

2026年10月16日
第2回AIセーフティシンポジウム

米国・アジアのAI政策動向

三部　裕幸
渥美坂井法律事務所・外国法共同事業　パートナー
弁護士（第二東京弁護士会）、ニューヨーク州弁護士
大阪大学招聘教授（社会技術共創研究センター）

Atsumi & Sakai

©Atsumi & Sakai 2026



シンガポール

AIエコシステム・AI政策・AIガバナンス

※　本スライド以降で使われる**「AI OS」**（AI operating system）という言葉は、3つの国・地域や日本・米国・EUの公式用語ではなく、**AI・データ・デジタルツイン・エージェント・制御・ガバナンス・セーフティ・アシュアランス等を統合した産業基盤という分析概念**として使います。

©Atsumi & Sakai 2026

シンガポールの訪問先



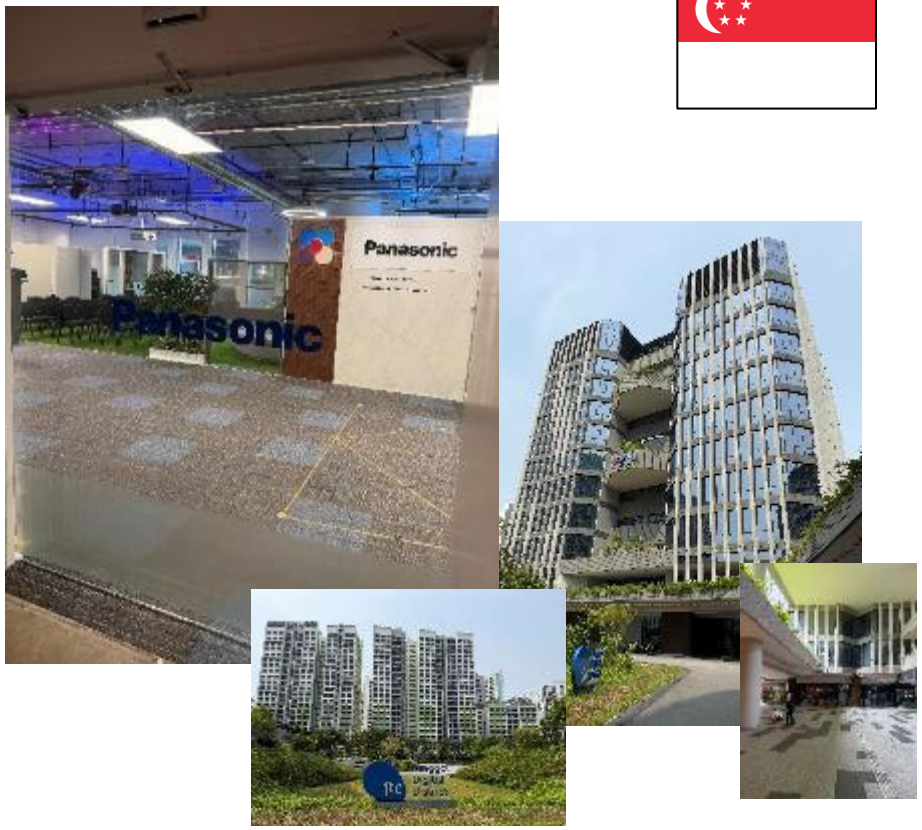
情報通信メディア開発庁
（IMDA）及び
AI Verify Foundation



経済開発庁（EDB）
及び
Digital Industry
Singapore



Simon Chesterman教授
（シンガポール国立大学
（NUS）及び
AI Singapore）



Panasonic R&D Center
Singapore

©Atsumi & Sakai 2026

シンガポールの強さはここにある



長年掛けて確立してきたICTのアーキテクチャをベースに

ガバナンス・テスト・アシュアランスを中核に、

- **ガバナンス（Governance）**：徹底したリスクの洗い出しと評価、そして企業を迷わせないガイドライン
- **テスト（Testing）**：自国・海外のテスト機関
- **アシュアランス（Assuarance）**：世界標準へ

世界企業・実証市場・ASEANをつなぐAI実装のハブであろうとする

グローバルスケール：世界企業の集結・安全な開発・実証、そしてASEANへ展開

世界企業とともに安全な開発 → 実環境での実証 → ASEANへ展開

©Atsumi & Sakai 2026

1. AIガバナンスは、顧客の安心を得て普及を加速する競争力



ガバナンスを「AI開発の制約」と見るのではなく、顧客・市場の安心を得て
実装と普及を加速する競争力として機能させる。その考えに賛同する
AI企業は、米国のフロンティアAI企業をはじめ、170社がシンガポール機関に参加

アマゾン、グーグル、マイクロソフト、メタ、IBM、デル、レッドハット、アドビ、オープンAI、アンソロピック、データロボット、
HPEなどの米国勢、ファーウェイ、センスタイム、テンセントなどの中国勢ほか
世界のAI主要企業は、統一的・標準的ガバナンスが必要だと考えている。それでなければ売れないと。

政策の進化

2019/20
Model AI Governance Framework (MGF)
企業が実装できる原則・手順

2022/23
AI Verify / AIVF
原則を技術テスト・自己検証へ

2024–25
GenAI MGF / Moonshot / Assurance
レッドチーミングや多様なテスターで検証

2026
Agentic AI MGF
ヒューマン・チェックポイント・技術統制を具体化

特徴

① シンガポールと参加企業共同で、詳細なリスク分析とその更新

② シンガポールがフレームワークを作るのではなく共創する。
内容はユースケースに沿った、企業が迷うことのないもの

③ その内容をダウンロードして適用した企業は、テストツールキットを
ダウンロードし、適合性を技術テストし、自己検証する。

④ 国際相互運用性を重視、EU・米国・OECD等との整合／クロスウォークを
実施。クロスウォークメンバーを用意、各国の最新状態を追跡

⑤ ガードレールをイノベーションの条件にする。
安全をブレーキではなく、実証・実装の基盤として扱う。

法的位置づけ：包括的AI法で一律統制するのではなく、共通ガバナンス＋既存の分野規制を組み合わせる。
しかし、法規制は必要になるかもしれない、そのときは必要な部分に個別法を設定する。

©Atsumi & Sakai 2026

2. ガバナンス・アーキテクチャは「理念」から「検証・保証・標準」へ進化



シンガポールは、20年前から、ICT社会のアーキテクチャを詳細に設計し、ぶれることなく継続した。そのことがAI社会にスムーズに移行できた要因であり、その時点で、大きなアドバンテージとなった。そして・・・

2019	2022	2024	2025	2026
Model AI Governance Framework	**AI Verify ツールキット**	**生成AIテスト／Project Moonshot**	**Global AI Assurance**	**国際標準／MGF for Agentic AI**
リスクを厳密に抽出した実装可能なガバナンス	自己診断・技術テスト	生成AIのリスクを技術的に検証 レッドチーミングもこの時点で採り入れ	多様なテスターとコンテキスト別評価、テスターは世界の10数社	綿密なクロスウォーク・国際標準化
		Project Moonshotのダウンロード数 3万		エージェントAIのリスクを技術的に検証

生成AIが世に出てすぐにリスクを技術的に検証する素早さ

開発 → 自己診断テスト → アシュアランス → 実装 → エビデンス →
フレームワーク／標準改訂という<u>フィードバック・アーキテクチャ</u>の形成が信頼を厚くしている

©Atsumi & Sakai 2026

3. 現状の動向：世界企業を呼び込み、AIの研究開発を共同で行い、シンガポールの世界級ともいうべき産業を使って実証・実装を行いながら「産業AI OS」を目指す



シンガポールには、世界のAI企業にとってメリットとなる要素が多々存在する。

① **各種支援策**が用意されている（今後も拡充される）
② **予測可能性の高い制度**、**ガバナンス／アシュアランス**の利用、**他機関との連携**
③ **シンガポール自体の世界レベル産業**が**実装市場**になる

シンガポール・台湾・韓国の共通点：グローバルテックを「外資」として使うのではなく、
共同開発・実証・人材・標準・サプライチェーンを通じて国内能力へ転換 → 高付加価値AIシステムの輸出へ

AI研究開発参加企業の例：NVIDIA、OpenAI、Google、Microsoft、AWS、Oracle、Mastercard、UBS、HSBC、Prudential、GE等70社超

AIビジネス環境が整備
AI／クラウド
半導体／産業技術
製薬／金融
HQ・R&D・
投資の呼びかけ

シンガポールで提供できること
予測可能性の高い制度
政府・企業との対話
テストベッド／サンドボックス
ガバナンス・アシュアランス
セクターデータ
研究機関との連携

世界級の実装市場
シンガポールは世界級産業が多い
金融・製造・ヘルスケア・
コネクティビティ
さらに物流・港湾
公共部門など
そこを実証・実装市場として利用可
例えば、当国の世界チップ生産
約10%、ウェーハファブ生産約5%

©Atsumi & Sakai 2026

4分野を重点化

（前ページの「③　シンガポール自体の世界レベル産業」のうち）



先進製造、金融、ヘルスケア、コネクティビティを選び重点化

この4分野の選定にはかなり明確なロジックがある

① **既に国際競争力**を持つ分野

② 4分野合計で**GDPの40%超**

③ **政府がデータアクセスや規制のサンドボックスなどを提供**することで**AI導入を加速できる**分野

④ そこで作った解決策を**世界にも展開できる**分野

「シンガポールが既に世界的競争力を持つ産業にAIを掛け算して、次の世界的競争優位を作る」

©Atsumi & Sakai 2026

先進製造｜Advanced Manufacturing

既存の世界級製造基盤を、AI-nativeな工場・産業へ転換



WHY｜なぜ選んだか

半導体、精密工学、バイオ医薬などの高度製造基盤と、多国籍企業の工場・R&D集積がある。

AI｜何をしようとするか

AIファクトリー／予知保全／品質検査／工程最適化／ロボティクス・フィジカルAI／共通AIモデル

Aim｜シンガポールの狙い

世界最高水準の工場と新しい製造AIソリューションをシンガポールで実証し、海外展開できる形へ。

なぜシンガポールにとって重要か

半導体・精密製造・電子産業など既存の強い製造基盤を維持・高度化することが国家競争力に直結。**世界の半導体の約10%、半導体製造装置の約20%をシンガポールが生産。**

