2024

脅威インテリジェンス
導入・運用ガイドライン

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

中核人材育成プログラム７期生　脅威インテリジェンスプロジェクト

目次

1 背景と目的

1.1 ガイドライン作成背景

産業活動における IT・OT システムの重要性は日々増大している。特に、近年はサービスの高度化や省人化を目的として、AI や IoT などの新技術の導入や DX の推進によって既存のシステムを拡張・自動化させる傾向にある。

産業活動のシステムへの依存度が高まるにつれて、サイバー攻撃による脅威も同様に増大している。その一例としてランサムウェアの被害額も年々増加の一途を辿っており、サイバーセキュリティの強化は組織の事業継続において、欠かすことのできない要素となっている。

石川朝久氏の著書「脅威インテリジェンスの教科書」では、サイバーセキュリティ分野における一般的なセキュリティ戦略・方針策定手法として、「コンプライアンスベース型アプローチ」を紹介している。[1]この手法は、フレームワークや法規制などをベースとしてセキュリティ成熟度の基準やあるべき姿に対して現時点での状態を分析し、そのギャップを洗い出す手法である。この手法は網羅的な評価が可能であることや組織のセキュリティ成熟度を評価しやすいという観点で有用であるが、対策の優先順位をつけることが難しいという課題がある。先述したように組織のシステムとサイバー脅威は日々増大しており、守るべき対象全てに対して一定のセキュリティ対策を行うことが困難になってきている。

一方、コンプライアンスベース型アプローチと対比される「脅威ベース型アプローチ」という手法がある。この手法はビジネス環境・特性に注目し、自組織を対象としうる攻撃グループ、脅威にフォーカスを当て特定脅威に関する事業への影響や攻撃可能性などをもとに対策の優先順位を判断するアプローチである。この手法は脅威の特定・分析の実施などより高度なサイバーセキュリティ成熟度が必要となるが、組織の守るべき対象に対して実際の脅威に基づいた対応をとることができる。表 1 にコンプライアンスベース型アプローチと脅威ベース型アプローチの比較を示す。この脅威ベース型アプローチを実現するための有効な手段の一つが脅威インテリジェンスである。

表 1. コンプライアンスベース型アプローチと脅威ベース型アプローチの比較

	コンプライアンス型アプローチ	脅威ベース型アプローチ
基本的な考え方	・基準やあるべき姿に対して現時点での状態を分析し、そのギャップを洗い出す手法	・具体的な攻撃手法や、ビジネス環境・特性に注目し、当該攻撃手法を適切に予防・検知・対応可能かを洗い出す手法
メリット	・体系的なアプローチが可能となり、全方位的かる網羅的な対策が可能 ・フレームワークに基づいて実施するため、横比較を行うことが可能 ・各項目を一定の基準で評価するため、成熟度評価を行うことが可能	・ビジネスに寄り添った特定の脅威に対して、対策の妥当性について説明可能
デメリット	・出てきた結果に対して、優先順位をつけることが難しい（脅威に基づいて有効性を示すことが難しい）	・評価の網羅性を担保することが難しい ・環境・シナリオ依存となるため、横比較を見据えた評価が難しい ・IT環境を適切に把握するため、分析には時間・専門性が必要

しかし、日本国内では海外と比較して、脅威インテリジェンスの活用は成熟していない現状に

[1] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.13 より

あり、概念そのものの認知度や、導入しているが有効活用できていない組織も多く存在する。日本という単位でも「National Cyber Power Index 2020」（Harvard Kennedy School Belfer Center）によれば、調査対象となった 30 カ国の中で、日本はサイバーセキュリティの総合指標において、9 位であったのに対し、インテリジェンス部門については 18 位という結果となっており、脅威インテリジェンスの未発展が日本の課題となっている。[2]

表 2. 日本におけるセキュリティ指標の総合評価 2020（Harvard Kennedy School Belfer Center）

	監視	インテリジェンス	商業および産業成長	サイバー防衛	情報操作	サイバー攻撃	国際規範および標準化
能力	22位	16位	6位	13位	13位	14位	11位
意識	25位	22位	17位	6位	17位	15位	15位

脅威インテリジェンスの取り組みを促進させることで日本のサイバーセキュリティ全体の総合能力の向上につながることが期待される。

ガイドライン作成にあたり、我々のアプローチとして脅威インテリジェンスに関する国内外の文献を調査した。主な文献として石川朝久氏の著書「脅威インテリジェンスの教科書」[3]を紹介する。当文献では、脅威インテリジェンスの基礎理論を紹介した後、組織ごとの目的を意識した脅威インテリジェンスの活用方法、各種フレームワークの使い方、インテリジェンスの収集・分析・活用・共有方法などを解説しており、本書のベースとして活用している。また企業ヒアリングを実施して脅威インテリジェンスの活用状況と課題感、活用事例を調査し、実際に OSINT ツールや有償のインテリジェンスサービスを導入し 3 か月間脅威情報の収集を実施した。その後収集した情報をもとに脅威インテリジェンスの活動ライフサイクルを実践し、ケーススタディとして本書にまとめている。

1.2 本書の目的

本書は、脅威インテリジェンスの導入・運用状況を海外と比較し、日本での活用が進まない理由を調査するとともに、具体的な導入・運用手段を解説することで、脅威インテリジェンスの普及を促進し、国家・組織のサイバーセキュリティの強化とサイバー攻撃による被害の低減につなげることを目的としている。

1.3 主な対象読者

本書では脅威インテリジェンスの導入・運用を主導するセキュリティ部門を主な対象読者として想定している。また本書では、脅威インテリジェンスを知らない組織をはじめ、導入に課題を抱えている組織、導入後に活用できていない組織など、幅広い組織層を対象としている。

また、脅威インテリジェンスのライフサイクルは、セキュリティ部門だけでなく、経営層や

[2] 「National Cyber Power Index 2020」https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

[3] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社

SOC 担当者とも協調する必要がある。そのため、セキュリティ部門を通して組織全体へ浸透させるべき内容を提供している。

1.4 本書の活用方法

本書は、第 2 章において脅威インテリジェンスの背景・動向、効果について論じ、経営層に脅威インテリジェンスの重要性を唱えるための提案書としての内容と、第 3 章以降においては具体的な導入方法について論じる技術書となるように構成されている。必要に応じて、先述した主な対象読者に含まれない経営層や SOC 担当者の理解向上にも活用していただきたい。

ただし、脅威インテリジェンスの導入にあたり、どの企業も即座に活用できるわけではない。インテリジェンスを活用するためには、一定レベルのセキュリティ成熟度が必要である。詳しくは第 3 章で説明する。

脅威インテリジェンス活用ケーススタディ第 10 章では脅威インテリジェンスの活用ケーススタディを例として掲載している。これから脅威インテリジェンスを開始する組織は参考にしていただきたい。

1.5 免責事項

- 本書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る。
- 本書に誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的 または黙示的な保証や条件は一切ないものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、著者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から 2 年間とする。

2 脅威インテリジェンスの概要

2.1 脅威インテリジェンスとは

2.1.1 脅威インテリジェンスの定義

脅威インテリジェンスを扱うにあたって、脅威インテリジェンスの定義を示しておく必要がある。この理由として、脅威インテリジェンスの定義が、取り扱われる組織、媒体によって異なり、本書の内容で認識齟齬が発生することを防ぐためである。本書においては「脅威インテリジェンスとは、サイバーセキュリティに関する脅威情報を収集・加工し、またそれらを分析することによって得られるインテリジェンスに基づく組織のセキュリティ対応における意思決定のライフサイクルを指す」ものとして取り扱う。

2.1.2 「脅威」と「インテリジェンス」の定義

2.1.1 節では、脅威インテリジェンスの定義について説明した。本節では、この脅威インテリジェンスを「脅威」と「インテリジェンス」に分けて、それぞれ定義される内容を脅威インテリジェンスの教科書を基に説明する。

まず、「脅威」とは、システムや組織に対し、害を与えるあるいは望まないインシデントを発生させる潜在的原因である。ここで、脅威インテリジェンスの原則は、脅威アクターの意図や攻撃手法、攻撃手法への対応策や攻撃される可能性を分析することにあり、この脅威を特定することは非常に重要である。脅威アクターは、個人・組織・グループからなる脅威主体のことを指す。また、脅威は「意図×機会×能力」の３要素から構成されおり、それぞれ以下を意味している。[4]

・意図：脅威アクターがターゲット組織を狙う目的・動機
・機会：ターゲット組織内に、攻撃実行を可能にする環境・条件が揃っている状態
・能力：目的を達成するために必要な脅威アクターが使う攻撃手法、および攻撃手法を実現するために必要な脅威アクターのリソース・スキル

脅威アクターは自身の意図と合致する企業に対し、脆弱性などの機会と自身の能力を鑑みて、特定の個社あるいは不特定多数に対してサイバー攻撃を仕掛ける。

次に、インテリジェンスについて説明する。脅威インテリジェンスでは、収集した情報を企業活動に応用するインテリジェンスに昇華させるためのライフサイクルを必要とする。このとき収集する情報を「データ」、データに背景情報といったコンテキストを追加したものを「インフォメーション」、インフォメーションに各組織の活動に活用可能なコンテキストを追加したものを「インテリジェンス」と呼ぶ。

[4] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.2 より

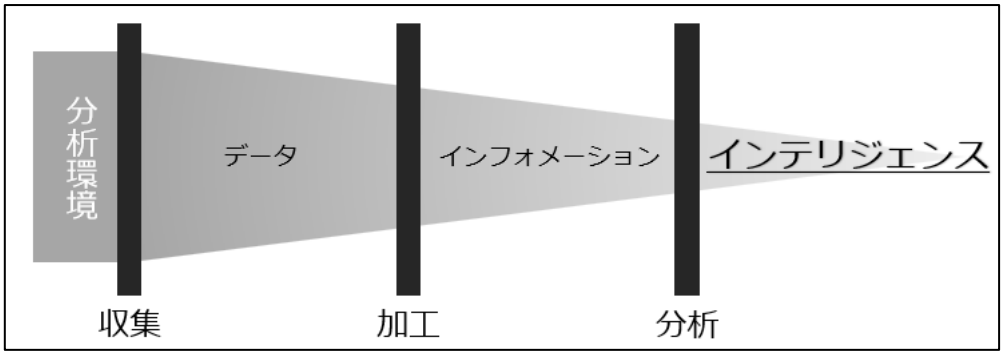


図 1.「データ」「インフォメーション」「インテリジェンス」のイメージ図

以下の表は「データ」「インフォメーション」「インテリジェンス」のそれぞれの例である。収集したデータを加工しそのデータが何を意味するか追加情報（コンテキスト）を付与したものがインフォメーションであり、遮断判断などの組織が活動するために必要なコンテキストを追加いたものが「インテリジェンス」となる。

表 3.「データ」「インフォメーション」「インテリジェンス」の例

分類	説明	例
データ	脅威となり得る情報（IPアドレス、マルウェアハッシュ、ツール名、アラート内容など）	IPアドレス
インフォメーション	データに背景情報といったコンテキストを追加したもの	悪用が確認されているIPアドレス
インテリジェンス	インフォメーションに各組織の活動に活用可能なコンテキストを追加したもの	特定の脆弱性に対して悪用実績があるIPアドレスであり、遮断することに対して業務影響がないことが確認できている

2.1.3 脅威インテリジェンスのライフサイクル

本書では脅威インテリジェンスのライフサイクルは①方針策定、②収集・加工、③分析、④配布、⑤評価の 5 つのフェーズに分類する。具体的な方策については第 3 章以降で説明するため、ここではその概要を述べる。以下図 2 に脅威インテリジェンスライフサイクルの概念図を示す。

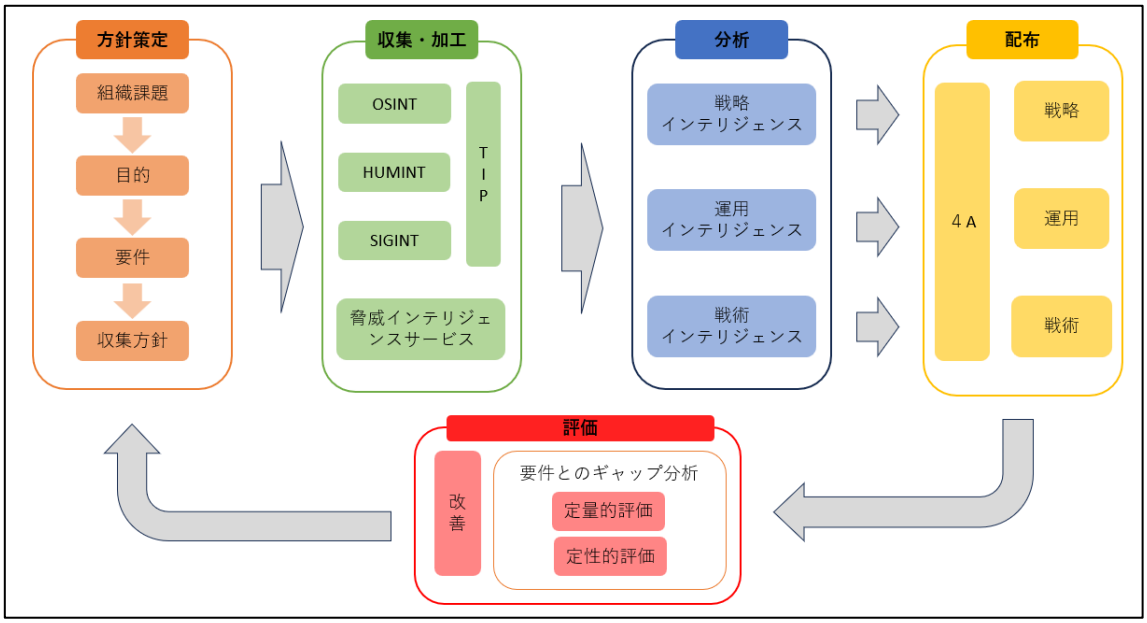


図 2.　脅威インテリジェンスライフサイクル

① 方針策定フェーズ
組織課題に応じたインテリジェンスの目的と要件を明確にし、求めるインテリジェンスに必要なデータの収集方針を定めることである。

② 収集・加工フェーズ
方針策定で定めた収集方針に従ってデータを収集し、収集したデータを分析しやすいようにインフォメーションへ加工する取り組みである。

③ 分析フェーズ
企業のインテリジェンス要件を満たすようにインフォメーションを分析し、意思決定に必要なコンテキストを追加したインテリジェンスを作成する取り組みである。

④ 配布フェーズ
作成したインテリジェンスを必要とする利用者へ配布する取り組みであり、利用者には経営層やセキュリティ部門、SOC 担当者以外にも同業界や関係省庁などの社外のステークホルダーも含まれることがある。

⑤ 評価フェーズ
脅威インテリジェンスプロセス全体を評価し、ライフサイクルの改善につなげる取り組みである。

2.2 脅威インテリジェンスの分類

アウトプットされるインテリジェンスは、目的・利用者・アウトプット形式によって分類される。分類の方法も、定義と同様に組織によって差異がある。本書においては「脅威インテリジェンスの教科書」を基に、「戦略的インテリジェンス」「運用インテリジェンス」「戦術的インテリジェンス」に分類する。[5]

「戦略的インテリジェンス」
近年のサイバー攻撃に関する脅威動向や外部環境の分析などによりリスクを明確にし、経営層によるセキュリティに関する意思決定、投資判断を支援するためのインテリジェンスである。

「運用インテリジェンス」
攻撃手法（戦術・技術・手順）の観点から脅威を理解し、ペネトレーションテストなどの短〜中期的なセキュリティ改善を行うためのインテリジェンスである。

「戦術的インテリジェンス」
日々のセキュリティ運用において、組織内部で検知、または外部組織から共有される攻撃シグネチャと脆弱性情報をもとに短期的にインシデントの予防・検知・対応に用いられるインテリジェンスである。

それぞれのインテリジェンスで取り扱う内容や要件、成果物などの詳細については第 3 章で紹介

[5] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.17 より

する。

2.3 脅威インテリジェンス導入の意義・必要性

脅威インテリジェンスのメリットの一部として自社のセキュリティ対応の優先順序付けができる点、サイバー攻撃に対してプロアクティブなセキュリティ対応を可能にする点、IR（Incident Response）能力の向上を図れる点が挙げられる。

既存のコンプライアンスベースに基づいたセキュリティ対応では、対応の優先順位をつけることが難しい状態にあった。保有する資産に対して一律の対応をとることは、組織としてのセキュリティ成熟度向上の観点では有用である。しかし、守るべき資産が増大する現状を鑑みると、リソース面での難しさがある。脅威インテリジェンスを導入することで、より警戒すべき攻撃手法から優先すべき対策を見つけ出すことができる。ただし、脅威ベースアプローチがコンプライアンスベースアプローチより必ずしも優れているというわけではない。脅威ベースアプローチに偏重しすぎると対策状況に偏りが生じる恐れがあるため、両者を並行して活用していく必要がある。

また脅威インテリジェンスを導入することで、今まで受動的であったセキュリティ対応をプロアクティブにすることができる。昨今、脅威アクターや攻撃手法が目まぐるしく移り変わる状況であり、セキュリティ対応も脅威動向に合わせて変化させて行く必要がある。平時から外部で発生している脅威を分析し準備しておくことで、ビジネスリスクを低減させることができる。

IR 能力の向上については、インシデント発生時に発見した攻撃者の痕跡をもとに、関連するそのほかの侵害情報や攻撃手法、脅威アクター情報を収集することで、痕跡以外の侵害の有無を確認でき、更なる被害を防ぐことができる。潜在的な侵害の発見の必要性については、近年のサイバー攻撃が攻撃者の侵入からインシデント発覚までの平均期間が約 1 年間だといわれており、実際に 2023 年発生した航空宇宙系企業の技術窃取においても、攻撃者は約 1 年間内部に潜んでいたとされている。したがって、高度な攻撃者によって既に侵入され、攻撃を受け続けている可能性も考慮する必要がある。脅威インテリジェンスを活用することで、攻撃者の痕跡が見つかった際に、その情報を起点として効率的にインシデント対応につなげることができる。

以上のような有効性も相まって、脅威インテリジェンス分野の注目は高まっている。”SANS 2023 CTI Survey”において、以下のようなデータが提供されている。[6]

[6] 「SANS 2023 CTI Survey」 https://www.sans.org/white-papers/2023-cti-survey-keeping-up-changing-threat-landscape/

図 3. 脅威インテリジェンス専任チームを持つ組織の推移（SANS 2023 CTI Survey）

この図は、組織における脅威インテリジェンス専任チームを持つ組織の推移を示している。2018 年からおおむね右肩上がりに上昇しており、脅威インテリジェンス分野への注目度が見て取れる。

また、我々で日本における脅威インテリジェンスの導入状況、課題を認識するために中核人材育成プログラム参加企業を対象にアンケート調査を行った。アンケートを行った 52 組織のうち、25 の組織において脅威インテリジェンスを導入していると回答し、10 の組織においては未導入であるが導入を検討していると回答があった。

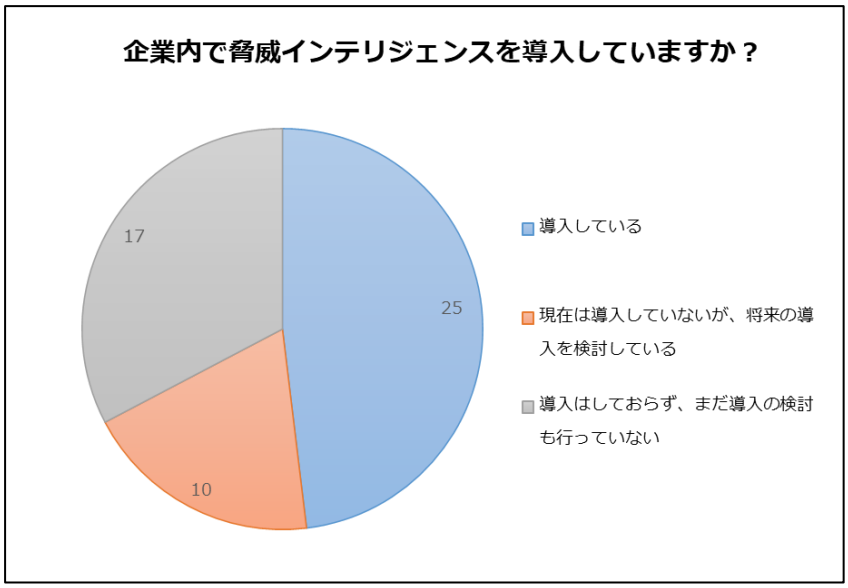


図 4. 脅威インテリジェンスの導入状況

約 70%の組織が導入済みまたは導入を検討しているという結果となり、脅威インテリジェンスの注目度の高さがうかがえた。また、導入済み組織に対する具体的な活用内容についての結果を図 5 に示す。

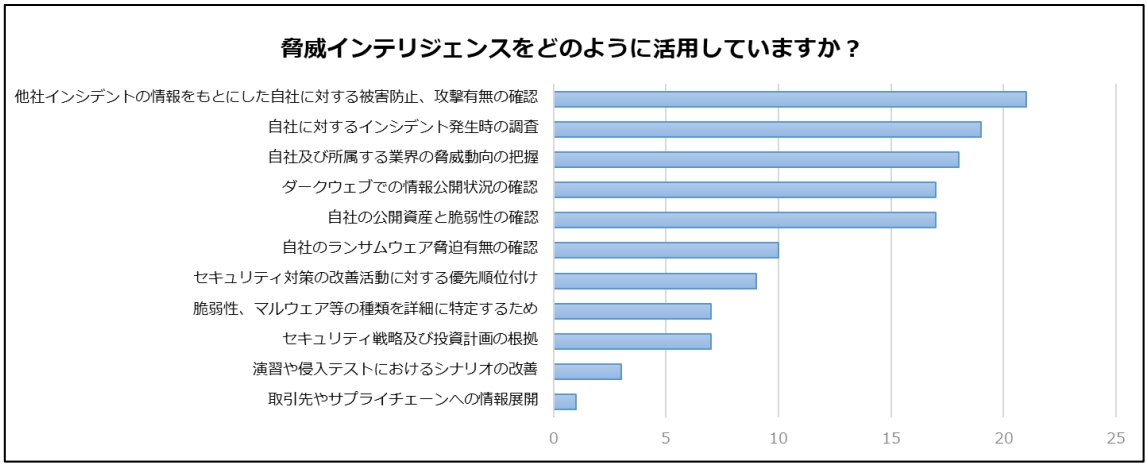


図 5. 脅威インテリジェンス導入済み日本組織における具体的活用内容

「他社インシデントの情報をもとにした自社に対する被害防止、攻撃有無の確認」、「自社に対するインシデント発生時の調査」などが多くあげられ、脅威情報を監視・運用に活用していることがわかった。一方で、「演習や侵入テストにおけるシナリオの改善」「セキュリティ戦略及び投資計画の根拠」に活用している企業は少なく、戦略面で活用していくには、まだ課題がある。

2.4 脅威インテリジェンスの動向・背景

脅威インテリジェンスという概念自体は古くから軍事的な単語として使用されてきたが、サイバーセキュリティ分野において事業会社へ浸透しだしたのはここ数年のことである。2.4 では脅威インテリジェンスが注目されてきた背景や動向を、PESTLE 分析と呼ばれる手法を用いて説明する。PESTLE 分析とはマーケティングで主に利用される手法であり、外部環境を政治的（Politic）、経済的（Economical）、社会的（Sociologic）、技術的（Technical）、法的（Legal）、環境的（Environmental）要因の 6 つの観点で分類する手法である。サイバーセキュリティの分野においても取り巻く環境を PESTLE 分析で整理することは有効である。

2.4.1 政治的要因（地政学上の脅威の増加）

地政学上の脅威とは、地理的な位置関係による政治的や軍事的な関係性を背景とした脅威のことである。一見サイバー空間において地政学的要素は考慮する必要が無いように思われるが、その認識には一部誤りがある。なぜなら、地政学的要因でサイバー攻撃対象を選定する可能性があるからである。例えば、ロシアによるウクライナ侵攻において、兵器による一般的な戦争も行われているが、並行してサイバー戦も行われているという実態がある。戦争における情報戦や相手戦力を削ぐ手段として、サイバー攻撃が活用されていることが明らかになっている。このような事態を踏まえて、” SANS 2023 CTI Survey “の調査ではインテリジェンスにおいて、地政学がどれほど重要であるかという内容についてのアンケートの結果として下図とおりとなっている。

