

# Microsoft Researchの最新AI研究のご紹介と AI普及に向けて検討すべき課題

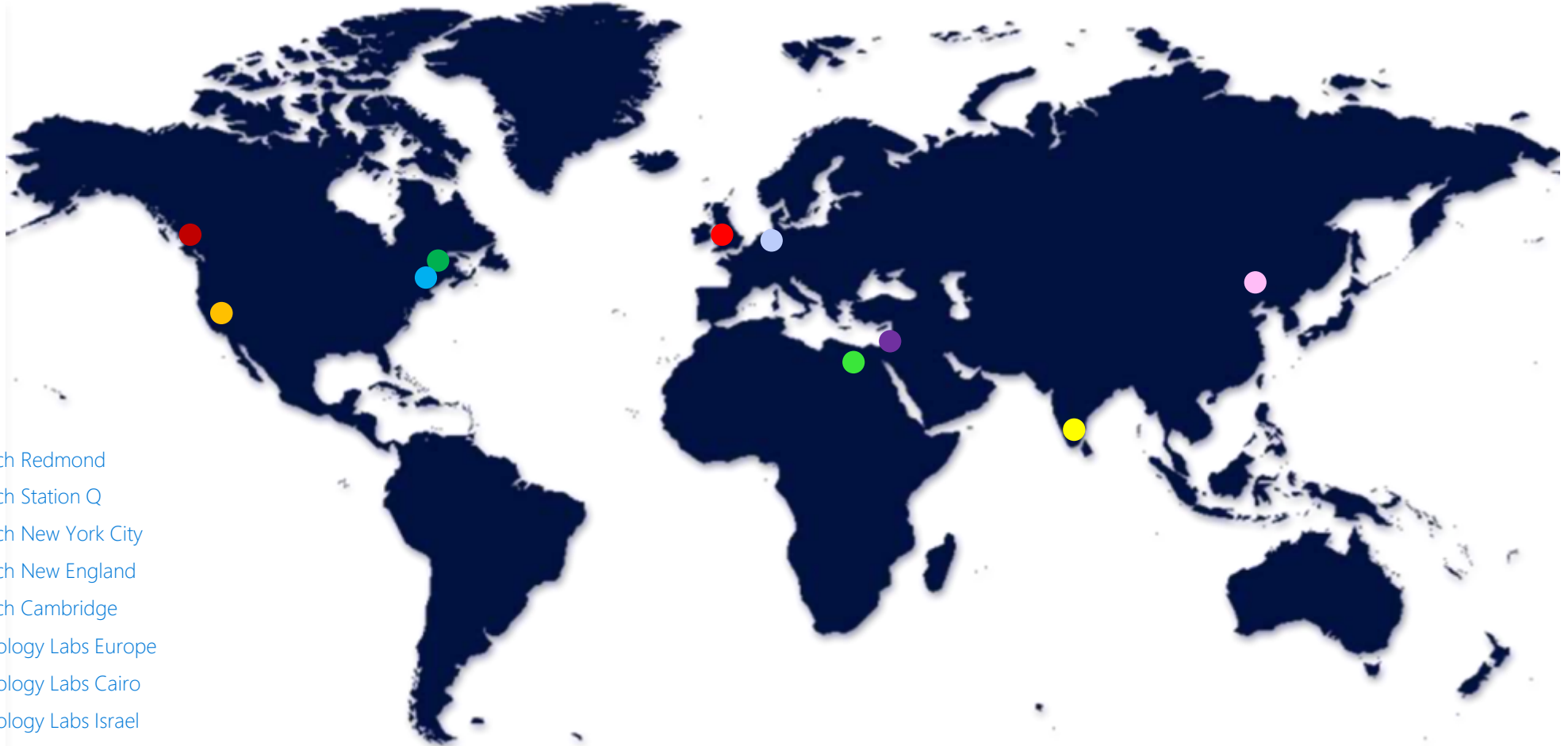
日本マイクロソフト株式会社  
執行役員 最高技術責任者 榊原彰



# MSR と Microsoft の AI

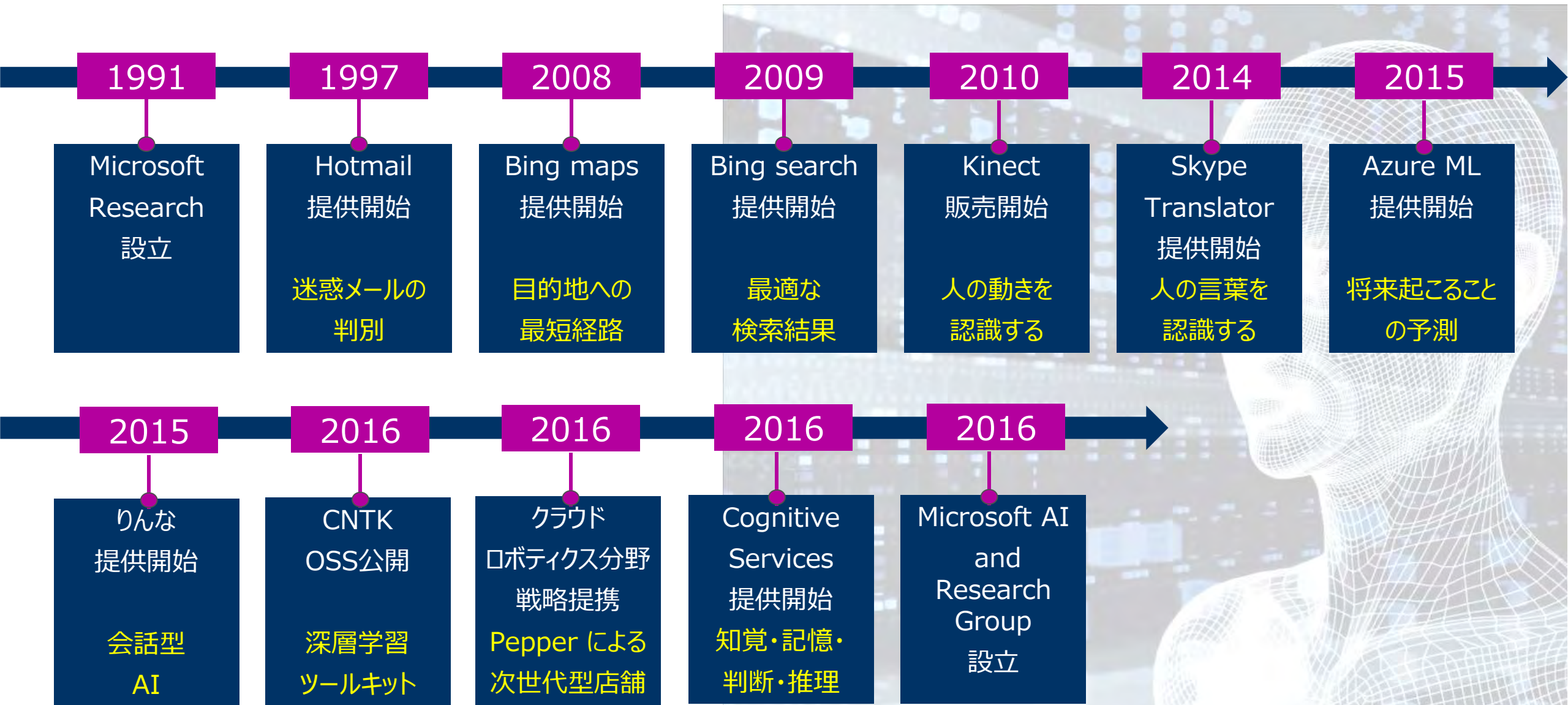


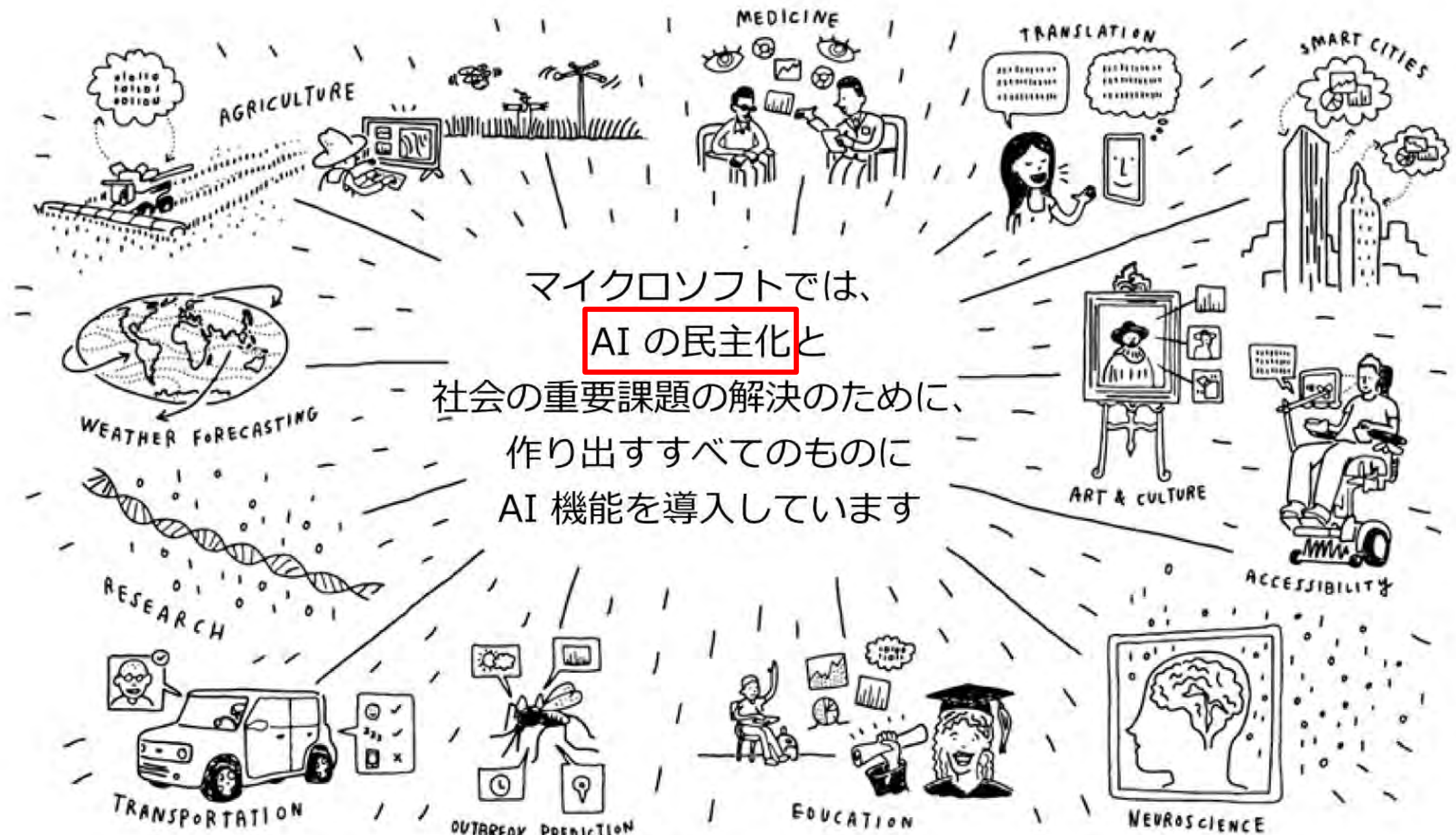
# Microsoft Research Labs



- Microsoft Research Redmond
- Microsoft Research Station Q
- Microsoft Research New York City
- Microsoft Research New England
- Microsoft Research Cambridge
- Advanced Technology Labs Europe
- Advanced Technology Labs Cairo
- Advanced Technology Labs Israel
- Microsoft Research Asia
- Microsoft Research India

# マイクロソフトの25年に渡るAIへの取り組み





## 人間中心のAIめざす 「代替」より「能力拡張」

米マイクロソフトのCEOに聞く

2016/11/15(木) 日本経済新聞

# AIETHER Advisory Panel: AI and Ethics for Engineering and Research

人工知能(AI)の開発レースで先頭集団の一角を占める米マイクロソフトが今夏に公表した独自の開発原則が注目されている。人間の「置き換え」ではなく「能力の拡張」を目指す立場を鮮明にし、開発企業としての説明責任の明確化やプライバシーの保護、偏見の排除などを掲げた。狙いや課題は何か。英紙フィナンシャル・タイムズ(FT)との共同インタビューに応じたサティア・ナデラ最高経営責任者(CEO)に聞いた。

