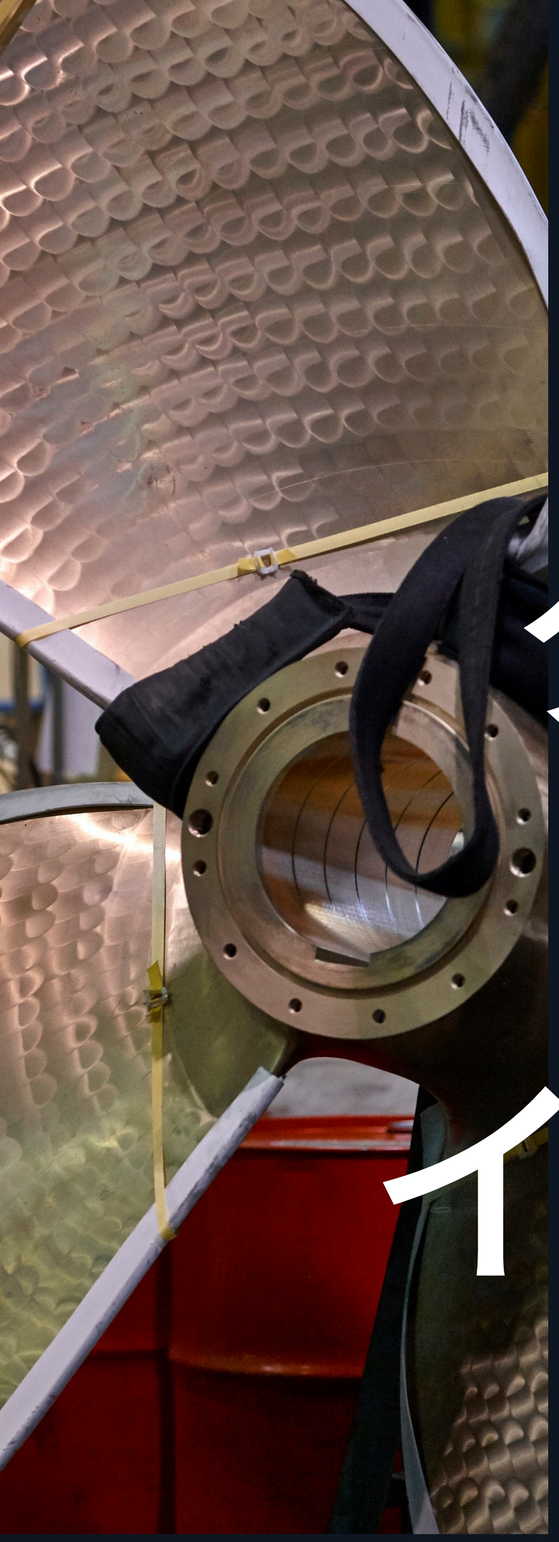
