# 空港における AI 活用事例，社会に広がる DX！

# AI・データサイエンスのビジネス化と直面するリスク

## （日立ソリューションズ・早稲田大学データ科学センターセミナーパネルディスカッションより）

（文責：早稲田大学データ科学センター　小林学）

## ■ はじめに

早稲田大学と株式会社日立ソリューションズ（以下，日立ソリューションズ）は，データサイエンス分野の人材育成や産学連携促進を目的とした学術交流協定を締結しており，連携の一環として，2022 年 3 月 9 日に「AI・データサイエンスのビジネス最前線と未来社会が直面するリスク」と題したオンラインセミナーを開催致しました．セミナーでは，講演①として日立ソリューションズの熊谷仁志氏から「空港の X 線検査への AI 活用事例」をテーマにご講演いただき，続いて，講演②として，本学社会科学総合学術院横野恵准教授より「(行動データを中心とした）最新のデータ倫理・ガバナンスに関する議論や研究のご紹介」についてお話いただきました．

講演後に行われたパネルディスカッションでは，セミナータイトルである「AI・データサイエンスのビジネス最前線と未来社会が直面するリスク」について様々な角度からそれぞれの専門性を活かした非常に深い議論が行われました．ここでは，パネルディスカッションの様子をご紹介致します．

パネルディスカッションのメンバーは以下の通りです．

| | | |
|---|---|---|
| モデレータ | 早稲田大学 データ科学センター教授 | 小林　学 |
| パネリスト | 株式会社日立ソリューションズ | 扇　　健一<br>米光　一也<br>熊谷　仁志 |
| | 早稲田大学 社会科学総合学術院准教授 | 横野　恵 |

## ■ AI・データサイエンスのビジネス化におけるステークホルダーの関係性

**小林：**

パネル討論のテーマ「AI データサイエンスのビジネス化と直面するリスク」では，この後の議論がわかりやすいように簡単な関係図（図１）を作りました．

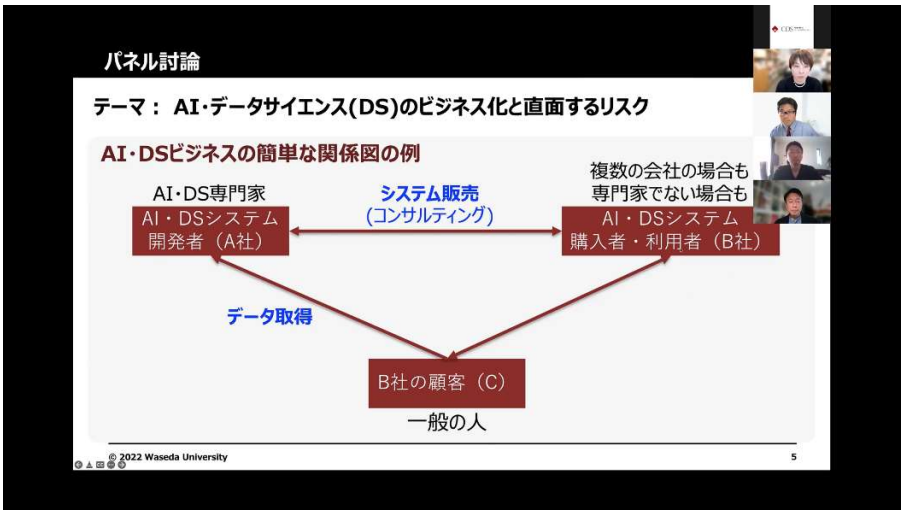


図 1

AI とデータサイエンスのビジネスでは，図 1 で示される関係性が多いように思います．図 1 ではまず，AI やデータサイエンスの専門家集団である AI データサイエンスシステムを開発する人，あるいは会社を A 社とします．また開発された AI データサイエンスシステムを導入し，利用して，企業活動をする会社を B 社としています．さらにこの B 社を利用する顧客を C としています．

図 1 では B 社は 1 社ですが，実際には複数の会社やステークホルダーで B 社が複数の会社からなるような場合もあります．また，B 社は AI やデータサイエンスの専門家でない場合も多く，専門家が作ったものを利用する立場である場合も多いです．

