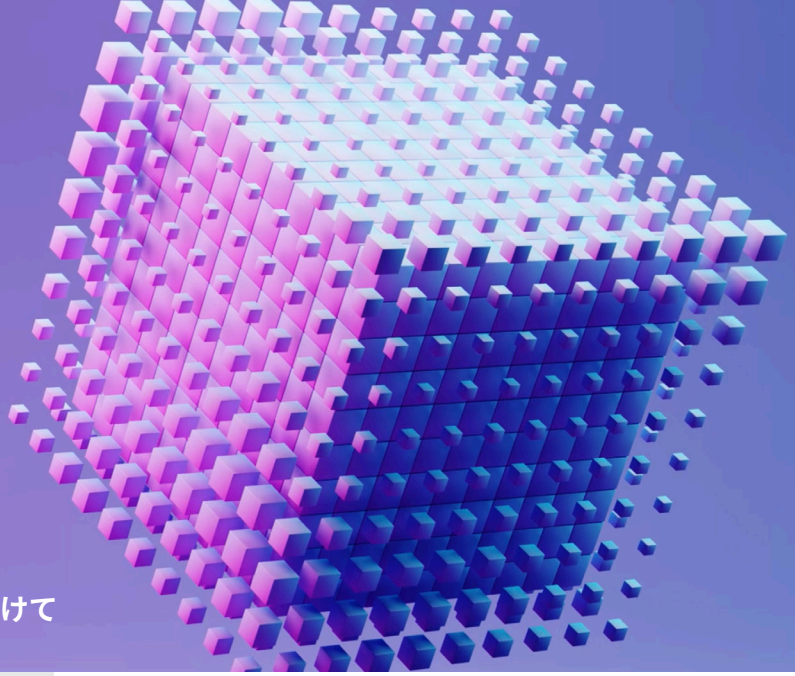
THE
kyndryl
institute



トレンドトピック：**準備に向けて**

執筆


**Klon Kitchen 氏**

**American Enterprise Institute（アメリカ企業研究所）の非常勤の上級フェロー**

Klon Kitchen 氏は、American Enterprise Institute（アメリカ企業研究所）で非常勤の上級フェローとして、国家安全保障と防衛技術、イノベーションの接点を研究の主題に据えています。同氏は研究を通じて、サイバーセキュリティ、人工知能、ロボット工学、量子科学に重点を置きつつ、サイバーセキュリティ、AI、ロボット工学、量子科学を中心とする新たなテクノロジーが、現代の国家運営、諜報活動、軍事作戦にどのような影響を与えているかを分析、解説しています。

AEI 加入前、彼はヘリテージ財団の技術政策センターの所長として、財団の部門をまたいで専門家を集め、国の重要なテクノロジー課題を理解し、政策づくりを主導していました。ヘリテージ財団の前は、Ben Sasse 上院議員（共和党・ネブラスカ州）の国家安全保障顧問を担当。米国のサイバー大戦略策定を任務とする有識者委員会「米国サイバー空間検討委員会」の創設に携わりました。


**Kyndryl Institute の詳細をさらに見る**
kyndryl.com/institute

# 新たなセキュリティ情勢に向けた AI の備え

人工知能（AI）は世界的な競争の構造を変えつつありますが、米国企業にとっての課題はもはや単なるイノベーションではありません。国家安全保障と企業責任が重なり合う地政学的環境の中で、いかに生き残るかが問われています。

**多**くの経営幹部が、活用事例の特定、インフラへの投資、導入の課題解決など、AI による変革の可能性を見据えて組織で準備を進めています。しかし、同じく重要な側面として注目すべきは国家安全保障への影響です。

**コ**ンプライアンスのチェックリストや広報危機管理の準備だけに限った話ではありません。AI 導入がもたらす、より広範な地政学的、経済的、安全保障上の影響と、米国とその国益を守る上で各組織が果たす役割を理解することです。

## 新たな国家安全保障上の責務

**AI** はもはやサプライチェーン最適化や、サービス効率化のための道具ではありません。戦略的資産であり、敵対する国々がかつてない執念で狙っているものです。米国政府はこれらを現実問題として捉えています。例えば、国防総省は AI を軍事的優位性を維持するための基盤技術と見なしています。連邦機関は AI の能

力に関連する技術に対する輸出規制を強化し、データの流れを監視し、重要なインフラの保護を重視しています。こうした行動は場当たり的なものではなく、現実の脅威に対する合理的な対応です。

