【イベントレポート】MyData Japan 2025 カンファレンス

AI・データ活用の進展と求められるガバナンス

はじめに

AIやデータの高度な利活用が進む中で、イノベーションを創出する中心的存在である企業には、適切なリスク管理、自主的なガバナンスが求められています[1][2]。他社とのデータ連携による新たな価値創出に向けた取組も進められ、データのライフサイクル全般のガバナンスや、安全なデータ連携を可能とする技術的な手法（プライバシー強化技術(PETs：Privacy Enhancing Technologies)についても、議論が進んでいます。

2025年7月17日に一橋講堂で開催された「MyData Japanカンファレンス2025　～MyData in Practice～」[3]にて、AI・データ利活用やガバナンスに先駆的に取り組まれる企業、事業者団体、有識者、政策担当者の方々に、AI・データ利活用の現在地と、今後企業に求められるガバナンスのポイントについて情報発信、ディスカッションをいただきました。

登壇者

経済産業省　商務情報政策局　情報経済課　情報政策企画調整官	永野　志保氏
一般社団法人AIガバナンス協会　理事	佐久間　弘明氏
プライバシーテック協会　事務局長	竹之内　隆夫氏
KDDI株式会社　Data&AIセンター プライバシーガバナンスグループ　グループリーダー	山崎　晃弘氏
PwC Japan有限責任監査法人　リスクアシュアランス部　パートナー	平岩　久人氏
池田・染谷法律事務所　弁護士	今村　敏氏
モデレータ：一般財団法人日本情報経済社会推進協会　電子情報利活用研究部 主幹	恩田　さくら

[1]「AI事業者ガイドライン（第1.1版）」（経済産業省・総務省、2025年3月）
[2]「DX時代の企業のプライバシーガバナンスガイドブックver1.3」（経済産業省・総務省、2023年4月）
[3]「MyData Japan 2025 ～MyData in Practice～」Webサイト

1.AI活用の取組とガバナンスの現在地

はじめに、AI活用の取組とガバナンスの現在地について、事業者の自主的な取組を支援する政策の観点（1-1）、事業者の実際の取組の観点（1-2）から情報提供いただきました。

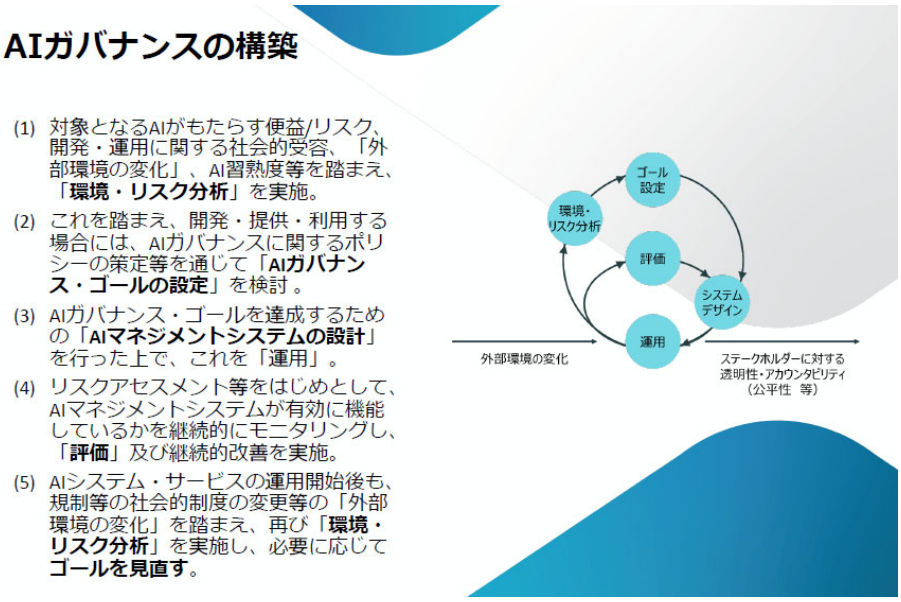
1-1. AIガバナンス関連施策の最新動向（経済産業省 永野氏）

講演資料

AIのガバナンス

経済産業省、総務省は、2024年4月に「AI事業者ガイドライン（第1.0版）」を取りまとめました。最新の動向を踏まえ、その後もリビングドキュメントとして更新しております（2025年3月に第1.1版に更新）[4]。このガイドラインは、AIに関係する事業者が、国際的な動向及びステークホルダーの懸念を踏まえたAIのリスクを正しく認識し、必要となる対策をライフサイクル全体で自主的に実行できるように後押しし、イノベーションの促進及びライフサイクルにわたるリスクの緩和を両立する枠組みを、関係者と連携しながら積極的に共創していくことを目指して策定されました。

このガイドラインは共通の指針を示しつつ、AI開発者、提供者、利用者ごとに取り組むべき事項を整理しています。ガイドラインの中には、AIガバナンスの構築についても示しています（下図）。



（出典）永野氏登壇資料

また、バリューチェーンにおける、AIガバナンスの留意点も2点挙げています。

1点目は、バリューチェーン/リスクチェーンの観点で主体間の連携を確保することです。複数主体にまたがる論点の例としては、AIリスク把握、品質の向上、各AIシステム・サービスが相互に繋がることによる新たな価値の創出、AI利用者や業務外利用者のリテラシー向上等が考えられます。また、主体間で整理が必要になりうる点の例としては、学習や利用に用いるデータや生成されたAIモデルに関する権利関係の契約等が考えられます。

[4]「AI事業者ガイドライン」（経済産業省Webページ）

2点目は、データの流通をはじめとしたリスクチェーンの明確化や、開発・提供・利用の各段階に適したリスク管理及びAIガバナンス体制の構築を実施することです。複数国にまたがるデータの流通に関しては、DFFT（Data Free Flow with Trust）の確保など国際的な取り決めにも留意しなければなりません。

