半導体企業を支援するStrider

イノベーション、コンプライアンス、半導体チップのグローバル・サプライチェーンを国家主体の脅威から守ります

概要

半導体企業は技術力と経済力の中枢で事業を展開しています。装置や材料から設計、製造まで、チップ・エコシステムのあらゆる領域が、自国内の製造能力の促進や輸出規制の回避をもくろむ国家支援型アクターの標的になっています。

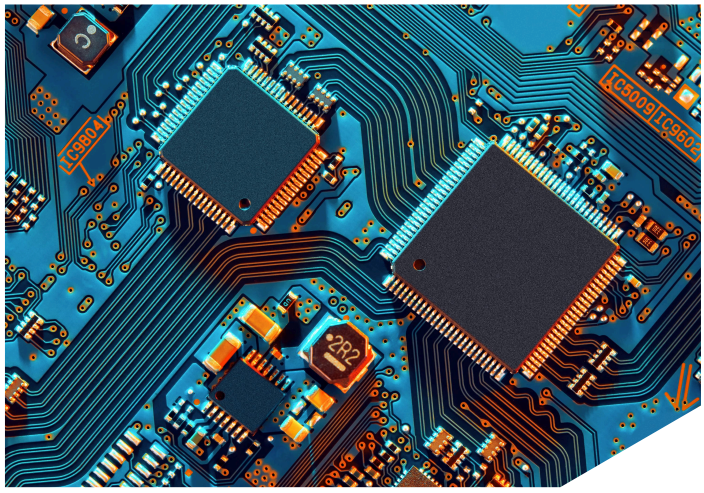
地政学的な圧力が強まる中、半導体業界のリーダーは、中核となる研究開発、人材、サプライヤー・ネットワークを守ると同時に、CHIPSおよび科学法、米国商務省産業安全保障局（BIS）の輸出規則、外国による所有権、管理又は影響（FOCI）に関する規制などの厳格なコンプライアンス基準を満たすことを求められています。

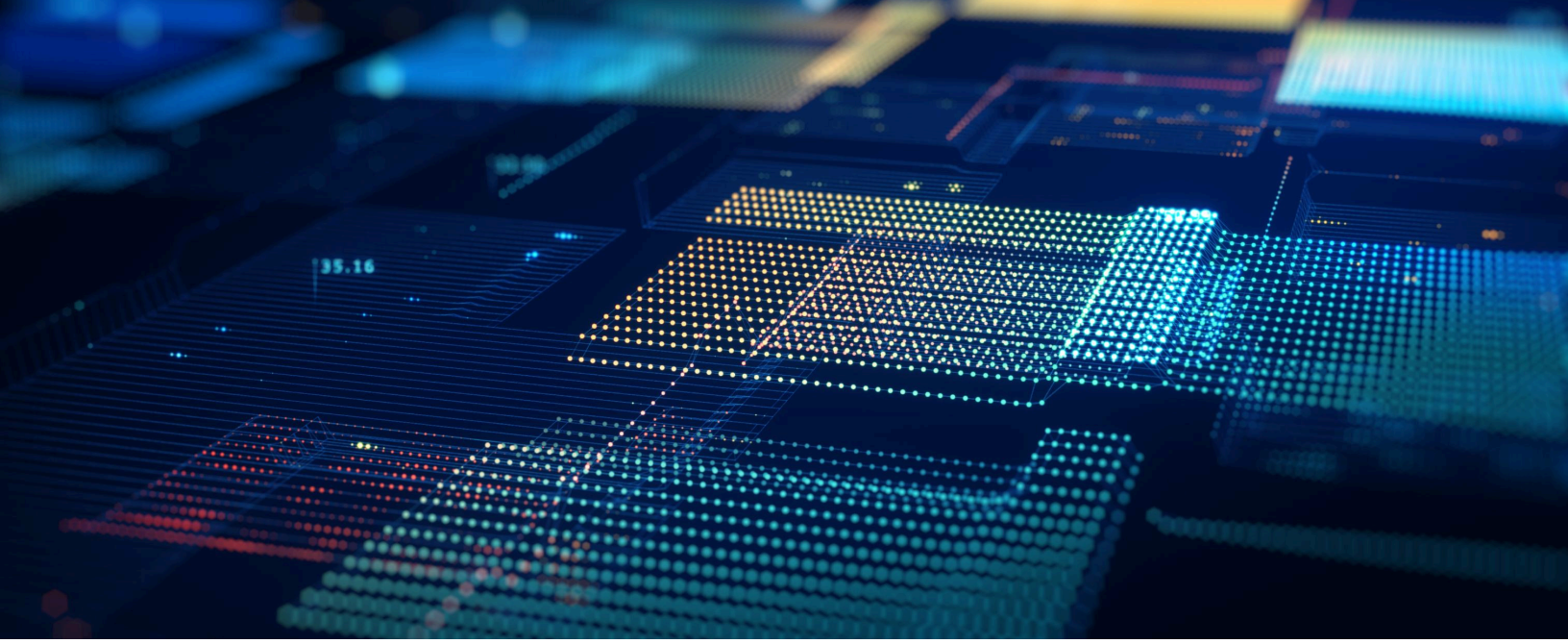
Striderの戦略的インテリジェンス・プラットフォームは、人々、企業、テクノロジーに影響を与える国家主体のリスクを可視化し、半導体企業による知的財産の保護、コンプライアンスの維持、サプライチェーンのレジリエンスの強化を支援します。