AIで何を狙うか

Embodied / フィジカルAI、AIファクトリー、自律化、品質・工程最適化を組み合わせ、製造競争力を継続的に引き上げる。

・・・・・・しかし、そこで止まるとも思えない。

AI研究開発参加企業との共同でどこまでAIエコシステム化できるか？ ：NVIDIA、OpenAI、Google、Microsoft、AWS、Oracle、Mastercard、UBS、HSBC、Prudential、GE等70社超

「工場にAIを導入」から「AIが工場を動かす」へ、そして「製造AI OS」を商品化へ？

©Atsumi & Sakai 2026

ヘルスケア｜Healthcare

医療の質・生産性・安全性を同時に高めるAI実装



WHY｜なぜ選んだか

高度な公共医療、統合された医療システム、医療データ、バイオメディカル研究基盤と強い政府関与がある。

AI｜何をしようとするか

診断／臨床意思決定支援／予防・ポピュレーションヘルス／業務効率化／生成AI・エージェント／創薬支援

Aim｜シンガポールの狙い

高齢化・医療人材不足をAIで補い、安全なヘルスケアAIをスケール。

なぜシンガポールにとって重要か

高齢化と医療需要増という明確な社会課題があり、同時に医療制度・バイオメディカル研究の基盤が整っている。

AIで何を狙うか

診療・予防・創薬・医療オペレーションへAIを組み込み、より良いヘルスケアと医療生産性の向上を両立。

AI研究開発参加企業との共同でどこまでAIエコシステム化できるか？ ：NVIDIA、OpenAI、Google、Microsoft、AWS、Oracle、Mastercard、UBS、HSBC、Prudential、GE等70社超

「医療AIの実証」から「安全にスケールするヘルスケアAI」へ、そして、「ヘルスケアAI OS」を商品化？

©Atsumi & Sakai 2026

シンガポールのAI・ロボティクス実証実験場：分散型「リビングラボ」構造

研究室内の試験でなく、都市・工場・建設・道路・港湾という「実環境」ごとに検証→実装→標準・安全要件の実験を同時に行う

① Punggol Digital District (PDD)

北東部・Punggol｜都市・建物・公共空間

複数事業者のAMR/配送・警備・清掃ロボットを同一街区で実証。
建物・エレベーター・ドア・Open Digital Platformとの相互運用、安全・商用性を検証

都市フィジカルAI／2026年本格化

② A*STAR ARTC

西部・CleanTech Park｜先端製造

産業用ロボット、協働ロボット、モバイルマニピュレーション、人間–ロボット協働、
デジタルツイン等。研究成果を企業の製造工程へ移す官民実装拠点。

製造AI・ヒューマノイド・ロボティクス

③ Jurong Innovation District / BAY

西部・Jurong｜建設・重機・産業

Bulim Autonomous Yardで自律型の掘削機／締固め機等を実環境試験。
ジオフェンシング・LiDAR・緊急停止・遠隔監視からフリート協調へ。

建設フィジカルAI

シンガポール

フィジカルAI／ロボティクス
実環境テストベッド・ネットワーク



実証実験場はシンガポールのAIの安全のキー

④ CETRAN (NTU)

西部・CleanTech Park｜自動運転

1.8haのAV試験施設。実車試験とシミュレーションを組み合わせ、自動運転車の試験要件・安全・標準を研究。

モビリティAI／安全・検証

⑤ MPA / Tuas Living Lab

南西部・Tuas / 港湾海域｜海事・港湾

海洋ドローン、自律運航船、通信、港湾自動化を実海域・実港で検証。
Tuas Living Labでは自動運転車等を次世代自動港へ接続。

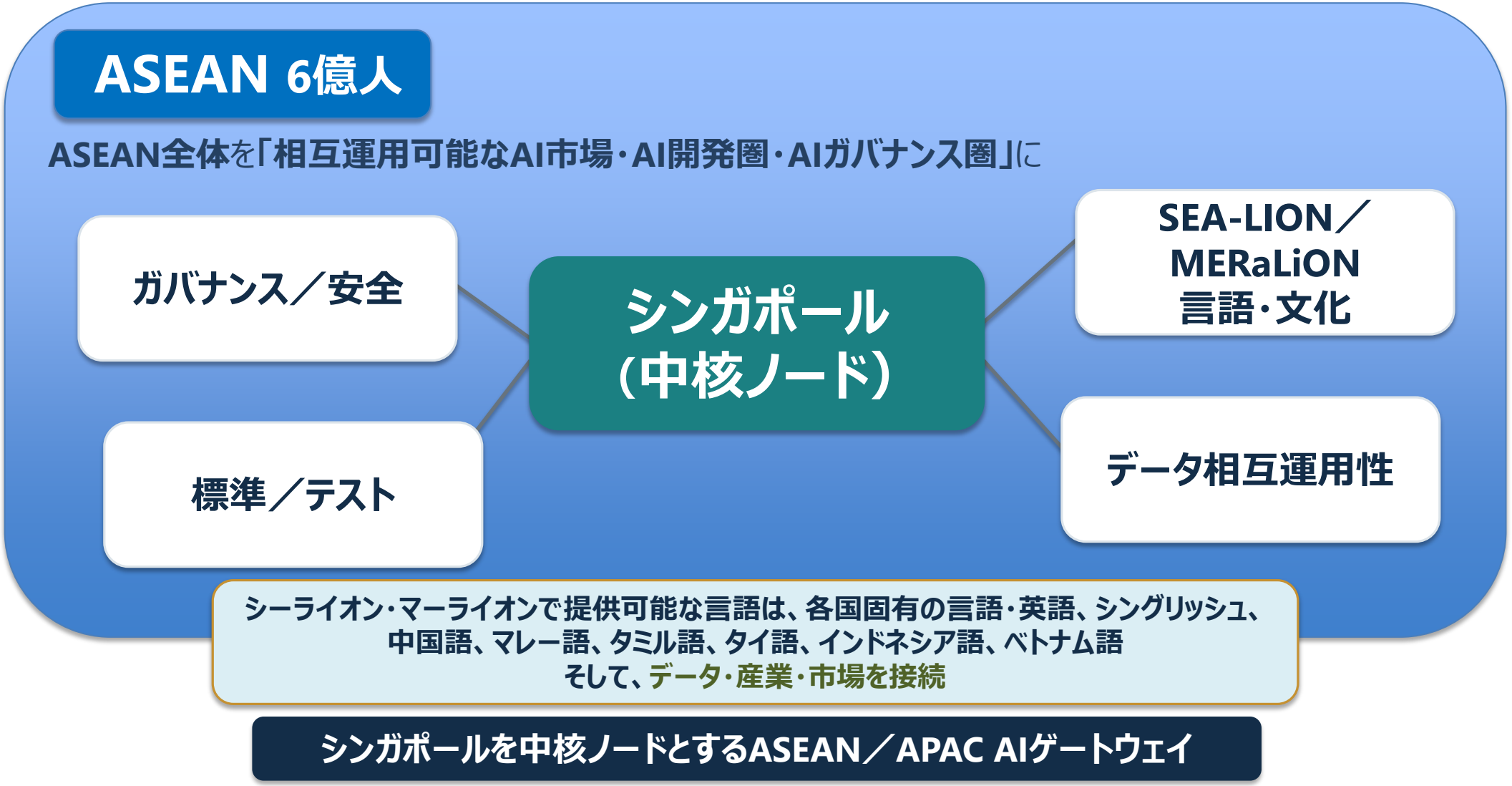
海事フィジカルAI／自動港

共通する実装思想

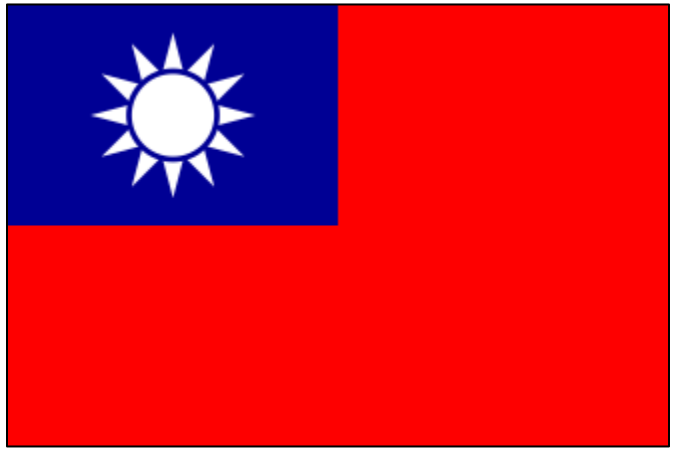
開発 → 実環境テスト→ 安全／ガバナンス → 実装 → 運用データ → 改良・スケール

©Atsumi & Sakai 2026

4. ASEANを「相互運用可能な地域AIエコシステム」へ



©Atsumi & Sakai 2026



台湾

AIエコシステム・AI政策・AIガバナンス

©Atsumi & Sakai 2026

台湾の訪問先

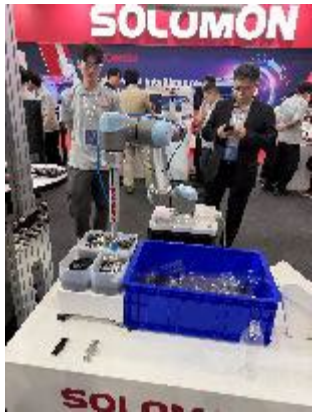
※画像はインタビューの場所であり、インタビュー対象者の所属先や対象機関とは限りません。



曾憲立氏
（台湾AI卓越センター及び国立台南大学）



- 国家科学及び技術委員会（NSTC）
- 中央研究院（Academia Sinica）の情報科学研究所（IIS）
- 財団法人国家実験研究院（NIAR）の科学技術政策研究・情報センター（STPI）



