

AI原則の実践の在り方に関する検討会

AI原則と公共調達

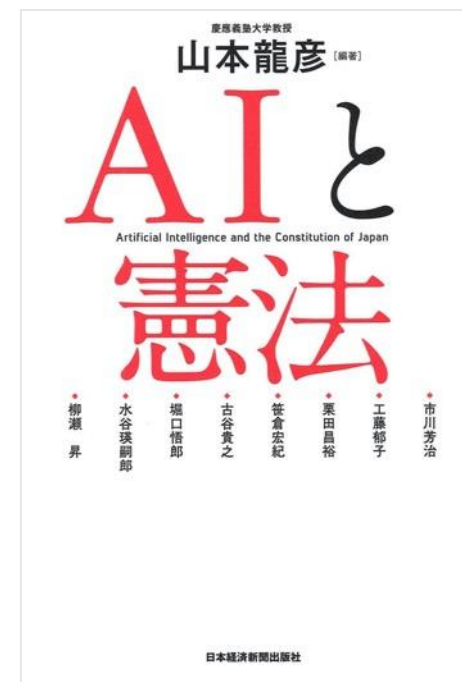
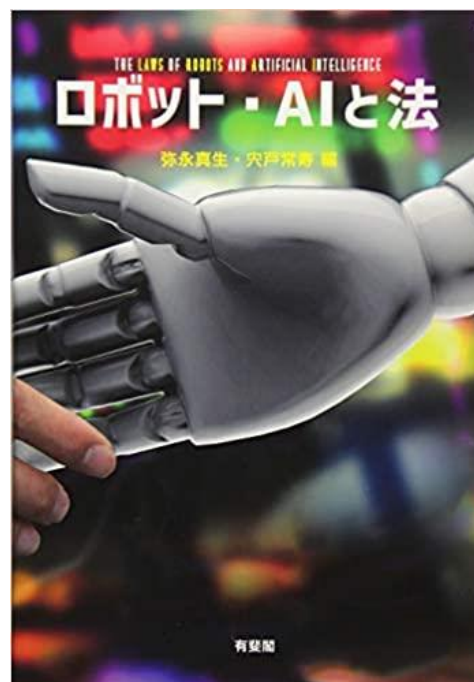
世界経済フォーラム第四次産業革命日本センター

プロジェクト戦略責任者

工藤郁子

自己紹介

- 世界経済フォーラム第四次産業革命日本センター プロジェクト戦略責任者
- 東京大学未来ビジョン研究センター 客員研究員、日本ディープラーニング協会 有識者会員、大阪大学社会技術共創研究センター 招聘教員等も務める
- 共著に、弥永真生・穴戸常寿編『ロボット・AIと法』、山本龍彦編『AIと憲法』、JDLA監修『ディープラーニング G検定 公式テキスト』など



世界経済フォーラム第四次産業革命日本センター

創設者：



WORLD
ECONOMIC
FORUM



AP i Initiative
Asia Pacific Initiative



経済産業省
Ministry of Economy, Trade and Industry

目的：第四次産業革命の恩恵を最大化するため、政策のオープンイノベーションを促進し、ガバナンスギャップを解消し、政策の互換性を確保する

パートナー企業：

- ・ アイシン
- ・ 日本電気
- ・ サントリーホールディングス
- ・ セールスフォース・ドットコム
- ・ SOMPOホールディングス
- ・ 武田薬品工業
- ・ デンソー
- ・ トヨタ自動車
- ・ 日立製作所
- ・ マッキンゼー・アンド・カンパニー
- ・ 三菱ケミカルホールディングス
- ・ 森ビル
- ・ 堀場製作所
- ・ エーザイ
- ・ 日本電信電話（NTT）

プロジェクト参画企業：

- ・ 三菱UFリサーチ・コンサルティング
- ・ デロイト トーマツ コンサルティング
- ・ 富士通
- ・ ベーカー & マッケンジー
- ・ ビザ・ワールドワイド・ジャパン



4段階、11のプロジェクト

Scale

1. Unlocking Public Sector AI: AI Procurement

Pilot

2. Empowering AI Leadership: Board and C-Suite Toolkits
3. Responsible Limits on Facial Recognition Technology
4. Human-Centred AI for Human Resources: toolkit for HR professionals
5. Chatbots RESET: Design frameworks for governing chatbots in healthcare
6. Responsible AI Certification
7. Generation AI: corporate governance for AI used by children and youth

Co-Design

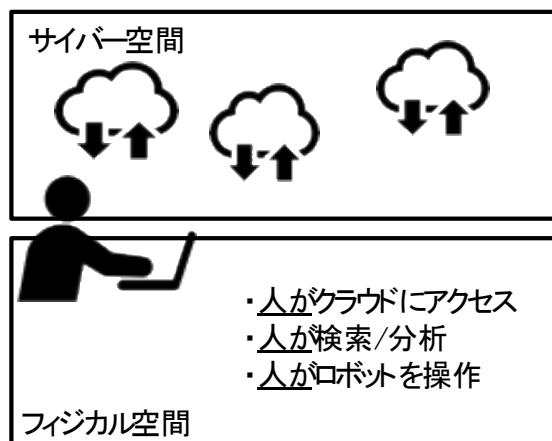
8. Responsible Use of Technology
9. AI Against Wildfire Risks
10. Improving Worker Trust, Engagement and Job Quality through Industry 4.0 Technologies