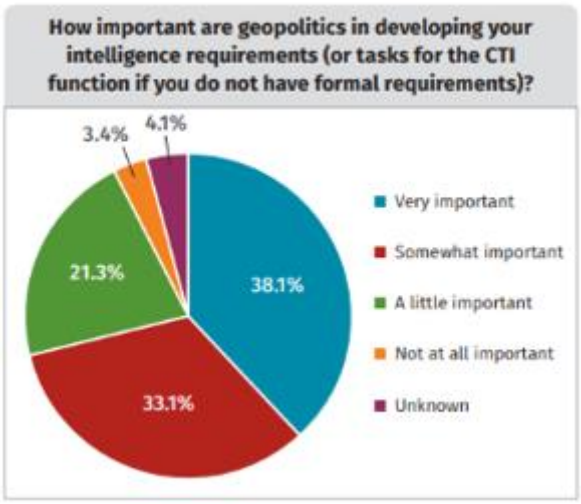


図 6. インテリジェンス要件における地政学の重要性（SANS 2023 CTI Survey）

非常に重要である（Very important）と認識した組織が 4 割近くにまでのぼり、9 割以上の組織（Very important + Somewhat important + A little important）が少なからず重要であると認識したことがわかる。このように、地政学上のリスクを考慮するにあたって、サイバー攻撃をスコープにいれる動きが高まっている。

次に、米国と中国間の技術デカップリングの問題について述べる。両国は産業技術戦略においてそれぞれ独立的な政策をとっている。米国においては、信用のできない国の製品や通信などを制限し、米国の通信技術やインフラを保護する「クリーンパス構想」を進めている状況にある。また、中国においては「一帯一路構想」や「中国標準 2035」によって中国を中心とした貿易体制や標準化を推し進めている。このように米国と中国において、双方のサプライチェーンを分断すべく技術的なデカップリングが進んでいる。

この状況に対して「ジオテクノロジー（技術の地政学）とサイバーセキュリティ」（PwC）において技術デカップリングがもたらすサイバー脅威について以下のように言及している。

米国と中国それぞれのサプライチェーン二極化の可能性がみられる中で、日本はその両方が交錯する領域に位置している。そのため、双方のサプライチェーンから、相手を牽制するためのサイバー攻撃を受けることが考えられる。そのサイバー活動の種類としては、双方のサプライチェーンが併存するところにはサイバースパイ活動、どちらか一方のサプライチェーンのみ存在するところにはサイバー破壊活動が想定できる。

また、国家単位でのセキュリティレベル向上には、脅威インテリジェンスを導入し、信頼のできる国家間で脅威情報を共有する必要がある。” Cyber Threats and NATO 2030 Horizon Scanning and Analysis “（CCDCOE）によると、日本は NATO と協力関係にあるが、脅威インテリジェンス分野の成熟度が低く、より強固な国際協調のためには、日本における

インテリジェンス能力と意識を向上する必要があるとされている。[7]

2.4.2 経済的要因（脅威分析結果から得られたサイバー攻撃による被害額の増加）

経済的利益を求める脅威アクターにおいては、ランサムウェアは依然として主たる手段である。2023 年におけるランサムウェア攻撃についての初期要求額および最終要求額は、2022 年と比較して 2 倍となっているといわれている。

ランサムウェアのような標的型攻撃による金銭の要求は大規模なサイバー犯罪組織や国家的サイバー組織のような高度で組織的に洗練された集団による攻撃が多い。脅威インテリジェンスを用いた大規模な脅威アクターの意図や戦術を理解することは、ランサムウェア攻撃よる被害と損失を大きく低減させるにあたって有用である。

2.4.3 社会的要因（企業への導入状況、業界動向）

脅威インテリジェンスは、事業規模に関わらず幅広い組織において活用されている。” SANS 2023 CTI Survey “によると、脅威インテリジェンスを活用している企業のうち、従業員数 500 名未満の組織が 28%を占めていた。このデータから、世界的なリーディングカンパニーだけでなく、あらゆる規模の組織が脅威インテリジェンスを重視していることが分かる。また、先述したように我々が行った日本組織向けのアンケート調査においても、導入済みまたは導入を検討している組織が約 70%を占めており、国内においても脅威インテリジェンス分野に対しての注目度が高いことがわかる。

2.4.4 技術的要因（IT 技術革新にともなう脅威の複雑化）

技術革新を背景に脅威の多様化が進んでいる。” ENISA Foresight Cybersecurity Threats for 2030 “に 2030 年までの注力すべき脅威が述べられている。[8]サプライチェーン侵害やディープフェイクを利用した情報操作をはじめ、新技術である IoT や AI の利用に起因する脅威、レガシーなシステムの利用に起因する脅威が挙げられている。また、これらの脅威に対応する技術が追い付いていないことも問題点として挙げられている。

これらの脅威について、本書執筆時点で表面化しているものも複数存在する。2022 年には大手自動車メーカに対してのサプライチェーン攻撃が発生し、工場停止を余儀なくされた。また、各国の選挙戦においても、懸念事項としてディープフェイクによる情報操作が挙げられている。

新技術導入につれて守るべき資産が増加しており、リソース面からも全ての資産に一律な対応をとることが困難になっている。脅威インテリジェンスを活用して、新たな脅威動向を注視し、自組織でのセキュリティ戦略へ適用することが、自組織を守るための有効な手段の

---

[7] 「Cyber Threats and NATO 2030 Horizon Scanning and Analysis」https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

[8] 「ENISA Foresight Cybersecurity Threats for 2030」https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

一つであると言える。

2.4.5 法的要因（セキュリティ・クリアランス制度）

日本で脅威インテリジェンス分野において他国に後れを取っている要因の一つとして、セキュリティ・クリアランス制度が確立されていないことが挙げられる。セキュリティ・クリアランス制度とは、国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセスを認める制度（経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議）である。[9]同盟国と脅威情報を共有するにあたって、共有相手の信頼性を測る指標としてセキュリティ・クリアランス制度が確立されているかどうかという点が重要視されている。

2024 年 5 月、セキュリティ・クリアランス制度を創設する法案が可決された。近しい内容の法律として、「特定秘密保護法」があるが、この法律に定義された「特定秘密」は「防衛、外交、特定有害活動の防止、テロリズムの防止」であり、必ずしも経済安全保障上の内容が包括されるわけではなかった。また、機密性の段階分けも「特定秘密」のみの単一階層であり、セキュリティ・クリアランス制度においては情報提供先と内容を階層分けすることが検討内容に記載されている。

具体的内容は本書執筆時点では決定していないが、今後各組織においてこの制度への対応が必要になる可能性がある。脅威インテリジェンスはもちろん、国家をまたいだ共同研究においても効力を発揮することが期待されており、組織の競争力向上に重要なファクターになることが予想される。

2.4.6 環境的要因（脅威アクターの動向と攻撃手口の変化）

攻撃観測数の多い脅威アクターは、年々変化し続けている。重要インフラに向けた攻撃について例を挙げると、2022 年には Conti や Hive といったランサムウェアグループが台頭したが、2023 年においては Royal や Black Basta というグループが特に観測されており、注目すべきグループは移り変わっている。新しいグループの出現や既存のグループの活動の変化により、攻撃手法や標的も変化している。これらのグループは高度な技術を駆使し、特に重要インフラを標的にすることで注目されている。

また、脅威アクターの使用する攻撃手法も年々進化し、多様化している。以前は従来型のマルウェアやフィッシング攻撃が主流であったが、最近では「Living off the Land Binaries And Scripts (LOLBAS)」技術が増えている。LOLBAS 技術では、既存のシステム管理ツールを悪用しており、攻撃の検知が難しいことが特徴である。例えば、主に電力、通信、エネルギー、交通、水道などの重要インフラを標的にしている脅威アクターである Volt Typhoon は、正規のシステム管理ツールを使用し、マルウェアを使わずに活動することで、検知を難化させている。このように、今日のセキュリティ対策においては、脅威アクターとその攻撃

[9]経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/siryou.pdf

手法を把握し、対策を講じる必要性が高まっている。

また、サイバー攻撃者側の環境も変化している。従来はいわゆるダークウェブをコミュニティフォーラムの場として活動していたが、国家組織によるダークウェブの検閲が高まるとTelegram のようなさらに匿名性の高いコミュニケーション環境へと移行している。Telegram は、攻撃者がセキュリティ機関や被害者に検出されにくい環境で、匿名による情報交換を可能にするツールとして使用されており、攻撃手法やゼロデイ脆弱性の売買、成功した攻撃の情報共有などが行われている。加えて、ビットコインなどの仮想通貨が身代金の受け渡しを容易にし、攻撃者が追跡されるリスクを低減している。また、仮想通貨は、取引の追跡が難しく、匿名性を維持しやすいため、ランサムウェア攻撃において好まれる通貨である。サイバー攻撃の被害を最小限に抑えるためには、攻撃者をとりまく環境の変化にも注目することが不可欠である。

このような背景を踏まえて、「NICTER 観測レポート 2023」（NICT）によれば、サイバー攻撃の観測数が年々増加している傾向にあると報告されている。[10]これは、新たな脅威アクターや攻撃手法の登場、既存のグループの活動変化、そしてテクノロジーの進化によるものといえる。特に、攻撃者が LOLBAS 技術を使用する傾向が強まっており、これによって攻撃の検知が難しくなっている。これらの要因が組み合わさり、サイバー攻撃が増加している。そのため、脅威インテリジェンスを活用し、注目すべき脅威アクターや攻撃手法および攻撃者環境の変化を迅速に把握し、セキュリティ対策につなげる必要がある。

2.5 脅威インテリジェンスの課題

2.5.1 国際的課題

国際的に抱える脅威インテリジェンスの課題としては、第一に戦術的インテリジェンスに注目されがちという点が挙げられる。これは、リアルタイムの脅威に対処するために重要だが、戦略的および運用インテリジェンスが軽視される結果となる。特に戦略的インテリジェンスは長期的な脅威のトレンドを分析し、組織全体のセキュリティ方針を強化するために必要である。運用インテリジェンスは脅威に対する自組織の検知・防御可否を検証するうえで重要である。各インテリジェンスによって目的・目標が異なるため、組織の要件に合わせて必要なインテリジェンスを選定し、適用することが必要である。

次に、脅威インテリジェンス分野における専任人材の不足も大きな課題となっている。高度な技術力と深い知識を持つ専門家は非常に需要が高く、供給が追いついていない状態にある。また、その知見の希少性ゆえに属人化する恐れもある。組織として、人材面の投資を強化することでこのような課題を解決する必要がある。

以上のように、脅威インテリジェンスは依然として新興分野であり、その取り組み内容のコンセンサスや人材育成が追い付いていない状態にある。業界として共通認識を持ち、成熟度を向上させることも、組織の脅威インテリジェンス分野の活用において取り組むべき事項の一つである。

[10] 「NICTER 観測レポート 2023」https://www.nict.go.jp/press/2024/02/13-1.html

2.5.2 日本特有の課題

日本の脅威インテリジェンス分野では、業界単位や組織での活用そのものが成熟していないことが課題として挙げられる。理由の一つとしてセキュリティ専門人材や、インテリジェンスアナリストの不足が挙げられる。また、インシデント情報などの共有を拒む文化的な障壁がその活用を妨げることも一因として挙げられる。多くの日本の組織では情報に関する責任の所在が不明瞭である。サイバーセキュリティに関する自組織の情報をどこまで共有し、他組織の情報をどこまで活用・共有すべきかについて明確な企業ポリシーがないため、情報を共有しないという選択をする場合がある。情報を公開することによるイメージの低下を恐れて、セキュリティインシデントを外部に共有することに心理的障壁が存在するため、信頼のできるコミュニティ形成にも取り組む必要がある。

特に、特定の業界を狙う脅威アクターに対しては、業界内の情報共有が重要である。競合組織だとしても、競争関係を超えて協力することでより安全なビジネス環境を構築し、共通の敵に対抗することが可能になる。

2.5.3 ヒアリング企業の課題

我々の行った日本における脅威インテリジェンスの導入・活用状況に関するアンケートの詳細に触れる。先述したように回答いただいた組織の約半数が脅威インテリジェンスを既に導入しており、未導入の組織の約 3 分の 1 が導入を検討しているという状態にあり、脅威インテリジェンスが注目度の高い分野であることがうかがえる。

しかし、導入済みの組織においても課題を抱えていることが分かった。以下脅威インテリジェンス導入済み企業の抱える課題についての調査結果を図 7 に示す。

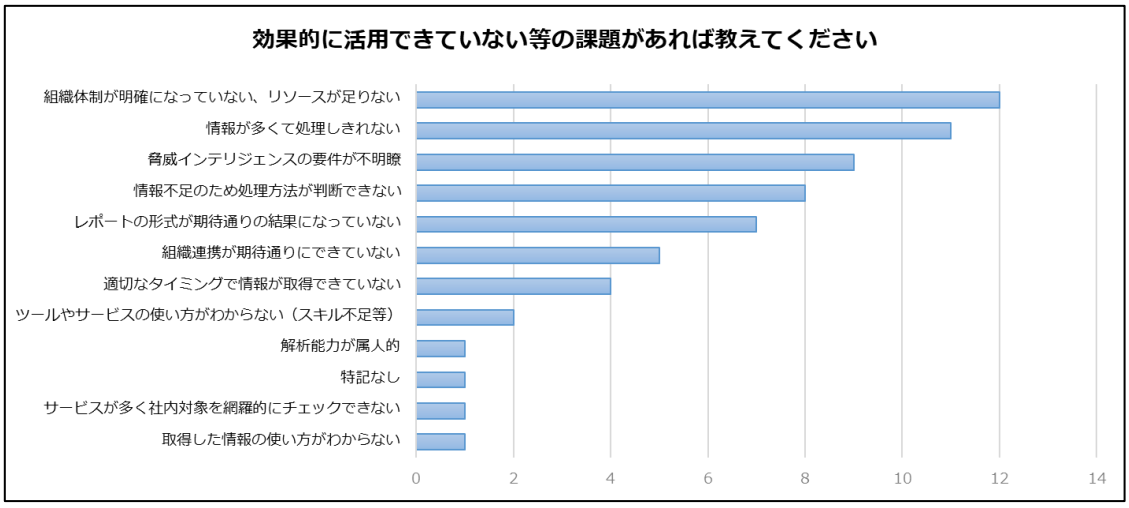


図 7. 脅威インテリジェンス導入済み組織の抱える課題

組織がインテリジェンスを何の目的で利用し、そのためにどのようなインテリジェンスが必要かといった要件が不明瞭であるが故に、期待するインテリジェンスを作成することができないことや、人的リソースの不足が大きな問題として取り上げられた。これらに関しては第 3 章以降の内容をもとに、適切な方針策定を行い、目的を絞ることで課題解決につなげてい

ただきたい。

また、導入を検討している組織における導入障壁についての調査結果を図 8 に示す。

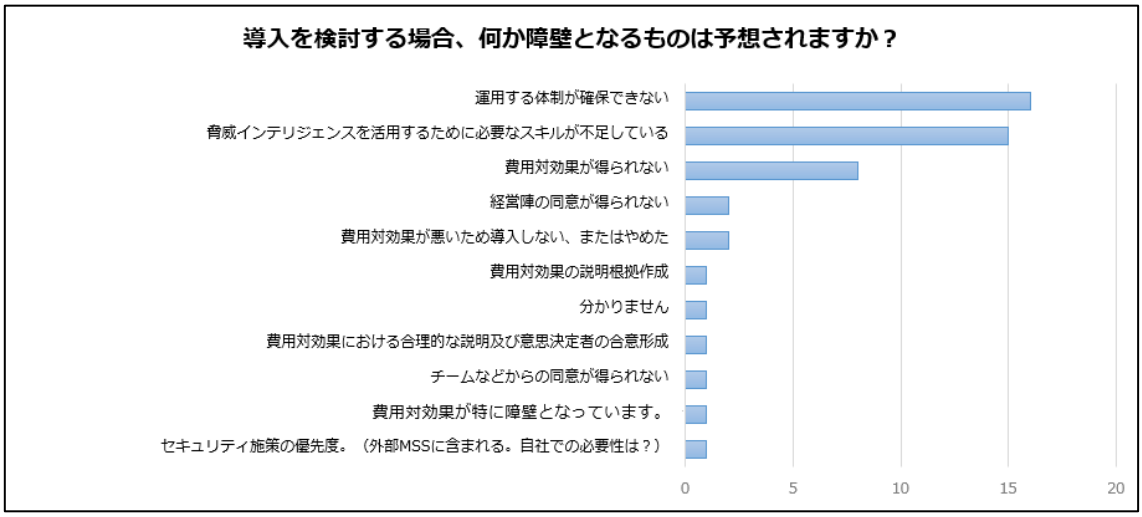


図 8. 脅威インテリジェンス導入検討組織における導入障壁

未導入組織においても、運用体制やスキルといった人的リソース面の課題が主であったため、第 3 章以降の内容を参考にしていただきたい。

3　脅威インテリジェンス活動の全体像

この章では、脅威インテリジェンス活動の全体像を明示するとともに、脅威インテリジェンスの適用に求められる組織的要件について解説する。以下に脅威インテリジェンスライフサイクルについての概略図を示す。

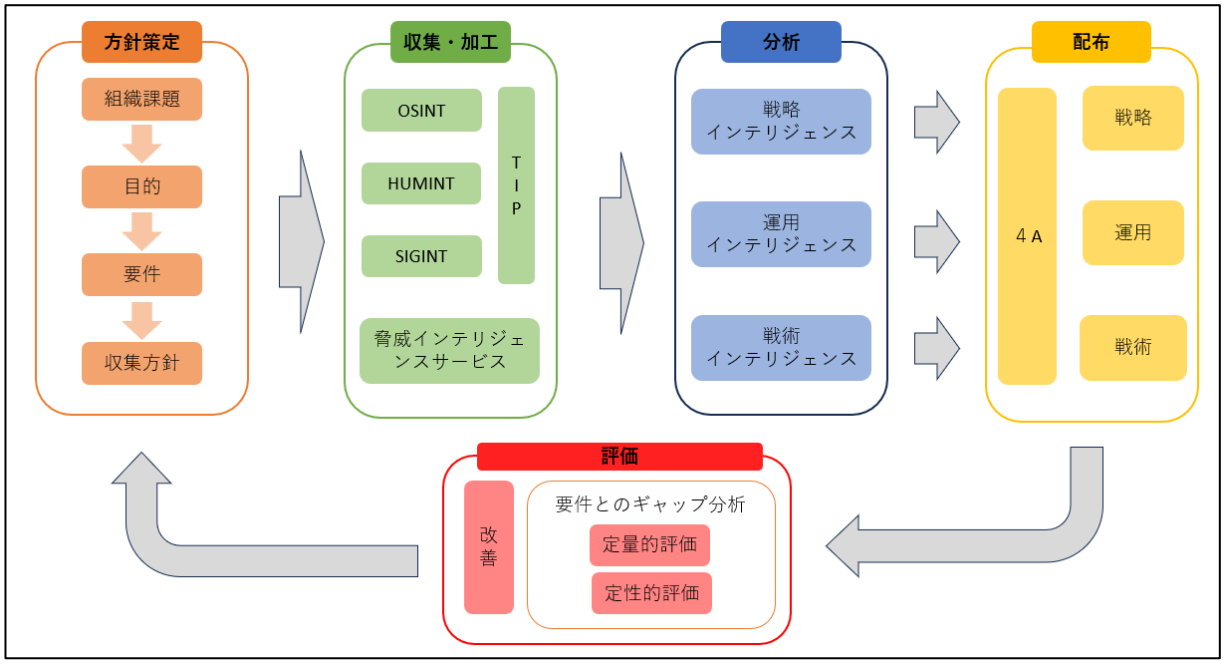


図 9.（再掲）脅威インテリジェンスライフサイクル

3.1　脅威インテリジェンス導入における基本指針

先述したように、脅威インテリジェンスとは特定のツールやサービスを意味するものではなく、自組織に関連する脅威情報を収集し、セキュリティ対策の意思決定を戦略・運用・戦術レベルで行うための情報（インテリジェンス）を作成・提供する取り組み自体を意味する。

本書では脅威インテリジェンスの取り組みを行うための基本指針とすべきライフサイクルを以下の①～⑤のように定義する。それぞれのフェーズの詳細な内容については第 4 章以降に解説する。

① 方針策定フェーズ

自組織のセキュリティ体制を整え、脅威インテリジェンス導入の目的を決定した上で、インテリジェンス要件や収集方針を検討する。

② 収集・加工フェーズ

実際に脅威情報を収集・加工する。

③ 分析フェーズ

自組織の特徴や資産、脅威への対応状況等をもとにリスク評価を実施し、セキュリティ対策の意思決定に資するインテリジェンスを作成する。

④ 配布フェーズ
作成したインテリジェンスを必要とする利用者に提供し、意思決定に活用する 。

⑤ 評価フェーズ
セキュリティを取り巻く環境や脅威は常に変化するため、作成したインテリジェンスの評価結果や外部環境の変化に伴い、ライフサイクルの改善を実施する。

3.2 脅威インテリジェンスに必要なセキュリティ成熟度

インテリジェンス情報を活用するためには、組織が一定のセキュリティ成熟度に到達している必要がある。「脅威インテリジェンスの教科書」において、具体的には以下２つの要件を満たしていることが必要であることが述べられている。[11]

・セキュリティを念頭にシステム計画、構築、維持を行う体制がある
・シグネチャベースの検知・対応をとる体制がある

例えば、戦略的インテリジェンスを活用するためには、経営層がセキュリティリスクを認識しており、セキュリティ戦略を定期的に計画する体制が必要である。また、外部環境における脅威情報を経営層に報告する機会が設定されていることが求められる。同様に、運用インテリジェンスを活用するためには、アラート検知時のみならず内部のログや外部脅威をプロアクティブに調査する体制・業務を組むことが可能であることや、脅威分析の結果をペネトレーションテストなどで確認する運用が可能であることが挙げられる。戦術的インテリジェンスにおいては収集した侵害情報をもとに自組織のシステムや機器のログ分析が可能であることや、侵害情報を登録し、検知・遮断するためのセキュリティ製品が導入されていることが要求される。このように、脅威インテリジェンスプロセスの有効活用には組織・プロセス・技術面での成熟が必要である。

ここでは、サイバーセキュリティにおける組織の成熟度を表すモデルとして” The Sliding Scale of Cyber Security “（Robert M. Lee）を図 10 に示す。[12]このモデルは以下のように成熟度を定義している。

- Architecture（設計による防衛）
  セキュリティを念頭にシステム設計、構築を行っている。
- Passive Defense（自動化した防衛）
  Architecture に加えて、自動化が進められている。
- Active Defense（巡回警備による防衛）
  自ネットワーク内の脅威を監視し、対応している。
- Intelligence（諜報による防衛）
  データを収集し、インテリジェンスを作成している
- Offense（攻撃的自己防衛）

---

[11] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.20 より

[12] 「The Sliding Scale of Cyber Security」https://www.sans.org/white-papers/36240/

脅威に対し、合法的手段による対抗や自己防衛を行っている。

図 10. The Sliding Scale of Cyber Security（Robert M. Lee）

このモデルにおいても、インテリジェンスを作成する前段として基本的なセキュリティ体制やログ分析が必要であることが示されている。脅威インテリジェンスを開始するにあたり、組織の成熟度は Passive Defense を満たしていることが望ましい。具体的に必要な要素の一例を以下の図に示す。

ステップ	人・体制・運用	プロセス	技術
Architecture	• セキュリティを意識したシステム計画・構築・維持・実行を行う体制がある状態	• セキュリティ（基本）ポリシーが整備され見直しの計画が制定されている • BCPの一環としてバックアップ手順が整備されている状態	• セキュリティ製品（Proxy、IDS、FW、EDR）などといった自動的にアラートを検知する仕組みが導入されている状態
Passive Defense	• 経営層がセキュリティリスクを認識しており、セキュリティ戦略を定期的に計画する体制がある状態 • セキュリティアラートやシステム異常をモニタリングする体制がある状態	• セキュリティ運用手順書が整備されており標準化レベルの状態	• SIEM等といったアラートを集約できる基盤があり一元管理ができる状態

脅威インテリジェンスの開始

ステップ	人・体制・運用	プロセス	技術
Active Defense	• 脅威情報を収集し、分析する体制がある • 脅威動向からシナリオを策案でき、方針、収集・加工、分析、配布、評価といったライフサイクルができる状態	• 外部環境における脅威情報を経営層に報告する機会がある状態 • 重要資産を把握しており優先順位付けができている状態 • 資産管理からすぐにアタックサーフェイスを特定できる状態	• インテリジェンスサービスといった分析できる基盤が導入されている状態 • 複数の内部ソースから手動的に情報が分析できるスキルがある状態

図 11. 脅威インテリジェンスに必要なセキュリティ成熟度の要素の一例

4　方針策定フェーズにおける実施事項

方針策定フェーズでは、以下の 4 つの手順で進める。

① 自組織の課題を明確にする
② 脅威インテリジェンスを活用する目的を定める
③ 目的を達成するために必要なインテリジェンス要件を定める
④ 要件を達成するための情報収集・分析手段を定める

脅威インテリジェンスを実践する際には、まず脅威インテリジェンスを活用する意義と目的を理解し、自組織の課題解決に必要な活動を明確にし、目的達成に必要なインテリジェンスを定めることが重要である。そのため、方針策定フェーズではまず、自組織の課題を明確にし、インテリジェンスを定める準備を進める。

