STRIDER

効果的な
経済安全保障プログラム
の構築

国家支援型リスクに先手を打つための3つの柱

目次

P.05

効果的な経済安全保障
プログラムの3つの柱

P.06

1つ目の柱

環境：内部リスク環境と
外部リスク環境の理解

P.10

2つ目の柱

戦略：事後対応から
事前対策へ

P.12

3つ目の柱

教育：
コミュニケーションが
信頼を育む

P.16

Striderの
製品ラインナップ

P.18

ケース・スタディ

効果的な経済安全保障
プログラムの実践

経済安全保障プログラムとは

経済安全保障プログラムとは、国家支援行為者から組織の経済的利益を守り、それによって組織のセキュリティと競争力を同時に強化する取り組みです。

経済安全保障は、データ分析や専門家（SME）の知見、多彩なツールを駆使して戦略的目標を達成する組織の包括的なセキュリティ戦略の要です。

Striderの経済安全保障プログラムの主要な目標は、意思決定者が十分な情報に基づいた選択を行い、潜在的な安全保障上の課題を予測・軽減し、リソース"配分を最適化できるようにすることです。

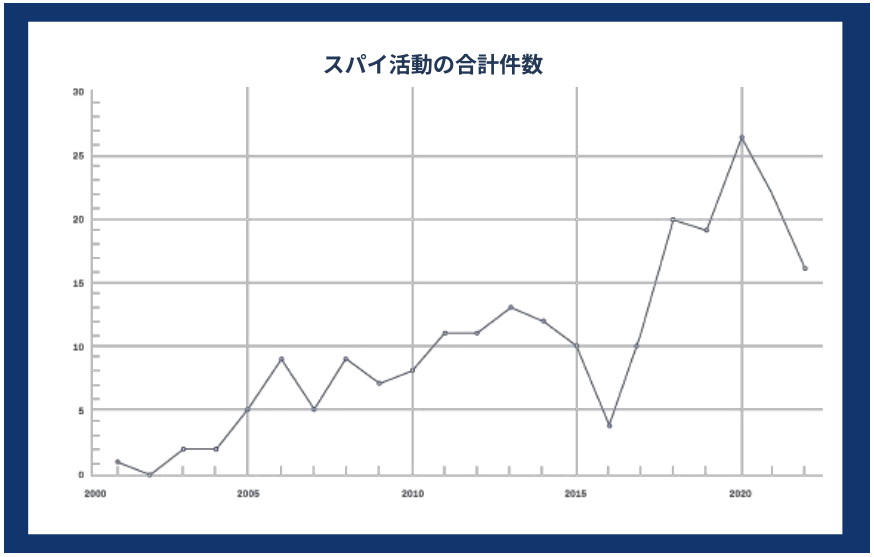
国家支援型リスクの現況

国家支援行為者とは、自国の戦略的利益を促進する目的で悪意ある活動を行う人物のことです。多くの場合、彼らは豊富なリソース、専門知識、ツールを自由に使えるため、標的を絞った高度な活動を行うことができます。

これまでも外国政府や国家支援行為者は、技術力や軍事力の拡大に役立つ情報を得るために戦術を駆使してきました。昨今、その実行方法がこれまでとは違ってきています。

以前は、国家支援行為者は、政府間レベルで機密情報を収集することに重点を置いていました。現在は、グローバル経済を利用して戦略的優位性を高めることに注力していることもわかっています。彼らは特に、人工知能（AI）、量子科学、半導体製造、バイオ医薬品、その他の技術産業などの破壊的技術に関心を持っています。これらのうち、いずれかの分野において業界リーダーとなることは、国家支援行為者の自国にグローバルな経済的優位性をもたらします。

この地政学的競争の時代にあって、多くの組織が国家によって知的財産が盗まれる危険にさらされています。



上のグラフは、中国によるスパイ活動インシデントのうち、公に報告された件数を経時的に示しています。特に興味深いのは、2015年にオバマ大統領と習近平国家主席が政府機関による商業スパイ活動制限に合意した後、スパイ活動の件数が大幅に減少している点です。ただし、この減少傾向は合意から1年以内に反転しました[1]。

効果的な経済安全保障プログラムの3つの柱

組織ごとに経済安全保障への対応レベルには差があります。現在どのレベルにあるとしても、多くの組織は段階的なアプローチを採用することで成功を収めています。小さいながらも狙いを定めた施策を積み重ねることで、セキュリティ・チームは強固なセキュリティ・プログラムを着実に構築できます。このような仕組みにより、組織は持続可能な保護の基盤を築きながら、進化する脅威に適応できます。