半導体業界のリーダーはStriderで次のことが可能になります。

- 従業員と請負業者に対してスクリーニングと継続的な審査を行い、隠れた関係性、虚偽の経歴、内部リスクがないかを確認します。
- サプライヤーのグローバル・ネットワークをマッピングおよび監視し、隠れた所有関係、フロント企業、FOCIリスクを検出します。
- 外国人材獲得プログラムの対象となる、価値の高い技術や専門人材を特定して保護します。
- 外部からの敵対的な接触や悪意のある通信を検出、ブロックして、機密性の高いプログラムに侵入しないようにします。
- 規制当局や投資家に対して、監査可能なインテリジェンスを通じて積極的なデュー・デリジェンスを行います。

Striderを使用すると、半導体企業は、事業の根幹を支えるプログラムの保護、国家安全保障上の規制の遵守、確信を持ったイノベーションの推進を、運用上のセキュリティを最高水準で保ちながら実現できます。





危険にさらされているもの

最近のインシデントは、内部脅威、知的財産窃盗、輸出規制違反がいかにして半導体分野のイノベーションや国家安全保障上の目標を危険にさらすことになるかを示しています。

- **TSMCへの輸出規制調査（2025年）[1,2,3]:** 製造したチップがHuaweiのAIプロセッサに搭載されていた疑いがあるとして、台湾積体電路製造（TSMC）が米国の調査を受けています。違反が認められた場合、10億ドル超の罰金が科せられる可能性があります。
- **NVIDIA製GPUの中国への迂回輸出（2025年）[4,5]:** 規制対象のNVIDIA製AIチップが、シンガポールとマレーシアの仲介機関を介して中国に不正に迂回輸出されていたケースは、グローバル物流ネットワークの脆弱性を露呈しました。
- **Micronのスパイ活動のケース（米国司法省、2018年）[6,7]:** MicronのDRAM製造に関する企業秘密の窃取を共謀したとして、米国司法省は中国の国営企業と台湾企業を起訴しました。このケースは、半導体分野の知的財産が恒常的にさらされているリスクを浮き彫りにしました。

ファブから設計会社、装置メーカーに至るまでの半導体サプライチェーンの複雑さが、悪用を可能にする数多くの侵入口を生み出しています。たった一つ弱点があるだけで、コンプライアンス、知的財産、長期的な優位性の喪失につながる可能性があるのです。