SOLOMON Technology Corporation



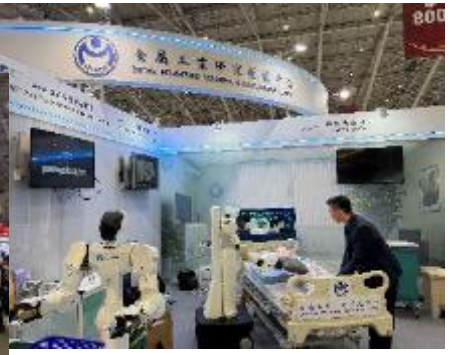
Taiwan AI Labs



デジタル発展部（MODA。日本の省に相当）

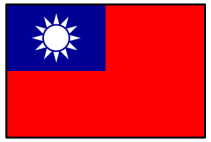






©Atsumi & Sakai 2026

① 強さ1：産業政策をAI実装基盤へ転換



「世界最強級の半導体・ICTサプライチェーン」を持っている国が、非常に早い段階から、産業AIを、自国の強さとして政策化した

2016年の5+2産業イノベーションと、2018年のAI行動計画は、セットで遂行するとされた。

2016年 5+2産業イノベーション

- スマート機械、アジア・シリコンバレー、グリーンエネルギー、バイオ医薬、国防／航空宇宙
- 新農業、循環経済（サーキュラーエコノミー）

OEM/ODM中心 → 高付加価値の製品・サービス・ソリューションへ

AIの産業化のベースであり、**蔡英文政権**が**台湾産業の高度化・デジタル化・国際競争力強化**のために**7つの重点産業群**を定め、**国家戦略として育成**する政策

2018年 AI行動計画

- **産業が課題を提示**
- **AI人材・研究者をマッチング**
- AIソリューション開発
- テストベッドを開く
- 規制緩和
- 産業実装

100以上のAIアプリケーション・ソリューションを志向

意味

- **台湾はAIを「研究テーマ」だけでなく、既存産業の高度化装置として早期に政策化。**
- 半導体・ICT・機械・医療等の強い産業基盤を、そのまま産業AIの需要側・実証側に転換

台湾が**極めて早い時期**に、**産業AIを、自国の強さとして政策化した**こと

©Atsumi & Sakai 2026

② 強さ2：「ハードウェアを捨てずにソフトウェアを取り込む」——海外企業との連携

台湾政府は当初から、外国企業との連携を単なる外国企業誘致ではなく、
台湾のハードウェア産業＋海外企業のAI → スマート製造／スマートヘルスケア等
→ 新しいAIエコシステムとして位置付けている。

台湾のハードウェア基盤

- TSMC／ファウンドリー
- 半導体サプライチェーン
- AIサーバー
- ODM／OEM
- エレクトロニクス
- 部品／中小企業

「世界最強級ハードウェア・製造エコシステム」を提供し、

世界企業のソフトウェア・プラットフォーム

- Microsoft、Google、NVIDIA などの外国AI企業
- それらが持つAIソフトウェア、AIモデル、クラウド、エージェント、デジタルツイン、産業用ソフトウェア

世界最高水準のAI・ソフトウェア企業を、台湾エコシステムの内部へ引き込む

接続後の産業価値

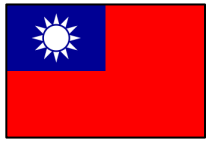
- スマート製造
- スマートヘルスケア
- 産業AI
- フィジカルAI
- ロボティクスAI

AIソフトウェアで米国企業と正面から全部競争せず、新しいAIエコシステム構築

台湾にとってのメリットは、**世界の企業にとってもメリット**であり、**大きなWin-winの関係**ができ上がる

©Atsumi & Sakai 2026

③ 強さ3：「AIを作る」だけでなく「物理世界へ落とせる」



これはフロンティアモデルそのものの性能競争とは違う、**実際の製造工場があるという強み。**
世界AI企業が参加する水平サプライチェーン型である。

【台湾と**マイクロソフト**の関係は親密】
- 2018年：AI戦略アライアンス
  - AIビッグデータ・技術・人材の3領域で協力
- 2020年：Microsoftがデータセンターへ大型投資

【台湾が**NVIDIA**と緊密になる理由】
- TSMCがNVIDIAの最先端GPUを製造
- AIサーバーの90%以上が台湾で組み立て可
- NVIDIAのサプライチェーンの中心が台湾（Quanta、Wistron、Foxconn）

【**NVIDIA**が台湾に求めるもの】
- 次世代GPUの製造能力
- AIスーパーコンピューティングセンターの共同構築
- AI医療・AI製造などの国家レベルの実証フィールド
- 台湾大学・AICoEとの研究連携（AIモデル最適化）



世界級ハードウェア × 世界級の海外AIソフトウェア × 台湾の高速実装力が台湾の強さ。
産業AI・フィジカルAI・ロボティクスAIを強くしようとしている段階にある。

台湾の世界級の物理サプライチェーン

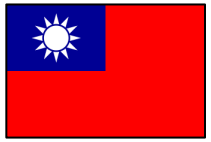
半導体製造／パッケージング
ICTハードウェア／電子機器製造
AIサーバー・サプライチェーン／ODM・OEM／部品

AI実装への転換

グローバルAIソフトウェア／プラットフォームを接続し、
産業AI・フィジカルAI・ロボティクスAIへ。
強みは「フロンティアモデル性能競争」と異なる

©Atsumi & Sakai 2026

台湾がロボティクスAIに強い理由——「部品→半導体→実証→量産」の近接も強み



- **2016年から主要産業に特化した政策**をとり、**AI行動計画**でも**産業AIを強化。**
- 単体ロボットではなく、**ハードウェア供給網**と**短い商業化サイクル**を**一体化できる**ことにも強み

① 世界級のハード基盤
モーター／センサー／カメラ
- 組込み基板・精密機械・部品
- ロボットの「身体」を国内供給網で支える

② 半導体エコシステム
- TSMCを核にAI・エッジAI向け半導体
- 先端プロセス／パッケージング
- ロボットの「心臓・知能層」と接続

③ 実証環境
- 工場・病院・物流・サービス
- AMR、医療・介護、検査・救災
- 研究成果を現場で素早く検証

④ 政策支援
- スマート機械／AIロボティクスを重点化
- 研究・実証・企業連携を支援
- 用途別に産業化を促進

⑤ 商業化
- 試作→実証→量産→海外展開

台南：近接した3拠点を役割分担

もともと研究～製造量産まで行える状況に合ったものを**結び付けて役割分担**し、**より全体のシナジーを強めようとしている**

沙崙 Shalun｜研究
- 国家レベルのAI・ロボティクス研究
- 先端技術・研究基盤を形成

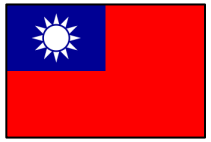
六甲 Liujia｜統合・実証
- 研究を実機へ変換、用途別実証
- 医療介護・物流倉庫・飲食サービス・巡検救災
- 海外スタートアップと台湾産業を接続

柳営 Liuying｜製造・量産
- 金属加工・機械・精密部品の産業基盤
- 南科の半導体・先端製造と接続
- 企業集積→量産→輸出

研究 → 実証 → 量産 → グローバルAIロボティクスサプライチェーンハブ

©Atsumi & Sakai 2026

台湾の医療・介護ロボティクスAI——「現場実装」と「自律化研究」を同時進行



- 病院・介護**現場を実証環境**にし、**画像AI・AMR・ロボット制御・ケアAIを産業化**

手術支援ロボティクス

- 輸入手術ロボットの活用・改良
- AI画像解析／術前計画
- 術中ナビゲーション
- 自律縫合・切開（研究段階）

病院物流・調剤

- AMRによる院内搬送
- 調剤自動化・薬剤管理
- 人手不足対策＋安全確認
- 病院の日常業務へ実装

介護・見守り

- 見守り／対話ロボット
- 自律移動＋生活支援
- 認知症ケアへのAI活用
- 高齢社会を実証市場に

次段階：高度自律化

- 感情・状態認識
- AIエージェントによる介護計画、自律判断＋ロボットアクション
- コグニティブケア・ロボティクス

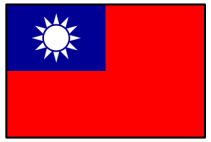
台湾型の競争力：医療ロボット単体ではなく「実装系」。シナジーを結び付けている

AI画像・モデル	→	半導体・エッジ	→	ロボット / AMR	→	病院・介護施設	→	量産サプライチェーン
画像診断／認識		低遅延・省電力		身体・移動・操作		実環境テスト		製品化・輸出

台湾の強み ＝ ハードウェア・サプライチェーン × 半導体 × 実環境テスト × 高速量産
→ 医療・介護を含む**フィジカルAIを「製品・システム」として海外展開できる基盤**

©Atsumi & Sakai 2026

台湾が医療AIに強くなった理由



- **「医療データ」だけでなく、社会需要・デジタル基盤・政策・現場・企業化が連鎖するエコシステム**
  - NHI医療データ → 臨床・介護ニーズ → AI開発・実証 → 医療現場への導入 → スタートアップ・産業化介護

① 世界最高水準の医療データ

- NHI：国民の99%以上が加入
- 診療・薬剤・検査データを20年以上蓄積
- 均質で欠損が少なく、研究利用制度も整備

医療AIの"源泉"

② 急速な高齢化

- 高齢者医療・介護ニーズが急増
- 転倒検知・歩行解析・認知症AIなどを実証
- 病院・介護施設が導入先になる

明確な社会課題

③ 医療機関のIT化

- 電子カルテの普及
- 病院間のデータ連携が進展
- AI導入障壁が低く医療スタッフのIT親和性も高い

実装できる基盤（ICTアーキテクチャができ上がっていた）

④ 政府の重点産業政策

- 5＋2産業イノベーション政策
- AI行動計画2.0／バイオ・医療を重点育成
- TAcc+・Garage+等でスタートアップを支援

政策・資金の後押し

⑤ 医療現場の協力

- 医療機関がAI研究・実証に理解
- 医師・研究者・企業の共同開発進みやすい
- 臨床現場でフィードバックを回せる

実証→改善の循環

⑥ 成功企業の連続創出

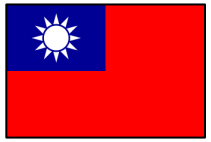
- 医療画像・診断支援・デジタルヘルス等で企業化
- 成功例が次の人材・資金・病院連携を呼ぶ
- 研究成果が市場へつながる