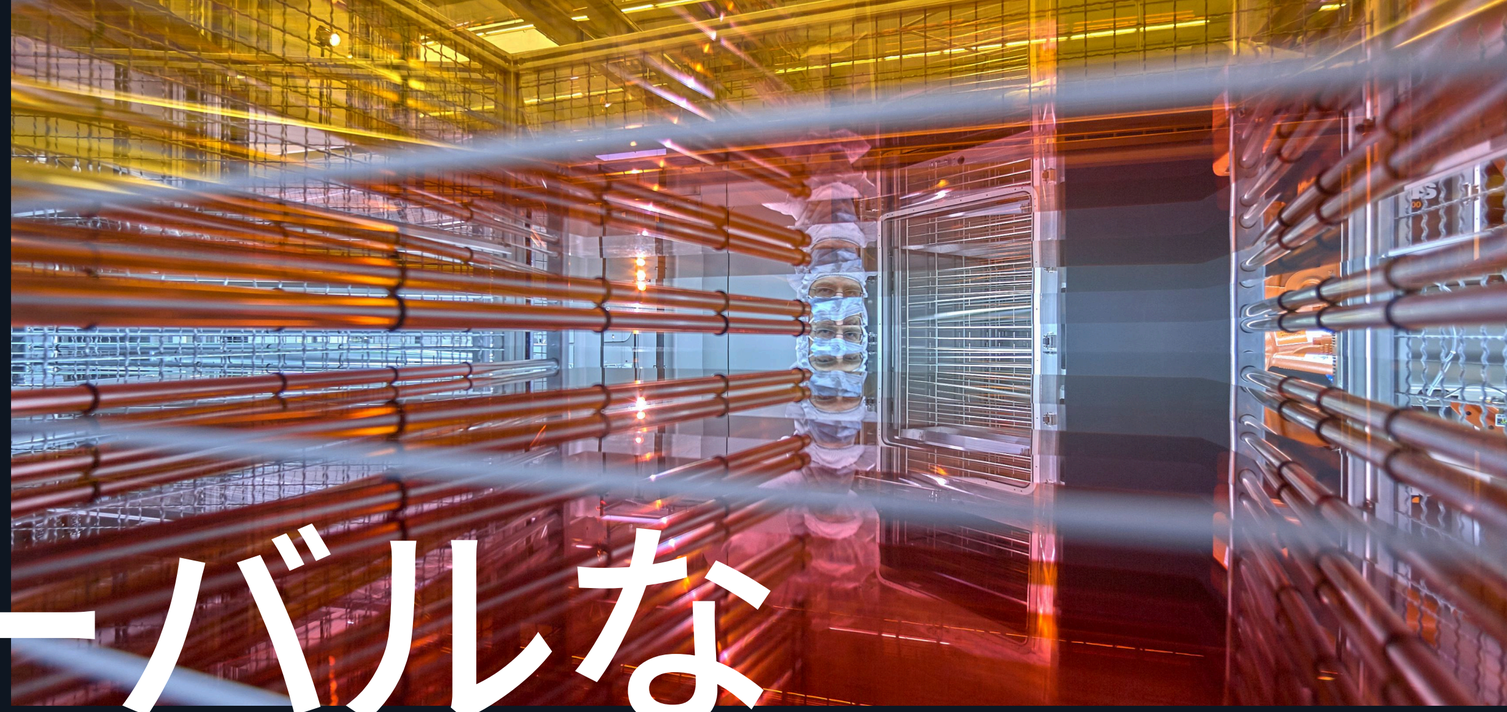




