エネルギー産業を支援するStrider

発電と電力網の安定性を国家主体の脅威から守ります

概要

Striderは業界最高水準の戦略的インテリジェンス・プラットフォームを提供し、国家主体のリスクの特定と軽減を支援します。オープンソースのデータとStrider独自のリスク評価方法を組み合わせることで、企業の事業や評判を損なう可能性のある隠れた脅威を明らかにします。

エネルギー分野の企業はStriderで次のことが可能になります。

- 電力網の中核を成す要素（変圧器、インバーター、光ファイバー・ケーブルなど）のサプライヤーを精査して隠れた所有関係や国家とのつながりが無いかを確認します。
- 機密性の高い職務（システム・アクセス管理者など）の従業員および採用候補者を、業務ネットワークへのアクセス権を付与する前にスクリーニングし監視します。
- 再生可能エネルギー、原子力、従来型の発電サプライチェーンのリスクを特定し軽減します。

Striderを使用してサプライチェーンと人材の情報を一つのプラットフォームで統合することで、エネルギー産業のリーダーは、効率性もコンプライアンスも犠牲にすることなく、事業の継続性と電力網の安全性を維持できます。

危険にさらされているもの

エネルギー供給網の完全性は、構成部品、接続、人といったそこに関わるすべての要素にかかっていますが、攻撃者もそれを知っています。最近のインシデントから、海外製のハードウェアや不正に関与している人員がいかにして重大な脆弱性を引き起こす可能性をはらんでいるかが分かります。

- **「ゴースト・マシン」に関する調査（2025年）** – 中国製インバーターを調査したところ、主要な通信装置に関して資料に未記載のものがあることが判明しました。こうした透明性の欠如は、潜在的な脆弱性が悪用され電力網の運用に混乱が引き起こされる懸念を提起しました。[1]
- **サイバー手段によるノルウェーのダムへの妨害行為（2025年）** – ロシアが関与するサイバー攻撃によってノルウェーのブレマンガーにある水力発電ダムが一時的に乗っ取られました。ハッカーは水門を開け、毎秒500リットルの水を4時間にわたって流出させました。このケースは、国家支援型行為者がエネルギー・インフラを標的にしている実態を浮き彫りにしています。[2]
- **華鋭風電が関与した風力タービンのケース（2018）** – 中国の風力タービン・メーカーが米国の占有制御ソフトウェアを盗み出したことで、再生可能エネルギーの大手企業の弱体化につながりました。この盗用によって何百人もが職を失い、また、経済的損失も甚大でした。このケースは、技術窃取が与える長期的な影響を明確に示しています。[3]

例えば韓国のサプライヤーであれ、テネシー州のエンジニアであれ、たった一つの弱点があるだけで電力網全体を外国勢力が悪用できる状態に陥れることができるのです。

[1] https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/?
[2] https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
[3] https://www.justice.gov/archives/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets#:~:text=The%20Court%20found%20that%20AMSC's,on%20Sinovel%20Wind%20Group%20LLC.

対策を怠った場合には次のことが起こる可能性があります。

- **電力網の混乱や停電：**遠隔停止機能を備えたインバーターなどの部品の侵害を通じて発生します。
- **規制当局による罰金や法的措置：**敵対勢力とつながりのある企業からの調達を制限するテキサス州のSB 17やFARA型の法案に基づいて科されます。
- **社会的信用の低下：**基幹インフラが国家主体の影響にさらされることで生じます。
- **知的財産および業務データの窃取：**原子力、再生可能エネルギー、送電網の運用に関わる専門人材をターゲットにした勧誘を通じて行われます。

エネルギー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
電力網運用の保護	国家支援型行為者が狙う、危険にさらされている技術、侵害されたコンポーネント、攻撃を受けやすい人員を特定することで、発電、送電、制御を支えるシステムを保全します。	**Insights** 狙われている技術や専門人材を追跡します。 **People Search** 採用者に国民国家とのつながりや虚偽の経歴・資格がないか精査します。
サプライチェーンの安全性の確保	隠れた所有関係や、基幹サプライヤー（変圧器、インバーター、ケーブルなど）と国家主体の組織とのつながりを明らかにします。	**Organizations Search** サプライヤーと親会社のつながりをマッピングします。 **Shield** リスクのあるドメインや通信がシステムに到達する前に警告を出します。
コンプライアンスのサポート	州および連邦のコンプライアンス規制に対応し、調達と人員の審査におけるデュー・デリジェンスを証明します。	**Organizations Search** サプライヤーをスクリーニングして、テキサス州のSB 17やFARA型の法案などの規制に対応します。 **People Search** 従業員や請負業者を事前スクリーニングして内部からのリスクを排除します。

貴社の電力網と基幹業務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People Search、Organizations Search、Shieldが、サプライヤーの精査、機密性の高い職務に就く人材のスクリーニング、変化する規制へのコンプライアンスの確保などを通じて、どのように最前線での防御を強化できるのかをご紹介します。

デモを申し込む →