以下に本フェーズにおける実施事項の概略図を示す。

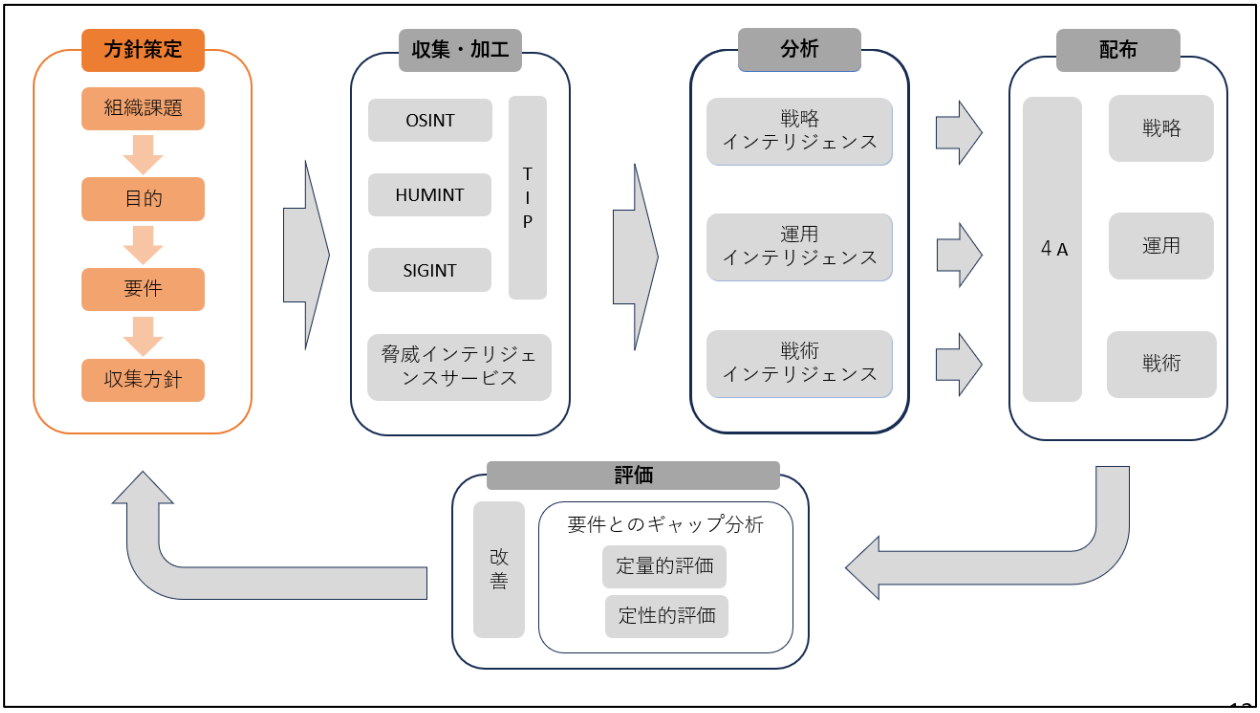


図 12.　ライフサイクルにおける方針策定フェーズの位置づけ

4.1　課題抽出

脅威インテリジェンスを開始するためには、始めに自組織の状況と取り巻く環境を深く理解する必要がある。まず、守るべき資産や業務プロセスの特定をして、自組織の状況を理解する。加えて、自組織を取り巻く脅威や外部環境を理解した上で、求められる組織成熟度を勘案しなければならない。第 2 章で紹介した PESTLE 分析も外部環境を分析する方法として有効である。この過程を通して、自組織のセキュリティ体制の問題点を洗い出し、解決すべき課題を設定することができる。

4.2　脅威インテリジェンスの目的の設定

脅威インテリジェンス活用には、目的を明確にすることが重要である。前節で設定した組織の解決すべき課題から、脅威インテリジェンスを通して実現する内容を、脅威インテリジェンスの

目的として定める。

第 2 章にて解説したように、脅威インテリジェンスのメリットとして、「対策優先順位付け」、「プロアクティブな対応」、「IR 対応能力の向上」が挙げられる。ここでは、課題整理を通して、自社に「一定のセキュリティ体制は確保しているものの、自組織の所属する業界でサイバー攻撃が発生した際に自組織として取るべきセキュリティ対応が定まっていない」という課題を解決しなければならない状況を例にとって説明する。この課題においては、同業界の他組織から共有される実際の侵害情報（不正なアクセス先 IP アドレスやマルウェアのハッシュ値など）をもとに、自組織に対する同様の侵害をプロアクティブに検知・防御するためにセキュリティ製品に侵害情報を登録する、といった活動が有効な手段の 1 つとして考えられる。従って、この例での脅威インテリジェンスを活用する目的としては、「自組織に影響がある可能性の高い脅威（同業他社で実際に直近で検知された脅威）を未然に検知・遮断する」と設定できる。

脅威インテリジェンスの目的や特に注力すべき取り組みは取り扱う組織によって異なる。ここでは、①サイバー攻撃によるインシデント予防と、②インシデント発生時の効率的な対処の 2 つの観点から以下の表に例示する。

表 4. 目的ごとの取り組み内容例

目的	説明
【インシデント予防】 自組織に影響を及ぼす可能性の高い脅威への事前対応、リスク管理	国内外で観測されている脅威動向をもとに、攻撃された際の影響や攻撃概要、使用されるテクニックやツール、脆弱性、対策方法を収集する。 収集した情報をもとに自組織の特徴や資産への影響、攻撃される環境の有無、対策状況をリスク評価し、必要な対策、セキュリティ強化を講じることで被害防止につなげる。 また、社外関係者より提供される実際の侵害情報をもとに、セキュリティ製品への検知・遮断ルールを追加する等の対策を講じることで被害拡大や再発防止につなげる。 **※可能性の高い脅威の一例** ・国内外で流行している脅威 ・自社・特定業界を狙った攻撃キャンペーン ・関連業界、地政学的関係のある他社のインシデント情報 ・自社・特定業界を狙う脅威アクターの動向
【インシデント発生時の効率的な対応】 インシデント発生時の拡大、再発防止	自組織で発生したインシデントや、セキュリティ製品での検知情報等をもとに、攻撃手口や使用されるインフラストラクチャを収集する。 発見された侵害情報以外の脅威を特定、セキュリティ製品への検知・遮断ルールを追加する等の対策を講じることで被害拡大や再発防止につなげる。

目的ごとに戦略的・運用・戦術的インテリジェンスに応じた目標を設定し、今後のフェーズにつなげることができる。「脅威インテリジェンスの教科書」を基に、以下にインテリジェンスごとの機能を示す。[13]

[13] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.17 より

表 5. 各インテリジェンスの機能

分類	説明	利用者
戦略的 インテリジェンス	近年のサイバー攻撃に関する脅威動向や外部環境の分析等によりリスクを明確化し、経営層が把握・セキュリティ戦略を計画するためのインテリジェンス	経営層
運用 インテリジェンス	攻撃手法（戦術・技術・手順）の観点から脅威を理解し、ペネトレーションテスト等の短～中期的なセキュリティ改善を行うためのインテリジェンス	セキュリティ管理部門 CSIRT
戦術的 インテリジェンス	日々のセキュリティ運用において、組織内部で検知、または外部組織から共有される攻撃シグネチャと脆弱性情報をもとに短期的にインシデントの予防・検知・対応に用いられるインテリジェンス	SOC

どのインテリジェンスを必要とするかは、自組織の目的に応じて選択する必要がある。例えば、自組織や関係企業において侵害情報が連携され早急に対応が必要な場合や、侵害情報の分析結果（使用される脆弱性やツール、攻撃テクニック、脅威アクター情報など）がない場合（ゼロデイ脆弱性など）においては、戦術的インテリジェンスとして侵害情報を直接セキュリティ製品に登録することが望ましい。一方、攻撃手法や脅威アクター情報などの分析結果が公表されている場合は、システム開発や運用時におけるペネトレーションテストのシナリオとして活用すること（運用インテリジェンス）や、今後のセキュリティ対策の優先順位付け、リスク管理、組織ポリシーの開発など、セキュリティ戦略の意思決定エビデンスとして中長期的な活用（戦略的インテリジェンス）が考えられる。

4.3 インテリジェンス要件の策定

設定した脅威インテリジェンスの目的をもとに、インテリジェンス要件を設定する。ここでは、アウトプットとして利用する成果物を設定した上で、インプットすべき情報を決定する。

前節「4.2 脅威インテリジェンスの目的の設定」にて例示した目的から導かれる必要なインテリジェンス要件は「他社で検知・発見した IP アドレス、マルウェアなどの侵害情報（IoC：Indicator of Compromise）と付随するコンテキスト（当該 IoC を利用する脅威アクターや攻撃キャンペーン情報）を収集し、検知・遮断対応の判断に必要な情報をアウトプットすること」である。

インプットすべき情報は多様であるが、脅威情報の分類方法について、David J Bianco 氏が提唱した” Pyramid of Pain “を図 13 に示す。[14]この考え方は、サイバー攻撃が、攻撃者の労力とコストのトレードオフの原理によるものとして、その困難性や価値を段階的に示したものであり、攻撃手法（TTPs）を最上位の概念とした上で、ハッシュ値を最下位として設定している。これは上位概念ほど攻撃者が容易に変更できず、防御者にとって有用であるということを示している。ただし、下位概念が上位概念に比べて劣るというわけではない。ゼロデイ脆弱性や新たな攻撃手法など、分析が未完了である状態や、関連ある企業への直近の侵害、または自社への直接的な侵害の際には、早期に特定が可能なハッシュ値や IP アドレスが優先されるケースもある。

[14] 「Pyramid of Pain」（David J Bianco）https://www.attackiq.com/glossary/pyramid-of-pain/

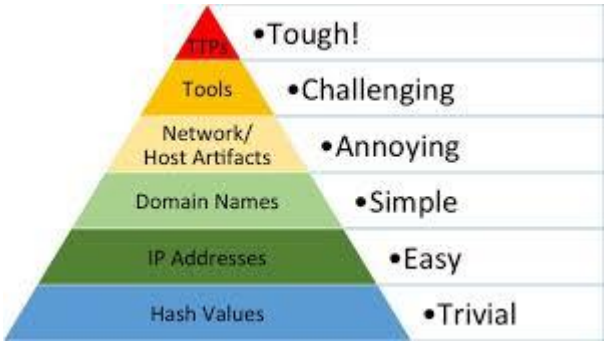


図 13. Pyramid of Pain（David J Bianco）

○脅威アクターについて

脅威アクターに関する情報を収集することは、自組織を狙う可能性がある脅威を特定するうえで重要な考え方である。脅威アクターを分析することで、そのアクターが実行する攻撃キャンペーン情報や使用する TTPs、インジケーター情報を関連付けることが可能であることや、自組織で発見された侵害情報をもとに脅威アクターを特定し、使用する TTPs を分析することで、発見された痕跡以外の侵害形跡の有無を確認することができる。

上位の脅威アクターほど明確な攻撃の意図を持っている可能性が高く、例えば国家支援型の脅威アクターは他国の重要インフラや先端技術の知的財産を狙うことがあり、第 6 章で解説する分析フェーズにおいて自組織の特性や業種などのコンテキストを分析することで、自組織を狙う可能性のある脅威アクターを特定することができる。以下に Greg Reith が拡張した、攻撃者と標的や目的の対応を示した" Pyramid of Pain "を示す。[15]

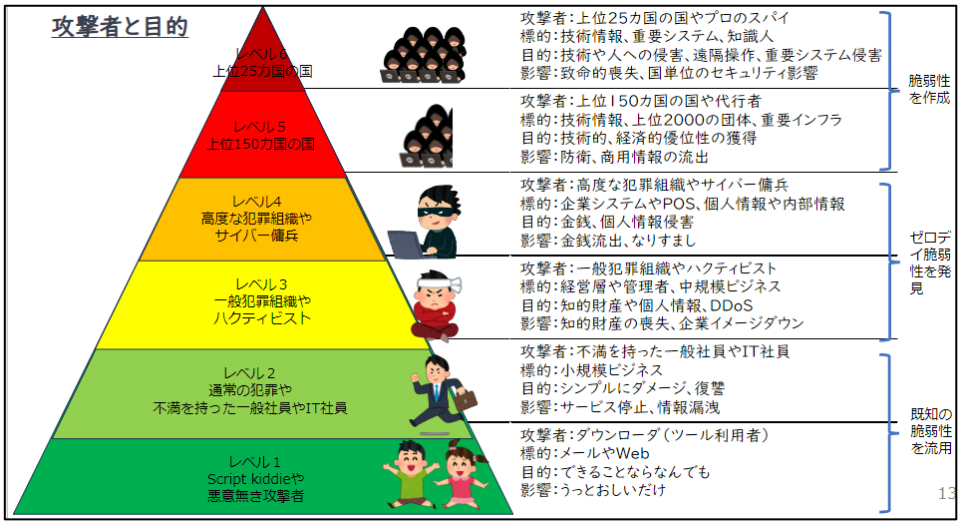


図 14. Pyramid of Pain（Greg Reith）（ガイドライン著者和訳）

4.4 インテリジェンス要件を満たす情報収集方法の検討

インテリジェンス要件を満たす脅威情報の収集技法は、OSINT、HUMINT、SIGINT に大別される。OSINT（Open Source Intelligence）とは、ニュース、SNS、専用ツールなどをもとに、公開情報からデータ収集を行う方法である。HUMINT（Human Intelligence）とは、内部ユーザか

[15] 「Pyramid of Pain」https://dynamite.ai/pyramid-pain-solarwinds-cyber-attack/

らの問い合わせ、外部組織やセキュリティベンダーからの通報、情報共有コミュニティとのやりとりなど、情報提供者からデータ収集を行う方法である。SIGINT（Signal Intelligence）とは、セキュリティ機器から取得できるアラート、ログ、パケットなどからデータ収集を行う方法である。これらの収集技法をもとに脅威情報を収集する必要があるが、その手段として実際に情報源へアクセスすることに加え、外部組織からの配信や、脅威インテリジェンスサービスを活用する方法、収集ツールの活用、脅威情報共有プラットフォームの利用などが挙げられる。

表 6. 脅威情報収集手段分類

分類	説明	例
OSINT（Open-Source Intelligence）	公開情報からデータ収集を行う方法	・セキュリティに関するニュース ・公的機関が公表する注意喚起情報 ・Webサイト、DNS等公開サーバから合法的に取得できる情報 ・個人、団体が公開している脅威情報
HUMINT（Human Intelligence）	人を媒介してデータ収集を行う方法	・組織内部からの通報 ・有償の脅威インテリジェンスベンダーからの情報 ・業界コミュニティの情報共有 ・ダークウェブ、Telegram上のコミュニティやり取り
SIGINT（Signal Intelligence）	機器やデバイス、システムからのアラートやログ等のデータを収集する方法	・Proxyログ ・IDS/IPS・EDRのアラート ・SIEMログ

インテリジェンス要件をもとに、これら様々な収集技法を用いて要件を満たす脅威情報を収集する必要がある。以下にそれぞれの具体的事例を示す。

表 7. 収集対象例

インプット例	情報の範囲	タイミング
【セキュリティニュース】 インシデント事例や脆弱性情報、セキュリティ動向等のニュースレポート	国内	日次
【脅威アクターの攻撃手法】 攻撃者のTTPsに関するレポートやツール、フレームワーク等	世界	四半期に1回
【脅威アクターの連携に関するチャットログの傍受】 攻撃者がターゲットとする組織に関する資産、脆弱性、攻撃手法	自社、所属業界	都度
【マルウェア分析結果】 攻撃に使用されたツールやファイル等のハッシュ値、挙動	世界	都度
【スキャンデータ（Shodan.ioなど）】 外部から見える自組織の公開資産の状況	自社	都度

4.4.1 OSINT における情報収集の一例

○公的機関による公開情報の収集

ここでは公的機関が一般に公開している脅威動向の例として、独立行政法人情報処理推進機構（以降、IPA）が提供する「情報セキュリティ 10 大脅威」や警察庁が提供する「サイバー空間をめぐる脅威の情勢等について」を紹介する。[16][17]「情報セキュリティ 10 大脅威」は情報セキュリティ専門家を中心に構成する「10 大脅威選考会」により、その年に発生したセキュリティ事故や

16 「情報セキュリティ 10 大脅威」https://www.ipa.go.jp/security/10threats/10threats2024.html

17 「サイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

攻撃の状況などから脅威を選出し、投票により順位付けして解説した資料である。脅威ごとの攻撃者や影響、攻撃手口、事例などが記載されている。

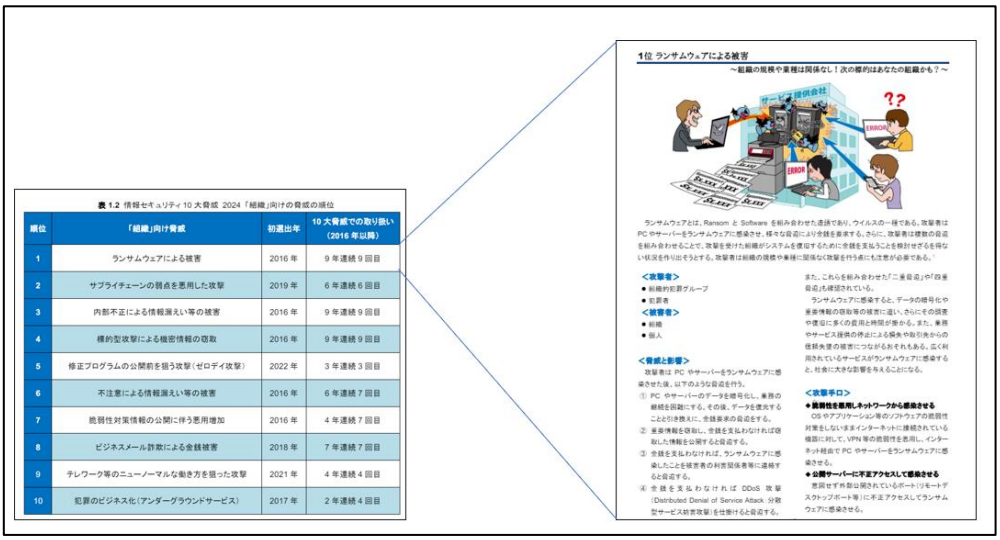


図 15. 情報セキュリティ 10 大脅威（IPA）

「サイバー空間をめぐる脅威の情勢等について」では、その年の半期ごとにサイバー空間の脅威の情勢として、被害が増加している特に注視すべき脅威を取り上げ、それら脅威を示す指標や事例、対象などをトピックとして取り上げたものである。

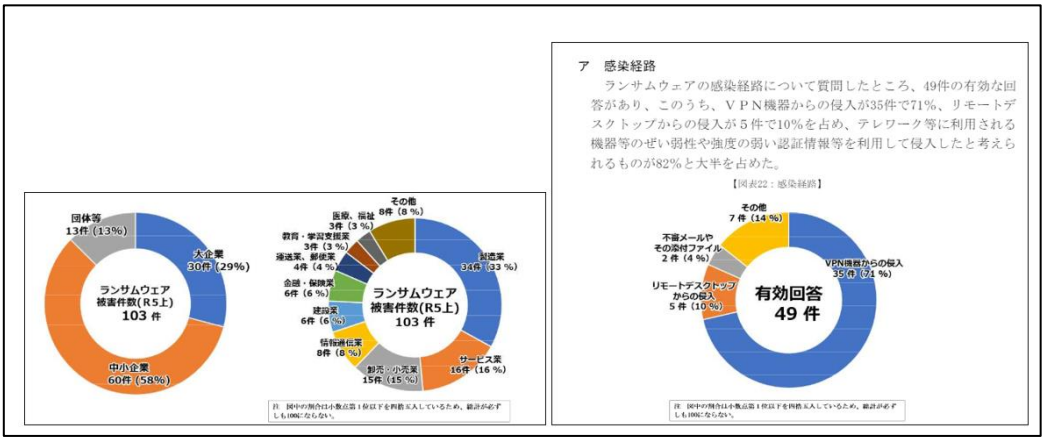


図 16. サイバー空間をめぐる脅威の情勢等について（警察庁）

○Web サイト、DNS などから合法的に取得可能な情報（OSINT ツール）

OSINT ツールとは、インターネットに公開されているサーバや IoT 機器などの資産情報やマルウェアの検体情報、脆弱性情報などを収集・分析するサイトやツールである。OSINT ツールを利用することで、自組織の保有する公開資産の把握やソフトウェア、潜在するソフトウェア脆弱性の情報や、攻撃者側が保有するインフラストラクチャ情報やレピュテーションスコア、マルウェア等の分析結果やふるまいを収集することができる。また、インターネットおよびダークウェブ上に公開されているメールアドレスやアカウント情報を収集するサービスも存在し、自組織の保有する認証情報の有無を確認することも可能である。以下に OSINT ツールの種類と使用用途の対

応表を示す。

表 8. OSINT ツールの種類と使用用途

分類	説明
公開資産の把握と確認	• インターネットに接続されている公開資産の情報を収集する • 自組織の資産で公開すべきでない資産が誤って公開されていないか調査する • 不審な通信先やウェブサイトを調査する
情報漏洩の有無確認	• メールアドレスやユーザアカウント、個人情報が漏洩していないか調査する
マルウェア情報の調査	• ファイルハッシュや実際のファイルをもとに、外部スキャンサービスの評価結果を調査する • ファイル実行時の挙動や通信先、稼働プロセスを確認する
ゼロデイやエクスプロイトの調査	• ゼロデイ観測情報や攻撃コードの公開有無を調査する
脆弱性情報の収集	• 新たに発見されたソフトウェア脆弱性やその評価結果を調査する • 悪用が確認された脆弱性情報を収集する
IPアドレスやドメインの情報収集	• 発信元IPアドレスのエリアやISP情報、使用履歴を調査する • ドメインの利用者、証明書の有無、DNSレコードの履歴を調査する
フィッシングサイトの調査	• フィッシングサイトの有無を調査する

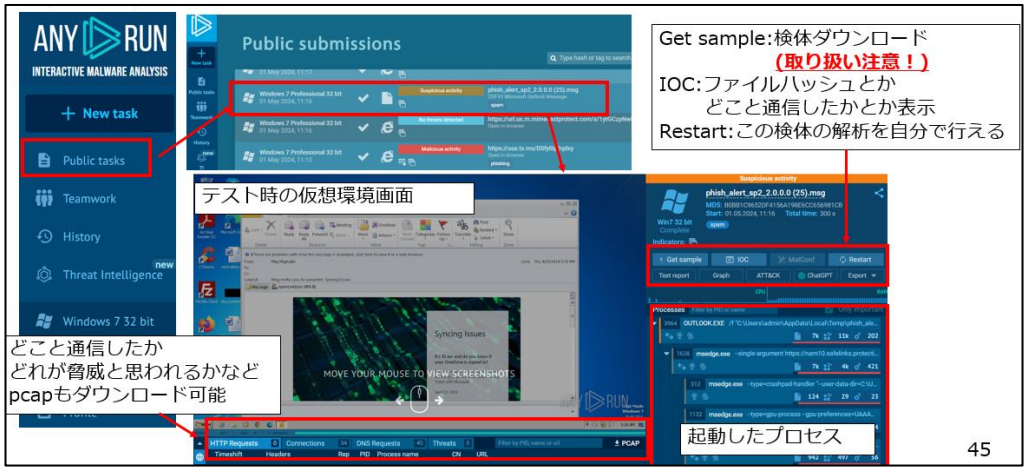


図 17. OSINT ツール使用例（Any.Run）

○個人、団体が公開している脅威情報（SNS など）

昨今は SNS も情報収集ツールの一つとして活用するケースがある。例えば、新たなソフトウェア脆弱性が発見された場合、SNS ツールでのメンション数を分析することで当該脆弱性の悪用流行を調査することができる。また、政治的思想を基に活動する攻撃グループ（ハクティビスト）は攻撃予告を SNS に投稿する傾向があるので、その投稿を収集し自組織に向けられた脅威を発見することができる。

4.4.2 HUMINT における情報収集の一例

○特定業界や組織への早期警戒情報

ここでは一般社団法人 JPCERT/CC（以降、JPCERT/CC）が提供する「早期警戒情報」を一例

にとる。[18]JPCERT/CC では、情報セキュリティに関する脅威情報やそれらの分析・対策情報を早期警戒情報として提供している。発信先として、国民の社会活動に大きな影響を与えるインフラ、サービス及びプロダクトなどを提供している組織上の情報セキュリティ部署もしくは組織内 CSIRT がある。提供対象に該当する組織は、JPCERT/CC に情報提供を依頼することで当該情報の収集が可能となる。

