オンライン及びアンケートで頂いた質問と回答の一覧

2023/12/7 10:02 版

項番	質問	回答
1	日本でもISOに従えば, AI Actをクリアできるということでしょうか?	(杉村さん) 残念ながら，そうではありません． AI-ACTを支える整合規格の多くはISOの規格になると思われますが，欧州独自の規格や，ISO以外の規格を最終的に整合規格とする可能性があります．また，認証制度については，地域・国の間で相互認証について合意が必要ですが，まだ，相互認証のスキームはまだ作れていません．そうありたいとは思っていますが，達成には多くの標準化以外の課題が存在しています．何よりも，業界からの期待の表明が大切です．
2	ご講演ありがとうございます。ガイドラインに対する海外からの反応やフィードバックはいかがでしょうか？	(大岩さん) 同様のガイドラインを公表している欧米の機関とは交流して、相互に基本的な考え方が一致していることを確認しています。 また国際標準化の場にもガイドラインの内容を提案して受け入れられています。
3	本ガイドラインでは,もしIncidentが起きた際の安全性の確保に関する要綱はどうなっているのですか、	(大岩さん) 深刻なインシデント発生時のリスク対応については、現状では機械学習AI利用の有無に依らず従来の規格等に依拠する事を社会的に求められると想定して、現在のガイドラインはつくられています。 第3版時点のガイドラインでは、リスクの分析と対応方針の決定については機械学習によらないシステムと同様に実施することを求め、それを実現するためにシステム中の機械学習要素がどのような品質を実現するべきかを定めています。AI特有の動作記録にまつわる問題などについては、ガイドラインのE項に関係しており、第4版で追加の整理を試みているところです。 そのうえで、ISO/IECなどでIEC 61508と対応するAI特有の安全性に関する技術仕様作りなどが進んでおり、AIと周辺システムの組み合わせでの安全性確保の考え方などについても整理が進んでいますので、社会的な受容状況も見据えながら今後の改定版ではAI特有の考え方を増やしていく方向を想定しています。
4	昨日の米大統領令では、2023.1のNIST AI 100-1（AI RMF 1.0）をガイドラインとしたDOC報告などの制度整備が明記されたように見えています。米国AI RMFの言及がありましたが、米国はRMFの下で機械品質品質ガイドラインや、ISO/IEC JTC 1/SC42に親和的な技術基準を制定するつもりなのか、全く別の方向性があるのか、ご存じの範囲があれば教えてください。 ご尽力の機械学習品質マネジメントガイドラインに準拠することが、米国の基準達成にも資することになるのか理解を深めたいと考えています。	(大岩さん) 米国の意図については推測しかできず、また米国は様々な政府機関が独自の動きを見せているので、お答えするのが難しいですが、米国の中で主要な動きを見せているNISTは欧州や日本を含めた各国と一定の連携を取っております。今後もルール協調に向けて、NIST等への働きかけを続けていきたいと考えています。

項番	質問	回答
5	４つのゆらぎについてもう少し詳しくご説明ください。	(中神さん、桑島さん) 4つのゆらぎの導出過程も踏まえて回答いたします。 4つのゆらぎは資料の補足資料（P19）に示すように、不確実性要因と品質特性の類似度合いに基づいて分類し、その結果をもとに定義しております。また、それぞれのゆらぎに割り当てた不確実性要因と品質特性に対し、どのような曖昧さが生じるかを検討した上で、その対策方針を考え方として定義しております。例えば、観測のゆらぎの場合は下記のようになります。 ■コンセプトの不確実性、シーンの不確実性、センサ特性の不確実性、要求分析の十分性、データ設計の十分性 曖昧さ：どのようなデータを集めておけばよいか。 対策方針（考え方）：AIの結果に影響するパターンを演繹的かつ帰納的※1に洗い出す。 ※1：ここではデータ設計完了までに特定できるパターンを演繹的、実際に開発して見つけたパターンを帰納的と呼んでいます。 ■シナリオカバレッジの不確実性、データセットの被覆性、データセットの均一性 曖昧さ：どのくらいの規模のデータを集めておけばよいか。 対策方針（考え方）：パフォーマンスとリスク回避性各々に対するデータカバレッジ方針を示す。※2 ※2：一般に製品ごと品質レベルは異なっており一律の基準を定義することは困難であると考えたため、「データカバレッジ方針を示す」という考え方としています。
6	To:浜谷様 社会的視点での議論には、どういった立場の人の参加が期待されるでしょうか。学術関係者や弁護士みたいなところというのはこれまでよく合った形（政府の有識者会議とか）だと思います。ただ、AIの社会受容を考えると特に一般市民の感覚といったものが非常に重要になると思いますが、企業として、ビジネスを展開する上で市民感覚をどう捉え反映すべきかといった策をお聞かせ願えればと思います。答えはないと思うので、これから議論をしていくポイントみたいなものでも構いません。よろしくお願いいたします。	(浜谷さん) ご質問ありがとうございます。　おっしゃるとおり、市民感覚を取り入れることは不可欠と思います。多様性（diversity)・包摂性(Inclusivity)の意識が公平性実現には重要と言われていますが、その意味でも、まさに市民感覚はキーですね。 市民感覚をどう捉え反映していくかは、ケースbyケースな部分が多いと思うのですが、個人的には、（「策」には程遠いものですが）例えば次のようなポイントに着目出来るのではと考えます。 ①想定ユーザ層の代弁者（ニーズや期待面、ユーザビリティ面を中心に、求められている公平性への期待などを正しく理解するために） ②開発チームとは「違う」属性（チーム属性をいくつか考え（性別、年齢、学歴、国籍、etc）　主たる傾向とは逆の属性を持つ人達に、特に開発上流で、違った視点からレビューしてもらう。セミナーの際にお話したように、「多様性によって認知バイアスを減らす」ために） 開発の上流で、こうした方からの意見を取り入れるのはとても重要なのですが、最初はは っきりしてない面も多いですし、アジャイルに、運用後も含めて、「捉えては検討＆対応＆発信」していくのだろうと思います。