A 社はシステムを販売しコンサルティング業務を請け負い，AI やデータサイエンスによる分析結果を提供することもあります．そのときに一般の人 C のデータを，実はシステムのフィードバックに使ったり，あるいはシステム開発に使ったりすることがあり得る．このような関係性が成り立っているケースが多いと思います．本日はこの関係図を基に，ビジネス化や直面するリスクがどういった形であり得るのかということを考えていきたいと思います．

## ■ AI・データサイエンスのビジネス化の課題

**小林：**

先ほど熊谷様のご発表で，AI を使うときの課題として挙げていただいたものも含めて，ビジネス化の課題を図 2 に示します．

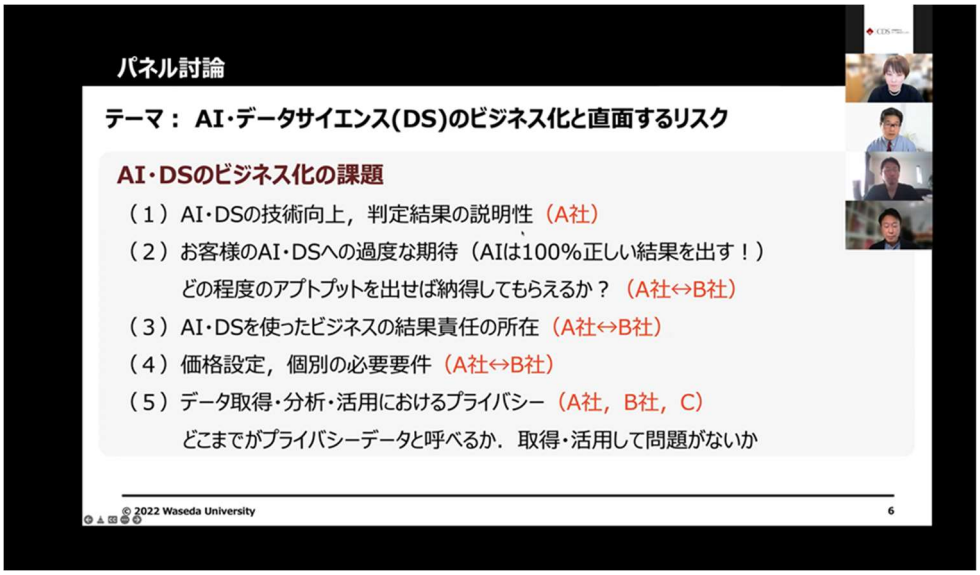


図 2

**熊谷**：

図 2 の（1）から（5）をそれぞれ説明します．

(1)「AI・DS の技術向上，判定結果の説明性（A 社)」

実業務では，新商品のように AI が未学習のものに追随していく必要があり，技術向上が必要です．未知のものに対する判断は人が圧倒的に強いです．AI は学習したものしかわかりませんので，精度向上・学習し直しが必要なこともあります．

判定結果の説明性については，例えば，システムのテストをした際になぜ誤認識したのかなど，主に導入時にお客様から説明を求められますが，説明が難しいというのが現状の課題です．

(2)「お客様の AI・DS への過度な期待（AI は 100%正しい結果を出す！)」

これは我々も課題として捉えています．お客様の中には，一般的な工業製品と同じ感覚で AI を捉えている方もいらっしゃいます．例えば AI で 90%検知できることをお客様に説明して導入していただこうとしても，残りの 10%に致命的な見逃しなどがあったらどうするんだということで議論になります．そうするとどうしても 100%でないと駄目だという結論になりがちです．

(3)「AI・DS を使ったビジネスの結果責任の所在」

現在我々が扱っている「X 線検査判定支援ソフトウェア」の AI に関しては，サービス提供元の B 社に判断の責任を負っていただいています．製品としても判定ソフトウェアではなく，人の判定を支援するソフトウェアと説明しています．