Scope

11. Responsible Investment in AI

なぜ AI&ML 公共調達？

人の介在が前提



前提

- ・静的（緩やかな変化）
- ・サービスと提供主体は一対一对応

IT/AI 公共調達

- ・ウォーターフォール型の開発が主流
- ・サーバーからアプリまでの垂直一体的なサービスの受発注が主流

人の手を介さない範囲の拡大



- ・動的（常に変化し続ける）
- ・多主体で複数システムを相互に連携（System of Systems）

- ・急な社会要請に迅速に対応できる調達、**アジャイル開発**への対応
- ・SoSを前提とした**責任分界点の整理**（モジュールでの受発注を可能に）
- ・**AIなどの最新技術**の公共部門の活用が必須（リアルタイムモニタリングなど）

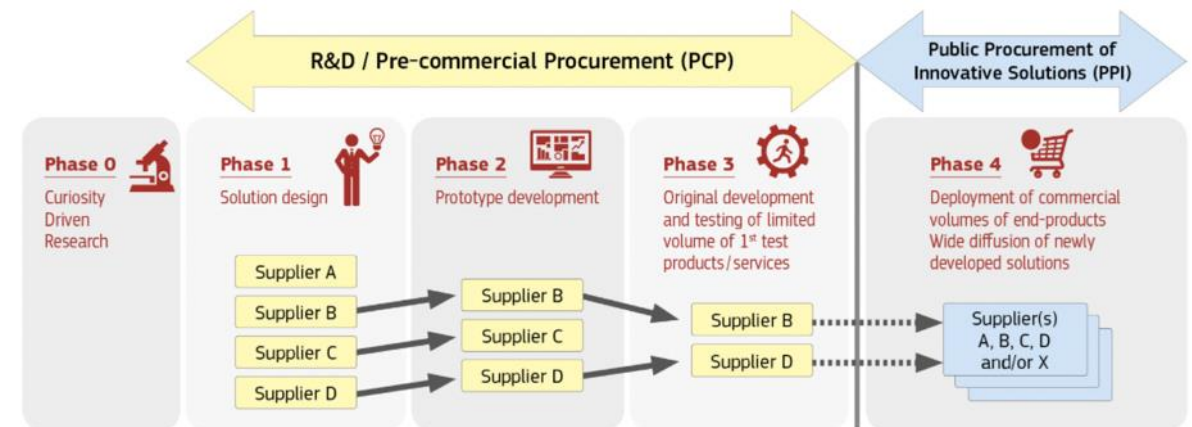
なぜ AI&ML 公共調達？

- 公共調達のために政府が策定する仕様書（要件定義書）は、ソフトローとして機能し、一定の行為規範性をもつ
 - × 企業・研究機関への直接規制（ハードロー）
 - × 企業・研究機関を名宛人としたガイドラインや指針
 - △ 裁判規範性
- 公共調達は、国・地域や時期によっても異なるが、概ね各国GDPの10-15%程度を占める
- ITシステムの開発・運用に費やされる金額は増加傾向（+ 研究開発投資や実証実験などの名目でも資金投入）
- この「市場規模」「購買力」を意識し、政府から倫理的・社会的な「シグナル効果」をもたらそうとの国際潮流

Procurement in numbers

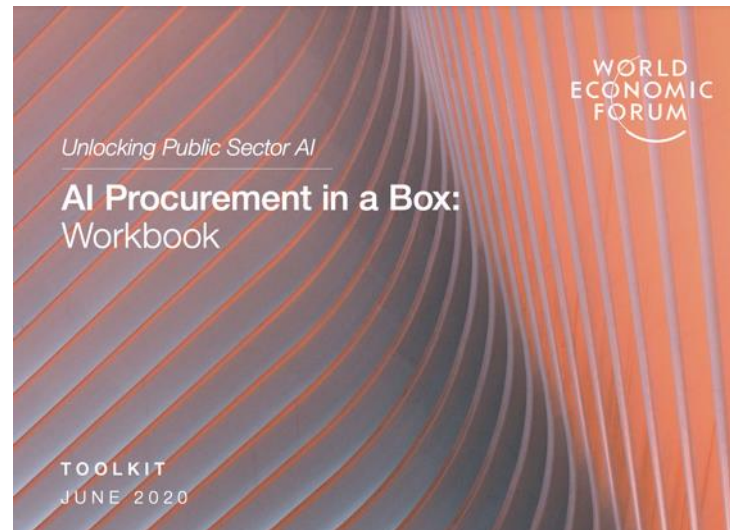
12% Of global GDP is spent following procurement regulation

\$11tr The cost of public procurement globally in 2018



AI&ML 公共調達ガイドラインとワークブック

- 公共部門によるAI&ML利用を見据えて、サービスやUXの向上に寄与し、政府とAIへのトラストを高めることを目指すべく、2020年6月、「AI公共調達ガイドライン」を公表
- 調達担当者のスキルアップを図るべく、「ワークブック」も同時に公開
- 上記について、イギリス政府と連携したパイロットプログラムを実施し、その報告書も公表
- 米州開発銀行に加え、ブラジル、アラブ首長国連邦、米国、イスラエル、日本など各国政府と連携中



