その情報で経営判断をして良いですか？

～脅威インテリジェンスから導く、リスクマネジメントの改善～

目次

2023 年 4 月

日本電気株式会社

1. サイバーセキュリティにおけるインテリジェンス

改めて注目される「脅威インテリジェンス」

日本においてもサイバーセキュリティインシデントの報道は珍しくなくなりましたが、その多くは適切に情報を入手し、対処を実行していれば防げたであろうものも少なくありません。VPN 機器の脆弱性を悪用したランサムウェア攻撃が注目を集めましたが、これらの脆弱性は修正パッチ公開から数年が経過しているものも存在し、資産や脆弱性の管理が適切に行われていなかった可能性を示唆しています。

ただし、世に存在する脆弱性の数は膨大であり、リソースも無限ではありません。そこで、脅威インテリジェンスを活用したセキュリティ対策があらためて注目されています。欧米諸国の先進企業では既に活用が前提とされていましたが、日本でも活用に向けた議論が進んでいます。2022 年 12 月に公開されたいわゆる防衛 3 文書(国家安全保障戦略・国家防衛戦略・防衛力整備計画)の内、今後の自衛隊の体制を示す「防衛力整備計画」でも、脅威インテリジェンスの活用を前提にすると思われる「サイバー・スレット・ハンティング機能」の強化が記載されました。

サイバー攻撃と防御の関係は、犯罪者と警察の関係に似ています。どうしても防御側が受け身なりがちで、新たな手口を犯罪者が真っ先に考案することも珍しくありません。脅威インテリジェンスというと何だかとっつきにくい語感ですが、このいたちごっこのギャップを解消するのに役立つものである、とまずは考えていただければと思います。本ホワイトペーパーでは、脅威インテリジェンスとはどういった考え方なのか、どのように活用できるのかを紹介します。

インテリジェンスとは

そもそもインテリジェンスとは何を指した言葉でしょうか。一時期は、「生の情報=Information」「分析した情報=Intelligence」のような説明を見かけることがありました。これは、インテリジェンスの簡単な説明としては間違っていませんが、あまりに簡略化しすぎているきらいがあります。

最も著名なインテリジェンス組織であるアメリカ CIA(Central Intelligence Agency)は、以下のようにインテリジェンスを定義しています。(筆者による抜粋と翻訳)

インテリジェンスとは、組織またはグループが安全や福利のために、競合する実体とその代理人に関する必要な情報を収集・分析することである。[1]

ここで重要なのは、「情報を収集・分析すること」です。CIA というと、スパイ活動が着目されがちですが、あくまでスパイ活動は上記目的を達成するための手段に過ぎません。収集・分析された情報は、米国大統領などに報告され、国家の政策決定判断の材料として使用されることになります。

日本におけるインテリジェンス組織としては、内閣情報調査室が代表例の一つです。内閣情報調査室が公開している役割「国内外の諸情勢に関する情報の収集・集約・分析・評価」についても見てみます。

当室では、メディア（新聞、雑誌、専門誌、 通信社ニュース、テレビ、インターネット等）からの膨大な公開情報のほか、学識経験者や民間の専門家等の様々な情報源との意見交換によってもたらされる情報、情報収集衛星による画像情報を収集・整理し、国内外の諸情勢に関する分析業務を行っています。また、外交・防衛・治安等の情報を担当する省庁によって構成されている「情報コミュニティ」の取りまとめ機関として、これらの省庁が収集・分析した情報を集約し、内閣の立場から分析・評価を行っています。[2]

ここでも情報の収集と分析が主な活動として記載されています。CIA の例と同じく、ここで収集・分析された情報も、内閣総理大臣などに報告され、やはり国家の政策決定判断の材料として使用されます。

2 つの組織を例に挙げましたが、その他のインテリジェンス組織においても、主要な役割は変わりません。つまり、インテリジェンスの役割とは次のように言い換えることが出来ると考えます。

意思決定や行動の判断材料となる情報を収集し、分析して必要な人物や組織に提供する機能。

意思決定の際には、必ずその元となる情報が必要となります。しかし、現代の複雑な社会環境の中では、意思決定者がそのような情報を直接収集・分析することは容易ではありませんし、バイアスの問題もあります。そこで、情報収集・分析機能を分離し、その分野の専門家集団に役割を担ってもらうという訳です。なお、インテリジェンスのもう一つ重要な特徴として、判断材料の提供が目的で、意思決定そのものは基本的には行わないことに注意が必要です。

