ホワイトペーパー

脅威インテリジェンス成熟度モデルを組織に適用する

EclecticIQの脅威インテリジェンス成熟度モデルは、サイバー脅威インテリジェンスに不可欠な8つの異なる領域で組織の機能を評価する方法を提供し、運用全体の不確実性とリスクの軽減を実現します。

目次

要約

企業や政府がサイバー脅威を意識するようになり、脅威の実体に合わせて対処できる脅威インテリジェンスの実践というビジネスニーズを優先するようになった。市場で提供される脅威インテリジェンス製品の多様性が増すなかで、新たな課題は、人、プロセス、テクノロジーへの投資決定をどこから始め、どのように導くかを判断することである。

Forrester Research社の報告によると、大企業の77%が、サイバー脅威インテリジェンス（CTI）の各機能の確立や改善について、優先度が高いか重要だと考えている[1]。

このホワイトペーパーでは、脅威インテリジェンスの取り組みの成熟度を評価し、将来の投資を導くためのフレームワークを提供する。

効果的な脅威インテリジェンスであるためには、リソースと予算に関して常に存在するビジネス上の制約の範囲内にとどまりながら、利害関係者の情報ニーズを脅威の状況の現実に合わせなければならない。この環境における成功の重要要素は、明確な内部のニーズに合わせた構築、主要利害関係者との連携、目的に適した人材、プロセス、およびテクノロジーの構築である。

1）Forrester Research社Rick Holland「The State of the Cyberthreat Intelligence Market 2015年6月23日

脅威インテリジェンスとは？

インテリジェンスの本質は不確実性を減らすことにある。不確実性によってビジネスの達成目標に矛盾が生じる場合、インテリジェンスはビジネスリスクの軽減に役立つ。サイバーインテリジェンスは、電子犯罪、ハクティビズム、テロ、スパイなどの脅威に対処する際の不確実性を軽減する。

このようにしてサイバーリスクを管理するには、サイバー攻撃者が隠そうとする情報が必要となる。インテリジェンスアナリストは、入手できる情報を収集して分析する直接的手段と間接的手段によって、この隠された情報を明らかにしなければならない。インテリジェンスアナリストは、事実を確かめてから、意思決定のための正確で信頼性が高く有効な推論を打ち立てて前進する。結果として得られる結論と予測は、
セキュリティ運用、インシデント対応、脆弱性管理、リスク管理、および取締役会レベルの意思決定の運用計画に大いに役立つ。