<https://www.weforum.org/reports/ai-procurement-in-a-box>
<https://www.weforum.org/projects/unlocking-public-sector-artificial-intelligence>
<https://www.gov.uk/government/publications/guidelines-for-ai-procurement>

AI&ML 公共調達に関する10の指針

1. アジャイル開発型プロセスによる調達	- ソリューションの詳細な仕様の設計ではなく、課題の定義とその解決に焦点を当て調達 - 生じる課題に応じて柔軟に開発できるアジャイル開発を推奨	6. データ利用に対する技術的・倫理的制限の強調、バイアスなどの問題への事前措置	- 対象となるデータの重要性、データの用途が公正であるか考慮 - 提案者にデータの限界性への対処について説明を要求。見逃している可能性のある制限に対処するための計画を策定
2. リスクの評価及びAI利用がもたらす公共利益の定義	- 見積もり時にAI起因のリスクを評価、技術的な代替解決策を検討。AIリスク調査の結果を踏まえた提案であるかも評価 - 公共の利益が評価軸であることを明示	7. 適切なスキルセットと多様性のあるチームの組成	- 調達においては領域横断型チームで検討、意思決定を行う - ベンダーにも適切なスキルセットを持つチームを組織することを要求
3. 国家戦略の一環としての調達	- AIに関する国家戦略やイノベーションに関連した産業戦略などを参照 - 関連省庁・機関と連携、知見を共有	8. アルゴリズムに対する説明責任や透明性の確保のための体制整備	- AIによる意思決定を可能な限り透明化 - システム内外でのインターオペラビリティを確保し、アカウントビリティを担保
4. 提案依頼書(RFP)への関連する法律やガイドラインの組み込み	- 関連するデータや、関連法律や行政規則等を事前調査、RFPに盛り込む - AIシステムに関連し得る企業秘密などの機密情報保護やデータプライバシーに配慮	9. AI提供事業者からの知識移転と長期的リスク評価	- AIを含むツールの取得にあたりアプリケーションの寿命を考慮 - 契約には、非専門家でも可能な運用方法などの知識移転やトレーニングを盛り込む
5. 技術・管理の側面から関連データへのアクセスの実現可能性を明確化	- 調達時に適切なデータガバナンスの仕組みを確保し、プロジェクトに関連するデータが利用できるか評価 - ベンダーとのデータ共有の有無・方法を明確にし、ベンダーにより使用・生み出されるデータへのアクセス権を確保	10. AI提供事業者間での公平・公正な競争条件の整備	- 幅広いAIソリューション提供者とさまざまな手段を通して連絡し、プロセスの早い段階から頻繁にベンダーに働きかける - AIソリューションのインターオペラビリティを確保し、ベンダーロックインを避けるためのオープンなライセンス条件を要求

AI&ML 公共調達ワークショップを日本でも

- 2021年12月9日・11日、日本センター主催で公共調達改革に関する 2Days ワークショップを実施
- Day1は、日本、イギリス、カナダ、ブラジル等の公共調達実務に関わるグローバルなマルチステイクホルダーが参加
- デジタル庁から座間国際戦略統括、吉田企画官が登壇したことをはじめ、日本から幅広い参加
- Day2は、中央官庁や地方自治体、国内大手IT企業やスタートアップ、シビックテックコミュニティなどの多様な関係者が集い、Day1の内容も踏まえ、日本語で討議
- 2日間の内容をまとめ、公共調達改革に関する提言を、2022年1月、デジタル庁に提出

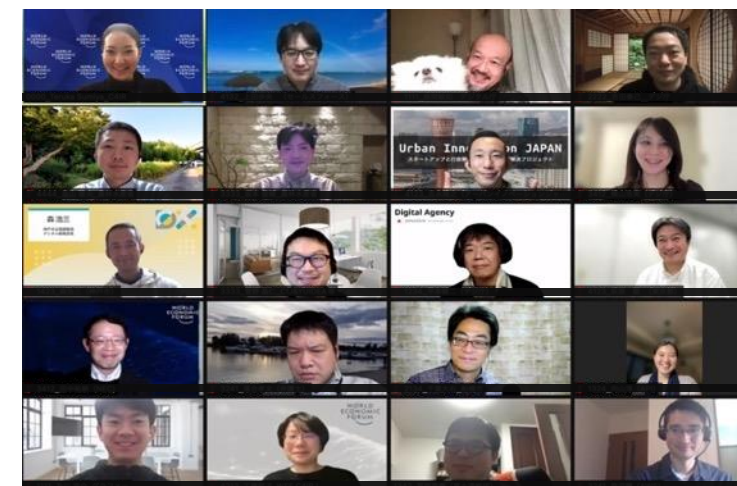


Day1

“Public Procurement 2.0 Webinar”

登壇者（敬称略）

- 座間敏如（デジタル庁 国際戦略統括）
- 吉田泰己（デジタル庁 企画官）
- Alexander Fiddes（英国政府 運転・自動車基準局 デジタルオペレーション部門長）
- Warren Smith（英 Dangersmith社 創設者、元・英国政府デジタル・サービス グローバルデジタルマーケットプレイス プログラム・ディレクター）
- Julián Torres Santeli（デロイトカナダ パブリックセクター データ・AI シニアマネージャー）
- Rafael Fassio（世界経済フォーラム第四次産業革命センター ブラジル政府フェロー）
- Hubert Halopé（世界経済フォーラム第四次産業革命センター AI・機械学習プロジェクト フェロー）



Day2

“Public Procurement2.0:
Multi-Stakeholder Workshop”

しかし...

