

緊急 WEB シンポジウム「新型コロナ感染症対策における IT 活用とプライバシー」  
2020 年 7 月 30 日（木）開催 [http://www.jlf.or.jp/work/kenshu\\_200710.shtml](http://www.jlf.or.jp/work/kenshu_200710.shtml)

講演録 5

「IT の利活用と個人情報保護・プライバシー権」

宍戸常寿教授（東京大学）

1. はじめに .....	2
2. 個人情報保護法制 .....	3
3. プライバシー .....	5
4. 「データの自由」と「データによる自由」 .....	6
5. 民間事業者からのデータ提供 .....	10
6. 接触確認アプリ .....	12
7. コロナ対策とデータ利活用の課題 .....	15
8. データ・ガバナンス .....	17

## 1. はじめに

ご紹介預かりました、東京大学の宍戸です。私はもともと憲法の研究者ですが、プライバシー・個人情報保護について研究をしている関係から、先ほどご紹介ありました COCOA の有識者会議や、また後でご紹介します Yahoo!におけるプライバシーに関するアドバイザーボードの座長として、この間の COVID-19 と ICT の利活用の関係について、多少考える機会がありました。

そのことについてお話ししながら、より一般的に、今後の Society 5.0 における ICT の利活用、個人情報・プライバシーとの関係について、今回のコロナの延長線上でさらに考え、またそのために、コロナの問題についても考えるといった視線の往復が必要であることについても、お話をさせていただきたいと思います。

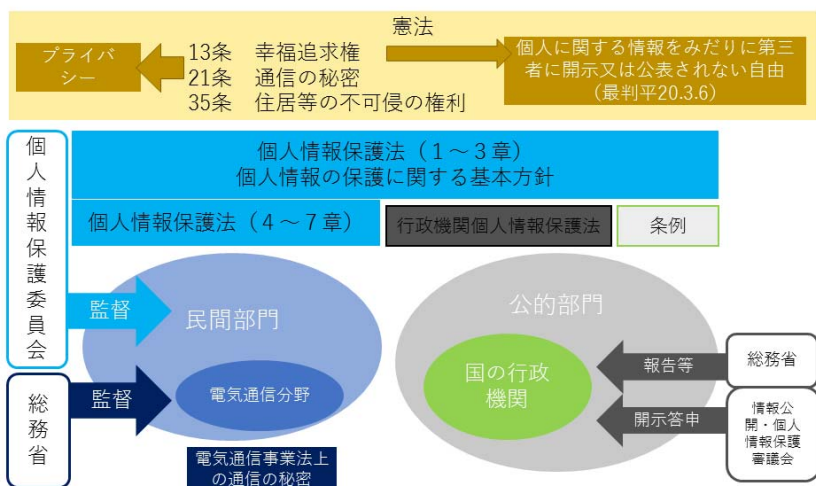


1

今日のお話は四題漸で、まず、お集まりの先生方はよくご承知のことかと思いますが、個人情報とプライバシーの一般的な整理をしたうえで、議論を組み替えて考えないといけないのではないかということについて、「データの自由」「データによる自由」という問題枠組み、あるいは視点を提示させていただきます。3つ目に、「With COVID-19」で日本で見られたさまざまな議論について、どういう教訓が引き出せるかについて、私の私見を述べさせていただきます。最後に「データのガバナンス」「データによるガバナンス」について、今回の事例を素材に考え、またその観点から、今後のウィズコロナ・アフターコロナについて考えてはどうかということをお話しさせていただきたいと思います。

## 2. 個人情報保護法制

### 個人情報保護・プライバシー・通信の秘密



2

そこでも、個人情報とプライバシーの関係ですけれども、ご承知の通り、個人情報保護法がまずあって、その基本法部分が民間部門と公的部門の全体に及ぶ。それと同時に、個人情報取扱事業者に対しては個人情報保護法の4章以下の規律がかかり、これについては、個人情報保護委員会が監督を行なっている。

またその中でも、特に通信の秘密については、総務省が電気通信事業法に基づく監督が、いわば重なって存在しています。

他方、公的部門におきましては、行政機関個人情報保護法が国の行政機関を対象都市、地方公共団体がそれぞれ独自の条例を設けております。そして、基本的には、それぞれの大員が自らの行政機関を、あるいは地方公共団体が自らを監督するという仕組みになっています。

