

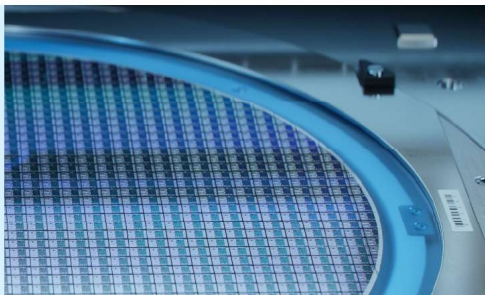


U.S. Chamber of Commerce
International Affairs
Asia

U.S.-Japan
Business Council

JUBC
Japan-U.S.
Business Council

Digital Economy



最先端デジタル技術は、今日の経済におけるあらゆる産業で中心的な役割を果たす。オープンで、安全で、信頼でき、相互運用可能で、強靱なデジタルインフラの発展は、経済成長と国家安全保障にとって不可欠である。日米経済協議会および米日経済協議会（以下「両協議会」）は、政策立案者が以下の提言を検討するよう求める。

1. 信頼できるAIの実装推進

AIガバナンスとセキュリティ: 米国と日本は、米国立標準技術研究所（NIST）のAIリスク

管理フレームワーク（AI RMF、日本のAI事業者ガイドライン、および広島AIプロセ

スからのベストプラクティスを活用し、信頼できるAIエコシステムを構築すべきである。両政府は、Agentic AIに関して、相互運用可能で、国際的に認められた標準、規範、テスト方法、および保証フレームワークの策定・普及を推進すべきである。

ガバナンスフレームワークは、各システムの重要性、自律性の程度、顧客への影響、および機密データへのアクセスを考慮し、リスクに応じて調整されるべきである。その際、分断された重複評価や規制を回避すべきである。また、フレームワークは、AIモデル全般の安全で責任ある利用を確保するとともに、AIおよびデータのサプライチェーンの整合性を保護すべきである。フロンティアAIモデルが自律的に脆弱性を発見する能力を発展させる中、両政府は、正当な研究、レッドチームingおよび防御目的の脆弱性発見が維持されるよう協力するとともに、モデルレベルの安全対策が、防御側の活動を阻害する一方で攻撃者を制約しない結果とならないようにすべきである。

AI人材育成: 人材育成では、リスクリング、アップスキリング、ならびにK-12および高等教育段階におけるAI・機械学習教育の拡充を優先すべきである。政府は、共同研究プログラム、実習・インターンシップの仕組み、AIの責任ある開発・利用に向けたAI倫理研修など、産学間の体系的なパートナーシップに投資すべきである。また両政府は、AIへの信頼と安全性を構築するため、誤情報・偽情報、AIシステムの脆弱性、規制遵守に対応する産業界主導の国民啓発活動を支援すべきである。

エネルギー効率の良いAIインフラ: 米国と日本は、手頃な価格で、信頼性が高く、エネルギー効率の良い技術と電源を備えたデータセンターおよびブロードバンドインフラへの投資を促進すべきである。両政府は、AIエコシステム全体を支える持続可能なエネルギー源および再生可能エネルギー源の開発も奨励すべきである。持続可能なAI開発を促進するため、両政府は、次世代半導体・プロセッサ、先進材料・ろ過技術、効率的な冷却技術などの省エネルギーイノベーションを通じ、AIスタック全体の最適化に取り組むべきである。

フィジカルAI: センシング、認識、制御を統合するサイバー物理連携システムを基盤として、フィジカルAIおよびロボティクスは戦略的技術となりつつある。両政府は、安全性、信頼性、相互運用性、テストに関する共通のアプローチを推進すべきである。テストベッド、規制サンドボックス、標準開発への支援は、責任ある展開を加速させる。ハードウェアとソフトウェアの統合が極めて重要であることを踏まえ、両政府は、最先端の国際技術を活用しつつ、国内および信頼できるパートナー間で重要な能力の強靱性を高める、オープンで協調的なアプローチを追求すべきである。加えて両政府は、フィジカルな展開を可能にするすべての基盤技術に関する研究開発を強化し、サプライチェーンの強靱性を高めるとともに、これらの技術のより広範な展開を促進するため、中小企業（SMEs）の参画を奨励すべきである。

2. 信頼できる自由なデータ流通の促進

信頼できる越境データ流通:両政府は、信頼できる越境データ流通を支援し、複数の法域にわたるデータに依存するAIサービスに影響を与える要件を含め、不要なまたは差別的なデータローカリゼーション要件を避けるべきである。両政府は、機密データを保護しつつ、責任あるデータ利用、研究、および越境連携を可能にする、相互承認された個人データ保護規制と研究開発の取り組みに向けて協力すべきである。

国際的に認められた標準:両政府は、グローバル越境プライバシールール（CBPR）フォーラム、APEC、およびOECDのトラストによる自由なデータ流通（DFFT）専門家コミュニティによって確立されたベストプラクティスと市場指向の運用ルールを用いて、データ相互運用性を推進すべきである。

産業データスペース:日本と米国は、日本のウラノス・エコシステム構想に示されているように、安全なデータ共有の基盤として、信頼性が高く相互運用可能な産業データスペースの整備を推進すべきである。こうした協力は、革新的な技術の進歩とサプライチェーンのセキュリティを支援し、安全な運用技術（OT）および製造データ・エコシステムがフィジカルAIのイノベーションの加速を可能にするであろう。