——なぜ開発原則を作り、公表したのですか。

「AIの開発を進めるにあたり、北極星のように動かない原則が必要だと考えた。AIはパソコンや携帯電話、インターネットに匹敵する『ネクスト・ビッグ・シング』だ。すべての人々、あらゆる産業を大きく変える力がある。だが、社内に



## マイクロソフトのAI開発原則

AIに求められるもの	「置き換え」ではなく「拡張」	人間を尊重し、支援するものとして設計されなければならない
	透明性の確保	どのような仕組みで動くかを人間がわかるように設計しなければならない
	多様性の維持	開発にはIT業界だけでなく、多様な人々の関与を求めなければならない
	プライバシーの保護	個人やグループのプライバシーを高度なかたちで守らなければならない
	説明責任の義務	予想外の行動に出た場合、その原因を特定し、再発を防止できるようにしなければならない
人間に求められるもの	共感力	他者に共感する力をAIが身につけるのは極めて難しい。だからこそ、AIと人間が共生する社会において価値を持つ
	教育	AIの普及には必要な知識とスキルを兼ね備えた人材の育成が欠かせない
	創造力	AIは人間の創造力をより豊かにし、拡張するが、創造力そのものは人間だれもが望む能力であり、それはこれからも変わらない
	結果に対する責任	様々な分野でAIの判断を受け入れることはあっても、その結果に対する最終的な責任は人間が負う

# AI 技術普及にむけた連携

AI 技術のリーダー  
5 社が連携

- Amazon
- Facebook
- Google
- IBM
- Microsoft



**Partnership on AI**  
to benefit people and society

AI 技術に普及にあたりベストプラクティスの共有や共通の課題について協議し、人や社会への AI の貢献

<https://www.partnershiponai.org/>

# OpenAIとの提携

Azure N Series

Azure Batch

Azure ML

CNTK etc.