産業エコシステム化

結論：台湾の医療AIは全国規模の医療データ × 実証可能な医療現場 × 政策支援 × 半導体・ICT力が結合した「実装型AIクラスター」

©Atsumi & Sakai 2026

台湾の主要AI実証・評価拠点——フィジカルAI／ロボティクスAIを中心に



- **分野別テストベッド**を整備し、**仮想評価 → 実機 → 実環境 → 行政・産業実装へ**接続

分野	代表的な拠点・仕組み	主な実証内容	備考
自動運転	Taiwan CAR Lab／台湾智駕測試實驗室	自動運転、V2X、道路環境、交通シナリオ	台湾を代表する実環境テストベッド
ロボティクスAI	沙崙 Robot Testing & Training Base	ロボット、ヒューマノイド、フィジカルAI	今後の中核
ロボティクスAI	National Center for AI Robotics (NCAIR)	AIロボット、サービスロボット、アルゴリズム→実機	2026年新設の国家拠点
製造・ロボット	ITRI Robotics / スマート製造実証設備	ロボット、デジタルツイン、マシンビジョン、協働ロボット	製造実装に強い
自動運転	ITRI Autonomous Driving / ADAS validation	SIL/HIL、コーナーケース、センサーフュージョン、AI認識	仮想＋実環境
AIチップ	ITRI AI Chip System Validation Laboratory	AIチップ、NN、データセット、SDK/API、性能検証	半導体国らしい特徴
AI製品安全	MODA AI Product & System Evaluation Center	LLM/AI製品の安全性、公平性、セキュリティ	ガバナンス側のテストベッド
政府AI	TryAI	LLM、TAIDE、ChatGPT、Gemini、Claude等	行政実装テストベッド
ドローン	複数のUAV/5G実証フィールド	自律ドローン、物流、通信、安全	フィジカルAIに接続
地域実証	AI Garden	農業、介護、ドローン、検査等	地域産業でフィールド検証

実証実験場は台湾のAIにおける安全のキーである

注目点

台南・沙崙

フィジカルAI／ロボティクスAIの実証クラスター化が進展

特徴

- ロボット／ヒューマノイド
- 自動運転／ドローン
- スマート製造
- AIチップ検証
- AI安全性／ガバナンス
- 行政・地域でのフィールド検証

評価

台湾は半導体・ICTの強みに加え、**AIを「実機・実環境で検証する能力」**を国家レベルで厚くしている。

©Atsumi & Sakai 2026

台湾「AI新十大建設」（10大プラン）——10本を3本柱で束ねる国家AI転換

「ハードウェア供給国」から「AIフルスタック国家」へ

半導体・ICT
既存の世界級強み

算力・主権AI
クラウド/HPC・データ

AIソフトウェア
産業別AI・エージェント

フィジカルAI
ロボット・実世界制御

社会実装・輸出
百工百業＋海外市場

① スマート応用 SMART APPLICATIONS

1 **全ての国民のスマートな暮らし**
交通・医療・建築・電力網・防災

2 **全産業におけるスマート応用**
中小企業まで産業AIを普及

3 **AIデジタル産業の頂点へ**
「Team Taiwan」＋輸出可能なAIサービス

② 重要技術 KEY TECHNOLOGIES

4 **シリコンフォトニクスにおける世界的リーダーシップ**
CPO・高速/低消費電力伝送

5 **世界をリードする量子技術サプライチェーン**
研究から応用・産業化へ

6 **AIロボティクスサプライチェーンの世界的拠点**
認知・感知・制御＋実装

③ デジタル基盤 DIGITAL FOUNDATIONS

7 **主権AIと計算資源インフラ**
HPC/クラウド・台湾語料・サイバーレジリエンス

8 **スマート政府とデータガバナンス**

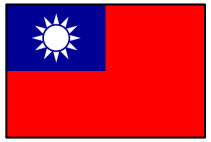
9 **AI人材エコシステムが世界をリード**
初等教育～産業・海外人材

10 **1,000億台湾ドル級の資金動員**
政府資金で民間投資を誘発

©Atsumi & Sakai 2026

AIガバナンス：共通リスクタクソノミを、各省庁の分野別規制へ変換する

台湾は、AI政策の当初からAIガバナンスを同時進行させてきたのではない。**AI政策を進める中で、リスクを明確に認識**し、**高速でAI基本法とAIガバナンスを整えて追いつきつつある**。



AI基本法 → 共通リスクタクソノミ → 各省庁がユースケース別に評価 → 法的拘束力ある分野別規範へ

リスクタクソノミ：組織が直面する様々なリスクを、種類・性質ごとに整理し、体系的に分類した「共通言語」。リスクは20種類に分類。

- **企業・国家間の競争激化**によって開発速度を優先し、**安全試験が不十分**なAIを導入するリスクまで含まれている。
- AI能力・資本・計算資源が少数の主体へ集中することや、雇用・不平等、人間の創作価値保全、環境負荷を含む**社会構造上のリスクも**対象となっている。
- さらに、**AIエージェントが権限を越えて外部システムへアクセスするリスク**や、**複数エージェントの連鎖反応まで**明記している。

ユースケース棚卸し → **リスク特定** → **リスク評価** → **リスク対応**

専門組織が、共通タクソノミを作り評価方法を揃えた。
最終的なガバナンスの権限・責任は各分野の所管官庁に残す。

各所管官庁が、法的拘束力があり直接執行可能な分野別規則を整備（ガイドラインやツールも）

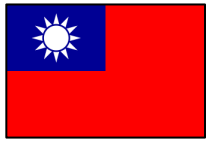
台湾型の特徴

共通性	省庁横断でリスクの言葉・評価尺度を統一
具体性	まず所管産業のAIユースケースを棚卸しする
責任	各所管官庁が最終責任を負う
法規制	必要な領域では既存法の改正・新ルールの整備を行う
産業振興	サンドボックス・評価／検証・データ開放も同時推進

＝「共通リスクアーキテクチャ＋分野別法規制」のハイブリッド型

©Atsumi & Sakai 2026

台湾のAI戦略におけるIOWN（アイオン――オール光ネットワーク）の意味



AIシステムが高度化しても、データを送る通信回線が溢れていれば機能しない。**十分な通信容量を確保**するための政策である。**台湾の主権AI・産業AIを地域横断／日台横断で動かす基盤候補。**

台湾の課題
AI計算資源・データを
低遅延／大容量／
省電力で接続

→

IOWN / APN
AIデータセンター・
都市・産業拠点を
光で直結

→

AI実装
スマート交通・医療
遠隔制御・画像解析

→

産業化・輸出
日台共同で技術・製品化
→ 国際市場へ

なぜ台湾に必要か

主権AI基盤	NCHCの計算資源や、台湾各地のAIデータセンター、将来の日本側AIデータセンターを高速接続
南部AIクラスター	台南・沙崙を核に、南科・台中・新竹を結ぶ国家レベルAI基盤へ
フィジカルAI・産業AI	遠隔自動運転、道路安全、AI画像解析など「リアルタイム性」が必要なAIを支える
医療AI	大容量医療画像の地域間伝送を高速化し、遠隔診断・医療資源共有を支える

日台協力の戦略的意味

台湾
半導体・シリコンフォトニクス
光電融合（CPO）・
通信機器・AI基盤

⇔

日本
NTT IOWN/APN
CPO・
ネットワーク技術

共同実装 → 技術・製品の自主能力 → 国際市場

単なる通信高速化ではなく、台湾の「主権AI」とスマートシティを支える
次世代デジタル基盤としてIOWNを位置付ける動き

©Atsumi & Sakai 2026



韓国

AIエコシステム・AI政策・AIガバナンス

©Atsumi & Sakai 2026

韓国の訪問先







Robot Plus Test Field及び
韓国電子技術研究院（KETI）



韓国知能情報社会振興院
（NIA）

©Atsumi & Sakai 2026

韓国AIの強さ

制度アーキテクチャ × フィジカルアセット × M.AX × 量産・輸出力 × ガバナンスの総合力

① 制度を実装へつなぐ継承力

約30年にわたり、基本法→国家計画→省庁実施→行政実装という型を更新・継承。

この継承には、AI基本法や現在のAIガバナンスにつながる基本的な考え方が含まれている。規制と施行令、ガイドラインがあり、弱者を置き去りにしない。

② 物理世界を持つ

半導体・自動車・電池・造船・鉄鋼・家電・物流・ロボットという大量のフィジカルアセット。

多くの先進国は、物理世界を中国、東南アジア等に逃がしてきた。韓国は、物理世界を維持し続けてきた。

③ AIで再統合する

M.AXでデータ・モデル・ロボット・工場・製品を統合し、Physical-world Industrial AI OSへ。

1995
情報化促進基本法
情報化・ICT産業基盤・国民生活

2009
国家情報化基本法
国家情報化を横断的に体系化

2020
知能情報化基本法
デジタル→知能情報社会へ拡張

2024/26
AI基本法
AI振興＋安全・信頼＋国家ガバナンス



継承されたもの

情報化・産業競争力・国民生活・情報格差・安全／信頼という**基本理念**を、技術変化に合わせて**「デジタル → 知能情報 → AI」へ拡張**。AI基本法自体は2024年成立・2026年施行であり、「AI基本法が20年前から存在した」という意味ではない。

©Atsumi & Sakai 2026

韓国のフィジカルアセットは、なぜこれほど強くなったのか

結論：政府主導の輸出工業化 × 財閥の大規模投資・垂直統合 × 産業クラスター × 世界市場への継続的な設備投資

1960–70s 輸出工業化 → 1970s 重化学工業化 → 1980–2000s 半導体・自動車・造船・電子
→ 2010s– 電池・HBM・スマートファクトリー → フィジカルAI
韓国の強さ＝「工場を持っている」ことではなく、
フィジカルアセットを更新し続ける投資（財閥）・工程・サプライチェーン能力を国内に蓄積したこと

① 国家の産業政策

- 輸出市場を前提に、鉄鋼・造船・機械・自動車・化学などへ資本を集中
- インフラ・金融・技術導入、人材育成を産業政策と連動
- その後も半導体、ディスプレイ、電池など戦略産業を継続的に高度化

