こういう危険性があるとちゃんと分かるように書いてあれば，あとはリテラシーの問題だ。だから，教育の話かなと。包丁が危ないというのと同じような話。使い方分かって，人刺しちゃいけませんよということが分かればいい。危ないものは触るなという教育。

**宍戸**　AIが普及しきって，みんなが包丁と同じくらい，AIとは何か分かるところまで来れば，この種の規制は不要になるかもしれない。

**鳥海**　いや，AIってなんだって，みんなが分かる時代ってのは，そもそも来ないですよ。今，ディープラーニングとかがAIと呼ばれているが，多分10年後ぐらいには，ディープラーニングをAIと呼ぶのだろうか。当たり前になってくるとAIって呼ばないと思うんです。自動化技術としか言わない。つまり，AIはそこまで特別なものというわけではないわけです。

**木暮**　AI研究の一つのトレンドに人工自我開発のような，すなわちAI自身が経験を踏まえて進化していくような技術の開発も進んでいます。すなわち，AI自体が自分で進化するようになると，もっとまた違う話になっていきますよね。それはもう想定外。

**鳥海**　そうなんですよ。AIが進化するとかは完全に想定外なんですよね。そういう話をイメージされると現状とかけ離れすぎています。ディープラーニングのことを考えるのであれば，ただのIT技術の話になります。

**木暮**　実際に自動運転車の場合，自動運転車の基本的な機能としての自動運転には，ディープラーニングだけでかなりのことができてしまっていて，それをメーカーが責任を持ってサービスとして提供し始めていますしね。

**鳥海**　つまり，人工知能だって言われているもののほとんどは，ディープラーニングなどの機械学習だっていうふうに整理しなくては。自動運転車についても，その中の技術のいくつかは，別にAIじゃなくてもできることですし。例えば，「今日は渋滞しそうだからこっちの道を走ろう」みたいな話って，カーナビでできるレベルの話です。もちろんその中ではAIと呼ばれる技術も入ってるかもしれないけど，われわれはカーナビの便利な機能くらいに思っていますよね。そこを分けるのか分けないのかどうなんでしょうね。ただ，自動運転車が走っていることを，10年後にみんながどう思っているでしょうか。多分，今自動運転と言われて考えることと，10年後に言われて考えることは全然違うと思います。それに対しても，包括的に考えなければ，意味がないでしょう。自動ブレーキなんて，10年前にやってれば，AIブレーキと呼ばれていてもおかしくないと思う。だけど自動ブレーキと呼ばれている。だけど技術的には別に，あれはAIといえばAIになります。名前にこだわるのではなく，良い技術が社会に浸透していくような仕組みにすることが大切ではないでしょうか.

## 5　利用者の責任

**宍戸**　話を原則のほうに戻しましょうか。適正利用の原則の中で，例えばAIのソフトのアップデートについて利用者がいつも気を付けてほしいという要請は，あってもいいと思うのですが。

**鳥海**　それもAIに限らない普通のことじゃないですか？　みんなソフト，アップデートしますよね。AIに限らずソフトウェアっていうのはアップデートするものっていうのが今じゃ一般的じゃないですかね。

**宍戸**　だからこの機に，AIだけでなく何でもソフトはアップデートするものですよ，という教育は必要ではないですか。

**鳥海**　OSが勝手にアップデートされるのと同じように，必要に応じてアップデートしなさいねということですね。

**宍戸**　エンドユーザーが自分できちんと更新しなさいという要請があれば，ずっと電源切っていたAIに久々に電源入れて，そのまますぐ使うとかいうことはやめてくれといえませんか。

**鳥海**　そういう場合は使えなくなってるように，開発者のほうがロックすることはできますよね。

**宍戸**　開発者が全部，責任を取らされる形でもい

いのでしょうか。

**実積**　では，こういう事例ではどうでしょうか。たまたま，アップデートする機能が壊れてました。それで，古いAI使ってました。事故が起きました。誰の責任なんですか。

**宍戸**　古いAIを使ってる者の責任ではないでしょうか。

**実積**　逆にアップデートしなくても，うまくいくケースがあったりする。アップデートするかしないかっていうのは，実際に具体的な不具合が発生して，人を傷つけたりとかしない限り，問題はないんじゃないのか。アップデートしろっていう話をなぜわざわざ書かねばならないのか。

**宍戸**　アップデートするように留意しなさい，と言ったほうがよくはないですか。

**実積**　そういったことは，適正利用の原則で読めるはず。そもそもアップデートだけに気を付ければ大丈夫っていう話でもない。アクチュエーターが付いてるんだったら油を差そうとか，自動運転車の外部監視カメラのレンズに泥が付いて見えないときは拭きましょうとか。これらを含めて適正に全部やってねっていうのが適正利用の原則ではないのか。アップデートだけ横出しする理由が分からない。