また、バリューチェーン、サプライチェーンの事業者間の契約については、経済産業省で、今年2月に「AIの利用・開発に関する契約チェックリスト」[5]を公表しましたので、参考にしていただければと思います。

プライバシーデータのガバナンス

経済産業省、総務省は、プライバシーデータのガバナンスについても検討してきました。

プライバシーに関する問題については、個人情報保護法を遵守しているか否か（コンプライアンス）を中心に検討されることが多かったですが、法令を遵守していても、本人への差別、不利益、不安を与える等の点から批判を避けられず、企業の存続に関わるような問題として顕在化するケースも見られます。企業は、プライバシーに関する問題について能動的に対応し、消費者やステークホルダーに対して、積極的に説明責任を果たし、社会からの信頼を獲得することが必要となります。経営者は、プライバシー問題の向き合い方について、経営戦略として捉えて対応し、企業価値向上につなげることが重要です。

プライバシーガバナンスの構築に向けて、企業がまず取り組むべきことをプライバシーガバナンスガイドブックとして取りまとめ、2020年8月に初版を公表、2023年4月に1.3版として改訂しました[6]。

ガイドブックの中では、経営者が取り組むべき3要件として、1.プライバシーガバナンスに係る姿勢の明文化、2.プライバシー保護責任者の指名、3.プライバシーへの取組に対するリソースの投入、を挙げています。また、プライバシーガバナンスの重要項目として、1.体制の構築、2.運用ルールの策定と周知、3.企業内のプライバシーにかかる文化の醸成、4.消費者とのコミュニケーション、5.その他のステークホルダーとのコミュニケーションを紹介しています。

1-2. AIガバナンスの現在地点とプライバシーガバナンスとの関係（AIガバナンス協会 佐久間氏）

講演資料

AIガバナンスの必要性

AIは技術的な不確実性が高く、特に生成AIが流行を始めてからの変化が非常に激しい状況です。世の中でいわゆる「AIインシデント」とみなされる事例も増えてきています。また、制度的な変化も激しくなってきています。日本においても、AI推進法が成立したばかりです。投資家の目線でも、AIリスクが取り沙汰されるようになってきていますが、経営層で「AIガバナンスの構築が完了している」という企業はまだまだ少ないのが現状です。実務を社会的なニーズに追いつかせることが、今求められていると思います。

AIリスクは、大きくセーフティリスクとセキュリティリスクに分けられます。セーフティというのは、意図せずに発生する性能や倫理面の問題です。例えば、ハルシネーション（嘘の情報の出力）による被害や、出力に差別が含まれて特定の社会グループの方が不当な取り扱いを受けてしまうこと、プラ

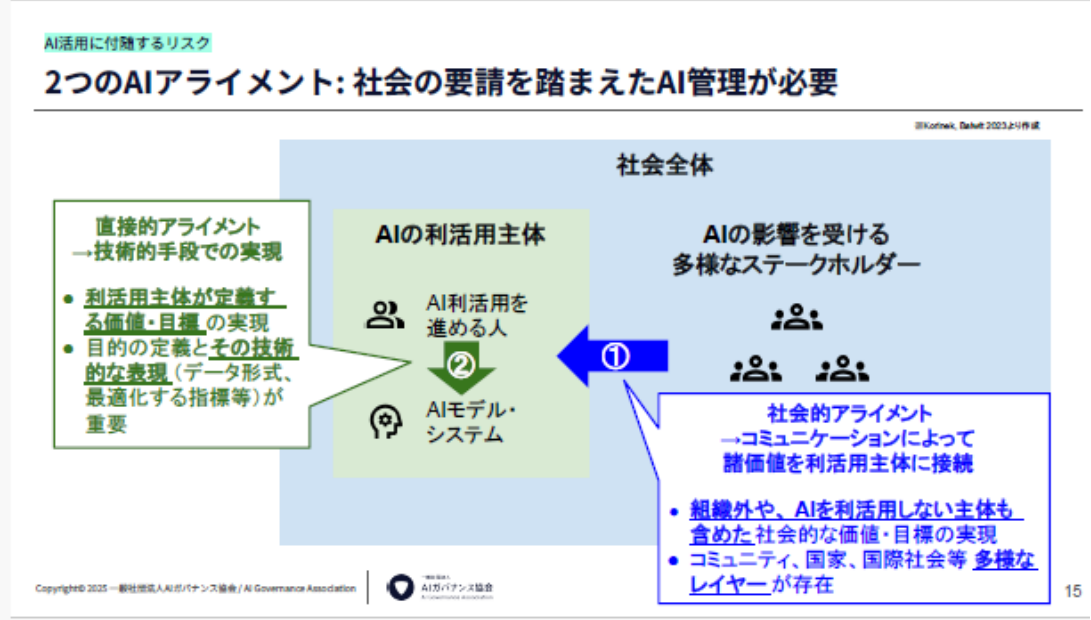
[5]「AIの利用・開発に関する契約チェックリスト」（経済産業省、2025年2月）
[6]「DX時代における企業のプライバシーガバナンスモデルガイドブック」（経済産業省Webサイト）

イバシー侵害などの例があります。セキュリティリスクは、どちらかというと悪意のある第三者がいるケースです。インシデントが多くなっており、AIに対する攻撃が行われたり、AIがサイバー攻撃に使われる場合も増えてきています。様々なリスクに対応しながらAIの活用を進めていかなければならない状況です。

