公表日	タイトル	内容説明
2022年4月27日	Microsoft: ウクライナでのハイブリッド戦争	Microsoftは、ウクライナに対するハイブリッド戦争で観測されたロシアの破壊的なサイバー攻撃の詳細をブログで発表
2022年3月7日	Google: ウクライナでのハイブリッド戦争	Googleの脅威分析グループ(TAG)は、ロシアの脅威者の多くから、エソポネージからフィッシング詐欺に至る活動を観測
2022年2月28日	Microsoft: ウクライナでのサイバー脅威活動、分析と情報源(更新版)	Microsoftは、ウクライナで激化するサイバー活動を監視し、潜在的な攻撃に関するインテリジェンスと、今後の攻撃に対する予防的防御を実施するための情報を組織に提供
2022年2月4日	Microsoft: ACTINIUMがウクライナの組織を狙う	Microsoft脅威情報センター（MSTIC）は、約10年前から活動し、ウクライナの組織やウクライナ問題に関連する組織へのアクセスを追求してきたACTINIUMという脅威グループに関する情報を共有
2022年1月20日	Palo Alto Networks: 脅威の概況、ロシアとウクライナのサイバー紛争が進行中	1月14日未明、ウクライナ政府の多数のウェブサイトを標的としたロシアによる一連のサイバー攻撃について報道。この攻撃の結果、多くのサイトが改ざんされたり、アクセス不能になったりしていることが判明

CISA と FBI は、脅威とサイバー攻撃に関する情報を共有する重要な責任を負っている。SolarWinds、Microsoft Exchange、Colonial Pipeline の攻撃を受け、2022 年 5 月にホワイトハウスは大統領令 14028 "Improving the Nation's Cybersecurity "を発行した。この命令は、FBI、CISA、情報機関の一部のメンバーなど、サイバー攻撃の調査や修復を担当する米国政府機関間の情報共有を改善することを目的としている。

また、FBI は、悪意のある行為者を阻止するために、正確なアトリビューション技術に支えられた ACD 技術を使用している。FBI は、その権限により、「捜査、情報収集、および悪意のあるサイバー活動のターゲットと緊密に連携して、犯人を特定し、再犯を阻止し、責任を負わせる」ことができると報告している。大統領政策指令（PPD）41 は、重要なサイバー事件が発生した場合の脅威への対応について、FBI を連邦政府の主導機関に指定し、大統領令 12333 は、米国内での情報活動の暴露、防止、調査について FBI を主導機関に指定し、合衆国法典第 18 編第 1030 条は、スパイ行為と対外防諜に関わるサイバー調査を指揮するよう FBI を指定している。FBI は最近、ランサムウェア・グループのネットワークに数カ月間侵入し、身代金を支払うことなく被害者のデータを解放するための復号化キーの取得とネットワークの完全シャットダウンに成功し、「ハッカーをハックした」と報告している。悪意のあるサイバー行為者を起訴する場合、FBI は必然的に、刑事訴追のための「合理的疑いを超える」基準に耐えられるようなアトリビューションの結論を出さなければならない。

これらの省庁は、自らの業務のために ACD やアトリビューション活動を行うだけでなく、これらの分野で民間企業への支援も行っている。例えば、NSA は、産業界、特に国家安全保障、国防総省、防衛産業基盤の分野と連携し、サイバーセキュリティ・コラボレーション・センター（CCC）を運営している。

- CCC を通じて、NSA は、産業界のサービス・プロバイダーと協力して、民間部門に向けられた国家によるサイバー活動や悪意のあるサイバー活動を検知し、それに対処している。
- 敵の戦術、技術、手順を迅速に検知し、そのツールや技術を妨害するために、民間団体やサービス・プロバイダーと共同で分析的な技術開発を行う。
- 民間企業やそのサービス・プロバイダーに対する脅威や脆弱性に関する積極的な情報提供や二国間情報交換を推進する。
- 特定された脆弱性について、民間企業や NSS への技術提供者に通知し、協力し、共同で緩和策を開発する。