今後技術が進化して AI が人の代替となっても，基本的に契約で責任の所在を明確化することが必要になると考えています．現在先行している自動運転の評価の基準などが参考になるのではないかと考えています．

(4)「価格設定，個別の必要要件」

価格設定については，このAIがいくらという値付けにはなっていません．AIのシステムでは，個別の要件に応じたオーダーメイドが多いです．そのため，X線に限ったニッチなAI利用においても，お客様によって少しずつ条件が違うので，学習モデルや個別のカスタマイズを行う必要があります．メーカーとしては全て同じものであれば効率的ですが，そうはなってないのが現状です．

(5)「データ取得，分析活用におけるプライバシー」

X線の画像がプライバシーを侵すかどうかといった点は，まだ深く議論がなされていません．個人情報ではないと思いますが，どのように折り合いつけるかというところが課題です．個人情報や，プライバシー，知的財産権などを配慮した上で，データを活用できるかできないか，お客様や関係各社と協議して契約で決定しておく必要があります．現在は，図1のA社・B社との間でX線データに関してやりとりしているという状況です．

**小林**：

具体的なイメージがつかめてきました．ありがとうございます．

次の質問です．図2の（2）と（3）の課題について，B社にはどのようにご説明されるでしょうか．これは，セキュリティにおける課題とも比較的近いのではと思っています．セキュリティに関してもお客様は100%セキュリティが担保できるのか，セキュリティが破られたときにあるいは何らかの欠落があったときに，責任の所在はどちらかという点を考えると，AI・データサイエンスとセキュリティに関しては，(2)，(3)については関連があるように思っています．

セキュリティの専門家であり，企業の立場として，日立ソリューションズの熊谷さん，扇さん，米光さんにお伺いしたいと思います．まずは熊谷様から紹介いただいた事例の場合にどうしているかご説明をお願いします．

**熊谷**：

わかりました．(2)「AIの100%神話」と(3)「責任の所在」について，特に(2)には，明確な答えがない問題ですが，現在，お客様にどのように説明しているかお伝えします．100%を求める方々にいくら数字を語っても響かないので，「人との比較」をご提案します．保安検査では100%の精度で検査を行っていると思いますが，場合によっては，時間をかけないと見つからないこともあると思います．ですので，同じ条件でAIと人を並べたときに，人を100%としたときにAIが人と同程度の精度であることを示します．

何度か人とAIの対決をしたことがありますが，「正解が10個あるうちの何個見つけるか」というテストに対して，AIは人と同程度の結果を出すことができます．ただ，AIと人が明らかに違うのは，AIは数打てば当たる的なところがあって，正解率は高いけれど誤認識も多いという傾向があります．

それに対して，人は見逃すことはあっても誤認識が少ないという傾向があります．AIの正解率と誤認識のバランスを見ながら，人と同じくらいの精度が出るところで納得していただくこと

が多いです．同じくらいの精度であれば，実際の現場で支援できる結果を得られることが多いためです．

(3)「責任の所在」については，「完璧です」といって売れれば良いかもしれませんが，そこまで過信はしていません．あくまで目的は支援という位置づけですので，B 社さんに責任を持っていただきます．自動運転のレベル 2 と同様のイメージだと思っていただくと良いと思います．人が基本的には責任を持つといったところで折り合いをつけているのが現状です．

**小林**：

ありがとうございます．扇様，セキュリティにおいてはいかがでしょうか．

**扇**：

はい．セキュリティも同じというお話がありましたが，まさにその通りです．セキュリティに対しても昔から 100%を求めている人がいました．ですが，最近では各企業においてセキュリティを担当する部署や人がおり，セキュリティは 100%ではないことを理解してくださっている人がかなり多くなっているのが実情です．マルウェアやランサムウェアが猛威を振るう中で，セキュリティ対策に AI が活用されています．マルウェアの分析や攻撃の分析においては，データもかなりの量がありますので AI の活用が欠かせません．

