地政学リスクが映す サイバーインテリジェンスの重要性

脅威を増すサイバー攻撃の動向、半導体分野への影響
企業がとるべき対応

PwCコンサルティング合同会社

地政学リスクとサイバー空間の脅威を別々に捉えていては、適切な経営判断を下せません。本稿では、経営に必要なインテリジェンスの本質、国・地域間の力学がサイバー空間へ及ぼす影響などについて考察し、サイバー攻撃のリスクに対する処方箋を探ります。

脅威を増すサイバー攻撃の動向、半導体分野への影響、企業がとるべき対応

地政学リスクが収まる気配はありません。ロシアによるウクライナ侵攻は1年以上たっても解決の糸口が見えず、台湾海峡を巡る米中のさや当てや北朝鮮のミサイル問題など東アジア情勢の緊迫度も高まっています。東西冷戦の終結から約30年たった今、米欧日を軸にする民主主義陣営、中露に代表される権威主義陣営、どちらにもはっきりとくみしない第三勢力が混在する「曖昧な新冷戦」時代を迎えています。

国・地域間の争いは実空間だけにとどまりません。デジタルの技術革新も加わり、今やサイバー空間が新たな争いの舞台となっています。姿かたちを変えるサイバー攻撃によって、政府や民間企業の機密情報、重要インフラは日々、脅威にさらされています。サイバーリスクは従来の常識では捉えられず、企業は日々より高度な対応に迫られています。

今後、注目されるのは半導体関連業界への影響です。半導体はあらゆる産業の基盤です。半導体の関連業界がサイバー攻撃を受ければ、網の目のように広がるサプライチェーンだけでなく、社会インフラそのものも止まりかねず、経済活動に甚大な影響を及ぼしかねません。

地政学リスクとサイバー空間の脅威を別々に捉えていては、もはや適切な経営判断を下せない時代になりました。地政学的な戦略意図を達成するためにサイバー攻撃が活用されていることに加え、サイバー空間における攻撃手段があるからこそ、その封じ込めや多面的な対応のために新たな政策や規制が生み出されています。いまや両者は相互の在り方を変容させる重要ファクターとして深く結びついています。そのため、地政学とサイバーのインテリジェンスを高め、成功事例を蓄積することで「統合知」として経営戦略に生かす必要性が高まっています。本レポートでは、経営に必要なインテリジェンスの本質、国・地域間の力学の変化によって生じるサイバー空間への影響、それらに伴いグローバルや日本の半導体関連産業に起き得るリスク、企業がとるべき備えや対応策などについて包括的に考察し、サイバー攻撃のリスクに対する処方箋を探ります。

地政学リスクとサイバー空間の脅威を別々に捉えていては、適切な経営判断を下せません。本稿では、経営に必要なインテリジェンスの本質、国・地域間の力学がサイバー空間へ及ぼす影響などについて考察し、サイバー攻撃のリスクに対する処方箋を探ります。