また、CISA は組織がセキュリティ能力をさらに向上させるのに役立つ、無料のサイバーセキュリティツールとサービスのリストを編集している。この生きたリポジトリには、CISA が提供するサイバーセキュリティサービス、広く使われているオープンソースツール、サイバーセキュリティコミュニティ全体の民間および公共セクター組織が提供する無料のツールやサービスが含まれている。提供されるツールのカテゴリーは、以下の目標によって構成される。

- 損害を与えるサイバーインシデントの可能性を低減する
- 侵入の可能性を迅速に検知するための手段を講じる
- 侵入が発生した場合の対応策を組織が確実に準備する
- 破壊的なサイバーインシデントに対する組織の回復力を最大化する

ISA は、サイバーセキュリティ評価ツール（CSET）も提供している。CSET は、「運用技術と情報技術を評価する体系的なプロセスを通じて、資産所有者と運用者をガイドするスタンドアロン・デスクトップ・アプリケーション」である。CSET は、組織がそのシステムとネットワークのセキュリティ状況を評価するのに役立ち、要約レベルおよび詳細レベルの両方の結果を提供する。CSET は、一連のアンケートを通じてユーザーをガイドする。評価結果は、長所と短所を示す一連のチャートと優先順位付けされた推奨事項、および組織がサイバーセキュリティリスクの姿勢を改善するのに役立つ他のリソースとして提供される。CSET にはいくつかの標準が組み込まれており、ユーザーの選択に応じて評価に含めることができる。これらのオプションの標準の例としては、NIST Cybersecurity Framework、NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations、Committee on National Security Systems Instruction (CNSSI) No.1253, Categorization and Control Selection for National Security Systems、さらに重要インフラ（産業制御システム、スマートグリッド、原子力施設など）向けの様々なサイバーセキュリティ標準が挙げられる。

NIST NCCoE は、産官学の専門家を集め、複雑な IT システムのセキュリティと国家の重要インフラの保護という現実的なニーズに取り組むコラボレーション拠点だ。NCCoE の目標は、企業や商取引のサイバーセキュリティを向上し、サイバーセキュリティの学習曲線を下げ、セキュリティ技術の革新を促進することである。NCCoE が提供する重要なリソースの 1 つに、NIST Special Publications series の実践ガイド達がある。各実践ガイドは、NCCoE が様々な技術や産業領域におけるサイバーセキュリティの課題に対処するために、市販の技術や標準をどのように適用してきたかを示している。産業ドメインには、5G、AI、モノのインターネット、サプライチェーン保証、ゼロトラストアーキテクチャなどの領域が含まれる。産業ドメインは、主に重要インフラに焦点を当て、エネルギー、金融サービス、製造業などの産業が含まれる。

4. 効果的なアトリビューションのための潜在的な障害

アトリビューションは、悪意のある行為者を特定し、サイバー防御を強化し、指導者に情報を提供する上で重要だ。しかし、特定の行為を正しい行為者に確実に帰属させることは、必ずしも容易ではない。そもそも誰の指がキーボードに触れていたのか、そもそも誰がこの人たちにキーボードに触れるように指示したのかを掘り下げることは難しい場合がある。もう一つの課題は、サイバーインシデントが発生した場合、アトリビューションに長い時間がかかり、すぐに価値を見いだせない可能性があることだ。

表 3-7 は、CTI およびアトリビューション情報をサイバーセキュリティ情報共有組織と共有する際の潜

在的な障壁の詳細を示す。

表 3-7. 効果的なアトリビューション情報発信を阻むもの.