ここまでは国家に関するインテリジェンスの観点で説明してきましたが、手元にある情報を元に意思決定を行うことは、大小問わずあらゆる組織が行っていることでもあります。例えば、外部コンサルタントや、法律事務所などに相談を行い、意思決定の補助を行ってもらうことは決して珍しくはないでしょう。こういった職業をインテリジェンス組織と言えるかは別として、専門家集団に情報の収集・分析を担ってもらうという考え方は、先程説明したインテリジェンスの役割そのものです。

脅威インテリジェンスとは

それでは、サイバーセキュリティ分野ではインテリジェンスはどのように扱われているのでしょうか。サイバーセキュリティでは、もっぱら脅威インテリジェンスという言葉が使用されています。この言葉の説明をいくつか引用してみます。

脅威インテリジェンスは、サイバーセキュリティの専門家が整理と分析を行う、根拠に基づいた、サイバー攻撃に関する情報です。[3]

脅威インテリジェンス（Threat intelligence）とは、情報セキュリティの専門家が分析・整理したサイバーセキュリティに関する情報の総称です。[4]

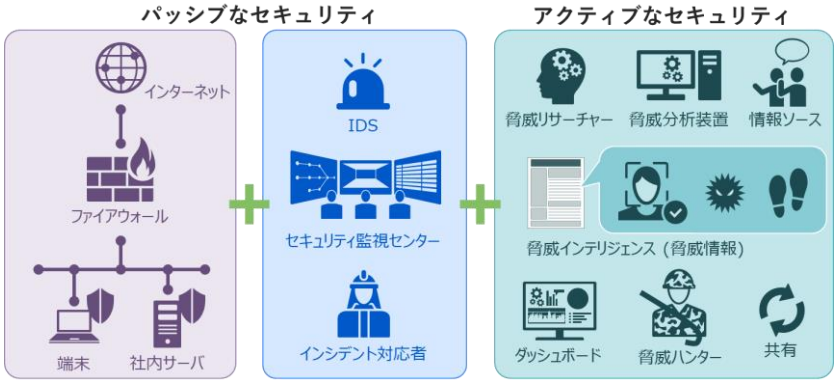
脅威インテリジェンスとは、攻撃者の動機、標的、攻撃パターンを理解するために組織によって収集、分析されたデータのことです。[5]

このように、前述したインテリジェンスの機能を、サイバーセキュリティの分野により特化させたものと考えることが出来ます。

サイバー攻撃のトレンド、注意すべき手法や脆弱性といった脅威情報を収集し、セキュリティ対策向上に役立つよう分析・提供する。

では、サイバーセキュリティに特化させた脅威インテリジェンスは、どのように活用できるのでしょうか。変わらない機能としては、意思決定者の判断補助です。例えば、ランサムウェアが流行しており、自分たちの組織も攻撃を受ける可能性があると分かれば、バックアップを強化する、サイバー保険に加入するといった判断が可能となるでしょう。

脅威インテリジェンスのもう一つの特徴としては、よりアクティブな防御を行うことが可能になる点です。（なお、ここで言うアクティブとは、ファイアウォールに代表されるようなパッシブなセキュリティの対比としての用語であり、オフェンスの要素は含みません。）サイバー攻撃の問題点の一つは、侵入済みの攻撃者や、既に起こってしまったインシデントにそもそも気づけないなどのギャップが存在することです。このギャップの解消法として、脅威インテリジェンスの活用があります。最新の攻撃手法の情報を収集・分析し、その手法が自組織への攻撃で使用されていないかを調査する、プロアクティブな防御に移行することが可能です。