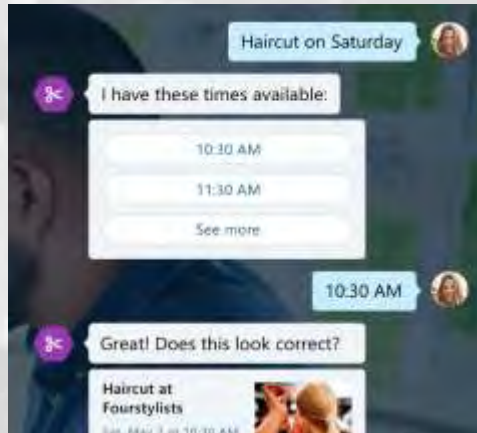




# 現在AIのサービスを展開している領域



パーソナルアシスタント  
(Cortana)



チャットボット  
(BOT Framework)



認識API  
(Cognitive Services)  
翻訳API  
(Microsoft Translator)



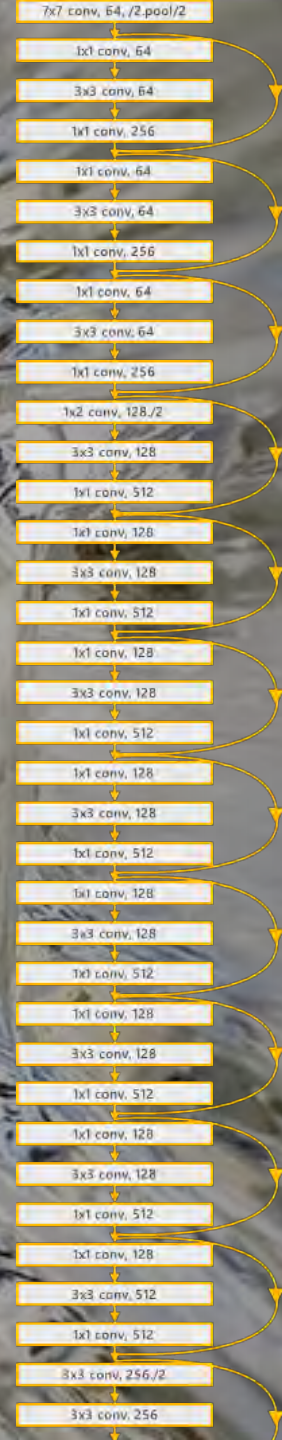
機械学習と開発環境  
(Azure Machine  
Learning Studio)



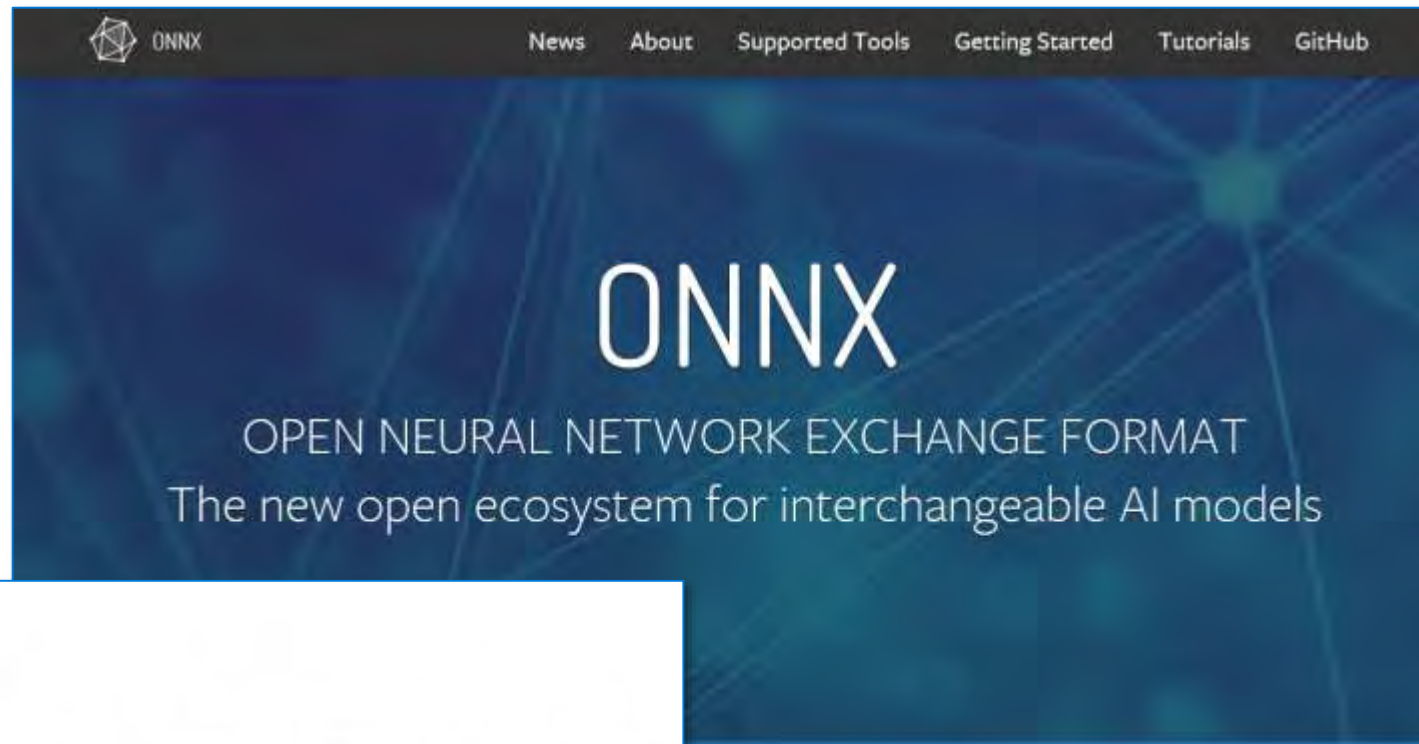
深層学習フレームワーク  
(Cognitive Toolkit)