障壁	説明
法務/ポリシー	個人情報や知的財産に関するプライバシーへの懸念、および不正な開示による法的影響についての認識
技術的障壁	共有組織のシステム間の相互運用性/互換性の欠如
インフォメーショナル	共有する情報が多すぎて処理できない、共有情報の適用性がない、信頼性のないデータ
オペレーショナル・セキュリティ	機密性の高い情報源や方法、あるいは情報の入手経路を推測できるような情報を広めないという要件
コラボレーション	プロセスの複雑さ、信頼関係の確立の難しさ、互恵性の欠如、参加者のタイプ、グループのサイズ
管理上の障壁	組織を「制御不能なリスク」にさらすことによる内部リスク回避と不信感、情報交換の非効率的な方法、共有情報の管理不備、情報共有のための信頼経路を確立する合意がないこと
組織上の障壁	リソースが限られているため消費できない、情報の利用を管理・制御する仕組みがない
パフォーマンス	必要なシステム技術のコストが高い、古い/信頼性のないデータに基づく誤検出のコスト、共有データを処理するためのリソースが限られている。
コスト	必要なシステム技術のコストが高い、古い/信頼性のないデータに基づく誤検出のコスト、共有データを処理するためのリソースが限られている。

第４節 アトリビューション機能の実装

前節では、アトリビューションの概要について説明した。本節では、アトリビューション活動が実際にど

のように行われるのか、またアトリビューションが基本的に分析プロセスであることを説明する。

アトリビューションは、観察された悪意のある活動の特定の要素を用いて、誰がという問いに答えようと試みる。

- TTPs（どのように）
- インフラストラクチャ、ツール、マルウェア（どこで、どのように、何を）。
- 動機（なぜ）
- ターゲット（どこで、いつ、なぜ）

初期のインシデントレスポンス活動とデータ収集が完了すると、収集したインテリジェンスとデータをレビューして分析し、その活動を特定の国、グループ、悪意のあるサイバー行為者に帰属させるという手作業のプロセスが続く。分析プロセスの後に、アトリビューション情報は、適切な事後措置や防御策を策定するために、組織の幅広い知識ベースの中に織り込まれる必要がある。組織の CTI および分析能力が成熟するにつれて、アトリビューション情報をますます活用して戦術、運用、および戦略の見通しを改善し、指導者や意思決定者を支援する必要がある。

帰属の疑いを立証できれば、たとえそれが単一の脅威要因に絞り込めなかったとしても、インシデント対応担当者が、特に調査の初期段階では容易に明らかにならなかったかもしれない特定のアーティファクトや方法論に焦点を当てることができるようになる。例えば、MITRE ATT&CK のようなフレームワークと最初のアトリビューション決定を組み合わせることで、悪意のあるイベントの前または後に脅威者が取った行動を分析者が特定するのに役立つ。

アトリビューションの確立は、一連の技術的なツールを使用するだけでは不可能であることを忘れてはならない。ツールによって明らかになったことを評価するためには、熟練し、訓練されたサイバーセキュリティ・アナリストの集団が必要だ。組織のサイバーセキュリティ運用は、アトリビューションに焦点を当てた成熟した分析能力なしには成熟しない。この小節では、アトリビューションプロセスの一部である情報と分析の種類を特定るが、これらのインプットだけでは、アトリビューションの結論を導き出すのに十分ではない。この作業には、好奇心と判断力を備えた経験豊富なアナリストが必要である。

Timo Steffens 氏は、「アトリビューションはプロジェクトのように組織化できず、分析を行うためのチェックリストも存在しない」と指摘した。アトリビューションへの取り組みは、確立された一連のプロセスや手法に従うことはできず、効果的なレベルのアトリビューションを達成することは期待できない。しかし、分析者が利用すべき最低限のベストプラクティスは存在する。ステファンズ氏は、マルウェア、インフラ、コントロールサーバ、テレメトリ、インテリジェンス、キュイボノ（MICTIC）フレームワークに従ってアトリビューションを確立するための 1 つの可能なアプローチを示しており、同氏はこれをダイヤモンド・モデルの「よりきめ細かいバージョン」と呼んでいる。

1. 企画・準備

サイバー攻撃におけるアトリビューションには、通常、技術的（どのように）、戦術的（TTP）、作戦的（何を）、戦略的（誰が、なぜ）の 4 つのレベルの脅威情報が分析される。技術的なレベルでは、特定のサイバー攻撃に使用された技術を示す、調査官が利用可能なさまざまなツールがある。同じツールや技術の多くは、インシデントレスポンス活動で利用される。