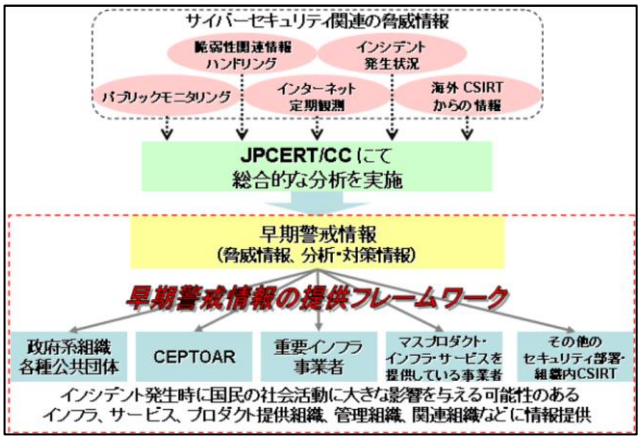


図 18. JPCERT/CC による早期警戒情報

○業界団体コミュニティによる情報共有

業種によっては業界団体によるセキュリティ情報共有の枠組みが存在する。その一例が ISAC（Information Sharing and Analysis Center）である。ISAC ではその業界に属する会員企業同士で情報共有や分析を行うことでインシデントの未然防止、発生時の迅速な対応を目的としており、金融、ICT、電力など 14 のセクターで展開されている。ISAC では SIGNAL という情報共有ポータルを用いて脅威情報の共有を行っており、特定団体間に限定して共有されるべき情報の収集が可能となるため、特定業界に特化した攻撃観測情報など、喫緊に対応すべき脅威の特定が可能となる。

○脅威インテリジェンスベンダーによるダークウェブモニタリングサービス

ダークウェブや Telegram などのいわゆるアンダーグラウンドフォーラム上でのハッカー同士のやり取りをモニタリングし、情報提供を実施するサービスが存在する。アンダーグラウンドフォーラムは通常アクセスできない場所でやりとりされているが、サービスを活用することで一般的に入手不可能な攻撃標的情報や犯行予告情報を入手することが可能である。

4.4.3 SIGINT における情報収集の一例

○自組織のセキュリティ機器からのデータ収集

IDS や FW などから収集できるネットワークトラフィックや WAF、プロキシ、EDR、アンチウィルスソフトのログ、アラート情報のデータを収集しインテリジェンスに活用する。これらの情報は外部から収集困難な情報であり、自組織で収集する必要がある。収集データが多く存在する

[18] 「早期警戒情報」https://www.jpcert.or.jp/wwinfo/

場合は、SIEM（Security Information and Event Management）を活用し、集約・分析を効率的に行う必要がある。特に、IoC 情報や TTPs を検証する場合、複数のデータを一括に分析することで自社に潜在する脅威の追加情報や攻撃経路の分析が可能となるため、脅威インテリジェンスを活用するにあたり、ログなどのデータを収集できるセキュリティ機器と SIEM の導入は必要な要件となる。

4.5 情報収集における考慮事項

○情報の正確性に関する考慮

脅威情報を様々な収集方法を用いて収集する際、特に OSINT により情報収集を行う場合は、その情報の正確性について考慮する必要がある。例えば、攻撃者による隠ぺいや陽動を含んでいる場合もあれば、収集者の技量により分析結果に違いが出る場合もあるため、どの程度信頼できる情報源であるかを確認する必要がある。そのため、同じ役割を持った異なる情報源、ツールを活用することでその情報の正確性を確認すること（エンリッチメント）や、公的機関やセキュリティベンダーなどの専門チームを活用することで、より正確性の高い情報を収集することも考慮すべきである。

○アウトプットにおける考慮事項

収集した情報が求める形式であることや、適切なタイミングで提供されることも考慮する必要がある。例えば、SOC 運用者が利用する戦術的インテリジェンスでは技術的な IoC 情報（侵害情報のファイル形式やハッシュ値など）が要求される。また、IoC 情報は攻撃者の切り替えが早く、鮮度が重要であるため、発見された侵害情報はその正確性と合わせて適切なタイミングで提供されることが要求される。

○組織リソースにおける考慮事項

組織内部のリソースを使った能動的な情報収集は、自組織に関連する情報を重点的に収集できる利点がある一方、情報の正確性や網羅性という観点においては収集を実施する人のセキュリティに関する専門的な知見を要し、集中的に業務を実施する環境を必要とする。効率的な運用を実施するためには収集業務の自動化や収集ツール、脅威インテリジェンス共有プラットフォーム（TIP：Threat Intelligence Platform）の導入を検討する必要がある。組織外部のリソースを使った受動的な情報収集は内部の専門的な人材を省力化できる一方、情報分析の際にトリアージが必要な情報量の多さやコスト面での負荷を考慮する必要があるため、インテリジェンス要件を定めたうえで必要な情報を重点的に収集できるよう RFP を定めて調達を実施することや、収集した情報についての専門家による追加レポートや分析要件を加えることで、コストメリットの確保に努めることが望ましい。

○脅威インテリジェンスサービスの利用など外部リソースを活用する際の考慮事項

外部リソースを活用する場合、自組織のインテリジェンス要件を満たすサービス、ツールを選定する必要がある。POC 等で利用イメージやインテリジェンス要件を修正することが重要である一方、サービス、ツールが先行し、インテリジェンス要件が明確でない場合はコストに見合った活用が困難になる可能性がある。RFP を策定する場合、インテリジェンス要件に加え、上述の考慮要素である収集対象となる範囲、提供タイミングを意識する必要がある。

5　収集・加工フェーズにおける実施事項

収集・加工フェーズは、方針策定フェーズで策定した収集方法をもとに実際にデータ収集をおこない、収集したデータを分析しやすい形で管理するフェーズである。ここでは、複数の情報収集方法を用いる場合の、情報一元化に利用される脅威インテリジェンス共有プラットフォーム（TIP）や脅威インテリジェンスサービスについて紹介する。以下に収集・加工フェーズにおける実施事項の概略図を示す。

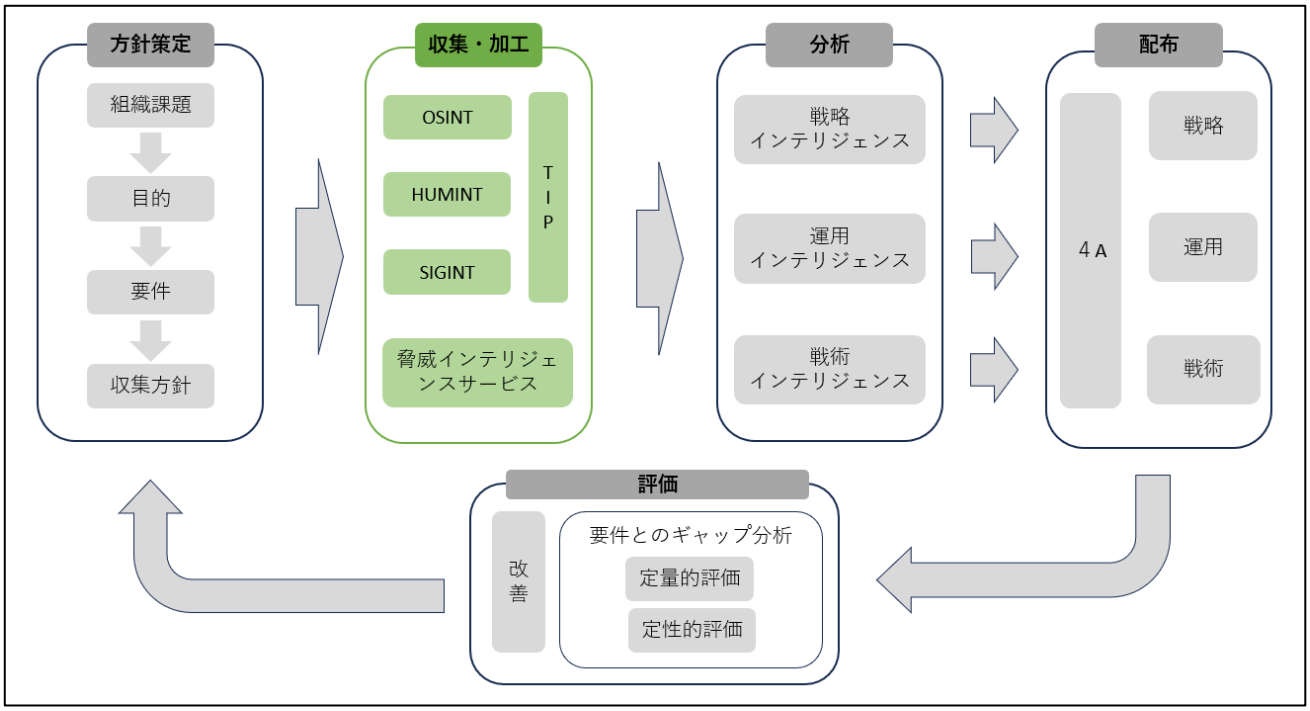


図 19. ライフサイクルにおける収集・加工フェーズの位置づけ

5.1　情報集約方法

ここでは、様々な情報源からデータを収集する際に一元管理するための方法やデータフォーマットについて説明する。

5.1.1 脅威インテリジェンス共有プラットフォーム（TIP）

脅威インテリジェンス共有プラットフォーム（Threat Intelligence Platform）（以下 TIP）とは，様々な脅威情報を収集し，分析，共有を一元的に行う基盤のことである。

TIP の主な機能としては複数の情報源から収集した情報を集約し，それらを加工することで情報同士の関連付けや分析を実施することが可能となる。また，内部テレメトリーのログやアラートを集約することも可能であり，外部から収集した脅威情報と内部情報の突合をすることでインテリジェンスの精度を高めることが容易になる代表的な TIP として、MISP（Malware Information Sharing Platform）や OpenCTI が挙げられる。脅威インテリジェンスの共有や他のセキュリティ監視ツールとの統合を実現するオープンソースの TIP である。MISP ではフィードと呼ばれる各種ベンダーやリサーチャーが OSINT で得た情報が公開されており、MISP を導入すること

で脅威情報を収集・保存・分析・共有することができる。OpenCTI も同様にオープンソースの TIP であり、複数ソースから得られる IOC などのサイバー攻撃に関する技術情報と非技術情報を、構造化、保存、整理、視覚化、蓄積することが目的のツールである。以下にそれぞれの比較を示す。

表 9. MISP と OpenCTI の比較

	MISP ◆具体的なインシデントレスポンス ◆日々の脅威インジケータの共有	OpenCTI ◆脅威インテリジェンスの広範な分析 ◆異なる情報ソースからのデータ統合
情報の構造化と統合	・柔軟なデータモデルを採用 ・自由に属性の追加、情報のカスタマイズが可能 ・イベントベースの情報管理	・STIX規格に基づいた高度な情報の構造化 ・脅威データ間の関連や文脈を明確に表現 ・グラフベースの情報の視覚化
UI	・直接的で機能的なUI ・主にイベントと属性に焦点を置いたインターフェース	・グラフィカルなユーザーインターフェース ・脅威情報の視覚的な分析と探索に優れる
データ統合と拡張性	・多くの外部ツールと連携可能 ・APIを通じた拡張性が高い ・データの取り込みと統合には手動操作が必要な場合が多い	・広範なセキュリティツールとの統合が容易 ・自動的に外部データを取り込むことができる
分析ツールと機能	・分析ツールは限定的 ・インジケータの追跡やパターン識別に有効	・豊富な内蔵分析ツールを提供 ・自動分析や複雑なリレーショナルデータの分析が可能

5.1.2 脅威インテリジェンスベンダーサービス

脅威インテリジェンスベンダーサービスを利用することで、収集フェーズ、加工フェーズ、および分析フェーズの一部業務をアウトソースすることができる。これにより、組織は内部リソースを最適化し、迅速かつ効率的に脅威インテリジェンスを活用することが可能である。さらに、ダッシュボードを提供するインテリジェンスサービスについてはグラフやスコアなどの情報が可視化された形式で提供され、複数の情報を一覧化でき、アラート発生時の迅速な対応や脅威インテリジェンス活動の実績の可視化が期待できる。

しかし、留意すべき点も存在する。まず、ベンダーから提供された情報は、自組織の資産状況やセキュリティ対策の状況、重要資産の判断など自社の状況に合わせて再分析する必要がある。また、脅威インテリジェンスサービスの利用にはインテリジェンスアナリストによる独自分析やハッカーコミュニティへの潜入など、専門的なチームによる情報提供が含まれることがあるためコストかさむことがある。

さらに、脅威インテリジェンスの導入と運用においては、目的と手段が逆転する恐れがある。つまり、脅威インテリジェンスサービスの導入そのものが目的となってしまい、本来の目的が疎かになるリスクがある。脅威インテリジェンスサービスはインテリジェンスを収集するための手段であり、最終的な目的は組織のセキュリティを向上させることである。このため、導入後も継続的に評価し、必要に応じて戦略を見直すことが重要である。

5.2 情報収集技法

5.2.1 RSS

RSS（Rich Site Summary）はウェブサイトの要約や記事の見出しなどを配信するための XML ベースのデータフォーマットである。OSINT を活用してニュースサイトなどから情報収集する場

合、RSS 対応のサイトであれば更新情報を自動で収集できるようになる。リソース面に課題を抱えている場合は、積極的に活用していく必要がある。

5.2.2 STIX/TAXII

脅威情報の連携を目的とした構造化記述形式として、STIX（Structured Threat Information eXpression）がある。STIX は JSON ベースで定義されており、攻撃者に関する IoC やマルウェア情報といった脅威情報に係るコンテキストを記述し、STIX 形式を取り込んだ情報は同形式で取り込まれた情報と関連付けを行うことができるため、加工処理を容易とする。こちらもリソース面に課題を抱えている場合は、積極的に活用していく必要がある。

TAXII（Trusted Automated eXchange of Indicator Information）は HTTPS を用いて STIX などの形式で記述されたサイバー攻撃活動に関連する脅威情報を共有するためのプロトコルである。TAXII を用いることで、サイバー攻撃活動の観測情報や検知指標などのデータをプログラム処理できるようになり、効率的な脅威情報の共有が可能となる。

6 分析フェーズにおける実施事項

分析フェーズでは、情報・加工フェーズで分類したインフォメーションを分析し、組織のセキュリティ対策の意思決定に必要なインテリジェンスへと昇華するフェーズである。このフェーズでは、インテリジェンスの種類・配布先によって配布に必要な情報が異なるため、分析方法も戦略的・運用・戦術的インテリジェンスによってその手法が異なる。以下に分析フェーズにおける実施事項の概略図を示す。

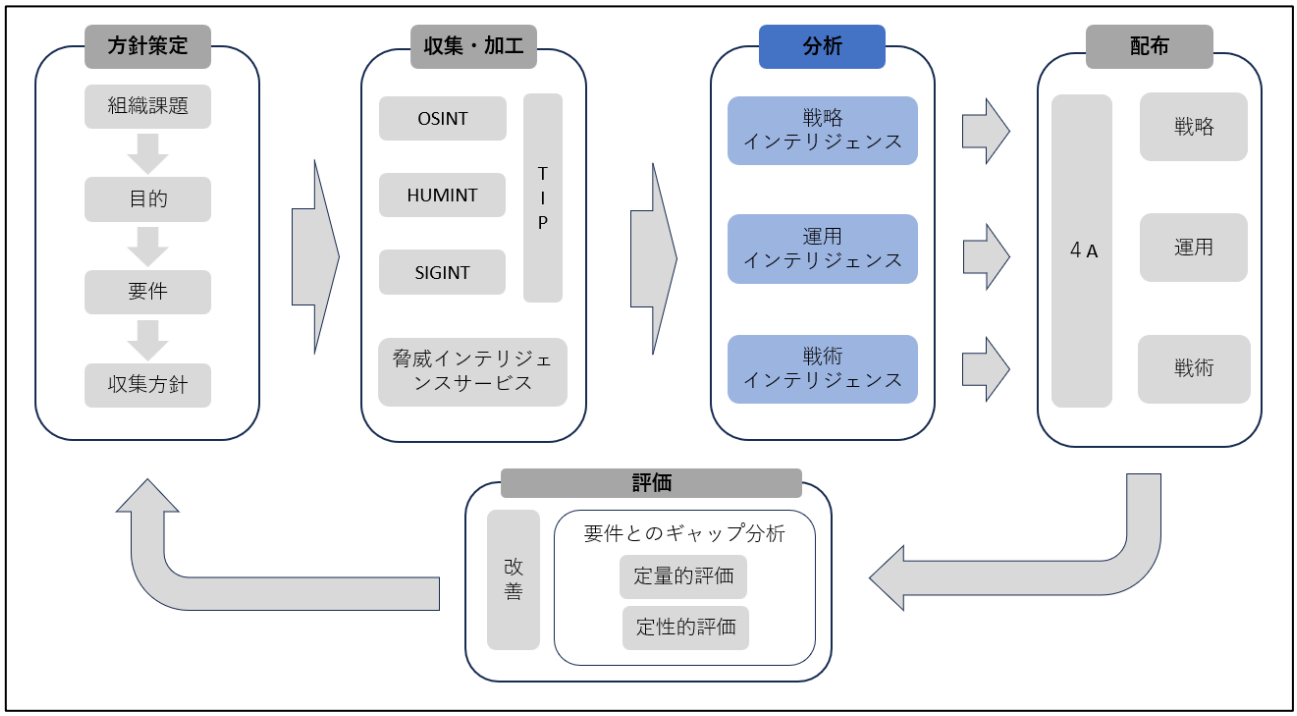


図 20. ライフサイクルにおける分析フェーズの位置づけ

6.1 戦略的インテリジェンスの分析技法

戦略的インテリジェンスの目的のひとつは、中長期的なセキュリティ戦略の立案や喫緊の優先すべき脅威のモニタリングの意思決定を行うことにある。収集・加工した脅威情報（流行の脅威情報や脅威アクターの動向、他社インシデント事例）をもとに、脅威に対する自組織のリスク評価を行い、意思決定エビデンス(セキュリティ戦略や特に監視すべき脅威のリスト)を作成することが分析フェーズに該当する。

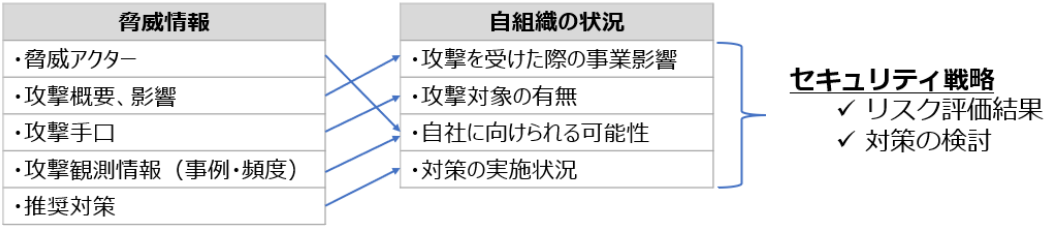


図 21. 戦略インテリジェンス分析例

脅威アクターは明確な意図と目的をもって組織を攻撃する可能性が高い。どの脅威アクターが

自社を攻撃目標とする可能性があるか分析するためには、自組織の特性や保有する資産、業種などの組織コンテキストを分析する必要がある。自組織を分析した結果を基に収集した脅威アクター情報から自組織を狙う可能性のあるアクターを推定し、該当のアクターが使用する攻撃手法や脅威を分析し、自組織の評価と対策を実施することが望ましい。

表 10. 組織の特性（コンテキスト）の一例

組織の特性（コンテキスト）	一例
・業種	・金融、通信、医療、教育、生活インフラなど
・地政学的コンテキスト	・影響するエリア、拠点など
・守るべき資産・事業	・重要な知的財産、サービス、個人情報など
・ステークホルダー	・官公庁、組織、コンシューマなど

攻撃対象の有無を確認するためには、組織が保有する IT 資産情報を整理しておくことが望ましい。例えば、攻撃手口として VPN 脆弱性を悪用した不正アクセスが考えられる場合、組織は自社が利用している VPN 機器とソフトウェアバージョンの一覧を管理する必要がある（資産管理)。自組織において資産管理が十分でない場合は、ASM（Attack Surface Management）を活用することも有効な手段のひとつである。ASM は外部から見た自組織の公開資産をスキャンし、使用されるソフトウェアやサーバ証明書情報などを分析するツール・サービスであり、ASM からの分析結果と脅威情報を突合することで、攻撃対象の有無を確認することができる。ただし、ASM はあくまで外部から見える資産情報であるため、実際に使用されているソフトウェアや製品と乖離がないか確認する必要があることは留意すべき点である。

戦略的インテリジェンスでは、脅威以外にも様々な外部環境が対象となるケースもある。外部環境の評価手法のひとつとして、PESTLE 分析がある。この分析手法では、自社に関連しうる要因を、政治的（Political)、経済的（Economic)、社会的（Sociological)、技術的（Technological)、法的（Legal)、環境的（Environmental）要因に分類し、多角的な観点から戦略を意思決定づけるエビデンスとして活用される。サイバーセキュリティにおいては、脅威情報（技術的・環境的要因）以外にも、複数の要因を考慮するほうが望ましい。

表 11. サイバーセキュリティ分野における PESTLE 分析

外部要因	一例
政治的要因	・技術的デカップリング ・産業用制御システムへの脅威アクターの攻撃の増大
経済的要因	・スマートシティの台頭 ・アウトソースされたITサービスへの依存度の高まり
社会的要因	・データ分析による意思決定の増加 ・日常生活におけるデジタル技術の指数関数的増大
技術的要因	・生成系AI、IoTデバイスの増加 ・ブロックチェーン技術の活用
法的要因	・各国のデータ規制法の取り組み ・各セクターでのセキュリティガイドラインの推進
環境的要因	・リモートメンテナンスにおける新技術使用の増大 ・一次産業の労働力の自動化

6.2　運用インテリジェンスの分析技法

運用インテリジェンスの目的のひとつは、脅威アクターが使用する攻撃手法をもとに、自組織にとってその攻撃が有効かどうか、攻撃を防御または検知可能か検証することが挙げられる。攻撃手法の分析には、脅威アクターの攻撃手法を体系的に整理した「MITRE ATT&CK」が利用されるケースがある。[19]「MITRE ATT&CK」は、サイバー攻撃の実行フェーズを偵察（Reconnaissance）～影響（Impact）の 14 フェーズに分類（Tactics）し、各フェーズで使用される攻撃手法（Techniques）を整理している。各攻撃手法には一意に特定するための識別子（T.●●●●）と、紐づく要素（攻撃グループ、ソフトウェア、技術・手順、対策）が設定されているため、脅威アクターごとに使用されるテクニックを識別子で分類することができる。

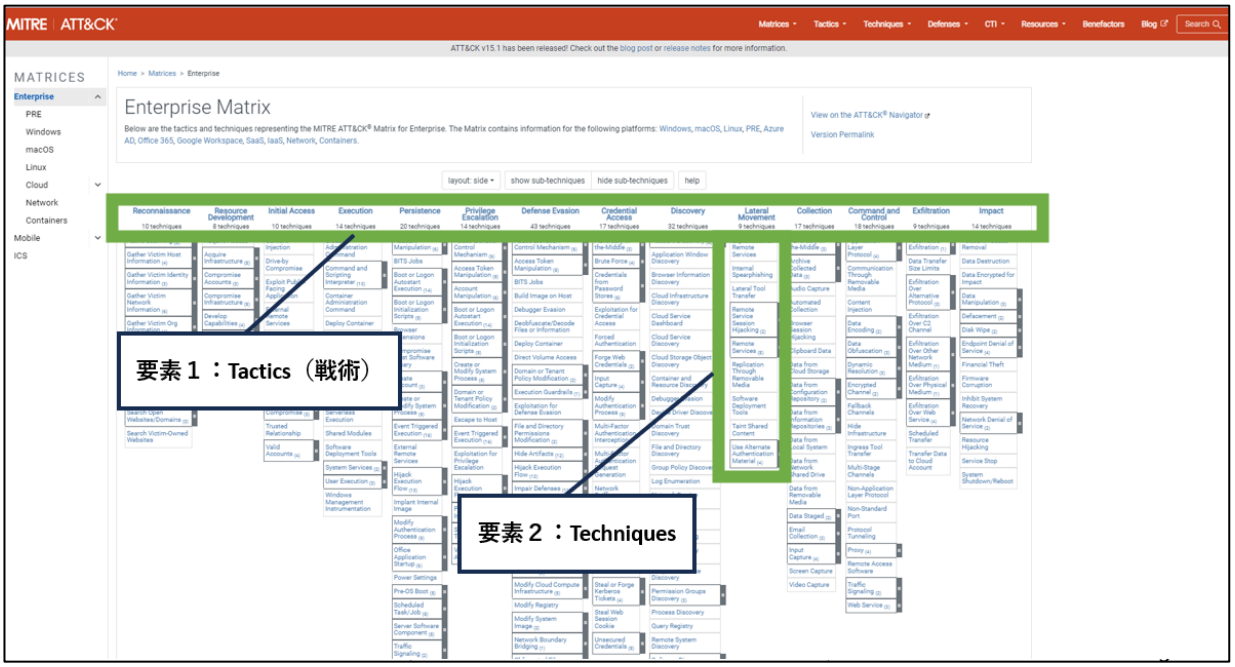


図 22. MITRE ATT&CK Enterprise

また、MITRE ATT&CK の攻撃手法を再現するオープンソースのツールもあり、実際に脅威アクターを模した自組織環境への攻撃検証を実施することで攻撃成功の有無を確認することができる。