セーフティリスクの例としては、先日決着した日本IBMの労使間の団体交渉も記憶に新しいところです。人事評価にAIを活用することを決定しましたが、AIがどのようなデータをもとに判断したかを会社側が開示をしていなかったことに対し、労働組合の側から異議申し立てが行われました。過度に広範にデータを収集しているのではないかというプライバシー侵害の懸念、その中にバイアスが含まれて、不当に評価される人がいるのではないかという差別の懸念、評価がそもそもブラックボックスになってしまい社員の改善の余地を奪ってしまうのではないかという懸念等、様々な議論がありました。最終的には、このケースでは透明性を向上させようということで、人事査定でAIが考慮する項目をすべて開示するという方向で調整がなされていきます。

ハルシネーションについては、例えば、ニューヨーク市が行政として導入したチャットボットで、法令違反を企業に対して勧めるような出力をしてしまったケースがあります。これは明確に違法な情報が出力されてしまったケースですが、個別の企業においても、例えば顧客情報等が漏えいしたり、誤った情報を出力してしまうことでステークホルダーに被害を与えてしまうというパターンはあります。

AI活用に付随するこういったリスクに対応する際の考え方として、AIアライメントを紹介します（下図）。AIアライメントとは、AIに対して使う人間や、作る人間の意図を実現させるように調整することを指しています。一般的には各企業が、自分たちが使うAIや作るAIに対して、何かしらの目標を実現させる（直接的アライメント）わけですが、それだけでは足りない時代になってきているのではないかと思います。社会的アライメントといいますが、組織の外、AIを直接使うことを選んでいない人々も含めて、様々な利益をAIガバナンスの中で反映していかなければいけないと思います。例えば、労働者がAIで査定されることを望んでいない状況下で、それでも企業がAIを導入するということになると、当然ながら影響を受ける労働者にとっての利益や、その方々にとっての透明性をしっかりと考えて実装をしていかなければなりません。その意味で、社会からの要請を組織がしっかりと受け入れるところ（①）と、それを実際に技術的に個々のシステムに導入するところ（②）の2段階が必要になってきます。逆に言うと、外部ステークホルダーの声をちゃんと聞けていなければ、社会的アライメントが失敗しますし、仮に、AI活用に関わるステークホルダーの様々な利益や回避すべきバイアスがわかっても、それを実現するために技術的にAIをどう調整すべきかがわからなければ、直接的アライメントが失敗することになります。外のステークホルダーとのコミュニケーションの次元と、それを実装する技術の次元、このどちらもがAIガバナンスに求められています。



（出典）佐久間氏登壇資料

AIガバナンスとプライバシーガバナンス

OECDでもAI原則が公表[7]されていますが、関連するOECDの文書[8]でも、個々のAIのプロセスにおいて、個人データを活用する場合や、個人に対する影響のあるような決定を行う場合には、プライバシーの観点を考慮する必要があるとされています。

実際にAIをつくるところまでのライフサイクルを考えても、（基盤モデルをそのまま活用する場合は別かもしれませんが、それ以外は）基本的には学習のためのデータ収集（場合によって、個人データ等の取得を伴う）が必要です。それに加えてモデル構築をする段階で、バイアス対策やセキュリティ対策を行っていく必要があります。さらにシステムの運用が始まってからも、新たに収集するデータも当然あるでしょうし、いつ攻撃されるかわからないので、基本的にはセキュリティ対策を継続的に行っていく必要があります。最後の出力の活用の部分においても、その出力を何に対して使っていくのか、透明性を担保することが求められています。AIガバナンスとプライバシーガバナンスは不可分に進めていかなければならないと思います。

企業のAIガバナンス実装状況と課題

AIガバナンス協会ではAIガバナンスナビという、AIGA会員企業がAIガバナンスの取組の成熟度を自己診断するツールをつくり、実装状況を把握しています。4月に実施した自己診断では、ルール・組織づくりが先行しており進捗が窺えますが、各リスク領域の技術的なリスク対策や、透明性の確保についてはスコアが低く、取組余地が大きいとの結果が出ています。

また、AI開発者と、それをビジネスに導入していくAI提供者、純粋なユーザ側の企業に分けてみると、やはりユーザ側の企業のスコアが低くなっています。これは自然なことなのですが、他社のSaaSの

[7] OECD updates AI Principles to stay abreast of rapid technological developments（OECD、2024年3月）
[8] 「AI, data governance and privacy Synergies and areas of international co-operation」（OECD、2024年6月）

AI製品を調達し、そのまま使っている場合が多いのではないかと思われ、そういった企業にもAIガバナンスをどうやって広めていけるかも課題なのではないかと思います。

2.データ活用の取組とガバナンスの現在地

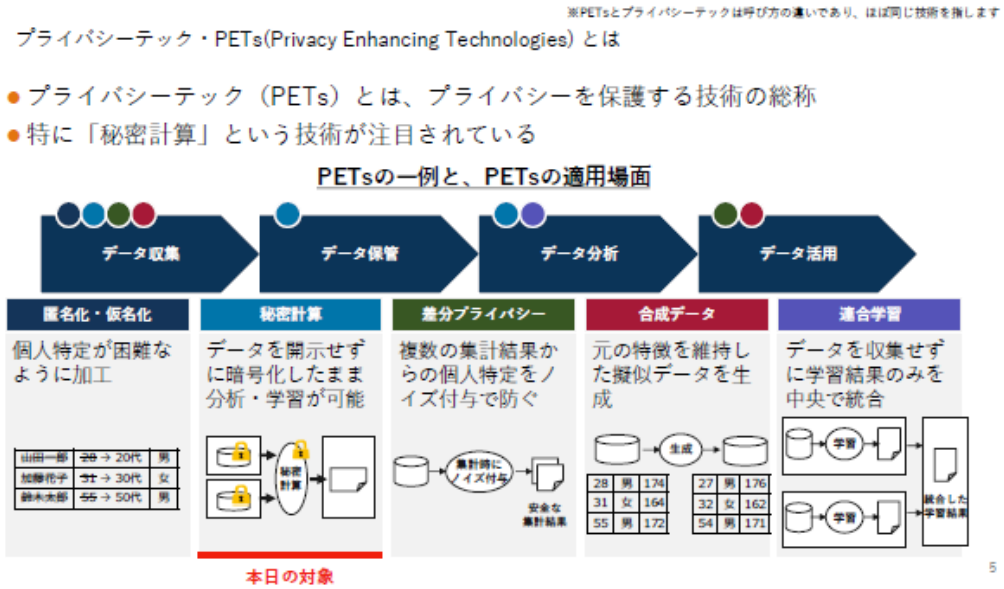
続いて、他社とのデータ連携による価値創出に向けた取組も進んでいるところ、データを安全に連携するプライバシーテック・PETsの観点（2-1）、実際にデータ連携・利活用を進められる企業様の観点（2-2）から情報提供をいただきました。