→ **国内需要だけでなく最初から世界規模の工場を持つ構造**

② 財閥系企業の役割

- Samsung・Hyundai・LG・SK・POSCO等が巨額設備投資を長期継続
- 部品→素材→製造→物流→販売まで系列・サプライチェーンを形成
- 不況期にも次世代設備へ先行投資できる資本力
- 工場・船・車・Fabから大量の操業データが蓄積

→ **財閥は重要。ただし「財閥だけ」で説明するのは不十分**

③ 集積の自己強化

- アンカー企業の周囲に、部品・装置・素材・エンジニアリング企業が集積
- 熟練人材、大学・研究所、産業団地が近接
- 工程改善→品質→輸出→再投資の循環

→ **フィジカルアセットと現場ノウハウが同時に厚くなる**

④ 米欧との関係

- 米欧が金融・ソフトウェア・プラットフォームへ傾斜したことは一部で追い風
- ただし「米欧が製造を捨てたから韓国が勝った」は過大
- 韓国自身の輸出志向、設備投資、学習、工程力が主因

→ **世界の分業変化を韓国が能動的に取り込んだ**

©Atsumi & Sakai 2026

M.AX：フィジカルAIフルスタックを「統合」する国家プロジェクト

2025年9月発足のM.AX Allianceは、2026年に約1,500社・機関、11分科へ拡大した。
韓国の世界級製造企業をプラットフォームの中核に据え、必要な（米国中心の）AI企業の能力を接続しようとしている。
その連携は、シンガポールと異なり、国家と外資企業ではなく企業同士の連携である。韓国のスタートアップと外資企業との連携も多い。
連携先米国企業は、NVIDIA、マイクロソフト、AWS、IBM、インテル、オラクル、OpenAIなど17社である。

フィジカルAIフルスタック

データ
製造データ生成・共有・活用
Manufacturing-X標準モデル

↓

AIモデル
AIファクトリー／次世代自動車
AIロボット基盤モデル

↓

Embodied製品
AIロボット／自律運航船
AI家電／AI半導体

↓

実装
AIファクトリー・ダークファクトリー
産業団地AX

↓

スケール／輸出
2030年 AIファクトリー500拠点目標
海外展開・輸出産業化

「研究成果 → 大量生産 → 世界市場」

R&D → プロトタイプ → 工場 → 大量生産 → グローバルサプライチェーン → 輸出

米国との違い

フロンティアAI・基礎研究では米国が圧倒的に強い。一方、韓国はAIを大量生産可能な工業製品へ落とす現場を持つ。

台湾との違い

半導体サプライチェーンでは台湾が突出。韓国は半導体に加え、自動車・船・電池・家電など物理領域が広い

日本との違い

ロボット部品・工作機械・精密技術では日本が強い。韓国は巨大企業群を軸に統合・量産・海外展開を速くつなげやすい。

©Atsumi & Sakai 2026

韓国フィジカルAI　実証実験場マップ（2026）

実証実験場は韓国のAIにおける安全のキーである

① 半導体｜首都圏（平沢・華城・器興）

Samsung Foundry / Memory の巨大製造基盤
HBM・AI半導体 → フィジカルAIの計算基盤
「AIを動かす半導体」と「AIで動くFab」が接続

② R&D・標準｜大田・KAIST / ETRI

世界モデル／ロボット基盤モデル／ヒューマノイド AI
OS → センサー → コントローラー → ロボット → 工場を実証
フィジカルAIの安全・信頼性・国際標準化も推進

③ AIファクトリー｜全羅北道

地域AXの先行拠点：AIファクトリー
製造データ・エージェント・ロボット・設備制御を統合
工場単位から地域産業クラスターへ拡張



④ 精密製造 / スマートファクトリー｜慶南・昌原

フィジカルAI事前実証 → 2026–30 慶南AX
PINN / LAMによる精密制御、設備最適化
中小・中堅工場を実際の検証環境として活用

⑤ 自動車｜蔚山

Hyundaiの大規模生産拠点＋次世代EV工場
AI・ロボティクス・スマート物流・自動組立
モビリティ × ロボット × 工場データの実装場

⑥ 造船｜蔚山・東南圏

世界級造船所をフィジカルAI実証資産として活用
溶接・搬送・検査・自律設備・デジタルツイン
政府が自動車・精密製造と並ぶ先行3産業に指定

©Atsumi & Sakai 2026

韓国のフィジカルAI・ロボティクスAI・医療AI——代表的な実証インフラ

研究室内のPoCではなく、「実環境 → 性能検証 → 認証・標準化 → 商用化」へつなぐ分散型テストベッド網

① KETI Robot Plus Test Field｜ソウル・水西

製造・協働ロボット／ヒューマノイド／アクチュエータ

- 5,950㎡・2棟、ロボット等80台超
- 加工・検査・搬送など製造工程で実証
- 2025–26：HL Mando等とヒューマノイド／AIロボット実証
- 性能検証 → 試験・認証 → 標準化・事業化

製造フィジカルAIの「実装入口」

② National Robot Test Field｜大邱

国家レベルの大規模ロボット実証基盤

- 多種・多数ロボットの実環境評価
- データに基づくロボット活用エコシステム
- サービスロボット共通プラットフォーム・安全認証
- 商用化を支える試験・標準・適合性評価

ロボット産業全体の共通試験／認証基盤

韓国型AI実証アーキテクチャ

フィジカルアセット＋ 実環境データ ＋ 試験／認証＋ 標準化＋ 実装

③ 光州 全市域自動運転テストベッド

モビリティ／自律AI

- 光州市全域 約500km²を実証空間化
- Hyundai・Autonomous a2z・RideFluxを選定
- AI自動運転の実道路データ・性能検証
- 技術開発 → サービス商用化を一体化

都市そのものをフィジカルAIテストベッドへ

④ 医療AIテストベッド｜病院ネットワーク

診断・予測・治療支援AIの臨床実証

- 医療データ中心病院 45施設が対象母体
- 2026年：20件の医療AI実証課題を新設
- リアルワールドエビデンス / 臨床的有効性を検証
- EMR・PACS連携など実運用まで確認

「AIを病院で実際に使えるか」を検証

共通する政策ロジック

R&D → 実環境実証 → 失敗／データ→ 安全・認証 → 標準化→ 商用導入・全国展開

⇒フィジカルAIを「製品」ではなく**産業システムとして実装**する能力

©Atsumi & Sakai 2026

AIガバナンス：AI基本法を法的な背骨として、国家計画・義務・検証・ガイドラインを接続



法律 → 施行令 → 具体的なガイドライン → 企業実装——「制度体系化型」のガバナンス

AI基本法の法的バックボーン

透明性	高影響AI／生成AI利用の事前告知、生成AI生成物の表示
安全性	一定規模以上のAIのライフサイクル全体のリスク識別・評価・緩和、事故モニタリング
高影響AI	リスク管理・説明・利用者保護・人間による監督・記録保存
AI弱者への配慮	**低所得者・障害者・高齢者など**情報利用上不利な立場にある人に情報利用機会と環境を提供
中小企業・農業等	**AI化が届きにくい、中小企業や家族経営、農業・漁業など**へも、**AI化の支援を及ぼす**
検証・認証	国が自主的検証・認証を支援。高影響AIは事前取得に努める

シンガポールとの違い：ガバナンスを先に実証・共創して育てるより、法律で国家体系を先に固定し、施行令・ガイドラインで行政実装へ落とす色が強い。

ガイドラインは詳細で具体的な内容

実装アーキテクチャ

AI基本法 → 産業振興・国家としての規制

↓

施行令 → 法律を運用可能な要件へ落とす
（例）高影響AIのリスク説明方法など

↓

ガイドライン → 事業者の透明性等の義務を具体化
（企業が判断・準備できる具体性を保ちつつ、中小企業・AI弱者を制度上考慮）

↓

分野／企業 → 既存業法＋AI追加措置で実装

＝ 産業振興と規制を同じ基本法体系に置く

©Atsumi & Sakai 2026

産業別マルチモーダル基盤モデルから世界モデルへ

「言語・画像を理解するAI」から「物理世界を予測し、ロボット・設備を動かすAI」へ

① 産業別マルチモーダル基盤モデル

製造・流通・ロボット・コンテンツ・公共向けに、国産LLM＋マルチモーダル知覚・生成をDomainOpsで展開

② ロボット基盤モデル

大規模マルチモーダルデータから知覚 → 理解 → 計画 → 行動を統合

③ 主権世界モデル

運動＋物理法則を学習し、未来状態を予測。合成データとシミュレーションを大量生成。

2026年に政府が明示したフィジカルAI開発パイプライン

世界モデル学習
物理的一貫性
長期予測

→

ロボット基盤モデル統合
シミュレーション
→実機への転移

→

実証・評価
製造・物流の
実環境

→

事例分析・再学習
失敗を学習し
反復改善

政府目標：世界モデルを適用したロボットの実作業成功率を、非適用時より20%以上改善。
LG Electronics主導でKT・KAIST・SNU・Robotis等10機関が参加、2年間で340億ウォン投資

ポイント：韓国は「産業別基盤モデル」だけでなく、フィジカルAIの中核である世界モデルを“主権技術”として内製しようとしている。

「Physical-world Industrial AI OS」へ

©Atsumi & Sakai 2026

K-Moonshot｜AI × 科学技術を「国家ミッション」にする

2026年始動 → 2030年「研究生産性2倍」→ 2035年「8分野・12国家ミッション」解決

K-Moonshot の本質

AIを研究ツールで終わらせず、国家の科学技術R&Dの「共通基盤」にする

研究データ	23研究機関等のAI-ready化
計算	スパコン＋政府GPU
AIモデル / エージェント	科学特化モデル・AI Scientist
自律実験	バイオ・素材等のロボティックラボ
PD型R&D	12ミッションを責任者が統合運営

時間軸

2026　戦略・12ミッション確定／推進団発足

3月：12ミッション確定　5月：PD 12名・K-Moonshot推進団

2030　研究生産性 2倍

Science × AIで研究の探索・実験・検証サイクルを加速

2035 12国家ミッションを解決

国家競争力の「大跳躍」を狙う最終目標

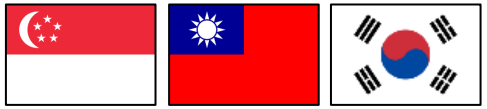
参考：
2026年 国家AI予算 10.1兆ウォン
MSIT「AI Transformation」5.1兆ウォン
MSIT「NEXT戦略技術」5.9兆ウォン