pwc

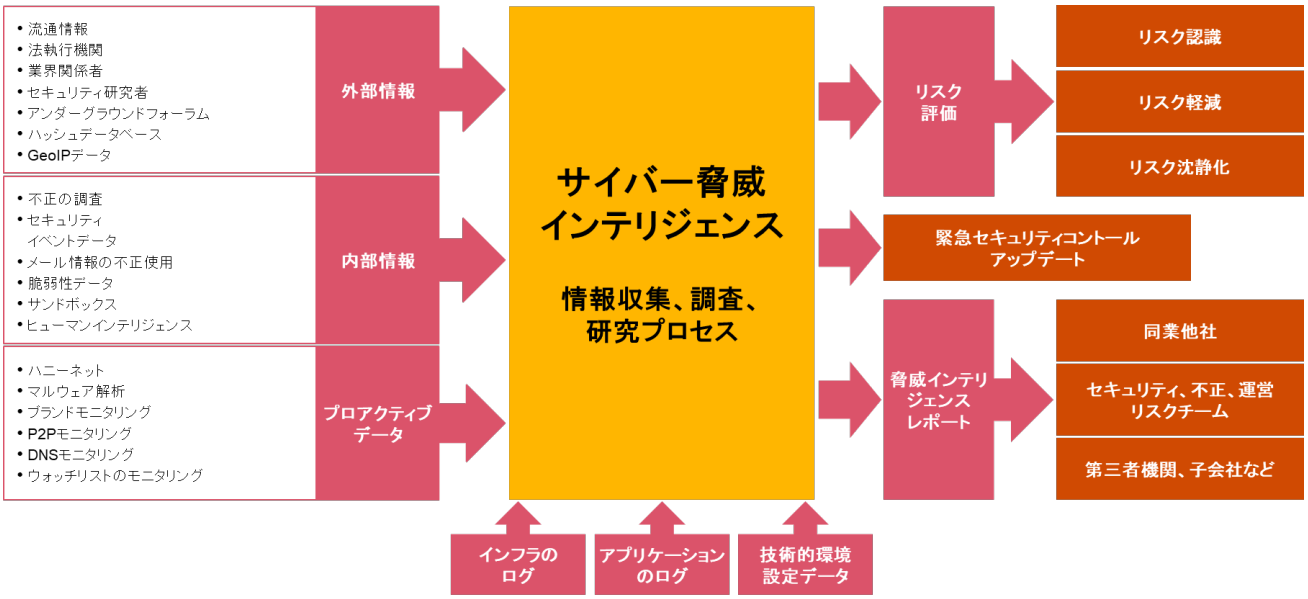
1. 企業経営に欠かせない「インテリジェンス」の本質

外部環境が変わり続ける中、変化の芽を事前に察知し、近い将来に取るべき最適な行動を探る能力（インテリジェンス）を磨くことが企業経営には欠かせません。国・地域間の力学争いに伴う安全保障の分野では、従来インテリジェンス主導のアプローチが最も有効な手段として受け入れられてきました。インテリジェンスがなければ直面する脅威を理解できず、効果的な運用能力を損なう可能性が高まるためです。

「防衛する前に脅威を理解する」という原則はサイバーセキュリティにも当てはまります。自社の業務環境からさまざまなデータを集め、処理と抽出を重ねて必要な情報を得る。それらを分析し、経営判断に生かせるような報告につなげる――。複数の行程をしっかり踏むことでインテリジェンスを醸成できるのです。そのためには、脅威、脆弱性、影響の3つの要素の組み合わせからリスクの種類を特定し、適切に評価したうえで優先順位を付けて対応する「リスクベースアプローチ」の徹底が欠かせません。

サイバー脅威インテリジェンスとは具体的にどのような構成をしているのでしょうか。収集すべき情報は非常に多岐にわたります。企業の外部および内部の情報のほか、マルウェア解析などプロアクティブなデータを集め、分析したうえでリスクを評価したり、報告書にまとめたりします。緊急度合いに応じてセキュリティコントロールを更新して対処することも求められます（図表1）。

図表1：サイバー脅威インテリジェンスの収集と分析



インテリジェンスを習得するには「自社のビジネスに関わるサイバー脅威のレベルと狙いを評価する」「対応するためのプログラムを作成して導入する」「監視と警告のレベルを高め、防衛体制を整える」「次世代技術を生かし、効果的なセキュリティ構造の計画、特定、実装を繰り返す」というサイクルを回すことが欠かせません。

一連の対応を企業内に根付かせるには相当の時間とリソースを要します。それでも、手遅れになるまで脅威に気付かないという事態は避けなければなりません。優先順位を付け、対策の網の目を徐々に小さくする。経営陣がインテリジェンスへの理解を深める。収集する情報の多様性を保つため、本社だけでなく事業会社などにも必要性を浸透させる――。こうした取り組みを着実にかつ素早く実践することが、インテリジェンスを磨く近道になります。