2-1. PETs(Privacy Enhancing Technologies)とガバナンス（プライバシーテック協会 竹之内氏）

講演資料

プライバシーテック・PETsとは

PETs（もしくはプライバシーテック）はプライバシーを保護する技術の総称です。主な技術は下図の通りですが、データの収集・保管・分析・活用のプロセスにわけると、別のプロセスに適用される技術もあるので、複数の技術を組み合わせて、より安全性を高めることも可能です。



（出典）竹之内氏登壇資料

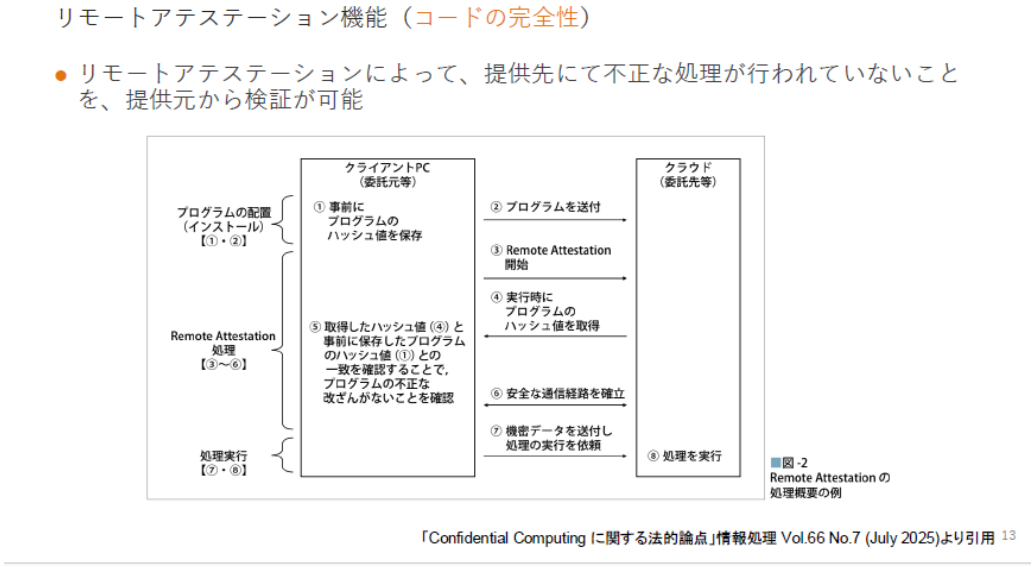
秘密計算とは

秘密計算は、データを暗号化・秘匿化された状態で処理できる技術の総称です。従来の暗号技術は、通信中のデータの暗号化、もしくはデータベースに保存中のデータの暗号化に主に活用されており、処理中のデータは暗号化ができなかったのですが、それを実現するのが秘密計算です。これにより、データの収集から廃棄まで、ずっと暗号化した状態でデータを取り扱うことができるようになります。

秘密計算にはいろいろな方式がありますが、ハードウェア方式（TEE（Trusted Execution Environment：信頼実行環境）/機密コンピューティング）は、AppleのiPhoneの生成AIが採用したこともあり、この1年で急激に注目されるようになりました。端末で生成AIを動かすには、処理速度が重たいので、一

部の処理はサーバ側で処理をせざるを得ません。TEEは、例えば処理中のメモリー内のデータを暗号化することで、データ処理をセキュアに行うことができます。生データのまま端末からサーバに送られるのでなくて、暗号状態でサーバに送る、暗号状態で生成AI処理をする、暗号状態で端末に戻すことができます。

AI時代は、処理をサーバ側で行わないと追いつかず、処理環境が外部にあることが多くなります。上記のように、データを暗号化により秘匿したとしても、クラウド側で勝手に変なコードが動いてしまうと、不正にデータが漏えいする恐れもあります。TEEには、当初実行するはずだったコードが不正に改ざんなどされていないかを確認する「リモートアテステーション（Remote Attestation）」という機能があります（下図）。ざっくりとしたイメージですが、実行前に実行する予定のソースコードのハッシュ値を保存しておき、実行のタイミングで、実行されているコードのハッシュ値と突き合わせて、不正がないかをチェックします。これによって、外部環境、処理基盤が安全であることが技術的に検証可能になります。



■図 -2
Remote Attestation の処理概要の例

（出典）竹之内氏資料

Appleは外部の暗号研究者等に対して、こういったサーバ側の処理が安全にされているのかを技術的に検証できる環境を、オープンに提供しています。発見された脆弱性に対する報奨金は1億円を超える金額です。

こういった技術的な動向を受けて、個人情報保護法のいわゆる3年ごと見直しの議論においても、プライバシーテック・PETsといった技術的手法を適切に位置づけることについて、検討が進められています。