しかしながら，一部では，セキュリティ対策にも 100%を求められるお客様もいらっしゃいます．その場合，実際の落としどころとしては 98%，99%ぐらいでチューニングしてご提供しています．ただし，お客様の環境によって，そのパーセンテージはどうしても変わってきます．マルウェアはファイルですので，お客様が多く保持しているファイルがどのようなものかによって，合う分析方法が変わってきます．お客様の環境に合わせて検知率を上げるようにチューニングすることを考えます．検知率を上げて限りなく 100%に近づけるチューニングというのもできますが，その分の誤検知が多くなります．100%に近づければ検知に要する手間は減りますが， 誤検知したものを捌く手間は増えますね．そのため，お客様に検知率，誤検知率のバランスをチューニングしていただき，どのくらいがちょうどいいのかを試してもらう方法をとっています．

AI は人と比べてものすごいスピードで判定します．セキュリティ対策では，マルウェアや攻撃に対して人が判定していたら間に合いません．AI が貢献できる力があると思います．しかしながら AI が苦手な部分もあるため，検知の支援といった AI が得意なところを AI に任せると良いと思います．

責任の所在については，プログラムの不具合の責任は取りますが，AI の能力に関する責任は取れず，あくまで支援をする形でしかないと思っています．

お客様によってはマルウェアと判断した根拠を求めたり，誤検知をした理由の説明をもとめられたりする場合もありますが，AI がどのような方法でデータを収集して分析し，判断しているかといった仕組みをお伝えしています．AI の支援する力を認めてほしいですね．責任の所在は，結局は人になると思います．

**小林**：

ありがとうございます．よくわかりました．それでは米光様，お願いします．

**米光**：

はい．扇さんの言う通り，セキュリティも過去 15 年前ぐらいは AI と同じような課題がありましたが，この 15 年を経て，社会的な総意が取れてきていると思います．これは，「社会はミスに対してどこまで許容するのか？」という空気みたいなものが，かなり関係していると思っています．

例えば，今の AI の問題も「AI だから仕方がない」というのが，どこまで許されるのか，そういう社会かどうかというのは，(2)と(3)の点では重要なので，セキュリティと同様に，この先 15 年ぐらいで，どこかに収斂していくと個人的には思っています．

あとは，対象のシステムですね．「皆さんが受けたテスト結果を AI が判定して，本来よりも 5 点低い採点をされてしまいました」といった問題を，学生の皆さんは，どう受け止めるのか，という話です。手術などの健康に関わるところでは，ミスは 0 にしたいでしょう．AI はどの分野なら適用できるのか，どこまでは許されるかという話だと思っています．ただ，AI がセキュリティと大きく違うのは，15 年前のセキュリティの問題の時は，代替手段がありませんでした．例えばコンピューターにマルウェアが感染するという脅威に対して，対策が 100%であろうがなかろうが，感染するくらいなら 80%の対策を入れなくてはいけないという状況でした．

ところが，AI で解決できる問題は，別の解決手段もいろいろと残されていることが多く，そういう意味で日本のような慎重な判断をする文化の国は，なかなか AI が広がりにくく，逆に海外だと広がりやすいギャップをすごく感じますし，このようなカントリーリスクがあるな，ということは聞いていて思いました．

**小林**：

ありがとうございます．非常に明確になりました．

セキュリティに関しては代替手段もそうですが，ないとどうにもならないという状態が先にあり，100%でなくても受け入れざる得ない状態が起こって，それを受け入れる上でどこまで精度を上げるべきかという議論になっています．今の AI に関してはまだそこまでできていないので，これから議論が起こると思いますが，セキュリティの例を考えると，必要性と重要性が明らかになっていく中でおそらく社会がそれを受け入れる形になっていくのではないでしょうか．

最後の米光様のお話で，分野ごとの許容範囲は起こってくると思いました．ただ便利なもの，要は音声認識といった，少し言葉を間違えたのは許せるけれども，手術などで間違いは許されないでしょう．そのトレードオフをどうするのか議論は残ると思いますが，必要性と重要性の議論は明確になったかなと思いました．ありがとうございました．