内部脅威プログラムを構築する場合、環境、戦略、教育の3つの柱に焦点を当てる必要があります。

1. **環境：**経済安全保障リスクに専任で取り組むチームは、外部と内部両方のリスク環境、とりわけ自社の技術に関連するリスクを理解している必要があります。

2. **戦略：**セキュリティ・チームは、関連するリスクを検知し、軽減できるよう、予防的な戦略を策定する必要があります。

3. **教育：**セキュリティ・チームは、国家支援型リスクに対する従業員の意識を高めるため、有意義な教育を提供する必要があります。

以降のセクションでは、3つの柱のそれぞれについて、組織の成熟度を評価する方法と、次に取るべきステップを見極めるための具体的な方法を紹介していきます。

1つ目の柱

環境

内部リスク環境と外部リスク環境の理解

予防的なセキュリティ対応を構築するための第一歩は、状況の把握です。組織のセキュリティを効果的に守るためには、外国勢力がどのような情報を求めているかという外部の理解と、国家支援行為者が自分の組織の技術や人材をどのように標的にしているかという内部の理解の両方が必要になります。

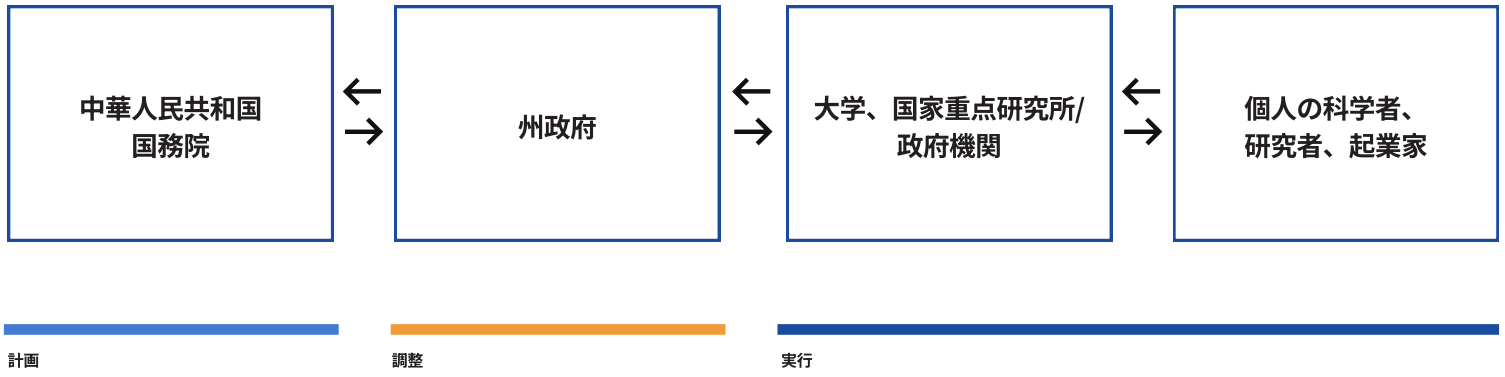
外部脅威状況

外国政府は、目的の技術を得るために、経済的国家戦略や国家支援行為者を用いた体系的なアプローチを採用することがよくあります。このような多面的な戦略には、中央政府と地方政府が共同で関与し、技術的目標の推進を目的としたインセンティブプログラムも組み込まれているのが一般的です。

外国政府がどの技術に関心を持っているかを先回りして把握するには、外国政府の戦略計画、経済目標、経済的国家戦略に関する政策が参考になります。

Striderの製品であるRangerでは、このような情報が直感的に理解しやすいダッシュボードに表示され、自社のイノベーション領域とどのように重なっているかを把握できます。

中国に関する外部脅威状況



内部脅威状況

セキュリティ・チームにとって最大の課題の1つは、リソースをどこに重点的に配分すべきかを見極めることです。そのためには、まず組織の「クラウン・ジュエル（王冠の宝石）」と言える、最も重要な知的財産（IP）と技術を特定することが必要です。次に、国家支援行為者が収集対象としている知的財産を把握します。この2つの領域が重なる部分こそ、セキュリティ・チームの対応を重点的に配分するべき領域となります。