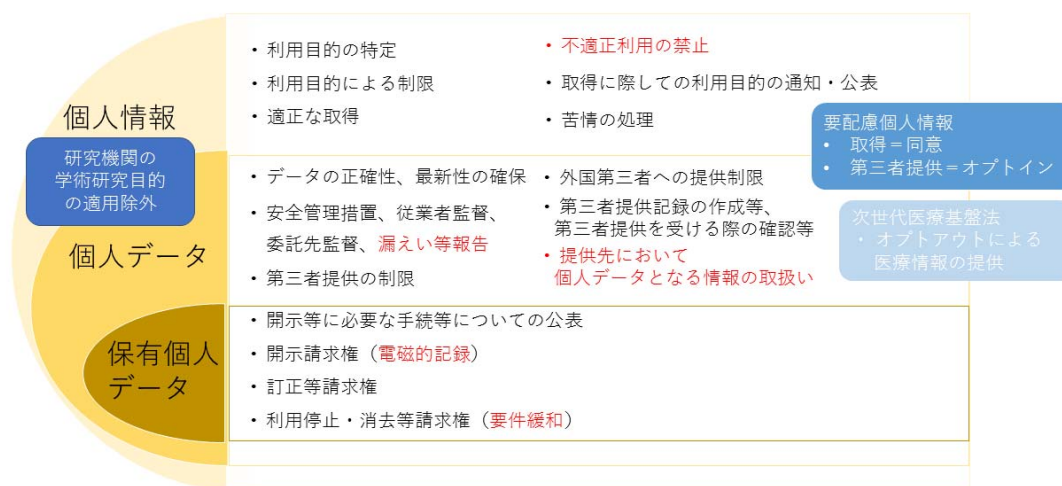
この点で公的部門における監督が十分とはいえないのではないのか、地方公共団体ごとに個人情報の定義や、規律・運用が異なる、「2000個問題」と言われる問題が起きているのではないのか。このような個人情報保護法制の不統一や、その機能が十分でないのではないということが、コロナ対策の問題を考える上でも、大きな背景になっています。

もう一言申しますと、個人情報保護法の後ろ側に憲法があるということは、孫先生と同じく憲法研究者である私としても強調したいところです。憲法21条の「通信の秘密」や憲法35条の「住居の不可侵」等が、もともと日本語憲法制定時においてプライバシーに相当するものを守っており、現在ではより一般的な意味での「私生活の平穩」が憲法13条の「幸福追求権」で保障されると考えられるようになっていきます。また、プライバシーとの関係は微妙でありますけれども、住基ネット事件最高裁判決（最判平成20年3月6日民集第62巻3号665頁）におきましては、個人情報に関する憲法上の自由が正面から認められてい

ます。

このように、プライバシーと個人情報に関する権利を、二元的にものを考えた方が良いのではないのかという点は、この後の私のお話にも関わってきます。

## 個人情報取扱事業者の義務



3

この図は、個人情報保護法上の個人情報取扱事業者の義務を簡単にまとめたものです。「個人情報」、「個人データ」、「保有個人データ」という事業者の側でのデータの持ち方、形態に応じて事業者の義務が決まり、またそれに相関する形でデータの主体、本人の関与の度合いが変わってくるというのが、基本的な個人情報保護法の建付けです。

赤字で書いた、たとえば「不適正利用の禁止」でありますとか、「提供先において個人データとなる情報の取扱い」は、2020年の個人情報保護法改正において新たに付け加えられた部分です。

今日議論している公衆衛生との関係ですと、たとえば民間部門の研究機関における学術研究目的での取扱いには、義務規定の適用が解除されます。しかし、私が勤めております、国立大学法人東京大学では、適用除外されていない。こういったでこぼこがあり、多機関連携での情報の分析や共有にさまざまな溝があることも、よく知られています。

また、たとえばコロナウイルス感染症にかかったといった情報は、2015年の法改正において「要配慮個人情報」になり、その取得には原則同意が必要であるとか、第三者提供はオプトインでなければいけないというように、保護が強化されました。他方、次世代医療基盤法が制定されまして、オプトアウト方式によって医療機関からの医療情報の提供を受けて、認定を受けた事業者が匿名加工情報にすることができるといった法制も整備されています。

これらが、コロナや公衆衛生と個人情報保護に関わる法の建付けになります。ただ、これらの個人情報保護法制は、基本的には事業者、あるいは行政機関による個人情報の取扱いに

対して、分野横断的に行政的な規制をかけるものです。先ほど申し上げましたように、個人情報、個人データ、保有個人データという形態に応じて、事業者・本人間の権限分配により、個人情報の有用性、あるいは行政の適正・円滑な運営とその保護のバランスを図るという建付けのものという理解しています。

### 3. プライバシー

## 個人情報保護とプライバシー

プライバシー	個人情報保護
私生活上の自由・平穩を内容とする基本的人権	事業者による個人情報の取扱いに対する、分野横断的な行政規制
情報の内容・性質・文脈等に応じ保護の要請が変化	事業者・本人間の権限分配により、個人情報の有用性、行政の適正・円滑な運営とのバランスを図る
主観的な感覚と紛争後の比較衡量	過剰規制または過少規制のおそれ

4

これに対してプライバシーは、私生活上の自由あるいは平穩を内容とする基本的人権であり、その情報の内容や性質、また取得や取扱い、特にその情報が本人に当てて使われる文脈等に応じて、その保護の強度は変わると考えられます。

プライバシーと個人情報保護の間には、最終的に個人の権利利益を守るという広い意味では共通の方向性がありますが、同時に法的な仕組みとしての違いも看過できないところです。

とりわけプライバシーについては、本人がどう主観的に感じるかによって、「プライバシー侵害である、ない」といった結論が分かれることも多い。実際には事態が発覚して紛争としてなった後、最終的には裁判での比較衡量において、そのプライバシー侵害が適法であるか、そうでないかというのが決まる。個別具体的な状況における、適正な判断に馴染むと同時に、その判断をいちいちやろうとすると大変であるといったところがあります。