グローバルな技術競争におけるイノベーションの保護

国家レベルのリスクを把握・低減するための
エグゼクティブ・ガイド

STRIDER

目次

概要：

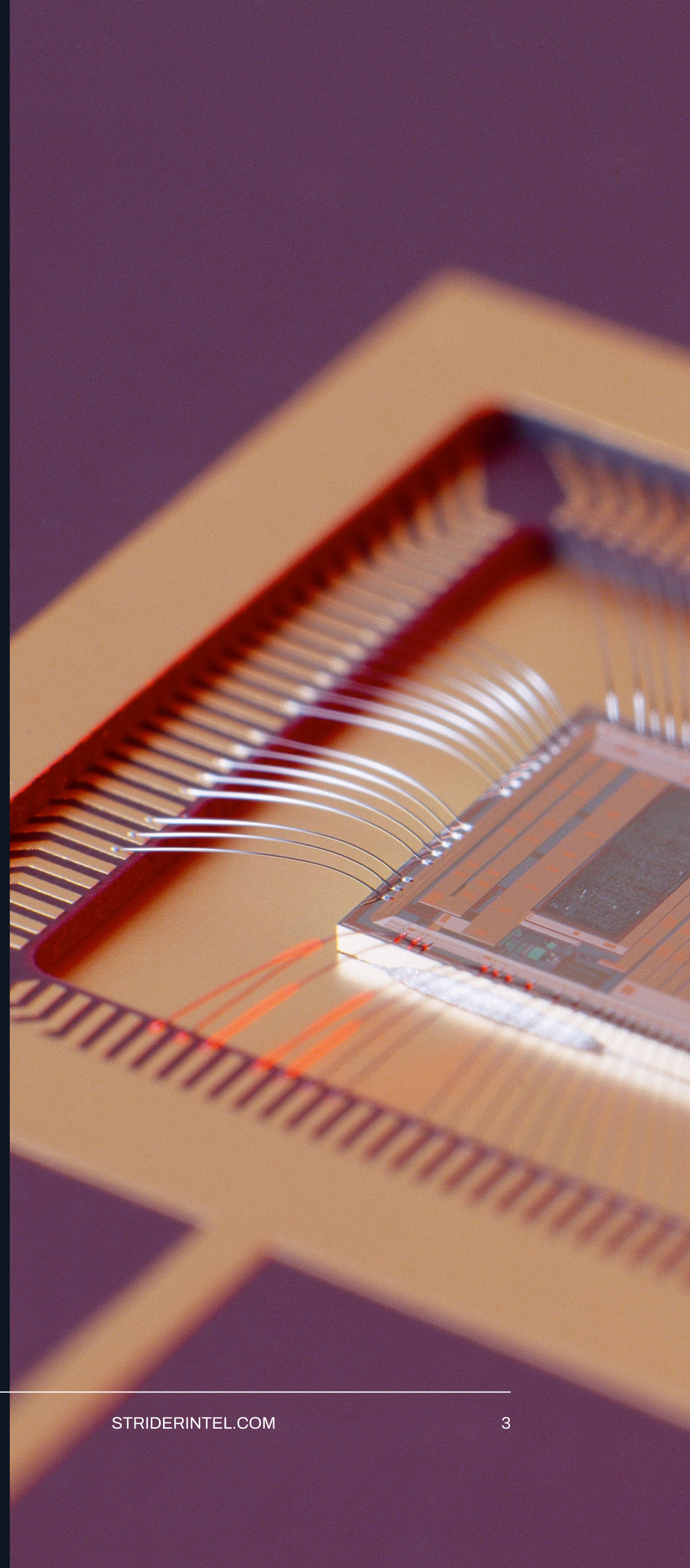
将来に向けた競争

イノベーションは進歩を促進させるとともに、グローバルな競争も促進させます。しかし、各国が新技術でリードしようと競うにつれて、優位性を得るために用いる戦術は変化しつつあります。

次の世界的影響力の波は、領域や貿易ルートではなく、科学・技術・データ分野における画期的発明によって決まるでしょう。敵対国の政府は、技術的優位性の確保に数十億ドルを投資しており、世界経済のオープン性や現代的な共同研究という性質を悪用することも珍しくありません。かつては健全なグローバル競争と思われていたものが、今ではアクセス権、影響力、支配力を巡る複雑な争いとなっているのです。

敵対国は専門家を採用し、内密のパートナーシップを構築し、他国の技術を黙って吸収して、自国の発展を加速させます。正式な産業政策を通じて行われる場合もありますが、国家とつながりのある企業や大学、研究プログラムといった目に見えにくいネットワークを通じて行われる場合もあります。どちらの場合も、世界的に価値の高いイノベーションを手に入れようと協調して取り組む点は同じです。こうした環境において、イノベーションは単なる競争優位性ではなく、国益と言えます。

重要なのは、企業が競争の中にいるかどうかではなく、
自社の優位性を維持しているかどうかです。



国家レベルのリスクとは何か

国家レベルのリスクとは、政府が国家的目標を進めるべく、場合によっては内密の手段や人を欺く手段を用いて戦略的活動を実施または支援することを指します。

こうした活動の例：

- 知的財産の窃取、技術の流出
- 人材の採用、内部者によるアクセス
- 隠れた意図のある学術的または商業的パートナーシップ
- サプライチェーンの操作、サイバー侵入

過去数十年の間、この種のスパイ活動は政府の機密データが対象となっていました。しかし現在では、民間産業、特に半導体、バイオ医薬品、航空宇宙、人工知能といった最先端分野も、国家主導のスパイ活動の標的となっています。