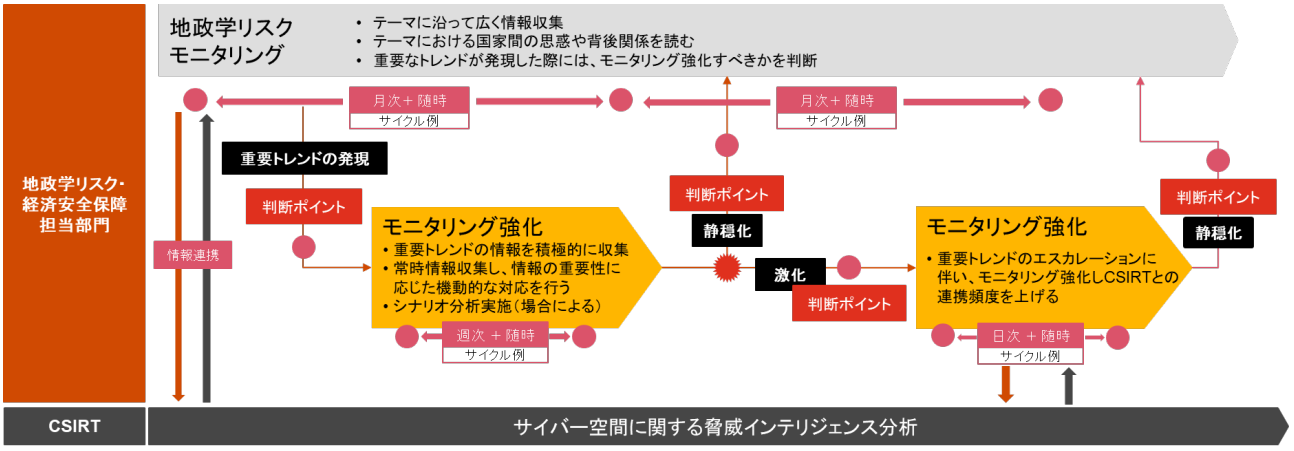
2. ひっ迫度が増す地政学リスクがサイバー空間に及ぼす影響

サイバーインテリジェンスはサイバー空間から得られる情報だけを対象にしていては意味を成しません。国・地域間の力学の変化という現実社会の動向もしっかり組み込まなければ、サイバー攻撃の脅威を抑え込むことは難しいでしょう。地政学とサイバーという2つのリスクへの対策を効果的にリンクさせ、相乗効果を高めることがますます重要になっています。

ロシアによるウクライナ侵攻では、ロシアに経済制裁を科した国などへのサイバー諜報活動が活発に行われている事実が浮き彫りになりました。国家間の争いとサイバー攻撃が密接に関わり合うのが現代のサイバー脅威の実態と言えます。そのため、国家の思惑に沿った脅威アクターの動きは、国際的な政治イベントとの関連性が高くなる傾向があります。選挙や国際会議、首脳会談などの大型イベントの時期をあらかじめ把握することは、備えの前提になるでしょう。

備えを手厚くするには企業内の連携が不可欠です（図表2）。地政学リスクや経済安全保障の担当部門が政治や規制、安保関連のイベントや情報を監視して今後起き得る展開や中長期的な地政学トレンドを分析する。CSIRT（Computer Security Incident Response Team）部門は、顕在化するサイバー攻撃者の動向や攻撃手法などの知見を積み上げる――。お互いに情報を連携してサイバー空間の脅威を精緻に分析することで、インテリジェンスの有効活用とセキュリティの体制整備を実現できるのです。

図表2：地政学リスクをモニタリングしてサイバーセキュリティに生かす



3. 世界で重要度が増す半導体業界に起こり得るリスク

地政学リスクとサイバー空間の脅威が複雑に絡まり合う中、注目度が高まっているのが半導体への影響です。あらゆるモノに使われる半導体の覇権を巡る争いは、米中対立における主要テーマにまで発展しています。対立が長期化し、激化すれば、日本の半導体産業、さらには日本経済への影響も一段と強まりかねません。日本企業には危機を「リスク」として備えるだけでなく、危機を「機会」に変える柔軟さも求められています。

まず、半導体産業の特性を見てみましょう。軍事・経済の戦略物資である半導体は、主要国の国策産業として国・地域の政策と密接に結びついています。世界に網の目のように広がるサプライチェーンも重要な点です。企画・設計、前工程、後工程ごとに多くの専業企業が関わり、地理的に偏在しています。地政学リスクの影響を受けやすい産業と言われる所以です。