8分野・12国家ミッション

- **先端バイオ**：新薬10倍加速｜脳インプラント
- **未来エネルギー**：多接合太陽電池｜核融合｜SMR船舶
- **フィジカルAI**：ヒューマノイド｜汎用フィジカルAIモデル/計算
- **宇宙・素材**：宇宙データセンター｜希土類
- **AI Scientist**：世界最高水準のAI科学者
- **半導体・量子**：超高性能/低電力AIアクセラレータ｜誤り訂正量子

©Atsumi & Sakai 2026

3つの国・地域の、AIエコシステム・AI政策・AIガバナンスの総括



3か国の**強み**

① ICT政策・AI政策の早い着手と確実な継続

② 自国の強みと弱みの的確な認識。強みの生かし方、弱み（AIソフト）の補い方が賢かった。
とりわけ、米国フロンティアAI企業との連携戦略が際立っていた。

③ 3つの国・地域は、自国の強みである産業の資産・強さを打ち出す産業AI戦略を採っている。
狙いは産業AI OSにあると考えられる。

④ イノベーションとガバナンスを**対立概念にせず**、ガバナンスをAI産業の必須の競争力にした。

3か国の**特徴**

① 3か国とも、**生成AI・マルチモーダルAI**を用意しつつある。
それぞれの主権AIを担保できるように、それぞれの工夫が織り込まれている。
② 3か国は、**弱者や中小企業など**、ICT化、AI化に遅れそうな対象を法律や仕組みを持って
救おうと継続してきた。
③ 3か国は、それぞれに違いはあるけれど、ICT・AIにおける**データ対応**を重視し、
その利用と、保護すべきものの両立を図ろうとしている。ただし、完璧には進んでいないかもしれない。

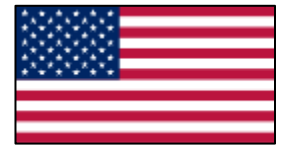
©Atsumi & Sakai 2026



米国

©Atsumi & Sakai 2026

「America」を単一のAI政策主体として扱うことの危うさ



米国のAI政策は、一枚岩の国家戦略ではなく、複数の権力・市場・規制体系が並立する**「連邦型ネットワーク」**

“America” ≠ 単一主体

ホワイトハウス / 連邦政権



AIアクションプラン、国家安全保障、輸出、計算・エネルギー、連邦調達

連邦議会

連邦AI法、予算、監督。超党派領域もあるが、党派・委員会で方向が分かれる



- 米国のAI企業は、トランプ政権のAIフルスタック輸出計画に全く従っていない。各企業は、独自の海外戦略に基づき、既にEU、英国、カナダ、アジア3か国と独自の連携を進めている。

連邦政府機関 / 規制当局

NIST・CAISSI、DOE、DoD、FDA、FAA、NRC、FTC等。目的・法的権限が異なる



民間セクター / 標準 / 裁判所

フロンティアAI企業、クラウド、半導体、産業企業、標準化団体、司法が政策実装を左右。
企業戦略は政権方針と必ずしも一致しない。

州

カリフォルニア、テキサス、コロラド等。
連邦より先にプライバシー・安全性・アカウンタビリティなどを規律

**『米国はAIをどう考えているか』ではなく、
誰が・どの法的権限で・どの産業／リスクを扱っているかを分解して見る必要性**

©Atsumi & Sakai 2026

連邦政府機関の組織関係図

・・・筆者が聴き取り調査をした機関
合計13機関



EOP（大統領府）

OSTP（科学技術政策局）
- 大統領への**「助言」**と、政府機関の**「調整」**が主な役目
- AIアクションプランをドラフト。プランのビジョンを共有、政府機関を調整

OMB（行政管理予算局）
- 政府機関のAI利用や調達などに関する**「政策」**である**メモランダム**を策定
  → **政府機関を拘束**
- 予算措置を講じる

他のオフィスや会議体も存在

予算上の監督 → **NSF（国立科学財団）**

OSTPによる調整、OMBのメモランダムによる拘束

15 Executive Departments（15の省）：各省は、EOPや他省と調整・役割分担

DOC（商務省）
- **OPSP（政策戦略企画室）**
- **Bureaus（局）**
  - **NTIA（国家電気通信情報局）**
  - **NIST（国家標準技術研究所）**
    - **CAISSI（SI標準・イノベーションセンター）**
  - **BIS（産業安全保障局）**
  - **ITA（国際貿易局）**
  - **その他の局**

DOE（エネルギー省）
- **OSTR（戦略技術ロードマップ局）**
- **OECT（重要・新興技術局）**
- **CESER（サイバーセキュリティ・エネルギー安全保障・緊急対応局）**

DOS（国務省）
- **CDP（サイバー空間・デジタル政策局）**
- **ACN（軍備管理・不拡散局）**
- **DDTC（防衛取引管理局）**

その他の省

DHS（国土安全保障省）
- **AI Corps（AI部隊）**

DOW（戦争省）
- **DARPA（国防高等研究計画局）**

（図の出典）本件の調査内容から筆者作成。組織の描写は網羅的なものではなく、また、わかりやすくするために正確性や学術的な厳密さを犠牲にしている点がありますので、ご了承ください。

©Atsumi & Sakai 2026

米国AIアクションプランとは（2025年7月公表）

AI競争で米国が勝利するためのロードマップ
- **中核はAIにおける米国のリーダーシップ**
- **3本柱は、【イノベーション】【インフラ構築】【国際外交と安全保障】**
- 3本柱に**共通**する**3つの原則**で構成

AIにおける米国のリーダーシップ

3本柱

柱1. イノベーション

柱2. インフラ構築

柱3. 国際外交と安全保障

3つの原則

これらの原則の具体策は、3つの柱に散りばめ

原則1. 恩恵はアメリカ人労働者が受ける
アメリカ人労働者がAI政策の核心

原則2. 客観的真実追及（透明性）
イデオロギー的偏見から自由

原則3. 悪意ある者の悪用防止等
悪意ある者の悪用や盗用など、
新興リスクや予期せぬリスクを防ぐ

政権のAIアクションプランは、**既存の規制負担を抑えInnovationを加速する姿勢**を示している。
しかし同時期に**連邦政府機関であるCAISSIはフロンティアモデルのセキュリティ措置を強化**し、
国家安全保障当局側は信頼性（Reliability）、頑健性（robustness）、操縦性（steerability）、
制御可能性（Controllability）の研究を要求している。

©Atsumi & Sakai 2026

AIを「フルスタック国家輸出」する

総取りという覇権主義 ➡ 他国はAI主権を主張 ➡ 米国AI企業の各国協調に合わせ変更



- 米国 AIアクションプラン（2025年7月） ＋ 大統領令14320号：米政府自身が“技術的支配”と明記
- フルAI技術スタックを同盟国・パートナーへ輸出する、米国のAIを世界のGold Standardにする
- 対象国・地域を指定して、政府金融・外交まで動員して売り込む仕組み
- ホワイトハウスが、American (AI技術＋ 標準＋ ガバナンスモデル）を世界で採用させると
- 2026年2月、米国政府自身が軌道修正

「下記の全てをセットで買え」

① Compute	Chip / Accelerator Server / Data Center
② Cloud & Data	Cloud / Network Data pipeline
③ Model	Frontier / GPAI AI systems
④ Application	Healthcare / Education Agriculture / Transport
⑤ Security	Cybersecurity Model security
⑥ Rules	Standards Governance models

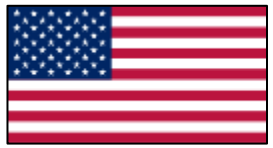
変更

国家が付ける「輸出加速装置」

米国は、各国が
AI主権を持つことを認め、
インフラ主権＋データ主権＋モデル主権＋政策主権
を各国がその管理下に置くことを支持すると表明

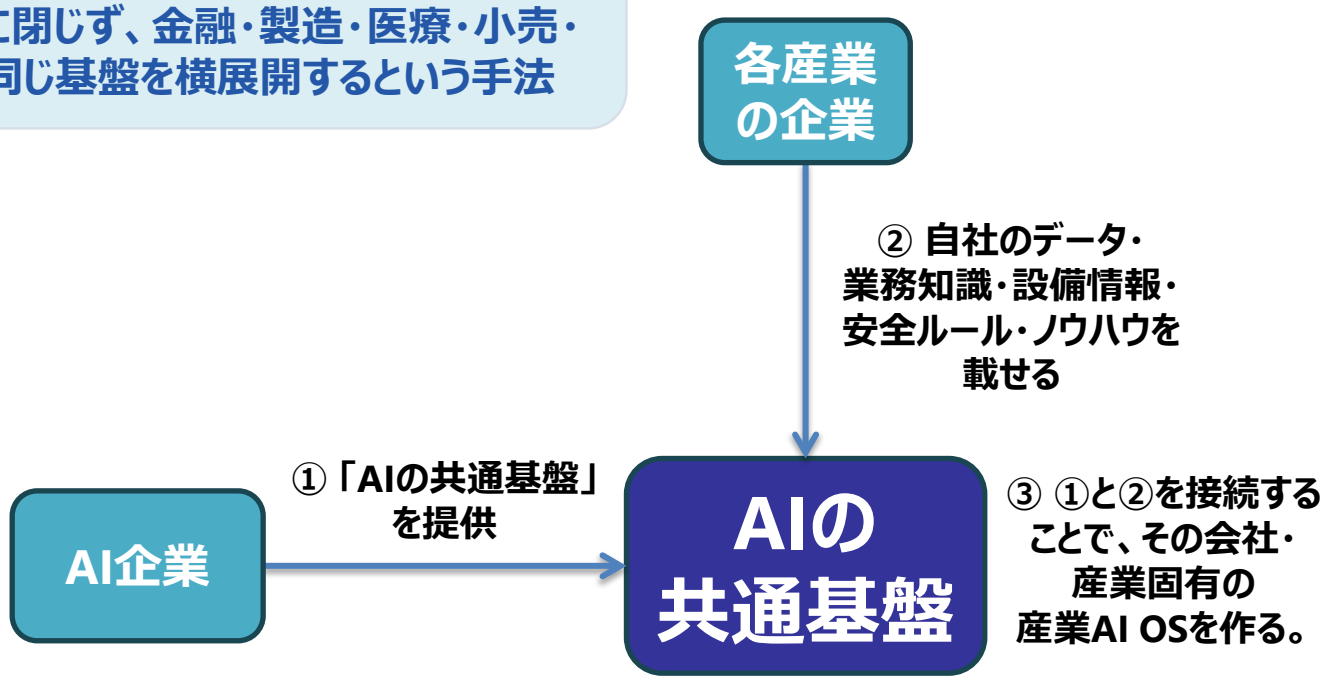
©Atsumi & Sakai 2026

米国の産業AI企業は「企業全体を覆う水平型AI OS」へ



- **米国の産業AI企業は、それぞれ自社内で、水平型の産業AI OSを作る戦略を採っている。**
  - 各社の2026年の公表からは、**業界横断の全社基盤へ向かう方向**が読み取れる