# 研究Projectのご紹介

- ONNX, Gluon
- BrainWave
- Malmö
- HPU2



# ONNX, Gluonでモデルの効率と可搬性を高める

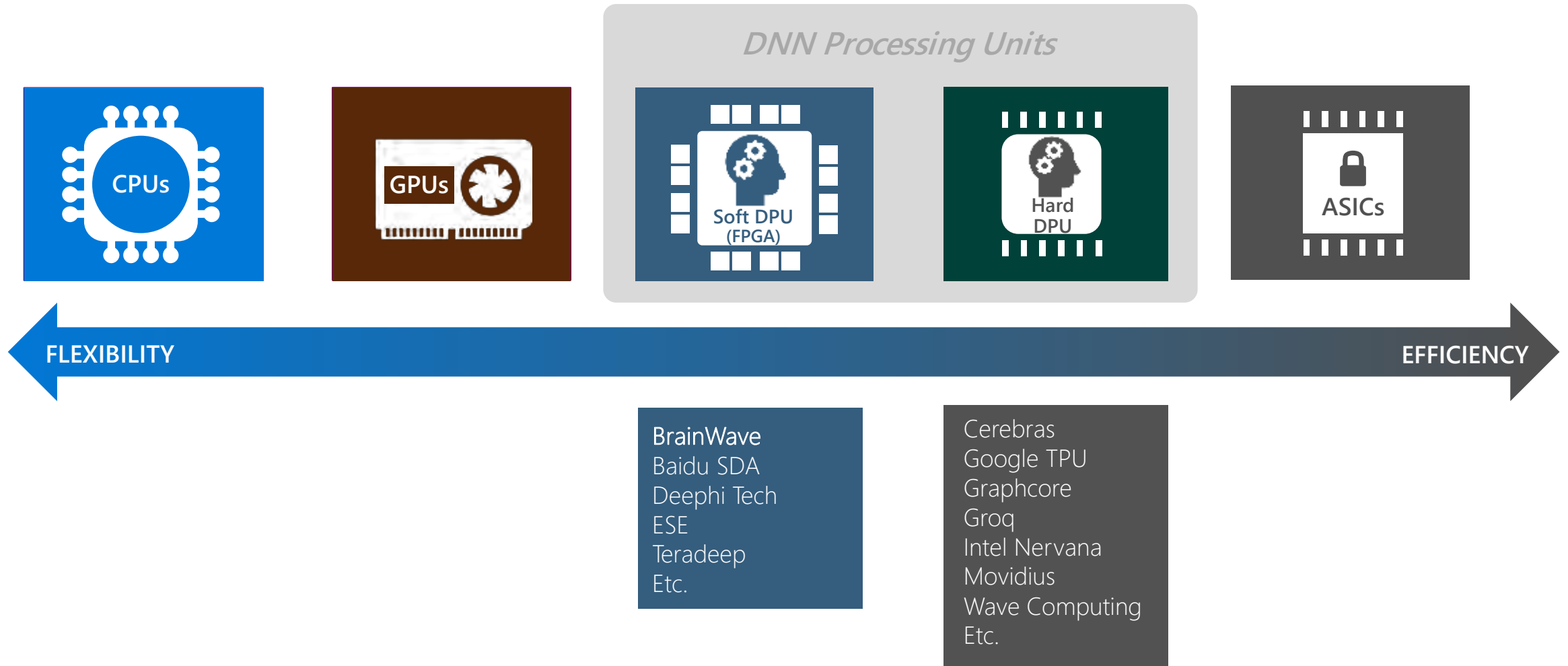


# Project BrainWave

- 高パフォーマンスの分散システムアーキテクチャー
- FPGAに統合されたハードウェアDNNエンジン
- 学習済みモデルをスムーズにデプロイできるコンパイラとランタイム

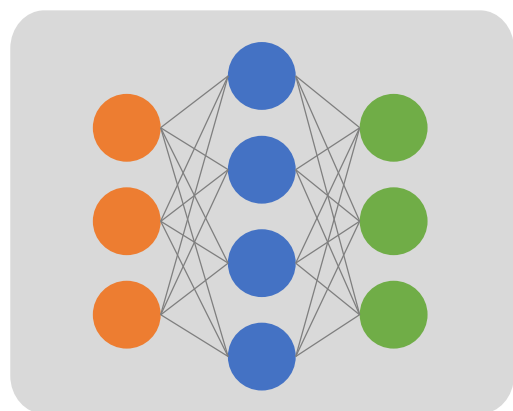


# DNNのための“シリコン・オルタナティブ”

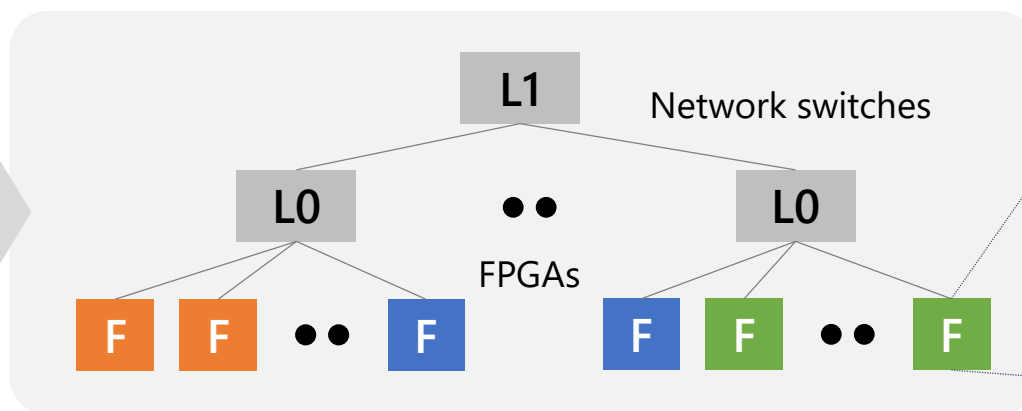


# スケーラブルなDNN H/Wマイクロサービス

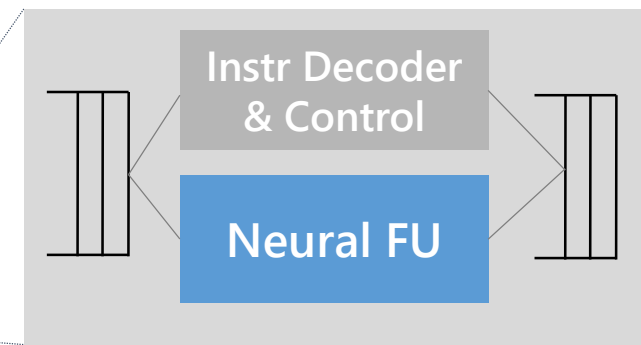
- ハイパフォーマンスのFPGAをMicrosoftのデータセンターネットワークに直接接続
- DNNの機能をハードウェアマイクロサービスとして提供
- DNNをリモートFPGAのプールにマッピング可能
- つまりサーバからソフトウェアなしで呼び出し可能



Pretrained DNN Model  
in CNTK, etc.



