能動的サイバー防御に寄与する脅威分析理論と地政学の応用

東京海上ホールディングス株式会社
石川 朝久

「国家安全保障戦略」（2022 年 12 月閣議決定）で掲げた「能動的サイバー防御（active cyber defense: ACD）」における法整備や能力構築が着実に進む一方、ACD を運用する上では、攻撃グループを把握する脅威分析が必要である。

本稿は、ACD を実現する上で必要な脅威分析について、その理論的枠組みと論点を提示する。

1．脅威分析理論の基本構造

脅威分析において、「脅威」とは攻撃者または攻撃グループを指し、その本質は、意図（Intent）、能力（Capability）、機会（Opportunity）の三要素によって構成される。このモデルは SANS Institute[1]などで提唱されている。意図は、攻撃の目的や動機を表し、能力は攻撃を遂行する技術やリソース、機会は対象環境の脆弱性や外部条件を意味する。三要素を組み合わせることで、特定組織にとって現実的な脅威像を把握することが可能となる。

2．３種類の分析技法

脅威分析は大きく３種類のレベルに分類される。

（１）Tactical Analysis

Tactical Analysis は、攻撃者が悪用した攻撃手法の痕跡、あるいは今後悪用する攻撃要素の情報を収集し、対策に活用するものである。攻撃者が残した侵害指標（IOC）[2]や攻撃可能指標（EOC）[3]を収集・分析し、日々のセキュリティ運用に活用する。侵害指標の例として、攻撃に悪用された IP アドレス、マルウェアのハッシュ値、残存する一時ファイルなどが挙げられる。一方、攻撃可能指標は、脆弱性や脆弱な設定、管理されていない端末やアカウントなどが挙げられ、過去に悪用された製品群、公開された攻撃コード、様々な脅威インテリジェンスも踏まえ、早期警戒や対策を実施していく。

（２）Operational Analysis

Operational Analysis は、攻撃者の攻撃手法（TTPs）[4]を分析し、防御アーキテクチャの設計やセキュリティ態勢の把握に活用する。具体的な攻撃手法は MITRE ATT&CK フレームワーク[5]、防御アプローチについては、D3FEND フレームワーク[6]、ENGAGE フレームワーク[7]に集約されている。

攻撃者が悪用した攻撃手法を MITRE ATT&CK フレームワークを利用して共通言語化する

---

[1] John Doyle, “Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends (Part 1),” SANS Institute, January 5, 2024.
[2] IOC（Indicator of Compromise）とは、実際に発生した侵害・攻撃手法を特定するための技術的特性情報を意味する。
[3] EOC（Enabler of Compromise）とは、筆者の知る限り Open Threat Hunting Framework にて初めて提唱された概念で、侵害を可能にする実現要因を意味する。
[4] TTPs（Tactics, Techniques, and Procedures）とは、攻撃手法を記述するフレームワークである。
[5] “MITRE ATT&CK,” The MITRE Corporation
[6] “D3FEND,” The MITRE Corporation
[7] “MITRE Engage,” The MITRE Corporation

ことにより、金融庁が提唱する「脅威ベースのペネトレーションテスト（TLPT）」[8]や脅威ハンティング[9]への応用、検知能力の可視化や検知能力ギャップの特定、攻撃者への能動的対抗策の検討が可能となる。

（3）Strategic Analysis

攻撃者の意図を把握し、マクロ環境の変化を踏まえて長期的リスクの変動を分析する。PESTLE 分析[10]など外部環境分析を通じ、組織の戦略的意思決定に資する情報を提供する。

なお、こうした分析は、エビデンスの蓄積の上で成立している。攻撃活動が発生した際、最初にわかる事実は攻撃者が残した侵害指標など、Tactical Analysis レベルの情報である。フォレンジック分析などを通じて、当該攻撃グループが悪用した攻撃手法の一部も判明するが、単体の情報だけでは攻撃キャンペーンとして認識する上では不十分である。こうした一つ一つのケースを蓄積していくことで、攻撃グループが悪用する攻撃手法や攻撃キャンペーンが Operational Analysis として整理され、さらに攻撃者の意図の分析（Strategic Analysis）にもつながっていく。

3．地政学の応用と「意図」の階層モデル

脅威分析の文脈でも、地政学の重要性が指摘されている。多くのセキュリティベンダーの脅威インテリジェンスレポートは、地政学的視点に言及している。また、Deloitte Global の Lincoln Kaffenberger 氏は、SANS CTI Summit 2024 で Geopolitical Cyber Risk Assessment Framework を提唱している[11]。一方、地政学がどのように脅威分析に応用するか理解する上では、攻撃グループが持つ「意図」について 3 種類に階層化して考える必要がある。

（1）技術的意図

最も表層的な意図は特定技術や資産を狙う具体的動機を示す技術的意図（Technical Intent）である。これは、「攻撃キャンペーン」から読み取れる意図に相当し、悪用された技術、狙われた資産、攻撃対象組織の特徴などから推測可能である。

（2）社会政治的意図

技術的意図の更に深層となる第二レベルでの意図として、攻撃グループが持つ社会・政治的な意図（Socio-Political Intent）が挙げられる。これは、スパイ活動や破壊工作など、政治的文脈に基づく動機であり、攻撃グループがサイバー攻撃を行う理由・動機・存在意義に相当する。