2-2. KDDIにおけるデータ利活用とガバナンスの取組（KDDI 山崎氏）

講演資料

ガバナンスの取組

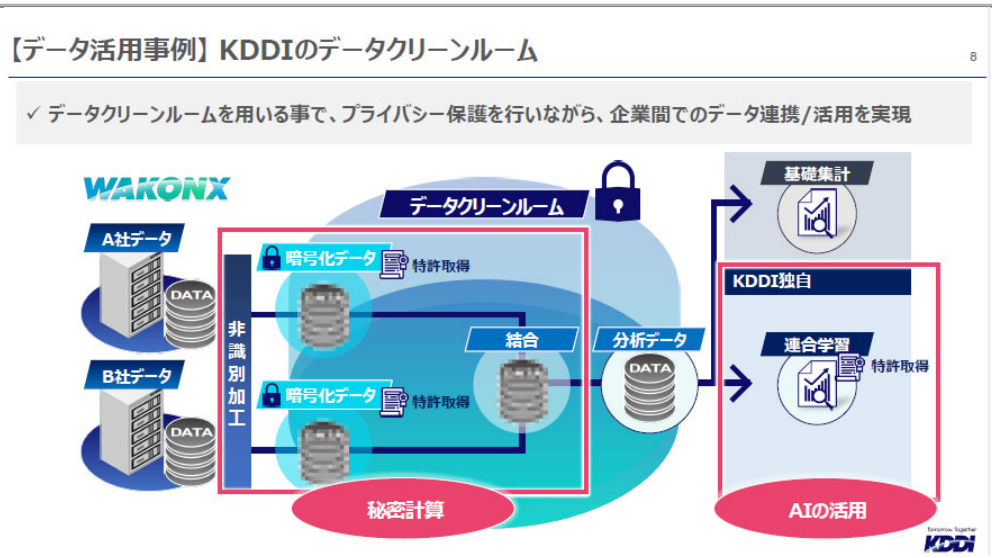
Data＆AIセンターは、正しくデータとAIを保護しながら活用することを目指しているKDDIの社内組織です。KDDIでは、データ・AIに関するガバナンスとして、プライバシーガバナンス、データガバナンス、AIガバナンスの3つのガバナンスに取り組んでいます。個人情報の保護などはプライバシーガバナンスとして、AI特有の開発時のリスク、人権、倫理といったリスクの対応などはAIガバナンスとして、データカタログの整備をはじめとしたデータマネジメントを適切に行うことをデータガバナンスとして整理し、それぞれが密に連携するために、1つの組織で3つのガバナンスに取り組んでいます。

プライバシーガバナンスについては、2020年に専門組織を立ち上げて今の形に発展しています。データドリブンに投資をするという意思決定をする中で、その両輪となるようなガバナンスも必要であるとの経営層の意思決定があり、社長直轄の組織として体制を作っていきました。経営層の理解があったことが、特に立ち上げ時に大きな力になったと思っています。体制を構築して社内のガバナンスを効かせていくことと、透明性やアカウンタビリティを確保するという意味でのお客様とのコミュニケーションを大切な軸としてとらえています。お客様とのコミュニケーションの事例として、プライバシーポータルというサイトで、お客様に対して当社がどういう姿勢でデータを扱っているのかの情報発信や、オプトアウトなどのコントロールの機能を集約して提供しています。新たな取組や考え方をリニューアルした場合にも、都度、ポータルを通じて情報提供しています。

プライバシーやデータガバナンスに係る課題を解決するテクノロジーも、広い意味でプライバシーテックといえるのではないかと思いますが、特に注力しているプライバシーテックの活動の一つに、同意管理機能（PPM：Privacy Policy Manager）の提供があります。お客様が様々な内容のサービスの規約、個々の同意内容を一つのサイトで確認できるようになっており、企業にとっても、データ分析等を進める際に、お客様の規約の同意状況を確認して、素早く、正確にデータ活用の判断ができます。

データ利活用の取組

データドリブンで進めるために、KDDIでは事業者間でデータをコラボレーションするという構想を掲げています。基本的にはグループ会社が中心になりますが、データクリーンルーム（図5）という形で、お互いのデータを連携し合い、自社のデータだけではわからない新たなインサイトを得ることを想定しています。それによって生み出された新たな価値を社会に還元していくというコンセプトです。具体的な取組としては、複数の会社が保有するデータを、元の個人データと対応関係がなくなる状態に加工し、データクリーンルームで、秘密計算によりデータの中身はわからない状態で結合し、最終的な統計的な結果を得ています。



（出典）山崎氏登壇資料

DXに取り組まれている企業であれば、自社のデータを活用し、売上の改善や業務の可視化を行うなどの取組は進められていると思います。さらに、データコラボレーションをすることで、他社のデータを掛け合わせて、例えば、小売業界を例とすれば発注の予測精度を上げるなどにつなげられると思います。これは、企業にとって売上の改善というメリットだけでなく、廃棄ロスの削減という社会的な意味もあります。データ活用するときには、最終的に、社会やお客様など、世の中に対してどういうメリットがあるかを意識したユースケースを検討することが重要だと思います。それによって、本人、データ主体にとっても、こういうことにつながるのであればデータを使ってもいいという納得感が生まれるとともに、それが透明性・アカウンタビリティの取組にもつながってくるのではないかと思います。