○サイバー攻撃訓練への活用（TLPT）

システム開発・運用時に行う侵入テストとしてペネトレーションテストがある。そのひとつとして、実際に脅威アクターが使用する攻撃手法を模した、脅威ベースのペネトレーションテストを TLPT（Threat-Led Penetration Testing）という。このテストシナリオでは、脅威インテリジェンスで分析した自組織を狙う脅威アクターの攻撃手法を用いることがある。TLPT では実システムやネットワーク環境を攻撃し、セキュリティ対策状況の確認だけでなく、攻撃発生時の自組

[19]「MITRE ATT&CK」https://attack.mitre.org/

織のレジリエンス力を検証することもできるテストとして、近年注目を浴びている。

6.3 戦術的インテリジェンスの分析技法

戦術的インテリジェンスではIoC情報を主に扱い、自組織へのセキュリティ製品などでの検知・遮断に活用され、侵害が自組織に到達する前に検知、遮断することや既に侵害が到達しているかどうか確認する目的で利用される。以下の表においては、IoC情報におけるデータとインフォメーション、インテリジェンスの例示を示す。コンテキストの含まれないIoC情報をデータとして取り扱い、IoCの持つ意味、役割を追加したインフォメーションに分類する。これらの情報は1日単位でも処理しきれないほどの量があり、分析フェーズでは自組織に影響のあるIoC情報として遮断判断の意思決定に必要なコンテキストを含んだものをインテリジェンスとして分析・作成することで、自組織へ影響がある可能性のあるIoC情報を抽出し、提供する必要がある。

表 12. IoC情報におけるデータ、インフォメーション、インテリジェンス

データ	インフォメーション	インテリジェンス
IPアドレス	C2サーバとして利用されるIPアドレス	国家組織の脅威グループがスパイ活動のために利用しているIPアドレスの１つ
ファイルハッシュ	マルウェアとして認知されるファイルハッシュ	Revilランサムウェアグループが Linux環境をターゲットとして利用するファイルハッシュ
URLまたはドメイン	脅威アクターが遠隔操作を実施するためのWeb shellが格納されたサイトURL	China Chopperが利用するURLであり、複数の脅威アクターに関連した多用途Web shell

ここではIoC情報の分析手法として「エンリッチメント」、「ピボッティング」の紹介と、IoCの収集・加工、分析、配布を自動化するためのツールである「SOAR」を説明する。

◯エンリッチメント

エンリッチメント（Enrichment）とは、取得したIoC情報の付帯情報や悪性レベルを関連付けるための手法であり、OSINTツール・サービスとして提供されているものもある。他組織から取得した付帯情報との関連付けや、複数ベンダーの診断機能のスキャン結果のサマリ、サンドボックス上での実行結果などにより、悪性スコアやプロセスの実行状況、脅威アクター情報を確認することができ、また不審サイトのドメイン、IPアドレスを調査することで、アクセス先の画面キャプチャからサイトの形態を確認することができる。

また当該ツール・サービスを活用する場合の留意点として、アップロードしたマルウェア検体の情報がツールを利用するその他ユーザに公開されることがあるため、組織の機微情報が含まれる場合、ツールの機能として提供される非公開の設定を活用し、組織の情報公開ポリシーに従って判断するべきである。

◯ピボッティング

ピボッティングとは、収集したIoC情報を内部環境、外部環境で分析した結果得られるそのほかの侵害情報を収集する手法であり、自組織で侵害が確認された際に、その他のアクティビティを特定する際に有効である。例えば、組織のプロキシサーバで不審な通信先へのアクセスが確認された際に、そのアクセスを行った端末を特定すると同時に、端末内で実行されたファイルやプ

ロセスを確認することでアクセス原因となったIoCを特定し、また、そのファイルがどこから取得されたのか、メールやアクセスログを確認することで特定することができる。ピボッティングの一部で利用されるログなどの痕跡から侵害情報を調査する手法を、「脅威ハンティング」と呼ぶ。また、ピボッティングの一環としてIoC情報をもとにOSINTツールや脅威インテリジェンスサービスから収集されている脅威情報を検索し、当該IoCが利用されるツール、手法、脅威アクターを特定することで、同様のアクティビティに活用される他のIoCを特定し、網羅的に検知・遮断対応することも可能となる。

○SOARによるIoCの自動処理の検討

自組織への脅威アクティビティが頻繁に見受けられる場合、IoCもその数が多くなる。そういった場合、IoCのコンテキストを都度確認することやセキュリティ製品での検知・遮断対応の手動実施が困難になることが予想されるため、自動化による処理を検討する必要がある。SOAR（Security Orchestration, Automation and Response）は脅威情報やアラートを集約し、検知ルールを自動適用することが可能となる技術である。

7　配布フェーズにおける実施事項

配布フェーズでは分析フェーズで作成したインテリジェンスを利用者へ提供するフェーズである。提供する際は、作成したインテリジェンスが効果的に活用できるものか（意思決定に繋がるインテリジェンスか）を検討する必要があると同時に、インテリジェンスに含まれる正確性・推論内容の評価を行う。また、一部のインテリジェンスにおいては社内関係者のみならず、ステークホルダー間で情報共有することで、より一層のセキュリティ対策が期待できるため情報共有に関する概念についても理解しておく必要がある。以下に配布フェーズにおける実施事項の概略図を示す。

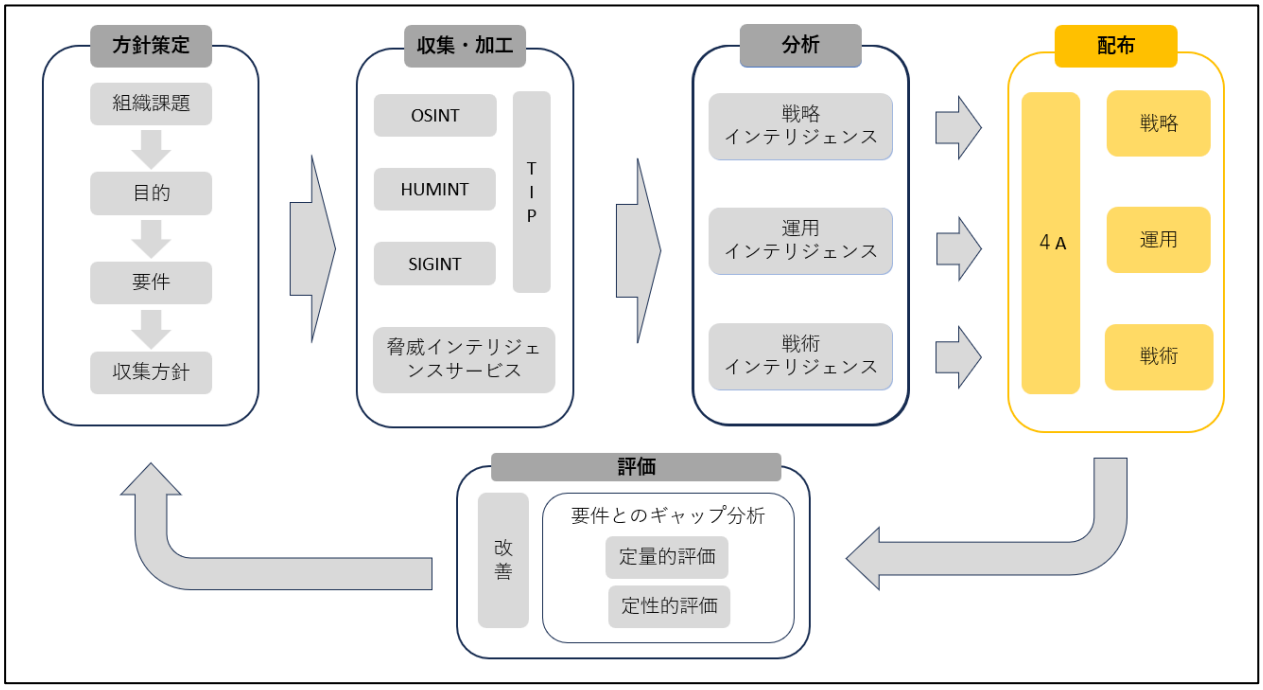


図 23. ライフサイクルにおける配布フェーズの位置づけ

7.1　意思決定につながるインテリジェンスとは

「脅威インテリジェンスの教科書」において、作成したインテリジェンスが意思決定に資するものか評価する指標として、４Ａという考え方を紹介している。[20] ４Ａでは、「正確であること（Accurate）」、「利用者目線であること（Audient Focused）」、「次のアクションに繋がること（Actionable）」、「適切なタイミングであること（Adequate Timing）」という４つの観点について評価を行う。特に、「正確であること（Accurate）」については、インテリジェンスがある程度の推測と不確実性を持つ特性上、重要な考慮要素となる。

[20] 「脅威インテリジェンスの教科書」／石川朝久［著］／技術評論社　P.7 より

表 13. 4A 指標

要素	戦略的インテリジェンス （配布例）経営層	運用インテリジェンス （配布例）CSIRT	戦術的インテリジェンス （配布例）SOC
インテリジェンス例	脅威動向をもとにしたセキュリティ戦略のレポート	自組織を狙う脅威アクターの攻撃シナリオ	他社から提供されたIoC情報
正確であること （Accurate）	外部環境情報には今後の動向の推測が含まれるため、組織の意思決定に必要な粒度の正確性が担保できているか	脅威アクターや攻撃手法が自組織に影響を与えるものか確認できているか	エンリッチメントなどによって侵害情報の正確性が確保されているか
利用者目線であること （Audient Focused）	提供されるレポートなどが経営層が理解・判断できる粒度で記載されているか	攻撃概要や影響、攻撃手口が整理されており、自組織への適用が想定される内容か	検知・遮断に必要な技術情報を含めて提供できているか
次のアクションに繋がること （Actionable）	経営層に承認が必要な情報を全て列挙できているか	ペネトレーションテストやTLPT、サイバー攻撃訓練など、今後のセキュリティ検証にて活用できる内容であるか	利用できる形式でインテリジェンスが提供されているか
適切なタイミングであること （Adequate Timing）	分析した外部動向が最新の状態でレポートできているか	攻撃手口が既に使われていないものでないか、分析結果は十分か	IoC情報が必要なタイミングで提供できているか

7.2 インテリジェンス情報共有の取り組み

公的機関やセキュリティベンダーによる観測情報とその分析結果が脅威情報として利用されることが多い。これとは別に、実際に侵害痕跡が確認された企業の観測情報、インシデント情報も脅威情報として用いることで、正確性と自組織への到達可能性という両面において絶大な効果を発揮する。総務省の「サイバー攻撃被害情報と公表のあり方について」では、外部連携を以下の3フェーズに分類している。[21]

① （非公開の）情報共有
② 所管官庁への報告
③ 脅威情報

インシデント情報の共有が必ずしも被害の報告となるわけではないことや、情報共有不足の課題をインシデントの公表が企業のセキュリティ対策の“落ち度”とみなされることを念頭に、組織名や組織の秘密情報など、脅威情報の共有に必要ないコンテキスト情報の秘匿性確保の取り組みについて記述されている。以下の表と図は同レポート内で定義されている情報の分類として被害組織の特定につながりやすい「情報」と被害組織の特定にはつながりにくい「技術情報」についての説明である。

表 14.「技術情報」と「情報」の分離について（総務省）

区分	説明	例
コンテクスト情報	個別組織名や対応経緯、被害内容など、被害組織に固有の情報を「コンテクスト情報」と呼ぶ。コンテクスト情報は、コントロールされずに拡散すると、被害組織が特定されたり、被害組織や被害組織の関係組織における二次被害にも繋がる恐れがある情報である。	• サイバー攻撃を受け漏洩した情報の件数や内容などの被害情報 • どのような対応を行ったのか
技術情報	攻撃に使用されたマルウェアや不正通信先情報などを「技術情報」と呼ぶ。技術情報は、他の被害組織でも同一の情報が見つかったり、すでに公開情報である場合が存在するなど、必ずしも被害個社に固有の情報ではない。（攻撃の種類によってはマルウェア内に標的組織（被害組織）固有の情報を含んでいる場合があるため、例外は存在する）	• 不正アクセス先のIPアドレス • マルウェアハッシュ値
技術情報とコンテクスト情報の中間の情報	被害の様態として、被害組織が利用していた特定製品の脆弱性が悪用されたり、被害組織以外の第三者の Web サイトや提供するサービスが攻撃の踏み台となる場合がある。この場合、攻撃手法を示す情報として、被害組織を特定する情報ではないが、製品の製造元やサービス提供元といった、第三者の組織名、製品名、サービス名が含まれることになる。	• 製品名や開発元組織 • サービス名

21 「サイバー攻撃被害情報と公表のあり方について」https://www.soumu.go.jp/main_content/000762951.pdf

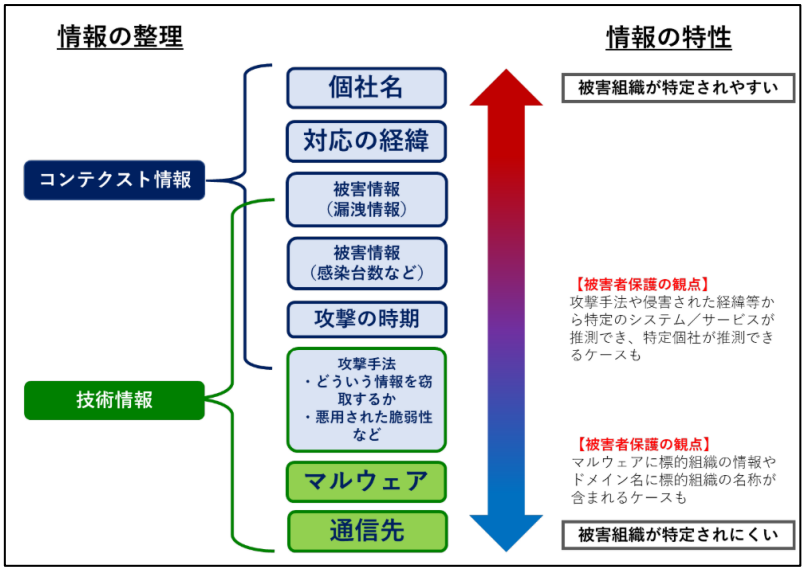


図 24. 技術情報と情報の区分（総務省）

同レポートにおいて、情報共有の時間軸と共有範囲を情報の種別ごとに適切なタイミングで共有することが重要であることが記述されている。

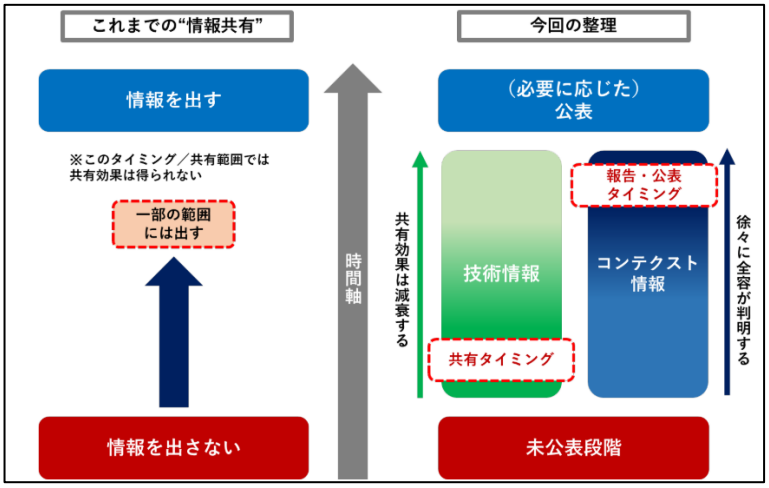


図 25. 情報共有の時間軸と共有範囲

日本では、サイバーセキュリティに関する情報共有コミュニティが複数存在する。重要インフラセクターとして指定された業界では各業界で SIG（Special Interest Group）が展開されており、秘密保持契約（NDA）をもとに IPA をハブとして組織間、SIG 間での情報共有する「J-CSIP」という取り組みがある。[22]

[22] 「J-CSIP」https://www.ipa.go.jp/security/j-csip/about.html

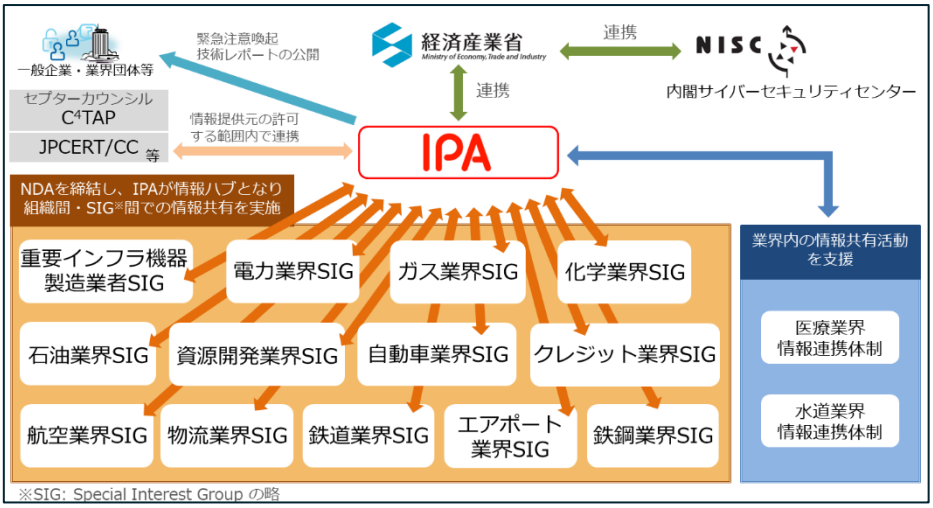


図 26. 各業界の SIG と公的機関の関係（IPA）

8 評価フェーズにおける実施事項

評価フェーズでは、インテリジェンスを配布した後にインテリジェンス要件とのギャップ分析を実施することで、次のインテリジェンスライフサイクルに向けての改善活動を実施する。セキュリティを取り巻く環境や脅威は常に変化するため、作成したインテリジェンスの評価結果や外部環境の変化に伴い、方針の定期的な見直しと継続的な活動が必要となる。以下に評価フェーズにおける実施事項の概略図を示す。

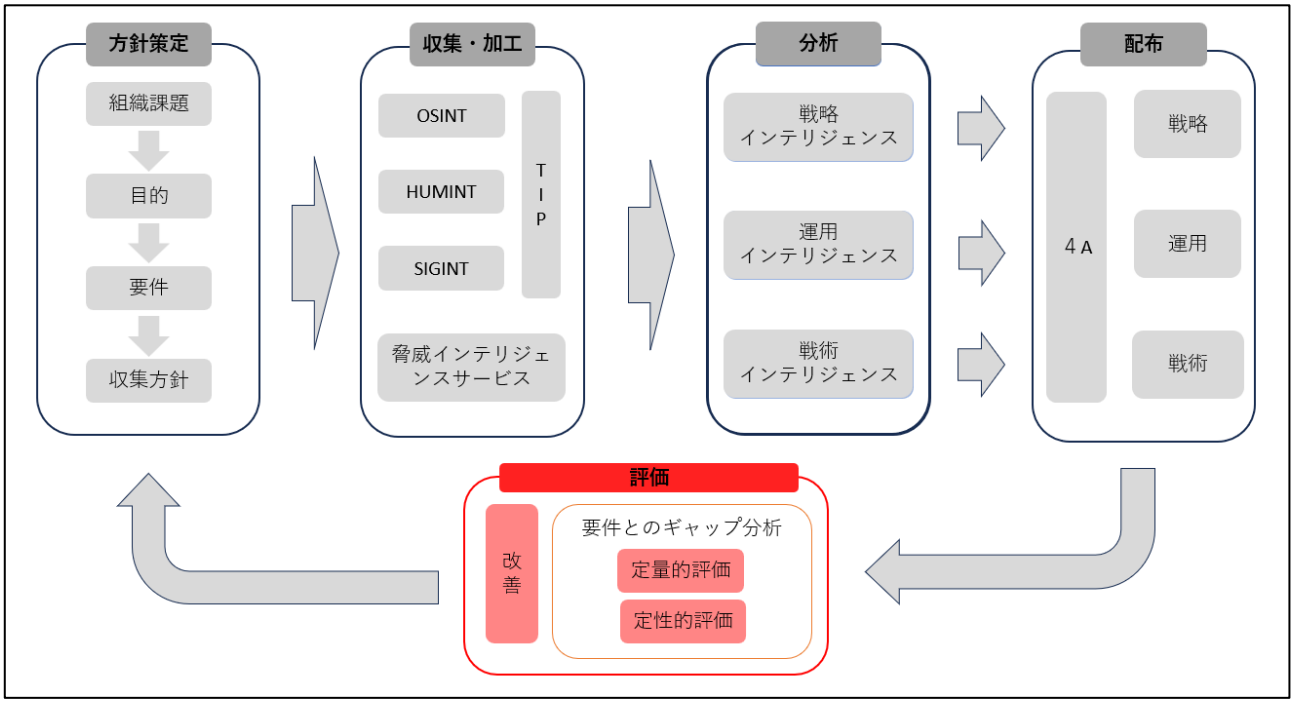


図 27　ライフサイクルにおける評価フェーズの位置づけ

8.1 フィードバックと要件とのギャップ分析

利用者に配布したインテリジェンスを評価するために、フィードバックと要件とのギャップ分析を実施し、経営層への脅威インテリジェンス活動のレポートやライフサイクルの改善に努めることが求められる。良いインテリジェンスに求められる 4 A の考え方を評価にも適用し、利用者へのフィードバックによる定性的評価や実際のインシデント件数、セキュリティ製品で設定した検知・遮断件数などの定量的評価を踏まえ、ライフサイクルの改善を実施する。また、方針策定フェーズで定めたインテリジェンスを活用する目的と比較し、達成度合いを確認することで、要件とのギャップを分析することも望ましい。以下の表にて、定量的・定性的評価の際の評価項目の一例を示す。

表 15. 定量的・定性的評価の一例

評価方法	評価内容
定量的評価	✓ 情報収集の件数 ✓ インテリジェンスの分析件数 ✓ IoCの対応実績と検知・遮断実績 ✓ 分析した脅威に対するインシデント発生件数
定性的評価	✓ 利用者からの満足度 ✓ インテリジェンス要件に対する充足度 ✓ セキュリティリスク、脅威動向への理解度 ✓ 経営層のセキュリティ意識向上度

8.2 ライフサイクルの改善

定量的・評価結果をもとにライフサイクルの改善を実施する。改善については各フェーズに改善点があるかどうか４Ａをもとに検討する。以下の表にて改善を支援するための問いかけ内容の一例を示す。第２章のセキュリティ成熟度評価の内容と合わせて組織のセキュリティ能力と脅威インテリジェンスの取り組み強化に取り組むことが望ましい。

表 16. ライフサイクル改善のヒント

フェーズ	問いかけ
方針策定フェーズ	✓ 組織課題：課題の状況に更新があるか？ ✓ 目的：課題に対する目的が一致しているか？ ✓ 要件：課題と目的とのギャップを埋めることができるか？ ✓ 収集方針：要件を満たす情報が取得できているか？ ✓ 必要な成熟度：組織リソース・ポリシー・技術が不足していないか？
収集・加工フェーズ	✓ 収集効率はリソースに対して十分か？（集約ツール、アウトソース、自動化） ✓ 収集容量は十分か？（ストレージの拡張、外部保管） ✓ 分析しやすい形で収集できたか？
分析フェーズ	✓ インテリジェンスに必要な情報が分析結果から得られたか？ ✓ 信頼性のある分析結果か？ ✓ 分析にかかる時間は適切だったか？
配布フェーズ	✓ 正確であること ✓ 利用者目線であること ✓ 次のアクションに繋がること ✓ 適切なタイミングであること

9　脅威インテリジェンスの成熟度評価

脅威インテリジェンスの取り組みを実施中の組織は、自組織の脅威インテリジェンスに特化した成熟度評価を実施することで取り組みを可視化することが考えられる。

組織の脅威インテリジェンスの取り組みにおける成熟度を評価する指標の一つとして、デルフト工科大学が提供する” Cyber Threat Intelligence Maturity Platform “がある。[23]下図のとおり、このモデルは組織の脅威インテリジェンスの成熟度をプログラムに必要な 5 つのドメインと 12 のテーマに分類し、6 段階でスコアリングする指標である。

