2023 年 3 月 6 日

# AI リスクを解決する Robust Intelligence Co-Founder：大柴 行人が自民党「AI プロジェクトチーム」勉強会で「攻めの AI ガバナンス」について講演

## ～AI リスク対策の必要性と、それに立ち向かうための新しいガバナンス観～

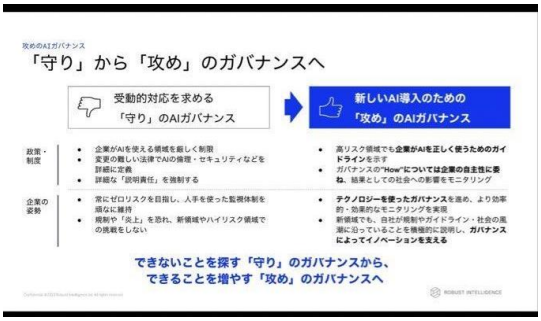
AI リスクを未然に防ぎ、企業の健全な AI モデルの運用“Responsible AI（レスポンシブル AI）”を実現するシリコンバレー発の AI スタートアップ・Robust Intelligence Inc.（本社：米国カリフォルニア州、CEO：ヤローン・シンガー、Co-Founder：大柴 行人、以下：ロバストインテリジェンス）は、2023 年 3 月 3 日（金）に自民党で行われた「AI の進化と実装に関するプロジェクトチーム」勉強会において、現代社会に広がる AI リスクと、それに立ち向かうための「攻め」の AI ガバナンスの考え方に関して講演を行いました。

ロバストインテリジェンスは、AI の開発中にモデルが引き起こす問題をあらかじめ検出する『AI Stress Testing』と運用中の AI の挙動の変化を即時に検知する『AI Firewall®』、そしてモデルに対し継続的な品質検証を可能にする『AI Continuous Testing』を搭載した AI ガバナンスプラットフォーム『Robust Intelligence Platform』を提供しています。これにより、開発段階からの AI モデルリスク管理や運用時の継続した AI モデル検証が可能となり、AI リスクを未然に防ぐことで、企業による“Responsible AI（レスポンシブル AI）”の実現に貢献します。
（https://www.robustintelligence.com/jp）

この度、ロバストインテリジェンスは AI リスクとガバナンスについての社会の認知を広めるため、日々広報活動や公益団体への協力を実施しています。今回は AI ガバナンスにテクノロジーの観点から取り組む日本市場でも唯一のプレイヤーとして、自民党の「AI の進化と実装に関するプロジェクトチーム」への勉強会に出席することとなりました。



勉強会の様子




解説する大柴

当日は、日本のテクノロジー界を牽引する伊藤穰一様と並ぶ形で、サンフランシスコからオンラインで講演を実施しました。創業者大柴からは、大きく下記3つのポイントについて解説しました。

**①AI リスクの重要性とトッププレイヤーたちの取り組み**

データドリフトの発生や差別的予測、敵対的入力など、AI の抱える様々なリスクは、あらゆる産業で対応を迫られる重要なイシューである。すでに、AI ガバナンス・倫理に関するポストの設置や、ガイドラインの制定など、アメリカや日本のトッププレイヤーたちはリスク対策に取り組み始めている。

**②日本企業にとっての「攻めのガバナンス（攻めガバ）」の必要性**

特に、日本においては AI リスクへの恐怖により導入を避ける企業や、導入した AI の「お守り」業務に工数をかけて効率を下げてしまう企業が多い現状があり、こうした課題が AI 利活用を妨げている。この点から、企業が AI リスクを適切に管理し新しい AI の導入を加速する、「攻めの AI ガバナンス」への思考の転換が AI 利活用の起爆剤になりうる。この「攻めガバ」を広められるかどうかが日本の AI 先進国になりうるかの行く末を大きく左右する。

**③政府とともに推進する「責任ある AI 活用」**

AI リスクを理解し、AI を安全に運用する「責任ある AI 活用」を広げていくためには、政府が AI ガバナンスの政策イシューとしての重要度を引き上げ、目指すべきガバナンスの目的や方向性を示すことが必要である。今後はロバストインテリジェンスも政府とともに、企業の挑戦を後押しする AI 制度設計を推し進め、産業界に広めていきたい。

ロバストインテリジェンスは、AI リスクに対応する企業のガバナンス構築を支援し、日本市場における AI 利活用の推進を図るべく、国に対する提言や、産業界を中心とした議論の場の構築といった活動を積極的に実施してまいります。

**【Robust Intelligence について】**

ロバストインテリジェンスは、2019 年にハーバード大学の研究者たちによって創業されたシリコンバレー発の AI スタートアップです。

AI には、従来のソフトウェアには存在しない、精度劣化や倫理的問題などの特有のリスクが存在します。ロバストインテリジェンスはこうした AI リスクに対応する企業のガバナンス構築を支援し、企業の健全な AI モデルの運用“Responsible AI（※）”の実現を目指しています。

具体的には、AI モデルの開発から運用に至るまで End to End でリスクを防ぐため、①開発時にモデルをテストする『AI Stress Testing』、②運用時にモデルを保護する『AI Firewall』、および③モデルを継続的に検証する『AI Continuous Testing』の 3 つのサービスから成るプラットフォームを開発・提供しています。

東京海上ホールディングス株式会社、株式会社セブン銀行、株式会社 NTT データ、NEC 日本電気株式会社（NEC Corporation）、PayPal Holdings Inc. 、Expedia Inc.、アメリカ国防総省など、国内大手企業や米国大手企業への導入実績を誇り、2022 年には「世界で最も有望 AI スタートアップ 100 社『AI100』」に連続で選出されました。

**【Robust Intelligence 会社概要】**

・設立年：2019 年
・所在地：US 94107 California San Francisco 1400 Tennessee St
・従業員数：70 人
・代表者：CEO & Co-Founder Yaron Singer、Co-Founder Kojin Oshiba（大柴 行人）
・主な投資家：Sequoia Capital、Tiger Global、Engineering Capital、Harpoon Ventures、In-Q-Tel
・URL：https://www.robustintelligence.com/jp