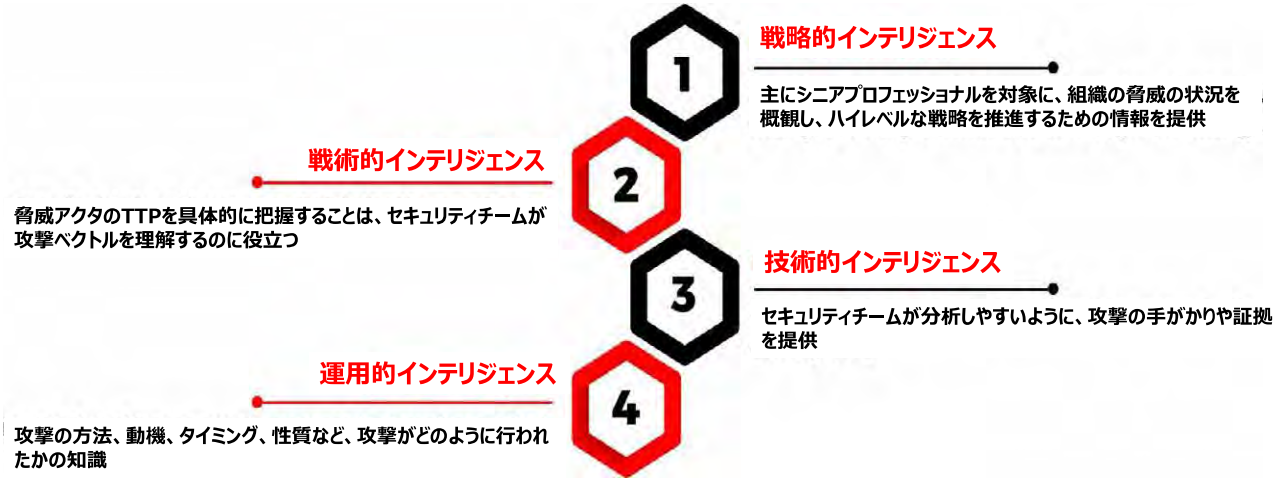

図 3-6：脅威インテリジェンスのレベル.[6]

アトリビューションを立証しようとする場合、作戦レベルと戦略レベルのインテリジェンスを明確に区別することは困難であり、両者はかなりの程度重複している。さらに、これら 4 つのレベルの分析は、決められた時系列や順序に従った段階的なプロセスであることはほとんどない。場合によっては、技術的な指標で悪意ある活動を特定する前に、地政学的な背景やその他の非フォレンジックな情報源が、帰属の最初の手がかりとなることもある。したがって、戦略的なレベルでの分析は、技術的な側面を検討する前に始めることができる。戦略的分析には、敵対者の動機に関する知識が必要であり、商業、軍事、経済など、他国の優先事項に対する理解によって導かれる。

2. アトリビューションプロセスをサポートする情報カテゴリー

アトリビューションプロセスはしばしば反復され、前述したように多くの種類の情報が利用される。本小節では、帰属プロセスで使用される情報のタイプについて説明する。

(1) 動機

サイバーイベントの調査が悪意のある意図的な行動を示すと仮定すると、その真の結果を評価するために、調査には数週間とは言わないまでも、数日かかる可能性がある。インシデント対応作業が進行している間、次の段階として、敵対的な行為の背後にある動機を確認することが自然だ。犯罪を目的とした行為なのか？不満を抱いた従業員による行動なのか？イデオロギー的な敵対者による抗議なのか？それとも、外国勢力の国家安全保障に起因するものなのか？もし、その行為が国家によるものと判断されれば、また新たな疑問が生じ、それぞれの動機を正確に把握するための緻密な追跡調査が必要となる。

[6] EC-Council. "https://twitter.com/eccouncil/status/12923949925106073"