価格設定については個別の案件になってくると思いますので，　もう 1 つの議題に移りたいと思います．

## ■　行動データのプライバシー保護

**小林：**

本テーマは主題でもありますが，プライバシーはセキュリティにも大きく関係すると思います．プライバシーデータの特に行動のデータについて考えていきたいと思います．

行動のデータや顔画像のデータなど，個人の情報が含まれるようなデータの取得・活用に関して議論をしたいです．活用すべきだという議論もあると思いますし，顔画像や個人情報を取られるのが嫌だという人ももちろんいると思います．先ほどの X 線検査の話をお聞きして，私は過去の鉄道の事件を少し調べてみました．この参考の URL（『日本の鉄道に関する事件 - Wikipedia』※1）を見ると，日本の鉄道に関する事件が一覧として出てきます．日本は世界の中では安全な国だとは思うのですが，とはいえ，実は鉄道に関する事件がかなり頻繁に起こっています．

ここで大きなものを 4 つぐらいご紹介します．新しい事件ですと，京王線の刺傷事件があります．これは 2021 年 10 月 31 日に起こりました．この事件は 24 歳の男性が刃物で他の乗客を切りつけて，液体をまいて放火し，18 人が重軽傷を負ったという事件です．事件を受けて新規の全車両において防犯カメラの設置を義務付ける方針を固めたことが書かれている点です．防犯カメラを設置するだけでこういった事件を未然に防ぐことができるかというと，すこし疑問に思うこともあります．

さらにその前の 2021 年の 8 月には，小田急電鉄の小田原線の車内で無差別の刺傷事件が起こっています．乗客の 20 才の女子大生が重傷を負ったほか 10 人がけがをした事件です．2018 年には，新幹線の中で殺傷事件が起こっています．のぞみ 256 号においてお客さん 3 人に対して，なたで切りつけて 1 人を殺害したという事件や，あるいは 2015 年にはのぞみ 225 号で，自分でガソリンをかぶって火をつけて，火災が発生した事件がありました．

この 4 つの他にも先ほどの URL での一覧を見ると結構載っています．こういうことを考えていくと，安全保障上，先ほどの防犯カメラをただつけるという抑止力で済むのかという話になります．こうした鉄道に関する事件の対策を考えると，鉄道に限らず，例えばイベント会場や遊園地なども，ある意味同様に考えることができるのではないかと思います．先ほどの AI 化による手荷物検査の実施についても当然考えることができると思います．実際に鉄道を考えたときに，中国では手荷物検査， 中国の駅の入り口， 特に北京の地下鉄では駅で X 線の手荷物検査を行っています． これを AI 化するということも考えられます． あるいは動作認識技術・行動追跡技術などを考えて，危険人物の抽出や検知などを何らかの技術で行うことも可能になっていくだろうということで，技術的な可能性はある訳です．そうすると AI・DS によって低コストで安全性を確保できる可能性があろうと思います．これはほんの一例です．

議論を進めるにあたり，まずここで皆さんにアンケートにご協力いただきたいと考えています．参加者の方には OK・NG をアンケートにお答えいただければと思います．

1 つ目が，AI 手荷物検査データの取得は，（手間も含めて）皆さん OK ですか，NG ですかです．次に，民間企業による顔画像や行動履歴等における個人データの取得利用は，この公共の安全のためであれば OK ですか．プライバシーということなので，顔画像や行動履歴等の個人データが OK か NG か．この２つをお答えいただければと思います．

【アンケート１】

民間企業による AI 手荷物検査データ取得は「OK」or「NG」？

【アンケート１結果】

OK　：　86．4%

NG　：　13．6%

**小林**：

86%が OK．結構多いですね．

では，次に．顔画像など行動履歴等の個人データの取得利用などは OK か NG かについてアンケートお答えください．

【アンケート２】

民間企業による顔画像や行動履歴等の個人データ取得・利用は「公共の安全のためなら OK」or「NG」

【アンケート２結果】

OK　：　41．9%

NG　：　58．1%

**小林**：

こちらは NG の方が結構増えてきましたね．

手荷物検査が OK の方が 80%以上いて驚いているのですが，2 番目の質問の個人情報の取得の方は NG が増えてきている，そういう状況ですね．ありがとうございます．少し，さきほどの私の言い方がきつくなってしまったでしょうか．事件の話を前面に出しすぎて，ミスリードしてしまったところがあるかもしれませんが，個人情報を取得するということが，今，事件の話をしたので安全面を重視して考えたということもあろうかと思いますけれども，個人情報のデータの取得に関しての半分ぐらいは OK という話が出てきていました．この結果をもとに，パネラーの方に，ご意見を伺ってまいります．