3.ディスカッション「AI活用、データ連携、企業に求められるガバナンスのポイントや課題」

企業に求められるガバナンスのポイント　――――――4者からの情報提供を踏まえて

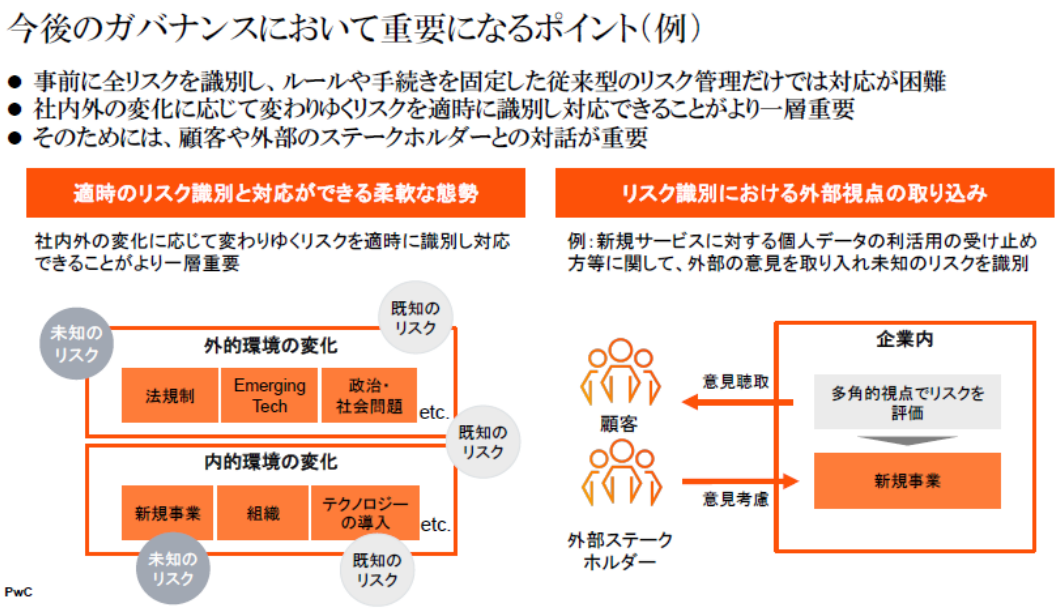
PwC 平岩氏：　今後のガバナンスに重要なポイントをまとめたので、それに即して、情報提供いただいた内容を振り返ってみたいと思います。

前提として変化が速いということは、リスクのマネジメントという点では、従来のように、事前にすべてのリスクを識別し、ルールや手続きに落とし込み、評価し、対応していくことが、難しくなっていくのだろうと思います。ただ、注意したいのは、従来型のリスクマネジメントの意味がなくなったということではなく、それだけでは対応できなくなってくるリスクの、重要性が高まっているということだという点です。

今後のガバナンスにおいて重要になるポイントですが（下図）、1点目としては、タイムリーに変化していくリスクを識別し、対応できる体制をつくれるかという点です。先ほど永野さんからお話のあったアジャイルガバナンスのコンセプトとも合致するものと思いますし、変化をとらえていくための組織の在り方として、山崎さんからお話しいただいた取組も事例となると思いますし、竹之内さんが紹介されたPETs・プライバシーテックの活用によって変化に対応できる部分が多く出てくるのだろうと思います。

2点目は、リスクの識別を、変化に対応して進める際に、自社内だけに閉じてできるかというと、必ずしもそうではないということです。技術が変わる、消費者の意識が変わる、社会が変わる、それに伴ってレギュレーションが変わっていく中で、すべての状況を自社だけでカバーしていくというのは、本当に難しい状況なのだと感じています。企業にとって、お客様、あるいはその先にいる消費者、外部の様々な専門家などの意見に耳を傾け、環境の変化をいち早く察知し、自社の考えている新しいサービスやデジタルソリューションに対するリスクについて、自分たちに見えていないものが何かないかと確認するプロセスを踏むことが、大変重要になってくると思います。

外部視点の取り込みという点を少し発展させていくと、社会とのインタラクティブなコミュニケーションにつながっていくのだと思います。自社が取り組んでいるリスク管理活動を、外部に開示していく、それに対するコメントをもらって、また改善していく、そのようなサイクルを回していけるようになることが、佐久間さんがお話になった社会的なアラインメントのきっかけの一つになるのかなと思います。外部に向けて開いていく、そんなリスクマネジメントの新しい在り方というのも、企業にとって重要になってくると思いました。



（出典）平岩氏登壇資料

弁護士 今村氏：　事業者の皆様が、個人情報保護・プライバシーの分野で一番悩まれているのは、法律が求める最低限の対応はしていても、世の中が許してくれないのはなぜか、という点だと思います。法律はどうしても世の中の動きの後追いにならざるをえない部分があって、法律を守っているだけでは社会の動きに必ずしも対応しきれていない部分が、難しさとしてあるのだろうと感じています。本日情報提供いただいた、政策側の観点や事業者団体側の観点のお話は、法律では必ずしもカバーできていない部分を、法ではないが、政府側、事業者団体側で、事業者の指針になるように、ガイドラインやガイドブックなどのソフトロー的なものを整備して、サポートしているという取組なのだと思います。

また、個人情報保護法の3年ごと見直しにおいては、現状、安全管理措置、匿名加工情報なのかというところで、がちがちのルールの中でしか使えていない、プライバシーテック・PETsの技術の部分についても、より使いやすい形で、本人同意を取らずに活用できる部分がもう少しあるのではないかとい

う形で議論が進んでいます。事業者団体の方が声を上げられたからこそ、いま議論が進んでいるのかなと思っています。

ガバナンスにおける課題感　――――――リスクアセスメント、透明性・アカウンタビリティの担保

佐久間氏：　先ほどご紹介したAIガバナンスナビの取組から、課題感が見えてきています。1点目は、リスクアセスメントやリスクベースアプローチをどう実装するのかという点です。あらゆるAIに対してとても厳しい管理体制で臨むことは、現実的でないし、現場での活用を妨げてしまいます。平岩さんがお話されたような、まだ予測できないリスクもあるので、これを踏まえてどのようにリスクを予測し、それを見積もって、ハイリスクとローリスクを分類するか、それをさらに売上やROICをはじめとする事業の他のKPIとどう比較可能にするのかは、悩んでいる企業が多い印象です。