Scalable DNN Hardware  
Microservice



BrainWave  
Soft DPU

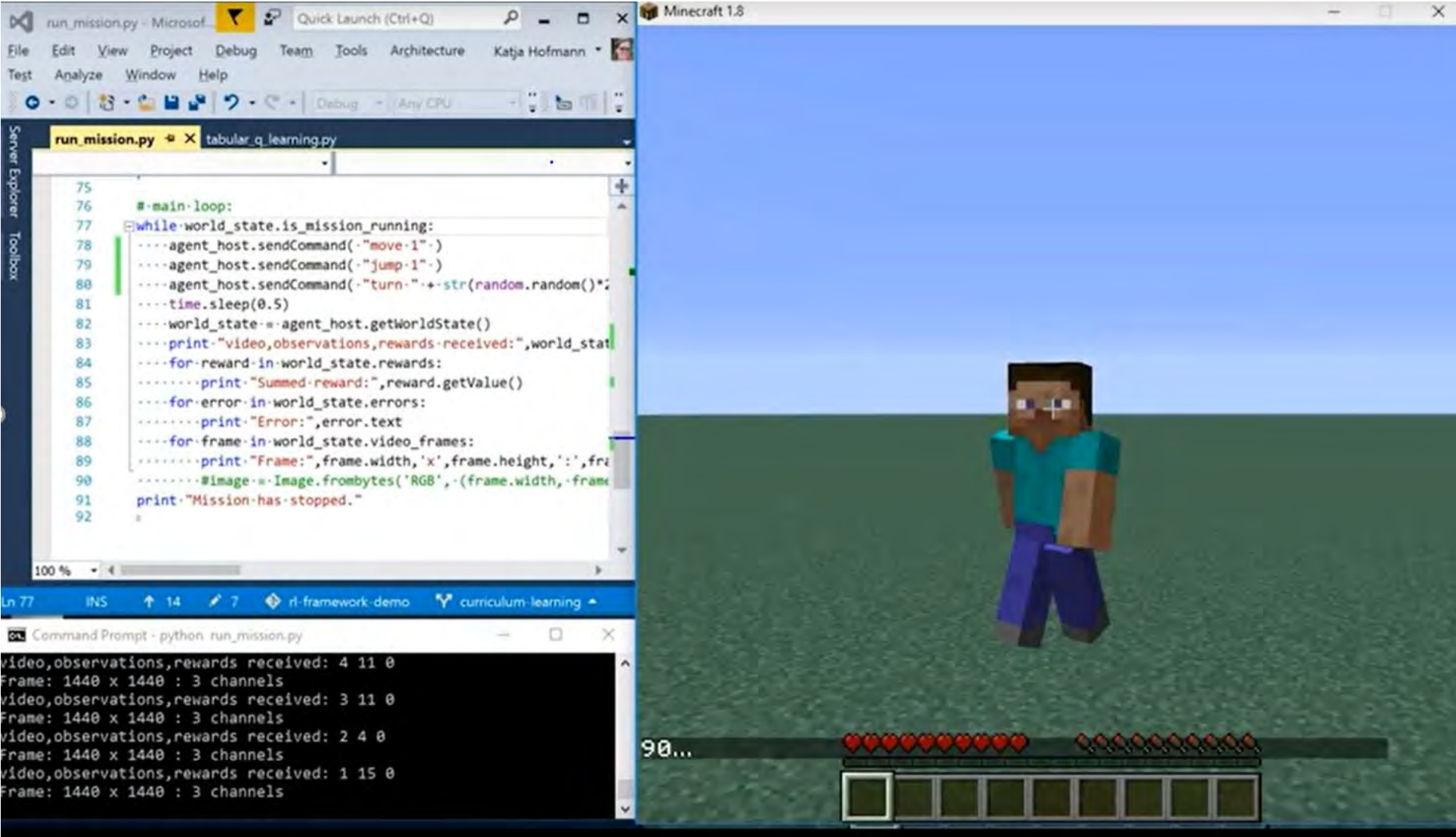
# Project Malmo

- AGIの構築を目指す
- 多様な事象の提供と強化学習
- AIトレーニングにマインクラフトの環境を使用
- GitHubに公開、MITライセンス



<https://www.microsoft.com/en-us/research/project/project-malmo/>

# Java用mod, MacOS/Linux/Windows用コード



The image displays a development environment with three main windows:

- run\_mission.py - Microsoft Visual Studio Code:** Shows Python code for a main loop that interacts with a Minecraft world state. The code includes commands for moving, jumping, and turning, along with sleep and state retrieval functions. It also handles rewards and errors.
- Command Prompt - python run\_mission.py:** Displays the output of the script, showing video frames, observations, and rewards received. The output is as follows:

```
video,observations,rewards received: 4 11 0
Frame: 1440 x 1440 : 3 channels
video,observations,rewards received: 3 11 0
Frame: 1440 x 1440 : 3 channels
video,observations,rewards received: 2 4 0
Frame: 1440 x 1440 : 3 channels
video,observations,rewards received: 1 15 0
Frame: 1440 x 1440 : 3 channels
```
- Minecraft 1.8:** Shows a first-person view of a player character in a flat, open world. The player's health, hunger, and experience bars are visible at the bottom of the screen.