**扇**：

手荷物検査，私は OK にしました．安全確保のためにする方がいいと思います．普通に考えて，空港，遊園地を含めいろいろな重要な施設に入るときには，検査されるのは分かっているのではないでしょうか．コンサート会場などもそうです．ですから，軽装でいったりするのではないですか．検査されたから何か感じるかというと，　私は当然だと思って受けています．

**小林**：

行動追跡に関してはどうですか.

**扇**：

行動追跡に関しては，私はNG，嫌です．これまで，マイナンバーなども漏れる漏れないという議論がありましたが，発行された瞬間から漏れました．届け先が間違ったなど．あり得ないですよね．民間企業に任せた場合にそういったことも起こり得ますので信用していないです．クレジットカードなども，安全のためにセキュリティコードがカードの裏に書かれていますね，それを使えば安全になると思われていたものが，最近だと，クレジットカード番号もセキュリティコードも両方漏れていますから，全く意味がないです．というのは，民間企業では，予算や経営層の考え方で，セキュリティに関する考え・対応が変わってくるためです，いいづらいことですが，ここでは厳しく言わせていただきます．顔をハッシュ値化，非可逆性のデータに変えて保存してもらう．何かがあったときには本人の写真など画像から同じハッシュ値というのを出してマッチングさせて調べる，というぐらいが限界ではないでしょうか.

**小林**：

わかりました．個人情報はそれだけだと特定が難しいデータにしておくことですね．ありがとうございます.

## ■ 行動データ等の取得・利用事例

**小林**：

ここで横野先生のご専門でいらっしゃるので，国内外の顔データや行動データ等の取得や利用等において問題になる，あるいはなったようなケースがありましたら教えていただけますでしょうか.

**横野**：

はい， 画面共有させていただいてもよろしいでしょうか.

私達がやっているプロジェクトでそういう情報を集めていますので， ご紹介させていただきます．このWebサイト（『DATA ETHICSプロジェクト　データ倫理最新情報』※２）ですが，ここにいろいろな個別トピックに関する情報を集めていて，位置情報，あるいは顔認識の技術を使った，あるいはHRTechと人事に関してこういったものを使うということについてです.

この顔認証，顔認識については，いろいろございます．基本的には直近で一番日本の中で議論されたものは，ここまでに議論に出ていたものにも関係しますが，顔認証ではなく顔認識だと思うのですけれど，JRが顔認識の機能を付けた防犯カメラを設置していたということで，これがこういう報道が出た後に，短期間のうちに中傷されたということなのですが，基本的には海外では規制の話がかなりされていて，日本では顔認識について，どういうルールのもとで使っていくのかということについて，まだ十分な議論をしていないという認識でいます.

参考になるものとしてこの中でも紹介していますが，この Web サイト（『あまりにも未熟な日本の「顔」画像利用の議論』（※３））辺りを見ていただくといいのではないかと思います.

それと先ほどのアンケートの件について， 少しコメントさせていただいてもよろしいでしょうか. アンケートで，民間企業による AI 手荷物検査で，データ取得は OK・NG かという設問になっていて，これが何を意味するのかによって大分違ってくると思います．そのときに荷物検査をして，それが付随するデータとともにストックされていくのか，それに対してまたいろいろな解析を行って，このアンケート２にあるようなハイリスクかどうかということを判断するための何らかの解析をするのかどうかによって全く違う話になると思います.

この２つの話，アンケート２の話もそうなのですが，これはその技術としてどうかという話よりは，セキュリティに関してどういうポリシーを取るかという話が本質だと思います.