米中対立がもたらす半導体産業への影響

次に地政学リスク、とりわけ米中対立による半導体産業のリスクシナリオを分析します。シナリオは大きく、①米国の規制が継続②米国による対中規制が加速③中国による台湾への軍事侵攻、の3つに分類できます。それぞれの影響について図表3にまとめました。

図表3：半導体産業からみた、3つのシナリオの影響

1 米国による対中先端半導体規制が継続	2 米国による対中規制のエスカレート	3 対立激化による中国による台湾軍事進攻
米国による対中半導体政策について、現状の先端半導体にフォーカスした現状が概ね据え置かれるシナリオ 中国にとっては事実上、台湾先端ファウンドリへのアクセスが断たれたままであるが、車載チップなどの自国内製造に係るグローバルサプライチェーンは概ね維持される	米国による対中規制において、中国の産業全般にわたる計算能力とその生産力を破壊する目的で非先端製品にまで範囲が拡大されるシナリオ 中国の半導体製造が台湾を中心としたグローバルサプライチェーンから分断され、中国国内で危機的な半導体不足が発生	中国による台湾武力侵攻が現実化することで、台湾の半導体生産が停止するシナリオ 中国により武力的に台湾ファウンドリが接収され、米国・同盟国のこれへのアクセスが断たれる

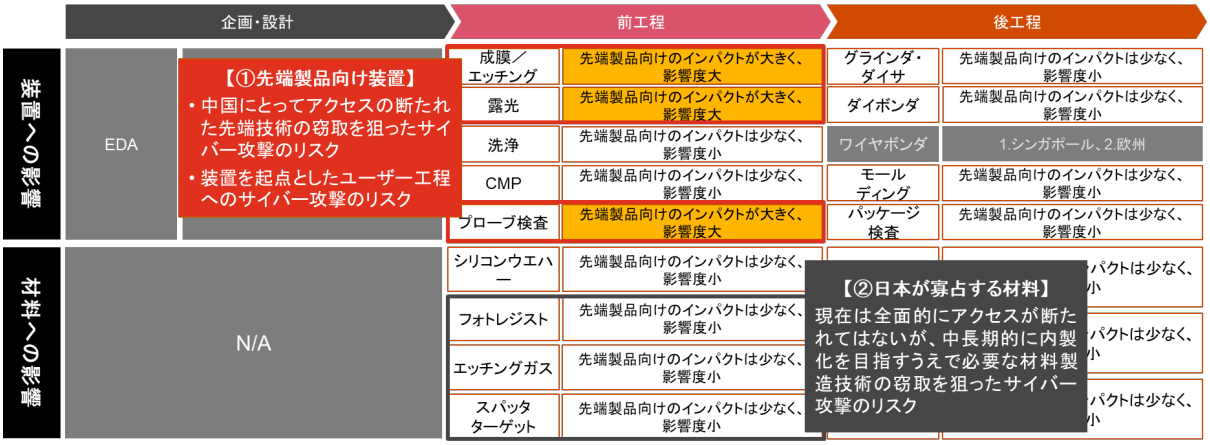
②や③は米中どちらに対しても甚大な損害をもたらすことから、合理的な意思決定とは言えません。日本が強みを持つ製造装置や材料への影響もはかり知れません。現状では①が最も蓋然性が高いと推測できます。ただ、国・地域間の衝突は経済合理性を無視して、一部の指導者の政治決定により起こり得るということも現実です。リスクはゼロではありません。事前の備えをいくつも施しておくことが、経営のレジリエンス（しなやかさ）とサイバー脅威への対応力につながります。

半導体サプライチェーンが直面するサイバー攻撃のリスクと影響

軍事・経済の戦略物資として半導体の存在感が日々強まるに伴い、半導体産業がサイバー攻撃を受けるリスクも高まっています。グローバルに広がるサプライチェーンにおけるサイバーリスクは「情報搾取」と「破壊」に大別できます。「情報搾取」については設計などの開発情報、装置オペレーションデータなどの製造情報、従業員の個人情報などが標的となります。「破壊」には装置破壊による生産拠点の操業妨害、企業活動の妨害などが挙げられ、企画・設計から前工程、後工程まで、幅広く狙われるリスクを抱えています。