「組織の『クラウン・ジュエル』とは、盗まれたり破壊されたりした場合に、組織に重大な損害を与え、場合によっては組織を崩壊させてしまうような情報やリソースを指します。これらは多くの場合、外部勢力や外国の敵対勢力が最も求めている資料でもあります。このようなクラウン・ジュエルを特定することで、対象の資産にアクセスできるすべての従業員が敵対勢力の標的となり得る可能性を具体的なイメージとして把握できるようになります。この一般的なリスク管理手法により、従業員の意識向上施策の重点領域が明確化されるとともに、内部脅威プログラムの分析活動のカスタマイズにも役立ちます」

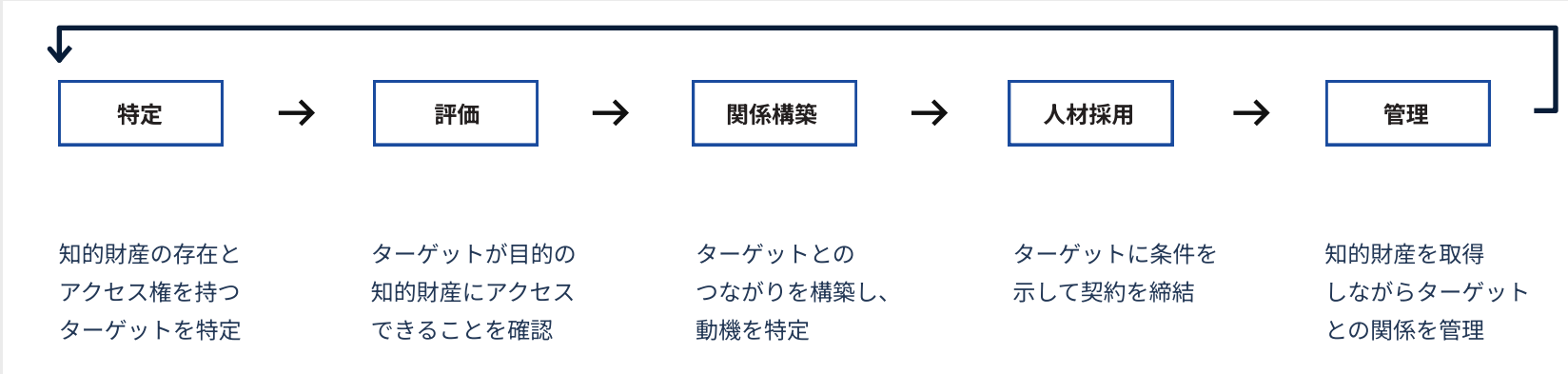
米国国家防諜安全保障センター

主要な知的財産や技術を特定することに加え、国家支援行為者の手口や人材採用サイクルを知っておくことも組織のリスクを特定する上できわめて重要となります。

サイクルの各部分で、関係構築の小さな手がかりが残されます。組織の中にあるこのような部分を突き止めることができれば、どの人材が最も標的にされやすいか、また、すでに悪意のある行為者が接触している可能性のある人材を特定する助けになります。

Strider製品のRangerは、オープンソースのインテリジェンスのみを使用して、最も標的にされるリスクの高い人材に関する補足情報を提供できます。この情報により、既存の経済安全保障ソリューションが補完され、調査において重要なコンテキストがもたらされます。

国家支援行為者の人材採用サイクル



2つ目の柱

戦略

事後対応から事前対策へ

数多くの潜在的リスクに常に注意を払う必要がある中で、セキュリティ対応はつい事後対応的になってしまいがちです。そのような状況では、セキュリティ・チームは各インシデントに対して暫定的なアプローチを取り、その場その場で発生するインシデントに個別に対応していくことになります。こうした対応は、その業務量の多さから有効に機能しているように感じられるかもしれませんが、包括的なアプローチを取り、予防的なセキュリティ態勢を構築することで、組織の成果は格段に向上させることができます。

防御可能で再現性のあるプロセス

セキュリティ・チームがすべてを防御することはまず不可能です。前のセクションでは、組織の知的財産および技術に優先順位を付け、最もリスクが高いものにリソースを重点的に配分し、国家支援型攻撃を効果的に監視できるようにする方法について説明しました。

優先順位を明確にすることで、その知的財産と技術の安全性を守るために必要な防御可能かつ再現性のあるプロセスを構築できるようになります。防御可能で再現性のあるプロセスは、効果的な経済安全保障プログラムに欠かせない要素です。このようなプロセスを構築することで、以下のような利点が得られます。