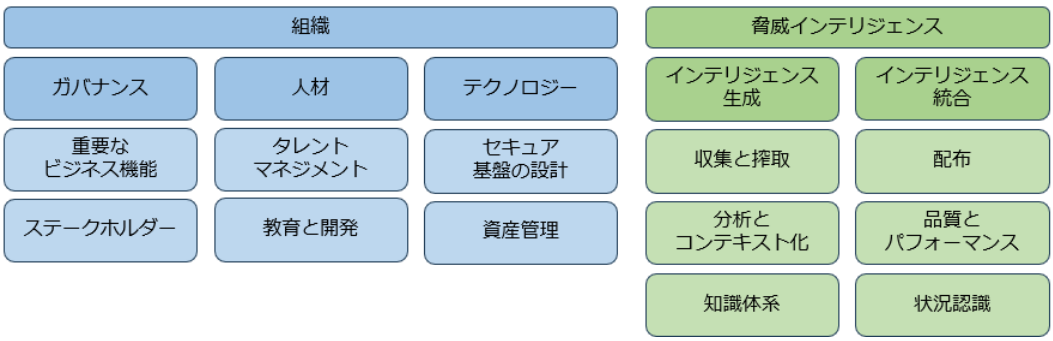


図 28. Cyber Threat Intelligence Maturity Platform（TU Delft）

○ガバナンス

事業目的・重要資産が特定されているか、それらの依存関係と組織全体に及ぼす影響が理解されているかを評価する。また経営層やステークホルダーと協力して意思決定に役立つインテリジェンス要件が定まっていることを評価する。

○人材

脅威インテリジェンスを利用できる人的リソース、必要なスキルの開発、その他必要不可欠な機能が組織全体にどのように配置され、定義されているか評価する

○テクノロジー

自組織のセキュリティ管理状況を理解し、脅威インテリジェンスを活用して防御を向上させる手段・技術資産の利用状況を評価する

○インテリジェンス生成

インテリジェンス要件を満たすために必要なデータを収集できているか、信頼性や一貫性を確保するプロセスが存在するか評価する。また収集したデータを分析し自組織に必要なコンテキストが生成できているか評価する

○インテリジェンス統合

生成したインテリジェンスが適切な関係者に共有され、関係者からのフィードバックによって

[23] 「Cyber Threat Intelligence Maturity Platform」https://www.cti-maturity.com/

品質の改善に継続的に取り組んでいるか、脅威動向の状況認識ができているか評価する。6 段階のレベルについては以下の図のとおりである。

表 17. 成熟度レベル

成熟度	説明
0 アドホック	活動は開始しているが、組織化されていない
1 定義済み	脅威インテリジェンスに特化した運用が形式化されている
2 統合済み	脅威インテリジェンスの活動が組織のプロセスと統合され始めている
3 管理済み	脅威インテリジェンスの活動を想定し、目標との適合を図っている
4 最適化	プロセスを体系的に分析し、最適化するための改善策を実施する
5 革新的	新しい脅威インテリジェンスの手法やツールを積極的に開発・導入している

また Cyber Threat Intelligence Maturity Platform は評価ツールとしての Web UI を提供する。現在どのような活動を行っているか、機能をどの程度実装しているかを 250 項目の質問により評価する。評価結果として組織内の脅威インテリジェンスの現在の成熟度に関する分析結果とプログラムの改善に必要な推奨項目を提供する。

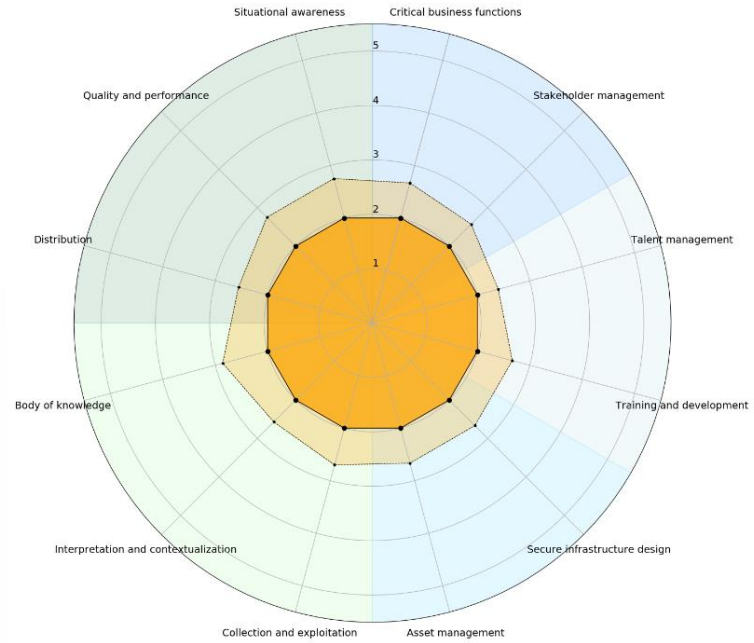


図 29. Web UI による成熟度評価結果の可視化

10 脅威インテリジェンス活用ケーススタディ

前章までの方針策定～配布フェーズをもとに、脅威インテリジェンス活用の一例を紹介する。ここでは5つのケースを想定し、ある程度網羅的な対応を記載しているが、脅威インテリジェンスをこれから実施する組織は、当ケーススタディを参考に自組織が必要なインテリジェンス、運用可能なインテリジェンスを5つの中から選定し進めることも可能である。

10.1 方針策定フェーズ

○インテリジェンスの目的と要件の整理

組織は脅威インテリジェンスを活用し、プロアクティブなインシデントの予防と、事後的なインシデント対応の両方を実施したいと考えている。また、組織に影響を与える可能性のある脅威と自社の対応状況を整理し、リスク管理を行いたいと考えている。これらの目的からインテリジェンス要件を以下のように整理した。

表 18. インテリジェンスの目的、必要アウトプットに紐づくインテリジェンス要件

目的	項目	アウトプット	インテリジェンス要件
【インシデント予防】 自組織に影響を及ぼす可能性の高い脅威への事前対応、リスク管理	国外、国内で流行している脅威	(戦略) ・ 経営層への脅威動向のレポート ・ セキュリティリスク状況の報告とセキュリティ戦略の策定	・ 脅威情報とその攻撃概要、影響、攻撃手口、発生頻度、推奨対策情報 ・ 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況 ・ 推奨対策の自組織の実施状況
	自社・特定業界を狙った攻撃キャンペーン情報	(戦略) ・ 経営層への脅威動向のレポート ・ セキュリティリスク状況の報告とセキュリティ戦略の策定	・ 自社、特定業界を狙った攻撃キャンペーン情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策 ・ 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況 ・ 推奨対策の自組織の実施状況
		(戦術) ・ IoC情報と付随情報	・ 攻撃キャンペーンに利用されるIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、内部評価結果）
	関連業界、地政学的関係のある他社のインシデント情報	(戦略) ・ 経営層への脅威動向のレポート ・ セキュリティリスク状況の報告とセキュリティ戦略の策定	・ 関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策 ・ 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況 ・ 推奨対策の自組織の実施状況
	自社・特定業界を狙う脅威アクターの動向	(戦略) ・ 経営層への脅威動向のレポート ・ セキュリティリスク状況の報告とセキュリティ戦略の策定	・ 脅威アクター情報とその動向、動機、攻撃事例とその攻撃概要、影響、攻撃手口、推奨対策
		(戦術) ・ IoC情報と付随情報	・ 脅威アクターが利用するIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、内部評価結果）
【インシデント対応】 インシデント発生時の拡大、再発防止	自社で観測した侵害情報	(戦略) ・ 調査結果のレポートと再発防止策	・ IoCの検知数と分析結果、IoC情報から分析した攻撃手法や経路、脅威アクターの情報
		(戦術) ・ IoC情報と付随情報	・ インシデントで検知したIoC情報 ・ インシデント調査で発見、分析した追加のIoC情報

○情報収集方法の検討と選定（RFP）

分析された脅威情報の収集を念頭に、インテリジェンス要件に即した脅威インテリジェンスサービスを選定する。次に定めたインテリジェンス要件に対して自組織でのみ収集できる情報と、外部から収集できる情報に分類し、求める収集タイミング、出力形式を定め、RFP として定める。こうして整理した結果を以下の表に示す。当ケーススタディにおける自組織で収集可能な情報として、「自組織の対策の実施状況」と「自組織での検知・防御情報」「自組織で発見されたIoC 情報」が主に挙げられるため、以下の表の赤字取り消し線のようにこれらは RFP の要件から除外する。

表 19. インテリジェンス要件をもとにした RFP 例

分類	インテリジェンス要件（RFP）	タイミング	出力形式
国外、国内で流行している脅威	• 脅威情報とその攻撃概要、影響、攻撃手口、発生頻度、推奨対策情報	2半期ごと	レポート
	• 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況	都度	レポート
	• ~~推奨対策の自組織の実施状況~~	ー	ー
自社・特定業界を狙った攻撃キャンペーン情報	• 自社、特定業界を狙った攻撃キャンペーン情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	都度	レポート
	• 攻撃手口から想定される自組織における攻撃対象の有無、~~検知・防御状況~~	都度	レポート
	• ~~推奨対策の自組織の実施状況~~	ー	ー
	• 攻撃キャンペーンに利用されるIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、~~内部評価結果~~）	都度	CSV
関連業界、地政学的関係のある他社のインシデント情報	• 関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	都度	レポート
	• 攻撃手口から想定される自組織における攻撃対象の有無、~~検知・防御状況~~	都度	レポート
	• ~~推奨対策の自組織の実施状況~~	ー	ー
自社・特定業界を狙う脅威アクターの動向	• 脅威アクター情報とその動向、動機、攻撃事例とその攻撃概要、影響、攻撃手口、推奨対策	2半期ごと	レポート
	• 脅威アクターが利用するIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、~~内部評価結果~~）	都度	CSV
自社で観測した侵害情報	• IoCの検知数と分析結果、IoC情報から分析した攻撃手法や経路、脅威アクターの情報	都度	CSV
	• ダークウェブでの組織機密情報、アカウント、メールアドレスの漏洩情報	都度	レポート
	• ランサムウェア脅迫の有無、自組織の侵害報告	都度	レポート
	• ~~インシデントで検知したIoC情報~~	ー	ー
	• ~~インシデント調査で発見、分析した追加のIoC情報~~	ー	ー

作成した RFP をもとにインテリジェンスサービスベンダーへ RFI を実施し、以下の表のように比較を行い、自組織のニーズに適したサービス、ツールを選定する。

表 20. RFP に対する各社サービスの比較イメージ

分類	優先度	インテリジェンス要件（RFP）	A社	B社	C社
国外、国内で流行している脅威	中	• 脅威情報とその攻撃概要、影響、攻撃手口、発生頻度、推奨対策情報	国外レポート＋アナリストの分析	国内レポート	国外レポート＋アナリストの分析
		• 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況	ASM機能あり（攻撃対象の有無）	なし	なし
		• ~~推奨対策の自組織の実施状況~~	ー	ー	ー
自社・特定業界を狙った攻撃キャンペーン情報	高	• 自社、特定業界を狙った攻撃キャンペーン情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	ダークウェブのモニタリング	なし	なし
		• 攻撃手口から想定される自組織における攻撃対象の有無、~~検知・防御状況~~	ASM機能あり（攻撃対象の有無）	なし	なし
		• ~~推奨対策の自組織の実施状況~~	ー	ー	ー
		• 攻撃キャンペーンに利用されるIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、~~内部評価結果~~）	あり	なし	なし
関連業界、地政学的関係のある他社のインシデント情報	中	• 関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	なし	なし	なし
		• 攻撃手口から想定される自組織における攻撃対象の有無、~~検知・防御状況~~	ASM機能あり（攻撃対象の有無）	なし	なし
		• ~~推奨対策の自組織の実施状況~~	ー	ー	ー
自社・特定業界を狙う脅威アクターの動向	低	• 脅威アクター情報とその動向、動機、攻撃事例とその攻撃概要、影響、攻撃手口、推奨対策	あり	あり	あり
		• 脅威アクターが利用するIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、~~内部評価結果~~）	あり	あり	あり
自社で観測した侵害情報	高	• IoCの検知数と分析結果、IoC情報から分析した攻撃手法や経路、脅威アクターの情報	あり	あり	あり
		• ダークウェブでの組織機密情報、アカウント、メールアドレスの漏洩情報	ダークウェブのモニタリング	なし	ダークウェブのモニタリング
		• ランサムウェア脅迫の有無、自組織の侵害報告	ダークウェブのモニタリング	なし	ダークウェブのモニタリング
		• ~~インシデントで検知したIoC情報~~	ー	ー	ー
		• ~~インシデント調査で発見、分析した追加のIoC情報~~	ー	ー	ー

サービス選定の際には、コストの他にアフターフォロー、その他機能（アラート、エンドポイント・セキュリティ製品との連携、ダッシュボードのカスタマイズ性など）を考慮し、自組織に適合するものを選定することが望ましい。

○情報収集方法の検討（自組織での OSINT、HUMINT、SIGINT）

脅威インテリジェンスサービスを利用しない場合に網羅的に情報収集を行う方法を検討する。サービスを利用しているが、追加の情報が必要な場合もあわせて検討する。例えば、A 社のサービスを利用する場合は「関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策」を収集する必要がある。ここでは、国内でセキュリティに関する取扱いのあるニュースサイトや JPCERT/CC、業界コミュニティからの情報収集を検討する。また場合によって、自組織での対策状況や防御状況、攻撃対象となるソフトウェアの取り扱い有無について、実際にサービス、システムを取り扱う所管部門にヒアリングすることも必要である。このように整理した結果が下表のとおりである。

表 21. 要件を満たす情報収集手法の検討

分類	優先度	インテリジェンス要件（RFP）	OSINT	HUMINT	SIGINT
国外、国内で流行している脅威	中	• 脅威情報とその攻撃概要、影響、攻撃手口、発生頻度、推奨対策情報	A社サービス 公開セキュリティレポート	–	–
		• 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況	A社サービス	所管部門 ヒアリング	Proxy,IDS/IPS, EDR,AVログなど
		• 推奨対策の自組織の実施状況	–	所管部門 ヒアリング	–
自社・特定業界を狙った攻撃キャンペーン情報	高	• 自社、特定業界を狙った攻撃キャンペーン情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	A社サービス	–	–
		• 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況	A社サービス	所管部門 ヒアリング	Proxy,IDS/IPS, EDR,AVログなど
		• 推奨対策の自組織の実施状況	–	所管部門 ヒアリング	–
		• 攻撃キャンペーンに利用されるIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、内部評価結果）	A社サービス OSINTツール	–	Proxy,IDS/IPS, EDR,AVログなど
関連業界、地政学的関係のある他社のインシデント情報	中	• 関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策	セキュリティニュース	・JPCERT/CCの注意喚起・早期警戒情報 ・業界コミュニティからの共有情報	–
		• 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況	A社サービス	–	–
		• 推奨対策の自組織の実施状況	–	所管部門 ヒアリング	–
自社・特定業界を狙う脅威アクターの動向	低	• 脅威アクター情報とその動向、動機、攻撃事例とその攻撃概要、影響、攻撃手口、推奨対策	A社サービス	–	–
		• 脅威アクターが利用するIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、内部評価結果）	A社サービス OSINTツール	–	Proxy,IDS/IPS, EDR,AVログなど
自社で観測した侵害情報	高	• IoCの検知数と分析結果、IoC情報から分析した攻撃手法や経路、脅威アクターの情報	A社サービス	–	–
		• ダークウェブでの組織機密情報、アカウント、メールアドレスの漏洩情報	A社サービス	–	–
		• ランサムウェア脅迫の有無、自組織の侵害報告	A社サービス	–	–
		• インシデントで検知したIoC情報	–	–	Proxy,IDS/IPS, EDR,AVログなど
		• インシデント調査で発見、分析した追加のIoC情報	OSINTツール	–	Proxy,IDS/IPS, EDR,AVログなど

また、インテリジェンス要件をもとにしたインテリジェンスライフサイクルを整理した結果、インテリジェンス要件の方針策定～評価までの流れは下図のとおりとなる。

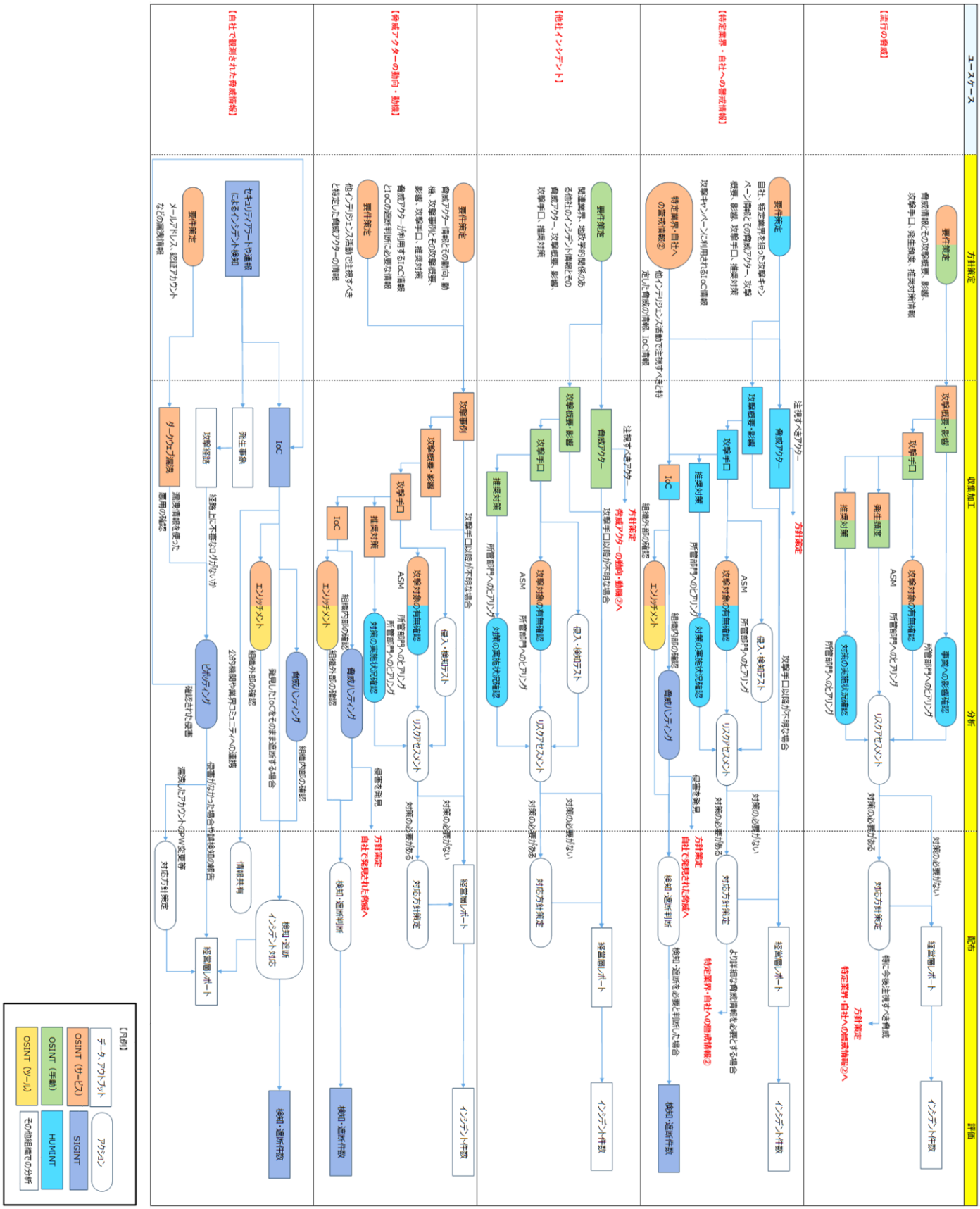


図 30.　インテリジェンス活動フロー

今回定めたインテリジェンス要件に対して網羅性のある対応フローとなっているが、実際には自組織で対応できる範囲の活動や自組織で必要な対応を追加して実施することになる。

以降のフェーズについてはインテリジェンス要件ごとにケーススタディを実施する。

10.2 ケーススタディ①：流行の脅威

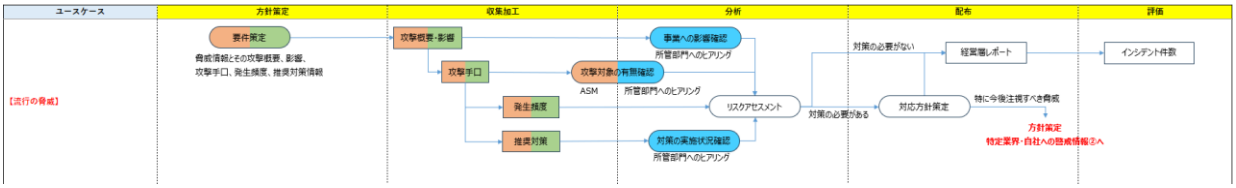


図 31. 流行の脅威に対するインテリジェンス活動フロー

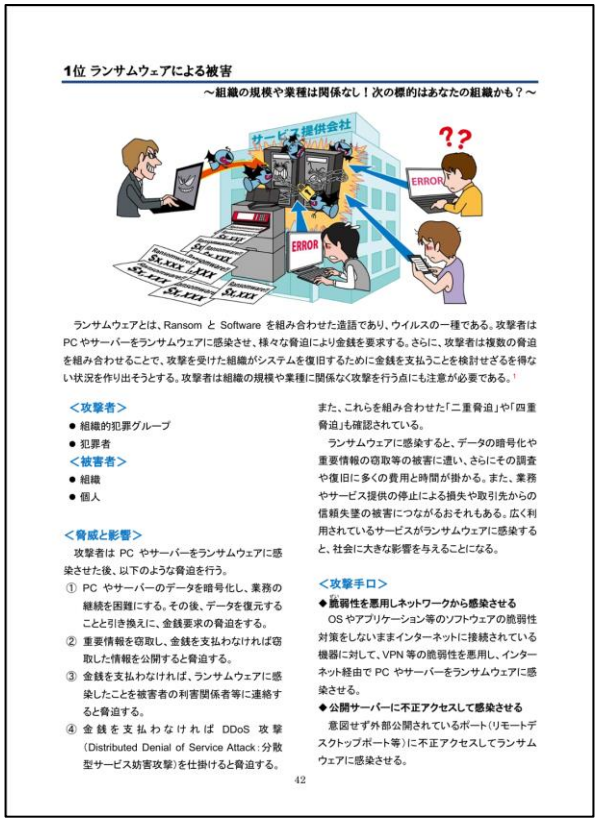
このケーススタディでは、流行の脅威に関わる情報を脅威インテリジェンスサービスと公開情報から収集し、アウトプットとして以下 2 つの戦略的インテリジェンスを作成するケースを取り扱う。

① アウトプット：経営層への脅威動向のレポート
　目的：経営層のセキュリティ意識の向上
② アウトプット：セキュリティリスク状況の報告とセキュリティ戦略のレポート
　目的：今後実施すべきセキュリティ対策の提案

収集・加工フェーズにおいて、IPA が公開する「情報セキュリティ 10 大脅威」と警察庁が公開する「令和 5 年上半期におけるサイバー空間をめぐる脅威の情勢等について」をもとに、流行している脅威として「ランサムウェア」にフォーカスを当てる。[24]

これらの公開情報から、ランサムウェアの攻撃概要として「PC やサーバを感染させてデータを暗号化することや重要情報を窃取することなどにより、復旧の対価に金銭を要求する攻撃」であること、攻撃手口と発生頻度として「VPN 機器からの侵入が最多となっている（ソフトウェア脆弱性の悪用）」こと、推奨対策として「該当機器のバージョンアップ対応」であることが読み取れる。

[24] 「令和 5 年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf



1位 ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～

ランサムウェアとは、Ransom と Software を組み合わせた造語であり、ウイルスの一種である。攻撃者は PC やサーバーをランサムウェアに感染させ、様々な脅迫により金銭を要求する。さらに、攻撃者は複数の脅迫を組み合わせることで、攻撃を受けた組織がシステムを復旧するために金銭を支払うことを検討せざるを得ない状況を作り出そうとする。攻撃者は組織の規模や業種に関係なく攻撃を行う点にも注意が必要である。[1]

＜攻撃者＞
- 組織的犯罪グループ
- 犯罪者

＜被害者＞
- 組織
- 個人

＜脅威と影響＞

攻撃者は PC やサーバーをランサムウェアに感染させた後、以下のような脅迫を行う。

① PC やサーバーのデータを暗号化し、業務の継続を困難にする。その後、データを復元することと引き換えに、金銭要求の脅迫をする。
② 重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する。
③ 金銭を支払わなければ、ランサムウェアに感染したことを被害者の利害関係者等に連絡すると脅迫する。
④ 金銭を支払わなければ DDoS 攻撃（Distributed Denial of Service Attack：分散型サービス妨害攻撃）を仕掛けると脅迫する。

また、これらを組み合わせた「二重脅迫」や「四重脅迫」も確認されている。

ランサムウェアに感染すると、データの暗号化や重要情報の窃取等の被害に遭い、さらにその調査や復旧に多くの費用と時間が掛かる。また、業務やサービス提供の停止による損失や取引先からの信頼失墜の被害につながるおそれもある。広く利用されているサービスがランサムウェアに感染すると、社会に大きな影響を与えることになる。