日本が強みを持つ装置、材料についても、直面するリスクの種類は基本的には同じと言えます。ただし、組込ソフトウエアの脆弱性を狙うなど、装置を入口にしてユーザー企業への攻撃を狙う手口があり得る点に留意する必要があるでしょう。先端製品向け装置では成膜やエッチング、露光といった前工程、材料では特に日本のシェアが高いフォトレジスト、エッチングガス、スパッタターゲットの3分野でサイバー攻撃のリスクを受ける蓋然性が高まっています（図表4）。いずれも米中対立の行方、特に半導体の国産化を国を挙げて狙う中国の動向には注意が必要です。

図表4：日本の半導体産業へのサイバーリスク



さまざまなリスクが混在する半導体産業にとって、リスクを「危機」と捉えるだけでは、成長への階段を上ることはできません。内部のリソースが限られる中、外部の知見も活用して、業界横断でセキュリティレベルを高める取り組みを加速することも求められます。

半導体製造装置メーカーでは、工場向けのサイバーセキュリティソリューションを提供する動きが見られるようになりました。自動化やロボット化が進む半導体の製造工程では、制御ソフトウエアの脆弱性がそのままサイバーリスクに直結します。装置にあらかじめ対策を施し、セキュリティとセットで商材にすれば新たな市場の開拓だけでなく、業界全体のセキュリティ水準の底上げにもつながる可能性が高まります。リスクを新ビジネス創出の「機会」と位置づけ、攻めの経営に転じるきっかけにすることが自社のケイパビリティ獲得につながるのです。

4. 変化し続けるサイバー攻撃に企業はどう備え、対応するべきか

サイバー脅威アクターは日々、企業活動のあらゆる「穴」を狙っています。PwCの観測によると、2023年3月時点で特定・追跡中の脅威アクター数は296、このうち製造業を標的とするのは47、さらに日本国内の半導体企業を標的とするのは3に上ります。

攻撃対象となるセクターは半導体のほか、政府や宇宙、防衛、テクノロジー、金融など多岐にわたります。特に半導体では米国、日本、オランダ、台湾が主な標的になっていることも確認されました。一般的なランサムウェアに加え、中国を拠点とする「Red Djinn」「Red Kelpie」「Red Typhon」の3つの脅威アクターも特定されています。Red Kelpieは中国の中期政策大綱「5カ年計画」で重視する分野ごとに標的を変えています。それぞれのセクターごとに強みを持つ国・地域に照準をあてて攻撃をしていることがうかがえます（図表5）。

図表5：脅威アクターのプロファイル

	攻撃対象国	攻撃対象セクター	特徴
Red Djinn	米国、日本、香港、タイ、カンボジア、ミャンマー、台湾など	教育、金融、政府、テクノロジー	• 少なくとも2012年から活動 • 当初は台湾・香港の政府機関が標的 • 近年は日本を含むテクノロジー関連企業が標的
Red Kelpie	米国、英国、日本、韓国、オランダ、ドイツなど	航空、教育、金融、政府、ヘルスケア、製造業、メディア、通信、テクノロジー	• 5カ年計画に沿って標的が変化 • 初期はテクノロジー企業、現在は金融、政府などより幅広い組織が標的 • 独自の攻撃技術・マルウェア開発能力を保有
Red Typhon	米国、英国、日本、台湾、ドイツなど	宇宙、防衛、政府、教育、NGO、プロフェッショナルサービス、テクノロジー	• 近年半導体業界への攻撃を確認 • Red Kelpieと攻撃ツールの共有が見られ、同グループの一部の可能性

Red Kelpieの代表的な戦術、技術、手順をまとめました（図表6）。米非営利研究機関MITRE（マイター）のATT&CK（Adversarial Tactics Techniques and Common Knowledge：サイバー攻撃の戦術や技術に関する共通知識の枠組み）に基づいた分析です。これによると、VPNや仮想デスクトップなどリモートアクセスサービスの脆弱性を突いて侵入する手口が増えています。侵入後、攻撃対象に自分たちの拠点をつくり、情報の持ち出しを狙います。