中国の AI に抱く野心は、とりわけ示唆に富んでいます。中国政府は 2030 年までに AI のグローバルリーダーになるという目標を明確に掲げています。この目標は、学術的な成果や業界での評価にとどまるものではなく、より広範な地政学的戦略の要になっています。中国の指導層は、AI が単に技術革新の勝者を決めるだけでなく、経済・技術・軍事分野における勝者を決めると理解しています。

この覇権への渇望は、さまざまな形で現れています。中国企業は、国内外で数百万人の市民を追跡する監視システムに AI を組み込んでいます。顔認識や犯罪予測による治安維持のような技術は、単なる社会統制の道具ではなく、世界的に影響力を行使するための仕組みです。さらに、中国の産業政策（AI 関連技術への補助金など）は、国内企業に世界市場で優位に立たせ、地政学的な対立が生じた際に利用できる依存関係を築いています。

この典型例が中国の世界規模のインフラ戦略である「一帯一路」のデジタル版シルクロードに AI システムを組み込み、中国の政治的・経済的な影響力を拡大しようとしています。この構想に関わる国の多くにおいて、スマートシティや行政システムに中国製の AI システムを採用しています。これら AI システムの導入国は継続的なサポート、更新、統合を必要とし長期的な依存関係を生じさせます。結果として、中国政府は世界規模で政治的・経済的影響力を行使することを可能とします。

敵対勢力が戦略的優位性を確保するための徹底ぶりを際立たせており、近年の米国の AI インフラを狙った事件もその傾向を裏付けています。

独自アルゴリズムにターゲットを絞ったスパイ活動は、ハードウェアも巻き込むサプライチェーンへの侵入となり、その脅威は巧妙かつ広範囲に及んでいます。例えば、中国製ハードウェア部品に埋め込まれた脆弱性の報告は、重要システムに潜むバックドア（不正な侵入経路）の可能性について警鐘を鳴らしています。机上の空論ではありません。高度に結びついたグローバル経済で毎日のように起きている現実です。

影響は、知的財産の盗難にとどまりません。敵対的な干渉がもたらしうる結果を考えてみましょう。AI システムが学習段階で改ざんされると、その結果は財務、運用、さらには生死に関わる重要な意思決定に影響が及ぶまで気づかれない可能性があります。これは仮定の話ではありません。機械学習システムへの攻撃は数多く報告され、急速に進化しています。

> 脅威は、独自アルゴリズムを狙うスパイ活動から、ハードウェア部品に入り込むサプライチェーン攻撃まで、巧妙かつ広範囲に及んでいます。

## 業界の役割が重要な理由

米国政府ができることには限界があります。中国では産業が国家の指示で動くのに対し、米国の強みは革新的な民間部門にあります。この民間部門の強みは光と影を併せ持ちます。一方では飛躍的な進歩を生む創造性と俊敏性を可能にし、他方では企業が自社事業についての国家戦略的な側面を軽視すると脆弱性を生むことにもなるからです。

> 国家安全保障上の危機に対処できないことは、各組織が抱える弱点ではなく、システム全体の問題です。グローバル経済は相互につながっているため、一つの拠点が侵害されるとその影響が連鎖的に波及する恐れがあります。

AI とサプライチェーンセキュリティの接点を考えてみましょう。多くの組織は、AI 導入を支える GPU、センサー、半導体などを外国製ハードウェアに依存しています。こうした部品が敵対国製である場合、バックドアや脆弱性を内包している可能性があり、システムの完全性を損なうだけでなく、重要分野全体の安全保障をを危険にさらすことになるかもしれません。近年の半導体不足は、これらのサプライチェーンがいかに脆いかを浮き彫りにしています。この脆弱性に悪意のある干渉のリスクが加われば、事態の深刻さはより明らかになるでしょう。

米国政府はすでに対策を打ち始めています。高度な半導体に対する輸出規制、重要産業の国内生産回帰、官民連携を強化する政策は、すべて共通の目標、すなわち米国の AI の未来を守ることを目指しています。しかし、これらの措置は、産業界の積極的な参加なしに成功しません。民間部門は傍観者ではなく、最前線に立つことを求められています。

企業にとって、単に制裁や規制の罰則を避けるだけの問題ではありません。競争力の問題です。強固なセキュリティ対策を整え、国家の方針と歩調を合わせている企業は、優位に立つことができます。それは、連邦政府との契約、海外顧客の獲得、地政学的な監視が高まる時代における風評被害の回避において優位な立場を得ることが出来るでしょう。官民双方の利害関係者が説明責任を求めるようになっているため、適応できない企業は厳しい戦いに追い込まれるでしょう。