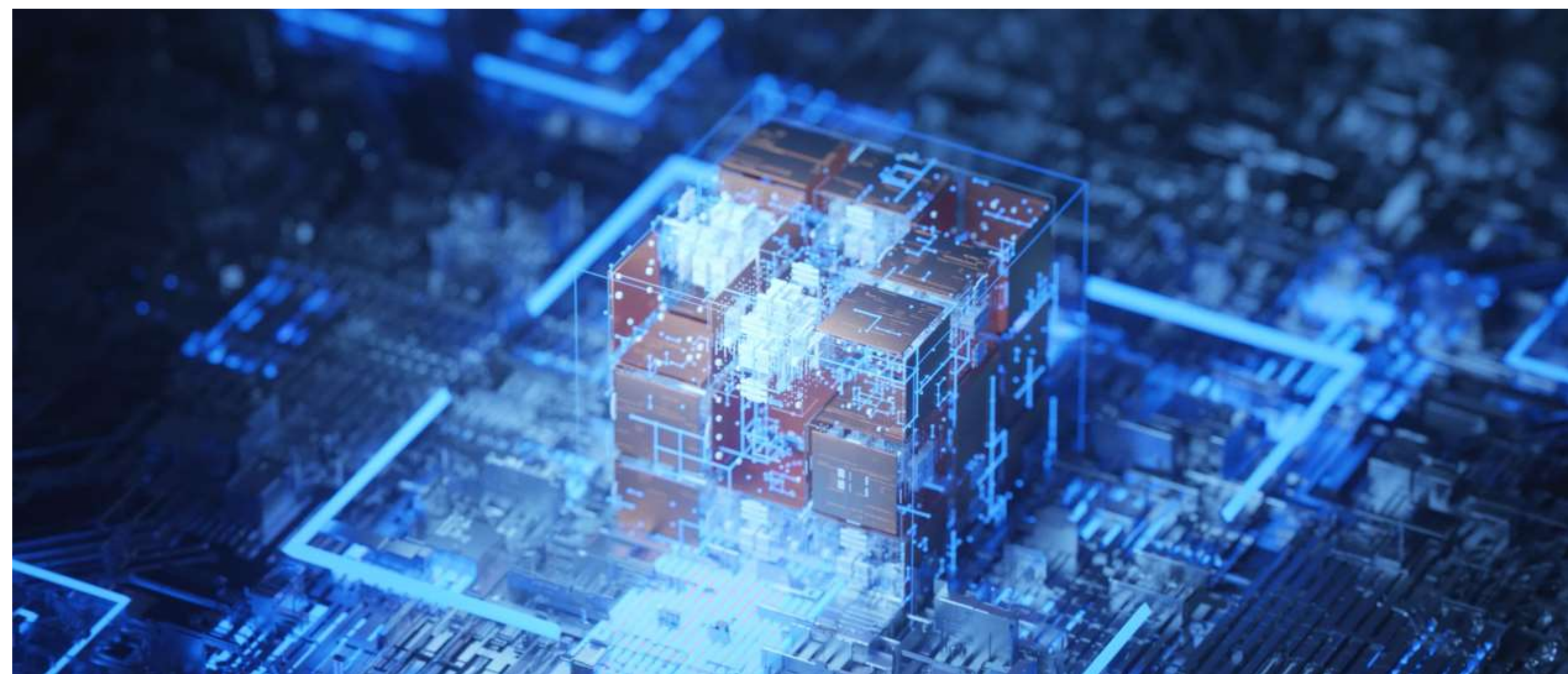


# HoloLens





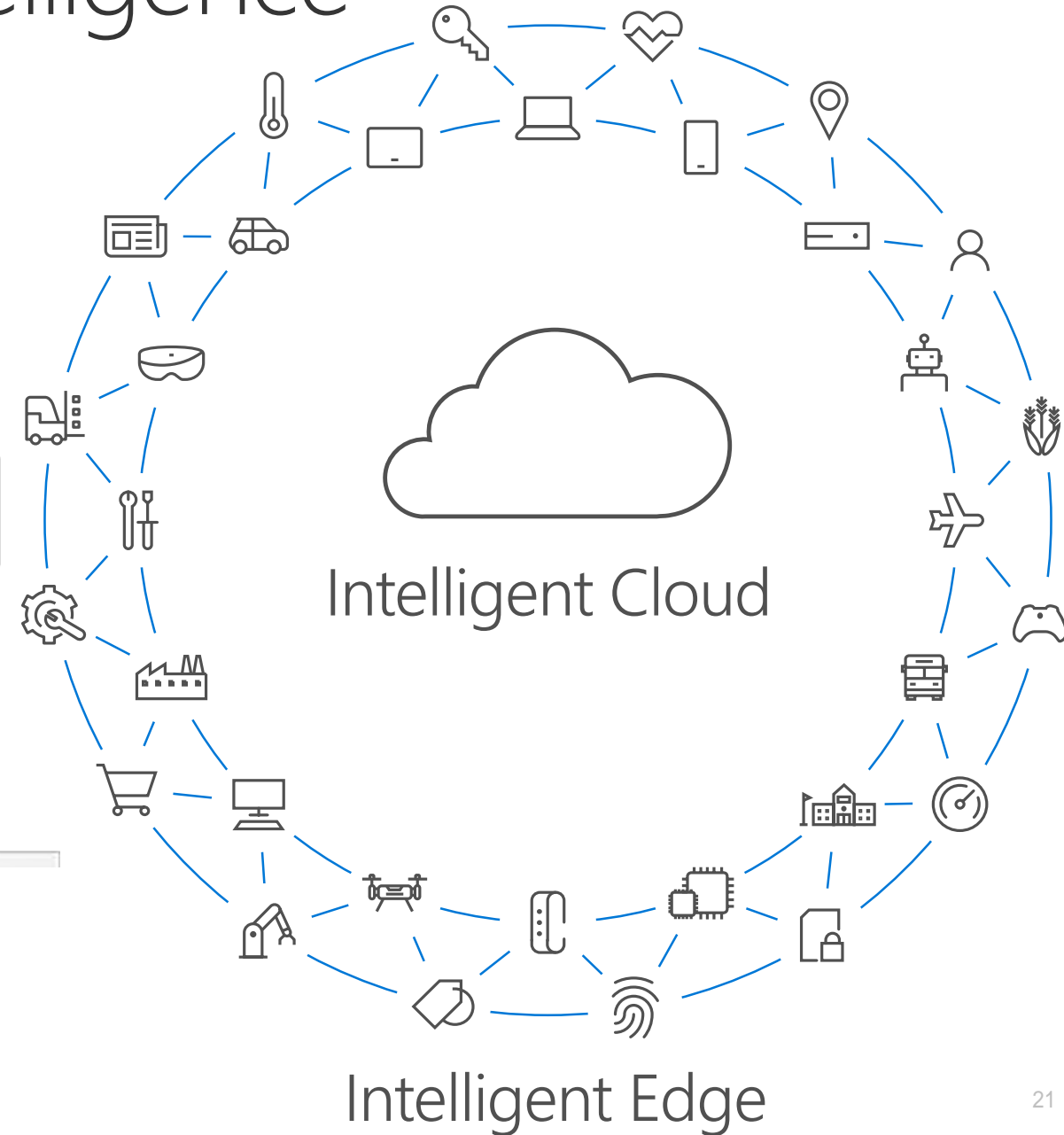
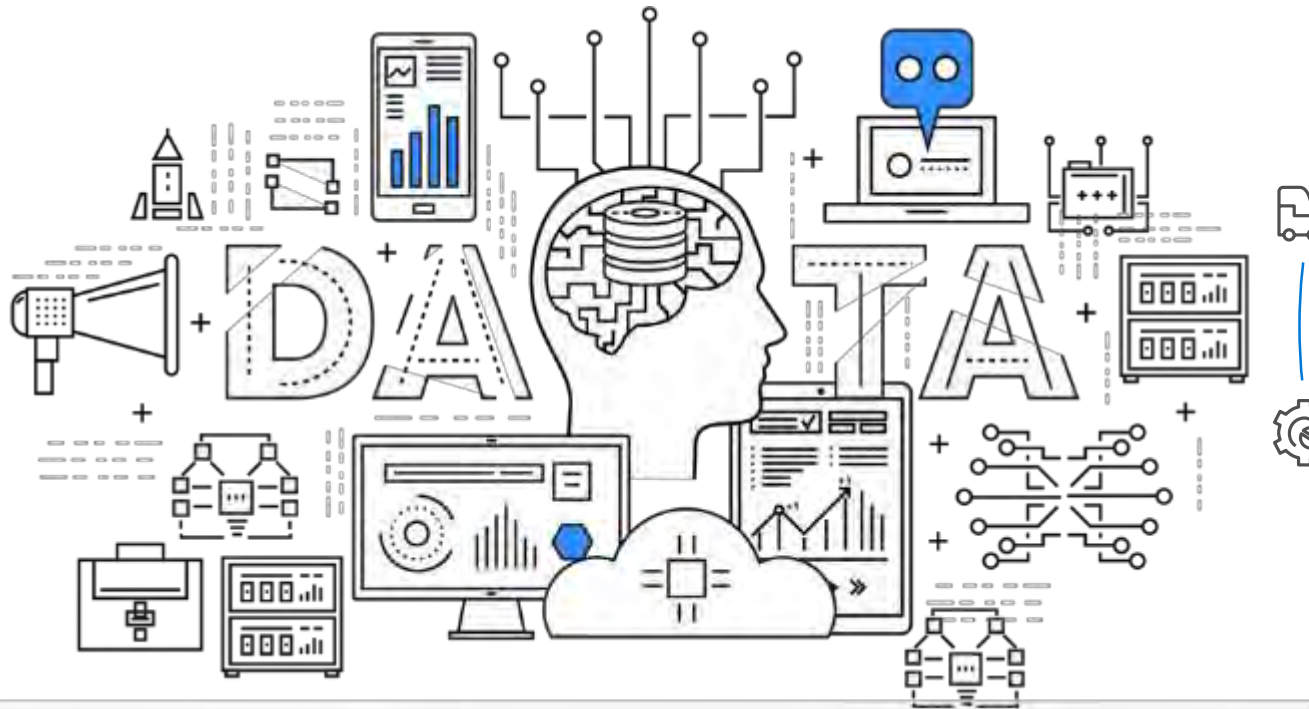
# 次世代のHPUボードには学習済みAIコプロセッサを搭載