現代の競争は、戦場ではなく、研究開発ラボ、取締役会議室、コードベースで行われています。

国家支援型
行為者の活動状況

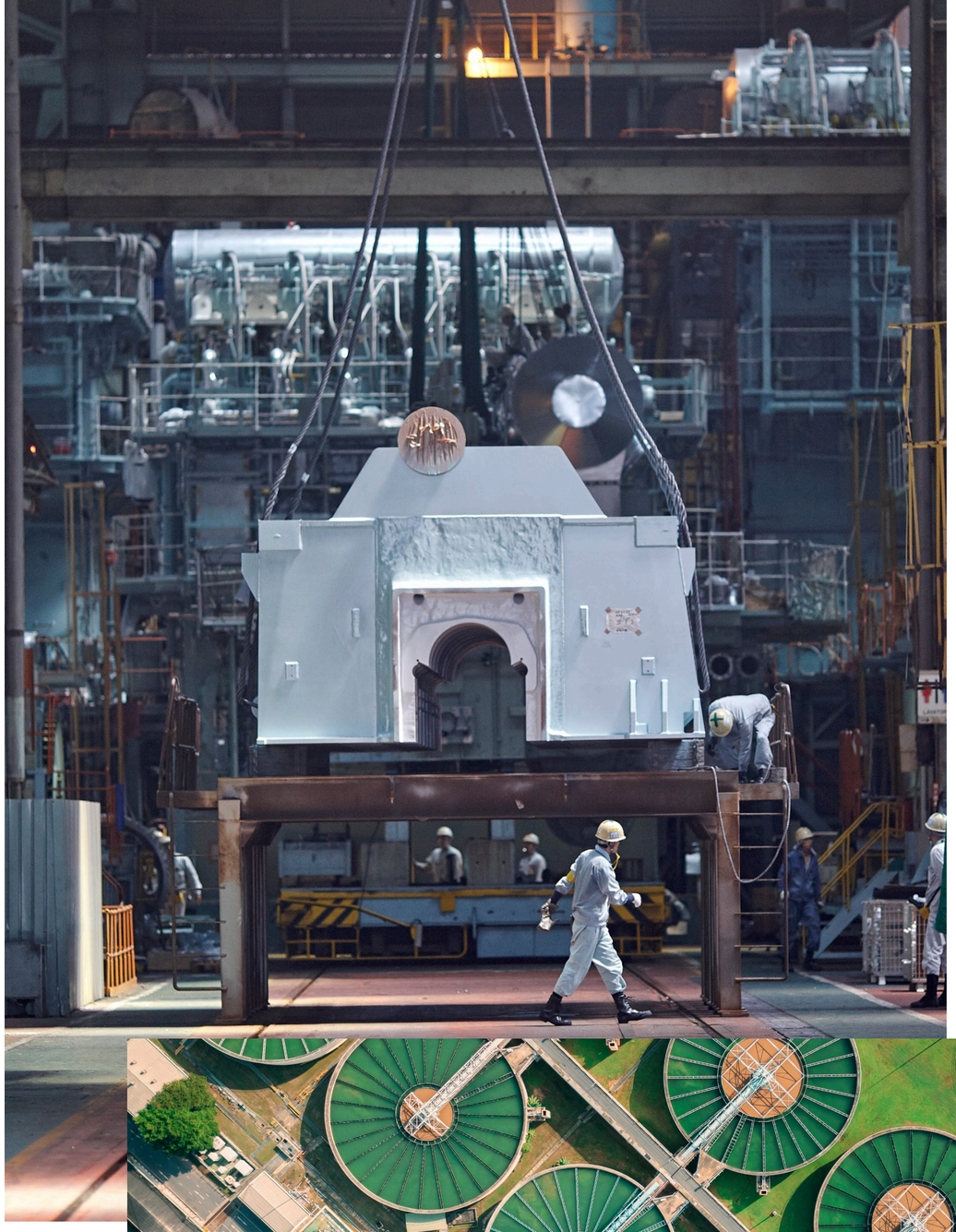
国家支援型行為者とは、他国の政府のために活動する個人や組織を指します。表向きは投資家や採用担当者、協力者、サプライヤーのように見えるかもしれませんが、彼らの最終的な目標は、自国の戦略的利益を上げることです。

現在、こうした活動はかつてないほど広範囲にわたり、組織化され、かつ持続的になっています。また、それらはもはや個別のインシデントではなく、政府機関、国営企業、大学、フロント企業にわたって協調的・長期的に行われるプログラムとなっているのです。