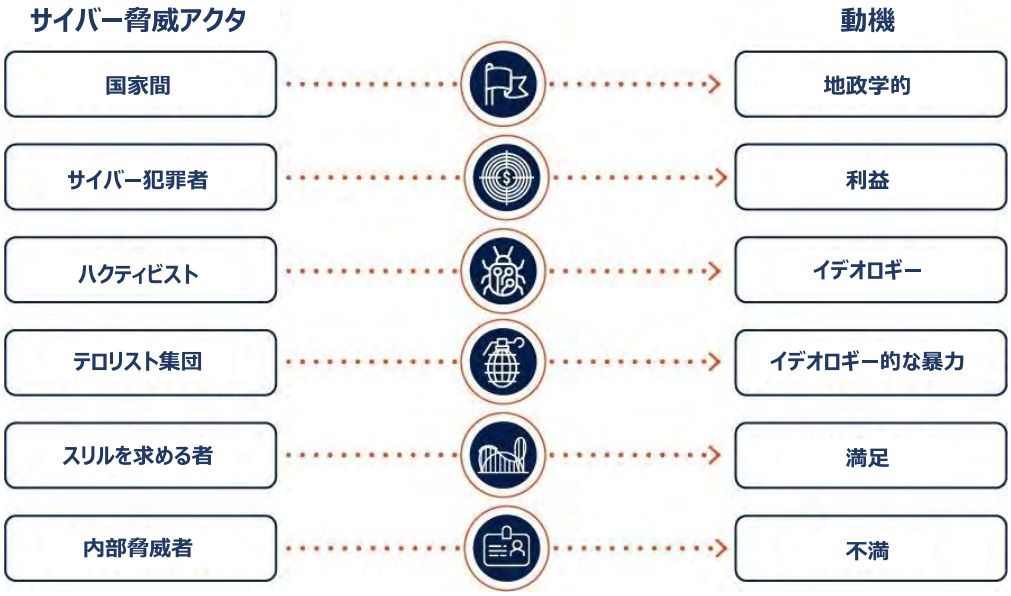

図 3-7：攻撃者のタイプに関連する動機.

特定の国家や国内の活動家の活動を特定しようとする場合、分析者は以下に示すような一連の質問をすることになる。

- 悪意のある活動は、情報収集のような単純なサイバースパイ活動か？もしそうなら、それは典型的な情報収集活動なのか、それとも国家が支援する商業スパイの活動の一部なのか？
- 後続の攻撃のための基礎固め（プレ・アタック）なのか？
- 特定のメッセージやシグナルを伝達するためのものなのか。その場合、メッセージは何か？
- 他の方法でターゲットの認識を形成することを意図しているのか（影響力の行使）、またその目的は何か。
- 選挙結果を左右するため、あるいはその信憑性に疑念を抱かせるためなのか。
- 敵対者を弱体化させるために、混乱と混沌を招くこと、または反対意見を煽ることを意図しているのか。
- 動機を決定する際、加害者が自らの行動をどのように見ているかを理解することが役立つ場合がある。彼らはいわれのない（サイバー）行動を意図しているのか。あるいは、（サイバー領域であれ他の場所であれ）自分たちに行われたことに対する報復行動と見ているのか。あるいは、相手が自分たちに対して行おうとしていると加害者が予想する動きに対する防御的な行動（予防的または先制的）として正当化するのか。

重要なのは、加害者（特に国家のエージェントや代理人）が自らの行動を隠そうとせず、その真の意図を隠そうとしたケースがあることだ。例えば、被害者のネットワークに危害を加えることを真の目的としていながら、自分たちの行動をランサムウェアと称して見せかけることがある。このような戦術は、特徴づけとアトリビューションの課題を複雑にしている。特定の悪意あるサイバー事象の徹底的な調査、加害者が時間をかけて公開した追加情報（故意または無意識）、および文脈的要因（地政学的動向など）の考

慮が、最終的に攻撃者の根本的な動機に関する重要な洞察をもたらす。

(2) 悪意ある行為者の背後にいるのは誰なのか？

悪意のある行為者の身元を確認する際に考慮すべきもう一つの要素は、誰が、あるいはどの組織が、悪意のある活動を指示または後援していた可能性があるかということだ。また、組織の指導層のどのレベルにおいて、悪意のある活動が承認されたのか、あるいは少なくとも支援/容認されたのかも考慮される。