「AI導入は、遠い未来の話にしか感じられない」

「PoC死とかアルゴリズム・バイアスとかのはるか手前でつまずいている」

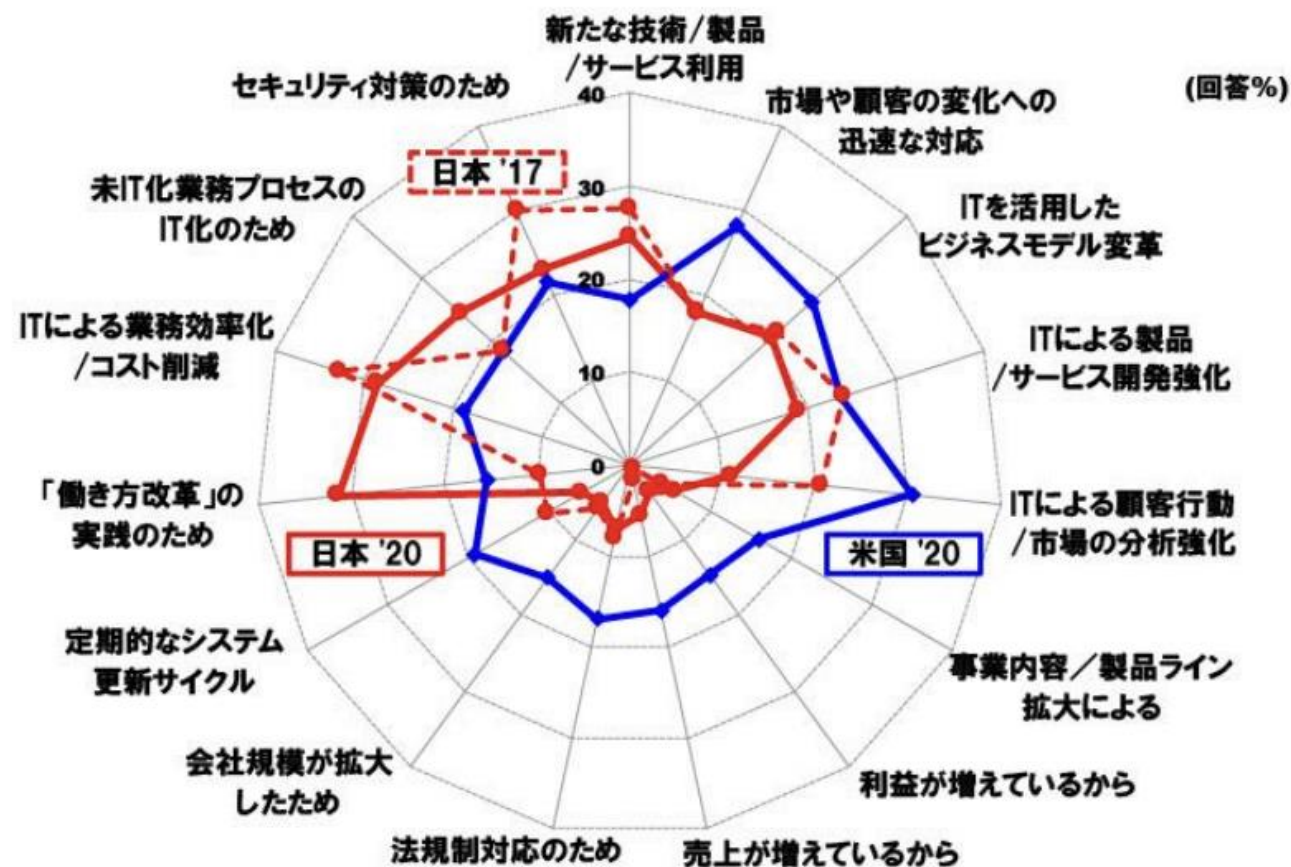
「既存ITシステム調達すら満足にできていない」

現場で何が起きているのか？

- 全体：ある種の公平性・透明性を重視しているため、ゴール・ベース/リスク・ベースが取れない
 - 裁量の逸脱・濫用の防止を目的として、公平に、あらかじめ決まった予算に沿って、形通りに予算執行したい
 - 「調達（選定）という狭い視点しかない」「情報システムが組織戦略として考えられていない」
- 予算要求・編成時
 - Value for Money が正しく評価されない
 - 「“コストは削るもの、投資は適正化するもの” という基本がわかっていない」「バリューに関する意識がないので、取れるリスクの範囲も分からず、先行投資できない」「プライスカップをつければ、IT予算30%削減は誰でもできるのに、それが成果扱いされる」
 - 技術サイクルと政府予算サイクルの不一致（cf. 憲法86条、財政法42条本文）
- 予算執行時
 - 最低価格落札方式の弊害
 - 「受注すればこっちのものだと思っている」「総合評価落札方式で技術点を高くする措置もあるが“付け焼刃”」
 - 「ベンダーロックイン回避ばかりが重視され、その他の価値（知識知見の蓄積、内部管理の容易さ、UXの統一感など）が犠牲になっている」
 - 予算執行が硬直化しており、開発・運用の不確実性を吸収できない
 - 「枠の管理もできない組織が、アジャイルなんてできるわけがない」「そもそも運用を含めたライフサイクルコストが評価されない」