標的の例：

- 二重用途（商用および軍用）の可能性のある新技術
- 最先端の知的財産や生産方法
- 上級職の科学者、エンジニア、研究者

あらゆるパートナーシップは、協力を得る機会でもあり、侵害を受ける機会でもあります。



イノベーション窃取のコスト

国家レベルのリスクによる影響は、抽象的ではなく測定可能です。米国経済は、商品の偽造、ソフトウェアの著作権侵害、企業秘密の流出によって、毎年推定2,500〜6,000億ドルを失っています。

こうした数字の背後には、試作品が海外に流出してしまったスタートアップ企業や技術がコピーされたせいで業績が低下したメーカー、画期的な発明が他国の特許下で再利用されてしまった研究チームなど、実際の企業や組織が存在するのです。

コストとは、単に金銭面のことだけではありません。イノベーションが奪われることで、信頼の損失、投資の停滞、競争力の低下につながります。

アイデアが失われると、グローバルな技術競争で後れを取ることは避けられません。

技術窃取の実例

学術協力か内密の人材採用か？

ハーバード大学の教授が、中国の人材採用プログラムに関与したことと中国企業から内密に研究資金を受けたことについて、米国当局に偽証した罪で起訴されました。同氏は著名な研究ラボのリーダーでしたが、金銭的なつながりや、中国の戦略的研究目標を推し進める協定を結んでいたことを隠していました。この事例では、国家主導のプログラムが学術的なオープン性を悪用して、米国のイノベーションや人材に近づく恐れがあることが明らかになりました。

出典：米国司法省

企業秘密の流出

米国の大手テック企業の元エンジニアが、自律走行車の部品の独自設計を盗み、その情報を国外に持ち出そうとしていた罪を認めました。検察側は、このデータ窃取によって同様の技術を開発している中国の競合企業が利益を得た可能性があると判断しました。この事例は、内部者によるアクセスやグローバル・モビリティが、国家とつながりのある技術獲得活動の促進にどう利用されるかを示しています。

出典：米国司法省

人材が標的となる経緯

競合国にとって、効果の高い手段の1つが人材の獲得です。競合国は、欧米の企業や大学から科学者やエンジニアを積極的に採用し、高報酬の職位、研究資金、キャリア上の名声を与えます。

こうした活動は、LinkedInでの専門職に関するメッセージや、カンファレンスへの招待、海外での研究のオファーなど、何気なく始まることがよくあります。しかしその背後には、知的財産や専門知識を引き出すことを目的とした体系的な人材採用プロセスが存在する可能性があります。

企業はこの人材採用サイクル（候補者の特定・評価・育成・採用・管理）を把握することで、自社の従業員や知識をより効果的に守ることができます。

従業員は企業の最大の資産であり、
最大の弱点でもあります。

中国の技術獲得モデル

中国は、「中国製造2025」や「中国5カ年計画」などの国家戦略を通じた技術獲得のアプローチを正式に発動しました。これらの構想は、国家計画と市場のメカニズムを組み合わせて、技術上のギャップを埋め、他国のイノベーションへの依存を減らすというものです。