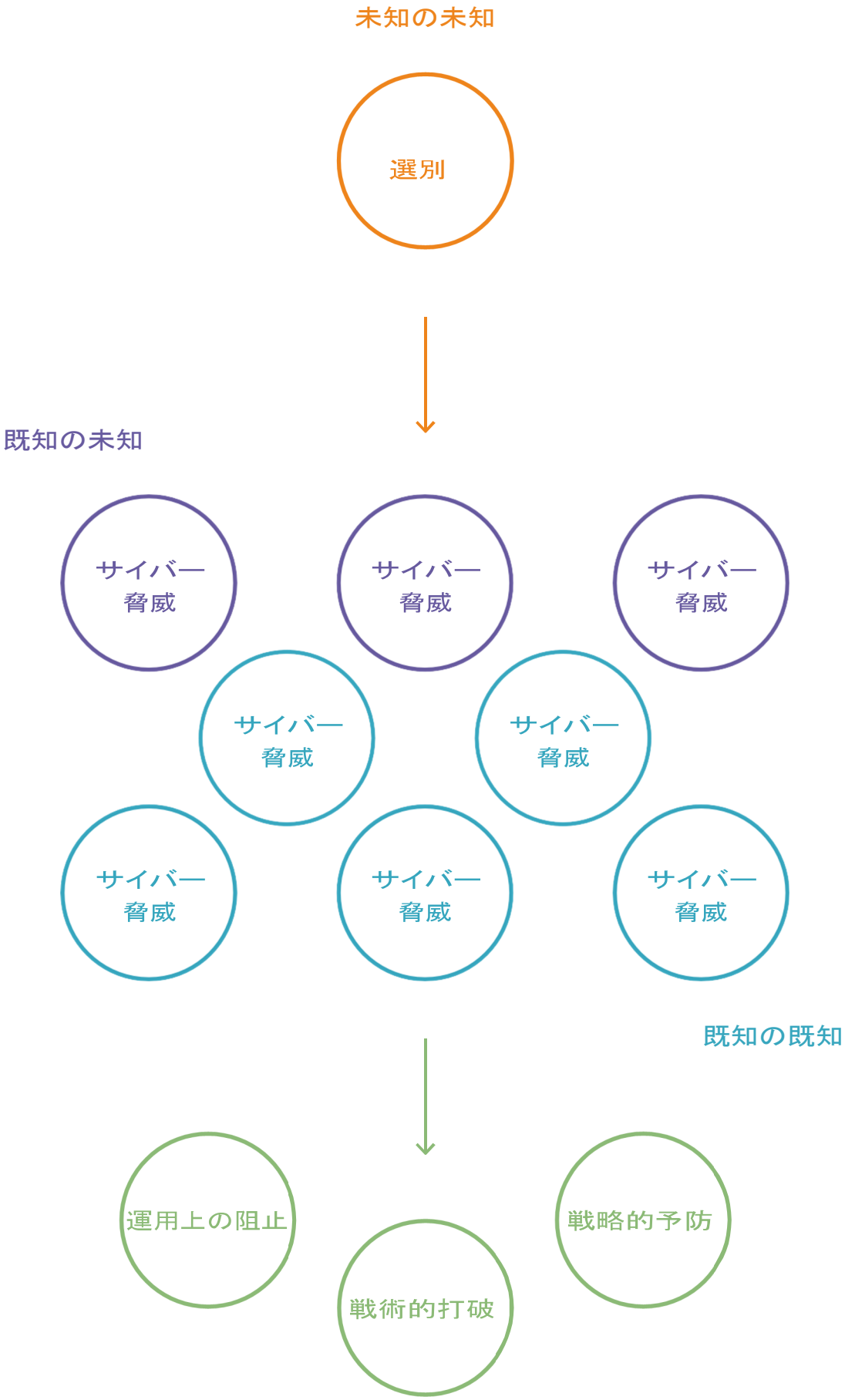
「インテリジェンスは常に、結果を変えるために行動できる情報と定義される。」

–英国政府国家インフラ保護センター

サイバー脅威インテリジェンスは、従来のインテリジェンス（諜報活動）の手法に従って、サイバー脅威に対する運用上、戦術上、および戦略上の対応に焦点を当てる。

脅威インテリジェンスのプロセスを説明する一般的な方法に、「既知」と「未知」の管理がある。最も危険なのは、私たちが知らない、または理解していない「未知の未知」の脅威である。したがって、インテリジェンスの最初のステップは、脅威の存在を発見することで、
これが「未知の既知」である。次にこれらを深く理解して「既知の既知」とするように努め、適切な措置を取れるようにする。このようなサイバー脅威の識別、理解、および措置の連続プロセスは、脅威インテリジェンスのプロセスをおおまかに説明したものである。

実用レベルでは、インテリジェンスは組織に対して、サイバー脅威を構成する、変化する敵対者のあらゆる機能と活動を防止、延期、または必要ならば打破する最善の方法を知らせる。インテリジェンス組織は、利用可能なリソースにおいて最も効果的な方法で、脅威に団結して対抗する方法を組織に知らせるために、変化する脅威の状況を絶えず評価する必要がある。


未知の未知
選別
既知の未知
サイバー脅威
サイバー脅威
サイバー脅威
サイバー脅威
サイバー脅威
サイバー脅威
サイバー脅威
サイバー脅威
既知の既知
運用上の阻止
戦術的打破
戦略的予防

脅威インテリジェンスの現状と、目標とする成熟度の評価モデル

EclecticIQの成熟度モデルは、ロバートM.クラーク(『IntelligenceAnalysis:A Target-Centric Approach』の著者)、脅威インテリジェンスに関するCPNI / CERT-UKの出版物、およびiSIGHTパートナーの脅威インテリジェンス成熟度モデルから着想を得ている。

組織のインテリジェンスに対するEclecticIQの成熟度モデルは、個別に8機能の成熟度を測定する5段階の評価尺度を規定する。

全般的に、このモデルは次の3つの広い領域で脅威インテリジェンスの成熟度を測定する。

1 ビジネスと脅威の現実との整合

脅威インテリジェンスへの投資が、ビジネスニーズ、リソースの制約、および脅威の状況との間でどの程度バランスが取れているかを測定する。成熟度モデルに関連する機能は次のとおりである。

- 利害関係者管理
- 要件管理
- 意識

2 理解する能力

分析機能によって、脅威インテリジェンスチームが、内部の利害関係者の情報ニーズに応じてサイバー脅威をどの程度理解できるようになるかを測定する。主な機能は、技術的指標を認定したり、組織や同等のエンティティが直面している主要なサイバー脅威を戦略的に追跡したりすることである。成熟度モデルに関連する機能は次のとおりである。