近年、サイバーフォレンジックは著しく進歩しているが、悪意のある行為者の正体（別の悪意のある行為者になりすましているかどうかも含む）を隠蔽するための技術の高度化もそれに歩調を合わせて進んできている。フォレンジックによる TTP の調査は、サイバー攻撃者の身元を確認する上で非常に有効だが、インテリジェンスは、アトリビューション結果の信頼性を高め、さらに重要なことに、悪意のある活動のスポンサーまたは指示者を確認するのに役立つ。悪意のある活動を指揮する組織に関するインテリジェンスは、広範なネットワーク監視、センサーの持続的な前方展開と監視、そして特に、こうした攻撃の元となる敵対的ネットワークへの侵入から得ることができる。後者の 2 つの情報源は、ほぼ間違いなく機密情報であり、民間企業のアナリストには一般に入手不可能であろう。

悪意のあるサイバー事象の特定と対応は、悪意のある行為者または他の者がサイバー事象の手柄を立てたり、責任を否定したりすると、さらに複雑になる可能性がある。フォレンジックが重要なのは、インテリジェンスと同様に、どちらかの証明または反証を助けるからである。アトリビューションによって明確な特定に至る上で大きな障害となっているのは、一部の国家がプロキシやその他の非国家機関を利用してサイバー攻撃を行うことが一般的であることだ。このような悪質なケースでは、フォレンジックとインテリジェンスだけでは、帰属やどの組織がその活動を促したかを明確に示すことができない場合がある。例えば、2020 年 7 月、2 人の中国人が、国家安全部（MSS）の広東省国家安全局（GSSD）と協力しながら、個人的な利益を得るために被害者を狙ったとして、米国司法省に起訴されたことがある。[7]

(3) 攻撃手法の高度化

サイバー脅威の主体は、その能力や洗練度において平等ではない。彼らは、その活動に必要な様々な資源、訓練、支援を受けている。サイバー脅威の主体は、単独で活動することもあれば、より大きな組織（すなわち、国民国家や組織的犯罪集団）の一部として活動することもある。熟練した悪意のある行為者は、例えば、セキュリティ研究者が使用している商用セキュリティツールを活用するなどして、与えられたタスクに有効であり、かつ／または防御側がその活動を特定することを困難にするため、容易に入手できるツールやテクニックを使用することがある。

最も巧妙な攻撃を行うことができる行為者の数は、国家を含めて比較的少ないため、攻撃の巧妙さのレベルを決定することで、悪意のある攻撃者の可能性を迅速に絞り込み、アトリビューション分析の焦点も

[7] U.S. Department of Justice, Public Affairs Notice, 20-675, July 21, 2020., https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

絞り込むことができる。以下に示す悪意のある攻撃者の種類とその巧妙さのレベルは、アトリビューション分析の出発点となる。

- Advanced Persistent Threats（APT）とは、高度な技術と技能を持つ最上位の脅威者のことを指す。APT は、高度な技術を駆使して、目標を達成するために複雑かつ長期的なキャンペーンを行うことができる。この呼称は、通常、国家や非常に熟練した組織犯罪集団にのみ使用される。
- 国家に代わって活動する国家支援型サイバー脅威主体は、主に地政学的な目的を達成するためにサイバー脅威活動を行う。彼らは、専用のリソースと人員を持ち、大規模な計画と調整を行う、最も洗練された脅威主体であることが多い。先進的なサイバープログラムを持たない国家は、高度なサイバー脅威活動を可能にするために、商業的なサイバーツールや世界的に増加する人材を利用することができる。また、一部の国家は、民間企業や組織的犯罪シンジケートと業務上の関係を結んでいる。
- サイバー犯罪者は、主に金銭的な動機で行動し、その精巧さは千差万別だ。組織的な犯罪集団は、多くの被害者に影響を与えることができる専門的な技術的能力に加えて、計画立案やサポート機能を有していることが多い。サイバーツールやサービスの違法なオンライン市場によって、サイバー犯罪はよりアクセスしやすくなり、サイバー犯罪者はより複雑で高度なキャンペーンを行うことができるようになった。犯罪的サイバー行為者、特に経済的利益を動機とする者は、身元を隠し、訴追を避けようとする。彼らは、ガバナンスや政策上の条件から、身元を隠すことが容易な場所を探す。
- ハクティビストは、イデオロギー的な動機でサイバー悪意ある活動を行い、一般的に国家が支援するサイバー脅威の行為者や組織的なサイバー犯罪者よりも洗練度は低い。これらの行為者は、テログループと同様に、多くの場合、展開にあまり技術的なスキルを必要としない、広く利用可能なツールに依存している。彼らの行動は、ターゲットに対して評判以上の永続的な影響を与えないことが多い。しかし、時には、これらの行為者は、ターゲットに物理的および金銭的な損害を与えることができる。
- インサイダー脅威は、組織内で働く個人で、セキュリティ境界で保護されている内部ネットワークにアクセスできるため、特に危険だ。インサイダー脅威は、不満を持つ従業員である場合もあれば、他の脅威要因に関連する場合もある。