## 業界でのより広範な利害関係

国家安全保障上の危機に対処できないことは、各組織個別の弱点ではなく、社会システム全体の問題になります。グローバル経済は相互につながっているため、一つの拠点が侵害されるとその影響が連鎖的に波及する恐れがあります。例えば、AI 搭載の物流プラットフォームが一つ攻撃されると、業界全体のサプライチェーンが混乱し、経済不安が増幅する恐れがあります。

さらに、敵対国が革新を続けるにつれて、攻撃能力と防御能力の差は広がっていきます。受け身の姿勢ではもはや通用しません。企業は、自社の AI 関連の取り組みにセキュリティを DNA に組み込む積極的な戦略を採用しなければなりません。技術的な解決策だけでなく、文化的、組織的な取り組みも必要です。

敵対国が重要インフラ（エネルギー網や交通網など）を管理する AI システムの意思決定に巧妙に介入することを想像してみてください。被害は当初の標的にとどまらず、社会的信頼の失墜、経済の不安定、さらには広範な地政学的な影響をもたらす可能性があります。こうしたリスクは、企業の規模や業界に関係なく、どの企業もより広範なエコシステムの確保における自らの役割を見過ごす余裕がないことを如実に示しています。

## 行動を起こす：リーダーのためのロードマップ

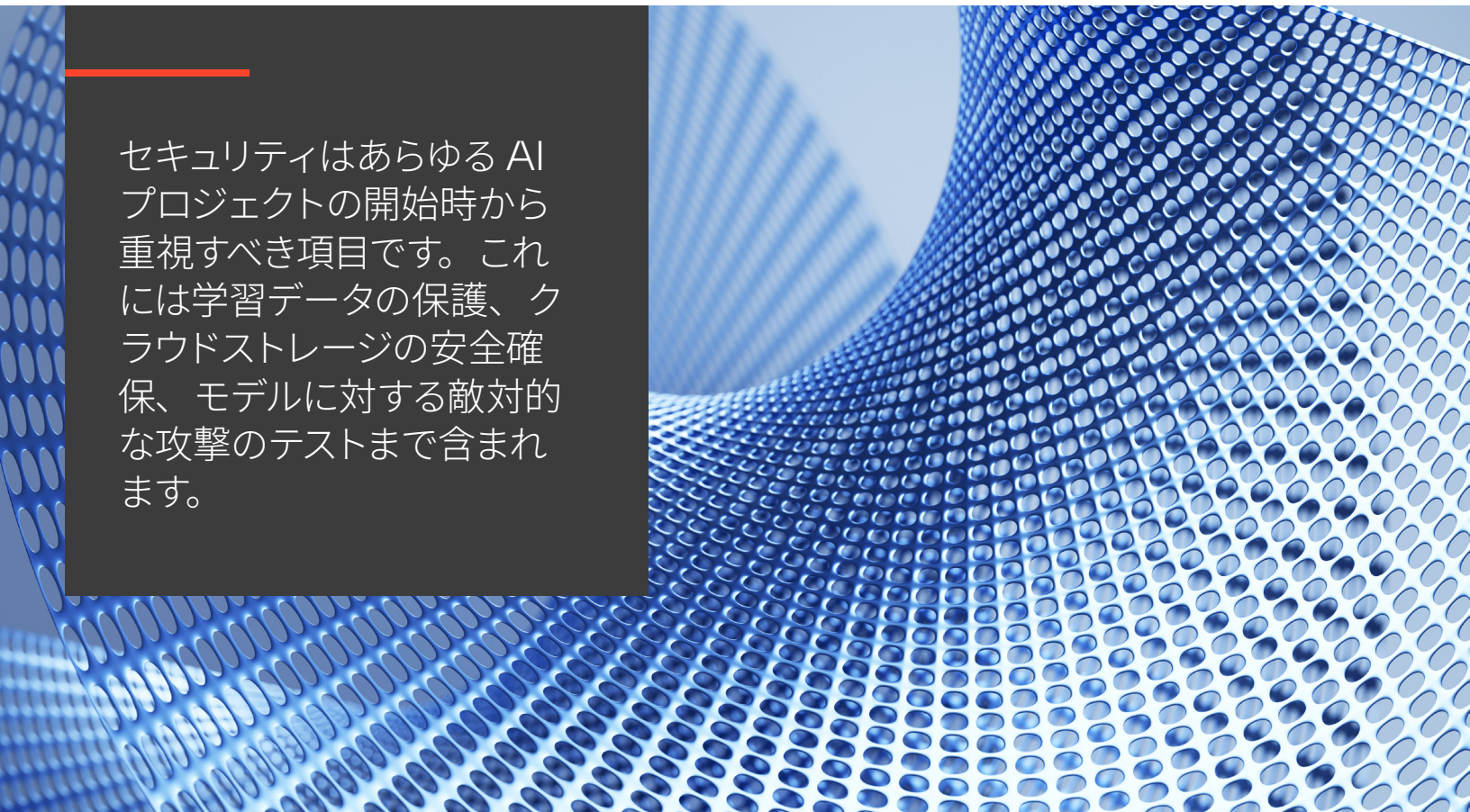
課題を真剣に受け止める準備ができている CEO や CISO にとって、国家安全保障上のリスクに対処するための手段がいくつかあります。