# ジェスチャー、周辺環境の画像認識と音声認識



# Data and Intelligence



IoT、ビッグデータ、AI・機械学習で  
変わるセキュリティ

# IoT, AI で変わる セキュリティ





“実際のところ、侵入をしようとするれば必ず侵入できる、  
これを受け入れる必要がある

顧客に対して言えることは：  
あなたの考えにかかわらず、あなたは戦いの只中にいる。  
そして、ほぼ間違いなく侵入されている。”

侵入を前提としたセキュリティ対策が必要

**Michael Hayden**

Principal – The Chertoff Group; Former Director  
of NSA & CIA





# サイバーセキュリティは経営問題

「Cyber security is a CEO issue」<sup>\*1</sup>

90%

企業の約7割はセキュリティ事故を経験 9割は未知の脅威が侵入済み<sup>\*2</sup>



200日以上

攻撃者が検出されるまでに被害者のネットワーク内に潜伏している  
中央値の日数は200日を超える



4.2億円

企業が被るデータ侵害の平均コスト<sup>\*3</sup>



79%

新テクノロジー採用の最大の障壁  
セキュリティ、プライバシーやコンプライアンスの懸念<sup>\*4</sup>



<sup>\*1</sup> Risk and responsibility in a hyper connected world: Implications for enterprises January 2014

<sup>\*2</sup> Verizon 2013 Data Breach Investigation Report

<sup>\*3</sup> Ponemon Institute Releases 2014 Cost of Data Breach

<sup>\*4</sup> APAC CIO 調査

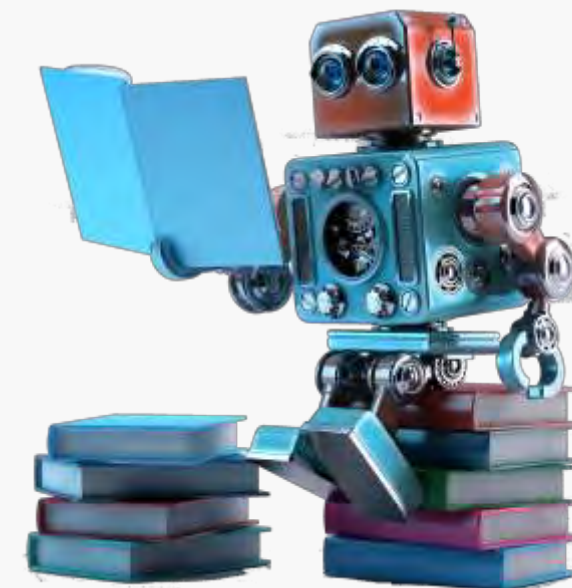
# セキュリティにおける現状

- ファイアウォールは分かりやすい攻撃しか防ぐことができない。
- 常に新たな攻撃手法が開発され続けている。
- 攻撃する側は場合によっては1年以上の時間をかけて侵入する。
- 「怪しいメール開けるな」は無意味。そもそも、真に計画された攻撃に怪しいメールは存在しない。
- ネットワークは必ず侵入される。ネットワーク分離は有効な手段ではない。

# 新たな脅威

1. 悪意・意図をもって気づかれないように少しずつデータにバイアスをかける。
2. ある時、少しずつ付加していたバイアスを正常値に戻す。

バイアスをかけられたデータを学習して作成されたモデルの動作は？



# 気になる知財との関係

- 特許

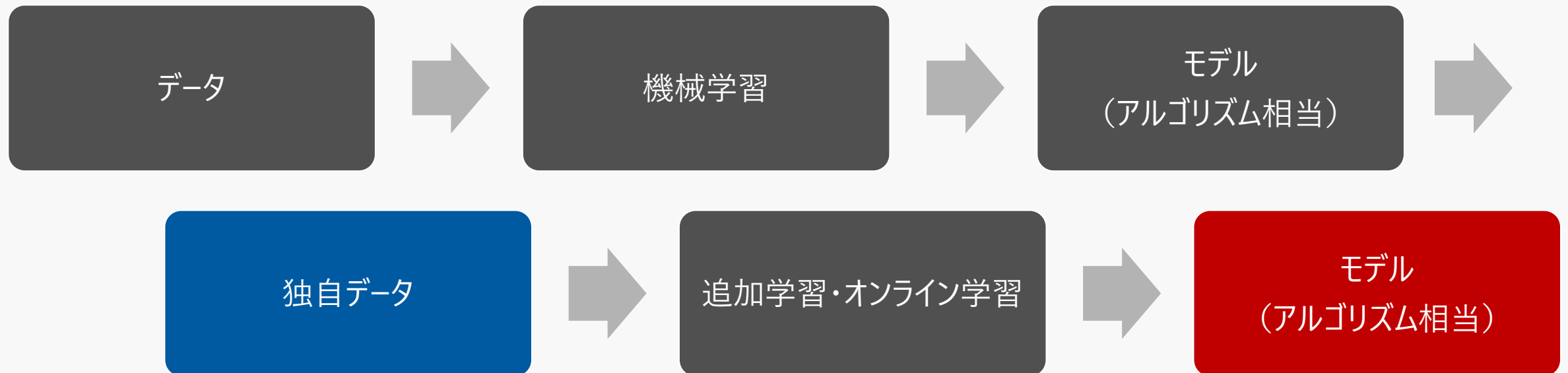
- 新規性（従来にはない新しいものである）
- 進歩性（知技術から容易にできるものではない）