一貫性：防御可能で再現性のあるプロセスがあれば、異なる状況下でも、一貫して同じ手順を適用できます。この一貫性により、セキュリティ・チームがアドホック的な対応を取った場合に起こりがちなミス、漏れ、見落としを減らすことができます。

効率性：しっかりとしたガイドラインと手順を決めておくことで、チーム・メンバーはより迅速に、自信を持って対応できるようになり、経済安全保障上の問題に対応する時間と労力を削減できます。

正確性：再現性の高いプロセスには、明確な文書化も定められていることが多いため、実施した手順の追跡や検証が容易になります。この文書化により、経済的脆弱性を悪化させる可能性のあるミスや誤解が発生するリスクを低減できます。

予防的なセキュリティ対応を導入するには、プロセスの範囲と目的の特定、プロセスの各手順の文書化、役割と責任の定義、意思決定基準の設定、対象となる利害関係者の招集など、いくつもの重要なステップが必要になります。

3つ目の柱

教育

コミュニケーションが信頼を育む

従業員、利害関係者、経営幹部に対して慎重な形で教育を実施することで、自身や会社に不利益をもたらす可能性のある人間関係に巻き込まれないよう、賢明な判断を下せるようにすることができます。

何より、日常的にトレーニングを実施することで、組織内の信頼の風土を強化させることができます。信頼レベルの高い職場は、働きやすいだけでなく、リスク報告の水準も高まり、結果的に知的財産の保護につながります。

対象者特化型トレーニング

国家支援行為者の標的にされている重要技術や知的財産にアクセスできる従業員を特定しましょう。 対象者に対して、特別なセキュリティ・トレーニングを実施し、彼らが標的になっていることを明確に伝えます。国家支援行為者が用いる戦術や手法、手順を事前に知っていれば、実際に接触を受けたとき、その兆候に気づくことができます。

従業員トレーニング

セキュリティは全員の責任です。企業の全従業員に対して、何に注意を払うべきか、潜在的なリスクにどう対応すべきかを周知徹底しましょう。透明性の高いトレーニングにより、組織全体に信頼の風土を築くことができます。

経営幹部向けブリーフィング

強固な安全保障プログラムには、経営幹部の賛同が不可欠です。定期的にブリーフィングを実施することで、国家支援型リスク、企業のリスク許容度、信頼の文化、そして関連する情報発信方針に関する認識を利害関係者間で統一することが可能になります。効果的な経済安全保障プログラムの重要性を伝え強調することは、経済安全保障チームの役割です。

トレーニング後の分析

すべてのブリーフィングやトレーニングを実施した後は、効果測定のためにフォローアップのミーティングやアンケート調査を行うことがベストプラクティスとされています。従業員全体の潜在的リスクに対する意識は高まっているでしょうか？各ブリーフィングやトレーニングについて、結果を測定するための戦略を立てましょう。

懸念事項共有の窓口

報告システムが整備されていない場合、速やかに整備してください。少しでも懸念があれば報告することを常に奨励します。国家支援型の窃盗行為は、従業員の間で広く共有され、話題にされるべき対象です。

なぜスパイになるのか

アーシュラ・M・ワイルダー博士の論文『なぜスパイになるのか：スパイ活動の心理学』によれば、あらゆるスパイ活動には、以下の3つの共通点があることが分かっています。

1. **機能不全の人格** — 信頼を裏切る行為を正当化できる自我
2. **危機的状況**—リスクを取る必要があるという認識
3. **手近な機会** — やっても逃げ切れるという思い込み

これらの要因を考慮することで、内部調査をうまく進めることができます。

知的財産の窃盗は、機会、危機、人格の3つが交わるところで発生します。

オープンソースのインテリジェンスで安全保障プログラムをアップグレード

Striderは、リスク管理とビジネス競争力に特化したAIを活用したインテリジェンス企業です。オープンソースのデータのみを活用し、セキュリティ、人材獲得、サプライ・チェーン・リスク管理をはじめとするさまざまなチームに役立つ重要なコンテキストとインサイトを提供しています。

STRIDERの製品ラインナップ

Ranger

Rangerは、組織内に潜む国家支援型リスクの特定、可視化、対応を支援します。Strider独自のオープンソース手法を活用し、国家支援行為者の標的にされるリスクが最も高い技術と人材を特定するのに役立ちます。