これに対して、個人情報保護法は、一定の条件に該当すれば個人情報として保護され、規律がかかる、そうでなければかからないということで、ある意味では、明快な行政規律を志向しています。しかしそうであるがゆえに、プライバシーの観点から比較衡量すれば許されるような情報の利用についても、あらかじめ同意が必要であるといった「過剰規制」となりえます。逆に、プライバシーリスクの観点から見れば問題になる情報の取り扱いであっても、

法律上の個人情報に該当しないという理由で保護がない、「過少規制」の恐れといった両方の問題があるところです。

この両者を架橋するために、たとえばプライバシーを自己情報コントロール権、ないし情報自己決定権のように本人の権利の側から理解をしたうえで、両者の統合を目指すという方向性がこれまで取られてきました。私もその方向性で処理できる問題は多いとは思っておりますけれども、現在起きている社会の変化の中で、違った視点も必要なのではないかと、最近考えるようになっております。

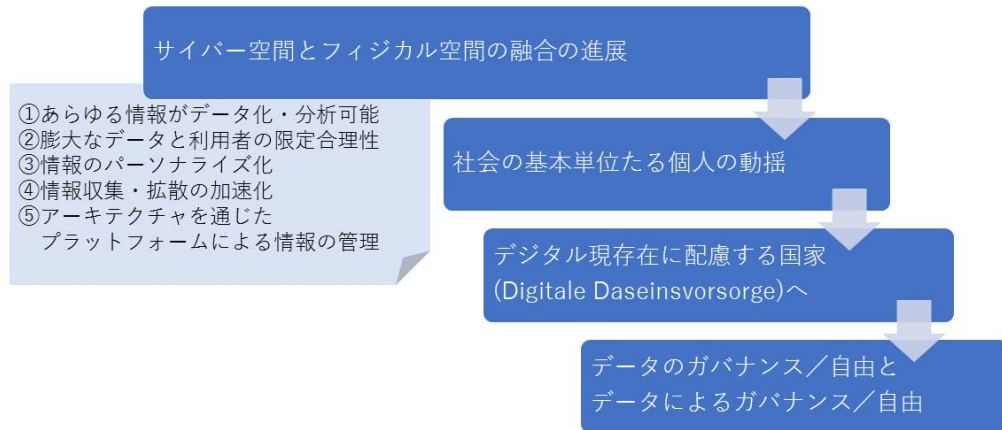
#### 4. 「データの自由」と「データによる自由」



5

そのことを、「データの自由」「データによる自由」という言い方で、少しご説明させていただきたいと思っております。

# 「ネットワーク空間」の生成



6

インターネット、あるいは情報通信サービスの普及により、サイバー空間とフィジカル空間の融合が進んでいることは、このコロナの状況の中で、我々が深く実体験として感じるようになったところです。

このようなサイバー空間とフィジカル空間の融合のドライブは、いうまでもなくデータであります。あらゆる情報がデータ化され分析可能なものとなり、膨大なデータが行き交う。そこでは、かつて自己情報コントロール権という言い方で想定していたように、利用者が自らのデータのコントロールを個別に行うことが、実質的には困難になってきているといった状況だと思えます。

また、情報が非常に急速に拡散したり収集されたりする、あるいは膨大な情報の蓄積分析の流れが、アーキテクチャーを通じたプラットフォーム事業者によって生み出されていることが、この融合を進めると同時に、さまざまな危険も生んでいます。

このような変化によって、我々の近代社会の建前である個人の自律と、その自律を守るためのプライバシー権といった考え方は、様々に動揺しています。デジタル空間上に自分たちのコピーが存在し、そのコピーに対する人々の評価によって、あるいはデジタルアーキテクチャー上の評価によって、フィジカルな自分の存在の在り方が最終的に規定されるといったことも起きてきています。

また、コロナウイルスの問題により、個人の自律の基礎となる「生存」が集合的に、しかも、どのようにリスクが発現するかがわからない形で脅かされる中で、自律よりも安全あるいは幸福を追求する動向も出始めている。

そういった「個人」が動揺している中で、デジタル化社会における我々の在り方、ここではさしあたり「デジタル現存在」という言い方をしておりますが、それに配慮するという、国家の在り方が求められると思えます。"Digitale Daseinsvorsorge" と書いておりますけれ

7

ども、平たくいえば、第二次世界大戦以降、ドイツにおいて社会保障や電気・ガス・水道といったインフラを、しっかり供給する。そういった社会国家の在り方を「存在配慮国家」と呼びましたけれども、今では、「デジタル現存在配慮」が求められているだろうと思います。

このような国家の在り方は、我々がこれまで自律と思っていた空間を、領域的には縮小させますが、しかしそれは同時に、機能的に、我々の生存や自律や自由を確保するものでなければなりません。今までの、空間的な自律の領域と国家の領域の線引きではなくて、基礎の部分は国家が自ら、あるいは国家が事業者に対して命じたり、コンタクトしたりする形で、確保し、その上の自律の領域をどのように作っていくかが、課題となります。