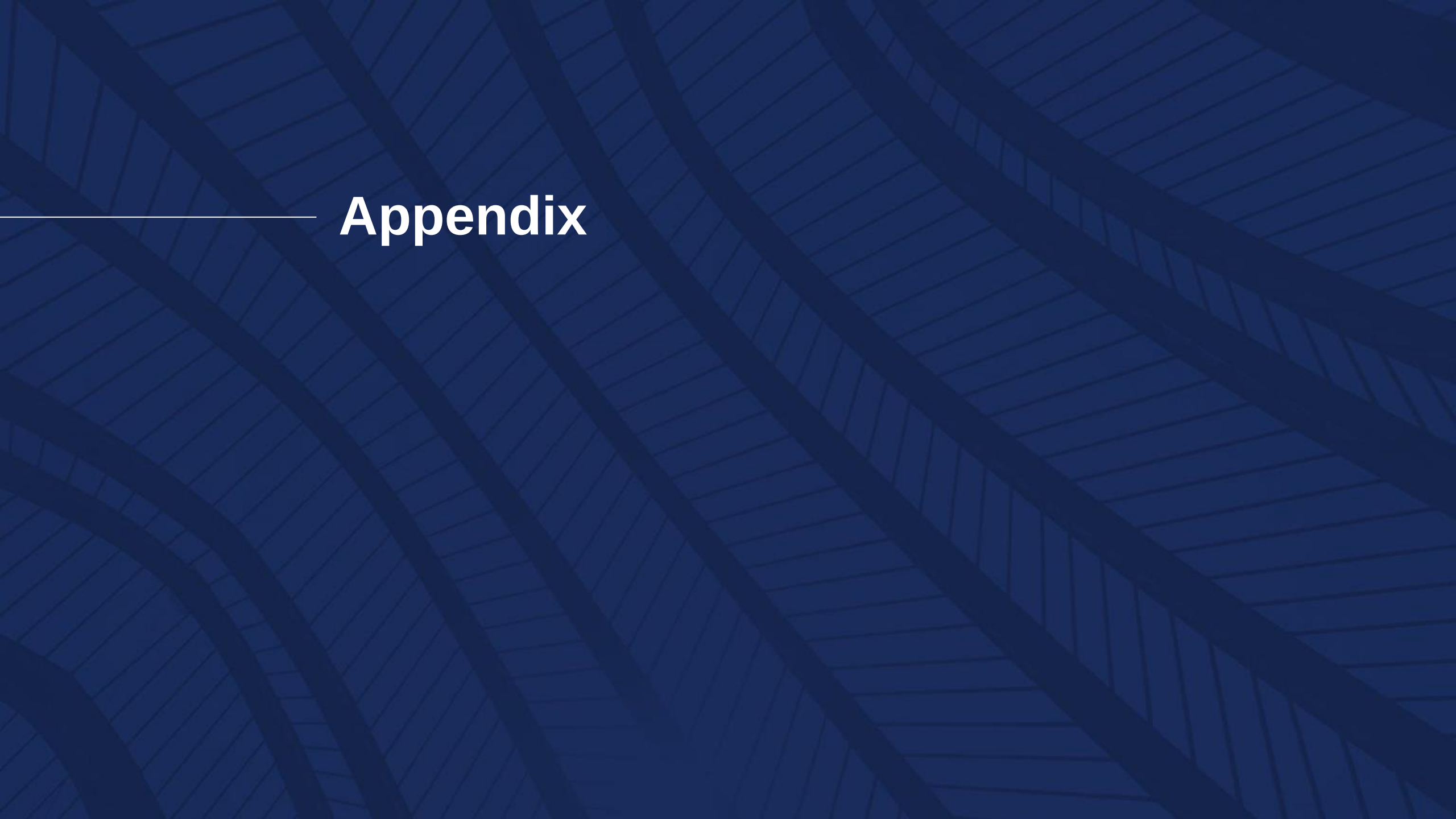
公共調達だけの課題ではなく、民間企業でも？

問：IT予算が増える理由として、どんなものが考えられますか。当てはまるものを3つまで選んでください。



結びに代えて：「隗より始めよ」を実現するために

- 「AI原則実践のためのガバナンス・ガイドライン」は非常に素晴らしい取組み
- 世界経済フォーラムが提案する「AI公共調達ガイドライン」とも重なり合う部分が多い
- ぜひ経済産業省さん自ら率先して、実践・実装いただきたい！
- とはいえ、多くのチャレンジがあることも理解している
- 悩みながら試行錯誤しているのは、日本だけではない
- お互いに学び合い励まし合う、グローバルな官民連携の「場」は提供可能
- 「ワークブック」「ワークショップ」などの実用的なツールも用意されている



Appendix

世界経済フォーラム

- 地球規模課題の解決をめざし、官民両セクターの架け橋の役割を担うスイス連邦政府下の国際機関
- ますます複雑化し、相互依存が進み、急速に変化する経済・技術・環境・社会の課題を、政府、ビジネス、市民社会が単独で解決することは至難
- 世界経済フォーラムは、より良い未来を構築するため、世界の様々なセクターからリーダー達が集まって協力が促進される、グローバルで独立した公平かつ未来型のプラットフォームを提供



17のプラットフォームを通じて、様々な分野で未来を構想

Shaping the Future of...