水平型の産業AI OS（分析概念）
1つの業界に閉じず、金融・製造・医療・小売・公共等へ同じ基盤を横展開するという手法

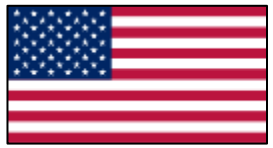


2026年の代表的なAI企業

OpenAI	Frontier	2/5
Anthropic	Claude	2/21 など
Google	Gemini Enterprise Agent Platform	4/22
Microsoft	Agent 365	5/1
AWS	Bedrock AgentCore	3/3
NVIDIA	Enterprise AI Factory	5–6月

©Atsumi & Sakai 2026

「産業AI OS」：安全性・ガバナンスの織り込みと開発スピード高速化



- **重要業務ほど、安全性とガバナンスが「商品機能」になる**
- **それでいて、市場投入競争は高速化**

① Pilot	② Connect	③ Govern	④ Production	⑤ Scale
PoC / もともとのエージェント	企業データ・ツールへ接続	**同時並行** 権限・政策・評価・監査	本番業務へエージェント投入	**継続** 全社・複数産業へ横展開

各社が組み込む「安全・統制の機能群」

ID	エージェントごとの身元・認証・誰のエージェントか
権限	最小権限、ツール・データへのアクセス制御
実行時ルール	ツール呼び出し前の許可・拒否、業務ルール
安全・セキュリティ	不正指示の注入・情報漏えい・隔離実行・認証情報
評価・監視	品質・挙動・費用・性能の劣化・模擬攻撃
監査・人の関与	ログ・処理履歴・承認・巻き戻し・障害対応

統制を「審査待ちの工程」から「実行時制御・再利用可能なルール」へ変え、導入速度と統制を両立

市場投入スピード：何が変わったか

2025 支援AI・チャットボット・個別試行

↓

2026 **エージェント基盤／本番運用・統制基盤／全社のAI運用層**

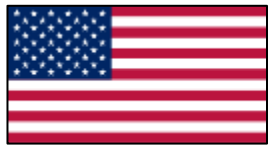
「新機能を数日～数週で出す」モデル企業の速度に、企業導入側も追随。
OpenAIは2026年2月時点で「約3日ごとに何かを出荷」と説明。

勝敗：モデル性能 × 業務のレベル × ガバナンス × 速度

米国勢は「業界別OSを個別に作る」より、1社の水平型AI OSを各業界へ適合させる。
安全・ガバナンスは、その横展開を可能にする「共通制御層」になりつつある

©Atsumi & Sakai 2026

連邦のAIガバナンス　ルール視点で見た米国



米国には「抑制的な」強みがある：厳然とした法規制、NIST、CAISI等、標準化機関、議会、州政府、裁判所、大学、研究者、保険会社、労働安全制度、製造物責任、企業内部のSafety Engineeringなど、複数の重層的なブレーキあるいはガバナンスが存在する

類型①
生命・安全保障・
経済安全保障・
インフラ保護・輸出管理等
↓
厳しい規制で対応
（法規制・Regulation等）

類型②
リスク産業のAI
（医療・創薬・化学・エネルギー・金融等）
↓
AI産業も**厳しい業法**に委ねられる
（法規制・Regulation等）

類型③
AI標準を広範・詳細に作る
（NISTのAI RMFその他）
↓
AI開発者の
リスク回避の道標とする

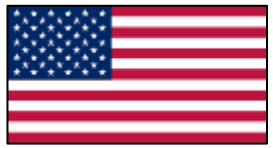
類型④
AIの急速な進化に遅れないための
AI企業向けの迅速対応
（CAISIと企業との連携、フロンティアAIモデルのテスト、国家安全保障関係脆弱性やCBRNEリスクの検討、ベストプラクティス文書やガイドラインなどの公表）

類型⑤　AI産業を促進するために行政を縛る統制

- **類型①②**については、**AI法**ができなくても、**リスク産業を対象とする厳しい現行法**が適用される。
- **類型③**と**④**は、**民間のAI企業群**と**合意を形成**しながら**辛抱強い活動**を行って作り上げている。そのベースは、AIが引き起こす、あるいはAI利用時に利用者が引き起こす（善意・悪意両方）リスクの洗い出し・評価・マネージのフレームワーク。
- だからこそ、**AI企業側も**、国が提示する標準に**抵抗感がなく**、**逆に安心感**を持って受け入れる。
- **類型⑤**は、AI産業を促進するために、アメリカの**民間部門**が官僚的な規制に縛られてはいけないとして、**行政機関を逆に縛る**方向性による**規制緩和**

©Atsumi & Sakai 2026

連邦政府機関のAIガバナンス　類型①・②



類型①　規制

生命・安全保障・経済安全保障・インフラ保護・輸出管理等に関しては、
AI産業であれ他の産業であれ**厳しい規制で対応**

セキュリティ関連のリスク
国土安全保障省（DHS）

セキュリティ全般を担当
税関、国境管理・沿岸警備、重要インフラ保護、救助、サイバーセキュリティ、テロ対策、災害対応、AIやデータ、金融関係

外部連携
- **AI産業の企業パートナー**（AnthropicやGoogleなど）
- **アカデミア**（HarvardやStanfordなど）

輸出管理上のリスク
国務省（DOS）と産業安全保障局（BIS）

武器輸出管理法（AECA）や**輸出管理改革法**（ECRA）等
- 5つの官庁による輸出管理
- **軍事用途**の場合**主にDOS**
- **デュアルユース**の場合**主にBIS**

AIなどの輸出に想定される**法的・行政的な抜け穴**と**執行上の抜け穴**の改善に、**DOSとBISは全力で取り組んでいる**
- AIは無形の計算結果や基盤データを含む→抜け穴が生じがち

類型②　業法

リスク産業（医療・創薬・化学・エネルギー・金融等）は**業法**の規制
- **ペナルティの重さは日本の比ではない**
- **それぞれの産業の特徴に応じて規制や指導**

医療分野

FDA（食品医薬品局）
- **連邦食品・医薬品・化粧品法（FD&C Act）**に基づき、**AIベース医療機器**の①**事前決定型変更管理計画**ガイダンスや②**市販前申請内容**ガイダンス案を発出　など

金融分野

SEC（証券取引委員会）
- **証券法制**に基づく**投資会社や証券会社の金融検査**において、**AI関連の検査**を行うことなどを明示

交通分野

DOT（運輸省）のNHTSA（道路交通安全局）
- **国家交通・自動車安全法に基づくFMVSS**（連邦自動車安全基準）を**自動運転システム（ADS）搭載車両に適用**、**安全基準の論点整理**

©Atsumi & Sakai 2026

連邦政府機関のAIガバナンス　類型③・④

類型③　NIST

商務省に属する連邦政府機関。省庁横断的に活動

Cybersecurity Framework（CSF）を作成
- 政府機関や企業向けのセキュリティガイドラインを公表。

AI Risk Management Framework（AI RMF）を策定
- 策定時には**主要AI企業**が**共同で詳細にリスク抽出・評価を行う**
- AI安全性評価やAI標準化の中心的役割を担う

- **AI RMF 1.0（約50頁）**を読む
- **Playbook**で**具体的な実装方法**を確認する
  - **多数の実装アクション**を収録
- **生成AI：GenAI Profile（約70頁）を併読**
- さらに細かな解説書も

日本のソフトローと何が違うのか？

- **連邦政府機関での調達時**に、**RMFを受け入れなければ不利**
- **規制の空白（拠り所となる既存法がない）**の場合に、**AI開発者のリスク回避の道標**に
- 標準に従ったと訴訟で示せば、**有利**に働く

類型④　CAISSI

AIの急速な進化に遅れないための施策
- NISTよりも「**クイックヒット**」を狙う。
- **活動のスピードが速い。公表も多いときは週に数本**

CAISSIの活動（例）
- AIモデルの**導入前にテスト**を実施。**国家安全保障リスクなど**を検討。結果は**企業にフィードバック**され、AI企業に、フロンティアAIの**リスク対策の拠り所**を与える。
- **国家安全保障に関わる脆弱性**や**CBRNEリスク等**の検討、ベストプラクティス文書やガイドラインなども公表

受け入れられる理由
- **主要なAI企業と任意の合意**を結んでいる
- さらに**AIコンソーシアム**として**300程度のステークホルダー**を集め、**研究・テスト契約**を締結
- **民間のAI企業群**にも**リスク対策の拠り所**となる**インセンティブ**あり

CAISSIは2026年、AIエージェントについて従来のソフトウェアとは異なる新しい**セキュリティ上の脅威**が存在すると整理している。

©Atsumi & Sakai 2026

現状はっきり見えている
産業AIの方向性

©Atsumi & Sakai 2026

産業AI競争の本質：各国は「AI Operating System」へ登る

評価軸を「モデル性能」から、再現可能な産業実装パッケージへ広げる

勝ち筋 ＝ AI知能層 × ドメインデータ× デジタルツイン × 制御/ロボット × 安全性/ガバナンス × アシュアランス × 継続運用

「このOSを導入すれば、工場・病院・港・金融機関を、安全にかつ人を尊重しながらAI化できます」という再現可能なパッケージにした企業・企業連合が非常に強くなる

① 知能層	基盤モデル / エージェント / 産業AI
② 産業層	工場・病院・港・金融のドメインデータ/ ワークフロー
③ 物理層	ロボット / 機械 / センサー / デジタルツイン / 制御
④ 信頼層	安全性 / ガバナンス / TEVV / アシュアランス / サイバー