Checkpoint

Checkpointを使用すると、サードパーティ・パートナーの候補を徹底的にスクリーニングし、制裁対象、制限対象の団体やその子会社（国有組織を含む）と関係がないか調査することができます。

Shield

Shieldは、Striderが提供する最高峰のメール・セキュリティ製品です。制裁対象、制限対象、または国有の団体から受信したメールをセキュリティ・チームがブロック、監視、調査できるようになります。

Sentry

Sentryは、人材、パートナー、協力者などの個人の国家支援型リスクとの潜在的なつながりを明らかにすることで、組織が安全に人材へのニーズを満たせるよう支援します。

サービス

Striderでは、一連のインテリジェンス製品に加え、オーダーメイドの実践的な安全保障開発サービスも提供しています。このサービスは、経済安全保障の取り組みをまだ立ち上げたばかり、または発展段階にある組織に対して、より成熟度の高い高度な取り組みへと引き上げることを目的としています。

現在の取り組みの成熟度にかかわらず、包括的な分析とインサイトに基づき、事後対応型から事前対策的なセキュリティ・プロトコルへと移行することができます。

ケース・スタディ

効果的な経済安全保障プログラムの実践

概要

Striderのあるクライアントは、Fortune 100に名を連ねるテクノロジー企業であり、きわめて競争が激しい革新的な業界で事業を展開しています。幅広い最先端技術と豊富な人材を擁する同社では、知的財産（IP）、技術、人材、サプライ・チェーンを国家支援型リスクから保護する必要性を認識しています。この目的を達成するため、同社はStriderの製品群、特にRangerを活用して、潜在的リスクを事前に特定し、重要な資産を保護しています。

事後対応より事前対策

国家支援行為者によって絶え間なく技術および人材を狙われるリスクに直面している同社は、事前対策的なセキュリティ対応を構築しようと考えました。その第一歩として、セキュリティ・チームは、最も脆弱な領域を戦略的に保護することから始めました。具体的には、国家支援行為者によって積極的に狙われている技術を特定し、その分野の専門知識を持つ従業員を守ることにしました。.

このような分野を特定するため、同社はStriderのRangerを活用しました。Strider製品のオープンソース・インテリジェンスにより、セキュリティ・チームは、最も狙われやすい技術についての重要な知見を即座に得ることができ、国家支援行為者から接触を受ける可能性が高い貴重な知識を持つ従業員を特定できました。

同社は、Striderのインテリジェンス・チームや当該分野についての専門家（SME）と連携しながら、事前対策型の安全保障戦略を設計し、実施しました。

対象となる従業員に対しては、国家支援行為者がよく用いる戦術、技術、手法を見破るための知識を習得するための包括的なトレーニングを提供しました。いざ国家支援行為者からの接触を受けた場合に有効な対応が取れるように従業員に備えさせました。

採用の企てを見破る

事前対策型トレーニングを実施してわずか2週間後、ある従業員が、国家支援行為者からのメッセージをLinkedIn (ビジネスに特化した世界最大のソーシャル・ネットワーキング・サービス) 経由で受け取りました。その内容は、多額の報酬や好待遇と引き換えに海外の企業への転職を持ちかけるものでした。この従業員は標的型の国家支援型脅威であると認識し、インシデントをセキュリティ・チームに報告しました。

このメッセージを受け、同社はStriderと連携して送信者に関する追加調査を実施しました。Striderの調査により、その人物は外国政府が直接支援する企業に所属しており、同社と直接競合する意図を持っていたことが判明しました。

このインシデントは、同社の事前対策型のセキュリティ戦略の有効性とタイムリーな対応力を実証する結果となりました。StriderのRangerを活用し、従業員に必要な知識とツールを慎重かつ積極的に与えることで、同社は重要な人材を守ることに成功しました。

国家支援型リスクがますます増加し、官民双方に脅威をもたらしている今、経済安全保障プログラムを構築することは最も効果的な防御策となり得ます。

現在のプログラムの成熟度にかかわらず、リスク環境を深く理解し、事前対策型のセキュリティ・プロトコルに移行し、適切な教育とトレーニングを実施することは、チームの成功と組織の安全性を高める上できわめて重要です。

御社の安全保障プログラムの開発をさらに強化する方法について、Striderに今すぐお問い合わせください。

STRIDERINTEL.COM