**鳥海**　そういえば，車のリコールって応じないと，どうなるんですか。面倒くさいから行きませんでした。事故りました。誰の責任なんですか。

**宍戸**　消費者法的には，企業が償う必要がある場合もありますね。

**鳥海**　となると，リコールと一緒という扱いで，アップデートについてはわざわざ書かないでメーカー側がアップデートの責任を取ると言うことにはならないでしょうか。

**宍戸**　リコールと同じだというと，全ての商品・サービスに共通することだから，およそAIガイドラインに書かなくてもいいということになりませんか。ガイドラインが必要だという議論は，まだAIに対する社会的受容性がない，信頼がないという前提で，AIの普及を図るためのものです。

**鳥海**　もう一点確認なのですが，これは一応，利用者が，AIを怖がらずに使わせるためなんですよね。

**宍戸**　そうです。一例として，アップデートはちゃんとしてくださいねと。

**鳥海**　利用者に負荷がかかるような原則を入れるということでしょうか。

**宍戸**　それほど大きな負荷でしょうか。

**鳥海**　アップデートをしなかったら，あなたの責任ですよねと言うことになるのですよね。

**宍戸**　「責任」と言っても，民事責任のような法的責任に該当するかどうかは，先の話です。

**鳥海**　でも事実上，こう書かれると，そういうふうに受け取ってしまいそうです。

**宍戸**　報告書案だと64ページ前後にありますが，ガイドラインを作るという話の前に，リテラシー教材のようなものを作るほうが良かったのでしょうね。

**鳥海**　それは全くその通りですね。

**宍戸**　消費者的利用者向けに分かりやすいメッセージを発信することが重要ではないか，という議論は分科会でもありました。それから，消費者的利用者ではないけれども，それに近い者として，先ほどの例に挙げられた自動運転タクシーの配送業者であるとか，普通のお医者さんについても同様ですね。

**鳥海**　商品化されたAIを使って商売をする人たちについてですね。

## 6　透明性の原則

**実積**　AIを使ってる人は，AIを使ってるんですよっていうのを，どっかで言わなきゃいけないとは思う。何にAIを使っているかという説明も必要だ。

**宍戸**　スーパーマーケットでカードを出して買ったりして，それでポイントが付いたりするのも，後ろでAIが働いていますよね。

**鳥海**　クーポンを出す場合，そのクーポンがAIの計算に基づいているということですね。一方で，AIに処理されているととられて規制が厳しくなるのが嫌だったら，これは統計処理で出してるんですよって言うこともできるわけですよね。

**宍戸**　おっしゃるとおりで，AIの定義に関わってくる。

**鳥海**　このガイドラインができて，AIを使うことに説明責任が生じて，負荷が上がるんだったら，みんな，これAIじゃないですよって言う可能性

もあるわけですよね。結局AIの定義が曖昧だと，「これはAIじゃない」と言えばAIじゃないって言い切れちゃうんですよね。

**実積**　でもAIに対する不安感を払拭するように，みんなで透明性原則は守りましょうっていう方向性がやっぱり必要なのではないか。

**鳥海**　それは過去の技術も，全て含むということでしょうか。今まで，ブラックボックスとして，中身については説明していなかった技術も含むのでしょうか。クーポンの出し方とか説明されたことないですけど.

**実積**　むしろ問題があった場合，AIということを理由として逃げれないということ。AIだからブラックボックスで中身は分かりませんっていう言い訳は許さないと。

**宍戸**　実はそこについては，まだ合意は得られていないと思います。透明性のイメージが，まだ人によってばらばらのままだと思います。一般に透明なほうがいいけれどもそれには当然限界もあるよねというレベルで，まとまっている感じがします。もう一歩進んで，より具体的な広告とか景品に落とし込んでいけば，実際には景品出してないのに，景品を出しているようなうそをついたら駄目だというのと同じ話になるように思います。ですから，本来は具体的な落とし込みをすべきなのに，現時点ではメタルール的だから，不十分なわけですね。

**鳥海**　例えば，自動運転車について考えてみます。なんかでぶつかって事故を起こした場合に，なぜぶつかったのかを解明しなければいけないということになりますよね。ガイドライン上では，このような解明しなければならないことをどのように捉えるのでしょうか。きちんとオープンにすれば良い，ということでしょうか。だけど現状では，ディープラーニング使って，学習した結果を用いた画像認識によって判断しているわけです。それに関して，例えば別の車にぶつかったときに，なんでこれを車と認識できなかったのかっていうことを説明するっていう責任が生じるっていう理解でいいですか？

**実積**　どうして自動運転車が回避できなかったのか，それはAIが対象を認識・理解できなかったからですっていうところまでは説明が必要。

**鳥海**　そうですね。これが車だとは認識しませんでしたと言います。例えばそこで，そもそも，根本となる画像認識の程度が低く，普通の画像認識であればできそうなのに，できなかったということになったとき，責任はどうなのでしょうか。できなかったこと自身が罪なのか，なんでできなかったのかまで突っ込むのか。それによって，その画像認識のシステムを作ったところに責任があるんでしょうか。