パッシブなセキュリティに脅威インテリジェンスによってアクティブを付け足す

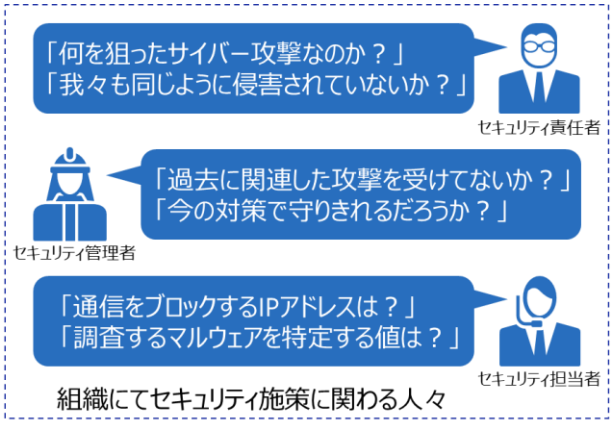
2.　立場によって異なる脅威インテリジェンス活用

受け手の立場によって必要なセキュリティ情報は異なる

脅威インテリジェンスの活用が難しい理由の一つとして、その情報を受け取る人物の立場によって、必要な情報が異なるという点が挙げられます。

例えば、マルウェアを使用したシステム破壊攻撃が報道されたと仮定してみましょう。このとき、CISO のようなセキュリティ施策の責任者の立場にある人物は「何を狙ったサイバー攻撃なのか？」「我々も同じように侵害されていないか？」といった、被害動向などの情報が必要となるでしょう。また、現場のマネジメントを行うセキュリティ管理者であれば、「過去に関連した攻撃を受けてないか？」「今の対策で守りきれるだろうか？」といった具体的な施策考察のための情報が必要です。SOC に携わるようなセキュリティ担当者であれば、「通信をブロックする IP アドレスは？」「調査するマルウェアを特定する値は？」といった数値やデータが必要となります。

このように、**必要な脅威インテリジェンスはその情報を活用する人物の立場によって形を変える**ため、異なる立場の人々に対し、不安を解消できるような情報が望ましいと言えます。



立場によって欲しい情報は異なる

脅威インテリジェンスの段階

立場によって必要な情報が異なるならば、提供先にあわせた脅威インテリジェンスが必要となります。これは裏返せば、受け手である自分たちが必要な脅威インテリジェンスの段階も把握しておく必要があるということです。脅威インテリジェンスでは、受け手の立場を戦略・戦術・運用の 3 段階に分けて表現することがあり、この場合それぞれ前述した責任者・管理者・担当者が当てはまります。自分たちが扱っている脅威インテリジェンスはどの段階にあるものなのかを常に意識することで、より効率的な活用が可能となります。

脅威インテリジェンスに関わる人物が SOC 担当者しかいない場合、CISO で活用できる情報は持て余しますし、逆に CISO が SOC の情報を貰ってもこれを活かすことはできません。

専門のチーム設置のススメ

立場によって必要な情報が異なるならば、脅威インテリジェンスの活用には複数のメンバーが必要なことは想像に難くありません。

しかも、これらの情報は完全に分断されているわけではなく、グラデーションのように連続していることがほとんどです。具体的なセキュリティ施策には責任者の方針が関係しますし、数値やデータも取得範囲などを事前に決めなければなりません。

そこで、情報収集・分析を専門的に行うチームを設置することができれば、以下のような機能を集約して効率的な運用が可能となります。

・継続的なリアルタイムでの情報収集
・幅広い情報ソースの管理
・分析能力
・報告書作成能力

一人 IT 管理者のような状況では、上記のような業務を行うことは非常に難しい上、複数の立場に向けて加工した情報を作成することはより困難であると考えられます。

アウトプットの重要性

専門チームの機能例として、報告書作成能力が含まれることを意外に思われる方がいるかもしれません。本ホワイトペーパー冒頭でも述べたとおり、インテリジェンスの機能には”提供する”ことが含まれます。どんなに優れた情報収集能力や分析能力を持っていても、適切なアウトプットを行えなければ、その能力を殺してしまう可能性があります。

また、複数の段階に分割された脅威インテリジェンスを考えると、報告相手にあわせた分析結果の伝え方も重要です。例え同じ分析結果であっても、そこから必要な情報を抜き出し、適切なフレーズや分量で報告書を作成するには、ある程度の訓練や経験が必要となります。

セキュリティ以外の知見も重要

専門チームの中核はセキュリティ分析ですが、チームの構成員は必ずしもセキュリティに知見の深い人物だけが要求される訳ではありません。情報収集には語学が、情報ソースの拡充や管理にはコミュニティとの交流などが必要となるように、セキュリティ以外の知見を活かせる場面も多々あります。