- ソース管理
- 分析と成果
- 共有

3 理解したことを制御/実施する能力

脅威を理解して制御する組織の能力を測定する。サイバー脅威を打ち負かし、妨げ、防止する組織の能力の調整責任を負うセキュリティ利害関係者が、確実に措置を取るようにする。主な機能としては挙げられるのは、関連する技術的指標、検出および防止システムの計測、および、変化する脅威の状況しだいで適切な投資とビジネス上の意思決定をどのように進めるかについてのビジネス利害関係者の関与である。成熟度モデルに関連する機能は次のとおりである。

- 配布
- 統合

成熟度モデル

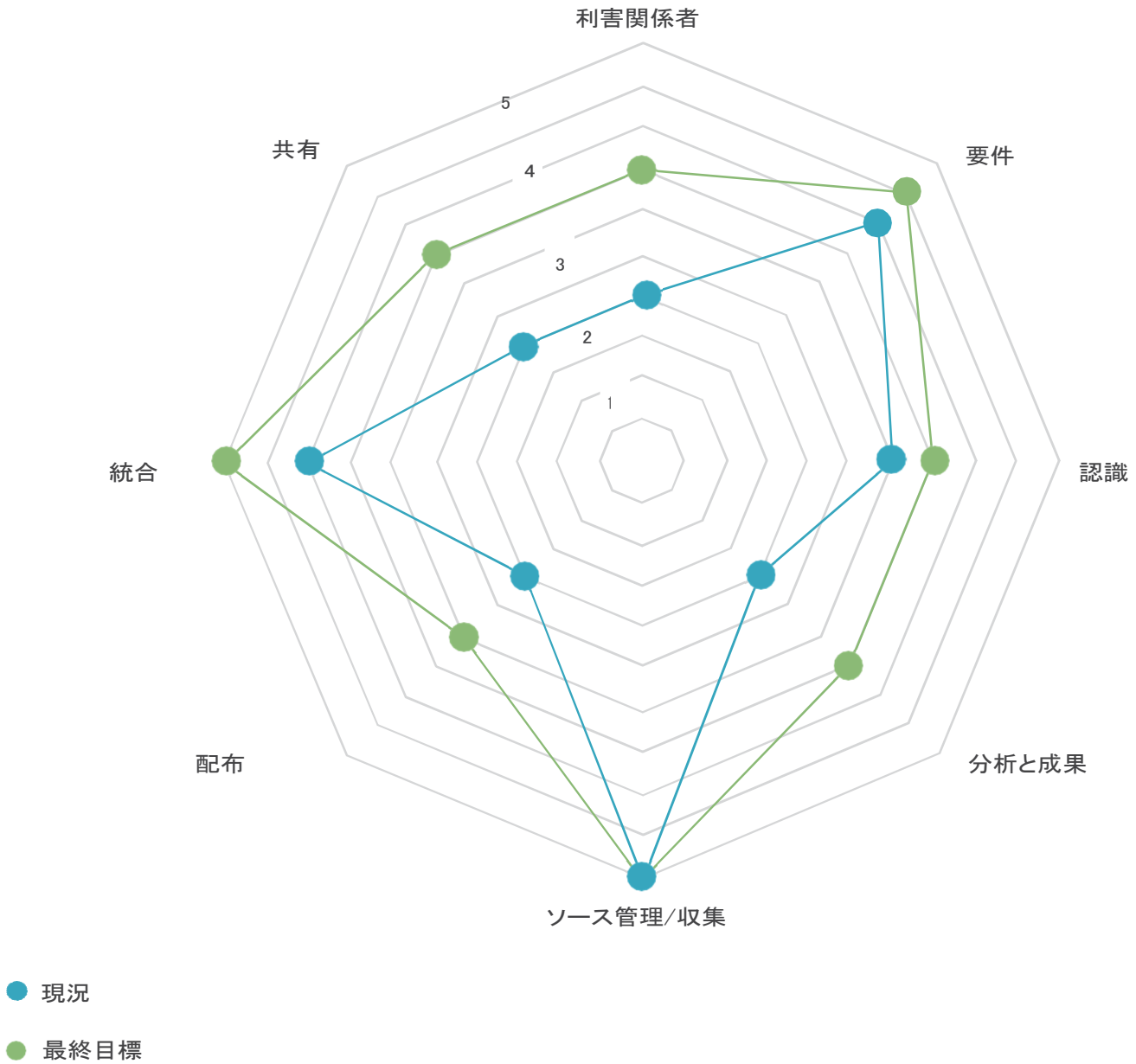
機能	ステージ1	ステージ2
利害関係者管理	脅威インテリジェンスとは何か、そしてそれに責任を負う事業機能についてほとんど、あるいはまったく認識していない	脅威インテリジェンスが利害関係者に影響することがあるが、ほとんど考慮されず、対処もされない
要件管理	要件がないか、または要件が利害関係者の意見に基づいていない	非公式または非定期のタッチポイントによる利害関係者のニーズの一般的な理解
認識	脅威を認識していない	一般的に（そして公に）議論されている脅威を認識している
ソース管理/収集 • オープンソース • 商用 • コミュニティ	• 無しまたは臨時	• ソース取得に関する不定期な意思決定 • 主にオープンソースか、または評判不明のソース
分析と成果	分析せず、ソースのインテリジェンスが直接配布または統合される	**認定** 受け取ったインテリジェンスは、自動または手動で強化され認定される
配布	インテリジェンスはソースから直接配布される	配布したインテリジェンスには、受け取る利害関係者との関連性を示す十分なコンテキストと信頼性の言明がある
統合	ソースから得たインテリジェンスは、セキュリティコントロールシステムとワークフローシステムに統合されない	インテリジェンスの指標は、セキュリティコントロールとワークフローコントロールに不定期で統合される
共有	共有しない	類似組織の個人と共有する