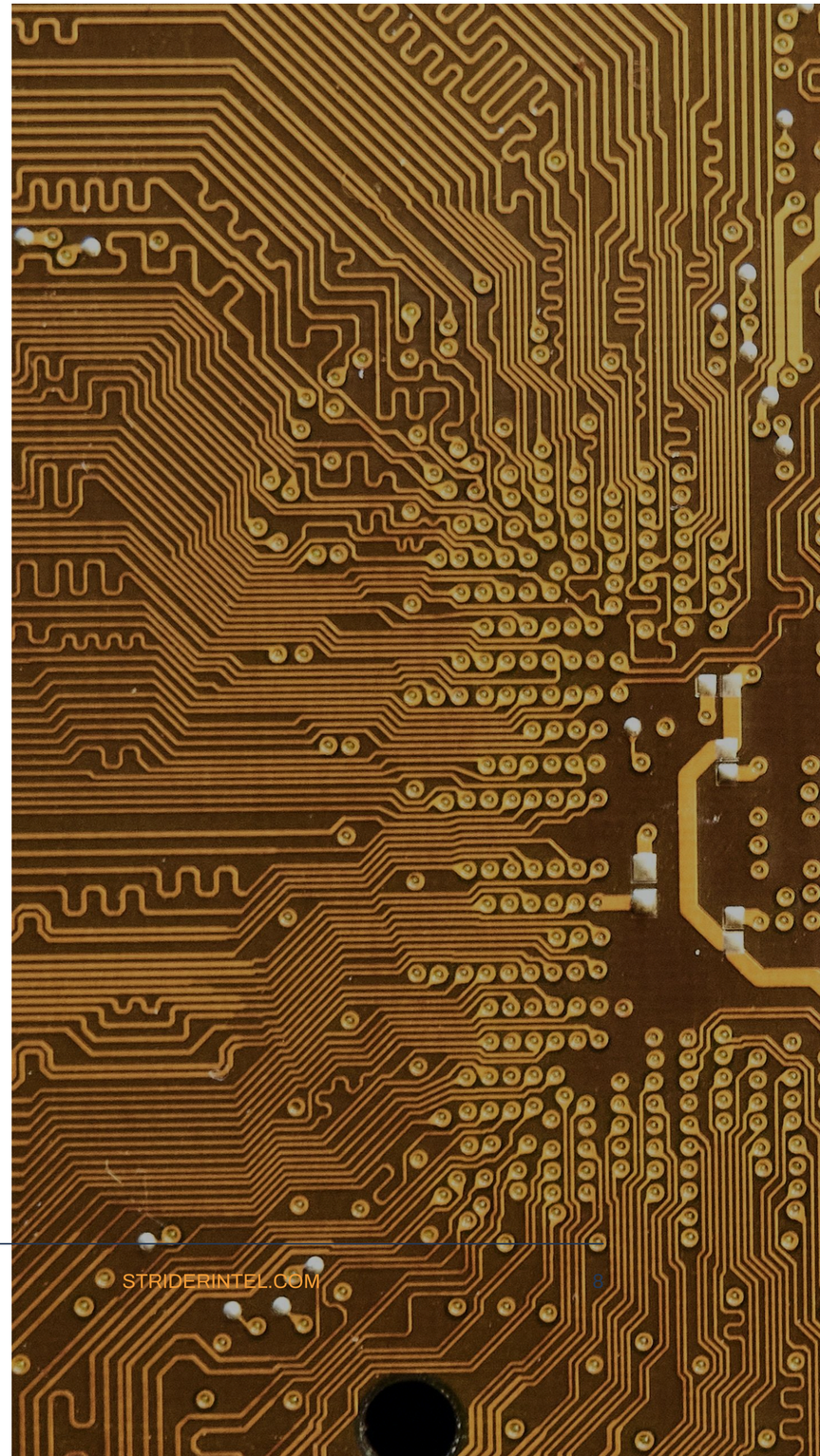
こうしたプログラムは「国産イノベーション」を強調しつつも、その成功の大部分は、以下の手段で外部から技術を獲得し、適応させることに頼っています。

合弁事業や学術協力

他国でトレーニングを受けた専門家を対象とした人材採用

企業パートナーシップや投資手段

このように協調的な社会全体での活動は、国家レベルのリスクがサイバースパイの範囲をはるかに超えて拡大していることを示しています。こうした活動は、世界規模での合法的な人材・データ・資本交換に組み込まれているのです。