そういった観点から見た時に、「データのガバナンス」とその裏側にある「データの自由」だけでなく、データによって人々が自由を実現するという「データによる自由」、また、データによって国家や社会、企業の在り方が変わっていくという「データによるガバナンス」が求められていると、問題状況を捉えておくべきだろうと思います。

## データのガバナンス／自由と データによるガバナンス／自由

	ガバナンス	自由
データの	<ul style="list-style-type: none"> <li>個人情報保護法制</li> <li>プライバシー・ガバナンス</li> </ul>	<ul style="list-style-type: none"> <li>私生活の平穩</li> <li>データ基本権 (情報自己決定権・自己情報コントロール権)</li> </ul>
データによる	<ul style="list-style-type: none"> <li>ガバナンス・イノベーション</li> </ul>	<ul style="list-style-type: none"> <li>デジタル社会における個人の尊重の実現</li> <li>サービスの高度化</li> <li>民主主義社会の発展</li> </ul>

7

4象限の書き合わせで整理しますと、我々が個人情報保護法という形で議論してきたのは、データのガバナンスの問題です。逆にプライバシーの本丸である「私生活の平穩」は、「データの自由」、とりわけデータ化されない自由、「データからの自由」という側面が強かった。

もはやデータ化されることは避けられない、しかし、そのデータの流れをコントロールしたいというのが「データへの自由」であり、情報自己決定権や自己情報コントロール権といった問題群であったと思います。

現在では、そういった要請も踏まえながら、「データのガバナンス」が、それも個人情報保護法制の形式的な遵守を超えた、プライバシー・ガバナンスが企業や政府等に求められることについて、後ほどお話をしたいと思います。

また、データが活用されることによって、一人ひとりの個人の尊重がよりよく実現されたり、サービスが高度化されたり、集合的には民主主義社会が発展したりということが、「データによる自由」として挙げることができます。また「データによるガバナンス」としては、企業や政府等のさまざまな主体が自らの在り方をより良くしていく、ガバナンス・イノベーションの促進も図られると思っています。

## データの自由

	個人→社会・政府	個人・社会→政府
データによる自由 (データによる個人的・社会的利益の享受)	知る権利	報道の自由
	情報銀行	
データへの自由 (データの管理、アクセス)	自己情報コントロール権 利用停止権 (利用されない権利)	議会制度 取材の自由 情報公開
	データポータビリティ	
データからの自由 (データ化されない自由)	プライバシー (私生活の平穩)	通信の秘密 住居の不可侵
	プロファイリングの規律	
	忘れられる権利	スコアリングの規律

8

データの自由の問題についてさらに整理をさせていただきます。先ほど「データによる自由」、「データへの自由」、「データからの自由」と申し上げましたが、これまで憲法学で議論されてきた、ここでは表現の自由系の問題を含むさまざまな権利自由は、試論的な整理の域を超えませんが、個人が社会や政府に対して要求する「個対共」の領域と、個人や社会というプライベートセクター、民の側から官の側に対して求める領域とに、整理できらうと思います。

こういった観点から、昨今の個人情報をめぐる議論について見てみますと、たとえば今回の個人情報保護法改正で強化された「利用停止権」や、これはまだ導入されていませんけれども、GDPR (EU 一般データ保護規則) で重視されているデータポータビリティは、「データへの自由」を強化するものです。

それから、プロファイリングの規制やいわゆる「忘れられる権利」、スコアリングの規律は、「データからの自由」を確保することによって個人を社会的な領域から防衛する、あるいは個人や社会が政府による過度のコントロールを防ぐといった機能を持っていると思います。

それから、情報銀行、情報信託機能といった取り組みは、「データによる自由」の部分を実現するために、本人の力をサポートする機能を持っている。このように整理できると身は思っております。

## 5. 民間事業者からのデータ提供



9

ここまで駆け足で、「データの自由」「データによる自由」について若干、お話をしてきましたけれども、こういった視点を踏まえながら、With COVID-19 の教訓として、まず2つの事例について触れたいと思います。

第1は、Yahoo! Japan から厚生労働省に対して、検索結果について一定の情報提供が行われた際の経緯です。

### Yahoo!・厚労省の情報提供協定

- どのようなデータなのか？
  - 基地局情報：場所と人、粗い、ドコモモバイル空間統計
  - GPS情報：場所と人、細かい、キャリアは原則持たない
  - 検索結果×位置情報：場所と人の頭の中
- どのような文脈で取得された情報なのか？
  - このために新たに同意により取得した情報（LINE）
  - 既存の目的で取った情報の二次利用（Yahoo!）

<https://linecorp.com/ja/pr/news/ja/2020/3148>  
<https://about.yahoo.co.jp/pr/release/2020/04/13b/>



10

厚生労働省が、IT 企業に対してコロナ対策、とりわけクラスターを発見するために情報

提供を求めまして、さまざまな事業者が対応したところです。

しかし、「IT 事業者はいろいろな個人に関する情報を持っているだろう。そして、それは統計化すれば個人情報ではなくなるから出してもらえるだろう」というのは、やや安直な話でございまして、まず2つばかり注意すべきところがあります。