図表6：Red Kelpieの代表的な戦術／技術／手順

MITRE ATT&CKに基づいた分析

偵察、開発、初期アクセス、侵入	永続化、権限昇格、防御回避	探索、認証アクセス、横感染、収集	遠隔操作	情報持ち出し、インパクト
オンラインに晒されたアプリケーションへのエクスプロイト	システムプロセスの作成と変更 サービスプロセス	ファイルとディレクトリの探索	難読化したデータ	C2チャンネルを介した持ち出し
リモートアクセスサービスの悪用	実行フローハイジャック DLLハイジャック	ネットワークサービスの検出	暗号通信路	
正当なアカウントの悪用	レジストリ／スタートアップフォルダによる自動実行	ネットワーク共有の探索	非アプリケーション層プロトコル	
ユーザーによる実行	難読化されたファイルまたは情報の解読	ネットワーク設定の検出	非標準的なポート	
コマンドライン	マスカレード （さまざまな偽装テクニック）	ネットワーク接続の検出	ウェブプロトコル	
システムサービス サービス実行		ユーザーアカウントの探索	指令＆制御通信の冗長化	
		ローカルシステムからのデータ収集		

こうした戦術、技術、手順のなかでも、特に警戒すべきサイバー脅威はVPN機器を狙った攻撃です。警察庁が公表した「令和4年度におけるサイバー空間をめぐる脅威の情勢等について」によると、システムへの侵入・感染経路の6割超がVPN機器でした。これは世界的にも同じ傾向です。ダークウェブやディープウェブでは、脆弱な機器を運用しているIPアドレスの一覧が売買されています。中国を拠点とする脅威アクターとの関連性では、「ゼロデイ」脆弱性の発見能力向上も大きなリスクです。ゼロデイ脆弱性とはソフトウエアに存在する未公開の脆弱性です。こうした脆弱性を悪用することで修正プログラム公開前（公開からの経過時間が0日）に攻撃を実施することができます。中国では2021年に脆弱性管理に関する規定が施行されました。従来欧米圏で開催されていたゼロデイ脆弱性を発見するためのハッキングコンテストを国内で開催し、関連技術を磨く環境を整えています。

日本企業は何をすべきか

高まるサイバー脅威のリスクに日本企業はどのように対抗すればいいのでしょうか。

1つはインテリジェンスを磨くことです。国内の半導体産業を取り巻く環境の変化とともに、サイバー犯罪者集団やランサムウェアなどのサイバー脅威の変化を、常に把握する体制を整えることが欠かせません。インテリジェンスを基にセキュリティ投資や対策実行の時期や規模、将来の計画をつくり、更新し続けることへの重要性が増しています。

2つ目はコンプライアンスの再構築です。半導体業界の国際団体「SEMI」が公表した半導体セキュリティ規格に沿ってアセスメントを実施し、自社のセキュリティ対策の「現在地」を客観的に把握して改善項目を洗い出すことが必要です。定期的に自社の対策レベルを把握し続けることで、あるべき対策の「将来像」を社内で共有することができるのです。

また、1つ目と関連し、改善に取り組む項目の優先度付けにインテリジェンスを活用することできます。脅威アクターが悪用するTTP（Tactics：戦術、Techniques：技術、Procedures：手順）と、既存のセキュリティ対策を基礎として「どのフェーズにどのような対策を適用するか」という戦略を不断に練り、策定し、実行する。「Threat-Informed Defense」を採り入れ、グループ全体で素早くシフトできるかどうかが、サイバー対策の成否を左右するといっても過言ではありません。

直面する課題がたくさんある中、一度に全ての課題に手を付けるのは人材やコスト、時間などを考えると現実的ではありません。しかし、サイバーリスクが加速度的に高まる今、対策を施さなければ競合と比べたサイバー脅威への防衛力は劣後しかねません。自社のポートフォリオやビジネスを取り巻く環境に応じて優先順位を付け、着実に取り組み続けることが、サイバーリスクを軽減する近道であり、有効な手立てになるのです。

執筆者

名和 利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

山本 直樹

PwCコンサルティング
合同会社
パートナー

村上 純一

PwCコンサルティング
合同会社
ディレクター

祝出 洋輔

PwCコンサルティング
合同会社
マネージャー

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html