＜攻撃手口＞

◆脆弱性を悪用しネットワークから感染させる

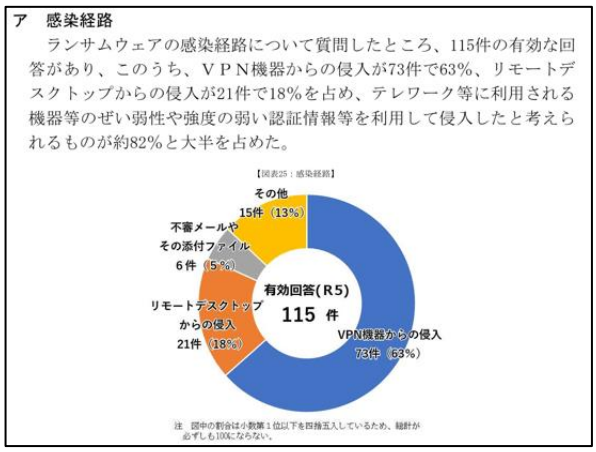
OS やアプリケーション等のソフトウェアの脆弱性対策をしないままインターネットに接続されている機器に対して、VPN 等の脆弱性を悪用し、インターネット経由で PC やサーバーをランサムウェアに感染させる。

◆公開サーバーに不正アクセスして感染させる

意図せず外部公開されているポート（リモートデスクトップポート等）に不正アクセスしてランサムウェアに感染させる。

42

図 32.　ランサムウェアの脅威の説明（IPA）



ア　感染経路

ランサムウェアの感染経路について質問したところ、115件の有効な回答があり、このうち、ＶＰＮ機器からの侵入が73件で63%、リモートデスクトップからの侵入が21件で18%を占め、テレワーク等に利用される機器等のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが約82%と大半を占めた。

【図表25：感染経路】

注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

図 33.　ランサムウェア感染の侵入経路の割合（警察庁）

また、攻撃対象の有無の確認においては、インテリジェンスサービスの一部機能である ASM 機能を使って自組織の公開資産の状況も収集することで、自組織が攻撃経路となっている VPN 機器を利用しているかどうか確認できる。ネットワークベースの ASM を利用する場合、実際にその機器とソフトウェアが実装されているか、分析フェーズにて所管部門に確認することが望ましいケースがある。これは、ASM が“外部から”確認、推測できる範囲の資産情報を分析している結果であり、実利用と誤差がある可能性を考慮している。ASM を利用する場合はまず、分析結果と実利用の状況の差分を分析することが推奨される。

分析フェーズでは、収集した情報から事業影響や対策状況などを追加したリスクアセスメントを実施する。

表 22. リスクアセスメントの例

		事業影響	被害想定	攻撃対象の有無	対策の実施状況	対応優先度
ランサムウェア・身代金要求	VPNを突いた攻撃 63%	社内ネットワークへの侵入によるデータの暗号化による業務停止	1週間の業務停止による 〇復旧費用 500万円	多数あり	未対応機器有	高
	標的型メール攻撃・マルウェアの送付 5%	社内情報漏洩または業務停止になる可能性大。	1週間の業務停止による 〇復旧費用 300万円	あり	社内周知 社内訓練済	中
	RDP 18%	--	--	--	--	--
DDoS・Webサイト停止		顧客がWebサイト閲覧不可になるが、事業は停止しない	1週間のWebサイト停止による 〇復旧費用 100万円	あり	CDN・WAFの導入済	中
フィッシング被害・クレカ情報の摂取		顧客のクレカ情報が漏洩するが、事業は停止しない	なし 騙される顧客が悪い	なし	なし	ー

配布フェーズではリスクアセスメントの結果、対応が必要となった場合、対応方針を策定（セキュリティ戦略）し、経営層へレポーティングを実施する。レポーティングする際の項目としては以下の内容が例として挙げられる。

・脅威の概要
・事業影響
・被害想定
・攻撃対象の有無
・対策の実施状況
・対応優先度
・対応方針

レポーティングの評価としては、定量的評価として、分析後に発生した当該脅威に関するインシデント件数や、インテリジェンス要件の達成度が考えられるが、そのほかにも経営層の理解状況や経営層間の情報連携の活用状況、意識向上度などの定性的評価の実施も考えられる。また、フォーカスした脅威に対して早急に対応が必要な場合は、自組織への警戒情報としてケーススタディ②の「特定業界・自社への警戒情報」として戦術的インテリジェンスが必要となるケースもある。

10.3 ケーススタディ②：特定業界・自社への警戒情報

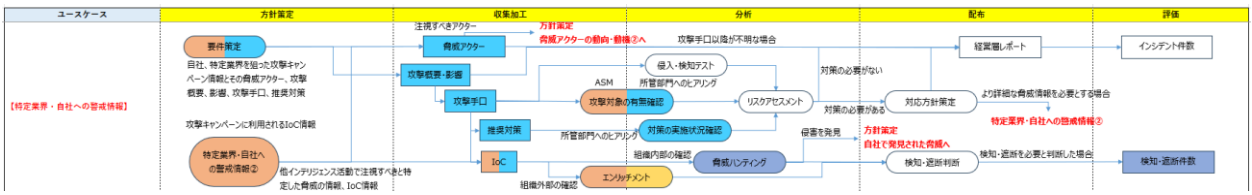


図 34. 特定業界・自社への警戒情報に対するインテリジェンス活動フロー

このケーススタディでは、自組織または所属する特定業界を狙った攻撃キャンペーン情報を事前に収集し、攻撃が自組織に到達する前にプロアクティブにセキュリティ対応を行うためのイン

テリジェンスを扱う。また、他のインテリジェンス活動でタイムリーに注意すべきと判断された脅威情報や悪用可能性のある脆弱性情報の収集などもこのケーススタディに含める。

このケーススタディでは、収集・加工フェーズにおいて過去に注意喚起として JPCERT/CC から公開された「日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起」（JPCERT-AT-2023-0029）の IoC 情報をもとに、戦術的インテリジェンスとして IoC 情報を分析し、遮断判断に必要な情報を収集する活動を検討する。[25]

図 35.　標的型サイバー攻撃活動に関する注意喚起例（JPCERT/CC）

まず収集・加工フェーズでは、注意喚起情報を受信することから始まる。方針策定フェーズにて「公的機関からの注意喚起情報」として JPCERT/CC からの注意喚起情報をメールで受信する、もしくは RSS で自組織の収集スクリプトや TIP の活用によって情報源が更新されたタイミングで新たな情報受信することを想定する。上述の JPCERT/CC からの注意喚起情報より収集・加工フェーズで必要な情報をマッピングすると以下の表のとおりとなる。

[25] 「日本の組織を標的にした外部からアクセス可能な IT 資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起」（JPCERT-AT-2023-0029）https://www.jpcert.or.jp/at/2023/at230029.html

表 23. 注意喚起情報から読み取るインテリジェンスに必要な情報

要素	
攻撃概要	日本の組織を標的にした外部からアクセス可能なIT資産を狙う複数の標的型サイバー攻撃活動 攻撃活動（A）：Array Networks Array AGシリーズの脆弱性を悪用する攻撃活動 攻撃活動（B）：Proselfの複数の脆弱性を悪用する攻撃活動 攻撃活動（C）：Array Networks Array AGシリーズ、Proself、Fortinet FortiOSおよびFortiProxy製品のいずれかの利用組織を狙う攻撃活動
攻撃手法	脆弱性を使った攻撃 CVE-2022-42897 Exploitなし(2023/11/30現在) CVE-2023-28461 Exploitなし(2023/11/30現在) CVE-2023-39415 Exploitなし(2023/11/30現在) CVE-2023-45727 Exploitなし(2023/11/30現在) **CVE-2023-27997 Exploitあり(2023/11/30現在)**
IoC	インディケータ情報：不正アクセス元のIPアドレス 154[.]31[.]112[.]129　173[.]249[.]201[.]243　35[.]229[.]146[.]251 45[.]32[.]49[.]130　45[.]32[.]252[.]239　45[.]66[.]217[.]106 45[.]32[.]33[.]120　95[.]85[.]91[.]15　139[.]162[.]127[.]90 167[.]71[.]207[.]51　176[.]97[.]70[.]81　194[.]102[.]36[.]128

この情報から、分析フェーズでは自組織が本脆弱性を含む機器の保有状況を確認し、脆弱性のあるバージョンの利用有無に関わらず、①侵害が自組織に到達していないか確認すること（脅威ハンティング）と、②今後遮断対応の必要があるかどうか判断するための情報（エンリッチメント）を分析することが求められる。

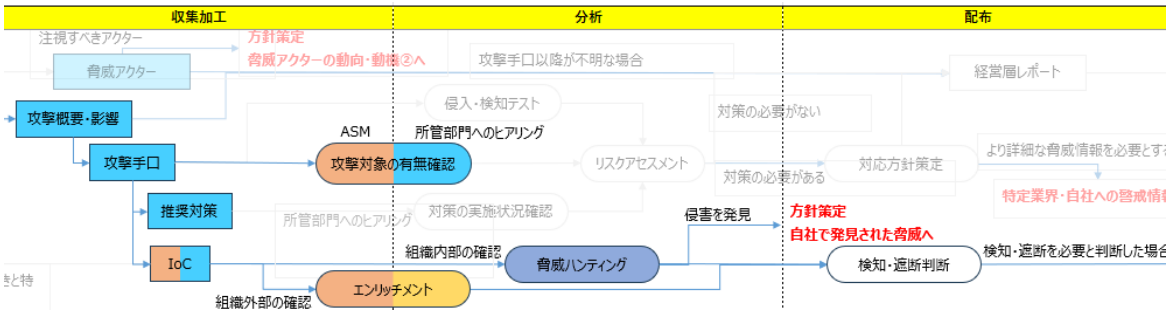


図 36. ケーススタディ説明範囲

○脅威ハンティング

侵害が自組織に到達していないかについては、ログを調査することで判断できる。例えば、今回は IoC 情報として不正アクセス元の IP アドレスが掲載されているため、プロキシログや FW ログ上で当該機器およびその他自組織の環境に対するアクセスを確認することが考えられる。また、組織内部のアクセス履歴を調査する場合、日常的にアクセスがあるかどうかも考慮する必要がある。例えば、IoC 情報として連携された IP アドレスが過去のものであり、現在は正規ユーザによって利用されている場合、遮断することで通常業務に支障をきたす可能性がある。後述の遮断判断に必要な情報として業務利用の有無を必要とする場合は、侵害到達の確認と合わせて業務利用の有無も確認することが望ましい。

○エンリッチメント

エンリッチメントには、情報源からの収集時に既に取得できる IoC 情報の追加情報や、脅威インテリジェンスサービスの分析結果として提供されるものが含まれる。また、自組織が OSINT ツールを使って能動的に分析する場合もある。組織は、これらの情報から自組織の遮断判断をどの情報に重きを置き対応するか検討する必要がある。

エンリッチメントの一環として、日常的なアクセスの有無に加えて業務への影響を確認する

ためには、該当 IoC の利用者や発行者情報などの IoC の出所に関する情報が必要である。例えば IoC が IP アドレスである場合は、どこの地域で使われているアドレスか、発行元の ISP（インターネットサービスプロバイダー）情報が該当する。IoC がファイル情報である場合はファイルの発行元組織の確認が必要である。ドメインの場合はドメイン取得組織、証明書の有無などが該当する。OSINT ツール、サービスを活用することで、収集した IoC に関する詳細情報を取得することができる。以下図は、OSINT ツールの一例である aguse を使って IoC の IP アドレスを検索した場合の例を示す。

図 37. OSINT ツール aguse を使った詳細情報の収集

その他遮断判断に必要な情報としては、外部のツールやレピュテーションスコア、アクセス先の情報、IoC の挙動、IoC の観測期間が挙げられる。レピュテーションスコアの判定を行うサービスの一例として、VirusTotal がある。このような OSINT ツールでは、ベンダー提供のセキュリティスキャンツールやブラックリスト、検知ルールに基づき、各ユーザがスキャンした結果をデータベースとして保有している。IoC 情報を検索することで、そのデータベースに基づいた悪性レベルを分析している。

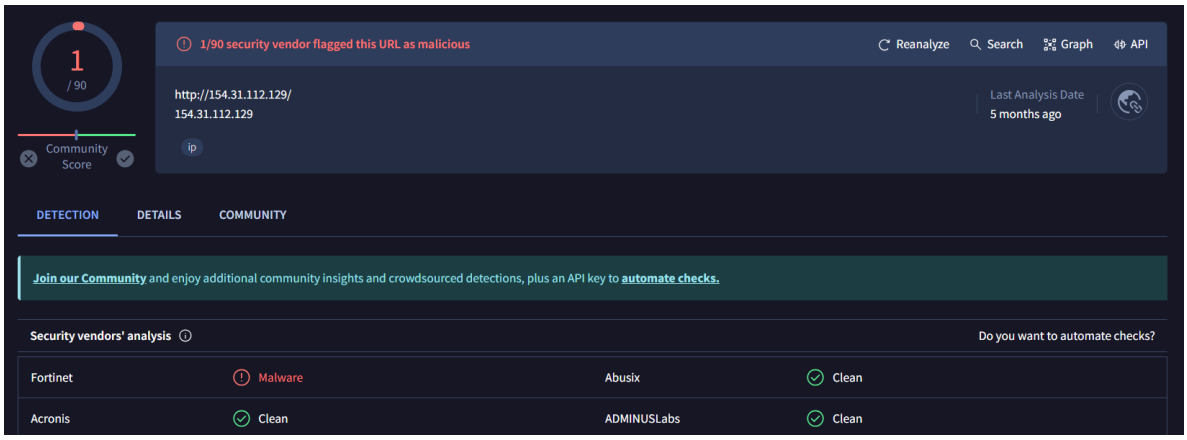


図 38. IoC 情報の IP アドレスサーチ結果（VirusTotal）

注意点として、レピュテーションスコアの判定に OSINT ツールを利用する場合、ツールごとに評価が変わる可能性があることと、スコアの根拠の有無を考慮する必要がある。従って、外部評価を行う場合は複数のツールやサービスで検証をおこない、判断材料を複数もつことが望ましい。

スコアの根拠は、遮断判断の際に業務影響の有無を考慮するうえで大きな価値がある。例えば、通信先の証明書が無い、暗号化通信が未設定である、といった場合では通信先がセキュアではないので遮断の判断ができる。

以上の分析フェーズにより、収集した IoC 情報を分析し、遮断判断の意思決定に必要なコンテキストを以下の表に整理する。

表 24. インテリジェンスに必要な付随情報の一例

要素	説明	例
IoC区分	IoCの種類（ネットワークベース、ホストベース、ファイルベースなど）	ネットワークベース
IoC	IPアドレス、MD5ファイルハッシュ、ドメインなど	IPv4アドレス：XXX.XXX.XXX.XXX
IoCの役割	IoCが何に利用されているか（C＆Cサーバ、攻撃元IP、トロイの木馬など）	不正アクセス元IPアドレス
発信元	IoC情報の提供元	JPCERT/CC
説明	提供元から得られるIoCに関する付随情報	標的型サイバー攻撃活動に関する注意喚起情報 以下の脆弱性の悪用が確認されたIoC情報 CVE-2022-42897 Exploitなし(2023/11/30現在) CVE-2023-28461 Exploitなし(2023/11/30現在) CVE-2023-39415 Exploitなし(2023/11/30現在) CVE-2023-45727 Exploitなし(2023/11/30現在) CVE-2023-27997 Exploitあり(2023/11/30現在)
業務影響に関する情報	誰から、どこから来たIoCか（IPアドレスの地域、発信元、発行元など）	IPアドレスの地域：｛国名｝ 発信元ISP：｛サービスプロバイダ名｝
各種ツールの分析結果	外部評価ツールによるエンリッチメントの結果	Aツール：malicious Bツール：10% ベンダーブラックリストに登録あり Cツール：4/90
内部検知	IoCの自組織のログ検知情報	なし
観測時期	IoCの観測された開始時期と終了時期	2023年3月～

表のように、IoC と付随情報をインテリジェンスとし、遮断判断を行う部門に配布する。また、インテリジェンス要件によっては IoC の数が膨大になることも予想されるため、外部評価ツールでの分析や IoC の発信元などの情報収集は API や TIP ツール、脅威インテリジェンスサービスを使って自動化を行うことを検討する必要がある。

10.4 ケーススタディ③：他社インシデント

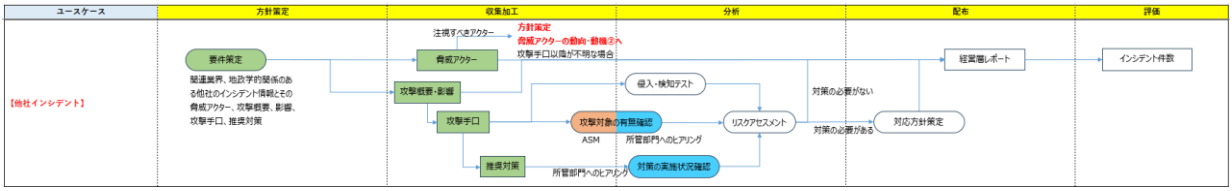


図 39. 他社インシデントに対するインテリジェンス活動フロー

このケーススタディでは、セキュリティニュースなどで収集した他社インシデント情報をもとにして、経営層への脅威動向のレポーティングや自組織への影響、対策有無を意思決定するためのインテリジェンスを扱う。当ケーススタディにおいては、他社インシデントが発生した際に経営層へレポーティングするための必要情報を整理することにフォーカスを当てる。

注意すべき点として、他社のインシデント情報はタイムリーに分析され、公開されるケースは多くないという点である。当該インテリジェンスはインシデント情報が最初に公開された直後に分析・配布されるものではなく、一定期間の分析を経て自組織で分析できるものである。実際に

Cyber Security Cloud 社の調査によると「1,000 件以上の個人情報を流出した法人・団体で サイバー攻撃発生から攻撃発覚までにかかる期間は 1 年以上」という分析結果を公表しており、同調査において「攻撃発覚」から「公表」までに要する期間は上場企業が 37 日だったのに対し、非上場企業は 111 日」とされている。[26]また、公表から詳細な分析、セキュリティニュースサイトなどで攻撃手口や推奨対策が公開されるケースとされないケースが存在し、公開までの期間も一定程度必要とされる。

他社インシデントの情報収集については、1 つの事例に対して一定期間に複数回レポーティングする可能性があることを念頭に、定期的な情報収集が必要となる。

分析フェーズにおいて経営層レポートに必要な情報を以下の表のとおり整理したうえで、情報の更新に合わせてレポーティングするインテリジェンスを作成する。

表 25. 他社インシデントにおける経営層レポートの項目例

要素	説明
発生企業	インシデントが発生した企業情報
発生日時	インシデントが発生した日
レポート日時	インテリジェンスの分析元となった記事の公開日時
被害内容	インシデントの内容、影響
原因	攻撃経路、攻撃手口
自社での発生可能性	攻撃手口となる資産、脆弱性、機会の有無
必要な対策	記事から読み取れる推奨対策事項 自組織状況を分析した結果考えられる対策

表 26. インシデント公表内容の追加に伴うレポート例

要素	説明
発生企業	某運航協会
発生日時	2023年7月4日 06:30頃
レポート日時	2023年7月5日時点
被害内容	名古屋港全ターミナルの作業停止
原因	ランサムウェアによる感染（LockBitによるものと報道あり）
自社での発生可能性	情報収集中
必要な対策	情報収集中 主要な感染ルートは、Webサイト、フィッシングメール、VPN装置、外部記憶媒体、不審なアプリケーションなど

要素	説明
発生企業	某運航協会
発生日時	2023年7月4日 06:30頃
レポート日時	**2023年7月27日時点**
被害内容	**データセンター内にあるNUTS（統一ターミナルシステム）の全サーバーの暗号化 全ターミナルの作業停止**
原因	**リモート接続機器「FortiGate」の脆弱性を悪用された不正なアクセス ※最新の重大な脆弱性に対応する修正を適用しておらず、セキュリティ運用体制に何らかの問題があった可能性がある**
自社での発生可能性	**VPN装置のOSバージョン及び脆弱性パッチは最新データ適用済みのため、同様の脆弱性による被害の発生可能性はない**
必要な対策	**済：VPN装置のOS及び脆弱性パッチの最新化**

10.5 ケーススタディ④：脅威アクターの動向・動機

このケーススタディでは、自組織・関連業界をターゲットとして活動する可能性のある脅威アクターの動向・動機にフォーカスを当て、アウトプットとして経営層への脅威動向のレポート（目的として経営層のセキュリティ意識の向上）、セキュリティリスク状況の報告とセキュリティ

[26] 「1,000 件以上の個人情報を流出した法人・団体で サイバー攻撃発生から攻撃発覚までにかかる期間は 1 年以上」
https://www.nikkei.com/markets/ir/irftp/data/tdnr/tdnetg3/20240221/ekyrf1/140120240221540621.pdf

戦略のレポート（目的として、今後実施すべきセキュリティ対策の提案）を作成する、戦略的インテリジェンスを主に扱う。国家が支援する脅威アクターについては、重要インフラの破壊活動や先端技術の知的財産情報の窃取など、組織、国家として影響が大きいサイバー攻撃の事例も存在する。従って、重要インフラ事業者や先端技術を扱う業界のセキュリティ強化の必要性を説明するうえで、脅威アクターの動向をレポーティングすることは重要であると考える。

情報収集フェーズにおいては、脅威アクター情報と使用する攻撃手口および手口の変化を分析することは非常にテクニカルであり、当該インテリジェンス要件を採用する場合、インテリジェンスベンダーのレポートやサービス、公的機関の公開するレポートを中心に収集することが望ましい。

分析フェーズでは、レポーティングに必要な情報を以下の表のとおり整理し、収集した情報を整理・分析する。

表 27. 脅威アクターの動向・動機における経営層レポートの項目例

要素	説明
レポートの目的（脅威アクターに関する報告）	実際に攻撃される可能性がある脅威アクターの実例をもとに、至近の脅威動向について説明する
アクター名	VoltTyphoon
アクター概要	Insidious Taurus（別名 Volt Typhoon）は、米国政府機関と政府の国際的な協力者らにより、**中華人民共和国（PRC）の国家支援型サイバー攻撃者**であることが特定されている。このグループは、おそらくは重大な危機ないし米国との紛争発生時に崩壊的ないし破壊的に行うサイバー攻撃に備え、**米国の重要インフラの IT ネットワーク内に事前に入り込む**ことに重点を置いている。 2024 年 1 月 31 日の公聴会で、FBI の Christopher Wray 長官は、米国と中国共産党の戦略的競争に関する米国下院特別委員会に対し、Volt Typhoon（Insidious Taurus）は「我々の世代の決定的脅威」と語った。
ターゲット・活動目的	米国本土および非大陸およびその領土内の、主に通信、エネルギー、輸送システム、上下水道システム部門の複数の重要インフラ組織の IT 環境を侵害したことを確認した。（米CISAレポートより） 南シナ海で動的な混乱が勃発した場合に混乱を引き起こし、通信や物資の移動をより困難にすることを目的とする。（DARKREADING）
攻撃事例	「Voltzite」がボルト・タイフーンの猛攻撃の一環としてアフリカの電力会社を攻撃 https://www.darkreading.com/vulnerabilities-threats/voltzite-zaps-african-utilities-volt-typhoon-onslaught
攻撃概要・影響	広範囲な偵察活動と潜在的な悪用を試みている（DARKREADING）

要素	説明
攻撃手口	① ASUS,CISCO,NETGEARなどのSOHO（Small Office Home Office）機器を侵害 ② Fortiのデバイスの脆弱性を突き侵入 ③ AD認証情報をFortiのデバイスから取得 ④ ネットワーク内の機器へのアクセス権を獲得 ⑤ 対象からデータ収集をしC2,LOTL（Living off the land）を駆使し検知を回避、潜伏 狙われる機器（DeCYFIR） Cisco, NetGear routers, SOHO routers, firewalls & VPN, Zoho
自社での発生状況	VoltTyphoonの**IoC**（ドメイン名、ハッシュ値等）を用いて○○でスキャンをかけたところ特に検知しなかったため、自社への影響は見られない
自社の対策状況（残存リスク）	• 当該脆弱性が発覚しているメーカを使用していない • 脆弱性情報を脅威インテリジェンスサービス等から収集し、リスク評価のうえ都度対応を行っている。 • ADのログインログや変更ログ等を監視している
対策方針	• 各機器へのログイン時の2要素認証化 • 認証・認可ロジックのレベルアップ