2点目は、透明性やアカウンタビリティについてです。ステークホルダーコミュニケーションを考えると、そもそもデータやAIをどう使っているのか、どこまでAIが処理しているのかを一定程度開示しなければならないし、そのAI活用によってユーザやステークホルダーにどういう利益があるのかということを、併せて説明をしていかなければならないと思います。ただ、情報を開示しすぎると、企業の事業戦略の根幹に関わる部分まで開示してしまうことになりかねないので、そのバランスをとるのが難しいと思います。

平岩氏：　いただいた2点は、裏表の関係、一体の問題なのかなと思いました。何が本当に危ないリスクなのということが明確にいえず、経営判断にかかる意思決定ができないというところが、活用のネックになってしまっていることもあります。技術が変わる、データが変わることで、AIのモデルが変わっていくという可変的な状況を前提とすると、どうしても、現時点ではこうだと思います、としかいえません。大事なのは、その時点の限られた情報の中で、最善の決定をこういう風にしましたと、対外的に自分の言葉で説明できることだと思います。その意味で、リスクベースアプローチの徹底ということと、対外的な透明性の確保というのは、裏表の関係にあるだろうし、それを積極的にやっていった企業が、社会からも信頼されるし、お客様からも信頼されるし、あの企業だったら大丈夫だよねと思っていただけるようになっていくのかなと思います。そのために実装していかなければいけないのは、組織体制でもあるし、リスクアセスメントの中で使える技術というのが多く出てきているので、そういった技術を積極的に活用していく、そんな企業が、競争力の面でも強くなっていくのかなと感じています。

山崎氏：　1点目のリスクアセスメントについては、企業の目線からいうと、体制を構築するというところと、人材を確保するというところは、大きな課題だと思います。リスクアセスメントを業務に落とし込むときには、一定の文書化をして、規定にして、業務プロセスに落とし込み、アセスメントする人材を配置して、それを体制として回していく必要があるわけですが、企業としてはかなりコストがかかる活動になります。アセスメントについても、技術から法律や政策動向までそれなりに広い専門性を持つ人材が必要になってくるので、そういった人材の確保や育成も課題になります。その解決策の一つとしては、冒頭、永野さんがご紹介の政府文書や、佐久間さんがご紹介のAIガバナンスナビのような一定のフレームワーク等を一つの指針にしながら、自分の会社にカスタマイズしていくというような形が取れれば、求められる専門性のハードルを少しずつ低くしていくことができるのではないかと思います。そういった取組には期待しています。

今村氏：　透明性、アカウンタビリティについては、誰に対する透明性なのか、誰に対するアカウンタビリティなのか区別して検討していかなければならないと思います。データ連携のような文脈では、自社内でどういう透明性をもって、どういう説明資料を残してという話もあれば、B2B間での、事業を連携する相手方との関係でどういう整理をしていくのか、データの主体になっている個人との関係、社会への説明との関係で、どういう整理学、どういう説明をするのかという、それぞれのステージがあります。

個人情報保護法の話だけであれば、法令違反のリスク、執行のリスクという目線での検討がほとんどですが、そこからさらに踏み込んで、このデータをこういう形で事業で活用すると、世の中にどういうハレーション、どういうリスクがあるかまで整理しなければならないところが、非常に難しいと思います。

ただ、個人情報保護法がそれを全く想定していないのかというと、必ずしもそうではないと思います。というのは、安全管理措置についてのガイドラインの解釈では、その事業者にどういう安全管理措置のレベルが求められているかについて、その事業の性質、取り扱う情報の量、質などを考慮した上で、必要な措置を講じよとされています。便宜的かつ、なにも答えていないような書きぶりではあるのですが、そういったことも踏まえて、実際、このデータを取得して、この事業者とこういうデータ連携をして、何をしようとしているという、そのビジョンの中で、透明性をどう担保するか、外に対しての説明、企業内での説明、横の連携での説明をどうしていくかを、それぞれ区別して検討していくということが求められるのかなと思います。

佐久間氏：　いずれの点も非常に重要だと思います。「この技術は絶対安全です」というような太鼓判を押せない状況がいろいろと潜んでいる中においては、プロセスへの信頼のようなものを担保することが必要になり、そこではステークホルダーによって異なる対応や説明のレベルが求められます。プロセスへの信頼を確保するための社内体制整備と丁寧なコミュニケーション、そして人を育てることも重要ということだと思いました。

平岩氏：　透明性に関連して、組織体制面・プロセス面で、ガバナンスの中軸を担う推進組織に、どのようなメンバーが必要かという議論がされることも多く、（伝統的には、個人情報保護法の対応など、法務部門が中心となっていたり、コンプライアンス部門、IT部門が中心となって、CoE（Center of Excellence）やバーチャルな推進組織を作るケースが多いかと思いますが）広報の方々を巻き込んではどうかと提言することが多いです。外部への発信、透明性の確保やパブリックコミュニケーションで、そのスペシャリストの力が必要になってくるので、ブランディングの一貫としてもそういった方々を入れてみてはどうかという話をさせてもらうことがあります。

竹之内氏：　Appleの例を先ほどお話しましたが、一般のお客様への説明だけでなく、技術がわかる方により深く説明するためにホワイトペーパーを出すだとか、ソースコードを開示したり、技術者が検証する環境をオープンに提供することも重要と思います。つまり、一般向けと専門家向けの両方をトータルでやっていくことによって、社会からの信頼を獲得できるのだろうと思います。

データ連携の社会的な意義

竹之内氏：　2021年にGAFAの時価総額が、日本の全企業の時価総額を超えたとの報道がありました。トップ企業は、データやAIの活用をどんどん進め、企業価値を高めていて、そうでない企業との差がますます開いています。グローバルの中における我々の立ち位置を強く意識すべきなのだろうと感じています。日本企業はどうすればよいか。やはり連携によるデータ活用が必要だと思います。