対応を怠った場合には次のことが起こる可能性があります。

- **知的財産の窃取と開発研究成果の流出：**独自のチップ設計、処理技術、EDAソフトウェアが内部アクセスやスパイ活動を通じて流出します。
- **規制上のリスクおよび法的リスク：**CHIPS法のガードレール、BIS輸出規制、ITAR規制の違反は、罰金、契約の停止、資格はく奪につながります。
- **サプライチェーンの侵害：** 隠れた所有関係や規制対象組織とつながりのあるサードパーティ・サプライヤーに起因して、コンプライアンス・リスクの連鎖が生じます。
- **業務の混乱：** 信頼できるサプライヤーの喪失や部品調達の制限により、製造の継続性が脅かされます。
- **信頼の低下：** 安全性とコンプライアンスが確保された運用を前提とする顧客、パートナー企業、規制当局の信用失墜につながります。

[1] https://jeffnewmanlaw.com/tsmc-faces-potential-fine-over-1-billion-for-violating-export-control-regs-for-selling-chips-to-chinese-companies/
[2] https://www.investopedia.com/tsmc-could-face-usd1b-us-fine-for-violating-export-control-rules-report-says-11711445
[3] https://techcrunch.com/2025/04/09/us-may-fine-tsmc-1b-over-chip-allegedly-used-in-huawei-ai-processor/
[4] https://techwireasia.com/2025/03/nvidia-chip-crackdown-malaysia-under-us-pressure-to-stop-ai-reaching-china/
[5] https://www.channelnewsasia.com/singapore/nvidia-chips-probe-singapore-malaysia-export-restrictions-shanmugam-4972321
[6] https://www.crowell.com/en/insights/client-alerts/u-s-charges-chinese-and-taiwanese-companies-with-trade-secret-theft-continues-vigilant-prosecution-of-chinese-economic-espionage
[7] https://www.justice.gov/usao-ndca/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage

半導体企業を支援するためのStriderの機能

機能	どのように役立つか	Strider製品の活用例
従業員と請負業者の継続的な審査	資格・経歴の確認と隠れた関係性の可視化を通じて内部リスクとコンプライアンス違反を未然に防ぎます。	**People Searchおよび改ざんされた履歴書のスクリーニング** ATSシステムまたはHRシステムと統合して、身元詐称や高リスクの関係性を雇用前に検出します。
サプライチェーンの完全性および輸出コンプライアンス	サプライヤー各層と投資家全体を対象に、隠れた所有関係、フロント企業、制裁リスクを明らかにします。	**Organizations Search** グローバル規模での経済的、人的なつながりをマッピングしてデューデリジェンスを強化し、CHIPS ActおよびBISへのコンプライアンスを確保します。
基幹技術および専門人材の保護	どの技術または内容領域専門家が外国のプログラムの標的になっているのかを特定します。	**Insights（「Technologies」タブ）：** 標的になっている技術と専門人材を正確に特定して、保護措置やリスク回避のための指導の優先順位を決定します。
通信の安全性確保と脅威の監視	国家とつながりのある情報収集主体や勧誘主体からの悪意のある接触を検出、監視します。	**Shield** 厳選された脅威インテリジェンス・データをSIEM/DLPツールに統合して、悪意のある通信に警告を出し監視します。
AIを活用したリスク分析	人材、組織、技術全体での調査の加速とインテリジェンスの統合を可能にします。	**Spark** StriderのAIエンジンを使用して、従業員、サプライヤー、研究開発エコシステム全体でインサイトを迅速に獲得します。

サプライチェーンとイノベーションを守る準備はできましたか？

ぜひデモをご予約ください。Striderの戦略的インテリジェンス・プラットフォームが、半導体企業による知的財産の保護、輸出管理コンプライアンスの維持、グローバル・チップ・エコシステム全体でのレジリエンスの確保をどのように支援するかをご紹介します。

デモを申し込む →