10.6 ケーススタディ⑤：自社で観測された脅威情報

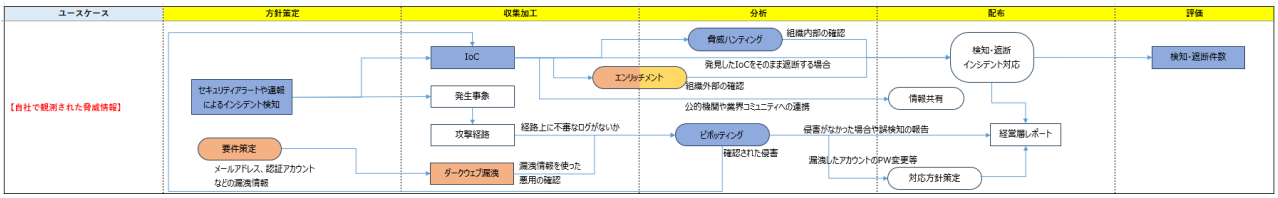


図 40. 自社で観測された脅威情報に対するインテリジェンス活動フロー

このケーススタディはインシデント対応の一環として、自組織のセキュリティアラートや標的型メールの開封などの従業員からの通報をトリガーにインテリジェンスを活用するケースである。ここでは戦術的インテリジェンスにフォーカスを当て、自組織で侵害情報が発見された際の対応を想定する。このケースにおけるインテリジェンスの目的としては、侵害があったか、もしくは疑わしい段階の IoC の評価し、悪性かどうか分析することと、発見された侵害以外の痕跡を見つけることである。

セキュリティアラートをトリガーに始める場合、EDR や IDS のふるまい検知機能などから実際

の IoC 情報が収集できるケースが考えられる。例えば、EDR であればデバイス上で実行・検知された不審ファイルのハッシュ値が該当する。また、IDS では不審な通信先の IP アドレスと通信プロトコルが該当する。その場合、既にセキュリティインシデントと思われる事象が確認されていれば IoC をすぐに遮断することが考えられ、不正なものと判断できない場合はケーススタディ②と同様に脅威ハンティングとエンリッチメントにより、悪性レベルを確認し IoC を分析することが考えられる。また、自組織で IoC が見つかった場合、①当該 IoC がどこから来たのか（侵害前の攻撃経路・活動）、②IoC がなにをしたか（侵害後の活動）という 2 点で他の侵害情報を見つける必要がある。例えば①について、マルウェアと思われるファイルを発見した場合、ネットワークログやデバイスのログから、そのファイルがどこから来たか（インターネット経由なら IP アドレスやドメイン、標的型メールであればメールアドレスなど）を特定し、新たな IoC 情報として追加する。②については、OSINT の外部評価ツールを用いて同様のファイルの過去の解析結果を収集することや、サンドボックス環境を提供するツールを用いてファイルの挙動やアクセス先、実行されるプロセスを確認することで新たな IoC 情報を得られる。

セキュリティアラートや従業員からの通報以外にも、ダークウェブ上での自組織アカウントや社内秘密情報の漏洩も既に侵害があったものとしてみなし、自社観測の脅威情報として扱う。社内のアカウントなど認証情報が漏洩している場合は、アカウントが利用されているシステムやデバイスなどのログや挙動を確認する。そして、侵害が確認された場合は新たに見つかった IoC 情報についても同様に遮断処置やエンリッチメント、脅威ハンティングを行い、初期の検知以外の侵害も除去することで、インシデント対応における原因の根絶・除去を網羅的に実施することができるようになる。

また、上記活動により発見された IoC は業界コミュニティや外部公的組織に積極的に連携することが望ましい。組織が相互に情報提供を実施することで、ケーススタディ②の自社・特定業界の早期警戒情報やケーススタディ③の他社インシデントをより効果的・迅速に実施することができる。

10.7 ケーススタディ⑥：経営層向け統合レポートの作成

ここまでのケーススタディでは個別のインテリジェンス要件を定め、それぞれ異なるタイミングでの経営層レポート作成について述べてきたが、組織によっては今後のセキュリティ戦略を策定するうえで年度末などの一定サイクルで包括的なレポートを作成、報告することもある。このケーススタディでは、「流行の脅威」「他社インシデント」「自社・特定業界への警戒情報」「脅威アクターの動向・動機」などの脅威動向に関する個別レポートを実施したうえで、年度末のタイミングで今年度の脅威動向をまとめ、自組織のセキュリティ戦略の重点要素に関するセキュリティ戦略をレポーティングするケースを想定する。

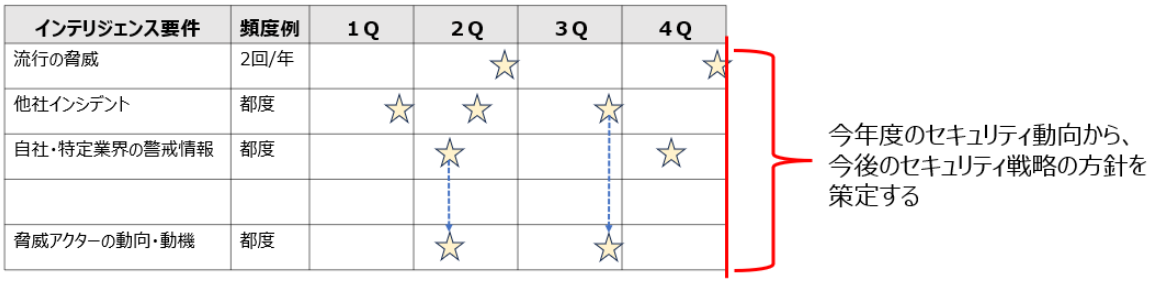


図 41. 経営層レポートの個別実施タイミングと統合レポートのイメージ

経済産業省が公開する「サイバーセキュリティ経営ガイドライン」において、経営会議でサイバーセキュリティリスクに関する報告を実施する際のレポート方向項目例として以下の内容がある。[27]

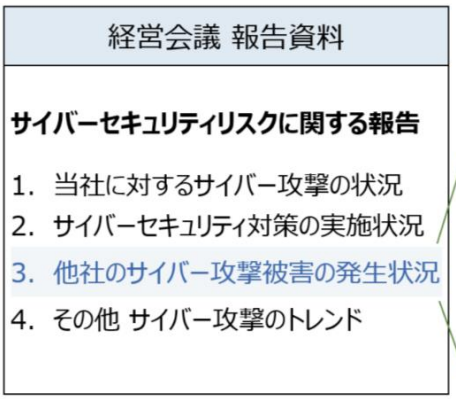


図1 経営委員会への
報告内容の目次例

表1 他社のサイバー攻撃被害の発生状況の報告例

発生企業	国内小売業	国内製造業
被害内容	一時的に通販サイトが利用できない状態。翌日サービス再開。	製品生産を担う取引先が自己増殖型ランサムウェアに感染。供給が月単位で滞った。
原因	DDoS攻撃	取引先のランサムウェア感染
自社での発生可能性	発生確率：低	発生確率：高
必要な追加対策	追加対策不要。運営を委託する自社WebサイトへのDDoS対策は実施済で、サーバダウンは受容する。	ネットワーク分離が必要。OA環境と倉庫は同一ネットワーク上にあるため、感染時の被害拡大が懸念される。

図 42.　サイバーセキュリティリスクに関する報告における経営層レポート項目例（IPA）

この図の事例においては、経営層へのリスク報告内容として①当社に対するサイバー攻撃の状況、②サイバーセキュリティ対策の実施状況、③他社のサイバー攻撃被害の発生状況、④その他サイバー攻撃のトレンドの 4 項目に整理しており、この事例をもとに今回ケーススタディとして実施した内容を照らし合わせると、以下の表のとおりとなる。

表 28. 経営層レポートの項目とケーススタディの関連性

項目	説明
当社に対するサイバー攻撃の状況	• 自社で発生したインシデント内容（**シナリオ⑤**） • 自社・特定業界への警戒情報（**シナリオ②**）
サイバーセキュリティ対策の実施状況	• 過去のセキュリティ戦略に基づいた対策の実施状況 • 脅威動向を基にしたセキュリティ対策（**全てのシナリオ**）
他社のサイバー攻撃被害の発生状況	• 他社インシデント事例（**シナリオ③**）
その他サイバー攻撃のトレンド	• 流行の脅威（**シナリオ①**） • 脅威アクターの動向・動機（**シナリオ④**）

上記の整理結果に加え、各ケーススタディの報告タイミングと報告内容を整理すると以下図のようになり、各ケーススタディの個別経営層レポートの内容を整理した結果と脅威動向にフォーカスした今後の重点取り組みの提案を行うこととなる。

[27] 「サイバーセキュリティ経営ガイドライン」https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

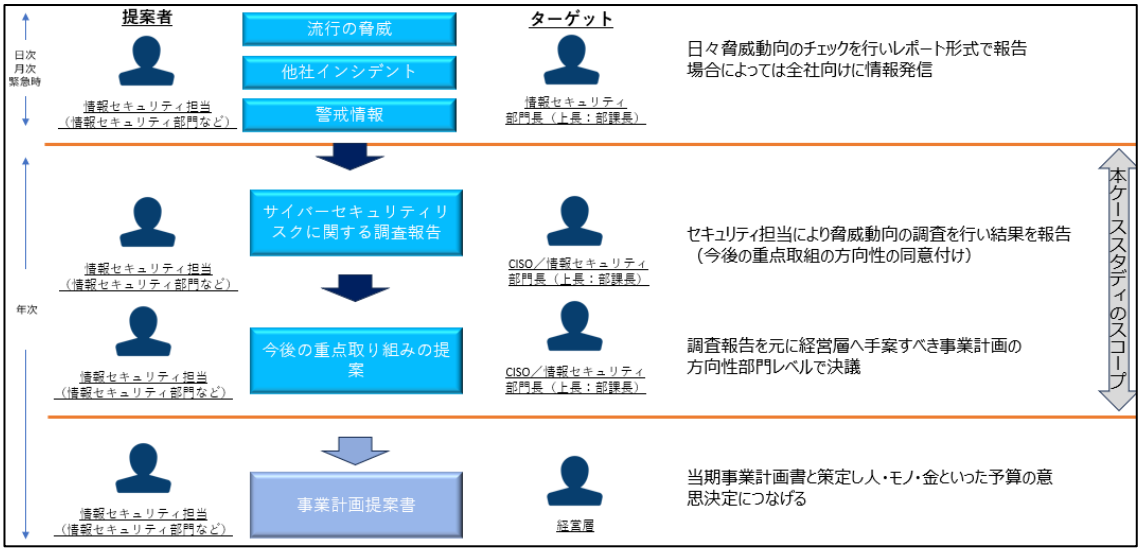


図 43.　個別レポートと統合レポート、セキュリティ戦略策定の流れ

ケーススタディ①～⑤の内容をもとに重点取り組みを検討した結果、以下表のとおり各ケースで関連性がある VPN 脆弱性を狙った脅威に重点をおくが方針の一例として考えられた。そのため、取り組み内容として VPN の機器管理や脆弱性対応の強化をおこない、セキュリティ戦略として必要なリソースや実施内容を定めていくことが想定される。

表 29. ケーススタディから分析される対応すべき脅威

項目	説明	ケーススタディ紹介事例
当社に対する サイバー攻撃の状況	• 自社で発生したインシデント内容（**シナリオ⑤**） • 自社・特定業界への警戒情報（**シナリオ②**）	（シナリオ②） • **VPN脆弱性を悪用した攻撃**に関する注意喚起情報
サイバーセキュリティ対策の 実施状況	• 過去のセキュリティ戦略に基づいた対策の実施状況 • 脅威動向を基にしたセキュリティ対策（**全てのシナリオ**）	–
他社のサイバー 攻撃被害の発生状況	• 他社インシデント事例（**シナリオ③**）	（シナリオ③） • **VPN脆弱性を悪用した**と想定される某運航協会へのランサムウェア攻撃
その他サイバー攻撃の トレンド	• 流行の脅威（**シナリオ①**） • 脅威アクターの動向・動機（**シナリオ④**）	（シナリオ①） • セキュリティ10大脅威における「組織」向け脅威1位ランサムウェアによる被害（攻撃手口として**脆弱性の悪用**） • ランサムウェア攻撃の手口として**VPN脆弱性の悪用が最多** （シナリオ④） • 特定業界をターゲットとした脅威アクターが**VPN脆弱性を悪用**して偵察活動を実施

10.8 （コラム）ケーススタディを実施したプロジェクトメンバーの所感

今回我々のプロジェクトは事業会社のセキュリティ部門所属のメンバーが大半であり、当ケーススタディを実践する中で、脅威インテリジェンスを事業会社としてどのように活用するべきかという観点を重視した。このコラムでは、ケーススタディを実施してみたメンバーの所感の一部を掲載するため、ガイドラインを活用する際に事業会社からの所感として参考にしていただきたい。

- 脅威インテリジェンスに学んだメンバーが集まってなんとか一つのケーススタディを完遂させたが、自社で行うには「人材確保」「組織的な体制構築」の両面で難易度はかなり高い。そのため、自社だけでなく業界単位で協力して進めていくことが脅威インテリジェンス活用の近道ではないかと感じた。また、プロジェクトに参加して、脅威インテリジェンスは手段ではなく、これまで行ってきた脆弱性対応や脅威ハンティン

グ、セキュリティ提案等の効果を高めるための一つの概念として理解することが大事であると感じた。

- ケーススタディでは脅威インテリジェンスの活用の流れをイメージすることが出来たが、前提として十分なリソースが必要であることもわかった。

- 過去のインシデント事例を基に活用方法を検討することで、実業務に落とし込んだ時のフローをイメージすることができた。一方、情報の鮮度が高く、必要な情報を含む他社インシデント事例を得るためには、情報共有の仕組みづくりとその成熟が重要であると感じた。情報共有の仕組みがない場合は、プレスなどが情報源なるため情報の粒度などは発信元の企業により大きく異なる。そのため、リアルタイムでの脅威情報を活用した対策などミッションクリティカルな活用は厳しく、経営層に対する情報共有程度にしか活用されない。他社インシデント事例の活用は課題があるものの、必要な情報が素早く共有することができれば、有効性を高められると感じた。

- 今回は脅威インテリジェンスを学んだメンバー数名である程度形にすることができたが、自社活用の際には脅威インテリジェンスの知識を浸透させて組織体制や人材を整える必要があると感じた。

- ケーススタディを通して、得られた情報から自社に役立つインテリジェンスに昇華するのはリソース（ヒト・モノ・カネ）が十分に必要であることを実感した。自社で同様の運用を想定するとある程度の自動化は必須であり、複数名の専門人材がいないと十分に活用できるインテリジェンスを形成できないように思えた。

- 脅威インテリジェンスをツールの総称ではなく、ライフサイクルと捉えなおすことが出来たのが良かった。ASM サービスや CTI レポート等の膨大な情報がある中で、自分たちが必要とする情報をしっかりと要件定義し活用していくことは簡単ではないと感じている。

- ライフサイクルとして方針-収集・加工-分析-配布-評価がまさにそうだ。脅威インテリジェンスを勉強するにつれ、（特にシナリオ作成フェーズは技術的レベルを要したアナリストがいないと難しいと思っていたが）成熟度レベルが低くても本プロジェクトを通してそれが可能だと感じた。特にケーススタディにおいては通常のガイドラインではないところまで踏み込んだものになっており、やって終わりではなく評価フェーズで経営層にレビューし改善までとまさに PDCA を盛り込んだ内容となっている。

11 （Appendix）コンプライアンス型アプローチとの融合

第 1 章で説明したとおり、脅威インテリジェンスのような脅威ベース型アプローチを従来のコンプライアンス型アプローチに組み合わせて運用することで、セキュリティ対策の向上が見込める。ここでは、コンプライアンス型アプローチの 1 つとして挙げられる、NIST Cyber Security Framework（NIST CSF）によるセキュリティ成熟度評価との関連性について説明する。[28]

11.1 脅威インテリジェンスの活用によるセキュリティ成熟度の向上

コンプライアンス型アプローチでは組織の現状とあるべき姿を網羅的に評価・把握できる利点がある一方で，対応優先度の決定に寄与しないという欠点がある。そこでコンプライアンス型だけでは不足する部分を脅威ベース型で補う形で活用することでセキュリティ成熟度の向上を図る。

例えば脅威インテリジェンスにおける脅威動向に着目し，それを NIST CSF 2.0 の特定や防御といった各機能に適用することで、具体的なセキュリティ対策立案や成熟度の向上に寄与することができる。以下の表では、NIST CSF 2.0 の一部機能を例に取り脅威インテリジェンスとの関連性を示す。

表 30. NICT CSF 2.0 と脅威インテリジェンスの関連

機能	サブカテゴリー	脅威インテリジェンスとの関連
統治	**GV.PO-02:** サイバーセキュリティリスクを管理するためのポリシー、プロセス、手順は、要件、脅威、テクノロジー、自組織の使命の変化を反映するためにレビュー、更新、伝達、施行される。	脅威動向を収集・分析し、戦略的インテリジェンスとして定期的にレポーティングを実施することで、リスク管理を行う。
	GV.OV-01: サイバーセキュリティリスク管理戦略の結果をレビューして、戦略と方向性を通知および調整する。	収集した脅威動向から自組織への影響や攻撃可能性、対策の実施状況を分析しセキュリティ戦略を策定する。
識別	**ID.RA-02:** サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	インテリジェンス要件として複数のソースから収集を行う。
	ID.RA-03: 内部および外部からの脅威が、識別され、文書化されている。	流行の脅威や警戒情報、他社インシデント情報を収集し分析・レポーティングを実施する。
	ID.RA-04: ビジネスに対する潜在的な影響とその発生可能性が、識別されている。	収集した脅威動向から自組織への影響や攻撃可能性、対策の実施状況を分析しレポーティングを実施する。
	ID.RA-05: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	同上
防御	**PR.IR-02:** 自組織のテクノロジー資産は環境の脅威から保護されている。	脅威動向からリスクアセスメントを実施し、保護状況と対策検討を実施する
検知	**DE.AE-07:** サイバー脅威インテリジェンスとその他のコンテキスト情報が分析に統合される。	収集した脅威動向、IoC情報をもとに内部・外部評価を実施し、意思決定に必要なコンテキストを分析する
対応	**RS.MI-01:** インシデントは、封じ込められている。	自組織での侵害が確認された際に、IoC情報をもとにピボッティングを行うことでそのほかの侵害を確認し、網羅的に封じ込めを実施する
	RS.AN-03: インシデント中に何が起こったか、およびインシデントの根本原因を特定するための分析が実行される。	IoC情報を分析し、攻撃経路や手口、ツール、テクニックを特定する。

11.2 成熟度評価における優先対策項目の順位付け

NIST CSF では「ティア」という概念を用いて対応状況を 4 段階で評価する。ティアは組織の対応状況を部分的である（ティア 1）から適用している（ティア 4）のいずれかの段階にあるかを示している。「ティア 1（部分的である）にあたると識別された組織は、ティア 2 以上を目指すことが推奨されるが、ティア 4 を目指すことが目的ではなく自組織のあるべき姿を達成するために用いる」と解説されている。

従って、脅威インテリジェンスを活用することで、自組織の背景や対策状況、脅威動向から自組織のリスクアセスメントを実施脅威ごとの対策用日が検討されるため、同プロセスにおいてセキュリティ対策の優先順位付けを支援することができる。

---

[28] 「NIST Cyber Security Framework（NIST CSF2.0）」https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

12 謝辞

本書の作成にあたり、文献の引用とレビューにご協力いただきました東京海上ホールディングスの石川朝久氏および技術評論社の皆様に感謝いたします。他にもご協力いただいた組織の皆様に脅威インテリジェンスの取り組みについてヒアリングさせていただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

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として本プロジェクトのメンターを実施いただきました門林雄基先生、満永拓邦先生および奈良先端科学技術大学院大学の方々、東洋大学の方々につきましても、ご指導・ご助言とともに、各検証機材のご支援を賜り続けてきました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをもとに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

【プロジェクトメンバー】

【リーダー】

二本松 立朗

【サブリーダー】

桐 明　零　　杉山　達哉

【メンバー】

岩田　真明	北島　稜平
下川部 一真	竹内　法彦
山本　将嗣	石村　祐太
小島　啓史	田鴎　健太
中角　直毅	平澤　泰山
平橋　智史	松 田　浩
大野　孝侑	荻　岳 仁
北谷　真聖	久保　貴司
繁田　大輝	渋 谷　篤
中野　貴裕	横道　太志
吉 里　将	

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。

13 付録

13.1 用語集（A-Z 順 -> あいうえお順）

用語	意味
IoC (Indicator of Compromise)	サイバー攻撃やセキュリティ侵害が発生している、または発生した可能性を示す証拠や手掛かりとなる情報のこと。 例）TTPs・ドメイン名・IP アドレス・ファイルハッシュ値 など
NDA (Non-Disclosure Agreement)	情報の共有に際して、共有した内容の目的外利用や第三者への漏洩を防止するため、情報管理の在り方について関係者間で結ぶ秘密保持契約のこと。
PoC (Proof of Concept)	一般的には、新しいアイデア、理論、または技術が実現可能であることを示すために検証をおこなうことを指す。 サイバーセキュリティの分野では特に、公開された脆弱性が実際に悪用可能かを実証するためのプログラムコードや文書を指すことが多い。
RFP (Request For Proposal)	システム構築・リプレイスを依頼する際にシステムベンダーに提出する、自社システムに必要な要件や実現したい業務（解決したい課題とあるべき姿）などを示した書類のこと。 システムベンダーは RFP をもとに具体的な提案を行う。
SIEM (Security Information and Event Management)	ファイアウォールや IDS／IPS、プロキシなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことで、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とした仕組みのこと。
SIG (Special Interest Group)	特定のテーマについて興味・関心のある人々の集まりのこと。
Telegram	ロシア発のインスタントメッセージアプリ。 匿名でのやりとりが可能であり、個人を特定されにくいため、プライバシーを重視するユーザに活用される。一方で、秘匿性が高いためにサイバー犯罪者グループで利用されることが多い。
TTPs (Tactics, Techniques, Procedures)	攻撃グループが利用する攻撃手法を Tactics, Techniques, Procedures の 3 つの階層で体系的に整理した内容のこと。 **Tactics**：攻撃者が達成したい目的 例）認証情報へのアクセス、権限昇格 など **Techniques**：目的を達成するために用いる技術 例）クレデンシャルダンピング、パスワードリスト攻撃 など **Procedures**：技術を達成するための一連のプロセス 例）パスワードリスト攻撃の場合 ダークウェブ等で流出したユーザ ID、パスワードを入手。 さまざまな Web サービスに対して、入手したユーザ ID、パスワードを自動的に入力していくツールを使用してログイン試行する。
悪性スコア	OSINT ツールなどで算出される、マルウェアなどの不正プログラムがどの程度悪性であるか示す定量的な指標のこと。
アンダーグラウンドフォーラム	ダークウェブや Telegram 上で運営されている、サイバー犯罪者同士で情報交換や金銭のやり取りをするための非公開のオンラインコミュニティや掲示板のこと。
攻撃キャンペーン	一定期間内において特定の組織／分野に対して特定の攻撃手法／攻撃インフラを用いて行われる攻撃活動のこと。

サプライチェーン	原材料や部材の調達、製品の生産、流通や販売など、製品が顧客の手元に届くまでの一連の活動プロセス、またはその一連の活動プロセスに関わる企業のこと。
サンドボックス	テストプログラムやマルウェア、不具合のあるプログラム等を実行するときに用いられる、通常のネットワークから隔離された仮想環境のこと。
スクリプト	コンパイルせずに実行できるプログラムのこと。
ゼロデイ脆弱性	ソフトウェアの脆弱性のうち、存在が世間に明らかになる前のもの。 ゼロデイ脆弱性を悪用して行われる攻撃を、ゼロデイ攻撃と呼ぶ。
ダークウェブ	匿名性保持や追跡回避の技術が使用されており、専用ソフトを使用しないとアクセスできない Web サイトのこと。
ディープフェイク	AI（人工知能）分野での用語である「ディープラーニング」と偽物でという意味の英語「フェイク」を組み合わせた造語で、AI を用いて、動画や音声を人工的に合成する処理技術を指す。あまりにリアルで高精細であることから、悪用されるケースが増え、社会問題となっている。
デカップリング	「分断」や「分離」という意味合いを持つ語。 ビジネスにおいては、国や地域間の経済分断の意で用いられることが多い。
トリアージ	もともとは医療分野における、災害時などに多数の傷病者が出た場合の傷病の深刻度等を加味した治療や処置の優先順位付けを意味する。サイバーセキュリティの分野では、セキュリティインシデント対応や脆弱性対応業務における、資産重要度等を加味した対応優先順位付けを指す。
ハッシュ値	データを固定長のランダムに見える値に置き換えることをハッシュ化と呼び、ハッシュ化された値をハッシュ値と呼ぶ。 データの秘匿性の向上やデータの改ざん検知等に用いられる。
プロアクティブ	「先を見越した」や「積極的な」という意味合いを持つ語。
ペネトレーションテスト	通信ネットワークで外部と接続されたコンピュータシステムの安全性を調査するテスト手法の一つで、既に知られている手法を用いて実際に侵入や攻撃を試みる方式。
ランサムウェア	悪意のあるソフトウェア(マルウェア）の一種。 感染したコンピュータを正常に利用できないような状態に置き、復元のために犯人への金品の支払いを要求する。”ランサム”は「身代金」の意。
レジリエンス	「回復力」や「弾力」、「復元力」という意味合いを持つ語。 ビジネスにおいては、災害やサイバー攻撃が発生した際、その状況に適応し、元の状態まで戻る能力の意で用いられる。