このような場面で活躍されている方が、脅威インテリジェンスのチームに加わることは、チームの実力向上に大きく貢献します。

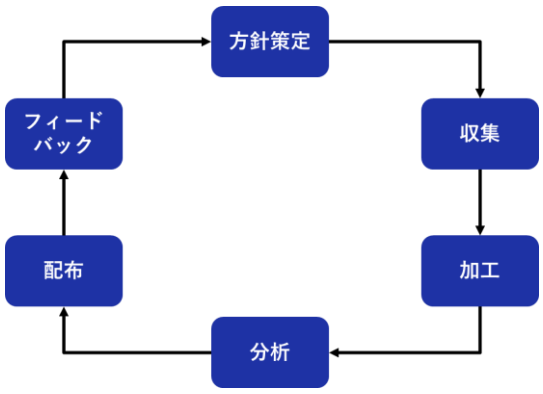
3.　脅威インテリジェンス活用の成熟

脅威インテリジェンスのサイクル

脅威インテリジェンスの活動はどこに始点と終点があるのでしょうか？インテリジェンスの定義を思い出すと、始点は情報の要求、終点は報告の提出と考えることができそうです。しかし、脅威インテリジェンス活動は一度切りでは終わりません。**絶えずセキュリティ上の脅威と向き合うことを考慮すると、始点と終点が繋がったサイクル活動の形態をとる必要**があります。また、要求と提出の間にも、複数の段階が存在しています。

一例として、インテリジェンスサイクル図を掲載します。サイクルのそれぞれの要素を見てみましょう。

・方針策定：インテリジェンスが答えるべき質問を策定する
・収集：質問に答えるために必要なデータの収集
・加工：データのフォーマット統一
・分析：収集されたデータを用いて策定された質問に答える
・配布：インテリジェンスを利用するステークホルダーに共有する
・フィードバック：質問に適切に答えられたかを確認する



インテリジェンスサイクルの例

あくまで一例のため、このサイクルや各パートの構成は場合により変更されますが、このようなサイクルに沿った活動を継続できるようになれば、脅威インテリジェンス活用ができていると言えます。

サイクルの強化

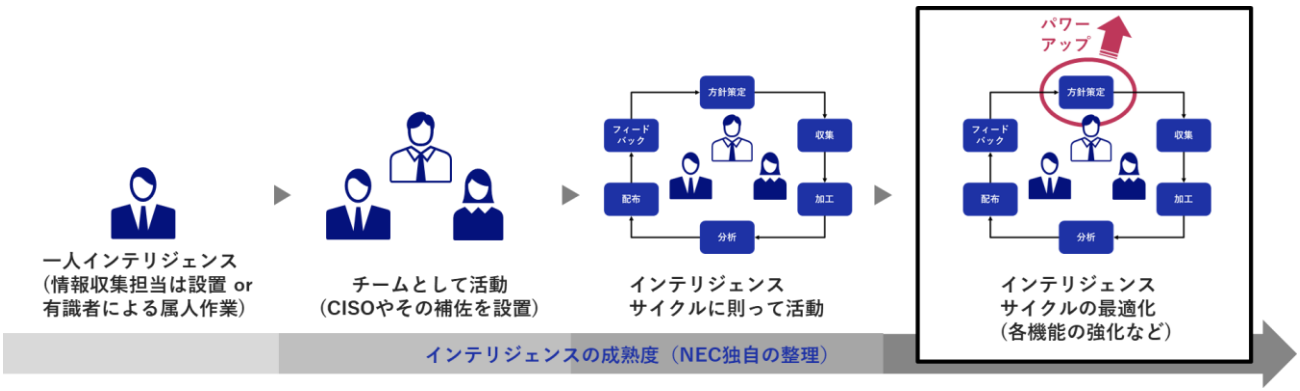
ここでは紹介しませんが、各パートを支援するためのツールや考え方は多数存在しており、自動化も進んでいます。できる限り手作業を削減することで、必要なプロフェッショナルの人数も減らすことが出来ますし、平準化も進めることが出来ます。後述するように、サイクルの各パート強化はより成熟度の高い活動ですが、より業務を効率化する手段として検討いただければと思います。

脅威インテリジェンスの成熟度

脅威インテリジェンスの成熟度はどのように判定すればよいのでしょうか。マニュアル整備や自動化など複数の考え方が存在していますが、ここでは前述したチームやサイクルに則った活動が行えているか、という軸で考えてみたいと思います。