スライドを共有させていただきたいのですが，空港の話もそうですが，セキュリティ対する考え方として，ルールベースでも，最初の話の中にもあったルールベースは，データサイエンスでいうルールベースとは違っていて，セキュリティに対してルールベースで考えるかリスクベースで考えるかという話がございます.

ルールベースは，手荷物検査ですと，こういうイメージがあると思うのですが，全例に対して一律の検査や審査を行う，その中で特に問題がある慎重な対応を必要と判断されるものが検知される場合もあるが，そういう場合を除きリスクは同程度にみんな持っているというような前提から入る，それがデフォルトのあるルールベースです.

これに対してリスクリベースは，個別のリスク評価がデフォルトであり，その評価に応じて異なる厳しさの検査を行うのはリスクベースということになります.

日本においてよくあることですが，技術を使ってどうしたいかということは，本当はこの大本のポリシーをどう考えるのかという問題である場合がとても多いと思います．もちろんこのルールベースとリスクベースは，両者排他的なものではなくて，ルールベースの場合にも，最初のお話あったように，経験の蓄積などそういうものによってリスクの判定が一定程度行われている，ただそれはインフォーマルな形式だし，全員に対して同じように事前にリスク評価を行うという前提ではないというところが違います.

その技術を用いるということの裏には，政治的ないし社会的な方針の原理原則の変更が実はあると思うのですが，そこに目を向けられずに，そこでどういう方針を取るのかということが曖昧にされたままに技術を導入するということにのみに着目をされてしまって，本来この部分でどういう考え方をとるかによって，その技術をどう使っていくかということも違ってくると思います.

先ほどの 100%を求める方もいらっしゃるという話がありましたが，100%が達成できたとしたら，完全にオートメイティッド・ディシジョン・メーキングしたいというご要望があるかかどうか．また，リスクベースのアプローチを用いた場合には，全員に基本あるいはその幅広く個別のリスク評価をするということが発生してきて，そこでそのデータテクノロジーを用いたリスク評価の方法を導入するかどうかは，基本的にはそういう整理になると思います．そこでプロファイリングなど，あるいはその自動化された決定というように GDPR と呼ばれるようなものが方法としては選択肢となり得ますが，これは無前提に導入していいものではなく，GDPR 等ではこ

れは具体的に規制をしています.

もちろん全く使ってはいけないということではありませんが，それを使う場合には一定の条件である，あるいは場合によっては代替措置を設けて，そういったものを選択することができるようにするということが条件になっています．そこで目指しているものが何なのかということです．それが政治的，社会的な意味での方針変更に関わるものかということと，そこがクリアになった上で，その技術そのものの問題としてプロファイリングなど自動化された決定というものにそれが当たるのであれば，正当化できる範囲での利用なのかどうかということを考える必要があるのではないかと思います.

話が飛んでしまいましたが，関連することをまとめてコメントさせていただきました.

**小林**：

ありがとうございます．行動履歴データを含めたデータのプライバシー保護，並びにそのデータ利用に関して，非常に明確になったと思います．非常に有益ですね．こういったことを知らないでシステムなりビジネス化するときに，会社側としては，今度非常に大きなリスクになってしまうということも含めて考えないといけないということでしょうか．非常に勉強になりました.

行動履歴というところで，先ほど扇様の方でもハッシュ化するよう，個人が特定できない形は必須じゃないかという点も議論としていただきましたので，誰かを特定してどうこうというよりかは，やはり，どういう行動がリスクに繋がるのかということを，特定の誰かというよりかは目的として，安全保障上だったら安全保障上に対してどういう形でそれを使えばいいのかという，その根本に戻ってちゃんと考えていかなければならないということですね.

## ■ 行動データ等の利活用に対する課題

**小林**：

最後に，今後おそらくスマートフォンや防犯監視カメラや，電子決済，IoT 機器等々において，データはどんどん取得されていき，さまざまなビジネスに活用され始めているのは事実だと思います．特に行動の履歴のデータのようなものに関して，皆さんのお考えをお聞きしたいと思います.