項番	質問	回答
7	AI開発、運用、メンテナンス等、入口から出口までのサイクルにおいて、適合性評価がどのように絡んでくるでしょうか。例えばISO27001は組織に対してですが、JFS規格のように、開発に対する要求事項、開発と運用に対する要求事項、開発と運用とメンテナンスに対する要求事項と、階層別規格として広げていくことも想像致しました。技術的要件については理解及ばず大変恐縮なのです。どうぞよろしくお願いいたします。（浦下様、岡本様へ。他の方が適当でしたら申し訳ございません。）	(浦下さん) AI開発、運用、メンテナンスのプロセスにおいて、AI特有の要素と従来型の要素に分ければ、後者に対する既存の規格に対する適合性評価の扱いは従来と大きく変わるところはありません。 前者のAI特有の要素については、適合性評価の対象となる規格がまだ充実しているとは言えませんので、それらについて、当社では商談(企画)時、開発納品時、運用保守時の品質保証プロセスを設定しており、現行のAIガバナンスへの取り組みでは各プロセスにAI観点での自己チェックと必要に応じたレビュー、審査を組み込んでおります。 (岡本さん) 安全性に関しては、現在、AIを機能安全に適用する方向で検討が進んでおり、AIQMガイドラインの内容もISO/IEC TR5469:AI and Functional Safety に対して提案が行われている。機能安全の規格については、技術的な基準だけでなく開発プロセスや保守なども含む規格であるため、これらの要求事項については機能安全をベースに検討が進んでいくものと思われます。
8	浜谷様へ　公平性の評価基準は世の中でも確立していない（様々な視点がある）と思います。IT企業はそれをどこまで考慮すべきでしょうか。社会問題までおいかけるとキリがないのでは？という気がします。	(浜谷さん) ご質問ありがとうございます。 はい、公平性評価基準は、法律面での縛りはごく一部ですし、また「こうやれば決められる」というモノ・標準も、私の知ってる限りでは存在しません。 ただ、少なくともIT企業が、開発チームだけでそれを決定するのはリスクがあると考えます。　　ある方向のバイアスを持ってるかもしれない開発部隊の外、さらに言えば、企業風土というバイアスも考えれば、やはり「外部」の方の意見も参考に、考慮すべき要件を検討していくのが良いのではないでしょうか。　　そうした方が「正解」を出してくださるとは全く限らないのですが、少なくとも違った視点に気づくきっかけを得るために。 巷をにぎわせている生成AIへのもろもろの懸念にも、「差別的発言をした」的な公平性問題はあって、LLMメーカー側がいろいろ策をねるようになってきました。　　出来る限り、問題が炎上し出すより前に、社会からの問題意識を早く察知して対策とる、というループを回すことは少なくとも欠かせないのではと思います。 的外れな回答になってしまっていたら何卒ご容赦ください。
9	小川様、山田様、若松様　生成AIを導入されているとのことですが、利用にあたって著作権侵害のリスクについてはどのような議論を経てどのようなポリシーに到達されているのでしょうか？	(若松さん) ・社内で策定したポリシー、基本方針と整合性を取りながら、利用環境を準備 ・入力した情報がインターネット上に流出しないクローズ環境での構築 ・気密性、データ保護情報セキュリティの観点からの利用ルール規定 ・出力された情報の正確性・信ぴょう性の確認、著作権・知的財産の侵害の可能性などについては、リスクを理解した上で使用するように、リテラシー向上のための社内教育の実施 参考URL：https://jpn.nec.com/LLM/Inhouse_case1.html (小川さん) AIへの入力情報、出力情報それぞれの著作権の扱いについて、文化庁からの発表等も踏まえた社内利用ガイドラインを作成しています。個々の案件では、社内有識者が相談に応じながら運用しています。