最初の段階は、情報収集担当は設置しているが、有識者による属人作業になってしまっているような**一人インテリジェンス**が想定されます。この段階では、情報の収集や分析、報告まで一人で対応するため、異なる立場にカスタムした情報の提供やサイクルに則った活動は困難です。
また、この担当者が情報を見落としてしまうと、それを拾い上げることもできません。

次の段階として、人数を増やして**チームとして活動している状態**が想定されます。この状態になれば1 人インテリジェンスの問題点の多くは改善されますが、まだサイクルに則った活動が出来ていないため、情報の取り扱い方やフォーマットなどに不備があります。このため、属人化はまだ解消されておらず、メンバー交代による負荷が高い状態が続いています。



3 つ目の段階として、**チームがインテリジェンスサイクルに則った活動が出来ている状態**が想定されます。この状態に達すると、業務のプロセスを可視化しやすくなるため、平準化やマニュアル化の効果が高くなり、メンバー交代や教育の負荷が改善されます。また、すでに一連のプロセスが完成しているので、他業務への応用など追加の業務にも対応しやすくなります。この段階に達すれば、脅威インテリジェンス活用は達成出来ていると考えてよいでしょう。

最終段階として、**インテリジェンスサイクルの各パートをより最適化していく状態**が想定されます。業務のさらなる効率化に加え、新たなビジネス領域の考察など、省人化によるプロフェッショナル能力の平準化とその恩恵を受けることが可能となります。

このように、インテリジェンスの成熟度はチームやインテリジェンスサイクル活動の状況で判定することができます。

ただし、日本の企業の多くが 1 つ目または 2 つ目の段階にあると推測され、3 つ目の段階に達しているチームはまだ小数なのが現実でしょう。実際、日本における脅威インテリジェンスのセミナー等は、そもそも脅威インテリジェンスとは何か、から始まることも多く、チームやサイクルを活用した活動を本題としたものは、それほど多くない印象を受けます。この点、日本はまだ遅れている分野のため、欧米の先端企業とははっきりとした差があるのが現状です。

NEC における脅威インテリジェンス活用

NEC においては、自社グループのサイバーセキュリティ体制向上に脅威インテリジェンスを活用しており、CISO を最終意思決定者として情報の収集・分析を行っています。また、自社環境だけでなく、お客様に納入した製品やサービスへの影響も考慮した活用を行っており、NEC の提供する価値が毀損されるような、経営上のリスクに対処しています。

また、お客様に対しての脅威インテリジェンス提供も行っており、内外における活用を今後も強化していく方針です。

まずは簡単なことから始めよう

とは言え、これまで脅威インテリジェンスに触れていないかった人物や企業がいきなりチームを構成してサイクルを回し始めるのは非常に困難です。一体何から始めればよいのでしょうか。

脅威インテリジェンスの本質は、**サイバー攻撃のトレンド、注意すべき手法や脆弱性といった脅威情報を収集し、セキュリティ対策向上に役立つよう分析・提供する**ことです。この情報収集や分析に約立つ簡単なことからまずは始めてみましょう。それは、一般のセキュリティニュースを追いかけてみることです。大手メディアやネットニュースでも構いません。サイバー空間においてどんなことが起こっているのかを把握することが最も大切です。セキュリティ運用において、どのような対策を優先していけばよいのかの適切な判断、いざ攻撃が発生したときの迅速な判断につながります。

これは、水泳を始めるプロセスにも少し似ています。ある程度の情報に触れて体が慣れたら、その質や分量を考慮したり、専門のチームを作成したりと、段階を進めてみるのがよいでしょう。

参考文献

[1] A Definition of Intelligence
https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-2-no-4/a-definition-of-intelligence/
[2] 内閣の情報機関としての内閣情報調査室の役割について
https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/yakuwari.html
[3] 脅威インテリジェンス
https://www.vmware.com/jp/topics/glossary/content/threat-intelligence.html
[4] 脅威インテリジェンスとは【用語集詳細】
https://www.sompocybersecurity.com/column/glossary/threat-intelligence-definition
[5] THREAT INTELLIGENCE サイバー脅威インテリジェンスとは
https://www.crowdstrike.jp/cybersecurity-101/threat-intelligence/