山崎氏：　自社のデータだけではなくて、他社のデータも活用できれば、価値が高まるというのは一般論としてあります。ただ、企業なので、それで利益を出すという目線も必要で、データ連携の構想は立ち上がるけれども、投資に対する利益が果たして得られるかが見出せずにしぼんでしまうという課題はずっとあったように感じます。そこに対する解決の方向性としては、やはり、社会に対してどういうメリットや便益がもたらされるのかを念頭に置きながら、データの連携を考えていくということなのではないかと思います。

データ連携における課題とソフトローの活用

山崎氏：　また、データ連携については、実際各論に落とした時には、課題がいろいろあるのだと思います。主だったものとしては、各社間でリスク基準やデータの取り扱いが違うので連携ができないとか、それを契約に落とし込むときにも非常に時間がかかるといった課題があると思います。試しにこうやってみようといった場合も、それだけで半年かかってしまう場合もあります。そのような状況の中で、今日お話があったような、ガイドブックや、契約条文のモデル条項を用いて、一定のリスクに対する判断基準を共有していくというのは、非常に重要な取組だと思っています。この基準に達していればお互い大丈夫なので、この基準に沿ってやりましょうといえるガイドのようなものが世の中に広まっていくことで、こういった課題についても、ハードルが下がっていくのかなと考えています。

今村氏：　事業者間のすり合わせについては、事業者ごとに思想が異なったりし、その調整がそもそもうまくいかない場合もあるのかなと思います。弁護士としてもご支援できる部分ですが、必ずしもすべてのシチュエーションで、代理人を立てて、弁護士を間に入れてできるわけではないと思います。そういう場合にこそ、思想を共通化するためのツールとして、政府や事業者団体が、考え方について整理している文書が、お互いにとって拠り所になる、ツールになるのかなと思います。こういう各社の違いみたいなところを埋める取組は、非常に重要なことだと思います。

永野氏：　契約に関するガイダンスとして、経済産業省が近年、整理、公表した情報をご紹介したいと思います。AIの利用が広まるとともに、AIの品質を向上させるチューニングパラメータとか、学習データ、教師データに価値が生まれて、個別に流通するケースが、ますます増えていくかと思います。このような動きはシステム・サービス全体の品質の向上や、システム・サービスが相互につながることによる新たな価値の創出の可能性をもたらす一方で、主体間または主体内の責任分界が不明確になるという問題が生じるため、ステークホルダー間の対話や取り決めがますます重要になると考えられます。

これについて経済産業省では、冒頭ご紹介した、「AIの利用・開発のチェックリスト」の親の関係に

ある「AI・データの利用に関する契約ガイドライン」[9]を公表し、契約のひな型と、留意点を整理しました。また、AIとは離れた話題になりますが、データ基盤事業者を通じた、データ保有者と、データ利用者のデータ連携についてモデル規約という契約の考え方を整理し、ホームページで公表[10]しておりますので、ご参考にしていただければと思います。

佐久間氏：　上記とは少々別の、セキュリティに近い視点からとなりますが、連携に関わるプレイヤーの中で、シャドーAIのようなものをなくすというのも大事なことです。あらゆる業務においてAIが活用される状態になると、想定しない内にAIにデータを入力していたといったようなヒヤリハットも生じていて、注意が必要かと思います。もともと使っていたツールにアップデートで急にAIが入ってきたりというケースもあります。AIバリューチェーンに関わるプレイヤーにおいて、「いつの間にかAIが入っていた」といったことを防ぐというのは、プラクティカルには重要かなと思います。

それぞれの立場からガバナンスの取組への参画を

今村氏：　佐久間さんの情報提供の中で、ベンダー企業側に比べ、ユーザ企業側の方が、ガバナンスに対する取組の進度について、スコアが低いとの紹介がありました。仕方のない面もあるのかなと思いつつ、ユーザ企業側にも、取組を期待したいところです。それには、データはどのように活用できるのか、プライバシーテック・PETsの技術はどこに利点があって、どういうところが保護されているからこそ、世の中に対して安心ですよと説明ができるのか、データ利活用の結果、どういうメリット・便益が出せるのかということが、自分たちの中で咀嚼できるということが、非常に重要なのではないかと感じました。

佐久間氏：　AIガバナンスの文脈でも、ユーザ企業側の方がリスクの把握がまだ進んでいないところがあります。でも、利用者の目線でも気にしなければいけないリスクがありますし、データ分析等のタスクを行う際には、不可避的に今後AIを使っていくことになると思うので、リスク感度を底上げしていく必要があるというのは感じています。

竹之内氏：　今後、データ利活用をさらに進めていく際のキーワードは「連携」だと思っています。企業・組織間の連携もあれば、社内の部門間の連携もあります。データ利活用、データ連携により、世の中に良い価値を出すということを共通の目的にして連携することが重要です。理系・文系と分けて考えるのは本来好ましくないですが、いわゆるDXは理系が注目されがちですが、連携にかかる仕事というのは、実はほぼ文系的なのだとも感じています。理系・文系を問わず総力戦で、部門間、組織間などの連携をしながら、進めていけるとよいなと思います。

佐久間氏：　先ほどお話もでたように、人材というところが大変大事だと思います。ぜひこのような取組に関わりたいという方は、いつでも声をかけていただければと思います。

以上

[9]「AI・データの利用に関する契約ガイドライン」（経済産業省、2018年6月）
[10]「データ連携のためのモデル規約解説と論点整理」（経済産業省、2024年6月）

本内容は、2025年7月17日に開催されたMyDataJapan 2025 カンファレンス（主催:一般社団法人MyDataJapan）Track A-4「AI・データ活用の進展と求められるガバナンス」の内容を取りまとめたものです。