- データと機械学習により作られたモデルは？



# 初期投資をどのように保護するのか

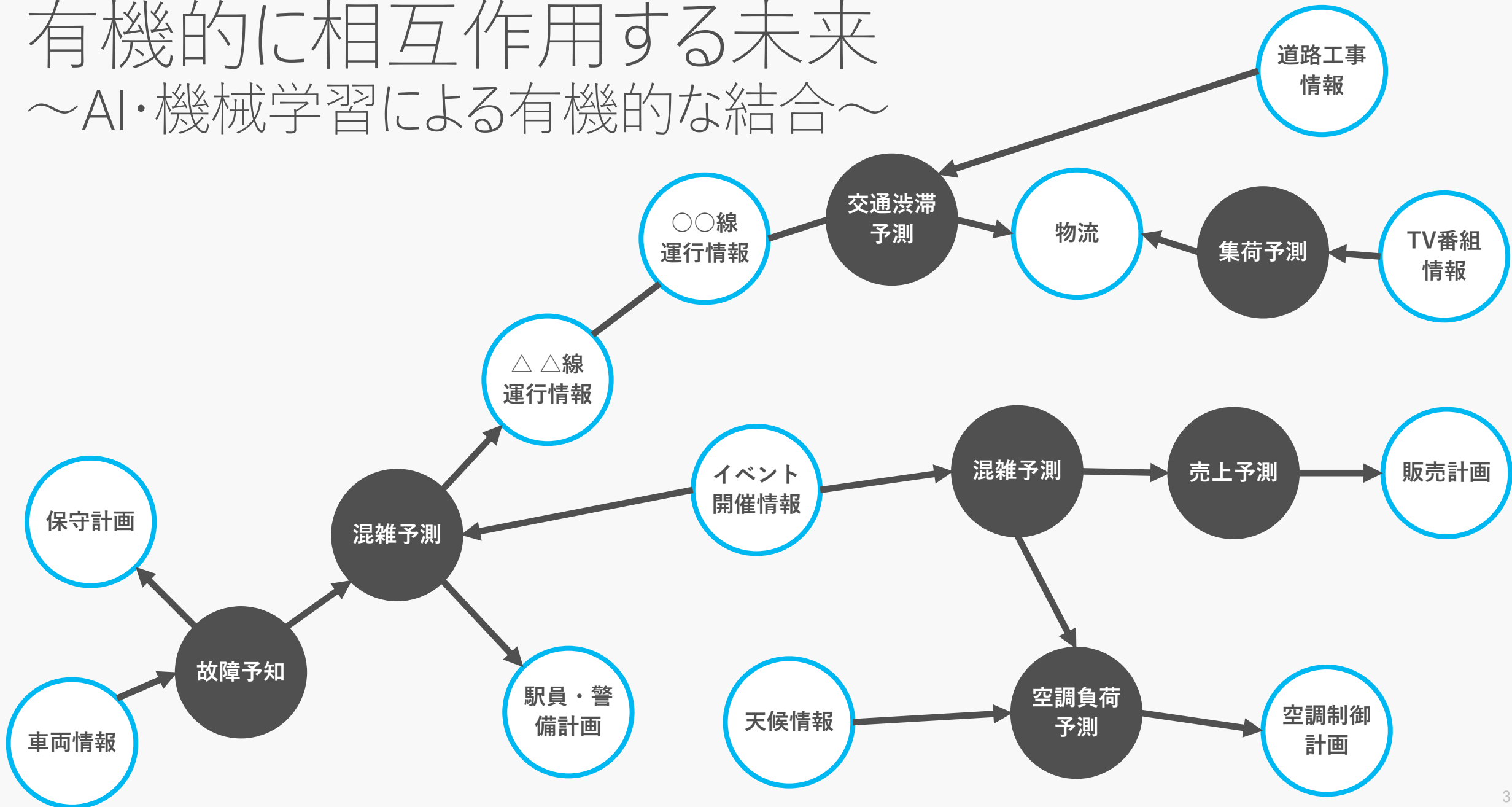
- 多大な投資、試行錯誤により造られた学習結果をどのように守るのか
- Webサービス、APIとしての提供による核心部分を非開示



A photograph of a group of people in a restaurant or cafe. In the foreground, a woman with long brown hair is seen in profile, looking towards the right. Behind her, a man with a beard is partially visible. To the right, another woman with long dark hair is looking towards the man. The background shows a blurred interior with tables and chairs. A semi-transparent blue horizontal band is overlaid across the middle of the image, containing the Japanese word 'まとめ' (summary) in white text.

# まとめ

# 有機的に相互作用する未来 ～AI・機械学習による有機的な結合～





# 実現されようとしている未来

小さいデバイスから人、車、公共交通機関、エレベーター、エスカレーターから街、都市のあらゆるモノが有機的につながり、自律的に運用・管理される世界



Empower  
every person and every organization on the planet  
to achieve more

---

地球上のすべての人々とすべての組織が  
より多くのことを達成できるようにする



# Microsoft

- 本書に記載した情報は、本書各項目に関する発行日現在の Microsoft の見解を表明するものです。Microsoftは絶えず変化する市場に対応しなければならないため、ここに記載した情報に対していかなる責務を負うものではなく、提示された情報の信憑性については保証できません。
- 本書は情報提供のみを目的としています。Microsoft は、明示的または暗示的を問わず、本書にいかなる保証も与えるものではありません。
- すべての当該著作権法を遵守することはお客様の責務です。Microsoftの書面による明確な許可なく、本書の如何なる部分についても、転載や検索システムへの格納または挿入を行うことは、どのような形式または手段（電子的、機械的、複写、レコーディング、その他）、および目的であっても禁じられています。これらは著作権保護された権利を制限するものではありません。
- Microsoftは、本書の内容を保護する特許、特許出願書、商標、著作権、またはその他の知的財産権を保有する場合があります。Microsoftから書面によるライセンス契約が明確に供給される場合を除いて、本書の提供はこれらの特許、商標、著作権、またはその他の知的財産へのライセンスを与えるものではありません。
- Microsoft, Windows, その他本文中に登場した各製品名は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。その他、記載されている会社名および製品名は、一般に各社の商標です。