第1に、そこで問題になるデータが、そもそもどのようなものなのかを、整理する必要があります。

たとえば、携帯事業者の基地局情報は、いわば「場所と人を紐付けるもの」ですが、基地局情報とは基本的には粗いものでありまして、統計的に「このエリアに人がどれだけいる」、「何時から何時にはどれだけいた」には適します。ドコモモバイル空間統計は、まさにこれですが、いわゆるコンタクト・トレーシングには適さないものです。

GPS 位置情報は、「場所と人を紐付けるもの」であって、基地局情報よりも細かく当てることができそうですが、そもそもキャリアは持たないことが多いものですので、キャリアに出せと言っても仕方がないわけです。

Yahoo!に求められていたのは、検索結果と位置情報の掛け合わせでありまして、強いて言いますと「場所と人の頭の中を掛け合わせる」ものです。人の意識している頭の中と場所の紐付けがコロナ対策に有効である限り、これは有用な情報であり得ますが、それに伴う、基地局情報や GPS 情報とは異なったリスクが、この情報にはあるということになります。

## Yahoo!・厚労省の情報提供協定

- 政府のガバナンス体制は？
  - 利用目的
  - 情報の範囲、保存期間
  - 安全管理措置
  - 関係者の範囲
  - 公表の方法
  - 第三者的チェック
- 利用者保護を求められる民間企業との協定で条件がつくことに

なお、本協定締結については、ヤフーが設置するプライバシーに関する外部有識者で構成される会議体（プライバシーに関するアドバイザリーボード）（※3）の座長を務める戸川常寿教授（東京大学大学院法政学政治学専攻）から以下のようにコメントいただきました。

「ヤフーと政府の間の協定が定める統計データ提供の取り組みは、新型コロナウイルス感染症の感染拡大という現在の過酷な状況下において、有益な施策の基礎となることが期待されます。しかし、この取り組みが適正に実施されるためには、いくつかの重要な課題をクリアしなければなりません。このため、私たち『プライバシーに関するアドバイザリーボード』は、これまでヤフーに対して、さまざまな助言を行ってきました。

そのようなプロセスを経て、今般、協定の内容として、政府が提供データの利用目的を確約し、その利用の成果を適切な時期に公表すること、適正な利用が担保されない場合などにヤフーが分析結果の提供を中止できることを、ヤフーと政府が合意したことは、大きな意義があるものと、私たちは評価しています。

この取り組みの実施にあたっては、ヤフーがサービス利用者のプライバシーを十分に保護することはもちろん、ご政府において、提供データが適正に利用されることを担保するために自身のガバナンスを機能させた上で、当該データを国民のために有効に活用していくことが極めて重要です。

この取り組みは、民間企業と政府が連携したデータ利用の在り方について、今後求められる仕組みのモデルとなるという点でも、先鞭をつける試みでもあります。私たち『プライバシーに関するアドバイザリーボード』は、この取り組みが、重要な課題をクリアした上で適正に、かつ透明性を高めた形で実施されるよう、また、その他のヤフーによる取り組みも含めて、利用者の視点や利益を踏まえながら、引き続き助言を行っていきます。」

<https://about.yahoo.co.jp/pr/release/2020/04/13a/>

11

2番目に注意しておかなければいけないのは、「どのような文脈で取得されている情報なのか」ということです。LINE と厚生労働省の協力した全国調査は、まさに「全国調査のために新たに利用者から同意によって取得した情報」ですので、その意味で二次利用ではないから、問題は少ないわけです。

しかし、Yahoo!の検索結果と位置情報を掛け合わせたデータの提供を求められても、これ

は普通にやろうとすると、本来は別の目的で取った情報の二次利用になりますので、本当にそういうことをやっていいのかという問題が起きます。

それから、注意すべきは、Yahoo!が出した後で、それを政府のほうでいったいどう使うんだということが、事業者の目線からはっきりしない。どういう利用目的なのか一つとっても、公衆衛生のためというのにはあまりにも抽象的です。具体的に何をしたいのか、そのために必要な情報の範囲はどこまでか、その情報はいつまで保存されるのか、安全管理措置はどうなのか、それに触れる関係者の範囲はどこまで、公表の方法はどうなっているのか、様々な問題があります。

この右側の絵は架空の地図ですが、たとえば Yahoo!が提供した情報に基づいて、「このエリアはクラスターがいる可能性が高い」ということを政府や関係者から公表され、それが正確かどうかにかかわらず、地域における差別の問題が生じた時に「だって、これは Yahoo!から提供されたデータですから」ということを政府の方が言うということが仮にあるようであれば、これは怖くて出せないわけです。

このような公表の在り方を含めて、ガバナンスがきちんと回っているか、またそれに対する第三者的なチェックの仕組みはきちんとあるのかも問題です。そういうものがなければ、民間事業者が他の民間企業に危なっかしくてデータを出せないと同じように、政府にも出せないわけです。