(4) 攻撃の重大性

悪意のあるサイバー事象の重大性、または影響力は、悪意のあるサイバー行為者の特定をさらにサポートすることができる。この重大性の判断は、主観的である場合もあれば、事実に基づく場合もある。

さらに、重大性または影響の決定をサポートするために、サイバーセキュリティ組織の外部の利害関係者と他の考慮事項が必要な場合がある。攻撃の重大性はすぐには明らかにならないかもしれないので、この帰属の要素は価値を持つようになるまで時間がかかるかもしれない。以下に列挙する基準は、インシデントの重大性の評価と特徴付けを支援することができ、実際の被害がすぐに明らかにならない場合に役立つことがある。

1. 敵の目的と意図された効果

2. 実際に発生した影響(脅威の主体が意図したよりも大きい、小さい、局地的、または広範囲に及ぶ可能性がある)
3. 関与した標的(政府、重要インフラ、金融など)
4. 攻撃で使用された TTP
5. その悪意ある行為が、より広範で大胆な行動パターンを示しているのか、それとも単なる単発の行為なのか

(5) 脅威行為者のスコアリング

インシデントレスポンスやイベントの分析時には必要ありませんが、スコアリング手法を適用することで、組織は脅威をより詳細に特定し、対応に優先順位をつけることができる。スコアリングの方法論はさまざまだ。一般に、スコアリング方法には、定義された一連の基準と、その基準を解釈するための水準が含まれる。組織によっては、数学的なスコアを適用して基準をさらに拡張し、そのスコアを比較に使用する方法を選択する（例：スコアの平均、重要性に基づく基準の重み付け、スコアの高さと低さに意味を持たせるなど)。

本小節では、分析者が帰属プロセスで最もリソースを投入すべき脅威の優先順位付けに役立つ、スコアリング基準の例を示す。

脅威行為者を評価するための基準

脅威のランク付けは、脅威行為者の意図と脅威行為者の能力に基づいて行われる。これらのランク付けを組み合わせると、総合的な脅威レベルが算出される。表 8 と表 9 は、脅威のスコアリング基準の例を示している。

表 3-8. 脅威行為者の意図のスコアリング.

脅威行為者のインテントのスコアリング	
意図レベル	**基準説明**
非常に高い (Focused)	脅威の主体は、着目しているシステムまたはサービスを攻撃することを主な目的としている。これらは通常、既知の、敵対的な、主要な外国の諜報機関によるものだ。 脅威行為者が標的システムまたはサービスについて詳細な調査を行い、システムまたはサービス固有の攻撃を作成したことを示す証拠がある。これには、特定のユーザーの行動(業務に関連すると思われるメールの添付ファイルを開くなど)に訴えかける、またはそれを利用するように設計された攻撃が含まれる。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を行い、攻撃の情報提供と促進を試みる可能性が非常に高い。 脅威行為者は、滅多に発生しない攻撃機会を利用するために待機し、攻撃を実行するために、複数の脅威行為者が連携する形でリソースを急増させる準