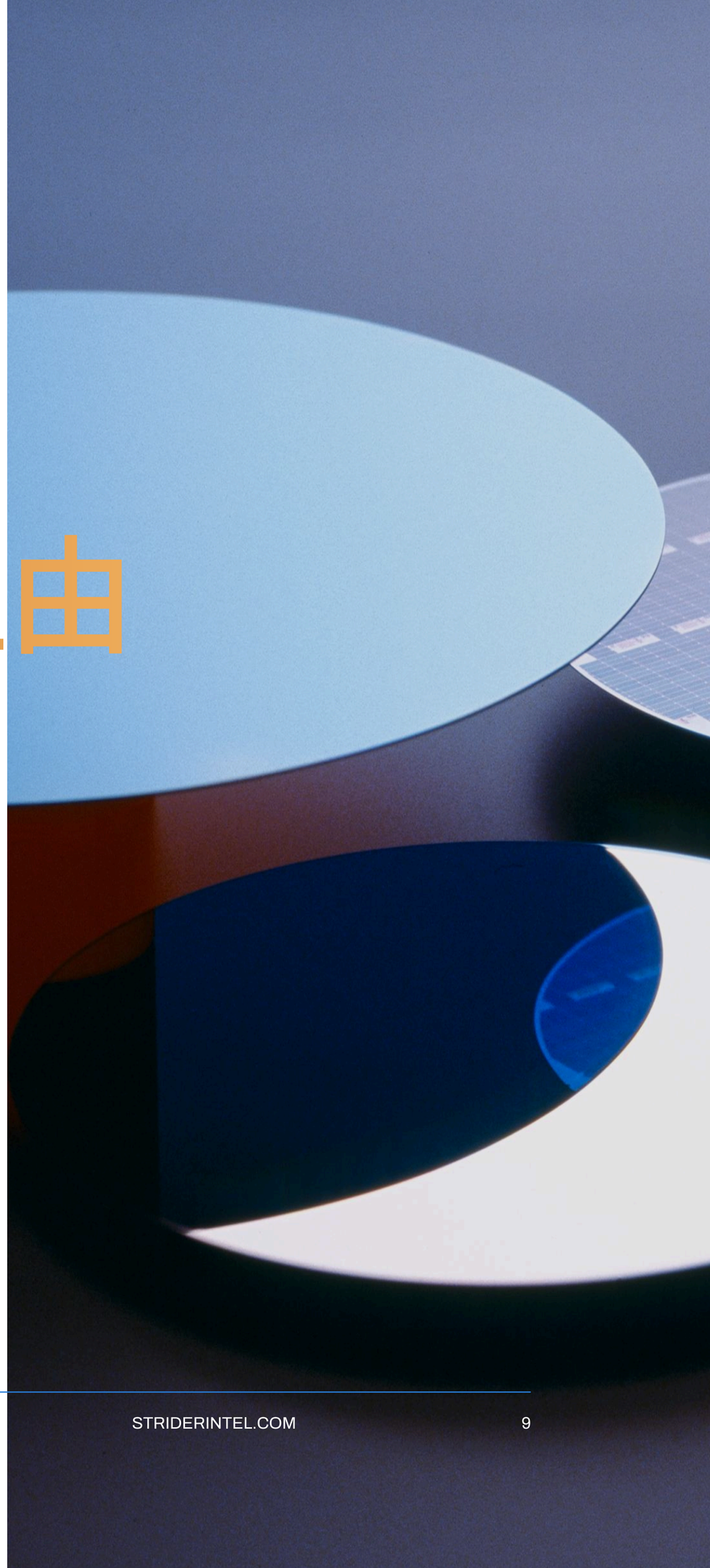


企業にとって
この問題が重大な理由

製造、バイオ技術、ソフトウェア、防衛といったどの先進分野でもそこに属する企業はグローバルなイノベーション・エコシステムの一部を担っています。この相互接続性は発展を促進させるだけでなく、リスクももたらします。

他国にとっての利益が自社のサプライチェーン、パートナーシップ、従業員とどう交わるかを可視化しなければ、自社の競争優位性が漏出する恐れがあっても容易に見過ごしてしまいます。

見えないものを保護することはできません。
最初に行うべき防御策は、認識することです。



組織的なレジリエンスの構築

国家レベルのリスクからイノベーションを守るために必要なのは、扉を閉ざすことではなく、明確に把握することです。組織の意思決定に戦略的インテリジェンスを組み込むと損失が生じる前に脆弱な部分を特定できるようになります。