そして、先ほど申し上げましたように、我が国の個人情報保護法制は、こともあろうに公的機関に対しての監視監督の体制が十分でないわけです。

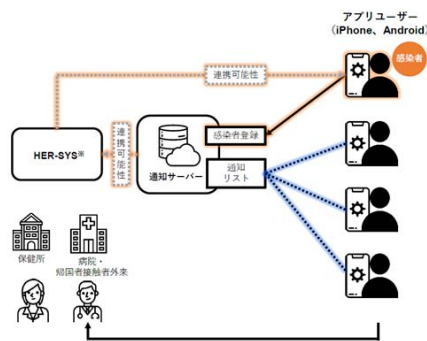
そこで、Yahoo!と厚生労働省の間について言えば、協定が結ばれて、その協定の中で、私が Yahoo!側のプレスリリースに合わせて、有識者会議の座長としてのメッセージを掲示しておりますけれども、「政府が提供データの利用目的を確約する」「利用の成果を適切な時期に公表する」「適正な利用が担保されない場合などに Yahoo!が分析結果の提供を中止できる」ということを、Yahoo!と政府が合意する。そういう形でプライバシー・バイ・デザインをいわば外から実現する形になったということは、あまり注目されておられませんけれども、この場で強調しておきたいと思います。

## 6. 接触確認アプリ

もう一つの事例は、先ほど羽深先生からご紹介ありました、接触確認アプリの問題です。羽深先生は事務局として大変なご苦勞をされて、それについてお話をすると、外から見てただけでも一日ぐらいお話ができそうですが、私から見えている論点を3つお話ししたいと思います。

## 接触確認アプリについて

- Google・AppleのBluetooth機能提供による協力
  - 端末間（人と人に近い）の接触、プライバシー配慮、本人同意
    - ⇨「国外事業者にふりまわされた」
    - ⇨アプリの利用目的（本人の行動変容、陽性者接触について通知を受ける）に「積極的疫学調査を盛り込みたい」
- 厚労省のHER-SYSとの連携可能性
  - 個人情報保護の監督監視体制が十分でない
  - アプリとの深い連携によるプライバシーリスクが評価できない→利用者への十分な説明ができない→普及の障害
- 利用者がアプリを入れるメリット？



<https://roppongi-kaigi.org/topics/2483/>

12

第1は、日本政府は最終的に、Google、AppleのBluetooth機能提供による協力に載ったわけです。これは「場所と人」ではなくて「端末と端末」、したがって疑似的に「人と人」の接触を把握する。たとえばGPSだと「人一場所一人」という形で情報を取ろうとするところ、接触確認アプリは「人と人」に近い形で、情報の扱い方としては有用です。それから、プライバシーに配慮された仕組みになっており、本人同意をベースとしていることは、羽深先生から先ほどご紹介あった通りです。

その意味で、これは有用な仕組みであるわけですがけれども、日本国内での報道等の受け止め方では、何か国外事業者に振り回されたかのような、昨今の競争政策や個人情報、消費者保護の文脈でのGAFAM叩きの延長線上のような議論がしばしば見られたのは、私は残念だと思っております。

また、アプリの利用目的は、基本的には「本人の行動変容」あるいは「陽性者接触について通知を受ける」というもの、つまり、Exposure Notification（直訳すると“曝露通知”）です。これに積極的疫学調査を盛り込めないかということが、公衆衛生の観点からはご希望があるのは当然であり、いろいろな議論がありました。

問題は、積極的疫学調査にするのであれば最初からそうするということであり、「そうでなくて、取り敢えず始めておいて、あとからなし崩し的に積極的疫学調査にも使えるようにする」ということになりますと、「結局、このアプリは何なのか？何が起きるのか」ということについてプライバシーリスクも評価できないし、打つべき手も打てない。国民、利用者に対して、きちんとした説明ができず、「安心してご利用ください」とはなかなか言えないわけです。きちんと利用目的を特定することが、議論の出発点になるということが、今回、よくわかったということなのです。

2点目は、厚生労働省の HER-SYS との連携の可能性の問題です。接触確認アプリについて有識者会議で議論している時には、HER-SYS が結局、「何をどう動かしていくのか」とか、「それに関わる保健所の方たちが、どういう研修を受けているのか」とかも含めて、よく分からないところがあります。また「事後的に HER-SYS がどのようなプライバシー上の問題を起すのか」ということについて、先ほどから申し上げていますように、行政機関個人情報保護法等では監督監視が十分及んでいないところがあります。

そうした中で、もともと COCOA で予定されている「濃厚接触者に通知を行う」という限りでの HER-SYS との連携を越えたことを、COCOA について行おうとする、ここでは「アプリとの深い連携」という書き方をしていますけれども、その場合にどういうことが起きるのが評価できないわけです。繰り返しになりますが、それは利用者に十分説明ができないということであり、普及の障害になりかねないわけです。

この点については、有識者検討会議では、もしそういうことがある場合には、また別途、検討する必要があるということを確認しております。

さらに、利用者がアプリを入れるメリットは何だろうかということです。たとえば「優先的に検査を受けられる」というメリットがまだないし、保健所のデジタル化等も必ずしも十分でない。「このアプリで通知を受けて、そこから検査を受けて、陽性である場合には病院で治療を受けて」というところまで、いわば一気通貫になっていますと、このメリットは非常にはっきりするわけですが、そうでない段階においては、繰り返しになりますが、本人の行動変容、陽性者接触について通知を受けることについて、地道に理解を得て普及を進めていくことしかないだろうと、私自身は思っています。