Advanced
Manufacturing
and Production



Consumption



Cybersecurity



IoT and Urban
Transformation

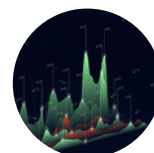
* 第四次産業革命センター



Energy,
Materials and
Infrastructure



Financial and
Monetary Systems



Digital Economy and
New Value Creation



Technology Governance:
Blockchain and
Distributed Ledger
Technologies

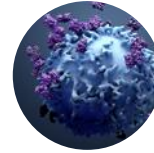
* 第四次産業革命センター



Investing



Media, Entertainment and
Culture



Health and Healthcare

* 第四次産業革命日本センター



Technology Governance:
Data Policy

* 第四次産業革命センター



The New Economy
and Society



Global Public Goods



Mobility

* 第四次産業革命日本センター



**Technology Governance:
Artificial Intelligence and
Machine Learning**

* 第四次産業革命センター



Trade and Global
Economic
Interdependence

世界経済フォーラム第四次産業革命日本センター チーム紹介

事務局



山室 芳剛
センター長



村木 茂大
事務局長



ジョナサン・ソーブル
グローバル・
コミュニケーション
責任者



工藤 郁子
プロジェクト戦略
責任者



岡田 萌乃
オペレーション・
コーディネーター



西澤 美穂
オペレーション・
コーディネーター



齋藤 悠
国土交通省
フェロー



神 亮介
外務省
フェロー



田宮 寿人
財務省
フェロー



樋口 道弘
農林水産省
フェロー



湯山 智教
金融庁
フェロー



隅屋 輝佳
アジャイルガバナンス
プロジェクト
スペシャリスト



岩田 太地
NEC
フェロー

省庁フェロー

アジャイルガバナンス

ヘルスケア・データ政策

モビリティ



藤田 卓仙
ヘルスケア・
データ政策
プロジェクト長



入野 好弘
サントリー
フェロー



岡島 正泰
SOMPO
フェロー



鈴江 康徳
SOMPO
フェロー



田中 祐耕
NEC
フェロー



沈 和曦
マッキンゼー
フェロー



伊藤 雄亮
トヨタ
フェロー



上坂 広人
デンソー
フェロー



鈴木 義一
アイシン
フェロー



本堂 聡
トヨタ
フェロー



余吾 博之
アイシン
フェロー



秋元 一郎
NEC
フェロー

AI

スマートシティ

データガバナンス



Rushi Rama
スマートシティ
プロジェクト長



平山 雄太
スマートシティ
プロジェクト長



遠藤 功
日立
フェロー



鍛 忠司
日立
フェロー



近藤 剛
NTT
コミュニケーション
ズフェロー



南雲 岳彦
MURC
フェロー



濱田 東香
デロイト
フェロー



原元 由貴
デロイト