	備をしている可能性が高い。
高 (Committed)	脅威の発生源は、持続的かつ頻繁にシステムまたはサービスを攻撃しようとしている。これらは、典型的には、外国の諜報機関、高度な能力を持つハクティビストグループ、テロリストグループ、および主要な犯罪組織によるものだ。 脅威行為者は、ユーザーの行動を特に利用することを目的とした攻撃の開発を含め、攻撃に数人を割くことをいとわないという証拠がある。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を行い、攻撃の情報提供と促進を試みる可能性がある。
中位 (Interested)	脅威の行為者は、頻繁にシステムまたはサービスを攻撃しようとしている。これらの行為者は、典型的には、小規模なテロ組織、ハクティビスト組織、組織犯罪集団であり、そのシステムまたはサービスがその組織にとって特に関心のあるものである場合である場合が多い。 脅威行為者は、攻撃に数人の人員を割くことをいとわない。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を試みることはないだろう。
低い (Curious)	脅威行為者は、時折、または偶然にシステムやサービスを攻撃しようとしている。このような行為者は、通常、単一問題の政治的圧力団体、アマチュアハッカー、テロリストに感化された個人（ローンウルフ）、調査ジャーナリスト、学者、商業的ライバルとなる場合が多い。 脅威行為者は、攻撃のためにごく少数の人々を割くことを望んでいる。脅威行為者は、ユーザーコミュニティに対して直接的な説得や強制を試みる可能性は極めて低い。
非常に低い (Indifferent)	脅威行為者がシステムやサービスに対して何らかの攻撃を試みる可能性は極めて低い。このような行為者は、通常、ビジネスパートナーであり、システムまたはサービスを攻撃していることが知られれば損害を受けるような、良い評判を持つ組織である。

表 3-9. スレットアクター能力スコアリング.

スレットアクター能力スコアリング	
能力レベル	**基準説明**

手強い (Formidable)	脅威の主体が極めて有能で、十分な資金を持つ外国の諜報機関のような場合。 • システムまたはサービスの侵入に数人年を割く • 標的を特定した攻撃を展開 • 標的システムやサービスに関する情報を複数の情報源から収集し、調整 • 長期的な攻撃のためにインサイダーを育成 • 大量の機器の導入 • 複数の脅威行為者を利用した攻撃の調整
重大な (Significant)	脅威の主体が有能で、大きな資源を持っている場合。例えば、中程度の資源を持つ外国の諜報機関、よく組織されたテロリストや犯罪者集団など。 • システムやサービスへの侵入に数人週を割く • 一般に公開されている攻撃ツールをすべて使用 • 特定の攻撃のためにインサイダーに影響を発揮 • 適度な量の機器を配置
限定的 (Limited)	小規模で組織化されたテロリストや犯罪者集団、あるいは有能な個人ハッカーなど、脅威の主体が適度な能力と資源を持っている場合 • システムやサービスへの侵入に数人日を割く • 一般に公開されている有名な攻撃ツールを使用 • 少量の機器を展開
小規模 (Little)	脅威の主体が、一般的なインターネットユーザーなど、ごくわずかな能力とリソースしか持たない場合。 • システムやサービスへの侵入に数人日を割く • ごく少量の機材で展開
非常に小さい (Very Little)	脅威の主体が、コンピュータやインターネットの初心者のように、能力やリソースをほとんど持たない場合。 • シンプルな「プラグアンドプレイ」プラグインデバイスとリムーバブルメディアの使用 • システムやサービスへの侵入に数時間を割く

ある時点では複数の脅威者が存在する可能性があるため、スコアは最も高い脅威者の意図と能力のレベルを反映する必要がある。サイバー脅威の性質や潜在的な脅威者に関する情報は常に進化しているため、脅威が大きく変化し、特定のシステムに対するリスクの再評価が必要であるかどうかを判断するために、定期的に脅威評価を見直すことが必要である。

脅威行為者の意図と能力に関する相対的なスコアは、全体の脅威レベルマトリックスで確認する必要が