## 7. コロナ対策とデータ利活用の課題

### With COVID-19から見えた課題

- DFFTにはB2G・G2G（国・地方）のデータ流通が不可欠
- 「プライバシー v s 公衆衛生」等の安易な図式に逃げ込まない
- データ利活用のメリットが行政や医療サービスを通じて国民に還元されるべき
- 具体的なデータ利活用のあり方に即した、具体的なプライバシーリスクを踏まえた、様々な視点からの議論の必要



13

この二つの事例から見えた課題ですが、一つには、昨今、DFFT（データ・フリー・フロー・ウィズ・トラスト）と言われますけれども、人々が安心して信頼してデータを出して、データが流通される際にはBtoB（企業と企業）だけではなく、BtoG、そして「国から地方へ」「地方から地方へ」「地方から国へ」といったGtoGのデータ流通が不可欠であると思います。

その中で、「プライバシーを優先して公衆衛生のためにICTを使うのは諦めるべきだ」とか、逆に「公衆衛生のためという、抽象的なお題目さえ掲げれば、プライバシーは後退すべきだ」という安易な図式に逃げ込んではいけないということです。先ほどのお話では、韓国にしても中国にしても、そんなことにはなっていないことには、意を強くしたところです。

それから、何のためにデータを使うのかについて、メリットが「行政や医療サービスを通じて国民に還元される」こと、それが見えて確保されることが、重要であると思います。

特に申し上げたいのは、先ほど吉峯先生からご紹介いただきましたように、ICTを使ったコロナ対策にはいろいろなことが考えられます。しかし、それはいわば抽象的な意味でのコロナ対策へのICT利用でして、実際には具体的なデータ利活用の在り方に即して、具体的なプライバシーリスクを踏まえて、さまざまな視点から議論する必要があるということです。

今までの公衆衛生対プライバシーかといった議論は、差異を考えずに「星」と言っているようなものです。星といっても、太陽もあれば月もあれば彗星もある、遠くの北極星もあるというように全然、違うわけです。それぞれに即した議論をしていくだけの思考の強靭さを我々は持たなければいけないと思います。

## With COVID-19から見えた課題

- データ流通の基礎となる個人情報保護法制（特に公的部門の監視監督体制）の不備

※米上院の提案

“Public Health Emergency Privacy Act”

- 公益の内容・性質や実効性との複雑な比較衡量、プライバシーリスクの発見・評価、制度を適法・実効的に構築・運用できるガバナンス体制の構想

※「COVID-19データベース構想」

14

当面の課題として言えば、データ流通の基礎となる個人情報保護法制、特に公的部門の監視監督体制の不備は、重大な問題ではないかと思っております。個人情報保護法制でしっかり下支えする仕組みをつくっておくことによって、同時に強めのデータ利活用、公衆衛生の実現ができるのではないかと考えています。

ちょうど今、アメリカの上院で、ある議員が、Public Health Emergency Privacy Act（PHEPA：公衆衛生緊急プライバシー法）を提案しております。そこでも同じような考え方が取られています。そこでは、プライバシーの権利として、安全管理だけではなくて、商用利用の禁止や同意の問題、それに関わる事業者はプライバシーポリシーを公表しなさい、いらなくなったデータは廃棄しなさいといった義務が書かれています。この法案は、マニュアル的な公衆衛生上の問題には適用せず、コロナ対策に関わるデジタルな情報について規定するものですが、同時に、コロナ対策でのデータの取扱いが、人々の市民権（Civil rights）にどのような影響を与えるか、そのインパクトを計っておかなければいけないというような内容も盛り込まれています。

先ほど羽深先生からご紹介いただいた、有識者会議の評価書にも通ずるような考え方が、アメリカでもやはり取られる、そう考える人はいるということ、この法案は示すものです。これはあくまで法案の段階ですけれども、これにもまた意を強くしたところです。

それから、2点目におきましては、公益の内容性質や実効性との間で複雑な比較衡量を行なって、そのプライバシーリスクを発見・評価する。そして制度を構築したり、既存の制度に乗っかってそれを運用するとののであれば、適法かつ実効的に運用できる。そういったガバナンス体制をきちんと作っておかないと、何かあった時に、急にドタバタとやっても付け焼刃でうまくいかないということになります。

この関係で、本日、厚生労働省において COVID-19 データベース構想に関わる会議が開かれたと伺っております。ここでは、COVID-19 に関するデジタルデータだけでなく、検体も含めてデータベースとしてきっちり構築する。政府であったり医療機関であったり、研究機関、大学などでしっかりとした研究をしていくためのデータベースを作るということが、今、政府で動き出しているようです。

私が勤めている国立大学法人東京大学もそれに関わっているようですが、こういった取り組みは積極的に推し進められるべきです。同時にこのデータベースについて、ガバナンスの仕組み、あるいはそのデータベースを研究者等が利用する条件等についても、「利用する研究者、あるいは研究機関において求められるガバナンスの在り方」を議論していくことが、今後、必要になってくると思っています。