フェロー



穂高 弥生子
バーカー &
マッケンジー
フェロー



望月 康則
NEC
フェロー



由良 淳一
富士通
フェロー



譲原 瑞枝
セールスフォース
フェロー

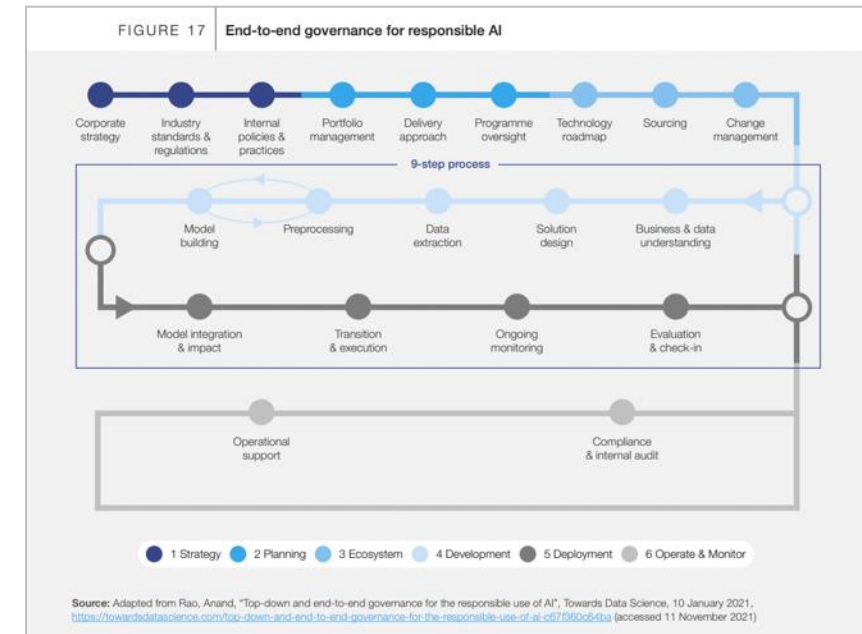
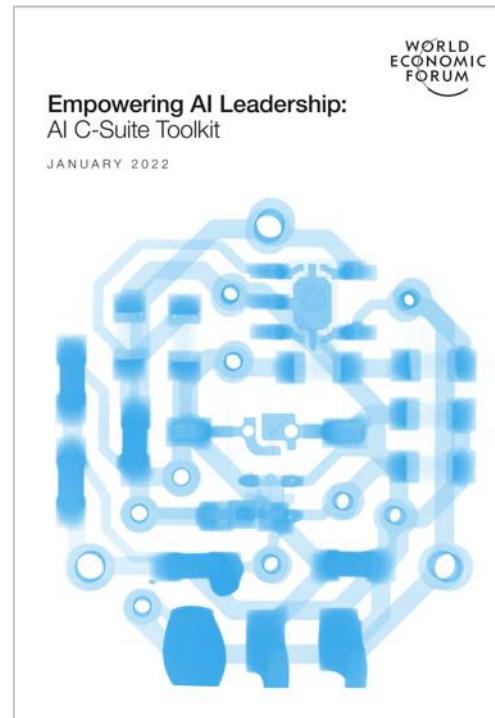
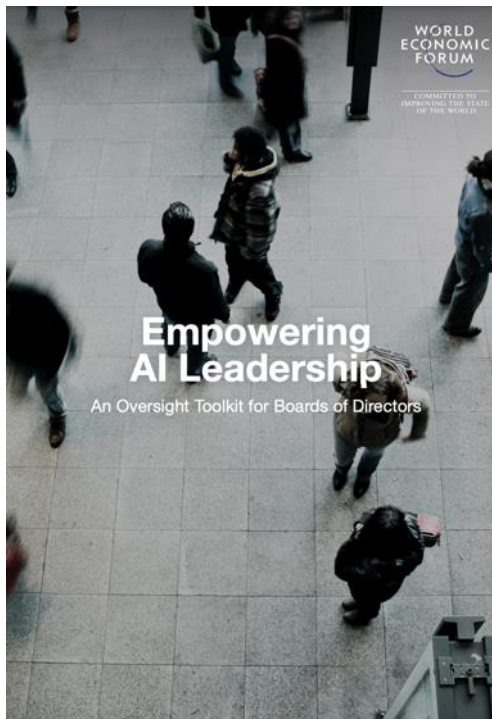
AI&MLプロジェクト例: モデルAIガバナンスフレームワーク

- シンガポール政府とAIガバナンスのフレームワークを共同開発し、2019年1月、ダボスで開催された経済フォーラムの年次総会で発表
- AIの開発・利用についてどのような価値を守るべきか（WHAT）に加え、どのように守るべきか（HOW）をモデル化
- 翌2020年1月、モデルフレームワークの第2版を公表



AI&MLプロジェクト例：経営幹部用AIツールキット

- 2020年1月の「ダボス・アジェンダ」をターゲットに、AI&MLに関するグローバルリーダーたちの学び合いを促進すべく、経営幹部がAIプロジェクトについて十分な情報に基づいて意思決定することに役立つ実用的なツールキット「AI Toolkit for Boards of Directors」を公開
- 2022年1月、「Empowering AI Leadership: AI C-Suite Toolkit」を公開



https://wef-ai.s3.amazonaws.com/WEF_Empowering-AI-Leadership_Oversight-Toolkit.pdf
<https://www.weforum.org/reports/empowering-ai-leadership-ai-c-suite-toolkit>

AI&MLプロジェクト例：顔認証技術の責任ある利用

- 顔認識/顔認証技術につき、2020年3月に示した概括的フレームワークを踏まえ、2020年12月に特定のユースケース（飛行機に搭乗する乗客への利用）に焦点を絞った白書を公開
- 日本からは、成田国際空港とNECが、共同設計と「自己評価調査票の検証」に参画
- 品質管理を含むマネジメントプロセスの具体化の一例

付属文書

付属文書A：成田国際空港の自己評価調査票回答例

1. 顔認証システムの適切な利用

評価に関する質問	成田国際空港による自己評価調査票回答
貴社の顔認証システムの代替案はありますか。そちらを導入しなかったのはなぜでしょうか。これらの代替案の長所と短所を判断するための基準は何ですか。	指紋認識と虹彩認識を代替案として検討しました。比較の結果、以下の点で顔認証の方が優れていると判断しました。 1. 乗客が機器を操作する必要がないため便利 2. 非接触形式で利用できるため新型コロナウイルス感染拡大時に有用だった 3. 誰も持っていない独自の情報を特別な操作なしに収集できる 4. ウォーキングベースというコンセプトが実現できる
貴社システムの目的に対する妥当性をどのように評価しましたか。	以下の3点で評価しました。 1. 高い顔認証精度 2. エンドユーザー（航空会社）の要件を高いレベルで満たせる 3. ウォーキングベース実現に向けた処理性能
貴社システムの目的に対処するための技術的な要件を、該当する機関が理解できる形式で記述してください。	主なポイントは以下のとおりです。 1. 高い顔認証精度 2. ウォーキングベース程度の速さ 3. 既存の航空会社のシステムとの互換性（大規模な修正が必要ない）