3. 新興技術における日米のリーダーシップ強化

半導体:あらゆる種類の半導体の戦略的重要性を考慮し、米国と日本は、多様化、国際協力、共同資金提供、および研究開発を通じて、原材料や専用材料から、デバイス製造、高度なパッケージングに至るまで、半導体サプライチェーン全体を確保するために協力すべきである。サプライチェーンのあらゆる部分を対象とする共同開発プロジェクトは、競争力を高め、現在のサプライチェーンの不安定性を克服することにつながる。両政府はまた、半導体材料、装置、および関連技術の取引を促進する透明性の高い政策を促進するため貿易障壁を削減し、同時に高度な製造サプライチェーンのコストを増加させる関税および非関税障壁を削減しなければならない。

量子技術:両政府は、量子ネットワークおよびコンピューティングシステムの実用化に焦点を当て、量子技術の共同開発を推進すべきである。量子コンピューティングは、デジタル経済を保護する暗号を損なう可能性があるため、米国と日本の双方にとって戦略的なサイバーセキュリティ上の課題でもある。量子システムが実用化に近づく中、両政府は、産業競争力を高めるための活用を重視するとともに、量子リスクを国家安全保障および経済安全保障上のシステムミックな問題として認識し、量子セキュア通信を推進しつつ、ポスト量子暗号を含む量子耐性暗号アルゴリズムへの移行を組織に促すための措置を講じるべきである。

両協議会はまた、必須材料のサプライチェーンを確保するとともに、相互運用性に関する国際的に認められた標準について産業界と協力するよう、政府に支援を要請する。

研究開発（R&D）およびイノベーション政策:両政府は、競争力のある税制優遇措置、先端製造施設に対する許可手続きの簡素化、官民の研究開発（R&D）パートナーシップへの安定した資金提供などを通じて、研究開発への継続的な投資を奨励する政策環境を育成すべきである。次世代プロセス技術および材料科学への長期的な設備投資を促す政策は、日米の技術的リーダーシップを維持するために不可欠である。また両政府は、両国間における重要技術関連の製品およびサービスの自由な流通を促進する、相互承認協定および調和された規制標準を追求すべきである。

4. 強靱な次世代ICTインフラの開発

接続性のためのオープン技術:米国と日本は、安全で信頼できるデジタル接続性を促進し、明確で安全なICT接続ソリューションを育成する政策を推進すべきである。これには、無線アクセスネットワーク（RAN）、無線ローカルエリアネットワーク（RLAN）、光伝送、ネットワーク管理、ならびに動的周波数共用（DSA）および自動周波数協調（AFC）など、周波数資源のより効率的な利用を可能にする技術を含む、仮想化され、オープンで、相互運用可能かつ標準ベースのネットワーク技術の奨励が含まれる。相互運用可能なアーキテクチャは、信頼できるベンダーの選択肢を拡大し、サプライチェーンを多様化する。6Gの開発に向け、両政府は、こうした相互運用の取り組みを継続するため、透明性のあるルール策定について連携しなければならない。

多層ネットワーク:両政府は、海底ケーブルと遠隔地でのカバレッジと災害時のレジリエンスを向上させる低軌道（LEO）衛星コンステレーションのような非地上系システムを統合した、国際通信に対する多層的なアプローチを取るべきである。政府はまた、信頼できるサプライヤーとの第三国海底ケーブルプロジェクトの資金調達において民間部門を支援すべきである。

5. 強靱なインフラのためのサイバーセキュリティ強化

AIを活用した脅威軽減: 米国と日本は、専門人材不足に対処しつつAIリスクを軽減する、安全なAIシステムとサイバーセキュリティソリューションを開発しなければならない。インフラのレジリエンスには、リスクベースのアプローチを通じた技術、政策および国際協力の統合が必要である。NISTサイバーセキュリティ・フレームワークなどのサイバーセキュリティ・フレームワークは、政府、重要インフラおよびサプライチェーン全体で活用されるべきである。両政府は、ソフトウェア部品表（SBOM）、IoTサイバーセキュリティ・ラベリング、セキュア・ソフトウェア開発フレームワークなどの標準の普及を主導すべきである。両政府は、成熟した是正プロセスを有するベンダーによる迅速なパッチ展開を可能にし、政府調達およびインセンティブ資金を通じてサポート終了（EOL）技術の廃止を加速するとともに、重要な運用を中断せずにパッチ適用またはオフライン化できないシステムを保護するため、AIを活用した補完的なセキュリティ対策を奨励するよう、脆弱性管理フレームワークを近代化すべきである。政府はまた、インシデント報告期限の整合化を図るとともに、協調的脆弱性開示（CVD）の枠組み外で、未修正の脆弱性情報の開示を義務付けることを避けるべきである。

国際協力: 先端技術を悪用したサイバー攻撃に対抗するため、共同イニシアティブには以下が含まれるべきである：機械学習とディープフェイク検出を統合したAIベースのサイバー攻撃検出モデルの開発；サイバー脅威インテリジェンスの共有；共同技術標準とパイロットプロジェクトによる量子安全通信システムの共同開発。

両協議会は、日本の能動的サイバー防御法制の趣旨を評価するとともに、その施行規則の策定にあたり、日米サイバー対話トラック1.5などの対話を通じて緊密な官民連携を継続し、透明性および比例性を確保するとともに、ICTベンダーに対する画一的な設計義務を回避するよう求める。

6. デュアルユース技術に関する戦略的協力の強化

フィジカルAI、ロボティクス、先進ICT、半導体、および量子技術の分野で、民間用途と国家安全保障用途の境界が曖昧になり続けているため、米国と日本は、セキュリティを保護しつつイノベーションを維持する、リスクベースで透明性のあるガバナンスフレームワークを推進すべきである。

優先分野には、より明確な技術分類、輸出管理と投資審査における透明性の向上と整合、より強力な研究セキュリティと知的財産（IP）保護、および産業界、学术界、政府間の信頼に基づく人材交流・協力が含まれる。これらは、企業にとっての予測可能性を向上させ、正当な商業および研究協力への不必要な障壁を回避する。