## 8. データ・ガバナンス

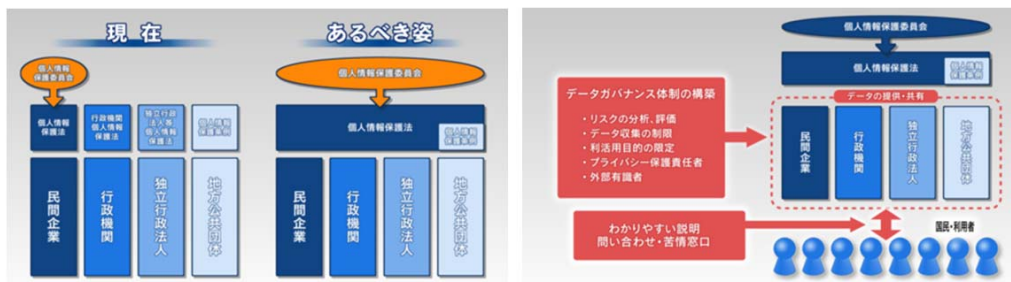


15

最後は付け足したいなものです、そういったデータ・ガバナンスを考えるうえでどういふ点が問題になるだろうかということです。

## データのガバナンス

- 最低限の統一的ルールとしての個人情報保護法制の整備
- 1事業者-1サービス-1消費者を前提とする法制からデータシェアリングを前提とする法制へ
- 複雑なプライバシー問題への対応の枠組み構築



穴戸常寿「デジタル化社会の現状と課題 ～データ活用とプライバシー保護の両立のために～」(NHK「視点・論点」7月20日)  
<https://www.nhk.or.jp/kaisetsu-blog/400/432938.html>

16

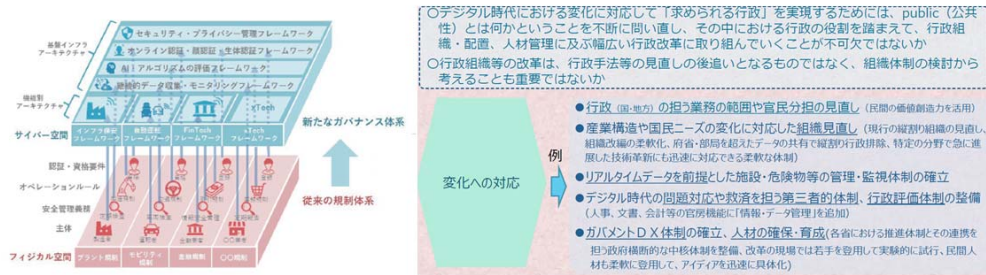
先ほどから申し上げておりますように、最低限の統一的ルールとして個人情報保護法制を整備し、公的部門、とりわけ地方公共団体等についても個人情報保護委員会の監視・監督が及ぶようにすることが、迂遠(うえん)なようですが、区画整理としてまず重要であるだろうと思います。

次に、現在の「1事業者が1消費者に対して、1サービスを提供する」という場面での個人情報のやり取りを基礎にした今の個人情報保護法制では、新しいプライバシー問題に対応できない。将来的には、BtoB、BtoG、GtoGを前提にしたデータシェアリングと、そのプライバシーリスクに応じた適切な監視監督が及ぶような法制に持っていかなければいけないだろうと考えております。

その関係では、公的部門も含めて、データを強度に取り扱う事業者・主体において、しっかりとしたデータガバナンス体制が構築されること、それが国民・利用者に分かりやすく説明されるということがあって、その主体間でのデータの提供・共有がなされるということが必要であると思っております。

# データによるガバナンス

- サイバー空間とフィジカル空間の融合を可能にする規制改革  
(左：経済産業省Society5.0における新たなガバナンスモデル検討会報告書)
- ネットワーク空間の公共性を考察し、規制改革を実現しよう、  
データを利活用した行政改革・公務員改革  
(右：行政改革推進本部デジタル時代における今後の行政改革の基本的方向性(仮)中間報告書案)



<https://www.meti.go.jp/press/2019/12/20191226001/20191226001-3.pdf>  
<https://www.gyokaku.go.jp/houkousei/index.html>

17

そうやってデータが使えるようになれば、「データによるガバナンス」になりますけれども、さらにサイバー空間とフィジカル空間の融合を可能にするような規制改革を進めていくことも可能になるでしょう。

左側に示したのは、経済産業省の「Society 5.0 における新たなガバナンスモデル検討会」の報告書です。こちらにも羽深先生が事務局として、非常にご苦労されているものですので、ぜひご一読いただければと思います。また、公的部門のガバナンスと言えば、ネットワーク空間の公共性を考察し、規制改革を実現し得るような行政改革、公務員改革が求められます。右側は、行政改革推進本部でそのような方向性の議論がなされていることのご紹介です。

在野の法曹の方々も、たとえば公務員になる、あるいは「公・共・私」の「共」という形で関わっていただいて、議論をリードしていただいことも必要ではないか。現在、CivicTech、GovTech、LegalTech として議論されているものの、より高次のバージョンとして求められるようになってきている時代ではないか、ということをお願いして、私からのプレゼンテーションとさせていただきます。

ご清聴ありがとうございました。