（3）地政学的意図

最も根底的な第三レベルの意図として、地政学的意図が挙げられ、国家戦略や国際関係に由来する大局的な動機を示す。

この階層モデルは、攻撃の背後にある多層的な要因を把握する上で有効だと考える。地政学的状況に基づく国家的意図により、攻撃グループが形成され、その攻撃グループの社会政治的意図により、攻撃キャンペーンが形成され、技術的意図として認識される。

階層モデルのメリットと課題

地政学的視座を導入することで、攻撃者の行動をより長期的かつ構造的に予測することが可能となる。特に国家主体の脅威アクターに対して、国際関係や制裁状況、軍事的緊張といった外部要因を考慮することで、攻撃の意図やシナリオを把握できる。

特に近年のリスク管理の考え方では、リスクシナリ

---

[8] 北原幸彦「国際動向を踏まえた金融機関における実効性のある TLPT に関する考察」金融庁（2025 年 7 月）

[9] 「脅威インテリジェンスを活用したセキュリティ強化のためのアプローチ」独立行政法人情報処理推進機構（2025 年 8 月 29 日）

[10] PESTLE 分析（もしくは PESTEL 分析）とは、政治（Political）、経済（Economic）、社会（Social）、技術（Technological）、法律（Legal）、環境（Environmental）の 6 つの要素の頭文字を取った言葉で、これらを分析することで自社を取り巻く外部のマクロ環境を把握し、意思決定や戦略立案に役立てる手法、またはそのフレームワークを指す。

[11] “Navigating the Digital Battlefield: A Framework for Geopolitical Cyber Risk Assessment,” SANS Digital Forensics and Incident Response, February 20, 2024.

オの拡張が必要とされている。カーネギー国際平和基金の研究レポート[12]によれば、「高い影響を与える運用リスクシナリオ」のみならず、「上流インフラ」や「外的ショック」による被害シナリオの蓋然性・詳細化を行う必要性に言及しており、こうした観点で地政学アプローチを応用することは有効だといえる。

また、「社会政治的意図」が異なる攻撃グループを分析する際、地政学的観点は全体像を裏打ちする重要な要素となる。例えば、北朝鮮系攻撃グループである Andariel は世界中の重要インフラに対して侵害し、機密性の高い技術情報や知的財産情報を盗み出すエスピオナージ活動に注力しながらも、活動の一環としてランサムウェアなどサイバー犯罪活動も実施していた[13]。言い換えれば、社会政治的意図は、観測する立場により異なる状況である。一方、地政学的意図から見ると、「経済制裁下において、公式経済は停滞しており、リモート IT 就業[14]など、非公式経済活動による外貨獲得の必要性」や、「核開発により国際的孤立を深め、米韓日との緊張関係が継続している」事実など、諜報活動と外貨獲得を同時に行う、強い動機があることがわかる。

一方で、階層モデルも汎用性には限界がある。第一に、サイバー犯罪グループは、地政学で表現される国家の意図・戦略に依存せず攻撃を行う点であり、地政学の応用は難しい。特に最近では、犯罪動機で緩やかに組織される攻撃グループの存在が挙げられる。Scattered Spider[15]は、複数の小規模グループが TTPs を共有し、標的や目的を流動的に変化させる集合的概念であり、国家主体とは異なる特性を持ち、海外では、”The Com”と呼ばれる。このような攻撃グループに対しては、地政学よりも技術的・戦術的分析の比重が高くなる。一方、コロニアル・パイプライン事件[16]のように、影響を及ぼしかねない事案においては、国家関与の有無や地政学的要因の切り分けが難しい。

第二に、攻撃グループの世界でも分業化が進んでいる[17]。代表的な例は、ランサムウェアサービスを提供する RaaS（Ransomware as a Service）や、初期侵入用のアクセスを提供する IAB（Initial Access Broker）の存在である。こうした分業化により、技術的な意図にも一貫性が見えづらくなり、分析が困難になる。

4. まとめ

ACD の実現には、単に防御技術や法制度の整備にとどまらず、攻撃主体を深く理解するための脅威分析が不可欠である。本稿で整理した通り、脅威分析は意図・能力・機会という基本構造を起点に、Tactical、Operational、Strategic 層に分けて行うことで、日々のセキュリティ運用から長期的なリスク管理まで幅広く活用できる。

さらに、攻撃グループの意図を「技術的」「社会政治的」「地政学的」という階層モデルで捉えることで、攻撃の背後にある多層的要因を理解し、国家戦略や国際関係と結び付けて予測することが可能となるため、さらなる実践的知見の蓄積が期待される。

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/

[12] Lincoln Kaffenberger and Emanuel Kopp, “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment,” Carnegie Endowment for International Peace, September 30, 2019.
[13] “NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets,” National Cyber Security Centre, July 25, 2024.
[14] Microsoft Threat Intelligence, “Jasper Sleet: North Korean remote IT workers’ evolving tactics to infiltrate organizations,” Microsoft, June 30, 2025.
[15] KELA Cyber Team「航空業界を標的とするサイバー犯罪グループ：Scattered Spider」KELA（2025 年 7 月 8 日）
[16] 小林偉昭「コロニアル・パイプライン事件他で米国サイバーセキュリティは激変予感」Tokio Cyber Port（2021 年 7 月 29 日）
[17] 「産業化と分業化がますます進むサイバー攻撃の実態を知る」Cybereason（2024 年 1 月 23 日）