3. バイアスと差別

評価に関する質問	成田国際空港による自己評価調査票回答
不当なバイアスは貴社のユースケースではどのように定義されていますか。	パスポートに組み込まれた集積回路 (IC) に顔情報が含まれており、他の空港でも採用されていることから、顔認証システムを採用しました。不当なバイアスとは、さまざまな人種の人々、そして車椅子利用者などの障害者に対する性能（指標：精度や認証時間）の差であると定義しました。ただしパスポートにICが組み込まれていない人や、国独自の理由でサポートを受けられない人は対象外としました。
それぞれの定義の評価に使用されている指標を説明してください。	システム全体のリスク分析の枠組みとしてISO 31000に基づくJIS Q 31000を使用しました。不当なバイアスの評価については、顔認証システムの検証項目としてNIST等によるパブリックレビューの結果をベンダーに提出させています。
貴社のリスク分析の枠組みはどうなっていますか。貴社のユースケースにおいて特定された不当なバイアスのリスク、そしてバイアスの評価を行ったエンドユーザーの特徴で記述されたグループについて説明してください。	システム全体のリスク分析の枠組みとしてISO 31000に基づきJIS Q 31000を使用しました。不当なバイアスの評価については、顔認証システムの検証項目としてNIST等によるパブリックレビューの結果をベンダーに提出させています。
このプロセスでは、リスクはどのように優先順位付けされていますか。競合する利害関係はどのように解決していますか。	システム全体の可用性とセキュリティを最優先としています。システム全体への影響を踏まえて個別機能のレビューを行っています。
このケースで適用された不当なバイアスの検出、特定、緩和のための既存のベストプラクティスについて説明してください。	NISTIR 8280で顔認証ベンダーをレビューし、選択を行った時点で最も優れたアルゴリズムを持つベンダーを選択しました。
特定された主なリスクを軽減するためにどのような行動計画を立てましたか。不当なバイアスのそれぞれのリスクについて、どのような緩和策が特定され、有効性を確保するためにどのように緩和策を評価しましたか。	不当なバイアスの評価については、顔認証システムの検証項目としてNIST等によるパブリックレビューの結果をベンダーに提出させています。選択時点ではNECのシステムが最も精度が高かったことから、そちらを運用と組み合わせることを決定しました。

10. 代替の選択肢と人間の常駐

評価に関する質問	成田国際空港による自己評価調査票回答
顔と写真付きの身分証明書を照合した結果、特に登録段階で偽造性が生じた場合、人間によるレビュープロセスを導入していますか。	人間によるレビュープロセスはありません。 搭乗者情報やパスポート情報などの確認のために航空会社のホストに情報を参照するクラウドサービスを追加することで、全自動化と誤検知の排除を実現しています。
顔認証システムでは、代替オプションは体系的に実装されており、	エラーが発生した場合には、現在の操作と同様の処理が手作業で行われます。 実施しています。現在、手動操作はスタッフが代わりに行っています。
人間によって操作されていますか（そのような操作スタッフは例外的な状況に対処する訓練を受けていますか）	現在、手動操作はスタッフが代わりに行っています。
合理的ですか。つまり不相应に不利な結果をもたらすことはありませんか（保安検査場の通過時間が2倍になるなど）。	既存のシステムと同等のシステムとして使用でき、以前と同じ処理時間で処理可能です。
バイOMETRICSの利用を拒否する人のための代替プロセスはありますか。	既存のシステムと同等のシステムとして使用できます。代替プロセスとして手動操作が用意されています。

https://www3.weforum.org/docs/WEF_Responsible_Limits_on_Facial_Recognition_Japanese_2020.pdf

AI&MLプロジェクト アウトプット例

Best practices



Governance frameworks



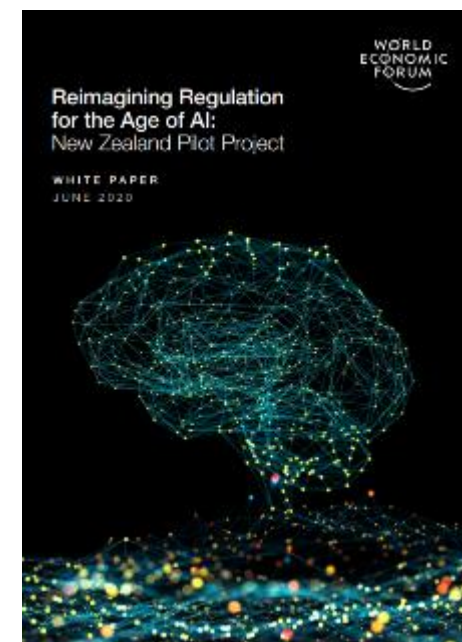
Use cases



Toolkits



Pilots



Thank you.

Questions?

C4IRJapan_info@weforum.org

Follow us:

