TLP：WHITE

戦いの原理・原則
と
サイバーセキュリティ

戦いの原理・原則と攻撃者の視点を参考に
適切なセキュリティ対策の考え方を理解する

2024 年9月

独立行政法人情報処理推進機構（IPA）

産業サイバーセキュリティセンター

第 7 期中核人材育成プログラム

卒業プロジェクト

はじめに

● 序文

「サイバーセキュリティは、非常に複雑で難しいです！」

ニュースなどでも言われているとおり、サイバー攻撃の脅威は日に日に大きくなり、ビジネスモデルの変化や革新的なテクノロジーの登場によって、サイバーセキュリティのことを理解することは益々難しくなっているように感じます。

そのような中、私たちは企業などのセキュリティ担当者としてサイバー攻撃から組織を守るため様々な業務を行っています。更に、ある程度経験を積んだ方であれば、組織のサイバーセキュリティ戦略の検討や予算執行のために経営・マネジメント層とコミュニケーションを取り、現場の事情を汲みながらセキュリティ事業を管理・推進していくことも多く、様々な悩みや苦しみを抱えているのではないかと思います。

そのため、多くの方は関連する書籍を読んだり、ベンダーが提供するトレーニングコースを受講したりして業務に必要な知識やスキルを身に付けます。実際に業務を行ううえでは、国際標準のセキュリティフレームワークやガイドラインを活用することも多いと思います。

しかし、それでセキュリティ担当者が抱える問題は解決しているでしょうか。

・ランサムウェア攻撃が流行っているが、どの程度のリスクがあるのか？
・なぜ、ＥＤＲやＳＩＥＭなどのソリューションが必要なのか？
・そもそも、本当にサイバー攻撃を受ける可能性はあるのか？どのような攻撃か？

上司やビジネスの現場からこのような質問をされたとき、根拠に基づいて自信をもって説明し、行動に移すのは非常に難しいのではないかと思います。

私もはじめはそうでした。勉強して覚えた単語を使い、「こう教えられたから」「書籍やフレームワークに書いてあるから」を根拠として説明しても、理解してもらうことは難しかったことを覚えています。同じように悩んでいる同僚もたくさん見てきました。

しかし、ある日先輩と話していた時に言われた、「セキュリティって戦術と同じだよな」の一言で、辛く・苦しくなるかもしれなかったセキュリティ担当者としての人生を大きく変えることができたと思っています。

※仕事柄、「戦い」は自衛隊に入隊した時から飯のタネであり、幹部自衛官となってからは「戦術」として基礎から叩き込まれ、普段の仕事のなかで常に意識し実践してきたつもりです。（そのように厳しく指導される、というだけではありますが）

戦術や戦いの原理・原則からヒントを得るという考え方は、ビジネスの世界ではかなり浸透しています。書籍や論文なども多数存在しており、世界中の経営者が戦いの原理・原則をビジネスに応用して大成功していますから、サイバーセキュリティの世界にもきっと通用するはずです。

本書では、戦いの原理・原則を分かりやすく解説するとともに、これらを活用してサイバーセキュリティをより深く理解するためのポイントを提供します。

・サイバーセキュリティとは一体何なのか
・誰が、何のために、どのようなサイバー攻撃をするのか
・セキュリティ対策をどのように行うのが適切なのか

技術的なスキルやテクノロジーに習熟するだけでは適切なセキュリティ対策を行うことはできません。サイバーセキュリティの本質や力学に目を向け、理解する努力を行うことで、自分の仕事に意義を見出し、刻一刻と変化する競争社会でも自立的に行動し、生き残っていく事ができるのではないでしょうか。

同じような悩みを抱えている全国のセキュリティ担当者の方々が、活気に満ち楽しくセキュリティの仕事をしていくための参考になれば幸いです。

● 対象読者

本書は、企業や組織のセキュリティ担当者、特に経営層と現場の橋渡しとしての役割を期待されている「セキュリティ中核人材」を主対象としています。

・セキュリティの方針検討や戦略立案、予算配分等について、経営層を補佐する
・現場が実施するセキュリティ対策を推進・統制・管理する
・基本的なセキュリティの概念や技術に習熟している

よって、サイバー攻撃手法やセキュリティ対策などについては、説明を省略している部分があります。それぞれの詳細については、解説書籍・Web サイトなどのリソースを活用してください。

また、本書の内容を上司・経営層などに紹介する際は、必要に応じ技術的な部分の説明について適宜サポートが必要です。

● 期待する効果

本書は、戦いの原理・原則を活用してサイバーセキュリティの本質と力学を紐解き・理解することにより、組織としてリスクに応じたセキュリティ対策を推進していくための「軸となる考え方」を養い、複雑で困難な状況でも、中核人材として自信を持って自立的に行動できるようにすることを狙いとしています。

・戦いの原理・原則を通じて、サイバーセキュリティの本質と力学を理解する
  －サイバーセキュリティを構成する要素（資産、脆弱性、脅威、リスク）
  －サイバー脅威とは何か、何のためにどのような攻撃を行うのか
  －セキュリティ対策を適切に行うための考え方
・攻撃者の目線から、サイバー攻撃そのものに関する理解を深める
  －自組織に対する脅威とサイバー攻撃手法の特性
  －サイバー攻撃によってリスクが発生するシナリオと可能性
・リスクに応じたセキュリティ対策の考え方を理解する
  －サイバーセキュリティの戦略と戦術
  －攻撃者の目線とリスクシナリオを踏まえ、対応の優先順を決める
  －課題に応じてフレームワークやガイドラインを使いこなす

リスク分析やセキュリティ対策の具体的な方法論を述べているわけではなく、読者の組織・環境でも柔軟に適用できる「考え方」に重点を置いています。

● 本書の構成

本書では、はじめに複雑なサイバーセキュリティの世界を読み解くための参考として戦いの原理・原則について簡単に解説しています。その後、それらに示された手順に従って、適切なセキュリティ対策を講じていくためのポイントを順に解説していきます。

・１章では、戦いとサイバーセキュリティの関係性と併せて、サイバーセキュリティを読み解くのに戦いの原理・原則を活用できる根拠とその有効性を説明します。
・２章と３章では、軍事組織が戦い方（作戦）を決定する時に使用する要素と手順を説明します。
・４章では、セキュリティ対策を検討する上で不可欠な脅威とサイバー攻撃に関する理解を深めるため、戦いの原理・原則の手法を活用し、攻撃者の目線で各種サイバー脅威及び攻撃手法を分析する方法を提示します。
・５章では、戦いの原理・原則における意思決定フレームワークを活用し、適切なセキュリティ対応の考え方や実践におけるポイントを提示します。

● 免責事項、注意点など

・このドキュメントは単に情報として提供され、内容は予告なしに変更される場合があります。
・本書の記載内容を、発行元の許可なく複写や転載することを禁じます。引用に関しては、引用部分を明確に区別し、出典を明記することで、著作権法の範囲内で行うことが認められます。これらの条件を遵守しない引用や転載は、著作権侵害となる可能性がありますのでご注意ください。
・このドキュメントに誤りがないこと、商品性または特定の目的への適合性に関する明示的または黙示的な保証や条件は一切ないものとします。
・本書に記載の内容は、作成者の見解に基づいております。独立行政法人情報処理推進機構、産業サイバーセキュリティセンター及び作成者の所属企業等の意見を代表するものではありません。
・本書の利用によるトラブルに対し、本書作成者ならびに関係者は一切の責任を負いません。
・本書では、過去に発生したサイバー攻撃の事例を適宜参考にしていますが、これらを解説する場面においては、サイバー攻撃者の意図を読み解く目的で主観的な推測を含んでいます。
・生成 AI 画像を使用している場合は、生成元を明記しています。
・本書表紙、P33～P38 及び「別紙第２」で使用しているアイコンは DALL･E3 で作成しています。

目次

第１章

まえがき

- この章では、私たちがこの課題に取り組んだ背景について説明します。
- セキュリティ対策を適切に行うためには、私たちが相対する「サイバー攻撃とセキュリティ」というものの本質と力学を正しく認識することが重要ですが、様々な要因からそれは難しいのが実情です。
- まずはサイバーというものを理解するのが難しい理由を理解し、どのようにこれを紐解いていくのかについてイメージアップしましょう。

１．１　サイバーセキュリティが理解困難な背景

サイバーセキュリティはビジネスの一部であるため、考慮すべき要件が非常に多く複雑です。さらに、ＩＣＴをはじめとする各種テクノロジーの上に成り立っていることから、取り巻く環境の変化が速く、これらの技術的な側面を理解していくことが必要です。

また、サイバーセキュリティは攻撃する側と防御する側の相互作用である一方、攻撃側の情報が断片的で不確実なこともあり、多くの人にとってサイバーセキュリティは理解するのが困難となっています。

・ＩＣＴテクノロジーは長い人類の歴史の中では始まったばかりであり、その進化は日進月歩、技術革新も頻繁に起こっています。セキュリティ中核人材はこれらのテクノロジーに関する専門的かつ幅広い知識が必要です
・ビジネス上の目標を達成するため、情報資産、サイバー脅威、セキュリティリスク、法規制等を考慮し、予算や人的リソースを割り当て、技術的な課題に対応しなければなりません。セキュリティ中核人材にはあらゆる側面の知識が必要です
・法規制上、私たちがサイバー攻撃をする側に回ることは許されていないため、敵対者の行動原理に関する研究は受動的にならざるを得ません。特に我が国ではその傾向が顕著で、「誰と争っているのか」意識せずに取り組みがちです
・サイバー攻撃も防御も、無形のデータの応酬が主体であり、その成果や影響を目に見える形で確認し、評価し、イメージアップするのは困難です

このような背景から、サイバーセキュリティはそもそも理解しづらい構造を有しているものと考えられます。

また、業務を行う上での前提として専門的な知識が必要なことから、企業や組織における人材育成や教育・トレーニングは知識や技術の習得がゴールとなってしまっている例が多く見受けられます。

よって、サイバーセキュリティには、①前提となる専門知識の理解、②サイバーという競争社会で戦うための知識の理解、③仮想空間上で行われる目に見えない争いという３つの壁が存在しているものと考えられます。

本書では、「戦い」という現実世界の話を活用して③の壁を乗り越え、①と②の理解を手助けできるように工夫しています。

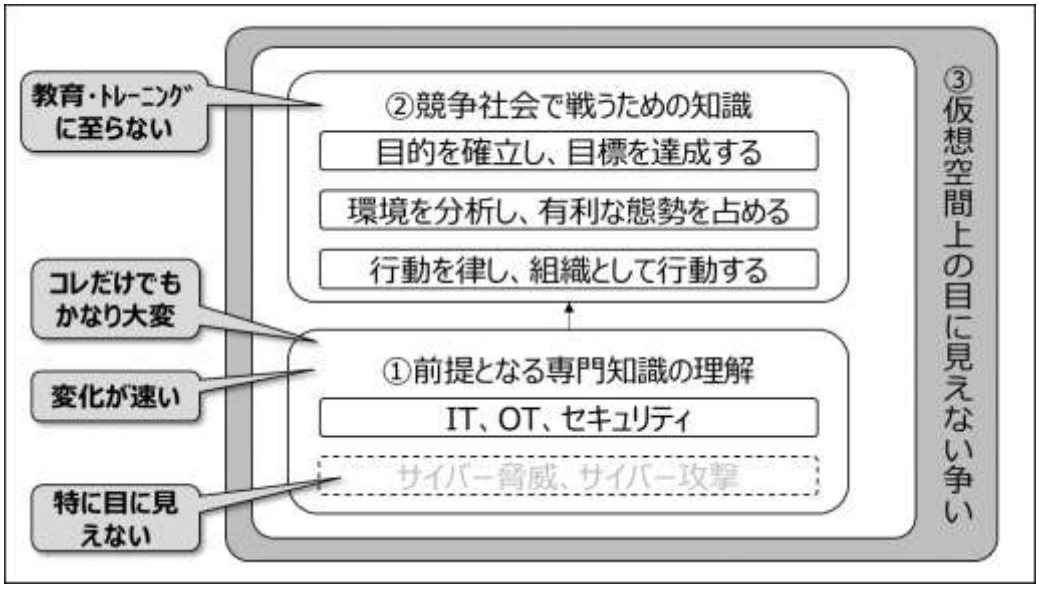


Fig1. サイバーセキュリティを理解するための壁

１．２　「戦い」とサイバーセキュリティの関係性

戦いとサイバーセキュリティの最大の共通点は、「意思を相反する自己と他者の争い（戦い、競争）である」ことです。

普段、何気なく仕事をしていると忘れてしまいがちですが、私たちの活動はサイバー攻撃によって不正に利益を獲得したり他者を陥れたりしようとする何者かから組織を守るためのものであり、目には見えなくとも敵対者が存在しています。

そのほかにも、戦いとサイバーセキュリティの共通点は多数考えられることから、本書ではサイバーセキュリティを理解するための教材として「戦いの原理・原則」を活用しています。

・組織としての大きな目的を達成するための手段として使われます
・対応方法を決める時には、自己・敵対者・周辺環境など様々な要素を考慮します
・コストパフォーマンスは、適切性の評価における重要な指標です
・敵対者との相互作用のみでなく、組織内の統制・ガバナンスも重要な要素です

逆に、サイバーにおける物理的な影響、特にあらゆるものが質量を持たないデータであり距離的な影響が少ない点については違いがあることに注意が必要です。

さらに、戦いでは状況に応じて攻撃的な行動と防御的な行動を選択又は組み合わせることができますが、サイバーの世界では攻撃的な行動が法令で禁止されているため、戦いの観点では非常に不利な状況とも言えるでしょう。このため、組織的な活動や協力体制の構築、防御側の強みを追求することが非常に重要となります。

※サイバーセキュリティの定義には「悪意によるサイバー攻撃への対策」以外にも、いわゆる「自損事故・管理不良などへの対応」を含むのが一般的ですが、本書ではその点をクローズアップした分析・解説は行っておりませんのであらかじめご了承ください。

１．３　なぜ、「戦いの原理・原則」を活用するのか

本書で戦いの原理・原則に着目する理由は以下の３点です。
① 大昔から練り上げられた「競争を有利に進めるための教え」である
② 戦いだけでなく、組織間のあらゆる競争にも適用可能な包括的なものである
③ 現実世界で発生する分かりやすい事象であり、イメージアップしやすい

「孫子」をはじめ、戦いの原理・原則と呼ばれるものは世の中に多数存在しています。人類の歴史は戦いの歴史であるといっても過言ではなく、古くは紀元前から研究と編さんが行われてきた歴史があり、現代でも「軍事学」などとして多くの国が研究・開発を行ってきました。

当然のことながら戦争で失敗すると多くの人が死に、国が亡ぶことに繋がります。このため、これらの原理・原則は国の存亡をかけて開発されたものであり、それだけ信頼性が高く、洗練されていると言えるでしょう。

また、戦いの原理・原則は極めて包括的なものからシチュエーションごとの詳細な方法論まで幅広く存在しており、このうち包括的なものは軍事的な戦争や戦闘のみならず、広くビジネス社会における企業間の競争から個人間の争いにまで応用することが可能な概念として取りまとめられています。

これらは、サイバーの世界における競争（サイバー攻撃とサイバーセキュリティ）にも適用でき、目線を変えて考えてみれば、世に言われている「適切なサイバーセキュリティ（やサイバー攻撃）」も、概ねこの概念に則っていることが分かります。
※マイクロソフト創業者のビル・ゲイツ氏をはじめ「孫子」をビジネスに応用している経営者は多く、解説書や解説動画も多数公開されています。

最後に、戦いは現実世界の出来事であるため、誰しもがその力学やアクション、結果と影響をイメージアップしやすいことが挙げられます。悲しいことですが、国家間の紛争やテロ事件は古くから現在に至るまで世界中で発生しています。

サイバーセキュリティも最終的には現実世界に影響を与えるために行われる手段ですが、そのほとんどは目に見えないサイバー空間の中で行われるため、ＩＴやサイバーセキュリティ上の用語だけでは理解しづらく伝わらない事が多々あります。

その結果、何のためにやっているのか、状況がどうなっているのか、それをやるとどうなるのかといった肝心な情報は、専門用語の理解に頼るか何らかの例え話に頼らざるを得ません。

このような理由から、本書では米軍や自衛隊でも取り入れられている「戦いの原理・原則」の中から、最も包括的で組織間のビジネス競争にも十分に適応可能なものをピックアップし、理解が難しいサイバーセキュリティの各種要素を紐解いていくこととしました。

第２章

戦いの原理・原則を理解する

（METT・９原則）

- 第１章では、サイバーセキュリティの世界が複雑であり理解が難しい理由と、それを理解するために現実世界で実際に起こっている事象「戦い」に着目する理由を説明しました。
- サイバーセキュリティの世界でも、各種フレームワークやガイドラインで取り上げられ、社内教育やトレーニングで言われているとおり、適切なやり方（あるべき論）が存在します。
- この章では、この「サイバーセキュリティ（やサイバー攻撃）のあるべき姿」をより深く理解するための教材として、戦いの原理・原則のうち、METT と９原則について解説します。

２．１　全体像

第一章でも触れた通り、人類の歴史は戦いの歴史と言っても過言ではなく、これまでに多くの戦争や紛争が起こってきました。そこで、多くの軍事組織は戦争に勝つための方法を必死で研究し、それを受け継ぎ・改良してきました。

戦いの原理・原則は色々な種類がありますが、本章ではサイバーセキュリティに適用できるよう、最も包括的な以下の二つを紹介します。

・「ＭＥＴＴ（メット）」・・・戦い方を考え、意思決定するための要素
・「戦いの９原則」・・・・・・戦いにおいて部隊が適合すべき要件

「ＭＥＴＴ」は、組織としての行動方針を考え、意思決定するためにあらかじめ必要な情報（インプット）を表したものです。一方、「戦いの９原則」は、実際に戦闘を行う部隊が組織として力を発揮し、有利な態勢を占めるために必要な条件を表しています。それぞれ観点が違うことに注意が必要ですが、いずれも組織が競争に勝つ（負けない）ための本質や普遍の法則をまとめ、継承されてきたものです。

即ち、私たちが何かの意思決定を行うときには、METTの各要素にあたる情報を収集・活用するとともに、戦いの９原則に適合した活動を行うことによって、より良い結果を得ることができると考えることができます。

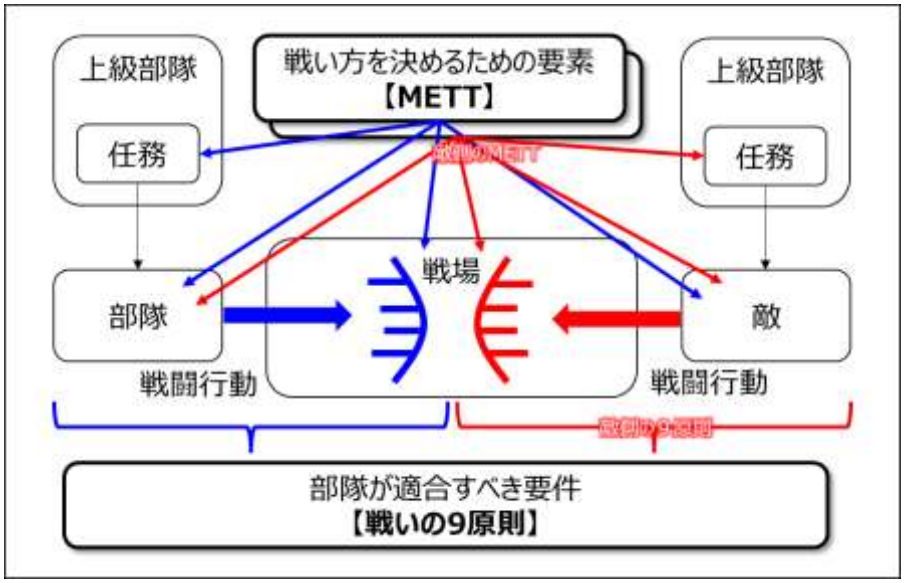


Fig2. METTと戦いの９原則の関係性

２．２　戦い方を決めるために必要な要素「METT」

> 彼を知りて己を知れば、百戦して殆うからず。
> 彼を知らずして己を知れば、一勝一負す。
> 彼を知らず己を知らざれば、戦う毎に必ず殆うし。

これは、「孫子」の有名なフレーズで、戦いにおいて負けないためには自分のことだけでなく敵のことを理解する必要があると説明しています。METTは脈々と続くこの言葉の派生形とも言えます。

METTでは、戦い方を決めるために　①目的と組織の任務（Mission）、②敵の状況（Enemy）、③地形と気象（Terrain＆Weather）、④部隊と友軍の支援（Troops＆Support）の４つの要素が必要であるとされています。

平地、市街地、山、海、砂漠など全く違う様々な特性のある戦場において、相反する意思を持つ敵と我の勢力が戦闘を行う場合、一つの意思決定や行動のミスが取り返しのつかない結果（≒敗北）に繋がります。

このため、軍事組織では戦い方を意思決定する際はあらゆる手段を使ってMETTで示されているような情報を収集・分析します。逆に言うと、どれか一つの情報要素が欠落していたり、間違ったりしていた場合、そこから出た意思決定（≒作戦）は適切ではない（≒失敗する）可能性が高くなると言えます。

サイバーセキュリティの世界でも、組織のセキュリティポリシーやセキュリティソリューション、インシデント発生時の動き方など様々な意思決定が存在します。

組織が適切な意思決定とセキュリティ活動を行っていくためにはどのような情報要素が必要なのか、そしてそれらに基づいて意思決定することの重要性を改めて理解しましょう。

２．２．１　Mission：目的と任務

意思決定に必要な要素の１つ目は、「目的と任務」（Mission）です。

私たちは今、具体的にどう行動するかを意思決定しようとしています。私たちが行うアクションはすべて組織としての目的や目標に合致していなければ意味がありません。このため、まず初めにこれを理解することが最も重要です。

- 組織はなぜこの戦闘を行おうとしているか
- 組織は私たちに何を期待しているか

これから行う意思決定は、これらの目的と目標を達成できる幅の中で行う必要があり、その「幅」の中で具体的な選択肢のどれを採用するかを決定します。逆に、どんなに条件が良く、利益が大きくて損害が少ない選択肢があっても、この「幅」を逸脱するようなアクションは選択肢に挙げるべきではありません。そのような行動は組織としての統制を乱し、大きな失敗につながる可能性があるため、アイデアとして提案する程度にとどめるのが適切でしょう。

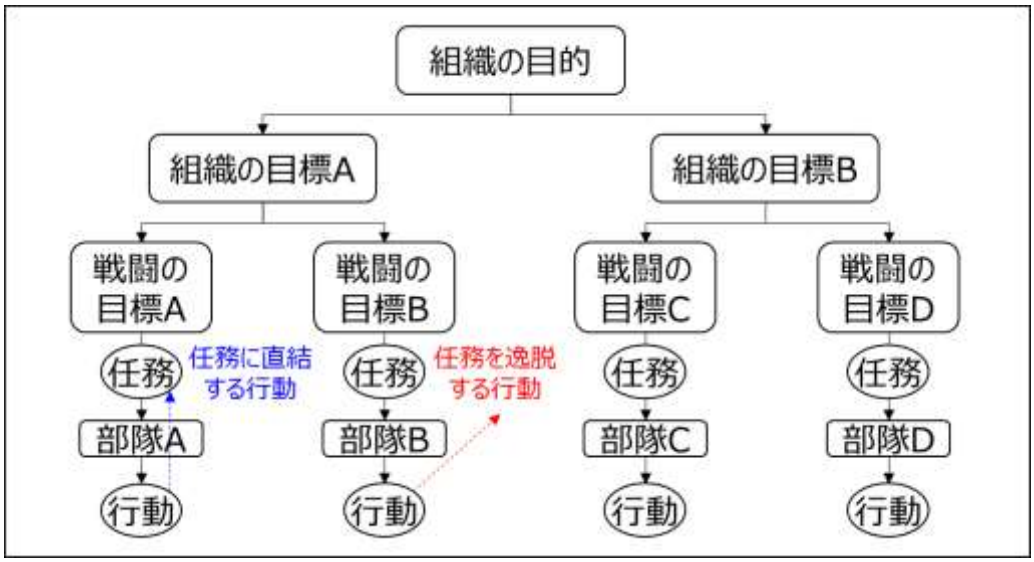


Fig3. 戦闘における目的、目標と任務

組織活動の一つであるサイバーセキュリティそのものにも「ビジネスに必要な情報資産を保護する」という大きな目的があり、そのための個々の活動にもそれぞれに目標が存在するはずです。

私たちは、検討している事業やアクションが間違いなく目標に向かっているか、組織としての目標達成に直接貢献することができるか、常にチェックする姿勢が求められます。

２．２．２　Enemy：敵の状況

意思決定に必要な要素の２つ目は、「敵の状況」（Enemy）です。

戦闘では、直接的又はそうでないにせよ必ず相手（敵対者）が存在します。対人格闘で例えるなら、相手が右利きであれば右からの攻撃を警戒する、攻めるときは左からなど、相手が右利きであることを意識した戦い方をしないと負けてしまいます。
当然のことながら、相対する敵の特性や状況は、戦い方を意思決定する上で非常に重要な要素であるといえます。

- 敵の戦力の規模や構成（どのような兵器を有するか）
- 所在する位置や準備状況
- どのような戦い方をすると思われるか

しかし、敵も私たちと同じように意思を持つ生き物であり、戦いを有利に進めるために情報を秘匿し欺こうとします。また、敵の状況は他の要素のように確かなものではなく、自ら情報収集しなければ勝手に集まってくることもありません。
よって、敵の状況という要素はMETTの中でも最も扱いや収集が難しいものですが、だからこそ部隊はあらゆる手段を使って敵の情報を集め、その真偽や確実性を検証して、戦い方を意思決定するために使用します。

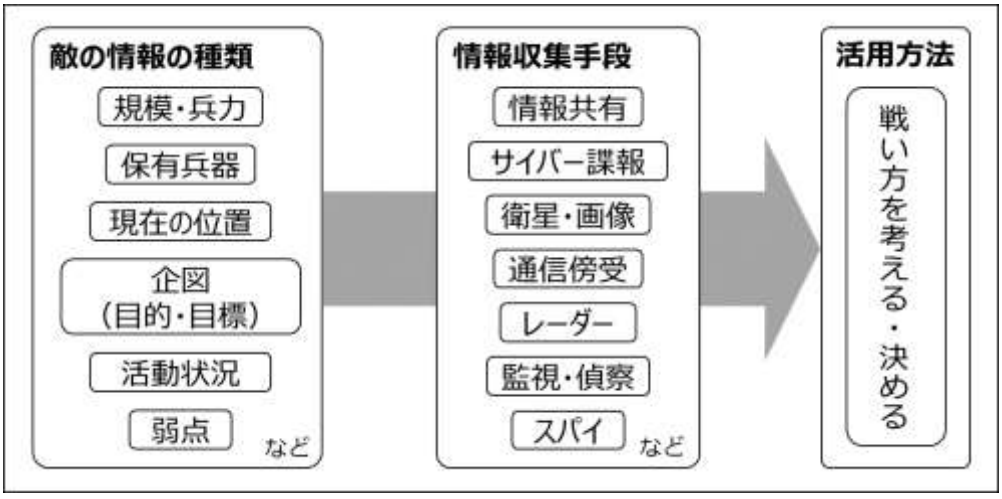


Fig4. 敵の情報の種類と情報収集手段

サイバーセキュリティにも必ず敵対者（＝サイバー攻撃者、サイバー脅威）が存在するため、意思決定の重要な要素であることは間違いありません。
しかし、サイバーセキュリティの難しい点の一つは、防御側からは攻撃者の姿が全く見えず、予想が難しいことです。反対に、攻撃者側はオープンな世界に晒された防御側の情報を自由に閲覧し、正体を秘匿して情報収集を行うことができます。
サイバーの世界では情報収集能力や「情報の量・質」に差が出やすいため、勝敗を決定づける最も重要な要因であるといっても過言ではないでしょう。

２．２．３　Terrain＆Weather：周辺環境

意思決定に必要な要素の３つ目は、「周辺環境」（Terrain＆Weather）です。

正確には、METTでは地形と気象を意味しますが、ここでは最終的にサイバーセキュリティの活動に置き換えてイメージアップするため「周辺環境」としています。戦闘が行われる地域の特性を表すものであり、組織のビジネス環境（ステークホルダー、法規制など）を含むものと考えられます。

戦闘が行われる地域は「戦場」と呼ばれています。ご存じの通り、戦場を形成する地形・気象は森羅万象にわたり、数えたらきりがありません。

- 陸、海、空、宇宙、電磁波、サイバー
- 平地、丘陵、山岳、砂漠、市街地、湿地、・・・
- 広大、狭小、縦長、横長、扇状地、凹地、凸地、・・・
- 晴れ、曇り、雨天、無風、強風、温暖、寒冷、高温、乾燥、多湿、・・・

戦い方を決めるうえで地形・気象が重要な理由は、それらが「力強い味方」にも「恐るべき敵」にもなり得るからです。神風によって日本が勝利した「元寇」や、断崖絶壁から奇襲攻撃を成功させた「一ノ谷の戦い」など、地形・気象が勝敗に直接作用した例は少なくありません。

て、地形・気象をはじめとした周辺環境に適合した戦い方を立案するのはもちろんのこと、それらを強みとして最大限利用した戦い方こそ最良と言えるのです。

Table1. 戦場の地形・気象に適合した戦い方

区分	種別	変化する特性	適応の仕方
領域	陸／海／空	物理的な特性	用いる兵器や行動が変わる
地形	平地／山地 ／市街地	広さや視界 遮蔽物の有無	部隊の集結や分散 隠れ蓑や弾避けとして利用
	河川・湖	移動の容易性	戦車や車両の移動を制限
気象	天気	行動の容易性、地盤の強さ	航空機の運用可否
	気温	人間の生活環境 水の形状	服装、宿営方法、活動条件 凍ると陸地に近づく
	風	臭い、煙、弾丸の動き	煙幕、化学兵器等の使用 弾道の計算・修正

サイバーに地形・気象の概念はあまり関係ありませんが、企業が行動する上では経済的な活動基盤や社会とのつながり等がこれに該当すると思われます。

軍事組織が地形・気象から戦い方に対して大きく影響を受けるように、社会情勢、顧客、サプライチェーン、地元自治体や監督省庁、さらに関係法令などは企業の活動に多大な影響を与えます。このため、組織がサイバーセキュリティに関わる意思決定を行う際は、企業を取り巻く周辺環境が自分たちの行動に及ぼす影響と、自分たちの行動が周辺環境に及ぼす影響の両面を考慮することが重要であると言われています。

２．２．４　Troops＆Support：部隊と友軍

意思決定に必要な最後の要素は、「部隊と友軍」（Troops＆Support）です。

部隊と友軍は、意思決定に基づいて実際にアクションを行う実行部隊のことを差します。具体的には、我が部隊の規模や構成、能力など、２つ目の要素である「敵の状況」と同じようなものについて自分たちのことを分析します。ここで重要なのは、この要素が「意思決定したアクションを行う主体である」ということです。

自分の能力を見誤り、本来達成不可能な目標を立ててしまった場合、その作戦は失敗する可能性が極めて大きくなります。俗にいう「無謀な作戦」です。このため、保有するリソースや戦力、能力などについては、努めて客観的かつ詳細・緻密に分析することが重要です。

- 規模や構成は努めて計数的に把握する
- 士気や練度、団結力など、個々の属性や無形の要素についても把握する
- 敵との相対評価を適切に行う（過小評価／過大評価しない）

Fig5. 部隊の能力や特性に応じた戦い方

軍事組織では、これらの要素を戦闘ごとにいちいち分析するのではなく、日々の活動や訓練の中で評価し、常に最新の情報を維持しています。部隊の練度向上と併せて、能力の把握が教育・訓練の目的だと言っても過言ではないでしょう。

友軍の支援も戦い方を決める重要な要素です。強大な友軍が存在する場合、その戦力を決定的なピース、決め手として考えることが可能だからです。

サイバーの世界では、業種・業界、事業規模やシステム構成など、自組織の特性や能力にあたる要素がこれに該当すると考えられます。サイバーセキュリティのためにどのような組織や人材を保有しているか、どの程度の予算を投入できるか、どのようなセキュリティアセットや機能を運用できるかは、意思決定を行ううえで非常に重要なポイントとなります。併せて、ISAC、業界団体などとの情報共有や連携は企業にとって強力なサポートとなります。友軍として最大限に活用できるようにしていきたいものです。

２．３　戦いにおいて部隊が適合すべき要件「戦いの９原則」

戦いの９原則は、戦闘を行う部隊が組織的に行動し、敵に対して優位な態勢を占めるために適合すべき要件であり、勝敗や優劣にも大きな影響を及ぼします。

戦闘では、組織として統制のとれた行動を行い、我の強みを活かし、敵の弱点を突くことが鉄則です。９原則はこれを行うための要件だと言えるでしょう。

また、９原則は攻撃／防御のいずれにも適用できる共通的な概念のようなものであり、これから派生した攻撃／防御それぞれ、また、個々のシチュエーションごとの原則も存在します。

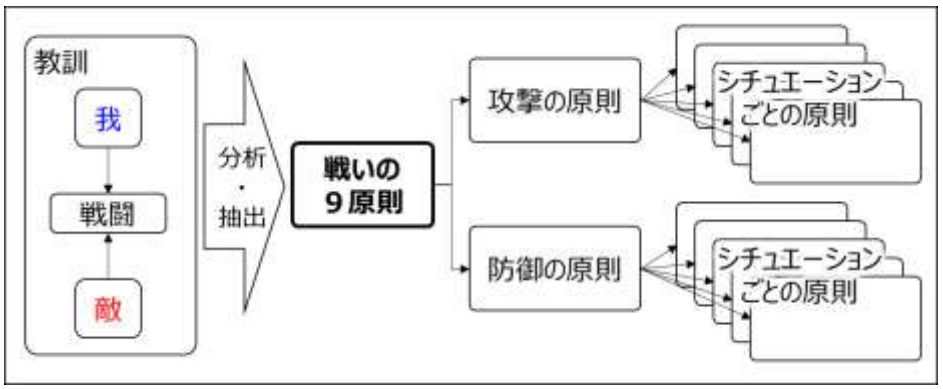


Fig6. 戦いの９原則の全体像イメージ

ここでもう一つ重要なのは、各原則はMECE（漏れや被りがない状態）ではなく、相互に関係性が存在するということです。

- 組織運用に関する原則（目標、統一、簡明）
  → 組織として統制のとれた行動をするための方法を示す
- 態度に関する原則（主動）
  → 組織としての活動スタンスや姿勢を示す
- 戦法に関する原則（集中、節用、機動、奇襲、保全）
  → 部隊の運用方法や行動方法を示す

よって、ある場面においてどれか一つの原則に適合すればよいという訳ではなく、戦いが始まる前から終わるまでの全局面で各原則を意識し、組織としてこれに適合した戦い方をすることが必要となります。

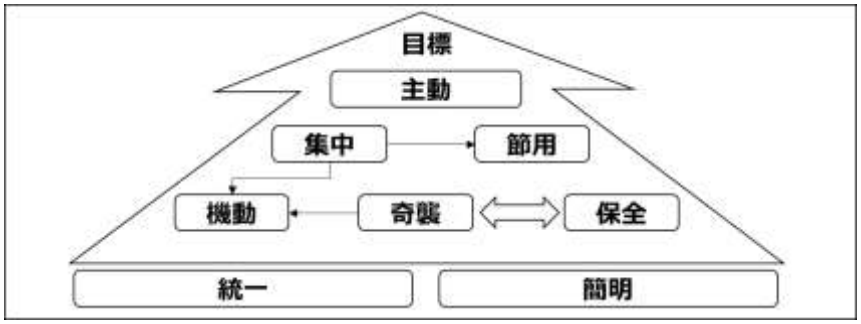


Fig7. 戦いの９原則相互の関係性イメージ

２．３．１　目標の原則（Objective）
→　組織として達成可能な目標を確立し、その達成のために努力を集中する
２．３．２　主動の原則（Offensive）
→　敵の先手を取り、主導権を維持する
２．３．３　戦力の集中の原則（Mass）
→　重要なポイントに対しては出し惜しみせず、戦力を集中的に投入する
２．３．４　兵力の節用の原則（Economy）
→　重要なポイント以外では、リスクを覚悟して必要最小限の戦力で戦う
２．３．５　機動の原則（Maneuver）
→　スピード感を持ち、臨機応変かつダイナミックに行動する
２．３．６　統一の原則（Unity）
→　指揮・統制系統を一本化する
２．３．７　奇襲の原則（Surprise）
→　敵の意表を突き、敵が予想していない行動により、対応のいとまを与えない
２．３．８　保全の原則（Security）
→　敵に有利な情報を与えない
２．３．９　簡明の原則（Simplicity）
→　作戦や行動はシンプルにする

※それぞれの原則の詳細な解説については、本文書の末尾に別紙として収録しています。過去の戦いにおける事例やサイバーセキュリティに置き換えた場合の事例などを用いて努めて分かりやすく表現しています。過去の戦いはなぜ失敗（成功）したのか？サイバーセキュリティのよくある失敗談（成功談）は、どの原則に適用できていなかった（していた）のか？ケーススタディを通して理解していきましょう。

別紙第１「戦いの９原則の解説」

戦いとサイバーセキュリティの関連性、類似性、近似性については第１章で述べた通りですが、敵対者・周辺環境との相互作用性や組織的に行動する観点から、サイバーセキュリティにおいても本質的にはこの原則に則った行動をとることは概ね適切だと考えられます。

各原則の解説では、サイバーセキュリティに置き換えた場合のケーススタディを紹介していますが、おそらくほとんどが「そんなの知ってるよ」「当たり前だ」と感じると思います。

なぜなら、それらは私たちが日ごろから触れているサイバーセキュリティの常識やお作法であり、フレームワークやガイドラインで「適切なあるべき論」として普及しているものと近いからです。これこそが、戦いの原理・原則がサイバーセキュリティに適用可能だと考え、紹介している最大の理由です。

２．４　軍事における情報の重要性

お気づきの方もいらっしゃるかもしれませんが、METT は情報（Input）そのものであり、戦いの９原則は適切な情報があって初めて成り立つものです。

・適切な情報が無いと、組織の目的に合致し、達成可能な目標は確立できません
・敵の弱点を突くことが重要ですが、情報がなければどこが弱点かわかりません
・防御では自分の弱点を守る必要がありますが、どこが弱点かわからなければ守りようがありません
・勝敗を決する重要なポイントに対して戦力を集中し、その他では節用することが望ましいですが、情報がなければどこが重要か見分けが付けられません

一般社会が情報化社会と言われ始めるのと時を同じくして、米軍をはじめとした軍事組織においても NCW（Network Centric Warfare：ネットワーク中心の戦い）の概念が確立し、より早く正確な情報を共有することで意思決定を迅速に行い敵に対して有利な態勢をとる戦い方が主流となっています。

このため、軍事組織はとにかく情報の収集や取り扱いにかなり力を入れています。偵察隊や情報部隊など情報の収集・分析を任務とする部隊が多数存在し、それ以外の部隊にも情報収集と報告は必ず任務として付与されます。斥候やスパイなどは、危険を冒して敵国や敵陣地内まで潜入し、情報を集めます。

また、情報を収集するためのセンサー～情報を分析するシステムや部隊～意思決定を行う司令部～戦闘を行う部隊の間はネットワークでつながれ、リアルタイムで情報をやり取りするシステムが構築されています。

反対に、このような情報ネットワークを切断して敵の意思決定や戦闘を妨害するという戦術も普通に行われています。（その手段の一つがサイバー攻撃です）

企業においても、経営戦略、商品販売やマーケティングなど他者との競争の世界では軍事組織と同じように情報を意識した活動が行われているのではないでしょうか。

情報の重要性はサイバーセキュリティでも同じです。より早く正確な情報を入手し、適切な戦略と戦術を立て、実行することが求められます。全てのアクションは情報から始まるのです。

第３章

戦いの原理・原則を理解する

（意思決定プロセス）

- 組織のセキュリティポリシーや戦略の立案、セキュリティ対策の検討と実装、セキュリティインシデント対応は、どのように行っていくのが適切でしょうか。
- これらはセキュリティフレームワークなどでも取り上げられているトピックですが、本書ではその背景や理由をイメージアップし、理解するための考え方を提供します。
- この章では、戦いの原理・原則のうち「意思決定プロセス」を解説し、他者との敵対関係における意思決定のポイントを理解します。

３．１　全体像

私たちがセキュリティ対応に迫られるときには、様々なトリガーがあります。

・組織や関係企業がサイバー攻撃を受けた
・機器の脆弱性が発表された
・業界のガイドライン、法規制への対応
・顧客や株主への説明
・上司から指示された

これらは、組織としてのセキュリティ対応方針を検討するような大きな場面も想定されますが、現場で行う個別的な対応などの局所的な場面も想定されます。

この際、それぞれの一場面のみを切り取って場当たり的に対応することもできますが、それが適切なセキュリティ対応と言えるでしょうか。長期的な運用パフォーマンスや全体的な効果、限られたリソースに応じた優先順位付けなど、考慮すべき要件は数多く存在します。

この章では、戦いの原理・原則のうち軍事組織が戦い方を考え、決定するための概念フレームワーク「意思決定プロセス」を参考にして、サイバーセキュリティの各場面における考え方のロジックと具体例を解説します。

「意思決定」と聞くと、経営層が組織全体の指針などを決定する場面を想定しがちですが、このロジックは担当者が個別のセキュリティ業務案件について検討する際にも共通の考え方であり、もっと言うと私生活における人間関係にも十分適用可能な強力なツールです。

意思決定プロセスの概要、各フェーズの目標・実施事項、サイバーセキュリティに置き換えた場合のイメージは表のとおりです。

Table2. 意思決定プロセスの概要

	１：任務の分析	２：作戦環境の分析	３：敵の分析	４：作戦の立案
目標	状況を理解し、達成すべき目標を特定する	戦場の状況など、戦いに影響を及ぼす要因を特定する	敵対者の目標と予想される行動を特定する	ここまでに特定した要因から、今後の行動方針を意思決定する
戦いにおける実施事項	●彼我の目的の分析 ●戦場の特定 ●彼我の戦力の比較 ●作戦方式の決定 ●作戦目標の確立	●地形の分析（重要地形の特定） ●気象の分析（影響と対応の決定）	●敵の目標の分析 ●敵がとり得る行動の列挙・分析 ●各行動の妥当性の評価	●行動方針の列挙 ●行動方針の比較・分析 ●行動方針の決定 ●作戦の立案→実行
サイバーセキュリティに置き換えた場合	●ビジネス目標の分析 ●組織に対する脅威の特定 ●セキュリティの目標の確立	●ビジネスプロセスの特定 ●情報資産・脆弱性の特定 ●現時点のセキュリティ態勢の把握 ●保護すべき情報資産の特定	●サイバー攻撃の目標（脅威事象）の特定 ●起こり得るサイバー攻撃シナリオの列挙 ●各シナリオの発生可能性の評価	●セキュリティ対策の列挙、比較、決定 ●セキュリティ対策の実装、運用、（インシデント対応）

簡潔に言うと、「目標は」→「環境は」→「相手は」→「どうするか」の流れになります。重要なのは、このプロセスが敵との戦い方を考え、決めていくための基本的なフレームワークであるということです。

組織がサイバーセキュリティの対策を検討・実装していくためのプロセスはいくつも存在しますが、これらを正しく理解し使いこなしていくためには、他者との敵対関係における意思決定のポイントを押さえておく必要があります。

３．２　METT・９原則との関係性

意思決定プロセスの各フェーズを見ると、第２章で紹介した METT と非常に似ていることに気づくかもしれませんが、ＭＥＴＴの各要素が意思決定プロセスの各フェーズという訳ではありませんので、注意が必要です。

・METT はあくまで「意思決定するための要素（情報）」です。意思決定の各フェーズで参照するものであり、フェーズそのものではありません
例えば、「任務の分析」フェーズでは部隊が達成すべき具体的な目標を決定するために、METT 全要素の表面的な情報を分析します
・９原則は「部隊が適合すべき要件（ガイダンス）」です。具体的には、最終フェーズで立案した作戦を実行に移す際、作戦指揮官が部隊を統率・運用する時に適用すべきものです

３．３　戦い方を検討・決定する手順「意思決定プロセス」

それでは、軍事組織が戦い方（作戦）を決めていく手順とポイントをフェーズごとに見ていきましょう。

３．３．１　Phase-1：サイバーセキュリティの目標を決める（任務の分析）

このフェーズでは、部隊と敵対者（「彼我」（ひが）と言います。）が置かれている状況を分析・理解し、部隊が達成すべき目標を特定します。

・部隊と敵対者の意図や目的を明らかにする
　－組織全体としての目的は、通常上級指揮官から示される
　－敵対者の意図・目的は、様々な情報や兆候から推測する必要がある
・意図・目的から、予想される戦場を特定する
・それぞれが保有する戦力を分析・比較し、強みや弱点を明らかにする
・状況を踏まえて、作戦方式を決定する
　－例）防御の後、味方の増援を待って攻勢に転じる／攻撃によって敵を撃破した後、特定地域を防御・確保する　などが考えられる
・部隊が達成すべき具体的な作戦目標を確立する
　－例）ＭＭ月ＤＤ日ｈｈ時まで敵の攻撃から防御し、＊＊＊地域を確保する
　などが考えられる

サイバーセキュリティに置き換えた場合、組織としてのビジネス目標と組織に対する脅威を特定し、セキュリティの目標を確立することに相当します。

サイバーセキュリティは組織のビジネス目標を達成するために行うものであり、組織に対する様々な脅威のうち、情報資産に対する脅威や情報資産に起因するリスクを低減することが目的と言えます。

始まりにあたるこのフェーズでは、組織のビジネスにおける資産とそれに対する脅威を特定し、どのリスクをどの程度低減するのかを明確にしておくことが必要です。

３．３．２　Phase-2：組織の資産と環境を分析する（作戦環境の分析）

このフェーズでは、予想される戦場の環境など、戦いに影響を及ぼす各種要因を把握・分析し、彼我にとって最も価値の高い地形（≒敵にとっての攻撃目標／組織にとっての守るべき目標）を特定します。

・戦場となる地域の地形特性を把握・分析し、戦いにおいて重要な意義を持つ場所を特定する
　－例）一帯を見晴らすことができる高所は彼我にとって価値の高い目標であり、
　　部隊の移動を制限する河川は戦術を検討する上で重要なポイントとなる
・戦闘が予想される時期の気象特性を把握・分析し、彼我の作戦行動に及ぼす影響を特定する
　－例）気象によっては部隊の行動が助長／制限されるため、これを予期して作戦を立てる必要がある

サイバーセキュリティに置き換えた場合、「戦場」は組織を中心とした情報システム・ネットワークであると考えられることから、リスク分析プロセスのうち「情報資産・脆弱性の特定」がこれに該当します。

併せて、ビジネス市場、顧客、取引先、法規制など組織のサイバーセキュリティ活動に影響を及ぼす外的要因についても把握しておくことが重要です。

３．３．３　Phase-3：組織に対する脅威を分析する（敵の分析）

このフェーズでは、敵対者の作戦目標を特定するとともに、具体的な行動を可能な限り正確に予測・評価します。

部隊のリソースは限られており、考えられる敵の行動全てに満足な対応をすることは不可能なため、何らかの優先順位に基づいてリソースを配分する必要があります。

効率的に部隊を配置・運用（攻撃であれば、敵がいないところを攻める／防御であれば、敵が来るところを守る）するため、このフェーズは極めて重要です。

・敵の作戦目標を特定する
　－例）ＭＭ月ＤＤ日ｈｈ時までに、＊＊＊地域で防御する我が部隊を撃破　など
・目標達成のため、敵が取り得る作戦行動（敵の可能行動）を列挙する
　－例）攻撃の経路、使用する兵器、攻撃開始の時期、使用する戦法　など
・敵の可能行動を評価し、採用の可能性（採用公算）を評価する
・敵の可能行動のうち、部隊の任務達成に重大な影響を及ぼし得るものを特定する

ですが、敵の行動を予想するのは難しい作業です。このため、軍事組織では以下の 2 点を重視して可能な限り正確な予測に努めています。

・情報の収集、評価に力を入れる
　－軍事組織には情報の収集や分析を扱う専門の部隊が多数存在し、作戦を情報によって決定していく文化が定着している
・敵の行動は、敵の視点に立って検討、予測する
　－我が部隊側からの視点だけでは、敵の表面的な部分しか見ることができない
　－METT を活用した「意思決定プロセス」を敵の立場で分析する

サイバーセキュリティに置き換えた場合、リスク分析プロセスのうち「脅威の特定」がこれに該当します。

組織に対してサイバー攻撃を仕掛けてくる脅威アクター、攻撃シナリオ、使用されるテクニックを特定し、リスクが顕在化する可能性を評価します。（被害事象ベースのリスク分析手法では、組織として許容できない事象から逆算的にサイバー攻撃シナリオを特定）

敵の行動を予測するのが難しいように、サイバー攻撃シナリオの発生可能性を予測するのは非常に困難であり、サイバーセキュリティにおける永遠の課題とも言えます。そのためにセキュリティベンダーのレポートを読み漁ったり、脅威インテリジェンスサービスを活用したり、様々なアプローチがあると思いますが、なかなか理解できていないのが現状ではないでしょうか。

第 4 章では、この悩みを解決するため、敵（サイバー攻撃者）の視点から攻撃シナリオやテクニックを分析・評価する取り組みを通じ、敵の行動に応じた適切なセキュリティ対策につなげるためのアイデアを提供します。

３．３．４　Phase-4：サイバーセキュリティの方針を決める（作戦の立案）

このフェーズでは、ここまでに分析・特定した各種成果を総合して、部隊の具体的な行動方針を決定し、これを軸として作戦計画を立てます。

・部隊の目標を達成可能な行動方針を列挙する
　－例）攻撃の経路、使用する兵器、攻撃開始の時期、使用する戦法　など
・各行動方針を比較・評価する
　－評価の切り口には、容易性（部隊の強みを活かし、敵の弱点を突けるか）、迅速性（目標達成に必要な期間）、リスク（兵員・兵器などの損耗度）などが考えられます。
・行動方針の決定と作戦計画の立案
　－比較・評価結果から、失敗の可能性が最も低いと思われるものを採用する
　－敵の可能行動のうちリスクの高いものに対するケアを検討する
　－採用した行動方針をベースとして、各部隊の配備や動きを組み立てて作戦計画を完成する

サイバーセキュリティに置き換えた場合、セキュリティ戦略の立案やセキュリティ対策の実装・運用、インシデント対応がこれに該当します。

ここでのポイントは、意思決定プロセスの各フェーズで特定した要素（セキュリティの目標、資産・脆弱性、外部環境要因、想定されるサイバー脅威と攻撃シナリオ）を総合的に分析することです。セキュリティ対策やその実装要領は、個別の情報にフォーカスして場当たり的に直感で決めてよいものではないことがイメージできたかと思います。

※サイバーセキュリティにおける意思決定を行うための具体的なポイントの解説は、第５章に記載しています。

コラム１　「ウォー・ゲーム」とペネトレーションテスト

Phase-4「作戦の立案」では、部隊の行動方針を比較・評価し、最も失敗する可能性が低いものを採用します。この際、より正確に比較するために軍事組織が行っている取り組み「ウォー・ゲーム（War-Game）」を紹介します。

ウォー・ゲームは、案出した部隊の作戦計画を使って行う机上シミュレーションのようなものです。敵の行動については Phase-3「敵の分析」で評価した敵の可能行動をベースとし、実際に敵役（レッドチーム）を立て、想定される戦場の地図やジオラマの上で対抗演習を行います。

レッドチームは、敵の兵器の特性・運用方法や戦法、ひいては思想や文化などにも精通した専門家が選定され、真に敵側の気持ちとなって攻防の応酬が繰り広げられます。そうすることによって、案出した作戦計画や予想される敵の行動にある問題点、ミスマッチを洗い出すことができるという訳です。

サイバーセキュリティにも似たような概念が存在します。ペネトレーションテストや敵対的エミュレーションです。
※敵対的エミュレーションは、レッドチーム演習や TLPT（Threat Led Penetration Test：脅威ベースのペネトレーションテスト）とも呼ばれます。

米国のセキュリティ教育機関 SANS によると、敵対的エミュレーションは「セキュリティ専門家（レッドチーム）が、攻撃グループの攻撃手法を使って疑似攻撃を行い、攻撃手法に対する組織のサイバーレジリエンスを向上すること」(1)と定義されています。ペネトレーションテストではシステムとしての堅牢性や防御・検知メカニズムの効果検証までを目的とするため、評価対象スコープはやや限定的とはなりますが、いずれも組織としてのセキュリティ態勢を評価するという意味では、ウォー・ゲームと大いに共通的な部分があると考えています。

せっかく実現・実装した組織のセキュリティ体制も、可能な限り実際的な方法で検証しない限り、その効果や問題点・脆弱点を効果的に発見することはできません。ペネトレーションテストや敵対的エミュレーションが浸透すれば、セキュリティの強化につながるのではないでしょうか。

軍事組織の文化や考え方がサイバーセキュリティに根付きやすい欧米諸国では、ペネトレーションテストや敵対的エミュレーションに対するニーズや意識が高まりやすく、日本に比べて市場が大きいため普及している（≒市場経済の原理からは価格が低い）のではないかと思います。

本書で触れているように、サイバーセキュリティと軍事的な視点やアプローチが融合していくことができれば、私たちがもっと気軽にペネトレーションテスト等を活用できる日が来るかもしれません。

第４章

戦いの原理・原則から

サイバー脅威を考える

- 組織のリスクを正確に分析するためには、組織に対するサイバー攻撃の脅威を具体的に特定することが望ましいとされていますが、これは非常に難しい作業です。なぜなら、私たちはサイバー攻撃者ではないからです。
- この章では、サイバーセキュリティにおける永遠のテーマである「サイバー攻撃の脅威」について、軍事組織の手順を参考にし、敵側の視点で分析・理解するための考え方と手法の一例を紹介します。
- 「誰が、何のために、どのようにサイバー攻撃を行うのか？」
  この問いかけに迫っていくことにより、セキュリティ対策を行う上でのポイントを探していきましょう。

４．１　敵を理解することの必要性

サイバー攻撃の脅威を理解すべきである理由は、以下の２点があると考えられます。

・サイバー空間における「攻撃と防御の全体像」を俯瞰的に理解するため
・サイバー攻撃への対応（セキュリティ）を適切に行うため
　－限られたリソースを有効に活用する
　－攻撃に応じて効果的な防御策を講じる

サイバーセキュリティには、何らかの目的でサイバー攻撃を行う人がいて、それらから組織のビジネスや資産を守る、「他者との敵対関係である」という大前提について述べました。私たちは、セキュリティ対策を考える前にまずはこの本質を正しく理解することが必要です。

そして、ほとんどの組織やセキュリティ担当者には、「セキュリティをやらなければならない」という意識はあるはずです。しかし、実際にやろうとしたとき、やり方に困ったり、適切に実装・運用できていなかったりするケースは多々あるのではないでしょうか。

・リソース（金、人、時間・・・）は有限であり、全部をやることはできない
・様々なやり方が考えられるが、何が適切なのか、具体的にどうすればいいのか分からない

では、何を根拠にして考え、判断すべきなのでしょうか。

サイバーという他者との敵対関係において、私たち防御側の状況や事情だけで物事決めるのは非常に危険です。サッカーや野球をするとき、相手チームの能力や戦術を理解せずに試合をして勝てますか？「孫子」にも記されているように、勝負は運次第か、負けることが多いでしょう。

また、相手の出方は詳細に分かれば分かるほどこちらが有利になります。敵の出方に応じて対応策を準備することができるからです。

逆に、敵の出方を知らないか、誤っていた場合は奇襲の原則によって極めて不利な立場となります。予測精度を上げる努力とは別に、「あくまで予測である」ことを念頭に、敵が予想通りに動かなかった場合のプランを準備しておくことも非常に重要です。

このため、サイバーセキュリティの業務を行う上では、サイバー攻撃者側の意図や狙い、具体的な攻撃手法などに対する理解が必要不可欠なのです。これらを理解することで、セキュリティ対策の説明に筋が通り、企業の複雑な環境でも自ら考え臨機応変に対応していくことができます。

４．２　誰が何のためにサイバー攻撃を行うのか

様々な組織やセキュリティベンダーが発行している各種レポート・記事などを見ると、「APT～」、「サイバー犯罪グループ」、「ハクティビスト」などのサイバー脅威アクターの名前をよく目にします。

彼らにはどのような背景があり、どのような組織構造や能力を持っているのでしょうか。また、何を目的にどのようなサイバー攻撃を仕掛けてくるのでしょうか。

レポートやサイバー攻撃の事例などで解説されている攻撃手法や推奨されるセキュリティ対策などの理解を深めるため、まずは「サイバー脅威アクター」というものの全体像を理解しましょう。

（アプローチ）
脅威アクターの分類やそれぞれの活動目的などについては、METTと意思決定プロセスのうち「敵の分析」の考え方を参考にし、サイバー攻撃者側の視点で考えてみます。

・脅威アクター（又はそのバックに存在する組織）は何をしたいのか？
・どのようなリソース（資金、人員、能力、設備・・・）を持っているか？
・サイバー攻撃は、組織にどのようなメリット又はリスクがあるか？
・脅威アクターを取り巻く環境（闇マーケット、犯罪ビジネスなど）は？

脅威アクターの分類については、Greg Reith 氏が提唱している”Prioritizing Cyber Threats”(2)を参考としました。このモデルでは脅威アクターをTier1からTier6の６段階のプロファイルに分類し、能力、標的、目的、影響、攻撃手法上の特徴などの観点から整理しています。
本書ではこのモデルを参考としつつ、努めてシンプルに理解できるように脅威アクターを以下の４つに分類しました。
・国家型APT
・サイバー犯罪グループ
・ハクティビスト
・個人の攻撃者

脅威アクターも私たちと同じ「人」であり、人が集まればそれは組織になります。よって、それぞれの組織の活動背景、メリット・デメリットなどに目を向けることで、より深く彼らのことを理解できるはずです。
脅威アクターについて理解することは、彼らが行うサイバー攻撃のシナリオや個々のテクニックの文脈を理解するのに役立ちます。

４．２．１　Actor-1：国家型ＡＰＴ

国家型 APT は、特定の国家の意思や指示、支援によってサイバー攻撃を行うグループであり、豊富なリソースを駆使した高度なサイバー攻撃によって極めて深刻な影響を与えることができます。

このアクターは、国家の政治的、軍事的又は経済的な優位性を獲得するため、利害を反する対象国やその重要インフラ、大手企業などに対して、情報窃取（サイバー諜報活動）、情報システムの破壊や機能の妨害などを行います。

国家が金銭獲得を目的としたサイバー攻撃を行うのは合理的ではありません。それはサイバー攻撃で得られる金銭的メリットと攻撃主体が発覚した際のリスクが割に合わないからです。一方、国の財政状況などによってはこれを目的とするケースも存在し、このようなアクターは犯罪グループよりも強力な目的意識、指揮・統制能力とリソースを有するうえ、あらゆる企業が標的となる可能性があるため、特に危険です。

近年では政府機関・重要インフラや大企業に対する攻撃の足掛かり、又は侵入経路としてサプライチェーンを構成する中小企業が標的となる事例も確認されています。わざわざセキュリティが強固な場所を狙う必要が無いため、攻撃者側にとっては理にかなった戦術と言えます。

この他、国家型 APT は次のような特徴を有していると考えられます。これらは他のグループとは一線を画し、セキュリティ対策の考え方や方法にも大きな影響を与えることから、このアクターの標的となり得るか否かは明確に意識する必要があります。

・諜報機関などと連携し、スパイなど人為的な手段を使うことも可能である
・長期間にわたって執拗かつ隠密に活動し、あらゆる手段を使って目的を達成する
・特定の時期や場所を狙い、確実に攻撃目標を達成することができる攻撃手法や隠密性の高い手法を必要とし、多くのリソースをつぎ込む可能性がある
・国家が攻撃主体であることが発覚した場合に国際問題に発展するリスクが大きいため、高度な偽装工作を行ったり、犯罪グループに肩代わりさせたりする可能性がある
・諜報や破壊工作だけではなく、ハッカー育成のためのトレーニングやスキル確認テストなどを実地で行っている可能性も指摘されている

米国のシンクタンクである Atlantic Council は、国家のサイバー攻撃に対する責任、態度、スタンスを「禁止する」、「黙認する」、「推奨する」、「自ら実施する」など１０種類に分類したレポート”The Spectrum of State Responsibility”(3)を発表しました。私たちはサイバー脅威を理解するためのツールや共通言語としてこれを活用することができます。

本書では脅威アクターを便宜上４種類に分類していますが、世の中に存在する脅威アクターを簡単に分類することはできません。彼らは意図や存在を隠していますし、２つ以上の特性を有するものや中性的なものもあるでしょう。例えば、以下のような場合が考えられますが、このような活動を識別するのは簡単ではありません。

・国家目的のために犯罪グループや個人ハッカーを雇うことがある
・国家目的に必要又は関係のあるサイバー攻撃であれば、政府はこれを無視する

脅威アクターについて理解するのは重要ですが、固定観念に囚われることなく、あくまで理解するための補助ツールであることを念頭に置いて活用するべきです。

別紙第２では、Atlantic Council のホワイトペーパーで紹介されている詳細な１０の分類と説明を紹介しておりますので、そちらも参照してください。

４．２．２　Actor-2：サイバー犯罪グループ

サイバー犯罪グループは、主に金銭的な利益の獲得を目的として組織されたアクターであり、ダークネットや犯罪者コミュニティを活用してサイバー攻撃をビジネスとして活動している不法なグループです。

構造上は一般的な営利企業と似た特性を有し、自ら又は依頼や契約などによってサイバー攻撃を行うほか、サイバー攻撃によって得た情報や技術などを不法に取引することで金銭的な利益を得ています。

・決済システムへの攻撃によって直接的に金銭を窃取する
・窃取した個人情報や機密情報を売買して利益を得る
・サイバー攻撃のためのツールや技術などを売買する
・他者からサイバー攻撃の依頼や発注を受け（仲介者）、サービス料を受け取る
・企業の重要な資産の暗号化や窃取した情報の流出をほのめかして脅すことにより、身代金を搾取する

よって、このグループの標的は大企業や重要インフラだけに留まらず中小企業や個人にまで及びます。また、活動目的や組織的な背景から国家型 APT よりも非常にアクティブ・大胆かつ無差別的にサイバー攻撃を行う傾向があり、近年ではサイバー攻撃のビジネス化・カジュアル化がますます進み、犯罪グループ以外のあらゆるアクターを巻き込んだ大規模なエコシステムが形成されていると指摘されています。

・攻撃ツールや攻撃プラットフォームなどの販売・貸し出しサービス
・身代金要求、ビットコイン交換、現金化、資金洗浄などのサービス
・認証情報の窃取・販売、対象企業への侵害代行サービス
・買い切りタイプのほか、サブスクリプションサービスも存在する
・表向きはセキュリティ目的（侵入テストサービスなど）を装い、政府機関や軍などから発注を受けてサイバー攻撃を実行する

これらのことから、このグループによるサイバー攻撃は表面化されやすく、被害規模（被害数や損害額）は各脅威アクターの中でも最も大きなものとなり、多くの企業や組織にとっては最も身近な脅威となっています。

目の前に迫る緊急性の高いリスクへの対応としては、まずはこのグループからのサイバー攻撃への対策を行うことが重要でしょう。

４．２．３　Actor-3：ハクティビスト

ハクティビストは、特定の主義・主張を流布することを目的としてサイバー攻撃を行う個人又は組織です。

このアクターの最大の特徴は、自身の主義・主張を流布するために、サイバー攻撃という手段を使って不法なメディア作戦を展開し、主義・主張に反する趣旨の活動を行う企業や関連する組織を標的とする点です。

このため、サイバー攻撃の目標（影響）ではなく、標的となる組織の特徴の点で他のアクターやグループ間の違いが現れます。

・国営メディアや民営のメディア企業　など
・このアクターの主義・主張に関連する活動を行う企業・団体　など
・企業や市民活動を統制又は支援する立場である政府機関や地方自治体など

しかし、「何をもって彼らの主義・主張と企業が関連しているか？」については、やや不明確なところがあります。主義・主張は、事業の種類など分かりやすい単位の物ではなく、特定の業務プロセスや使用している材料、ひいては地政学や宗教的なつながりにまで幅広く発展する可能性があるからです。

したがって、何をもって彼らの標的になるかは、ほとんどの場合、完全に彼らの主観、独断と偏見によって決まっていることが多いものと思われます。一部では、企業名やホームページ上の記載、地名などに起因して攻撃対象となってしまったケース※もあり、予測不能な場合も多々ありますので、注意が必要です。

※2012 年に発生した国土交通省霞ヶ浦河川事務所（茨城県）に対するサイバー攻撃では、「霞が関」と「霞ヶ浦」を間違えて攻撃を受けた可能性が指摘されている。

https://www.nikkei.com/article/DGXNASDG3104D_R00C12A8CC0000/

「アノニマス」などの著名なハクティビストグループは、主義・主張や場合によっては標的のリストなども公開していることが多いため、ある程度予測や対応は可能かもしれません。

また、目的はどうあれ、サイバー攻撃で使用されるテクニックや戦術は犯罪グループなどと近しいものがあると思われますので、特に名指しで犯行予告をされるなどのケースでなければ、特に意識して対策するようなものではないかもしれません。

歴史的に宗教や地政学的な緊張が高い地域では、国家の主義・主張に基づき国家型 APT がサイバー攻撃を行うケースも確認されています。この場合、政治的又は軍事的な優位性を獲得する目的で極めて高度な能力とリソースを持つグループが関与するため、特に注意が必要です。

４．２．４　Actor-4：個人の攻撃者

個人的な恨みや欲求を満たすためにサイバー攻撃を行う個人であり、他のアクターと比してリソースやスキルは低級な傾向があります。

SANS Institute によれば、脅威は「意図」、「機会」、「能力」の３要素が備わったものと定義(4)されており、企業の従業員などの個人をサイバー攻撃に駆り立てるものは以下の通りであるとされています。

・意図
　－所属している組織への恨み（待遇や報酬など）
　－特定の個人への恨み（人間関係など）
　－自分の存在や能力を他人に知らしめたい
・機会
　－情報システムにアクセスできる環境や権限（それが合法であり自然な状態）
・能力
　－サイバー攻撃に使える知識やツールなどを手に入れた

このアクターで特に注意すべきは「内部脅威」です。彼らは企業の内部事情や弱点を知っている点、重要なアカウント・サーバなどにアクセスできる権限を有している可能性がある点です。

彼らのアクティビティは正規のシステム操作に紛れ、検出・対応することは困難であるうえ、外部脅威が行う偵察・武器化・侵入などをバイパスして直接本丸を攻撃することが可能です。

また、政府機関や大企業にとっては別の厄介な問題も孕んでいます。このアクターが国家型 APT や諜報機関などから買収・脅迫されると、最も深刻な脅威にレベルアップしてしまいます。

・意図・・・個人レベルでなく国家レベルの悪意へと変貌し、極めて高度な作戦の一部に組み込まれる
・機会・・・このアクターが元々持つ詳細な情報と強力なアクセスを引き継ぐ
・能力・・・国家型 APT の持つスキルやリソースが加わる

これらのことから、個人の攻撃者（内部脅威）を侮ることはできず、むしろどの企業にも存在し得る差し迫った脅威として認識するのが正解だと言えるでしょう。併せて、悪意のない従業員によるミスや誤操作も忘れてはならない脅威です。誤った認識や操作によって悪意のあるサイバー攻撃と同様の影響が発生する可能性があります。

４．２．５　小まとめ：脅威アクターに思いを馳せる

各脅威アクターの詳細については、**別紙第２**をご覧ください。左側のページは、Greg Reith 氏の”Prioritizing Cyber Threats”(2)と本分析チャートから考えられる脅威アクターの特性を METT の情報要素に当てはめて整理したものです。

Fig8. 別紙第２左ページ「脅威アクターの特徴シート」の一例

・**M：活動目的**：脅威アクターがサイバー攻撃を行う目的（モチベーション）を指す。脅威アクターの背景を理解し、サイバー攻撃により現実世界で何を引き起こそうとするかを理解するのに役立つ。
・**E：サイバー攻撃の標的**：脅威アクターの標的に関する考え方を指す。自組織がこの脅威アクターから狙われる可能性があるかを理解するのに役立つ。
・**T：関係する情勢や法・規制**：脅威アクターの活動を左右する外部環境を指す。活動が活発化する要因や活動を制限する要因を理解するのに役立つ。
・**T：組織とリソース**：脅威アクターの組織構成や能力を指す。考えられる組織規模、指揮系統、保有する資源・スキルは、この脅威アクターが選択し得るサイバー攻撃の手段や深刻度を理解するのに役立つ。

右側のページは、脅威アクターの活動目的と、サイバー攻撃によってどのような影響を与えるのかについて分析した結果をチャートによりビジュアル的に表現しました。

各脅威アクターの活動目的について、「PEST フレームワーク」(5)を参考にして分類し、サイバー攻撃の目標（起こし得る事象）との関連性や繋がりを示しています。

【脅威主体】
脅威アクターを活動の目的やサイバー攻撃を行う標的などの特徴から４つに分類。

【目的】
脅威アクターの活動目的を、PEST を軸に現実世界に対して与えたい効果（影響）ごとに分類。これらは、本来必ずしもサイバー攻撃で達成されるものではなく、企業買収、外交的手段、友好的手段など他の方法でも達成することができるのがポイント。

【サイバー攻撃の目標】
上記【目的】の達成に向けて実施するサイバー攻撃の種類。

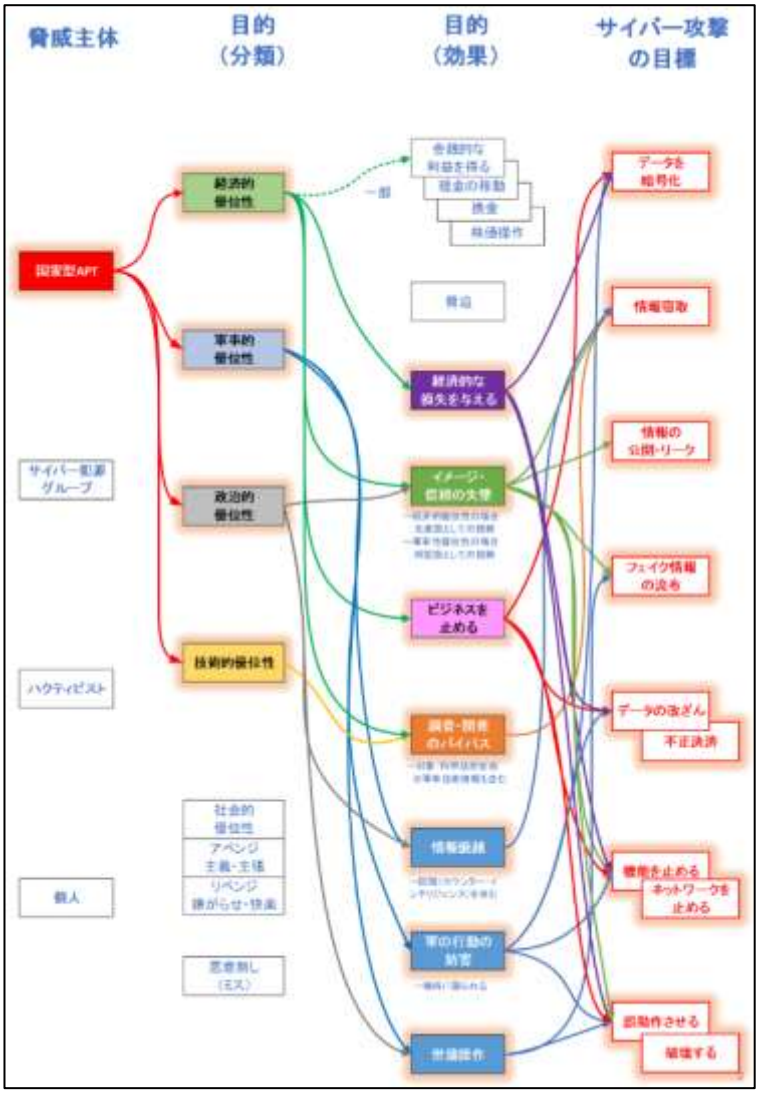


Fig9. 別紙第２右ページ「サイバー攻撃の目的と目標チャート」の一例

このシートを活用することにより、各脅威アクターがサイバー攻撃を行う目的とそのために引き起こす現実世界での事象をひと繋ぎに説明することができます。

反対に、サイバー攻撃によって発生した事象が、何のために、誰によって引き起こされたかを逆算的に考えることもできます。

普段私たちはセキュリティ対策を考えるときに「私たちが何をされるか（されたか）」という受動的な観点に焦点を当て、そこまでの情報のみで対応を考えがちです。このチャートでは、そのサイバー攻撃事象によって脅威アクター側がどのようなメリットを得たいのか？それを考えているのは誰なのか？をひと繋ぎに理解し、リスク分析やセキュリティ対策に説得力を与えることができます。

興味深いのは、すべての脅威アクターが、サイバー攻撃によって考えられるすべての影響を起こし得るということです。活動目的はそれぞれ別であるにも関わらず、あらゆる影響が発生し得ることが分かります。一方、被害・影響の大きさ、深刻度、標的の考え方には脅威アクターごとに明確な違いがあることも分かりました。このような違いを理解することも組織のリスクとセキュリティ対策を考える上では極めて重要です。

最後に、前節でも述べましたが、この分類は脅威に対する理解を促進する目的で便宜上行っているもので、実際の脅威を明確に線引きすることはできません。それは活動目的、標的の考え方、外部要因、組織構成とリソースの観点において、中間的な属性である場合や複数の属性を併せ持つ脅威アクターも考えられるからです。

また、脅威アクターを理解する上では、政治的、歴史的、地政学的、文化的な文脈に関する知識が必要不可欠です。サイバー攻撃者と私たちは生まれ育ってきた環境も常識も根本的に異なります。私たちの常識は彼らには通用しません。

「企業に対して、誰が、どの様なサイバー攻撃を行うのか？」この質問のうち、特に国家レベルの脅威によって引き起こされる企業のリスクを適切に特定し、対応していくためには、このような文脈にも目を向けていくことが求められます。

別紙第２「脅威アクターと攻撃目的」

４．３　どのようにサイバー攻撃を行うのか

サイバー脅威アクターはそれぞれの活動目的や背景に応じ、現実世界に対して何らかの影響を与えメリットや恩恵を享受するために、様々な手段の中から「サイバー攻撃」を選択します。サイバー攻撃でなくても、もっと簡単に・安く・早く・確実に目的を達成できるのであればそちらを選ぶでしょう。複数の手段を組み合わせるかもしれません。

・経済的な優位性を得るのであれば、企業買収や正当な市場競争でも良い
・軍事的な優位性を得るのであれば、ミサイルや軍事侵攻でも良い

同じように、「情報を窃取する」のような一つの目標を達成するのに使用可能なサイバー攻撃の手法（テクニック）は無数に存在します。情報を得るのであれば、直接対象組織に出向いてスパイ活動をすることもできますし、ネットワーク機器の脆弱性を悪用して侵入し、マルウェアを使用してデータを窃取することもできます。４．２．４で述べた通り、対象組織内の職員や委託契約先のエンジニアを買収又は恐喝するという手法も考えられます。

代表的な脅威モデリング手法であるMITRE ATT&CKフレームワークを例にとると、Enterprise（企業）環境を対象としたものだけでも２０２種、ICS（制御システム）環境を含めると２８５種もの攻撃テクニックが列挙されています。(6)

これは、あくまでMITRE社がテクニックの観点で整理・統合して分類したものであり、悪用する脆弱性や対象となる機器・ソフトウェア・機能、それらの設定、使用する攻撃ツールなどの観点も考えると、実際には「無数に存在し、今後も無数に生まれる」ものだと考えて差し支えないと思われます。

それでは、攻撃者は何を考えて無数にある手法からどれかを選び、サイバー攻撃を実行するのでしょうか。あなたが攻撃者ならどうしますか？

４．３．１　無数にあるサイバー攻撃手法の「価値」を評価する

戦いの意思決定プロセスにおける「敵の分析」の手法をベースに、攻撃者になったつもりで考えれば、正解は分からずとも「考え方」は見えてきます。そのためには、攻撃者にとっての各攻撃手法の価値やメリット・デメリットを考えます。

・攻撃の容易性、条件の複雑さ・・・簡単な方が良い、条件が少ない方が良い
・攻撃に必要なリソース・・・・・・少ない方が良い
・攻撃による効果・・・・・・・・・大きい方が良い
・攻撃者側が負うリスク・・・・・・少ない方が良い

参考として、ソフトウェアの脆弱性の深刻度を評価する手法に「CVSS（共通脆弱性評価システム）」があります。CVSS では脆弱性そのものの技術的な特性を表す基本評価基準として以下が定義されています。(7)

・攻撃の難易度（AV:攻撃元区分、AC:攻撃条件の複雑さ、PR:必要な特権レベル、UI:必要なユーザ関与レベル）
・影響度（S:スコープ、C:機密性・I:完全性・A:可用性への影響）

これらは、脆弱性を管理する組織側としての危機感や対応の優先度を判断するために使用する指標の一部ですが、裏を返せば攻撃者にとっての脆弱性の「価値」とも言い換えることができます。

今回のアプローチでは、MITRE ATT＆CK に記載されている各攻撃テクニックを対象とし、以下の観点で評価を行いました。

・攻撃の容易性（CVSS の 4 つの観点をそのまま使用）
・期待できる効果の大きさ
・攻撃に必要なコストの量
・攻撃主体が発覚するリスクの大きさ
・攻撃の確実性・任意操作性（運任せでなく、攻撃者がコントロールできるか）

別添１「攻撃者にとっての攻撃手法の価値評価シート」

注意点として、各手法の評価値はあくまで定性的な物であり、その時の状況などの細かな変数が無数に存在するため、このシートを企業がそのまま使うことは推奨されません。本書はベースとなる考え方やロジックを提供するものであり、企業の環境や当時の状況に応じて自ら考える力をつけることを目的としています。

４．３．２　Result-1：攻撃手法にも市場経済の原理は適用される

細かい部分を見れば一部の例外が存在するのは間違いありませんが、分析結果全般として言えることは、一般的な市場経済の原理や概念はサイバー攻撃手法の世界でも概ね共通しているということです。

・大きな効果が見込めるものは、コストが高く使うのが複雑でリスクが高い
・反対に、安く、簡単でリスクが低いものは、効果も低い
・価値の高い攻撃手法は、共通化され、攻撃者の市場に出回りやすい

これらの一般的な価値観をもって現在のサイバー攻撃事案やセキュリティソリューションの流行などを見てみると、以下のような考察も可能です。

・高価値で共通化された攻撃手法はより多く悪用され、広く世間に認知される
　→対応するセキュリティ対策や製品も多く開発・導入される
・効果は大きいがコストが高い攻撃手法は、あまり悪用されない
　→防御側はあまり危機感や現実感が湧かず、対策に投資しづらい

なお、「コスト・リソース」の概念はやや難しいですが、防御側にとってのセキュリティのコスト・リソースと同じように考えると良いでしょう。ツール等の購入費用、従業員の人件費、技術習得に必要な時間、運用する施設・設備・・・経営の世界では全てお金に換算して判断していると思いますので、それと同じです。
リソースを投入して開発した製品や育成した技術者は、適切に使えばそれ以降はランニングコストだけで効果を発揮し続けていくことができます。コストを考える場合はこのような概念も併せて考慮する必要があります。

サイバー攻撃者も人であり、サイバー攻撃もセキュリティも人の生活の一部であることから、私たちの普段の生活や仕事と似た感覚をもって（ある意味では親しみを持って）理解しようとする姿勢が重要ではないでしょうか。
ここで忘れてはならないのは、コストパフォーマンスを正しく理解するためには、ＩＴやサイバー攻撃／セキュリティに関するテクノロジーについて、少し踏み込んだ知識が必要不可欠だということです。

４．３．３　Result-2：攻撃手法の価値は脅威アクターごとに異なる

攻撃手法の「一般的な」価値は４．３．１で述べた通り分かりやすいものですが、脅威アクターの背景や活動目的によって、それぞれの価値の重要度や優先順位は異なる可能性があります。

Table3.　脅威アクターが重要視する「価値」

脅威アクターの懸念事項	脅威アクターにとっての価値（重要度）			
	国家型APT	犯罪グループ	ハクティビスト	個人
攻撃の容易性	極めて低い	低い	高い	高い
攻撃に必要なコスト	極めて低い	高い	低い	極めて高い
期待できる効果	極めて高い	高い	高い	低い
主体が特定されるリスク	極めて高い	低い	極めて低い	高い
確実性・任意操作性	極めて高い	高い	低い	極めて低い

・国家型 APT では、必要リソースよりも国際問題に発展するリスクや失敗そのものを恐れ、膨大なリソースをつぎ込んででも確実に標的を仕留めるようなやり方を好むでしょう
・犯罪グループの世界では、より市場経済に近い原理が働き、グループ間の競争によってサイバー攻撃のコストパフォーマンスが全体的に押し上げられ、攻撃ツールなどの市場シェアや広報活動のようなものが存在するかもしれません
・ハクティビストは自分の活動を相手や世間に知ってもらう必要があるため、サイバー攻撃における「成功」の概念は特徴的です。
・個人の攻撃者は他の脅威アクターと比較すると、リソースが少ない傾向にあるため、攻撃コストを最も重要視するでしょう。攻撃を行う意義も、趣味や腕試しといった日常の延長線上の活動であるため、攻撃を行うことの影響や確実性はそこまで求めないでしょう。

４．３．４　Result-3：攻撃手法ごとに特徴があり、攻撃者にとっての有利性がある

MITRE ATT&CK フレームワークでは、偵察行動から目標達成に至るまで２８５種もの攻撃手法があると整理されていますが、それぞれの攻撃手法にはそれぞれの特徴があります。本書では、４．３．１項で整理した指標に沿って、それぞれの特徴を評価しました。なお以下にはサイバー攻撃における初期侵入時の攻撃手法を例として３つ記しています。

Table4.　物理侵入における攻撃の特徴と有利性

脅威アクターの懸念事項		攻撃の特徴	攻撃者にとっての有利性
攻撃の容易性	攻撃元区分	物理的	低い
	攻撃条件の複雑さ	条件が多い	低い
	必要特権ﾚﾍﾞﾙ	認証・許可が必要	低い
	ﾕｰｻﾞ関与度	必要	低い
攻撃に必要なコスト		偽造行為が必要	低い
期待できる効果		目標に対しより接近が可能	極めて高い
主体が特定されるリスク		発見のリスク有	低い
確実性・任意操作性		時期と場所を選択可能	高い

・この手法は、対象組織側との直接的な接触を必要とすることから、攻撃の容易性やコスト、リスクの面で攻撃者にとっては間違いなく手を出しづらい
・一方、一度アクセスに成功し、信頼を得ることができれば、情報収集から実行フェーズまで幅広く、極めて効果の高いアクションが可能となる

Table5.　ゼロデイ脆弱性の開発における攻撃の特徴と有利性

脅威アクターの懸念事項		攻撃の特徴	攻撃者にとっての有利性
攻撃の容易性	攻撃元区分	ネットワーク	高い
	攻撃条件の複雑さ	高度なハッキングスキルが必要	低い
	必要特権ﾚﾍﾞﾙ	不要	極めて高い
	ﾕｰｻﾞ関与度	不要	極めて高い
攻撃に必要なコスト		専用の不正プログラムの作成が必要	極めて低い
期待できる効果		セキュリティ対策を無効化できる	極めて高い
主体が特定されるリスク		検知されにくい	高い
確実性・任意操作性		時期と場所を選択可能	高い

・ゼロデイの脆弱性を開発又は買収するには、億単位の膨大な資金を必要とする
・防御側からすると、この手法は防御・検知が理論上不可能であり、極めて大きな効果を期待することができる
・一度使用してしまうと、防御側に研究・対策されゼロデイではなくなる可能性があるため、まさにアクターの威信をかけた乾坤一擲の一撃として使うであろう

Table6.　有効なアカウントを悪用することにおける攻撃の特徴と有利性

脅威アクターの懸念事項		攻撃の特徴	攻撃者にとっての有利性
攻撃の容易性	攻撃元区分	ネットワーク	高い
	攻撃条件の複雑さ	正規のログイン情報のみ必要	高い
	必要特権ﾚﾍﾞﾙ	不要	極めて高い
	ﾕｰｻﾞ関与度	不要	極めて高い
攻撃に必要なコスト		なし	高い
期待できる効果		セキュリティ対策を無効化できる	極めて高い
主体が特定されるリスク		検知されにくい	高い
確実性・任意操作性		時期と場所を選択可能	高い

・この手法は、クローズドソースの検索・売買、別のサイバー攻撃によって獲得したアカウント情報を使って正規の手続きにより対象組織を侵害する
・MitreATT＆CK によると、初期アクセス、永続化、権限昇格、防御回避の実に４個の戦術（Tactics）で使われる、共通的で重要なテクニックであることが分かる
・アカウント情報は意外と安価かつ軽易に入手することができる
　－ダークウェブでは、１件数百円程度の値段で売買されている
　－初期パスワードのまま運用されるネットワーク機器は非常に多い。（令和４年の総務省調査では、自宅用 Wi-fi のパスワードを変更しているユーザは全体の18.6%しかいなかった。）(8)
・以上のことから、攻撃者にとってはコストパフォーマンス、リスク、確実性などの全ての指標においてトップクラスの価値がある

このように、攻撃手法には様々な観点で差異が存在することが分かります。脅威アクターごとのリソース上の制約や重視する特徴と併せて考えると、サイバー攻撃のシナリオを特定するのに有用なコンテキストが見えてくるでしょう。

別添２「MitreATT＆CK における重要・共通テクニック分析シート」

４．３．５　Result-4：攻撃手法の選び方は脅威アクターごとに異なる

４．３．３項では脅威アクターごとのサイバー攻撃で重要視する価値、４．３．４項では各攻撃手法の有利性について述べました。もちろんこの２つの観点には関係性があり、数ある攻撃手法の中から、脅威アクターにとって適切な攻撃手段が選択されることが予想されます。

以下には、国家型 APT がサイバー攻撃で初期侵入を行う際の攻撃手法を選択する際の比較結果を記します。

Table7.　国家型ＡＰＴが攻撃手法を選択する際の比較

脅威アクターの懸念事項	国家型ＡＰＴが持つ重要度	攻撃者にとっての各攻撃手法の有利性		
		例１ 物理侵入	例２ ゼロデイ 脆弱性の開発	例３ 有効な アカウントの悪用
攻撃の容易性	極めて低い	低い	高い～極めて高い	高い～極めて高い
攻撃に必要なコスト	極めて低い	低い	極めて低い	高い
期待できる効果	極めて高い	極めて高い	極めて高い	極めて高い
主体が特定されるリスク	極めて高い	低い	低い	高い
確実性・任意操作性	極めて高い	高い	高い	高い

国家型 APT が重要視する価値は「期待できる効果」「主体が特定されるリスク」「確実性・任意操作性」ですが、有利性がゼロデイ脆弱性開発より有効なアカウントの悪用の方が特定されるリスクが少ないことから、初期侵入は例３の攻撃手法が選択されることが予想されます。

ただし、主体が特定されるリスクで有利性が劣るもののゼロデイ攻撃の開発もかなり有利性の高い攻撃手法であるため、有効なアカウントを悪用する攻撃手法とは平行で準備を行う可能性も十分に考えられます。脅威アクター側のリソースが潤沢であればあるほど、実現できる攻撃手法は豊富になり、且つ同時に実行できてしまうのです。

次に、個人の攻撃者がサイバー攻撃で初期侵入を行う際の攻撃手法を選択する際の比較結果を記します。

Table8.　個人の攻撃者が攻撃手法を選択する際の比較

脅威アクターの懸念事項	個人の攻撃者が持つ重要度	攻撃者にとっての各攻撃手法の有利性		
		例１ 物理侵入	例２ ゼロデイ 脆弱性の開発	例３ 有効な アカウントの悪用
攻撃の容易性	高い	低い	高い～極めて高い	高い～極めて高い
攻撃に必要なコスト	極めて高い	低い	極めて低い	高い
期待できる効果	低い	極めて高い	極めて高い	極めて高い
主体が特定されるリスク	高い	低い	低い	高い
確実性・任意操作性	極めて低い	高い	高い	高い

個人の攻撃者が最も重要視する価値は「攻撃に必要なコスト」です。例に挙げた攻撃手法を比較すると、有効なアカウントの悪用がコストの観点で有利性が高いため、国家型 APT と同じく例３の攻撃手法が選択されることが予想されます。

国家型 APT とは異なり、個人の攻撃者には十分なリソースが備わっていないため、ゼロデイ攻撃脆弱性の開発を攻撃手法として選択することはまずないでしょう。

２つの脅威アクターについて不正侵入を行う場合の攻撃手法を比較しましたが、結果は両アクターとも同じ結果になりました。これは、有効なアカウントの悪用という攻撃手法そのものが、総合的に有利性の高い攻撃手法であるためです。言い換えると、脅威主体に問わず有効アカウントの悪用は魅力的な攻撃手法であることになります。一度防御側に思考を戻して考えると、このような有利性の高い攻撃手法ほど、対策の優先度を高くするべきでしょう。

別紙第３では、特徴の異なる２つの脅威アクターが過去に引き起こしたサイバー攻撃事例を引用し、METT と戦いの９原則を活用して背景を分析しました。

脅威アクターがサイバー攻撃を仕掛けようと思ったとき、標的を決めるとき、初期侵入の時、最後に目的を達成する時、何を考えてどのようなアクションを選択するのか。いずれにしても推測の域を出ることはありませんが、脅威インテリジェンスなどによってその精度を高め、企業のセキュリティ対策に活かすことが重要なのではないでしょうか。

別紙第３「戦いの原理・原則から考えるサイバー攻撃者の戦術」

コラム２　破壊的なサイバー攻撃は日本で起こるのか？

世界では、重要インフラへの破壊的なサイバー攻撃の発生が確認されています。核開発プラントの破壊や、電力インフラの停止など、一地域や一国家単位での影響が発生しており、日本の重要インフラが同様の攻撃を受けた場合も、混乱は避けられないと思います。

ただ、日本では重要インフラへの破壊的なサイバー攻撃は発生していません。なぜ日本で発生していないのでしょうか。今後も発生しないのでしょうか。

この疑問を解消するために、海外事例の背景について考えていこうと思います。重要インフラへの破壊的なサイバー攻撃は国家型 APT によって為されていると言われています。逆に言えば、サイバー犯罪グループやハクティビスト、個人は積極的に重要インフラを狙わない、もしくは狙ったが業務影響が発生する前に失敗しているとも受け取ることができます。

この理由は、攻撃目標への到達が容易ではないためであると考えられます。攻撃目標への到達には、ネットワークから侵入するか、物理的にプラントに接近又は侵入する必要があります。しかし、プラントはインターネットや IT システムから隔離されていることが多いため、ネットワークからの侵入は困難であり、物理的なプラントへの侵入については、古くからの安全設計や入退室管理などが寄与し、いずれにしても IT システムと比べてサイバー攻撃が容易ではないシステムとなっています。

しかし、こういったシステムに対しても、国家型 APT のように豊富なリソースを持った脅威アクターは攻撃を成功させることが可能でしょう。

では、国家型 APT が重要インフラへの破壊的なサイバー攻撃を目論む理由は何でしょうか。

彼らは政治的目的を抱えており、それを実現するためにサイバー攻撃を行います。本書でも解説したように、政治的目的とは、諜報活動（カウンター・インテリジェンスを含む）、破壊工作、世論操作や国家の基盤プロセスへのダメージなど多岐にわたり、戦争を含めた外交手段の一つとしてサイバー攻撃を選択しています。

数ある手段の中でサイバー攻撃を選択するメリットは、攻撃対象に接近する必要がない、攻撃元特定リスクが低い、占領後にインフラの使用が可能、人命や環境への影響をある程度コントロール可能なため国際的イメージ低下を防ぐことが可能、以上のような 4 点が挙げられます。

これらのメリットは紛争が発生する前段階の活動において、特に効果を発揮します。ロシアとウクライナ間の紛争において、2015 年（ウクライナ西部）と 2016 年（ウクライナの首都キーウ）に発生した大規模停電も、これらのメリットを生かして戦略的な目的に向けた破壊工作を行ったものかもしれません。

一方、2022 年 2 月以降、国家間の軍事的な対立が明確となってからは、ロシアはミサイル等の兵器も併用して発電所などのインフラを破壊しています。電力インフラを標的とした新たなマルウェアも発見されましたが、ウクライナ政府とセキュリティ企業の対応により失敗したとされています。物理的な破壊や国際的な批判を許容するのであれば、このような方法の方が確実に目的を達成することができるでしょう。

このような背景から、紛争が日常的でない日本では破壊的なサイバー攻撃が起こり得るコンテキストが整っていない状態にあり、攻撃が発生していない状況も説明することができます。

しかし、この状態が続くとは限りません。防衛白書などで指摘されているように、昨今の台湾をめぐる中国情勢は軽視できるものではなく、日本も影響を受ける可能性が高いと言われています。本コラム執筆時点でも、中国による台湾を包囲する軍事演習が行われており、いつ直接的な対立が始まってもおかしくない状態にあります。

そういった背景を鑑みて、NISC（内閣サイバーセキュリティセンター）により策定された「重要インフラのサイバーセキュリティに係る行動計画」を基に官民一体となったサイバーセキュリティ対策に臨んでいます。

重要インフラ事業者として、経営的なメリットを期待することはできませんが、国民生活と経済活動における基盤の維持を使命とする以上、無視することはできないのではないでしょうか。また政府としても、欧米などと同じように、今以上に国としての強力な推進体制と重要インフラ企業への手厚いバックアップが必要となってくるのではないでしょうか。

現在日本への影響は顕在化していないように感じるかもしれませんが、重要インフラへの破壊的なサイバー攻撃を行うための情報収集や仕込みは既に始まっているのかもしれません。

コラム３　「ゲームチェンジャー」がサイバーセキュリティにもたらすもの

”ゲームチェンジャー”という言葉をご存知でしょうか？元はスポーツの世界で使われた用語で、ゲームの途中で交代して試合の流れを一気に変えてしまう選手。転じて、状況や動向を大きく変える人物や出来事のことを指します。

例えば第一次世界大戦で登場した戦車はゲームチェンジャーのいい例でしょう。
戦車が登場するまでの戦場は前線から本陣まで幾重にも長大な塹壕を張り巡らせて待ち構えるという防御側が優位な戦術が取られていましたが、英国が世界で初めて”戦車”を戦場に投入したことで防御側有利の戦場は一変し、戦車を要とした攻撃側有利の戦術に代わっていきました。

サイバーセキュリティにおいても革新的な技術や装置といったゲームチェンジャーの現出により既存のルールや戦場が一変させられてしまう可能性があります。

例えば現在暗号化に用いられている技術の一つに RSA 暗号があります。これは桁数の大きい素因数分解の計算が困難であることを利用して暗号鍵の生成を行い、その膨大な計算量から現在の計算機では実質解読不可能であることを暗号鍵の安全性の担保にしています。しかし膨大な計算量を持つ計算機、量子コンピュータが実用化された際には現実的な計算時間内に破られると予想されており、今後 30 年以内に危殆化すると予測されています。

AI に関しても近い将来にシンギュラリティ（技術的特異点）の到来が予測されています。既に AI は画像生成や大規模言語処理などの分野で広く使われており、量子コンピュータのように特別新規性のある技術ではありません。しかしながら AI 技術は加速度的に成長を続けており、未来のある時点で人間の知能を大幅に凌駕するとされています（2045 年問題）
既に AI をサイバー攻撃に利用する動きは始まっており、標的型メールの文面生成や、著名人のディープフェイク動画といった形で悪用が確認されています。これらの深刻な問題点は、シンギュラリティを迎えていない途上の現時点でさえ、一見しただけでは本物と見紛う精度に達しているという点が挙げられます。

第４章では攻撃者の目線でサイバー攻撃について論じてきましたが、近い未来ゲームチェンジャーの現出によって本書で分析した脅威アクターのプロファイルは崩れてしまうでしょう。

しかしながらゲームチェンジャーが現出しても変わらないものがあります、それは攻撃者の目的と戦い（他者との敵対関係）の原理・原則です。歴史を振り返ってもこれまで様々なゲームチェンジャーの登場によって戦術は根底から変わってきましたが戦いに勝利するという目的と、それを実現するための普遍的な力学・ロジックである戦いの原理・原則は変わっていません。今後訪れる技術革新によりサイバー攻撃やセキュリティの手法はさらに複雑化し多様化していきますが、その本質は大きく変わることはないと考えられます。我々に求められるのは不変の本質を踏まえた上で、変化を捉え、臨機応変に対応する“不易流行の意識”ではないでしょうか。

第５章

戦いの原理・原則から

サイバーセキュリティ対応を考える

- 第４章では、攻撃者側の視点から、脅威アクターや攻撃シナリオ・手法に関する理解を深めました。
- この章では、意思決定プロセスを参考にして、自組織の環境に応じてサイバーセキュリティを考えるための実践的なポイントを解説します。
- 併せて、私たちにとって心強い武器であるセキュリティフレームワークやガイドラインをしっかり武器として使うための方法やよくある企業の悩みを解決するためのヒントについても紹介します。
- 「これだけ見れば大丈夫」というようなベストプラクティスではありません。企業のセキュリティ担当として、複雑な組織の現状に合わせて適切なセキュリティを組み込むためのロジックを提供します。

５．１　意思決定プロセスを参考にしたセキュリティ戦略と戦術

第３章では、軍事組織の意思決定における概念フレームワークとして意思決定プロセスを紹介しました。本章では、このプロセスを応用して企業のセキュリティリスクを分析・特定し、サイバーセキュリティの戦略と戦術を考え、適切に実装・運用していくためのポイントを解説していきます。

Table2. 意思決定プロセス（再掲）

	１：任務の分析	２：作戦環境の分析	３：敵の分析	４：作戦の立案
目標	状況を理解し、達成すべき目標を特定する	戦場の状況など、戦いに影響を及ぼす要因を特定する	敵対者の目標と予想される行動を特定する	ここまでに特定した要因から、今後の行動方針を意思決定する
戦いにおける実施事項	●彼我の目的の分析 ●戦場の特定 ●彼我の戦力の比較 ●作戦方式の決定 ●作戦目標の確立	●地形の分析（重要地形の特定） ●気象の分析（影響と対応の決定）	●敵の目標の分析 ●敵がとり得る行動の列挙・分析 ●各行動の妥当性の評価	●行動方針の列挙 ●行動方針の比較・分析 ●行動方針の決定 ●作戦の立案→実行
サイバーセキュリティに置き換えた場合	●ビジネス目標の分析 ●組織に対する脅威の特定 ●セキュリティの目標の確立	●ビジネスプロセスの特定 ●情報資産・脆弱性の特定 ●現時点のセキュリティ態勢の把握 ●保護すべき情報資産の特定	●サイバー攻撃の目標（脅威事象）の特定 ●起こり得るサイバー攻撃シナリオの列挙 ●各シナリオの発生可能性の評価	●セキュリティ対策の列挙、比較、決定 ●セキュリティ対策の実装、運用、（インシデント対応）

意思決定プロセスは、「敵との戦い方を考え、決めていくためのフレームワーク」でした。これは、他者との敵対関係において行動方針を意思決定していくことに特化した基本的な考え方の概念です。

戦いと同じく他者との敵対関係であり、ビジネスなど多くの要因が絡み合うサイバーセキュリティの世界では、意思決定のプロセスも非常に複雑です。

このため、リスク分析の手順やセキュリティ対策の方法を論じたフレームワーク・ガイドラインは多数発行されていますが、それをただ読むだけでは企業の環境とリスクに応じた対応を適切に行うのは難しいかもしれません。

意思決定プロセスを学び、応用することで、サイバーセキュリティにおける複雑な意思決定のポイントをシンプルかつ的確に理解することができます。そして、様々な手法が開発されたリスク分析、戦略立案、セキュリティ対策の選択と実装における目的と前後関係を整理し、企業の置かれた状況に応じて適切に行動していくことができるでしょう。

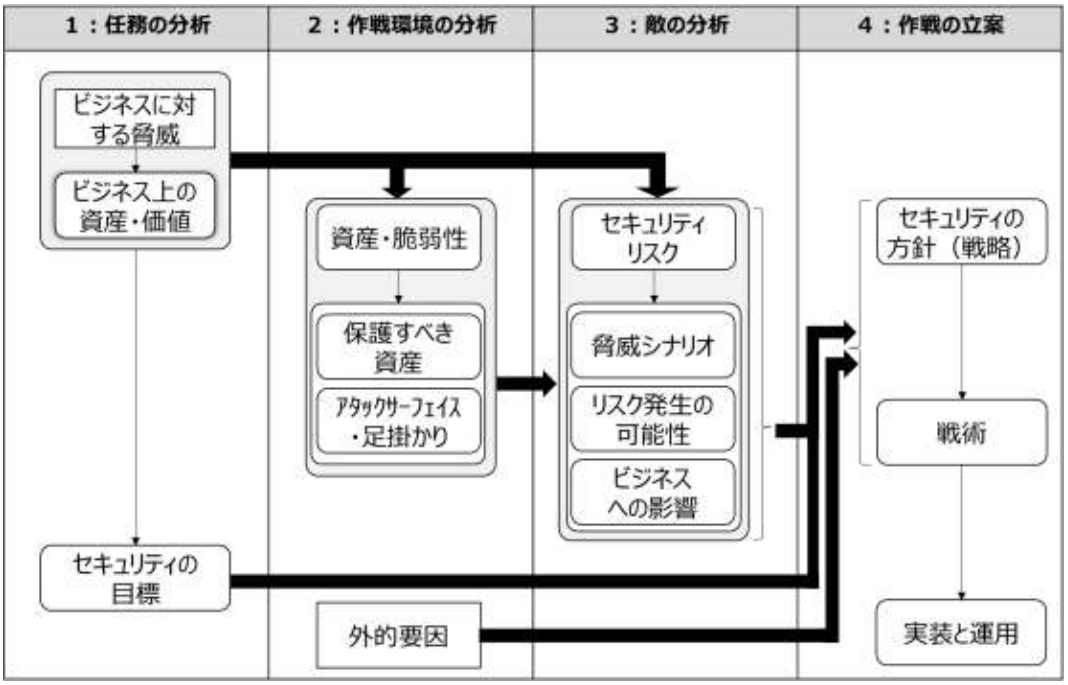


Fig10. 意思決定プロセス相互の関係性イメージ

５．１．１　Phase-1：サイバーセキュリティの目標を決める

このフェーズは、組織としてのセキュリティ戦略と戦術を決める演繹的アプローチの最初の一歩であり、ビジネスの目標と組織に対する脅威を特定し、セキュリティの目標を確立します。

この段階でビジネス目標や脅威を特定するのは、Phase-2 以降の分析をより正確かつ効率的に行い、企業経営のマクロの視点から具体的なセキュリティの目標とアクションを決めていくためです。

ビジネス目標は経営層から示され、多くは収益の増加、コストの削減、市場シェアの拡大、顧客満足度の向上、持続可能な成長などが挙げられるでしょう。重要インフラに関わる企業では、事業の維持も極めて重要なビジネス目標の一つかと思います。

それぞれのビジネス目標の達成に必要不可欠な事業・資産や情報などを特定することで、企業としての価値（≒守るべきもの）を理解します。

Table9. ビジネスにおける資産と価値

ビジネスにおける資産（例）		価値（守るべきもの）
独自の情報	組織戦略、知的財産、個人情報、営業秘密	情報が必要な人にだけ伝わること
提供・運営するサービス	金融、課金・徴収、品質	情報が偽りなく正しいこと
	生産プラント、機械設備、ECサービス	機器やサービスが稼働していること
客観的評価	株価、ブランドイメージ、顧客満足度、信頼	評価が好意的で高いこと

次に、企業の資産価値が何からどのように脅かされる可能性があるかを特定します。企業にとっての脅威源はサイバー攻撃者だけではありません。自然災害、火災、テロ、法・規制の変化なども対応が不十分であれば上記の価値を棄損する可能性があります。

このフェーズではあらゆる脅威源を列挙し、それによって企業の価値にどの程度の影響を及ぼし得るのかを分析します。Table10 では企業に対するあらゆる脅威（オールハザード）を列挙しています。

Table10. 企業に対する脅威とサイバーセキュリティにおけるリスク対応

脅威（ハザード）		原因	サイバーセキュリティにおけるリスク対応				
			回避	移転	低減		受容
					被害の予防	回復・復旧	
人為的災害	サイバー攻撃	悪意	○	○	○	○	○
	誤動作、火災・爆発・流出						
		劣化、誤った操作など	○	○	○	○	○
	法・規制の変化	世界又は業界全体としての流れや関係性				○	
	コンプライアンス						
	国際情勢						
	テロ・戦争						
自然災害	洪水・地震・津波	自然の摂理		－		○	－
	感染症						
	台風・竜巻						
	火山の噴火						
	小惑星の衝突						

企業はすべての脅威（ハザード）に対応する必要がありますが、企業によって影響の度合いや対応の可能度には違いがあるため、具体的な被害見積（発生可能性と影響度）と対応に必要なコストなどを天秤にかけて検討する必要があります。

このうち、サイバーセキュリティで対応を検討するのは、情報資産への影響を低減する措置（**橙色部**）及びサイバー攻撃に対するすべての対応（**緑色部**）でしょう。

一方、機械・プラントなどの誤動作、火災・爆発・流出事案（**水色部**）についてはサイバー攻撃によっても発生し得ることから、プロセス設計、計装、安全などの取組とサイバーセキュリティ対応を密接に連携して進めることが重要です。

最後に、企業としてのサイバーセキュリティの目標を決定します。「どの脅威が」、「どの価値に対して」、「どのような影響を与え得るのか」を特定し、対応方針を確立します。

サイバー攻撃以外の脅威で予想される被害はほとんどが物理的な停止・破壊（サービスの棄損）と、それによる信頼の低下（客観的評価の棄損）であり、対策は比較的シンプルです。

一方、サイバー攻撃では、情報資産の機密性や完全性を含め、あらゆる価値が侵害される可能性があります。（それも、気づかないうちに、顔を見たこともない人から、いとも簡単に！）

このため、サイバー攻撃は他の脅威と比べて可視化しにくい脅威であり、対応要領も複雑になってしまうのです。

戦いの原理・原則を踏まえたうえで重要なのは、はじめに組織全体としてのビジネス目標、脅威、リスクを明確にし、それに従って演繹的に詳細なリスク分析と対応策の検討を進めることです。この全体像を理解できていない場合、以下のような問題が発生する可能性があります。

・個別のセキュリティ事業や仕事に繋がりが無く、目標を見失う
・リスク分析や資産把握などの作業で、スコープの設定を誤る
・セキュリティのためのセキュリティになる

この後のフェーズで行う作業は、全てここから始まり、全てが繋がっています。

５．１．２　Phase-2：組織の資産と環境を分析する

このフェーズでは、企業が保有する資産（特に、情報資産）と企業活動に関係のある周辺環境（法・規制、ガイドライン、市場、顧客、関連企業など）を調査・分析し、セキュリティ対策を行う対象と活動に影響を与える外的要因を特定します。

ここでも、まずは各要素を特定する目的に着目します。

・情報資産と脆弱性
  －企業が守るべきものを明確化する（裏を返せばサイバー脅威が攻撃の目標として狙うものでもある）
  －セキュリティ対策の対象・適用範囲を明確化する（サイバー攻撃の途中経路や中間的な目標となり得るものでもある）
・周辺環境
  －サイバー攻撃やその対応に影響を及ぼす、又は影響を受ける可能性のある外的要因を特定する
  －企業が適合・遵守しなければならない取り決め、又は特別な配慮や処置が必要な要因を特定する

ポイントは、ただ企業が保有する情報資産や関係先をとにかく列挙するのではなく、「企業として守るべきもの、攻撃者にとってサイバー攻撃の足掛かりになり得るものを特定する」という目的を意識しながら行うことです。

この意識があれば、何を把握しなければならないのかについて思いを馳せることができ、一つの情報資産が持つ様々な属性（名称、型番、ソフトウェアバージョン、ファームウェアバージョン、設置場所、管理部署、ネットワーク設定情報・・・etc）の見え方が変わります。

そして、収集・管理すべき情報に優劣をつけ、実効的な資産管理業務を行うことが可能となるでしょう。

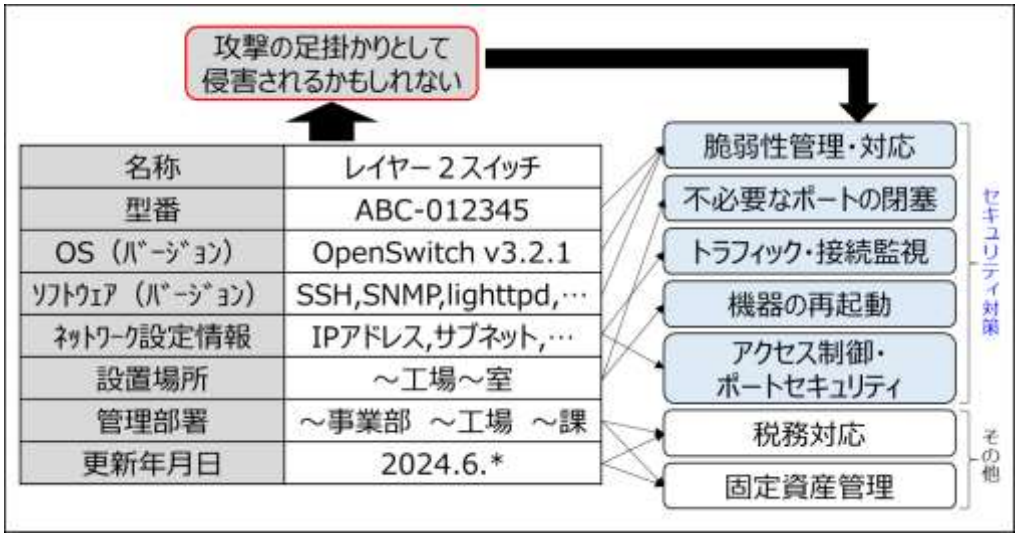


Fig11. 資産の属性と管理目的のイメージ

しかし、ＰＣ、サーバ、ネットワーク機器、クラウドだけではなく、データ、従業員、施設、制御機器なども合わせると、企業は極めて多くの資産を保有しているため、多くのガイドラインでは「分析のスコープを絞る」ことが推奨されています。

では、何を基準に分析のスコープを絞りますか？

企業にとっての重要性？特定の情報システムや工場？ＯＡシステム・制御システムなどの区分？答えは一つではなく、本書ではその答えを提示しません。企業の特性・状況や、リスクを分析する必要に迫られたトリガーなどによっても変わります。

最も危惧すべきなのは、あまり深く考えずにスコープを絞ってしまうことや、一度決めたスコープに固執（又は盲目的に過信）し、この後のフェーズで見直しに迫られた時や例外的な事象が発生した時に見直し・修正を行わないことです。

意思決定プロセスの全体像を理解していれば、それがいかに危険であるかに気づき、状況に応じて自立的に判断し対応していくことができるはずです。

これらのことから、対象スコープを慎重に検討するとともに、ビジネスの目線とサイバー脅威の目線をもって情報資産を見つめ、守る対象（≒攻撃の目標）、アタックサーフェイスとなり得る機器やソフトウェア、悪用される可能性のある脆弱性などを特定します。

周辺環境（外的要因）については、とにかく網羅的に列挙し、それらの位置づけや組織にとっての影響を特定することが必要です。法・規制は適合しないこと自体が企業のリスクにつながる恐れもあり、その他の要因についてもリスクの評価やセキュリティ対策の検討・実装・運用に大なり小なりの影響を及ぼします。２．２．３で触れたように、これらの要因が「企業の味方にも敵にもなり得る」ことを意識して分析していきましょう。

また、法・規制や業界ガイドラインは、国・国民や業界全体に対するリスクを包括的に分析した結果生み出されたものであり、特定の企業を守る目的で設計されたものではありません。よって、全体への貢献や標準化の観点から適合することには意義がありますが、企業としてのリスク対応とは分けて考えなければなりません。

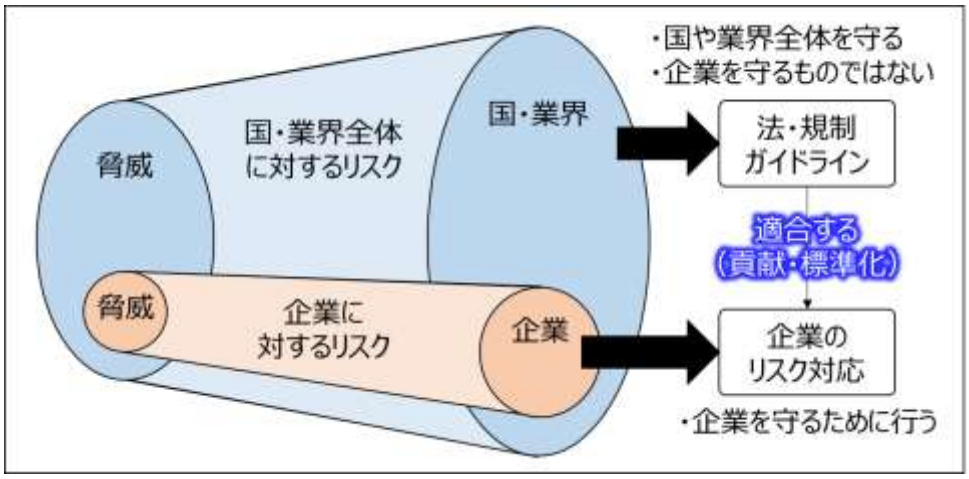


Fig12. 法・規制とガイドラインの意義

事業被害ベースのリスク分析手法では、企業として回避したい事象とそれに至るシナリオを特定し、次いでそれに関連する情報資産と脆弱性を特定していきます。いずれにしても、Phase-1 で分析した企業としてのビジネス目標、脅威、セキュリティの目標をブレイクダウンして具体化していくこと、そして Phase-2 と Phase-3 間の関連性を明確に理解することです。

・資産ベース　　：何を→（誰が）→どの様に侵害し→何を引き起こすか
・事業被害ベース：何が起こるか→（誰が）→どの様に→何が侵害されるか

このとおり、これらの考え方はアプローチの順番が違うだけで、リスクを評価するには資産（脆弱性）、脅威、プロセス、影響の各要素を含めた総合的な評価が必要不可欠です。企業の特性などによって適切な手法は変わりますが、リスク分析の要素やプロセスの意義・関連性などを理解して行うことが求められます。

５．１．３　Phase-3：組織に対する脅威を分析する

Phase-1 では、企業のビジネスや情報資産・価値に対して、サイバー脅威がどのような影響を与える可能性があるかについて特定しました。このフェーズでは、組織がリスクを評価し、セキュリティ対策の優先度や実施方法を決めていくための最終段階として、サイバー脅威によって引き起こされる影響とシナリオ、そしてリスクが実際に発生してしまう可能性を具体化します。

このプロセスでは私たちの目に見えないものを分析していくことになります。特にリスクが発生する可能性とその具体的なシナリオは、防御することしかできない私たちにとってはまさしく未知の世界となるため、第４章で解説した手法を参考に、可能な限り正確にこれらを予測することが求められます。

分析の順番には諸説ありますが、戦いの意思決定プロセスを参考とした重要なポイントのみ説明します。

一つ目は、Phase-1 で特定したビジネスにおける資産と価値、そして、それらに対する脅威と影響を意識することです。

流行りのサイバー脅威アクターや攻撃手法をベースにしたり、それのみを取り上げたりしているケースが見受けられますが、その脅威・手法は本当に企業のビジネスに対する現実的で差し迫った脅威なのでしょうか？脅威の分析は独立して行ってもあまり意味はありません。企業のリスクを特定するためには、ビジネスに対する脅威を分析する必要があります。

事業被害ベースのリスク分析アプローチは、まさにこのポイントを押さえた手法であり、企業のビジネスを起点として脅威シナリオを分析していくことができます。

二つ目は、Phase-2 で特定した具体的な情報資産と脆弱性を活用し、可能な限り具体的かつ現実性のある脅威シナリオを考えることです。この際、脅威シナリオや発生の可能性を詳しく分析していく過程で、予想していなかった場所や機器が実は攻撃者にとって重要であったり、予想していなかったアクションが行われたりする可能性があります。この場合、情報資産の価値、アタックサーフェイス、スコープなどの見直しが必要であり、状況によってはサイバーセキュリティの目標自体を変えなければならなくなることもあります。

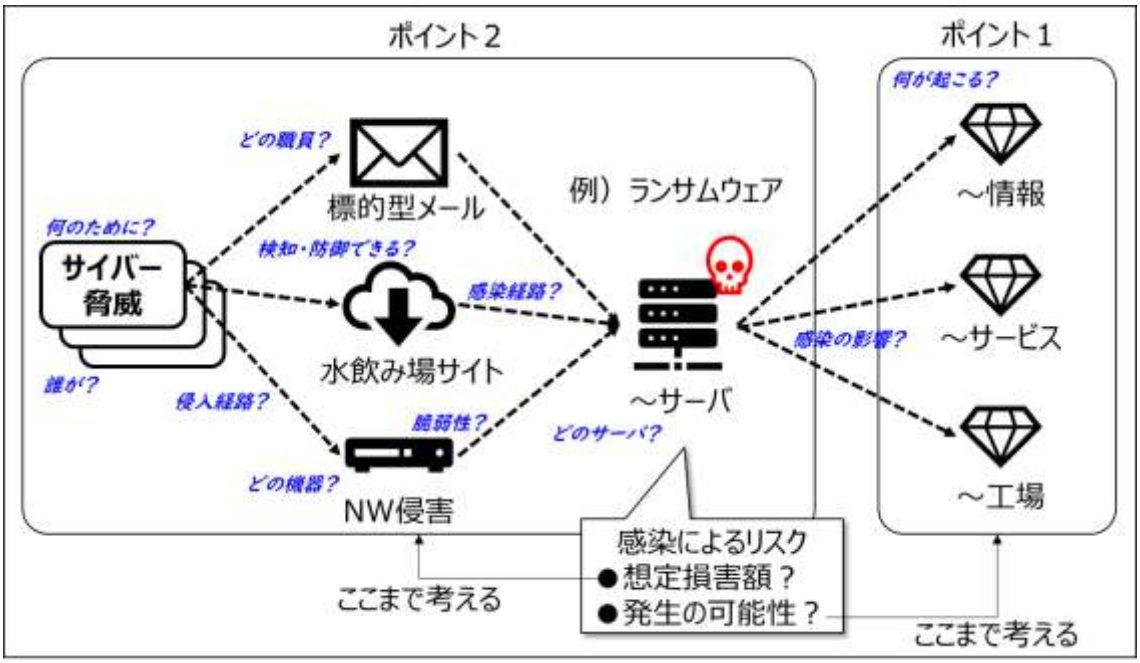


Fig13. 脅威特定におけるポイントのイメージ

企業においてこの業務をシステマチックかつ持続可能な方法で実現していくためには、資産管理、脆弱性管理、脅威インテリジェンス管理をソリューションやツールによって統合することが最善でしょう。しかしながら、本書で解説しているような「本質と力学」を理解し・意識できていなければ、多くの場合は無駄な投資をしてしまっているか、もっと悲惨なシナリオでは「できている」という危険な誤解を生んでしまうでしょう。

この他、脅威シナリオを分析する際の実践的なヒントは第４章に記載してありますので、そちらを参照してください。

５．１．４　Phase-4：サイバーセキュリティの方針を決める

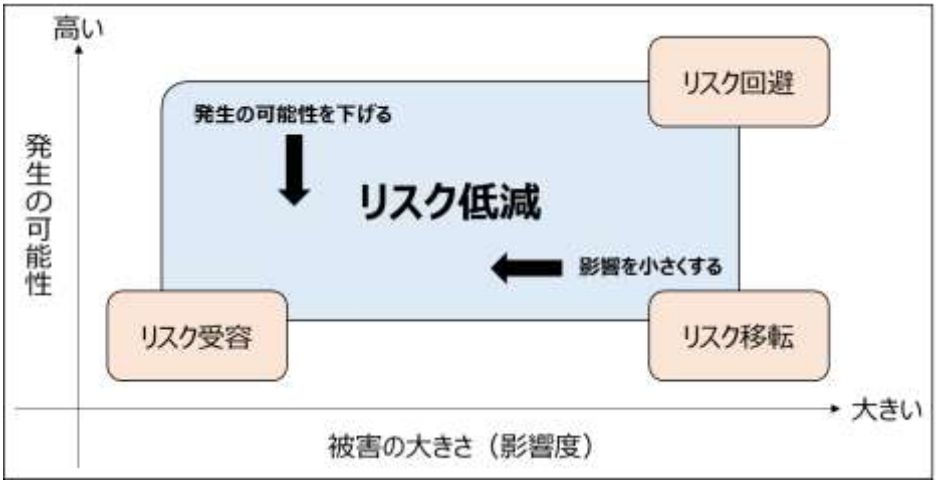


Fig14. リスク対応の方針

Fig14 は、リスク対応方針の種類（回避、移転、低減、受容）を示しています。はじめに、リスクが発生する可能性と影響の大きさから、どの対応を行うのか決定します。

私たちセキュリティ担当者の出番となるのは、主に「リスク低減」です。これまでのフェーズで分析してきた成果を活用し、サイバーセキュリティの目標を達成するための戦略と戦術を検討し、意思決定していきます。

セキュリティの戦略と戦術はそれぞれが独立して効果を発揮するものではなく、相互に関連し、助長し、時には相互に補完し合うことが必要です。戦いにおいて様々な特性や能力を持つ部隊が組織的に機能を発揮することが重要であるのと同じように、セキュリティの戦略と戦術にも共通の目標、機能的な統一、簡明なインターフェースと操作性などの組織的な一面が存在します。

このため、全体としては演繹的なアプローチの中で組織としての柱・指針となるサイバーセキュリティの戦略が必要です。具体的には、セキュリティ防御策（境界防御、アクセス制御、データ保護）、インシデント対応、レジリエンス、人材の確保・育成、社内外のコミュニケーション、法務・ガバナンス、継続的な監視と改善、技術的なサポートなどの方針を検討するとともに、相互を連動・連携させ、リソースの配分（投資）を検討します。

まずこのレベルにおいて、Phase-1 で決めたサイバーセキュリティの目標（見直し・修正されているかもしれない）に対してズレやブレが無いか、それぞれの戦略の間に矛盾や摩擦が無いか、相互に連携されているかについてチェックしましょう。

次に、Phase-2 で列挙した外的要因をチェックし、各戦略に適応します。法・規制への適合方法、関係機関との連携方法などを具体化し、セキュリティポリシー、セキュリティ対策、各種計画（インシデント対応計画、ＢＣＰなど）に組み込みます。

最後に、それぞれの戦略に合わせて具体的なセキュリティ対策や事業を計画・実行するとともに、その状況をモニタリングして適宜改善を図ります。これは所謂ＰＤＣＡサイクル（計画、実行、評価、改善）であり、評価と改善に関わる活動はあらかじめ事業や計画に盛り込んでおくことが必要です。

サイバーセキュリティの戦略と戦術を意思決定していくためには、各フェーズを切り離さずにしっかりと連動させ、資産、脅威、リスクを具体化することです。セキュリティ対策の実装・運用方法（戦術）を検討する際は、Phase-2・3 で分析した詳細な情報資産と脅威シナリオを使って、蓋然性の高いリスクを効果的にケアすることが重要です。

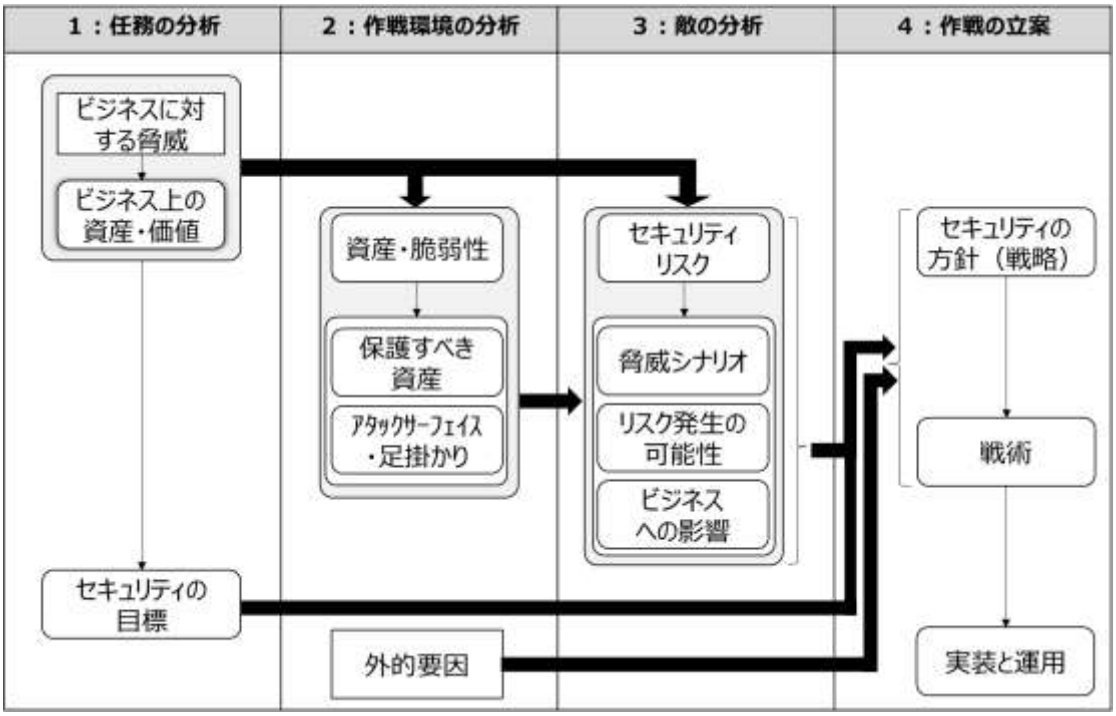


Fig10. 意思決定プロセス相互の関係性イメージ（再掲）

５．２　フレームワーク・ガイドライン活用のポイント

世の中には多数のセキュリティフレームワークやガイドラインが存在します。

フレームワークやガイドラインは、過去の経験や専門家の知見に基づくベストプラクティスを提供します。ある程度共通的な指標を使って組織の状態や成熟度を評価でき、組織は効率的かつ効果的なセキュリティ対策を導入することができます。

また、多くのフレームワークやガイドラインは、法的要件や業界標準に基づいて設計されています。これにより、組織は法規制に適合しやすくなり、国や業界が求める基準をクリアするとともに、コンプライアンス違反による罰則や罰金を回避することができます。

しかし、フレームワークやガイドラインに関する理解不足や組織の状況把握が不十分である場合、以下のような懸念があります。

・内容の理解不足により、不必要なセキュリティ対策を過剰に実施してしまうことや、反対に重要な対策が不十分となる、または法規制やコンプライアンス要件を満さなくなる可能性があります。
・組織の状況やニーズを把握せずに標準的なガイドラインを適用すると、限られたリソースが効率的に活用されず、コストの無駄遣いにつながります。
・組織の文化を考慮せずに額面通りにガイドラインを適用すると、従業員の反発や抵抗を招き、セキュリティ対策の導入がスムーズに進まないどころか、「できている」との危険な誤解を招いたり、逆効果になったりすることがあります。

これらの懸念を解消するためには、フレームワークやガイドラインの内容を深く理解し、組織の具体的な状況やニーズに合わせて適切なフレームワークやガイドラインを選び、必要に応じてカスタマイズすることが重要です。また、定期的なレビューと改善プロセスを導入することで、セキュリティ対策の有効性を継続的に向上させることができます。

参考に執筆時点における主要なセキュリティフレームワーク・ガイドラインの一覧（例）を記載します。

【フレームワーク・ガイドライン一覧（参考）】

名称	概要
【経済産業省・IPA】 サイバーセキュリティ経営ガイドライン	経営者がサイバーセキュリティリスクを認識し、リーダーシップを発揮して対策を進めるための指針を提供します。経営者が守るべき3原則と10の重要項目を示します。
【NIST（National Institute of Standards and Technology）】 CSF（Cyber Security Framework）	業種や規模に関わらず組織のセキュリティ成熟度を測る指標を用いて現在のセキュリティ状態を評価し、目標とするセキュリティレベルを設定するプロセスを詳述します。
【NIST】 SP800 シリーズ（SP: Special Publications）	情報セキュリティのベストプラクティス、ガイドライン、手順、標準、推奨事項を提供します。
【NIST】 SP 800-37 情報システム及び組織のためのリスクマネジメントフレームワーク	セキュリティとプライバシーリスクを管理するための分類、選択、実装、評価、認可、監視のプロセスを提供します。
【NIST】 SP 800-53 組織と情報システムのためのセキュリティおよびプライバシー管理策	セキュリティおよびプライバシー管理策を提供します。リスク管理、アクセス制御、個人情報保護、及びセキュリティ監視などが含まれます。
【NIST】 SP 800-82 産業用制御システム(ICS)セキュリティガイド	ICS における一般的な脅威と脆弱性、リスク軽減のための推奨対策を示し、システムの設計から運用、保守に至るまでのセキュリティ管理を詳細に説明しています。
【NIST】 SP 800-171 非連邦政府組織およびシステムにおける管理対象非機密情報（CUI)の保護	連邦政府機関との契約に基づき CUI を取り扱う非連邦組織が遵守すべき要件が詳細に記載されています。主要なセキュリティ管理策には、アクセス管理、意識向上訓練、監査、構成管理、識別認証、インシデント対応などが含まれています。
【NISC（内閣サイバーセキュリティセンター）】 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書	重要インフラのセキュリティ向上を目的として、リスクアセスメントの実施方法、リスク対応計画の策定、サプライチェーンのリスク管理、コンティンジェンシープランや事業継続計画の策定などを詳細に説明しています。
【IPA】 制御システムのセキュリティリスク分析ガイド	制御システムに対する資産ベースおよび事業被害ベースのセキュリティリスク分析手順、リスク値の評価、リスク低減策、継続的なセキュリティ対策の維持と改善を促進するためのガイドラインを提供しています。

【IPA】 組織における内部不正防止ガイドライン	内部不正防止の基本原則、内部不正対策の体制構築の重要性、管理のあり方、及び事例集やチェックシートが記載されています。テレワーク対応、雇用の流動化対策、セキュリティ技術の進展への対応、重要法改正への対応も含まれています。
【デジタル庁】 政府情報システムにおけるセキュリティ分析ガイドライン	ベースラインアプローチと事業被害アプローチを組み合わせてリスク分析を行い、セキュリティ・バイ・デザインの実現を目指します。分析手法の具体的な手順と実施プロセスを示しています。
【JIPDEC（日本情報経済社会推進協会）】 CSMS ユーザーズガイド	リスクアセスメント、セキュリティポリシーの確立と伝達、訓練活動、管理策の選択と導入、維持管理について説明されています。システムインテグレータや CSMS 認証の取得に関する情報が含まれています。
【JIPDEC】 ISMS ユーザーズガイド	情報セキュリティ管理システム（ISMS）の導入と運用方法を解説しています。リスク評価、セキュリティ対策の実施、継続的な改善を通じて、組織の情報資産を保護するための手順やベストプラクティスが記載されています。
【日本電気協会】 電力制御システムセキュリティガイドライン	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電気工作物に対しては、本ガイドラインに基づく対策が求められる。
【国土交通省】 鉄道分野における情報セキュリティ確保に係る安全ガイドライン	鉄道分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を 推奨基準としてまとめたもの。
【 JPCERT/CC （ Japan Computer Emergency Response Team Coordination Center）】 CSIRT ガイド	CSIRT の構築と運用について解説するもので、情報セキュリティインシデントへの対応方法、リスク評価、外部組織との連携などを中心に説明しています。
【日本シーサート協議会】 CSIRT 人材の定義と確保	CSIRT の役割や業務内容に応じたスキルセット、追加教育の必要性、具体的な役割モデルを示し、企業が適切な人材を確保し、効果的に CSIRT を運用するための指針を提供しています。
【総務省】 ASP・SaaS における情報セキュリティ対策ガイドライン	ASP および SaaS サービスに対して適切にセキュリティ対策を実施するための指針を提供します。情報資産の管理、組織的および運用的対策、物理的および技術的対策に関する詳細な指針を含みます。

【経済産業省】 ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引	SBOM の概要、導入のメリット、導入プロセス、および運用に関する詳細なガイドラインを提供しています。
【日本セキュリティオペレーション事業者協議会】 セキュリティ対応組織の教科書	セキュリティ対応を行う組織において、どのような機能や役割、人材が必要かまとめられています。以下の効果が見込まれます。 ・セキュリティ対応組織の立ち上げ ・セキュリティ対応の現状評価 ・セキュリティ対応における運用の改善 ・グローバル組織におけるセキュリティ対応の共通認識
【MITRE】 ATT＆CK	サイバー攻撃の戦術と技術を体系的にまとめたフレームワークです。攻撃者の行動や手法をカテゴリ別に分類し、セキュリティ専門家が脅威を理解し、防御策を策定するための指針となります。
【Lockheed Martin】 Cyber Kill Chain	サイバー攻撃のプロセスを 7 つの段階（偵察、武器化、配信、エクスプロイト、インストール、コマンド＆コントロール、目的達成）に分けたフレームワークです。このモデルにより、攻撃者の行動を可視化し、各段階で適切な防御策を講じることができます。

「組織の具体的な状況やニーズに合わせて適切なフレームワークやガイドラインを選び、必要に応じてカスタマイズすることが重要」であることを思い出してください。これらはサイバーセキュリティの複雑性に対応するため一般的にかなりのボリュームがあり、読む人を圧倒し、気を抜くと小説やよくあるビジネス図書のような感覚で読んでしまっている可能性があります。

いきなり内容を読み始めず、まずは俯瞰的に全体像を理解することに注力し、企業の課題認識にマッチしているか、どのように活用していくか、そして最終的に課題を解決できそうか考えましょう。

・作成・発行の背景、想定読者（企業）、期待できる効果を理解する。
企業の特性や課題認識とマッチしていない場合、望むような効果を得ることはできない。
・記載内容や方法（考え方を示す／手順や方法のベストプラクティスを示す／網羅的なナレッジを提供する／ベースラインを提供する）を理解する。
盾を剣として使ってはいけません。想定されている利用方法に沿うことが重要です。
・要求のレベル、拘束力（法律／規制／推奨）を理解する。これは、サイバー攻撃の脅威とは別のリスク（コンプライアンス）に直結します。

活用する場面においては、そのまま取り入れるか、企業の特性に合わせて取捨選択する、カスタマイズして応用するなどの方法を検討します。フレームワーク・ガイドラインは、間違いなく特定の企業を対象として作られていません。少し難しくなりますが、多くの場合は後者を選択せざるを得ないでしょう。

５．３　戦いの原理・原則から、サイバーセキュリティの課題解決を考える

ここまで、戦いの原理・原則を参考にしてサイバーセキュリティの本質や力学、考え方と実践のポイントを解説してきましたが、実際の現場では解決するのが難しい課題が山積しています。

・仕事はたくさんあるけど、そんなに人も予算も時間もない！
・ウチは資産管理ちゃんとやってるよ。何か問題でも？
・脅威インテリジェンスをやりたいけど、敷居が高いな〜・・・
・セキュリティ、あれもやりたい。これもやりたい。どうしよう。
・＊＊部門がセキュリティのことを理解してくれない。困った！
・お高いセキュリティソリューションを導入したけど、使いこなせてる？
・不審メール対応訓練って、なんか意味あるの？

これらは、セキュリティの現場あるあるです。ここまでに解説してきた内容を踏まえれば、解決のためのロジックがある程度イメージできるはずです。別紙第４では、親しみやすい４コマ漫画を使って、セキュリティ現場あるあるを解決していくためのポイントをＭＥＴＴと戦いの９原則を使って解説しました。本書の最後に、重要なポイントをおさらいしておきましょう。

考え方が分かっても、それを組織の中で実践し変えていくのは並大抵のことではないでしょう。ほとんどの場合はうまくいかない事の方が多いのではないでしょうか。それでも、うまくいかない原因を考え、特定し、納得し、改善するための努力とアクションを継続していくことが重要なのだと思います。

本書をここまで読んだ方には、そのために必要な考え方の道具が見え始めてきていることでしょう！

別紙第４「サイバーセキュリティの課題解決のヒント」

まとめ

本書では、組織としてリスクに応じたセキュリティ対策を推進していくための「軸となる考え方」を養い、中核人材として自信を持って自立的に行動できるようにすることを狙いとしてここまで解説してきました。最後に全体を振り返ってみましょう。

1章では、サイバーセキュリティが極めて複雑であるという背景を鑑みて、戦いとサイバーセキュリティの関係性と併せて、サイバーセキュリティを読み解くのに戦いの原理・原則を活用できる根拠とその有効性を説明しました。

2章では、他社との敵対関係における情報要素のフレームワークである「METT」と、他社との敵対関係における組織活動、戦法に関するフレームワークである「戦いの9原則」について述べました。

3章では、他社との敵対関係におけるアクション分析・決定手順のフレームワークである「意思決定プロセス」について述べました。

4章では、2章で解説した「METT」、「戦いの9原則」を基に、セキュリティ対策を検討する上で不可欠な脅威とサイバー攻撃に関する理解を深め、攻撃者の目線で各種サイバー脅威及び攻撃手法を分析する方法を提示しました。

5章では、3章で解説した「意思決定プロセス」を活用し、サイバーセキュリティの戦略と戦術を決定するプロセスを解説しました。考慮すべき要件は非常に多く複雑ですが、この概念を学ぶことにより、各プロセスの相互関係や外してはならないポイントを理解することができました。

これまで述べてきた考え方は、本書を読んですぐに身につくものではなく、日々の業務の中で意識し・使い続けることで理解を深め、活用できるようになるものとなっています。また、戦いの原理・原則は、「広くビジネス社会における企業間の競争から個人間の争いにまで応用することが可能な概念」と1章で述べています。セキュリティに限らず多様な目的で意識することで、より使いこなせるようになるでしょう。

あとがき

本書を手に取っていただき、そして、最後まで読んでいただきありがとうございました。

日々、脅威と複雑性が増大するサイバーセキュリティの世界で生きていく私たちセキュリティ中核人材は、多くの知識と経験を必要とする極めて困難な仕事にチャレンジし、経営層と様々なビジネスの現場を繋ぐ橋渡しとしての役割を期待されています。

そのようななか、企業のセキュリティリスクを特定し、適切に対策をとっていくのは並大抵のことではありません。難しい課題に直面した時、思わず率直な答えが欲しくなってしまうものですが、そんなものは存在しませんし誰も教えてはくれません。必要なのは、自ら考え行動していく力と自信だと思います。

本書では、そのためのヒントとして「戦いの原理・原則」を参考にし、サイバー攻撃とセキュリティの本質と力学を理解し、状況に応じた最適解を自ら考えるためのロジックを提供しました。本書で解説したことも、本当にそうなのか？違うとしたらどうなのか？自社の環境ではどうなのか？・・・たくさんの疑問を持ったのではないでしょうか。それでいいのだと思います。

サイバーセキュリティの姿・形はこれからも凄いスピードで変化していくことでしょうが、この考え方と姿勢は紀元前から紡がれてきた人類の英知です。これからの時代でも「状況を観察し、分析し、対応する」ことさえ忘れなければ、そのスピードに対応していけるはずなので、安心してください！本書を読んで何か心を動かされた方がいらっしゃれば幸いです。皆様のサイバーセキュリティの人生がより良くなることを願っております。

最後に、先ほど「必要なのは、自ら考え行動していく力」だと言いましたが、もっと大切なものがあります。それは困難なセキュリティの仕事を一緒に考え、やってくれる仲間です。この業界も繋がりの輪がどんどん広がっています。日本全体でセキュリティを盛り上げ、一緒に悩み、それ以上に楽しんで、そしてサイバー攻撃による悲しい事件を少しでも減らしていくため、これからも手を取り合っていきましょう。

「戦いの原理・原則とサイバーセキュリティ」プロジェクトメンバー　一同

【参考文献】

《参考文献》
・米国陸軍. Field Manual 3-0 Operations. 2022 年版, 米国陸軍, 2022, 280p.
・米国陸軍. Field Manual 5-0 Planning and Orders Production, 2022 年版, 米国陸軍, 2022, 408p.
・木元寛明. 戦術の本質 完全版. 初版, SB クリエイティブ, 2022, 287p.
・石川朝久. 脅威インテリジェンスの教科書. 初版, 技術評論社, 2022, 385p.
・陸上自衛隊幹部学校修親会. 戦理入門. 増補改訂版, 田中書店, 1975, 185p.
・防衛省. 令和 5 年度版防衛白書. 日経印刷株式会社, 2023-7, 522p.
・サイバーセキュリティ戦略本部. 重要インフラのサイバーセキュリティに関る行動計画. 2024 年改訂版, 2024-3-8, 62p. https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf
・Thomas Kranz. サイバーセキュリティの教科書. 初版, マイナビ出版, 2023, 367p.
・Ben McCarty. サイバー術 プロに学ぶサイバーセキュリティ. 初版, マイナビ出版, 2021, 271p.
・野島 良. “量子コンピュータとその暗号化技術への影響”. 総務省
https://www.soumu.go.jp/main_content/000655118.pdf , (参照 2024-05-31).
・上髙原 賢志. “ゲーム・チェンジャーを考える”. 防衛省. 2020-07.
https://www.mod.go.jp/asdf/meguro/center/img/04_symposium3.pdf ,(参照 2024-05-31).
・Telegraph Media Group. “Schoolboy hacks into city's tram system”. The Telegraph. 2008-01-11. Schoolboy hacks into city's tram system (telegraph.co.uk),
https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html, （参照 2024-05-31).

≪引用≫
(1) SANS Institute. “Adversary Emulation using CALDERA”.
https://www.slideshare.net/slideshow/adversary-emulation-using-caldera-232232038/232232038,（参照 2024-5-9）.
(2) DYNAMYTE ANALYTICS. “The Pyramid of Pain in the SolarWinds Cyber Attack”.
https://dynamite.ai/pyramid-pain-solarwinds-cyber-attack/, （参照 2024-3-5）
(3) Atlantic Council. “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”. 2012. 8p.
https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF,（参照 2024-5-14）.
(4) SANS Institute. “Security Intelligence: Introduction(pt2)”. 2009.
https://www.sans.org/blog/security-intelligence-introduction-pt-2-/, （参照 2024-5-20）.
(5) Wikipedia. “PEST analysis”. https://en.wikipedia.org/wiki/PEST_analysis, (参照 2024-5-1)
(6) MITRE. “ATT&CK”. https://attack.mitre.org/, (参照 2024-5-1)
(7) 独立行政法人 情報処理推進機構. “共通脆弱性評価システム CVSS v3 概説”. 2022 年 4 月 5 日.
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html, （参照 2024-5-22）.
(8) 総務省. “2022 年度 無線 LAN 利用者意識調査結果概要”. 2022 年 3 月.
https://www.soumu.go.jp/main_content/000897264.pdf, （参照 2024-5-24）.

【謝辞】

本書の作成にあたり、国立研究開発法人情報通信研究機構（NICT）主席研究員 伊東寛様、日本 Proofpoint チーフエバンジェリスト 増田幸美様、IPA サイバーレスキュー隊（J-CRAT）様には大変貴重なご意見や情報をご提供いただきました。ここに深く感謝申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師である、越島一郎先生、橋本芳宏先生、佐々木弘志様にはプロジェクトのメンター・講師として、ご指導・ご助言をいただきました。改めて御礼申し上げます。

最後に、本プログラムに快く送り出してくださった所属企業の皆様方に、深く御礼申し上げます。この 1 年間、非常に広範囲かつ専門的な学びを得ることができ、本プログラムでしか得られない知見を得ることができました。誠にありがとうございました。

【プロジェクトメンバー】

【隊長】
吉里 将

【副隊長】
桑原 大河　竹内 法彦

【隊員】

岩田 真明	小山 千尋	桜井 真彦	杉山 達哉
須田　貴	谷口 智哉	永廣 武士	二本松 立朗
平澤 泰山	宮﨑　竜	山本 将嗣	

別紙第１

「戦いの９原則の解説」

01 目標の原則

～最後の勝ちを得るにはどうしたらいいかを考えよ～

【解説】

- あらゆる行動において、獲得したい結果と影響を明確に理解し、そのために必要な行動を取らなければならない
- 目標は組織の目的に直接寄与し、かつ、達成可能でなければならない

【事例】

～奥平信昌の長篠城籠城戦～

- 武田勝頼率いる約18,000人の兵に対し、約500人の兵で迎え撃たなければならない籠城戦ではあったが、20日間長篠城を死守しきった
- 籠城の目標を「織田・徳川同盟軍の援軍が来るまでの死守」と現実的なものにすることで、籠城する兵たちの士気を保ち、結果的に織田・徳川連合軍が長篠の合戦勝利につながる大きな要素となった

長篠の戦い図屏風

【引用】Wikipedia

https://commons.wikimedia.org/wiki/File:Battle-of-Nagashino-Map-Folding-Screen-1575.png

【サイバーセキュリティのケーススタディ】

「工場の操業維持」を重要目標とする企業のセキュリティ担当A氏は、セキュリティポリシーの見直しや監視システムの連携などの業務で、この目標を意識して調整を行った。各部署は足並みを揃えて協力し、利害を超えて良好なコミュニケーションが行われた。

→ **ひとつの目的・目標を共有し、達成に向けて全社が協力して活動できたケース**

「工場の操業維持」を重要目標とする企業のセキュリティ担当B氏は、サイバー攻撃の予防と検知のみに着目したソリューション導入や優秀なアナリスト雇用を行った。しかし、サイバー攻撃を完全に防げず、ある日発生したインシデントで壊滅的被害を受けた。

→ **達成困難な目標に固執し、本来重視すべきレジリエンスを軽視してしまったケース**

～心得～

一、セキュリティのための組織作り、取り決め、サイバー攻撃対策は、すべて組織としての目標の達成に向けて構築すべし

二、セキュリティソリューションは、目標に応じて使うべし

02 主動の原則

～善く戦う者は、人を致すも人に致されず～

【解説】

- 攻撃・防御に関わらず、敵に対して主動性を獲得し、これを維持することが目的を達成するための最も効果的かつ決定的な方法である
- 敵の弱点を突いて自分の意志を強要し、自分に有利な条件を設定することが必要

【事例】

～湾岸戦争：砂漠の嵐作戦～

- イラクがクウェートに軍事侵攻したことから、アメリカをはじめとする多国籍軍がクウェートの解放を目的として行った作戦
- 多国籍軍は、当初イラクの防空網を無力化して航空優勢を獲得。引き続き、空爆や巡航ミサイルによって司令部、通信施設、平坦施設などを破壊した
- 主動性を確保した多国籍軍の地上作戦は100時間という短期間で大勢が決し、イラク軍は敗走した

炎上する油田上空を飛行する多国籍軍の戦闘機

【引用】Wikipedia

https://commons.wikimedia.org/wiki/File:USAF_F-16A_F-15C_F-15E_Desert_Storm_edit2.jpg

【サイバーセキュリティのケーススタディ】

A社は、保有する特許情報と個人情報を重要な情報資産と特定した。サイバー攻撃のリスクを想定し、重要な情報を厳重にバックアップするとともに暗号化を導入した。

→ **敵の攻撃目的を予測し、事前に主動的な対策を実施できたケース**

ある日、A社は業務PCに対する外部からの不正アクセスを検知した。セキュリティ担当者は直ちに不正接続を切断することなく、状況を把握しつつ攻撃者の証拠を収集し、警察当局と連携して攻撃グループを一網打尽にした。

→ **受動に陥らず敵をコントロールし、効果的な対応を実施できたケース**

～心得～

一、サイバーにおいても当然に攻撃側が有利である。しかし、防御側も主動権を握る信念を持ち、攻めの姿勢で臨むべし

二、主動権を握るためには、常に先を読み、先手を打つべし

03 戦力の集中の原則

～戦術とは一点に全ての力をふるうことである～

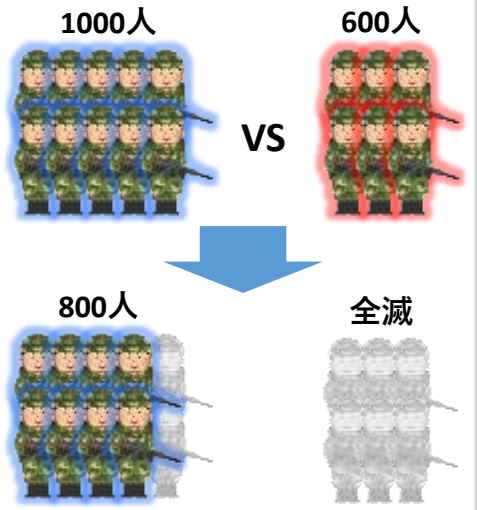
【解説】

- 他の原則が均衡している場合、基本的には戦力の大きい方が必ず勝利する
- 目標を達成するための決定的なポイントに対して資源を集中的に投入する。逆に、敵対者が好きな場所に戦力を集中することを拒否することも重要である

【事例】

～「2-1＝1」ではない？ランチェスターの法則～

- 「ランチェスターの法則」は、戦争における戦闘員の損耗の度合いを数理モデル化したものであり、一対一ではなく集団対集団の特性が反映される
- 自軍が1,000人、敵軍が600人で戦闘を行った場合、単純な引き算では600人を損耗するが、実際には200人程度しか損耗しない可能性が高い
- この法則は、広くビジネスでも応用されている



【サイバーセキュリティのケーススタディ】

ある日、A社のWebサーバに対してDDoS攻撃が発生した。A社はISPと連携して対応しようとしたが、攻撃者は手を変え時期を変え執拗に攻撃してくる。A社は対応に追われて疲弊していき、攻撃者はA社の株価を下げるという目標を悠々と達成した。

→ **攻撃者が圧倒的な物量をもって防御側の対応を制圧するケース**

某敵対国家は、無尽蔵の資源をもって様々な手段でサイバー攻撃を仕掛ける。今回は電力インフラ停止を目標としてサプライチェーン上の中小企業が狙われ、内通者による工作やゼロデイ攻撃を含む同時多発的な攻撃によりサイバー攻撃は成功した。

→ **圧倒的な資源を有する国家支援型APTが中小企業に攻撃を集中したケース**

～心得～

一、物量は戦いにおいて最も基本的かつ重要な資源である。物量上の弱者が強者に勝つためには、策が必要と認識すべし

二、防御側は受動に陥りやすく、資源を分散しやすい。重要なポイントを見極め、そこに資源を集中すべし

04 兵力の節用の原則

～すべてを追うものはすべてを失う～

【解説】

- 資源は有限であるため、可能な限り効率的に運用しなければならない
- あらゆる場所に資源を均等に割り当てた場合、いずれの場所でも敗北する結果となりかねない。第二義的な箇所ではリスクを覚悟し、最小限の資源で臨むべきである

【事例】

～古代ローマの戦争術～

- 古代ローマの戦争術では一部の町や村を無視したり、小規模な抵抗を受け入れたりしながら主要な戦略的目標にリソースを集中した
- 第二次ポエニ戦争では、ローマがカルタゴを攻撃する際、小規模な都市や町は制圧せず、大規模な戦力をカルタゴへ向けて集中させ、カルタゴは致命的な敗北を喫した

Created with DALL·E3

【サイバーセキュリティのケーススタディ】

A社は新しいサービスを展開する予定で、そのサービスには顧客の個人情報や機密データが含まれている。A社の重要なデータやサービスに直接影響しない古いシステムには脆弱性や攻撃リスクが存在するが、それらは受容し、主要な攻撃目標となりえる新しいサービスのセキュリティ対策にリソースを重点的に配置した。

→ **リソースを効果的に配分し、重要な対象を保護しつつリスクを管理したケース**

B社は複数のサイバー攻撃を検知したが、優先すべき事項を定めずに場当たりに、分散して対応にあたった。そのため、主要な資産を保護するアクションが後手に回った。

→ **全ての事象に対応しようとして、重要な資産を保護できなかったケース**

～心得～

一、メリハリのある戦力運用を可能とするため、戦いの使命を決する場所を特定すべし

二、致命的となる箇所以外では、リスクをとる勇気をもつべし

05 統一の原則

～船頭多くして、船山に登る～

【解説】

- 一人の指揮官が責任を持つことが望ましい。責任を分散させることは、戦闘のストレスの中で誤解を生み、作戦を失敗に導く
- 組織が一つの共通の目的を達成するためには、指揮系統も統一しなければならない

【事例】

～八甲田山雪中行軍遭難事件～

- 1902年1月、日露戦争を予期した日本陸軍第8師団歩兵第5連隊は、厳寒地での作戦を想定して八甲田山で雪中行軍訓練を行った
- 案内人の不在や装備の不備などが原因で参加者210名中199名が死亡することになった事故
- 本来、行軍部隊の指揮官は中隊長であったが、同行した上級部隊長や参謀による相反する命令など、指揮系統の混乱も原因のひとつと言われている

真冬の八甲田山

【引用】Wikipedia

https://www.flickr.com/photos/99247795@N00/3158371916/

【サイバーセキュリティのケーススタディ】

サイバー攻撃により化学プラントが損傷し操業停止に陥ったA社は、社長をトップとする対策委員会を直ちに設置し、地域住民・従業員の安全確保と操業の早期再開を当面の目標として全社一丸となって対応して、経営への影響を最小限に食い止めた。

→ **緊急対応のための指揮系統を確立し、組織的に行動できたケース**

サイバー攻撃により製造プラントの停止に陥ったB社は、該当事業所と各部門が連携して事故対応にあたったが、部門間の意見の食い違いや役員からの指示によって現場は混乱し、操業停止が長期に及んだほかブランドイメージの失墜や株価暴落を招いた。

→ **インシデント対応の指揮系統が乱立し、努力が発散して失敗したケース**

～心得～

一、意思決定や指示の系統を適切にし、これを遵守すべし
二、緊急事態を想定し、通常よりもシンプルかつ強力な指揮系統を準備して、トップダウンの指示により迅速に対応すべし

06 機動の原則

～力を、重要な場所へ、早く動かす～

【解説】

- 機動とは、敵軍との関係において、敵軍を不利な状況に追い込み、我に有利な態勢を占めるために行う戦力の移動である
- 機動力を発揮するためには、柔軟性と予備力の確保が必要である

【事例】

～秀吉の中国大返し～

- 備中高松城の戦いにあった羽柴秀吉が、本能寺の変の知らせを受けた
- 秀吉は毛利氏との講和を速やかに取りまとめ、主君の仇明智光秀を討つため、全軍を取って返し、京に向けて中国路を前進した
- 秀吉は備中高松城から山城山崎までの約230kmを踏破し、摂津・山城国境付近の山崎の戦いにおいて明智光秀の軍を撃破した

Created with DALL·E3

【サイバーセキュリティのケーススタディ】

サイバー攻撃に対応したA社は、被害が発生した工場を主体として被害拡大防止と操業復旧を行いつつ、広報部・法務部が先行的に顧客や関係省庁への対応を実施した。この際、CSIRTはその時点の状況によって活動の重点項目を設定して対応した。

→ **限られたリソースを柔軟に運用し、有利になるように臨機応変に対応できたケース**

A社は、インシデント対応計画において、緊急時の対応要領や連絡系統などを綿密に記載する一方、当時の状況に応じた行動ができるように工夫するとともに、緊急時に運用可能な人員や予算の見積もりを行っている。

→ **厳密性と柔軟性のバランスをとりつつ、予備力の確保を意識できているケース**

～心得～

一、サイバーの世界では物質的な質量が関与しづらい。即ち、攻守ともに機動が発揮しやすく、効果が大きくなるものと心得よ

二、厳密と柔軟のバランスをとり、必ず予備を確保せよ

07 奇襲の原則

～サイバー攻撃者にとって最大の武器～

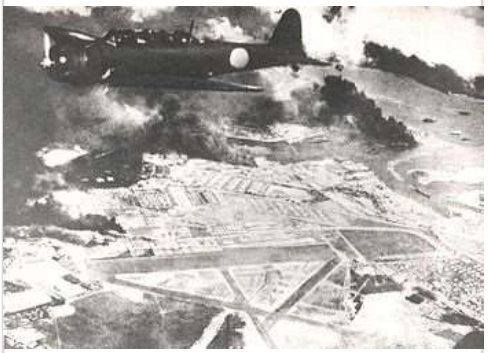
【解説】

- 相手の予期していない場所、時間、量、方法等で意表を突き、有利な態勢を占める
- 奇襲の成功は、2,000対1の数的優位を獲得することと同じ効果を有すると言われる
- 奇襲は、相手に対応のいとまを与えないようにすることを目的とする

【事例】

～真珠湾攻撃～

- アメリカ側の虚を突くために極秘裏のうちに進められた作戦であり、航海中に発見されないよう、気象条件の悪い航路を進み、無線の使用も禁止された
- 日本は米戦艦4隻を撃沈、その他の戦艦・巡洋艦などに大損害を与え、188機の航空機を破壊した
- 日本の損害は航空機29機、特殊潜航艇5隻のみであり、虚を突かれたアメリカ側は有効な反撃ができなかった



炎上する真珠湾上空を飛行する日本軍攻撃機

【引用】Wikipedia

https://commons.wikimedia.org/wiki/File:Pearl_Harbor-_Nakajima_B5N2_over_Hickam-_80G178985.jpg

【サイバーセキュリティのケーススタディ】

サイバー攻撃者は、A社の機密情報を窃取するためサイバー攻撃を企んでいる。A社は境界防御やSIEMの導入などのセキュリティが強固で苦戦していたが、物理対策がほとんどされていない拠点を発見し、そこからシステムの奥深くに侵入することができた。

→ **防御側が予想し準備していなかった場所から、容易に侵入を許してしまったケース**

サイバー攻撃者は、B社のプラント操業を妨害するためサイバー攻撃を企んでいる。A社は年末年始の休暇で監視員が減少し、緊急時の連絡体制に不備がある事が判明したため、1月1日の朝に攻撃することとした。

→ **防御側に気の緩みや心の隙ができる時期を狙って攻撃を仕掛けるケース**

～心得～

一、サイバー攻撃者が虎視眈々と奇襲を狙っていると思え
二、予測できていない攻撃には対応できないことを肝に銘じよ
三、奇襲は方法だけではない。攻撃者の気持ちで考えよ

08 保全の原則

～壁に耳あり障子に目あり。敵に塩を送るな～

【解説】

- 敵対者も原則に従い行動している。つまり優位性を得るためにこちらの情報を探ったり、奇襲を仕掛けようと狙っている
- 不用意に自らの情報を晒すことは敵対者に利する行為に直結するのである

【事例】

～キスカ島撤退　ケ号作戦～

- 第二次大戦中、日本軍は制海・制空権を完全に握られたキスカ島からの撤退作戦を決行、米軍に一切気づかれることなく無傷での撤収に成功した
- 視界ゼロに近い濃霧に紛れて目視発見を避け、レーダーを装備した艦船を用いることで優位性を保って臨んだことが成功の要因として挙げられる
- その後米軍は撤退に気づかないまま上陸作戦を実行、濃霧の中で同士討ちにより被害を出している

Created with DALL·E3

【サイバーセキュリティのケーススタディ】

A社ではセキュリティ対策の一環としてハニーポットの設置を行っている。ある日、攻撃者がA社ネットワークに侵入したが、スキャンなどを行っているうちにSOCが検知し、十分な対策ができた。

→ **情報の秘匿と欺瞞により攻撃者に対する妨害が功を奏したケース**

B社では刷新した社内システムをモデルケースとして自社サイトで紹介している。その結果、攻撃者は労せずして偵察活動を完了し、外部から不正アクセスによってごく短時間で社内サーバから情報を窃取することができた。

→ **攻撃者が公開情報を元に攻撃プランを立て、迅速に攻撃を成功させたケース**

～心得～

一、自組織の情報が外部からどこまで見えているかを確認すべし
二、雉も鳴かずば撃たれまい。わざわざ敵に有利な情報を与えるな
三、情報の負けは戦の負けであると心得よ

09 簡明の原則

～"Simple" is Best!～

【解説】

- 錯誤と混乱に満ちた戦場では、情報の伝達には時間がかかり、劣化する
- 計画、命令、指示などを伝えるときは、できる限りシンプルかつ直接的である必要がある
- 命令や指示に限らず、通常、すべての物事は努めてシンプルな方が適切である

【事例】

～古代ローマ軍のマニプルス戦術～

- 共和制ローマ時代の戦術で、部隊を100人程度の小さな単位で編成し、柔軟性と機動性を確保した
- 大規模な軍隊による力押しが主流だった時代だが、地形や敵の状況に応じて戦闘スタイルを変える方法により、共和制ローマの拡大に貢献した
- この戦術のポイントは、角笛や管楽器による信号を使った指揮だと言われている。指揮官は音によるシンプルな命令によって大部隊を縦横無尽に動かした

Created with DALL·E3

【サイバーセキュリティのケーススタディ】

A社はセキュリティ強化に力を入れており、サイバー攻撃の検知や防御、ログの収集などのために様々なソリューションを導入している。しかし、製品間の連携のためにネットワーク構成や設定が複雑となり、現場エンジニアがそれらを使いこなすのは至難の業である。

→ **セキュリティ対策を複雑にしすぎたため、十分に効果を発揮できていないケース**

サイバー攻撃が発生したA社は、対応要領を十分に検討し、各部署に対して細かい指示を出せるように準備した。しかし、被害は瞬く間に拡大し、顧客や監督機関からも問い合わせが殺到。準備した指示では対応できず、現場には誤解も広がった。

→ **命令・指示が複雑すぎて実行できず、インシデント対応に失敗したケース**

～心得～

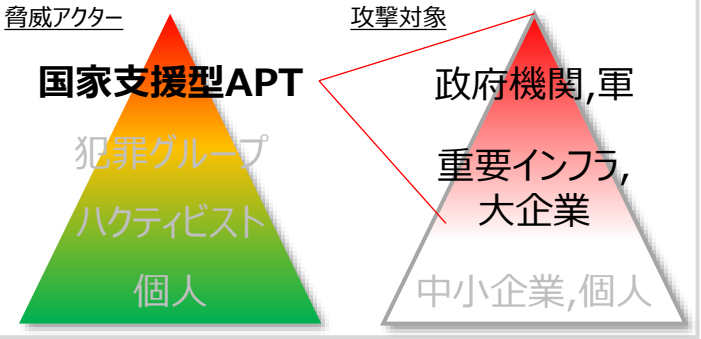
一、手続きやシステムの構築は、可能な限りシンプルを心掛けよ
二、緊急時のコミュニケーションでは、共有すべき項目を厳選して定型化し、伝達チャンネルをあらかじめ準備すべし

別紙第２

「脅威アクターと攻撃目的」

国家型APT

国家型APTは、無尽蔵のリソースを有する最も強力な脅威アクターです。
グループが属する国家の意思に従い、深刻な被害を伴う大規模なサイバー攻撃を行う可能性があります。



M 活動目的

- 政治的、軍事的、経済的又は技術的な優位性を確立する
- 軍事・科学技術等の調査・開発をバイパスするため、知的財産や機密情報を窃取する
- 紛争など特定の時期において、対象国の政府、軍隊、又は市民の活動や経済活動に打撃を与えるため、重要インフラや関連システムを停止又は破壊する
- 金銭の獲得を目的として活動するAPTも存在する

E サイバー攻撃の標的

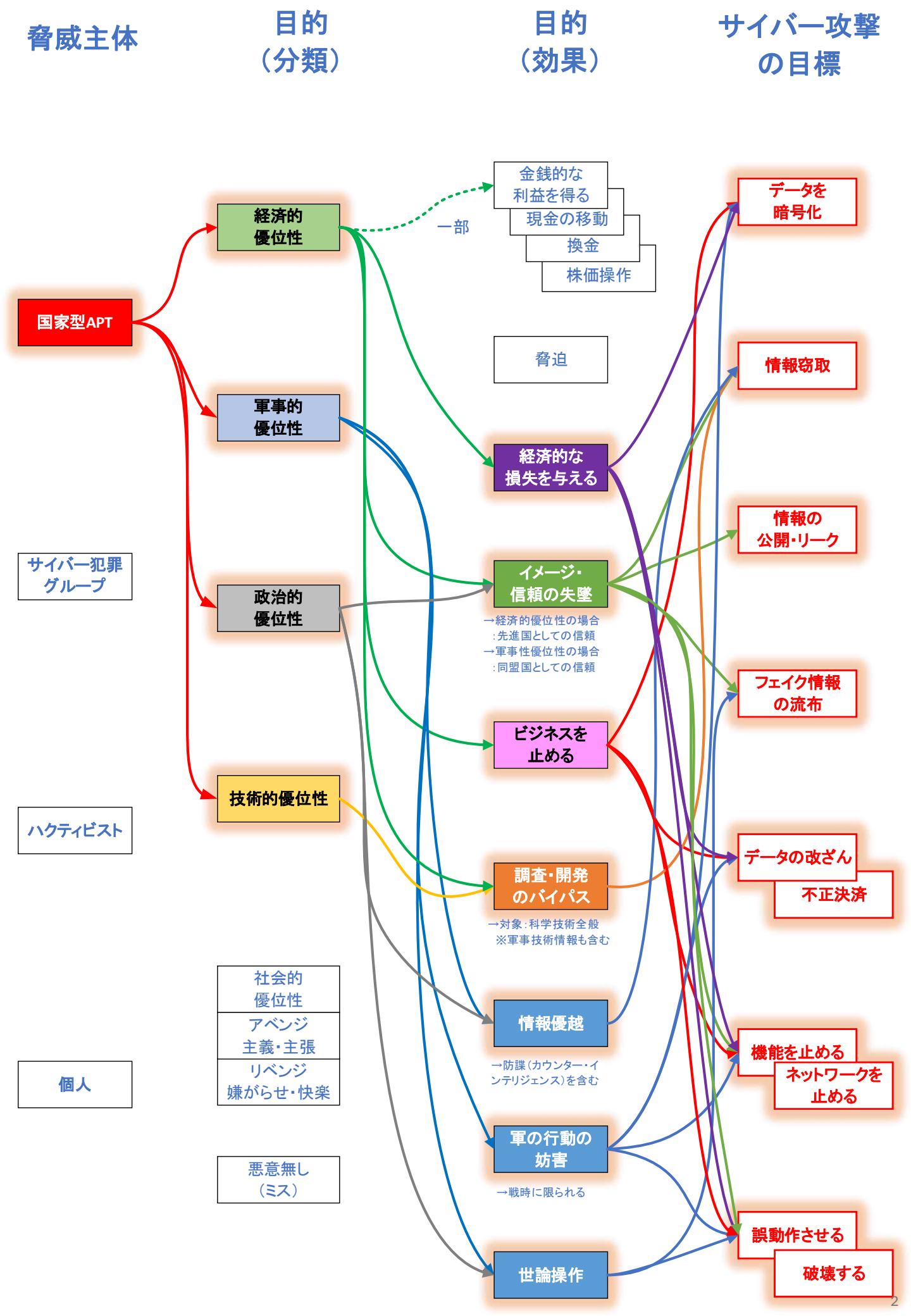
- 主に、対象国の政府機関、軍隊、重要インフラや大企業などが攻撃の標的となる
- これらを攻撃するための足掛かりとして、サプライチェーンを構成する関連企業が狙われることもある
  – 侵入経路や情報源としてのサプライチェーンの侵害
  – 対象組織に影響を及ぼすことを目的としたサプライチェーンへの攻撃

T 関係する情勢や法・規制

- 国家間の政治的、軍事的、経済的な対立に大きく左右される
- 特に、これらの緊張が増大する時期、あるいは技術的な転換点や経済発展を望む時期において、活動が活発化する可能性がある
- 法規制の制限を回避するため、犯罪グループなどに攻撃を肩代わりさせる可能性がある

T 組織とリソース

- 国家レベルの豊富なリソース（資金、人員、情報、技術、設備など）を有し、目的達成のために必要なあらゆる攻撃手段を使用することが可能
- 長期間にわたって攻撃を継続する能力を有し、不正アクセスだけでなく対象組織への潜入や協力者獲得工作など、軍事組織に準ずる高度な作戦を行う可能性がある
- 軍事組織や大企業に準ずる構成をとり、高度に指揮・統制された行動を行う


脅威主体
目的（分類）
目的（効果）
サイバー攻撃の目標
国家型APT
サイバー犯罪グループ
ハクティビスト
個人
経済的優位性
軍事的優位性
政治的優位性
技術的優位性
社会的優位性
アベンジ主義・主張
リベンジ嫌がらせ・快楽
悪意無し（ミス）
一部
金銭的な利益を得る
現金の移動
換金
株価操作
脅迫
経済的な損失を与える
イメージ・信頼の失墜
→経済的優位性の場合：先進国としての信頼
→軍事性優位性の場合：同盟国としての信頼
ビジネスを止める
調査・開発のバイパス
→対象：科学技術全般
※軍事技術情報も含む
情報優越
→防諜（カウンター・インテリジェンス）を含む
軍の行動の妨害
→戦時に限られる
世論操作
データを暗号化
情報窃取
情報の公開・リーク
フェイク情報の流布
データの改ざん
不正決済
機能を止める
ネットワークを止める
誤動作させる
破壊する

国家のサイバー攻撃に対する責任の分類（国家関与度スペクトラム）(2)

概　要

国家責任のスペクトラムは、アナリストが特定の攻撃や攻撃キャンペーンの責任をより正確に明確にするためのツールです。
このスペクトラムでは、国家が攻撃を無視する、助長する、または実行するかに応じて、責任の度合いを10のカテゴリーに分けています。責任の範囲は、攻撃を引き起こす可能性のある不安全なシステムを持つだけという受動的なものから、自ら攻撃を計画し実行する能動的な国家政府まで多岐にわたります。

関与度	カテゴリ	解説
禁止 ↓ 不十分 ↓ 黙認 ↓ 推奨	1	**国家は禁止している。**国家政府は、第三者による攻撃を防止するために協力します。攻撃はその領土内から発信されるか、単にそのネットワークを通過するかもしれません。この責任は、協力しているものの、攻撃に関与する不安全なシステムに対して一定の責任を負うという、最も受動的なものです。実際には、国家は自国の国境内にある数千万から数億台のコンピューターの適切な行動を常に確保することはできません。
	2	**国家は禁止しているが不十分。**国家政府は協力的であり、第三者による攻撃を阻止しようとしますが、実際にはそれができません。国には適切な法律、手続き、技術的手段、またはそれらを使用するための政治的意志が欠けているかもしれません。その国自体が被害者である可能性があるにもかかわらず、攻撃を止められないこと、そしてそもそも不安全なシステムを持っていることに対して、ある程度の受動的な責任を負います。
	※以下の4つのカテゴリでは、前の2つとは対照的に、国家が積極的に攻撃を無視または助長しています	
	3	**国家は黙認している。**国家政府は第三者による攻撃を知っていますが、政策として公式な行動を取ることを望んでいません。政府は攻撃者の目標と結果を黙認し、検出を避けるために彼らに情報を提供することさえあります。
	4	**国家が推奨している。**第三者が攻撃を制御し実行しますが、国家政府は政策として彼らを奨励します。この奨励には、国家運営の報道機関による社説や、攻撃の目標に公開で同意する指導者が含まれます。政府のサイバー攻撃部隊や諜報機関のメンバーが、勤務時間外に支援的な「レクリエーションハッキング」を行うことを奨励されるかもしれません。国家は調査に協力する可能性が低く、攻撃者に情報を提供する可能性が高いです。

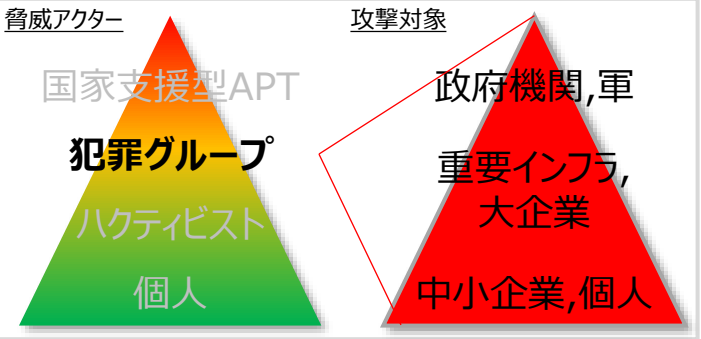
国家のサイバー攻撃に対する責任の分類（国家関与度スペクトラム）(2)

関与度	カテゴリ	解説
支援	5	**国家が支援する。**第三者が攻撃を制御し実行しますが、国家は何らかの支援を提供します。例えば、政府内の同じ考えを持つ個人と攻撃グループとの間の非公式な調整です。政府は、自分たちの政策を推進するために、サイバー部隊のメンバーに勤務時間外に「レクリエーションハッキング」を行うよう奨励するかもしれません。
調整	6	**国家による調整。**国家政府は第三者の攻撃者を非公開で調整し、ターゲットやタイミング、その他の運用の詳細を「提案」します。政府はまた、技術的あるいは戦術的な支援を提供することもあります。形成された攻撃と同様に、政府はサイバー部隊のメンバーに勤務時間外のハッキングを奨励するかもしれません。 最後の4つのカテゴリでは、国家は攻撃を無視または奨励するだけでなく、それを直接指示または実行しています。
	※以下の4つのカテゴリでは、ここまでの6つとは違い、国家が自らサイバー攻撃を指示又は実行します	
指示	7	**国家による指示。**国家政府は政策として第三者に指示して攻撃を行います。これは、政府のサイバー部隊による直接攻撃ではなく、最も「国家支援」の攻撃です。国家の管理下にある攻撃者は、国際法の下で事実上国家の代理人とみなされるかもしれません。
一部による実行	8	**国家の一部による攻撃。**国家政府のサイバー部隊の一部が攻撃を実行しますが、国家の指導者の認知や承認なしに行われます。国家指導者が攻撃を知った場合、それを止めようとするかもしれません。例えば、地方部隊や若い将校が上級将校の目の届かないところで反撃を試みるかもしれません。さらに懸念されるのは、国家指導者と対立する大規模な官僚機構による高度で持続的な攻撃です。現在の先例に基づけば、国家はこうした暴走した攻撃に対して国際裁判所で責任を問われる可能性があります。
実行	9	**国家による実行。**国家政府は政策として、自らのサイバー部隊を用いて攻撃を直接制御し実行します。
統合	10	**国家による統合。**国家政府は第三者の攻撃者と政府のサイバー部隊を統合し、共通の指揮統制を持ちます。命令と調整は正式または非公式であるかもしれませんが、政府がターゲット、タイミング、テンポを選択する際に統制します。攻撃者は事実上国家の代理人です。

【引用】https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF

サイバー犯罪グループ

サイバー犯罪グループは、金銭的利益の獲得のためにサイバー攻撃を行う組織的な脅威アクターです。
近年、サイバー犯罪は高度にビジネス化しており、国家、他の犯罪組織や個人との金銭的な契約によって活動します。



M 活動目的

- 金銭的利益の獲得を目的とすることが多く、個人情報や知的財産をターゲットとする。盗難したデータを闇サイトで売買したり、ランサムウェアなどを用いて機密情報を人質に身代金を要求したりすることもある
- 攻撃グループとしての実績を上げ、攻撃依頼者からの信頼を得る

E サイバー攻撃の標的

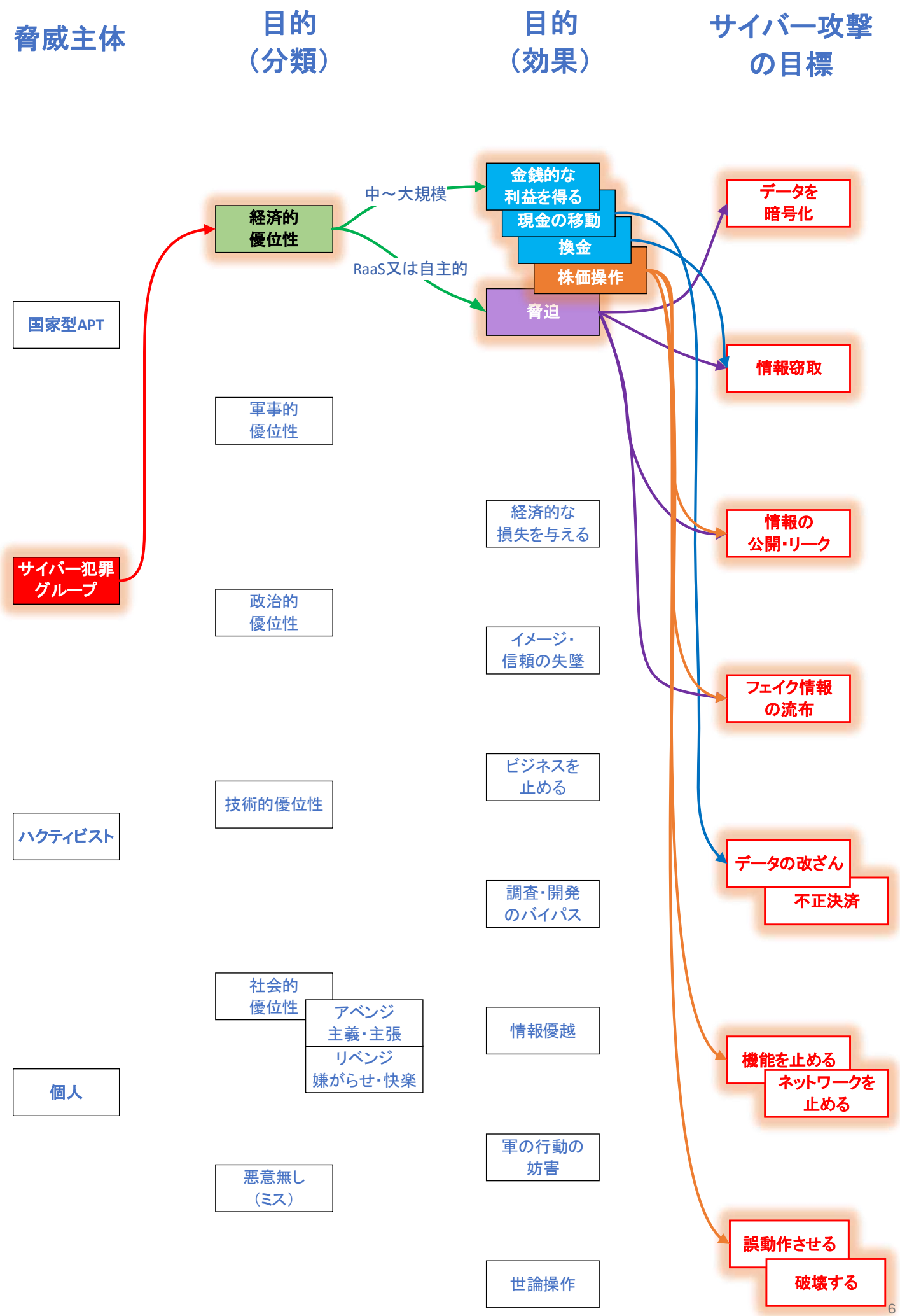
- 金融機関：直接的な金銭的利益を得られる
- テクノロジー企業：革新的な技術や知的財産を狙う
- 公共インフラ：社会的な必要性が高いため、高額の身代金が期待できる
- 中小企業：大企業よりもセキュリティ対策が行き渡ってない傾向があるため、迅速かつ容易に利益を得られる可能性がある
  サプライチェーンの弱点として、踏み台目的で狙う可能性もある