商品は単体AIではなく「産業を動かす運用体系」へ



米国：最強の部品群、ただし国家OSは「連邦型」

- 知能層・クラウド・半導体・医療/創薬などは世界最高水準。
- 製造AIも弱くない。NISTは2026年ロードマップでデジタルツイン・ロボティクス・自動システムまで扱う。
- FDAはAI医療機器を既存の医療安全制度に組み込み、トータルな製品ライフサイクルで評価。2026年9月時点で1,600超を承認。
- 特徴はNIST・DOE・DoD・FDA・民間が分散するFederated Architecture。**国家が単一産業へ束ねる色は相対的に弱い。・・・産業主導だけで強さを維持できるか？**

AIが物理世界へ降りるほど、統合・安全・制御の競争になる

©Atsumi & Sakai 2026

EU・英国：「物理世界 × 信頼性」を武器に「包括OS」へ

EUは産業・計算資源・規制を統合、英国はAIの安全性＋金融・ライフサイエンスで補完
プラットフォーム化の加速には、米国のフロンティアAI企業の参画が大きく貢献

EU：産業AIの「統合プラットフォーム化」が加速

産業資産
自動車・機械・化学・エネルギー・医療
＋強いドメインエンジニアリング

AI基盤
AI Factories / Gigafactories
Data Labs / Skills

実装
Apply AI：10戦略産業＋公共部門
“AI first” / 中小企業へ展開

信頼性
AI法＋テスト / サンドボックス
法的予見可能性を競争力へ

Siemensは先行候補……かなり手強い

TIA Portal / Xcelerator / デジタルツイン / 自動化にAIエージェントを重ね、**NVIDIAと公式に**、“Industrial AI Operating System for the physical world"を構築中と、2026年1月に発表した。

この計画は、**10年来の計画のようだ。Microsoftとは2017年から**深い連携。
また、**NVIDIAとは2022年から**Siemens Xcelerator + NVIDIA Omniverseの接続、現在の関係に至っている。

このようにして、Siemensの製造AI OSは進行中である。

英国：EU外だが欧州連携を強化

- AI Opportunities Action Plan：産業全体へのAI導入を成長政策化
- Modern Industrial Strategy：金融・ライフサイエンス・先進製造等へAIを展開
- AISI：フロンティアAIの能力・セキュリティリスクを技術評価し、政府の安全知を形成
- ドイツAISI等との評価協力を開始。EU制度内に入るのではなく、欧州の安全性ネットワークと接続。

英国の付加価値
金融 × ライフサイエンス
× フロンティアAIの安全性

→ EUとは「統合」より相互補完・連携

©Atsumi & Sakai 2026

「各国共通する方向性」：産業AI競争は「モデル性能」から「産業OS」競争へ

勝敗を分けるのは、既存産業 × AI × データ × 計算 × 実証 × ガバナンス × 販売網を一体化する能力

EU	英国	シンガポール	台湾	韓国
世界級産業を横につなぐ	安全性を産業価値へ	ガバナンスを市場基盤へ	ハードウェアを知能層へ	フィジカルアセットをAI化
製造・ロボット・医療・航空宇宙・エネルギー AI Factories / Gigafactories 共通データ・テスト・AI法 →「域内産業AI OS」	AISI / フロンティア評価 金融・医療・創薬・リーガルAI 米国フロンティア企業との深い接続 →「アシュアランス型AI OS」	ガバナンス / アシュアランス / テストベッド 金融・製造・医療＋グローバルテック ASEAN/APAC Gateway →「信頼できる産業AI OS」	半導体・ICTサプライチェーン NVIDIA・Microsoft等との接続 クラウド / エージェント / 産業AI →「ハードウェア起点AI OS」	半導体・自動車・造船・バッテリー・ロボット AIファクトリー / フィジカルAI / デジタルツイン →「フィジカル世界の産業AI OS」

産業AI OS競争は熾烈だ。現状、EUのSiemensが群を抜いているが、上記の国々も内容が充実して、しかも素早い。この競争に対応する必要がある。

**単品のAIを売るのではなく、
産業固有のデータ・ワークフロー・安全・規制・実機制御まで束ねた
「再利用可能な産業AIアーキテクチャ」を商品化し、
導入後のデータで継続改善する。**

©Atsumi & Sakai 2026

日本に残された時間：『束ねる時間』が間に合うか？

2026–2027年が設計・実証・国際連携の勝負どころ。2028-29年頃には各地域の標準的な産業AIスタックが固定化し始める可能性

2026–2027 設計・選択

- 日本の勝ち領域を絞る
- 共通アーキテクチャを決める
- 海外スタックを選択的に取り込む
- ガバナンス/TEVVを同時設計

2027 実証・リファレンス化

- 実工場・病院・物流等で検証
- ドメイン データを蓄積
- 失敗→改善のフィードバック
- 海外顧客が買えるリファレンスを作る

2028–2029頃 市場・標準の定着

- AI OS/プラットフォームの切替えコスト上昇
- データ・エージェント・認証が囲い込み要因に
- 海外標準への追随だけでは価値獲得が困難に

脅威：「ガバナンスが利き、アシュアランスがあり、相互運用性のあるシステム商品」へ変換する前に、**他国の産業AI OSが日本より早く顧客接点を取り込んでしまうこと。**

先頭集団は、
確実にもっと早いだろう。

国・産業が今すぐ束ねるもの

① ドメインデータ / データスペース
② 産業基盤モデル / エージェント
③ デジタルツイン / フィジカルAI
④ 共通リスクタクソノミ・TEVV
⑤ セクター別ガバナンス / 認証
⑥ ガバナンス・安全を含むテストベッド / 規制のサンドボックス
⑦ API・相互運用・海外標準等について本質を押さえた詳細なクロスウォーク

©Atsumi & Sakai 2026

お問い合わせ

三部　裕幸

渥美坂井法律事務所・外国法共同事業　パートナー

　弁護士（第二東京弁護士会）、ニューヨーク州弁護士

大阪大学招聘教授（社会技術共創研究センター）

〒100-0011　東京都千代田区内幸町2-2-2

富国生命ビル（総合受付 16階）

Tel: 03-5501-2276

E-mail: hiroyuki.sanbe@aplaw.jp

Eightでの名刺交換用
QRコード（三部裕幸）

当事務所に関するリーガル・ノーティス

1.渥美坂井法律事務所・外国法共同事業について

渥美坂井法律事務所・外国法共同事業（当事務所）は、①渥美坂井法律事務所弁護士法人（第二東京弁護士会所属、代表社員弁護士渥美博夫）（以下「当弁護士法人」といいます。）と当事務所に所属する多くの外国法事務弁護士とが、外国弁護士による法律事務の取扱いに関する特別措置法（以下「外弁法」といいます。）に定める外国法共同事業を行い、②当弁護士法人と、日本の民法上の組合である渥美坂井法律事務所・外国法共同事業（代表弁護士坂井豊）（以下「組合組織」といいます。）の各弁護士とが、共同事業を行い、法律事務所を共にするものです。さらに当弁護士法人と、組合組織の各弁護士は、ヤンセン外国法事務弁護士事務所のマークース・ヤンセン外国法事務弁護士（ドイツ連邦共和国法）と外弁法に定める外国法共同事業を行います。当事務所とその外国法共同事業は、日本の弁護士（イングランド及びウェールズ事務弁護士である者を含みます。）に加え、ニューヨーク州、カリフォルニア州、中華人民共和国、大韓民国、インド、スリランカ民主社会主義共和国、連合王国*、オーストラリア クインズランド州の法を原資格国法とする外国法事務弁護士を擁しています。州法を原資格国法とする外国法事務弁護士はその国の連邦法についても助言を提供することができます。当事務所では、弁護士と、それぞれの登録に係る原資格国法に関する法律事務を行うことを職務とする外国法事務弁護士とが協働して業務を行っています。

当弁護士法人はまた、ロンドンオフィスとして英国子会社たるAtsumi & Sakai Europe Limited（Director: 金久直樹日本国弁護士）を有するとともに、ブリュッセルオフィスとしてAtsumi & Sakai Brussels EU（代表パートナー: 亀岡悦子ブリュッセル弁護士会Bリスト弁護士・ニューヨーク州弁護士**）、ニューヨーク提携オフィスとしてAtsumi & Sakai New York LLP（代表パートナー：バニー・L・ディクソン外国法事務弁護士（ニューヨーク州法））、ホーチミンオフィスとしてAtsumi & Sakai Vietnam Law Firm（Director：入江克典日本国弁護士）をそれぞれ有し、これらのオフィスを通じても助言を提供しています。また日本においてA&S福岡法律事務所弁護士法人（パートナー：臼井康博弁護士）と提携関係を有するとともに、フランクフルトオフィスたるドイツ連邦共和国における法務・税務サービス提供法人たるAtsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater（現地代表：フランク・ベッカー ドイツ連邦共和国弁護士**）とも提携関係を有しています。

*渥美坂井法律事務所弁護士法人はイングランド及びウェールズのソリシターズ・レギュレーション・オーソリティによる規制の適用を受けていません。
**日本における外国法事務弁護士の登録はありません。

2.法律問題に関する助言等について

当事務所による別段の明示がない限り、法律問題に関する当事務所のいかなる助言その他意見の表明も、(i) 日本法、又は当事務所の外国法事務弁護士の登録に係る原資格法以外の外国法に関するものは当事務所の特定された弁護士の、(ii) かかる原資格国法に関するものは当該法をその登録に係る原資格国法とする当事務所の特定された外国法事務弁護士の、判断においてされるものです。

※ 本資料の内容は、一般的な情報提供を目的としており、個別案件についての法的助言ではありません。お問い合わせ等は、上記弁護士までご連絡くださいますようお願い申し上げます。