第一に、地政学的なリスク評価を実施することです。地政学的な観点からAI活用のサプライチェーン、パートナーシップ、データ関連業務を評価します。ハードウェア部品はどこから調達しているのか？使用しているクラウドのベンダーはどこなのか？また、ベンダーはどの国・地域の法的規制を受けているのか？これらの問いに対する答えは、詳細なリスクマップを作成するのに役立ちます。地政学専門のコンサルティング会社と提携し、国際政治の変化が自社の脆弱性にどのように影響するかを把握しましょう。

次に米国政府との協力です。国防総省、国務省、商務省などの連邦政府機関と正式な関係を構築します。AI セキュリティに焦点を当てた官民連携に携わり、「国家人工知能イニシアチブ」などの連邦政府の取り組みに参加してください。コンプライアンスを超えた連携により、新たな脅威に対する知見が得られ、組織のセキュリティ体制を強化するツールにアクセスできるようになります。

三つ目は、AI のライフサイクル全体に「Security by Design（設計段階からのセキュリティ）」を組み込むことです。あらゆる AI プロジェクトは、開始時からセキュリティを中核に据える必要があります。これには学習データの保護、クラウドストレージの安全確保、モデルに対する敵対的な攻撃のテストまで含まれます。導入後の AI 動作における異常を監視するための自動化システムを実装します。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などを活用して、リスクの特定と軽減を標準化することを検討します。

最後に、組織の自己回復力の構築です。AI に関する国家安全保障上のリスクは技術的なものだけではなく、業務や行動様式にも及びます。セキュリティ専門家、法律顧問、技術者を含む組織横断型チームを編成し、総合的なアプローチを確保しましょう。従業員が新たな脅威を認識し対処できるように訓練し、イノベーションの中にセキュリティの観点が組み込まれる文化を醸成することが不可欠です AI に起因する混乱を想定したシナリオ演習を定期的にシミュレーションし、自らの備えの状況を確認し、潜在的な弱点を特定します。リーダーとしての立場を活かし、AI セキュリティに関する業界横断的な標準やベストプラクティスの策定を訴えてください。同業者、業界団体、政策立案者と協



力し、民間部門のイノベーションを公共部門の優先課題と整合させる取り組みを推進してください。安全で強靭な AI エコシステムの構築に貢献することで、自社の安全性が強化されるだけでなく、責任ある業界リーダーとしての評判も高めることができます。

## 結論

AI の台頭は、これまでにないチャンスと同時に重大な責任をもたらします。CEO や CISO は、この相反する課題をマネジメントするための特別な立場にあります。すでに複雑なデジタル変革を乗り越えて組織をリードしてきた能力は証明済みです。今求められているのは、そのリーダーシップを拡張し、国家安全保障リスクが高まる時代における AI の広範な影響を考慮に入れることです、。

企業は孤立して運営されているわけではありません。それぞれは、グローバルな力学に影響され、同時にそれを形成する、巨大なエコシステムの一部となっています。AI に関する備えの中で、国家安全保障の観点に対応することは、自社の将来を守るに止まらず、米国が安全・競争力・自由を維持するための中核的な役割を担うことを意味します。

リスクは高いですが、その影響力も同様に大きいです。今こそ断固として行動する時です。変革をもたらすテクノロジーの担い手として、あなたがたはイノベーションと強靭性の双方を左右する鍵を握っています。問われているのは、適応できるかどうかだけでなく、リーダーシップを発揮できるかどうかです。

その答えが、皆さんがどのようなリーダーとして語り継がれるかを決め、同時にシステム全体の安全性を決定づけることになります。