T 関係する情勢や法・規制

- 国際関係の緊張や政治的不安は、サイバー犯罪グループの活動を誘発することがある
- データ保護を含めた情報セキュリティ規制やインターネット上の不正行動の監視、国際的な協力協定が整備されセキュリティレベルが向上されることで、サイバー犯罪グループは活動しにくくなる

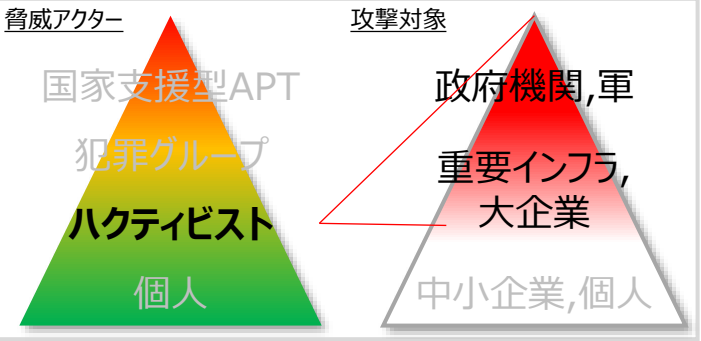
T 組織とリソース

- 組織規模は様々だが、企業と似た構造となっており、組織内で分業・連携しながら活動する（グループリーダ、技術者（ハッカー）、事務スタッフ、情報提供者など）
- 国家支援型APTほどではないが、様々な攻撃を行うための技術的リソース、資金、標的情報や情報網を有する


脅威主体
目的
（分類）
目的
（効果）
サイバー攻撃
の目標
国家型APT
サイバー犯罪
グループ
ハクティビスト
個人
経済的
優位性
中～大規模
RaaS又は自主的
軍事的
優位性
政治的
優位性
技術的優位性
社会的
優位性
アベンジ
主義・主張
リベンジ
嫌がらせ・快楽
悪意無し
（ミス）
金銭的な
利益を得る
現金の移動
換金
株価操作
脅迫
経済的な
損失を与える
イメージ・
信頼の失墜
ビジネスを
止める
調査・開発
のバイパス
情報優越
軍の行動の
妨害
世論操作
データを
暗号化
情報窃取
情報の
公開・リーク
フェイク情報
の流布
データの改ざん
不正決済
機能を止める
ネットワークを
止める
誤動作させる
破壊する

ハクティビスト

ハクティビストは、特定の主義・主張を流布することを目的としてサイバー攻撃を行う個人または組織によって構成される脅威アクターです。攻撃の発覚を恐れず、むしろ宣伝的な活動を行う点で他の脅威アクターと大きく異なります。



M 活動目的

- 自身の主義・主張を広く世間に流布する（環境破壊や捕鯨への反対など）
- 主義・主張に反する組織の活動や業務を直接的に妨害する
- 意図的に攻撃の痕跡を残したり、メッセージを発信することにより、自分たちの存在を世間にしらしめ、社会的発信力を高める

E サイバー攻撃の標的

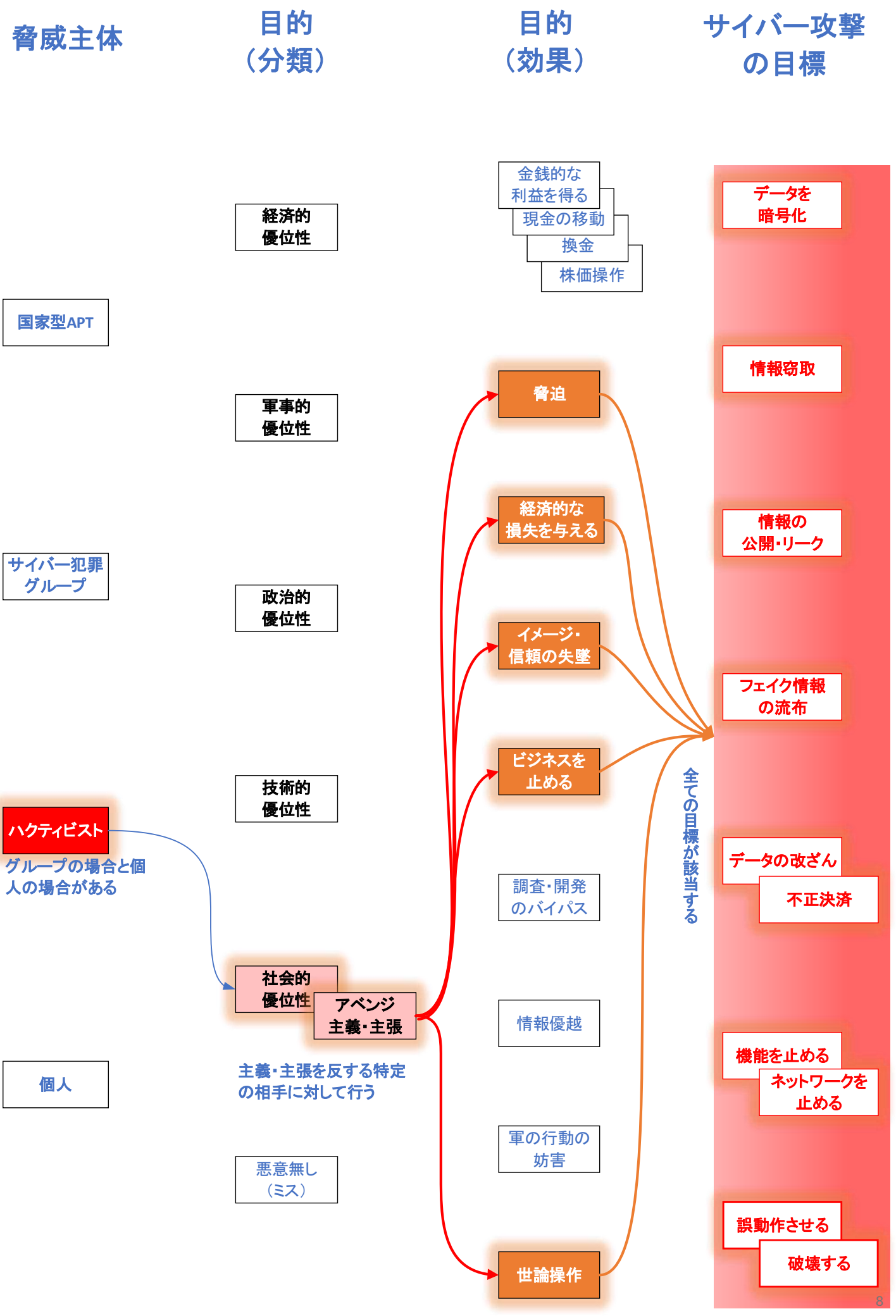
- 基本的には、攻撃者の主義・主張に反する組織を狙う傾向にある
- 時には、メディアに取り上げられるために、注目度の高い組織を無差別に狙い、話題性を獲得しようとすることもある

T 関係する情勢や法・規制

- 政治的、軍事的、経済的なトレンド（環境問題、宗教問題、LGBT問題など）に大きく左右される
- 世界的に注目を集めるイベント（国際会議、国家行事や大規模デモなど）がある場合に活動が活発になることが多い

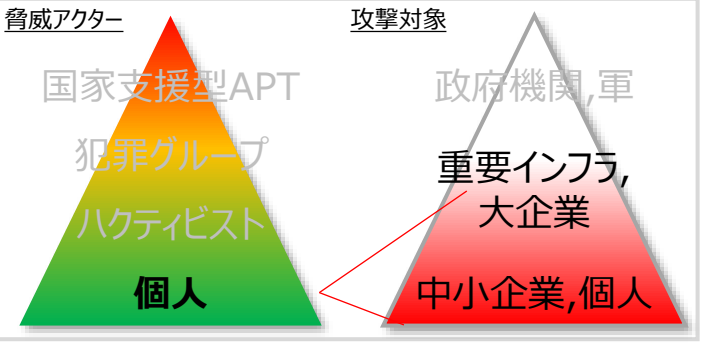
T 組織とリソース

- 個人または共通の目的を持った組織によって構成される
- グループ内の一部が異なる主義主張のために活動することもあり、犯罪グループと比べると緩い統制関係であることが予想される
- 個人から大規模なグループまであり、組織規模と保有リソースも大小様々である


脅威主体
目的
（分類）
目的
（効果）
サイバー攻撃
の目標
経済的
優位性
軍事的
優位性
政治的
優位性
技術的
優位性
社会的
優位性
国家型APT
サイバー犯罪
グループ
ハクティビスト
グループの場合と個
人の場合がある
個人
アベンジ
主義・主張
主義・主張を反する特定
の相手に対して行う
悪意無し
（ミス）
金銭的な
利益を得る
現金の移動
換金
株価操作
脅迫
経済的な
損失を与える
イメージ・
信頼の失墜
ビジネスを
止める
調査・開発
のバイパス
情報優越
軍の行動の
妨害
世論操作
全ての目標が該当する
データを
暗号化
情報窃取
情報の
公開・リーク
フェイク情報
の流布
データの改ざん
不正決済
機能を止める
ネットワークを
止める
誤動作させる
破壊する

個人の攻撃者

個人的な恨みや欲望を満たすためにサイバー攻撃を行う人であり、攻撃手法は比較的低級です。
一方、組織における内部犯行の場合は、外部脅威よりも容易に攻撃が可能であり、被害も大きくなるため注意が必要です。従業員による悪意のないミスもこれに含まれます。



M 活動目的

- 特定の企業や個人に対する嫌がらせや復讐（リベンジ）
- 習得したサイバー攻撃手法を試してみたいという好奇心や、世間に能力を示して自己顕示欲を満たすための攻撃

E サイバー攻撃の標的

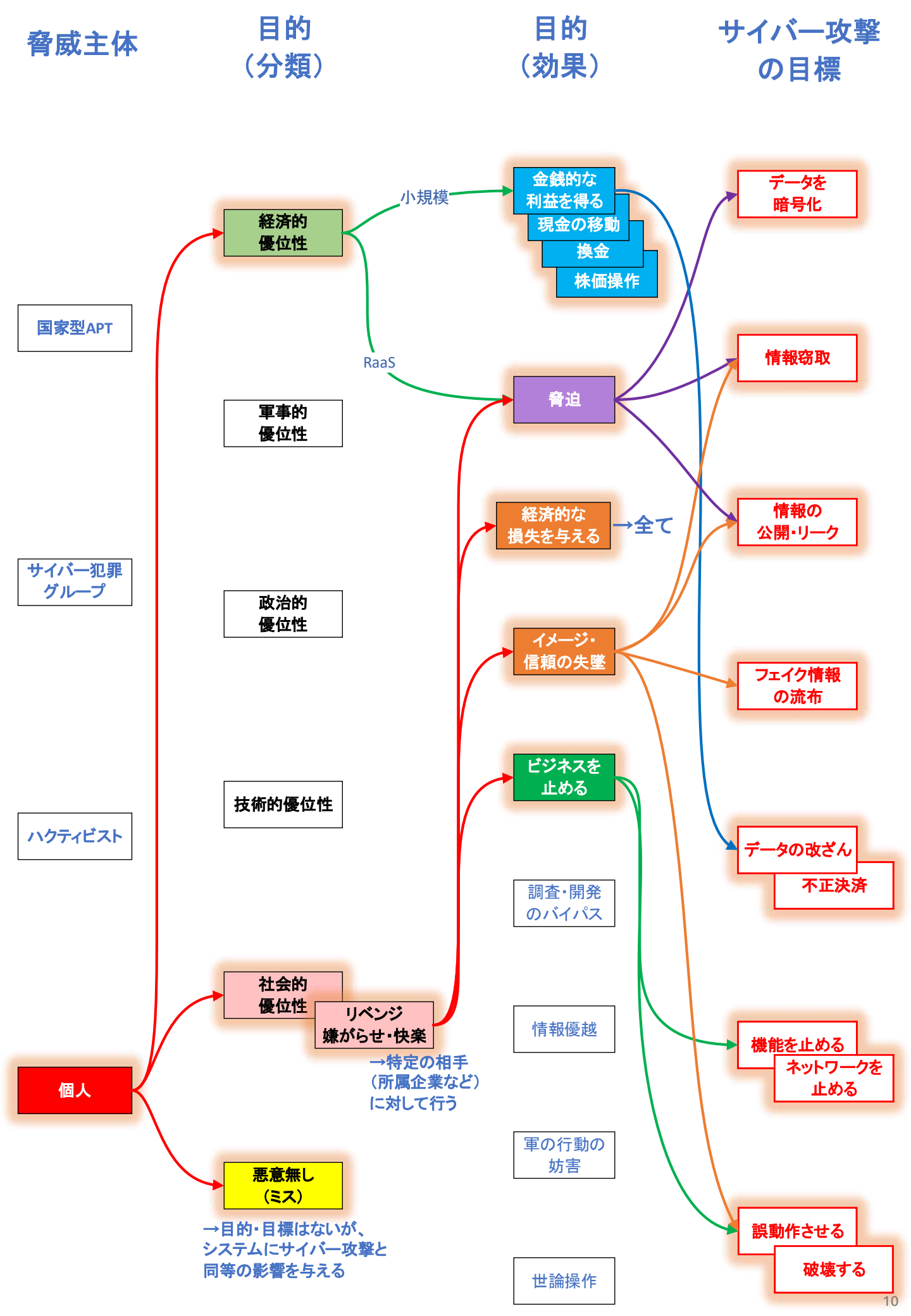
- 特定の企業組織又は個人
  - 低すぎる給与や不当な扱い等により、従業員の恨みを買った企業又は職場
  - 私生活で何らかの恨みを買った個人
  - 自己顕示欲を満たすのにちょうどいい、セキュリティ対策レベルの低い企業

T 関係する情勢や法・規制

- 国際的・社会的な情勢に影響されることは少ないと思われる
- 所属組織（前所属も含む）の風土、待遇や、個人的な人間関係等が関係する可能性が高い

T 組織とリソース

- 単独での犯行であるため、容易に入手可能なスキルや攻撃ツールを使用する
- 恨みの度合いによっては、長期間に渡り綿密な計画を立てる可能性がある
- 内部犯の場合、内部情報に精通しており、特権などを駆使して脆弱な箇所を攻撃することがある
- 企業に恨みを持つ個人が国家支援型APTに買収され、犯行に及ぶことがある


脅威主体
目的
（分類）
目的
（効果）
サイバー攻撃
の目標
国家型APT
サイバー犯罪
グループ
ハクティビスト
個人
経済的
優位性
軍事的
優位性
政治的
優位性
技術的優位性
社会的
優位性
悪意無し
（ミス）
→目的・目標はないが、
システムにサイバー攻撃と
同等の影響を与える
小規模
RaaS
金銭的な
利益を得る
現金の移動
換金
株価操作
脅迫
経済的な
損失を与える
→全て
イメージ・
信頼の失墜
ビジネスを
止める
調査・開発
のバイパス
情報優越
軍の行動の
妨害
世論操作
リベンジ
嫌がらせ・快楽
→特定の相手
（所属企業など）
に対して行う
データを
暗号化
情報窃取
情報の
公開・リーク
フェイク情報
の流布
データの改ざん
不正決済
機能を止める
ネットワークを
止める
誤動作させる
破壊する

別紙第３

「戦いの原理・原則から考える

サイバー攻撃者の戦術」

本別紙では、脅威主体の目線になりきり、脅威主体がサイバー攻撃を行う際にどのような考えを行っているか、ＭＥＴＴと戦いの９原則に沿って分析してみましょう。

なおそれぞれのケースは、実際にサイバー攻撃を受けた事例と、被害を受けた企業から提供された詳細情報を参照しておりますが、不足している情報については私たちのほうで想像を膨らませ、情報を付加しておりますのであらかじめご承知おきください。

１　サイバー犯罪グループの場合

４．３節でも述べたとおり、サイバー犯罪グループは経済的優位性を獲得するため、組織としてサイバー攻撃を仕掛けます。実際にサイバー犯罪グループが攻撃を行う際の、ＭＥＴＴと戦いの９原則がどのように関連するのか、段階を追って分析してみましょう。ここでは、実際に日本で発生したサイバーインシデントをもとに、ランサムウェアの感染および機密データの窃取被害を引き起こした標的型攻撃の事例を参照しています。

＜事例の概要＞

- とある企業（ここではＡ社とします）は、第三者（以下、サイバー攻撃者とします）によるランサムウェアを用いた標的型のサイバー攻撃を受け、複数の業務主幹サーバの暗号化、アクセスログ削除の被害を受けた。
- サイバー攻撃者は、リモート接続機の脆弱性を利用することで、Ａ社社内ネットワークに不正アクセスし、探索行為を実行していた。
- 第三者はサイバー攻撃決行時、外部と接続しているクラウドサービス上から不正侵入し、ＥＤＲ機能を停止させたうえでランサムウェアを展開した。またサイバー攻撃完了後は、イベントログの消去も行っている。

▶▷▷▷▷▷　次頁「**⓪ 攻撃の前段階**」に続く

⓪　攻撃の前段階

攻撃の前段階では、主にサイバー犯罪グループが経済的優位性を得られそうな標的を探す段階です。

この時点のＭＥＴＴと９原則は以下のとおりとなります。

【ＭＥＴＴ】

Ｍ：目的	**標的ターゲットから金銭又は金銭に変換できる資産を奪う**
Ｅ：敵の状況	未定（セキュリティに付け入る隙がある企業）
Ｔ：法、規制	**法、規制はある**
Ｔ：組織、リソース	**偵察班、攻撃実行班など組織として活動している高度の攻撃ツール、ノウハウも有している**

【９原則】

目標	**・バックドアファイルを無効化しランサムウェアを仕掛ける** **・機密データ等の情報を奪う**
主動	未定
集中	未定
節用	未定
統一	**・目標達成のため、組織内で連携を行う**
機動	未定
奇襲	未定
保全	**・攻撃や偵察の証跡をなるべく残さない**
簡明	・組織内で情報共有を行う。

２．２項で述べたとおり、ＭＥＴＴは**戦い方を決めるために必要な要素**となることから、自組織の目的やリソースなどが当てはまります。この目標達成のため、脅威主体が持ちうる攻撃ツールやハッキングスキルが有効に発揮できる標的（企業や団体など）を索敵します。

一方で、９原則についてはほとんど未定の状態です。２．３項で述べたとおり、戦いの９原則は**戦いにおいて適合すべき要件**となります。攻撃者がサイバー攻撃を実行する際、攻撃者にとって優位な状況にするためには、適合すべき要件を明確にしなければなりません。そのためにも標的を偵察し、侵入口や攻撃手法を決定するための情報を取得する必要があります。

▶▶▷▷▷▷　次頁「**① 標的の特定**」に続く

①　標的の特定

サイバー犯罪グループの偵察班が、脆弱性を有するリモート接続機器を活用しているＡ社を発見しました。Ａ社のホームページ等、公開情報を閲覧したところ、Ａ社は工業系の大手企業であり、技術情報や顧客情報など、攻撃者にとって魅力的な資産を有していそうであったため、サイバー攻撃の標的とすることを決定しました。

この時点のＭＥＴＴと９原則は以下のようになります。

【ＭＥＴＴ】（標的情報の追加）

Ｅ：敵の状況	**・Ａ社** **―リモート接続器に脆弱性を残している** **―大手工業企業** **―技術情報や顧客情報を有していそう**

【９原則】（標的に対する奇襲の追加）

奇襲	**・リモート接続器の脆弱性をついて不正アクセスを行う**

Ａ社からすれば、リモート接続器に脆弱性が残っている事態であると認識できていない。もしくは自社がすぐにサイバー攻撃を受けることはないだろう（後回しの対応）と高を括っているかもしれません。しかしサイバー犯罪グループからすれば、その油断こそが攻撃が成立する（奇襲の原則）絶好の機会となってしまっています。

▶▶▶▷▷▷　次頁「**② 標的の偵察**」に続く

②　標的の偵察

脆弱性を利用し、不正アクセスを行えたとしても、どのようなネットワーク構成なのか、どのようなドメイン管理をおこなっているのか、最終的に窃取する資産情報がどこに格納されているかを把握する必要があります。サイバー犯罪グループが初期偵察を行った結果、以下の運用を行っていることがわかりました。

- Ａ社はドメイン管理機能を外部と接続しているクラウドサービス上に構築している
- セキュリティ対策としてＥＤＲ機能を導入している
- セキュリティ対策として各機器のログを収集している
- リモート機器は従業員の事務端末と接続するために用いられている。
- 事務端末（アカウント）はドメイン管理されており、ドメイン管理サーバは限られたユーザのみアクセスできる

判明した情報は、サイバー犯罪グループがサイバー攻撃を行う際の戦略を立てる際に必要となる重要な情報（ＭＥＴＴにおけるＥに該当）です。この情報をもとに、攻撃の戦術を考えることが可能となり、攻撃プロセス中の具体的な行動目標を決定していくことでしょう。

なおＭＥＴＴと９原則は以下のように更新されます。

【ＭＥＴＴ】（標的情報の追加）

Ｅ：敵の状況	**・Ａ社** **―リモート接続器に脆弱性を残している** **―リモート接続器を用いて事務端末と接続される** **―事務端末（アカウント）はドメイン管理されている** **―Ａ社は外部に接続するクラウドサービスを利用しており** **クラウド上にドメイン管理機能を構築している** **―ＥＤＲ機能を導入している** **―ログ収集・管理を行っている**

【９原則】（攻撃時の行動目標を追加、攻撃プロセスの詳細は未定）

主動	**・ドメイン権限を奪う（攻撃時の行動目標）** **・ＥＤＲ機能を停止させる（攻撃時の行動目標）**
節用	**・未定（偵察した情報から、最適な攻撃プロセスを決定する）**
機動	
保全	・攻撃の証跡をなるべく残さない **←ログ情報を削除する（攻撃時の行動目標）**
統一	**・攻撃実行班に、偵察して判明した標的の詳細情報を伝える**
簡明	

行動目標が決まりましたが、サイバー犯罪グループは偵察を続けることでしょう。この時点からの偵察は、標的の特徴を掴むためでなく、攻撃の成功確率を引き上げるための弱点情報を求めるために目的が変わります。例えば、ダークウェブを用いて標的の情報（メールアドレスや使用している機器など）を検索するかもしれないですし、不正アクセスしたポイントから稼働しているサービスや開放ポートなど偵察する可能性も考えられます。

▶▶▶▶▷▷　次頁「**③ 攻撃プロセスの計画**」に続く

③　攻撃プロセスの計画

攻撃者は②の結果から、攻撃者にとって最適な攻撃プロセスを計画します。ここまでの情報で、A 社のネットワークには「偵察時にも利用したリモート接続器」と「外部と接続しているクラウドサービス」の 2 つの侵入経路が存在しています。侵入経路が変われば攻撃プロセスも異なります。４．３．４項で述べた「攻撃者にとって価値の高い攻撃手法」に沿ってそれぞれの攻撃プロセスについて評価を行ってみましょう。

Table1.　サイバー犯罪グループが攻撃プロセスを選択する際の比較（一例）

脅威アクターの懸念事項		サイバー犯罪グループが持つ重要度	ケースA ドメイン管理サーバへアクセス可能なユーザのアクセス情報を盗聴する		ケースB 外部クラウドサービスから直接ドメイン管理サーバへアクセスする	
			攻撃の特徴	攻撃者にとっての有利性	攻撃の特徴	攻撃者にとっての有利性
攻撃の容易性	攻撃元区分	低い	ネットワーク	高い	ネットワーク	高い
	攻撃条件の複雑さ		パケットを盗聴しログイン情報を入手する	高い	正規のログイン情報のみ必要	高い
	必要特権ﾚﾍﾞﾙ		ドメイン管理サーバへアクセスできる権限が必要	低い	不要	極めて高い
	ﾕｰｻﾞ関与度		必要	低い	不要	極めて高い
攻撃に必要なコスト		高い	なし	高い	なし	高い
期待できる効果		高い	認証機能を侵害することで 以降の攻撃が容易になる	極めて高い	セキュリティ対策を無効化できる	極めて高い
主体が特定されるリスク		低い	検知されにくい 隠蔽を用いる	高い	検知されにくい	高い
確実性・任意操作性		高い	ドメイン管理サーバへアクセスがあるか不確実	低い	時期と場所を選択可能	高い

ケース A の場合、高い権限を有するアカウントがログインする行動が必要となり、確実性は低くなってしまいます。一方でケース B の場合、外部クラウドサービスから侵入しなおすことで、ユーザの関与は不要となり、確実性が高くなります。攻撃者側から考えてみたとき、ケース B の攻撃プロセスの方が魅力的なプロセスであることがよくわかります。ケース B の課題はクラウドサービスのログイン情報を把握することになりますが、A 社がデフォルトの設定から変更していなければ総当たりのログイン試行で突破できるでしょう。偵察段階でダークウェブを利用し該当するクラウドサービスのログイン情報を入手することができていれば、より確実性は増すことになるでしょう。

攻撃は単一でなく、同時並行で仕掛ける攻撃事例も多く見受けられます。主軸の攻撃はケース B とした裏で、かく乱目的も含めケース A の攻撃手法も継続して行われる可能性も考えられます。

比較した結果から、サイバー犯罪グループ内では外部クラウドサービスから侵入する計画（ケース B）で決行することにしました。攻撃プロセスが決定した段階で、９原則に当てはめた攻撃者側の行動目標は以下のとおりになります。

【9原則】（攻撃時の行動目標を追加、攻撃プロセスも決定）

主動	**・ドメイン権限を奪う（攻撃時の行動目標）** **・ＥＤＲ機能を停止させる（攻撃時の行動目標）**
節用	**・外部クラウドサービスから不正侵入し、ドメイン権限を有した状態でログインする（行動時の行動目標）**
機動	
保全	・攻撃の証跡をなるべく残さない **←ログ情報を削除する（攻撃時の行動目標）**
統一	**・攻撃実行班に、偵察して判明した標的の詳細情報を伝える**
簡明	

▶▶▶▶▶▷　次頁「④ **攻撃の実行**」に続く

④　攻撃の実行

攻撃計画がより具体的になったところで、あとは実行に移すのみです。さらに攻撃成功確率を引き上げるため、不正アクセスが企業側に発見されても早期対応が難しくなるようサイバー攻撃は深夜に決行することにしました。サイバー攻撃の目標は機密データの窃取やランサムウェアの設置ですが、かく乱目的で、企業に対しＤＤｏＳも平行して仕掛けることにしました。

【9原則】（攻撃プロセスの行動結果）

目標	・機密データ等の情報を奪う→個人情報及び個人情報の窃取（**行動済み**）
主動	・ドメイン権限を奪う（**行動済み**） ・ＥＤＲ機能を停止させる（**行動済み**）
集中	・権限の低い事務アカウントからアクセスするのではなく、外部クラウドサービスからドメイン管理機能にアクセスし高い権限を獲得する（**行動済み**） **・同時並行でＤＤｏＳを仕掛ける（かく乱目的）**
節用	
奇襲	**・攻撃を深夜に決行する（行動済み）**

計画どおりに攻撃計画を実行していても、想定外の事態に遭遇することも多いでしょう。しかし、サイバー犯罪グループで所持している様々な攻撃ツールを有効的に活用し、臨機応変に対応し、突破していることでしょう。

▶▶▶▶▶▶　次頁「**⑤ 目標の達成**」に続く

⑤　目標の達成

ＥＤＲ機能を停止させることで、あらゆる基幹サーバを自由自在にコントロールできるようになりました。最後にバックアップファイルを削除し、各サーバにランサムウェアを仕掛け、操作したサーバや端末のログ情報を削除することで攻撃プロセスは完了しました。最終的な９原則は以下のようになります。

【９原則】（攻撃目標の達成）

目標	**・バックアップファイルを無効化しランサムウェアを仕掛ける（行動済み）**
保全	**攻撃の証跡をなるべく残さない** **←ログ情報を削除する（行動済み）**