**宍戸**　今の点は，政府は「自動運転に係る制度整備大綱」（2018年4月17日）で比較的明確に整理をしたところです。AI利活用原則案ではまだ，利用者がこういうことに気を付けましょうね程度です。しかし自動運転の場合には，今までと同じく，程度の低い車を出した者が責任を取り，程度が低くなければ運転者が責任を取る，という基本的な枠を決めていきます。この今までのルールを前提にすると，問題は，車の程度が低いかどうかをどうやって明らかにするかです。物の瑕疵によって生じた事故なのかそうでないのかが分かるようにすることが求められているところ，AIや自動運転だと分かりくくなります。だから自動運転に対応して，物の瑕疵なのか運転者の過失なのかを明らかにする仕組みを実装する必要があります。具体的にはドライブレコーダーの実装を義務づけることが考えられます。このように，法規制はガイドラインよりも上のハードルを越えてかけるものですので，問題は，それと同じように全分野で法規制をかけるかどうかだと思います。

**実積**　一つ質問です。自動運転車に乗っていたとしても利用者が選択しないと自動運転モードにはならないですよね。程度の低いAIということを知らずに，自動運転モードに移行した場合の責任はどうなるのでしょうか。

**宍戸**　自動運転に委ねたか委ねていないか，利用者が触ったのかどうかも，ドライブレコードを入れれば分かることを前提に，自動運転モードに移行した場合が問題になりますが，この場合は，現行の製造物責任法の問題等に回収されて，それは仮に本人が程度が低いと分かっていても，程度が低い物を提供した者の責任だと思います。

**鳥海**　自動運転であれば，いろんなメーカーが作っていけるから，対抗策として別なメーカーの製

品を使うという方法もありますからね。

**宍戸**　このように具体的に義務化を考えられるのは，まずは自動運転だけだと思ってます。法規制は，人の命に関わる問題でない限り，そのぐらいのタイミングでなければ，イノヴェーションや研究を阻害するのではないか，と私は思っています。だからその代わりとして，利用者にこのぐらい気を付けようねぐらいのもののほうが，いまのところは良いのではないでしょうか。ハードローよりはソフトローを緩めに浅くかけておいて，様子を見ながらソフトローを変えたり，ハードローに切り替えたりしたほうが，健全ではないかと思っています。

## 7　終わりに

**鳥海**　まだまだ議論はつきないですし，原則のごく一部についてしか突っ込めませんでしたが，紙面の都合上この辺でいったん締めたいと思います．皆様最後に一言ずつお願いします．

**宍戸**　今日は私が「悪魔の代理人」役で，ずいぶん話しすぎたような気もしますが，先生方の率直な疑問や指摘には共感するところが多いですし，また自分自身改めて考え直す機会を与えていただいたように思います。AI 利活用原則案は，本来，AI の研究開発に全ての責任を寄せて研究開発を阻害することのないようにという観点から考えられるべきものであり，今後，AI 開発ガイドライン案と統合して現時点で必要な範囲に，簡潔に整理し直すことも検討すべきだと個人的には思っています。引き続き，経済や技術と，法学の対話を続けさせていただければと思います。

**実積**　AI のような新しい技術の開発や利活用について考える場合，政府の介入はできるだけ抑制的にすべきだと思ってます。むしろ，サービス提供側の情報公開を充実させること，今回の場合は，AI を使っているのか否かをしっかり情報提供することを前提に，利用者のリテラシー改善を行い，「危なそうだから使わない」「怖いから使わない」という選択肢を確保しておけば，多くの局面には対応できるのではないかと考えています。そのうえで，サンドボックスなり特区を活用して，提供側に意欲的なトライアルを促す一方で，発生した問題については，まずは民間ベースに個別対処するという方向で。「危なそうだから包括的なルールやガイドラインをかけよう」という方向では，せっかくの新産業が日本に根付きませんし，長期的には新サービスを利用できない消費者が損をしてしまいます。さらに言えば，「新しいもの」に対し，日本がどの程度寛容になれるのかが試されている気がしてなりません。不可避的に生じる失敗に対してある程度の寛容さを持たずにはその先の果実は手に入れられないと思えてなりません。

**木暮**　じつは私は東京で生まれ育ち，仕事もしてきました。5 年ほど前に青森へ移住してきてはじめて地方暮らしをして痛感したことは，大都市圏と地方とを一括りでまとめるのは難しいということ。例えば本日たくさん話題に出た自動運転車の話で言えば，地方では赤字を抱えて次々に路線バスでさえ廃止になった区間がたくさんあります。しかし，自動走行バスが実現されれば，運用のコストは有人運転よりも抑えられるでしょうから，廃止になった路線が復活できるかもしれません。それによって地域の再生にもつながっていくかもしれない。案外，ICT の応用が成果を出せるのは，大都市圏よりも地方なのかもしれません。現在，AI を含め ICT を巡る法は国内で一元的に決められていますが，地方に目を向けていただくともう少し違う視点で検討しなくてはいけない事項も出てくると思います。大都市圏と地方での生活を体験した立場として，地方ならではの課題についても今後情報を収集していこうと考えています。今回は遠路はるばる青森までありがとうございました。

（2018 年 5 月 26 日収録）