主なステップ：

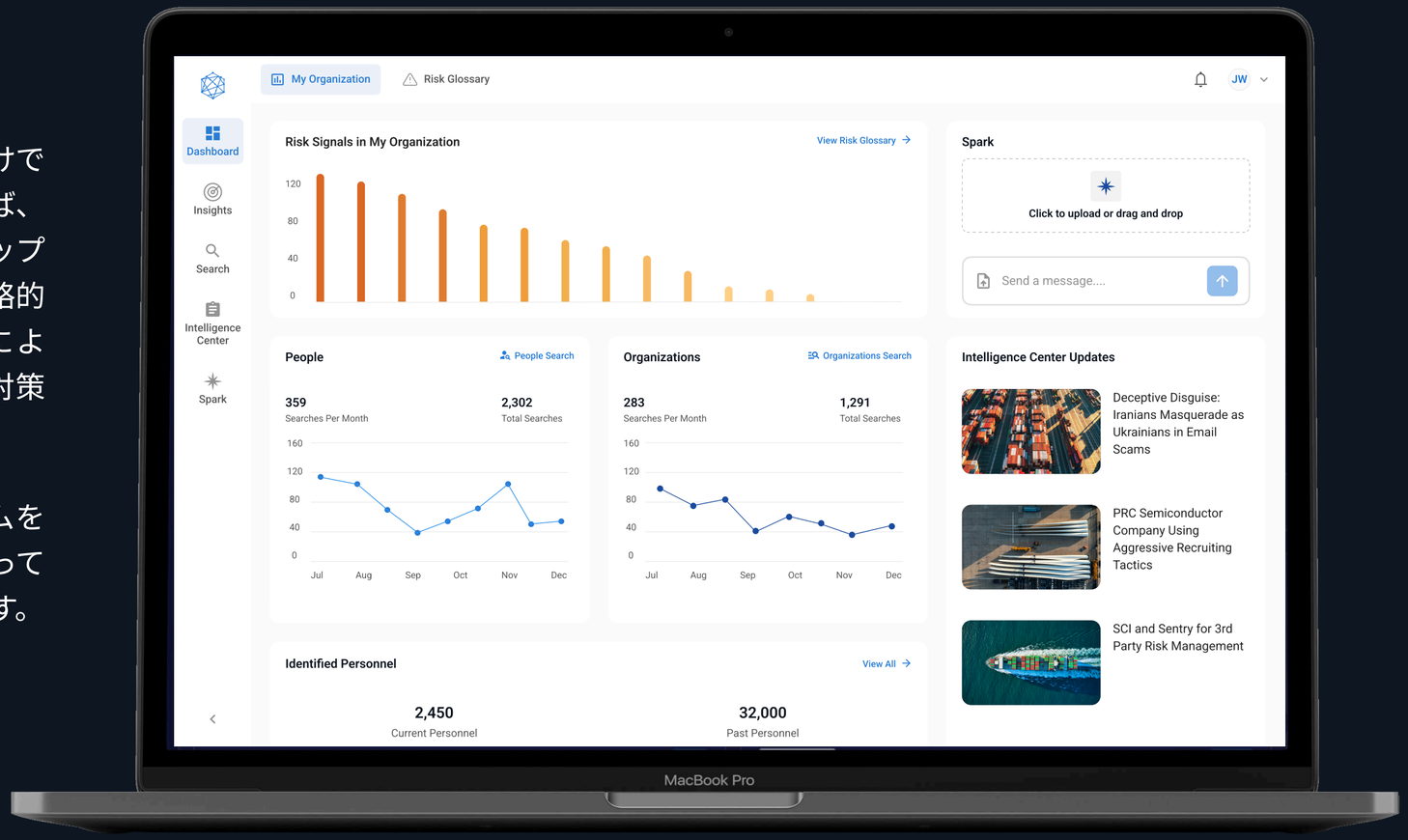
- 人材、技術、パートナーシップにおけるリスクを評価
- オープンソースや独自のインテリジェンスを用いてリスクを監視
- 人材採用時やデータ共有時の危険信号についてチームを教育
- セキュリティ部門、法務部門、執行部門間で協力し、戦略のすり合わせ

正しい情報を得ることで、組織のセキュリティが事後対応型から事前対応型に変わります。

自社の優位性を守る
インテリジェンス

グローバルな技術競争に勝つには、イノベーションだけでなくインテリジェンスも必要です。Striderを利用すれば、グローバルな人材、サプライチェーン、パートナーシップにわたる目に見えない国家レベルのリスクを暴く、戦略的インテリジェンスを備えることができます。これにより、社内のリーダーが自信を持って、先を見越した対策を取ることができるようになります。

Striderの戦略的インテリジェンス・プラットフォームをご覧いただくと、AIを活用したインテリジェンスによって国家レベルのリスクを特定・低減する方法がわかります。



Striderの戦略的インテリジェンス・プラットフォームをご覧ください
striderintel.com/strategic-intelligence/

STRIDER