ランサムウェアによって暗号化されたサーバを復元するためには、身代金要求に応対するか企業側次第ですが、少なくともダークウェブに販売することで利益を得ることが期待できる機密データを入手することができました。

▷　次頁「**サイバー犯罪グループがサイバー攻撃を行う場合**」のまとめ

改めて、今回取り上げた事例においてサイバー犯罪グループが行った一連の攻撃の流れと思考プロセスをまとめました。

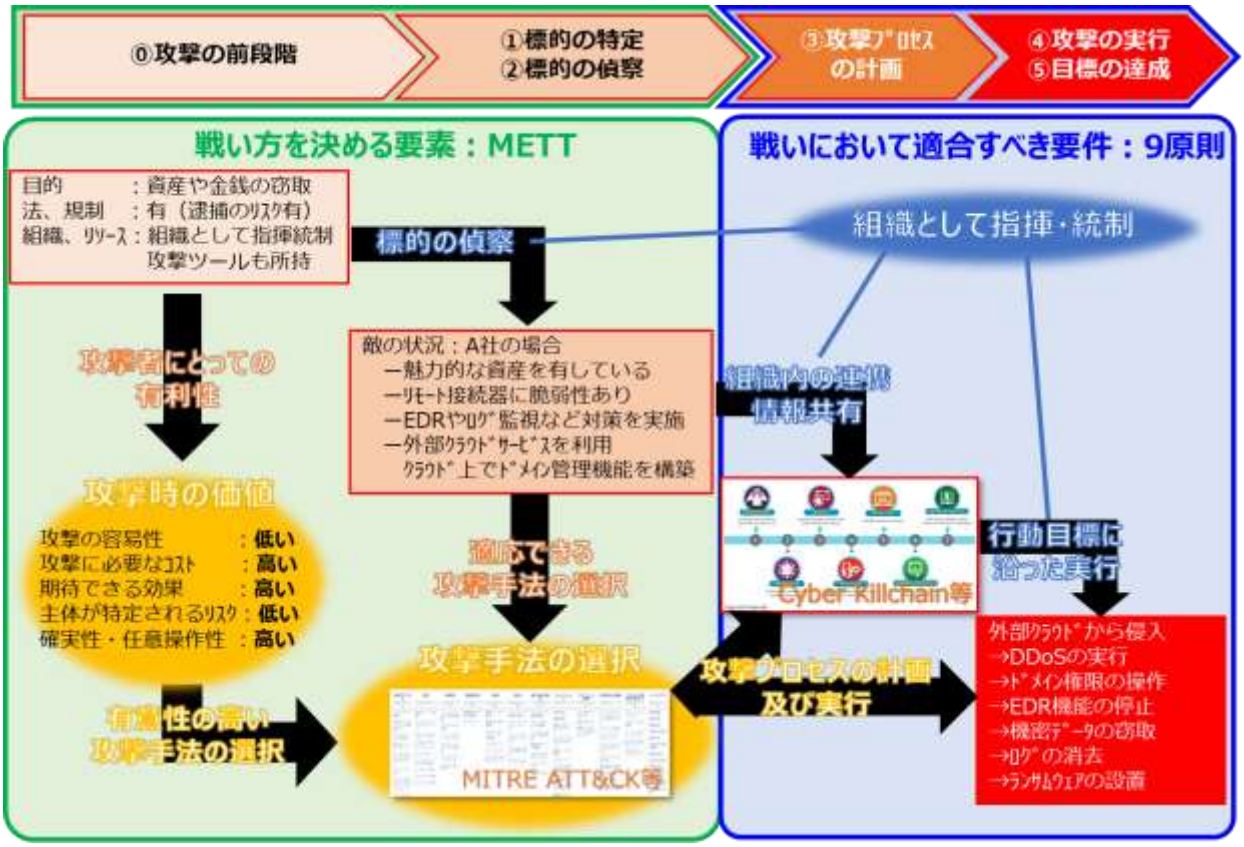


Fig1.　サイバー犯罪グループが攻撃を行った際の思考プロセス（一例）

「④　攻撃の実行」段階でも触れましたが、攻撃計画を実行している最中にも様々な状況変化や新情報が発生することでしょう。しかし、組織として情報が統制され、攻撃ツールの機能を把握し、事前の偵察中に得た情報から攻撃の戦略・戦術を立てていることで、目標が明確になっており、攻撃実行班の行動には迷いや無駄が少なくなっているに違いありません。

「**サイバー犯罪グループの場合**」のシナリオ終了　◀

２　個人の攻撃者の場合

４．３節でも述べたとおり、個人の攻撃者は自身の承認欲求を満たすためや組織への怨恨によりサイバー攻撃を仕掛けます。本シナリオで、個人の攻撃者がサイバー攻撃を行う際、ＭＥＴＴと戦いの９原則がどのように関連するのか、ポーランドの鉄道会社が運営する路面電車が１４歳少年のサイバー攻撃により脱線した事例をもとに段階を追って分析してみましょう。

参考：https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

＜事例の概要＞

- １４歳少年がポーランドの鉄道会社が運営する路面電車停留所に物理侵入し、車両の進路を切り替えるポイント制御装置を不正操作するために必要な情報を窃取した
- 窃取した情報を元に、TV リモコンを改造しポイント制御装置を制作した
- 制作した装置を用いて無線端末からポイント制御装置を遠隔操作し、車両を脱線させた

▶▷▷▷▷　次頁「**⓪ 攻撃の前段階**」に続く

⓪　攻撃の前段階

攻撃の前段階は攻撃者が標的を探す段階です。今回の事例では犯人が１４歳の少年であることを考慮して、目的は自身の承認欲求を満たす（技術力を誇示する）ことであると仮定します。

この時点のＭＥＴＴと９原則は以下のとおりとなります。

【ＭＥＴＴ】

Ｍ：目的	**自身の技術力を誇示する**
Ｅ：敵の状況	**社会的有名度がある（標的の特定はまだ）** **且つ自身の技術力や予算に見合った組織**
Ｔ：法、規制	**法、規制はある**
Ｔ：組織、リソース	**ハッキング能力や無線通信の知識を有している** **攻撃のための資金や組織的な構成はない**

【９原則】

目標	**覚えた技術を用いてハッキングを成功させる**
主動	未定
集中	未定
節用	**個人且つ若年者のため低コストで実現する**
統一	―（個人での犯行のため）
機動	**自身の行動範囲内に拠点がある**
奇襲	未定
保全	未定
簡明	個人での犯行であるため指揮系統はなく簡明である

少年は個人且つ若年者であることから、以下の条件を満たす組織に攻撃を仕掛けることを考えます。

- 自身のスキルを拠り所にするため攻撃が低コストで可能であること
- 今後の作戦行動を容易にするため自身の行動可能範囲内に拠点があること
- 自身の技術力を誇示するために世間にインパクトを与えることができること

▶▶▷▷▷　次頁「**① 標的の特定**」に続く

①　標的の特定

少年が自身の技術力と予算や行動可能範囲を考慮した上で技術力を誇示するに相応しい相手として、鉄道会社をサイバー攻撃の標的とすることを決定しました。少年は鉄道インフラの事故を起こせば世間の注目を浴びることができるため、鉄道会社を標的にしたと考えられます。

この時点のＭＥＴＴと９原則は以下のとおりとなります。

【ＭＥＴＴ】（標的情報の特定）

Ｅ：敵の状況	**鉄道会社**

【９原則】（標的に対する影響の追加）

目標	**車両を脱線させる**

▶▶▶▷▷　以下「**② 標的の偵察**」に続く

②　標的の偵察

少年が鉄道会社の偵察を行った結果、停留所内の車両の運行に係る制御装置に物理的にアクセスすることが可能であると確認できました。少年は停留所内に物理侵入することで速度制御装置及びポイント制御装置の情報を窃取することに成功します。

この時点のＭＥＴＴと９原則は以下のとおりとなります。

【９原則】（標的に対する奇襲の追加）

奇襲	**停留所に物理侵入し速度制御装置及びポイント制御装置の情報を窃取する**

鉄道会社からすれば、制御装置の情報窃取が行われることはないと高を括っていたと思われます。しかし、その油断こそが奇襲として攻撃が成立する絶好の機会となりました。

▶▶▶▶▷　次頁「**③ 攻撃の実行**」に続く

③　攻撃の実行

少年はここで判明した情報から、攻撃者にとって最適な攻撃プロセスを計画します。少年がここまで窃取した情報で、速度制御装置或いはポイント制御装置に不正な信号を送信して車両を脱線させることを企てます。攻撃対象が変われば攻撃プロセスも異なります。４．３．４項で述べた「攻撃者にとって価値の高い攻撃手法」に沿ってそれぞれの攻撃プロセスについて評価を行ってみましょう

Table2.　個人の攻撃者が攻撃手法を選択する際の比較

脅威アクターの懸念事項		個人のサイバー攻撃者が持つ重要度	ケースA 車両の速度制御を異常操作させ脱線させる		ケースB 車両の進路切り替え装置（ポイント制御装置）を異常制御させ脱線させる	
			攻撃の特徴	攻撃者にとっての有利性	攻撃の特徴	攻撃者にとっての有利性
攻撃の容易性	攻撃元区分	極めて高い	ネットワーク	高い	ネットワーク	高い
	攻撃条件の複雑さ		速度制御信号を改ざんし送信する	低い	ON、OFFの信号を送信する	極めて高い
	必要特権ﾚﾍﾞﾙ		不要	高い	不要	高い
	ﾕｰｻﾞ関与度		不要	高い	不要	高い
攻撃に必要なコスト		極めて高い	複雑な制御が必要	低い	ON、OFFの制御なのでTVリモコンの改造で送信可能	極めて高い
期待できる効果		高い	車両を脱線させる	高い	車両を脱線させる	高い
主体が特定されるリスク		低い	不要	低い	不要	低い
確実性・任意操作性		高い	時期と場所を選択可能	高い	時期と場所を選択可能	高い

ケースA（速度制御装置）の場合、制御が複雑あることから不正信号を送信することが煩雑になります。それに比べケースB（ポイント制御装置）はON・OFFの制御で完結するため制御が容易です。

比較した結果から、少年はテレビのリモンコンを改造してポイント制御装置の遠隔操作端末を作成し、その端末によりポイント制御装置を不正操作し、車両を脱線させました。

９原則に当てはめた少年の行動計画は以下のとおりになります。

【９原則】

主動	**遠隔操作端末を作成できたことで時間的・目標的主導権を得た**
節用	個人犯罪者かつ若年者のため低コストで実現する **→遠隔操作端末はテレビリモコンを改造した**
奇襲	● 停留所に物理侵入しポイント制御装置の情報を窃取する ● **第三者にポイント制御装置が遠隔操作されまいと油断しているところを突いた**

少年はテレビリモコンを改造することで遠隔操作端末を作成しました。この端末の制作費用は非常に低コストであることが予想できます。これにより、少年は効果的な攻撃手段を低コストで得ていたことから節用の原則の観点において、非常に優れていたと言えます。また、この遠隔操作端末により、少年は時間及び目標的主導権を得ることができ、鉄道会社が予期していなかった攻撃を仕掛けることができたことから、主動・奇襲の原則の観点において優れていました。

▶▶▶▶▶ 以下「**④ 目標の達成**」に続く

④ 目標の達成

車両を脱線させたことで少年は世間の注目を浴び、自身の技術力を誇示したことで目標を達成することができました。

▷ 次頁「**個人の攻撃者がサイバー攻撃を行う場合**」のまとめ

改めて、今回取り上げた事例において個人の攻撃者が行った一連の攻撃の流れと思考プロセスをまとめました。

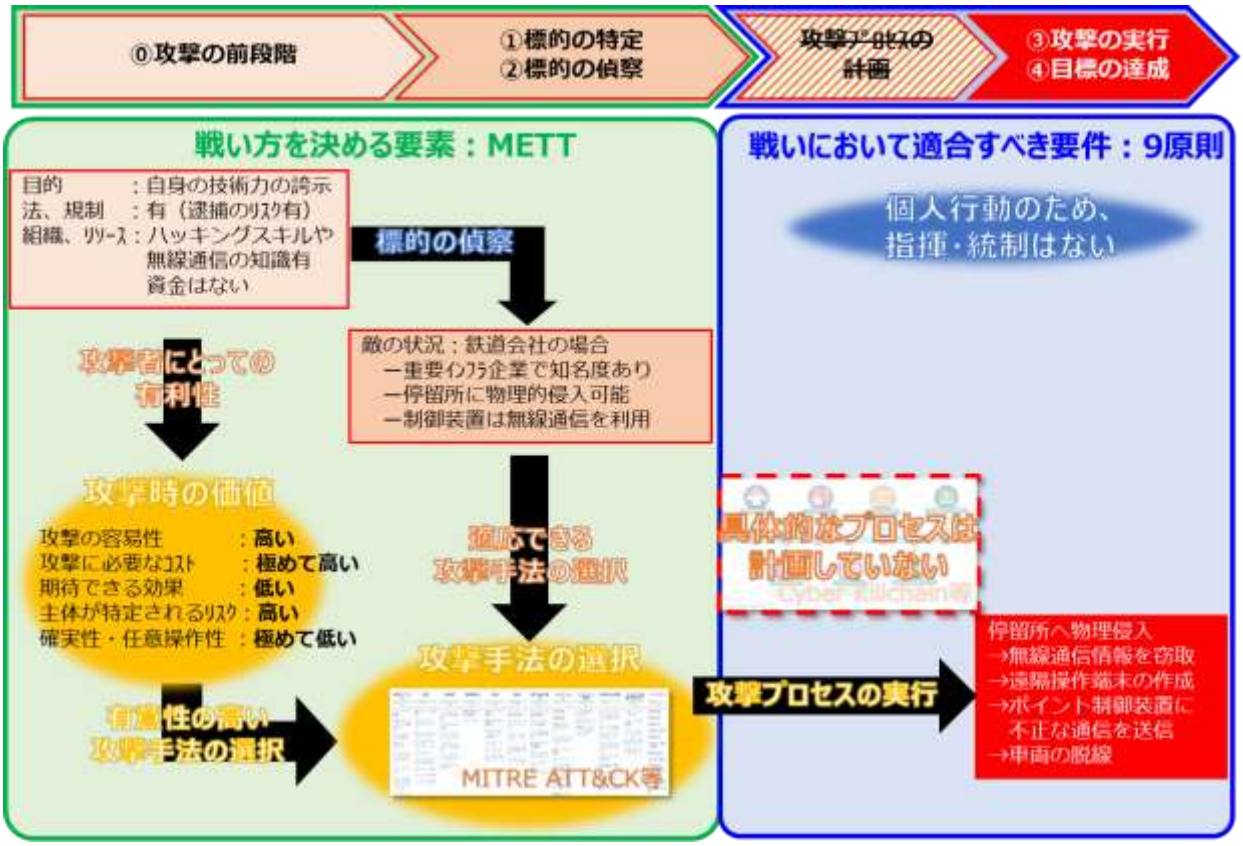


Fig2.　個人の攻撃者が攻撃を行った際の思考プロセス

本インシデントの事後になりますが、犯行を行った少年は現場に攻撃の痕跡を残してしまい、逮捕されてしまいました。攻撃の痕跡は記事には掲載されておらず、監視カメラに映ったのか、現行犯として身柄を拘束されたのかは不明です。これを戦いの９原則における観点からすると、保全の原則で優位性がとれていなかったと言い換えることができます。

しかし、鉄道会社にとって少年が逮捕されれば「勝ち」になるのでしょうか。少年にとって逮捕されることは「負け」になるのでしょうか。鉄道会社は脱線による運用の停止と、企業のイメージダウンというダメージを被り、少年は自信の技術力を誇示する結果になりました。戦いにおけるそれぞれの勝敗の捉え方は様々であり、勝ち負けについては第三者が決めるものではありません。本事例では攻撃者側の分析しかしていませんが、考察内だけで整理したとき、間違いなく少年は「勝ち」を手にしています。

「**個人の攻撃者の場合**」のシナリオ終了　◀

３　まとめ

サイバー攻撃被害を受けた企業や団体から、インシデントが発生した原因の報告記事を見聞きします。その内容は攻撃を受けた被害規模や攻撃を許してしまった原因、予想される攻撃プロセスなど、攻撃によって残った結果のみであることがほとんどです。

しかし、一例のように俯瞰して引き起こされたインシデント全体を整理してみると、インシデントの報告内容は攻撃した結果が残した断片的な情報にすぎません。なぜ攻撃者はその企業を狙ったのか、なぜその攻撃プロセスとしたのか。攻撃者にとっての価値や思考を少しでも知り、攻撃の戦術を予想することで、企業や団体の守るべきもの、守り方をより洗練することができることでしょう。

別紙第４

「サイバーセキュリティの課題解決のヒント」

セキュリティリスクの分析

～何を何から守るか？セキュリティの第一歩～

このフェーズでは、情報資産と脅威から組織のリスクを特定し、優先順位を検討します。

- 資産ベース、シナリオベース、事業被害ベースなど様々な手法・アプローチが存在
- セキュリティリスクは、脅威、脆弱性、影響度と発生可能性の要素を踏まえて評価する
- その後、評価したリスク（リスク値）に基づき、必要なセキュリティ対策を実施していく

【戦いの原理・原則を参考とした課題解決のヒント】

ちゃんとやろうとすればするほど、リスク分析は大変な作業です。時間、お金、人員など多くのリソースを必要とします。

Point	【集中・節用】リスク分析は極めて重要な業務です。他の業務とのバランスをとりつつ、必要なリソースを必ずアサインしてもらいましょう。
着眼	● 投入可能なリソースに応じて対象範囲を絞る ● コンサルなど外部の活用も視野に入れる

実情ではリスク分析を簡易的に行ったり対象範囲を絞るのはやむを得ません。しかし、やり方を誤ると極めて危険な状態（やった気になっている状態）を招きますので細心の注意が必要です。

Point	【任務】リスク分析はセキュリティの一丁目一番地です。ここでの失敗はセキュリティ全体に悪影響を与えることを再認識しましょう。
着眼	● 対象範囲を絞るときは特に慎重に議論する ● 現場の専門家も巻き込み、ビジネスオーナー又はリスクオーナーを長として行う

～ 心 得 ～

一、リスク分析はセキュリティ全体の成否を左右するものと心得よ
二、苦しくても、対象範囲の焦点化、コンサル活用などで乗り切れ
　※実施しないは負けだと思い、細心の注意を払うべし
三、分析に必要な専門家を加え、しかるべき責任者の下で行うべし

情報資産と脆弱性の特定

～自分自身を知るのは案外難しい～

この業務では、セキュリティで保護すべき情報資産と保有する脆弱性を特定します。

- 組織のビジネスプロセス全体を理解し、各プロセス間の関連性や依存性を把握する
- ビジネスに必要な情報アセット（機材、ソフトウェアなど）と保有するデータを把握する
- ビジネスプロセスや情報アセットが保有する脆弱性を把握し、管理する

【戦いの原理・原則を参考とした課題解決のヒント】

企業では税務や監査、業務利用など様々な目的で「資産の管理」が行われています。しかし、多くの場合、セキュリティにそのまま使うのは困難です。

Point	【目標】資産管理のやり方は目的に応じて違うので、盲目的に「できている」と考えるのは危険です。まずは現状を正しく認識しましょう。
着眼	● 組織として出来ている事／出来ていない事を正しく認識することから始める ● 共通的な部分は活用することを追求する

資産管理は対象物が膨大なうえ、常に最新の状態を維持しておかないと、思わぬところに脆弱性を生むことになってしまいます。

Point	【節用】作業を効率化して、限られたリソースで確実に作業を継続していくための「仕組み」を構築しましょう。
着眼	● 慎重に議論して、管理対象を厳選する ● 資産管理ツールを導入して効率化する

～ 心 得 ～

一、セキュリティのための資産管理が本当にできているか？
　　まずはそこから始めるべし。ここでの慢心は命取り
二、地図なくして戦はできぬ。大変だからと諦めることなかれ
三、大変な作業（緻密・継続・集計）は機械にやらせるべし

脅威・被害事象の特定

～彼を知らず己を知らざれば、戦う毎に必らず殆うし～

この業務では、組織のビジネスや情報資産にリスクを及ぼす要因を特定します。

- セキュリティリスクの発生源を分析する
- リスクが発生するシナリオや手法、関連する脆弱性などを分析する
- 脅威や被害事象が顕在化する可能性（組織にリスクを与える可能性）を分析する

【戦いの原理・原則を参考とした課題解決のヒント】

サイバー攻撃による被害の増加や高度化から、脅威インテリジェンスの必要性が高まっています。しかし、導入には多額のリソースを要するため、導入は簡単ではありません。

Point	【目標・節用】情報収集は有償の物だけでありません。事業規模や活用目的に応じて無償のレポートなども積極的に活用しましょう。
着眼	● IPAなどの官公庁が発行している資料 ● セキュリティベンダーが発行しているレポート

サイバー攻撃に関する情報は世の中に溢れかえっており、真偽や重要性の判断は一層難しくなっています。そのような中でも、有用な情報を選別して活用していくことは企業にとって非常に重要です。

Point	【METT】サイバー攻撃者側の立場や気持ちになって考えましょう。情報に色彩がつき鮮明になることで、見え方が変わってきます。
着眼	● 攻撃者の種類や攻撃の目的に着目する ● 自社の業種や事業規模から脅威を想定する

第４章へＧＯ！

～ 心 得 ～

一、情報を制する者はサイバーセキュリティを制す。「集め方」、「見極め方」、「貯め方」、「使い方」にまで思い致すこと
二、お高い情報＝価値ではない。IPAのサイトは宝の山
三、セキュリティも恋愛と同じ。敵側の目線で考えてみるべし

セキュリティ戦略の立案

～戦略の失敗は、戦術や作戦では取り返せない～

このフェーズでは、特定したリスクへの対応方針や対応方法を議論します。

- リスクとリソースを比較し、対応の方向性（回避、移転、低減、受容）を決める
- 組織としてのセキュリティ体制（組織、人、プロセス、機能など）を決める
- セキュリティ体制を構築する方法や中長期的なロードマップを策定する

【戦いの原理・原則を参考とした課題解決のヒント】

組織のセキュリティ戦略は、将来にわたって安定的に経営していくための道標です。しかし、技術的な要因や敵という不定要素も相まって、適切な戦略を考えることは非常に困難です。

Point	【METT】考慮要件が非常に多く難しい問題ですが、４つの意思決定の要素を外さないように注意しましょう。
着眼	● 難しい問題こそ、シンプルに考える ● 困ったらMETTと９原則を思い出す

リソースが無限であればいいですが、実際にはそうはいきません。限られた資源を使ってどのような組織を作るか、人材を確保・育成するか、どのように守るかを考えるのは頭を悩ませるところです。

Point	【集中・節用】リスク分析の成果から、重要な目標に資源を集中しましょう。そのためには、別の正面ではリスクを取る必要があります。
着眼	● リスクや効果は金額ベースで定量化する ● リスク受容こそ、明確に意思決定する

～ 心 得 ～

一、戦略が5cmずれたら、現場では5kmずれると心得よ
二、シンプルに考える道具として、戦いの原理・原則を活用せよ
三、リスクに応じた投資にすることがポイント。そのためにもリスクを適切に評価するための知識とスキルを身に付けよ

セキュリティのための組織づくり

～セキュリティの最大の敵は「当社」かもしれない～

この業務では、部署や人の配置を検討し、役割と責任に応じて権限を設定します。

- セキュリティを確保していくうえで必要となる能力と業務機能を洗い出す
- 業務機能を部署やチームに区分・配置し、必要な人材や機材などをアサインする
- 部署間の連携要領を踏まえて組織全体としての運営の仕組みや手続きを作る

【戦いの原理・原則を参考とした課題解決のヒント】

セキュリティの責任は全てセキュリティ部門にあると誤解されがちです。責任区分が不適切で曖昧だと、部署間の摩擦や緊急対応の遅れを招きます。

Point	【統一】指揮系統は一つであることが最良です。ビジネス全体とのバランスをとり、適切な責任区分を目指しましょう。
着眼	● リスクオーナーを明確化する ● ビジネス上の役割や責任を重視し、それに対して必要なセキュリティ上の能力を検討する ● 努めてシンプルにし、文書化して明示する

セキュリティは全社で取り組むべき課題であり、各部門が一丸となって協力しないと絶対にうまくいきません。

Point	【統一】セキュリティ部門だけが騒いでも多くの問題は解決しません。組織全体に影響を持つ責任者や部署の力が必ず必要です。
着眼	● トップダウンで指示してもらえるように動く ● 文化として定着するまで根気強く活動する

～ 心 得 ～

一、CVE-0：人間。いかに素晴らしいシステムも、運用する人間・組織によって神にも悪魔にもなるものと心得よ
二、問題発生時は、目先の処置に終始せず組織・文化にも目を向けよ
三、トップダウンで指示し、文化として現場に定着するまで尽力せよ

セキュリティシステムの構築

～見せかけだけじゃない、難攻不落の城～

この業務では、セキュリティを確保するために必要な機材やソフトウェアを導入します。

- サイバー攻撃を予防または検出するための仕組みを導入する
- サイバー攻撃に備え、ビジネスの代替手段や被害を軽減するための仕組みを導入する
- 状況により、監視業務や解析業務などのアウトソーシングを調整する

【戦いの原理・原則を参考とした課題解決のヒント】

異常を検出し迅速に対応するためには、ソリューション間を連携させて使いこなすことが重要ですが、多くの組織ではそれが障壁となっています。

Point	【簡明】セキュリティシステムはシンプルな構成を追求し、運用する人材の人数や能力も考慮して設計・導入しましょう。
着眼	ソリューションはファミリの統一が望ましいが、リスク分散とのバランスをとる

未掌握の裏ルートは攻撃者の恰好の侵入経路です。未監視のため侵害を検出するのも困難です。

Point	【奇襲】敵に奇襲の糸口を与えるのは愚の骨頂。監査はこのような不正の発見にも有効です。
着眼	監査の方法を工夫し、規則の抜け穴を確実にチェックできる仕組みを整えましょう

攻撃に使える情報が意図せず公開されている場合が多く、多くの企業では問題だと捉えていません。

Point	【保全】情報公開の基準を設定し、全社で認識を合わせ、それぞれの部署でチェックしましょう。
着眼	セキュリティ部署で目を光らせるのは限界があるので、組織文化となるよう根気強く訴える

～ 心 得 ～

一、ソリューション、使いこなす所まで考えてから設計・導入すべし
二、ゼロトラストが流行っても、境界防御を軽視することなかれ
三、構築したシステムやセキュリティ機器の情報は、外に漏らすな

監視とインシデント対応

～百年兵を養うは一日これを用いんがためなり～

このフェーズでは、日常的にシステムを監視し、有事の際は被害拡大前に食い止めます。

- システムの状態やデータ、不審なアクティビティなどをリアルタイムで監視する
- 不審なものを発見した場合、想定される被害範囲や原因などを速やかに特定する
- インシデントだと判断した場合、被害の拡大を防ぎ、早期に復旧を図る

【戦いの原理・原則を参考とした課題解決のヒント】

ビジネスにおいてインターネットとの繋がりや情報の共有・連携が大前提となった現代では、セキュリティリスクをゼロにすることは不可能です。

Point	【主動】防御・検知のための機能や活動のほか、インシデント発生を前提とした準備をしておこう。
着眼	● リストアまで、実際にやってみることが大事 ● マニュアル整備や訓練にもリソースを投入する

ほとんどの組織では、正常性バイアスによって「インシデント発生を前提とした投資」には消極的な傾向があります。

Point	【METT】このような場合、身をもって脅威を体感し、正しい危機感をもってもらうのが一番です。
着眼	攻撃デモ、ペネトレーションテスト、脅威エミュレーション、経営層向け危機管理演習などの活用

インシデントが発生すると、サイバー攻撃対応のほか、外部対応などやるべきことが同時多発的に発生しますが、CSIRTのリソースは限られています。

Point	【機動】状況ごとに重要な正面を見極め、貴重なセキュリティ人材のリソースをうまくアサインしよう。
着眼	対策本部等を設置し、全体の指揮を統制する

～ 心 得 ～

一、サイバーに無菌室は無い、予防と同じくらい対応の準備を怠るな
二、投資提言、言ってダメならやらせてみる
三、インシデント対応では、俯瞰的な目線でCSIRTを運用すべし

セキュリティ体制の改善

～最悪なのは、失敗から何も学ばないことである～

このフェーズでは、業務、訓練、インシデント等の教訓を踏まえてセキュリティを改善します。

- 業務の経過、訓練の成果、インシデント対応の状況などを観察・記録する
- 成功や失敗の要因を分析し、改善すべき点と助長すべき点を分析する
- 教訓を次につなげるため、セキュリティの組織、プロセス、機能等の見直しを行う

【戦いの原理・原則を参考とした課題解決のヒント】

不審メール訓練をやって、セキュリティリテラシーだけを評価して満足していませんか？悲しいことに、不審メールを開く人は絶対にゼロにはなりません。

Point	【METT】業務や訓練の成果は組織の現状を表すものです。報告だけで終わらず、改善し行動につなげることが重要です。
着眼	● 予防～検知～対応～復旧のライフサイクルを評価し、課題を洗い出す ● 組織、プロセス、機能の観点で評価する

「リソース不足」はセキュリティの体制づくりや改善における永遠の課題です。多くのセキュリティ担当者は、やる気とこの問題の間で頭を悩ませています。

Point	【目標】この状況は責任の所在が曖昧です。リスクに対応するのか受容するのか明確にしましょう。
着眼	● リスクオーナーに明確に意思決定してもらう ● 意思決定してもらえない場合は、資料や説明方法を見直して何度でもトライする

～ 心 得 ～

一、攻撃者も、日々改善の努力をしていることを忘れてはならない
二、訓練の目的や意義は、練習が半分／課題発見が半分と心得よ
三、今日から始めよう。「リソース不足」禁句令

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター（ICSCoE）