**熊谷**：

私個人の意見では，データが使われることは，いたしかたがなく，あとは程度の問題であろうと考えています．例えば，情報提供に見合う価値のあるサービスであればいいと思います．今でも携帯電話の位置情報など取られていると思いますが，そういうものはメタデータとして使われていて，例えば私が街中で倒れてこの人が誰だかわからないとなったときに，これは熊谷だとわかるような認証技術はありがたいと思います．ただ先ほどのお話にあったように，行動データを勝手に取られていて，誰か知らない人がそれを見てるというのは気持ちが悪いので，そういうのは嫌だと思っています.

**扇**：

そうですね. 私は, 将来的には個人で全部管理できるようにしてほしいという思いがあります. 情報を取ったとしても，どこに情報を与えるか，削除などのコントロールは全部個人でできるようにしてほしいと思います．そうなると今，総務省などで考えられている情報銀行という仕組みでしょうか，とても強固なシステムの中に個人情報を入れておいて，そこから，各企業がデータを取得できるかできないかを個人がコントロールするという形にすれば，許せるといったところでしょうか.

**米光**：

私はプライバシーよりも，データの利活用を優先したいというスタンスですが，先ほど横野さんのおっしゃった，問題のどこにフォーカスするかによって確かにアンケートの結果の捉え方は結構変わります．アンケートを取った時の話の流れだと，電車の中に監視カメラをつけて犯罪を防ぐとか，遊園地の中でも同様に犯罪を防ぐというような使われ方の話の流れの中での質問だったので，先ほどの OK と回答した 42%という学生さんの割合は，結構高い数字だと思いました．どちらかと言うと，私のスタンスはマイノリティーだと思っていたので.

あと横野さんのお話の中の「100%を求める」の話は，ほぼ責任の問題（1%であってもミスが起こった時に誰がミスの責任を取るのか，という問題）のことを気にされての発言ですね.

**横野**：

そうですね．私としてはいろいろデータを活用して便利になっていく，イノベーションが起こっていくということは，基本的には歓迎をしています．ただ，先ほども触れたのですが，それは単なる技術的な問題ではなく，基本的な価値など社会の中でのルールそのものを変えないといけないような意味を伴うものである場合もあると考えています.

顔認識の問題などはそのような側面があると思うので，基本的にはルールをきちんと作りながらやっていくことが重要で，ルールが明確化されていない中でどんどん使っていくのは，すごく不安があると思っています.

また，ルールが作れない中でどんどん先に進んでいくと，日本では起こりづらいと思うのですが，ある程度枠組みを作っておかないと実際の方が先行したときにそれがコントロールできなくなってしまうということは常に思っています．ですので，ルールを作るということも含めながら，そういったものの開発や実装を行っていくということはやはり重要だと思っています.

**小林**：

ありがとうございます．技術の進み具合と，データ倫理，あるいはそれの法整備や，ルール作りが同時進行で進んでいる訳ではないというところに大きな問題があるということですね．こういった議論そのものがおそらく重要で，こういったところからルール作りの必要性や，あるいはどういう形であれば使っていいのかというコンセンサスを社会的に醸成する必要性があるということでしょうか

今回の議論はすぐ答えが出るものではないですが，ビジネス化するときにはこれらも含めて全体を考えて答えを導くようにしていかざるを得ないということが非常に参考になりました．

皆さんどうもありがとうございました．以上でパネル討論は終了します．参加者の皆様にもお礼申し上げます．どうもありがとうございました．

**[参考文献]**


※１　日本の鉄道に関する事件

出典：フリー百科事典『ウィキペディア（Wikipedia)』　2022 年 3 月 9 日参照

URL：

https://ja. wikipedia. org/wiki/%E6%97%A5%E6%9C%AC%E3%81%AE%E9%89%84%E9%81%93%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E4%BA%8B%E4%BB%B6

※２　DATA ETHICS プロジェクト　データ倫理最新情報　2022 年 3 月 9 日参照

URL：

https://dataethics. jp/resource/resource_category/06/

※3　あまりにも未熟な日本の「顔」画像利用の議論　2022 年 3 月 9 日参照

URL：

https://note. com/nfi_japan/n/n171811f65949