ステージ3	ステージ4	ステージ5
脅威インテリジェンスは利害関係者に定期的に送られ、常に考慮され、対処されている	脅威インテリジェンスは標準的なインプットとして取り込まれ、サイバー関連の課題に関する意思決定に定期的に利用されている	脅威インテリジェンスは標準的なインプットとして取り込まれ、主要な意思決定には積極的に助言が求められる
利害関係者のニーズを理解するための定期的で安定したタッチポイントがある	利害関係者のニーズを理解するための定期的で安定したタッチポイントがあり、受け取るインテリジェンスに臨時のフィードバックがある	利害関係者のニーズを理解するための定期的で安定したタッチポイントがあり、受け取るインテリジェンスに定期的で継続的なフィードバックがある
脅威アクターの能力や動機の傾向など、脅威についていくらかの認識がある	一般的な脅威の傾向について深い見識があり、アクターの能力や動機、執拗さなどをよく理解している	脅威アクターの能力や動機、執拗さや、一般的でなく的を絞った脅威も含めて、最も関連性のある脅威を認識している
• ソースの取得と再調整に関する定期的な意思決定 • 幅広くほとんどが評判の高い情報源	• ソースを取得、評価、再調整する調達手順が明らか • 多くの信頼できる有名な情報源があり、独自の分析機能を定期的に収集	• ソースを取得、評価、再調整する調達手順が明らか • 信頼できる情報源の大規模なセットに、有名でニッチな情報源も含まれ、独自の収集機能や分析機能を安定的に供給
IOC管理 技術的指標と観察可能なコンポーネントが品質管理とともに培われている	**ケース管理** しきい値基準が明らかなため、具体的な脅威を深く理解するためには、いつ臨時のケースごとの共同調査をするのがインテリジェンスに妥当であるか定められている	**脅威管理** 脅威は本部の記録で事前に戦略的に管理されている。既知の脅威を理解するために継続的な調査を事前に行う
配布インテリジェンスの対象は特定の利害関係者である	インテリジェンスは、主要な仮説を検証してテストするために、利害関係者と協力して作成される。インテリジェンスの成果は関連する利害関係者に直接送られる	利害関係者は、インテリジェンスレポートのタイミング、配布方法、および主題を完全に制御でき、必要時には関連トピックの対象となるインテリジェンスを受け取る
インテリジェンスの指標は、セキュリティコントロールとワークフローコントロールに定期的に統合される	インテリジェンスの指標は、コンテキスト、優先度、特定の対処方針に関する情報とともに、セキュリティコントロールとワークフローコントロールに統合される	インテリジェンスの指標は、コンテキスト、優先度、特定の対処方針に関する情報、ならびに周辺状況の分析とインテリジェンスへの明確で分かりやすい掘り下げとともに、セキュリティコントロールとワークフローコントロールに統合される
個人や中度の機密グループとの準定期会議を通じて共有	組織の関係を介した、または機密性の高い信頼できるグループ内での臨時共有	組織の関係を介した、または機密性の高い信頼できるグループ内での常時共有

成熟度モデルの利用

組織の脅威インテリジェンスの構築または改善計画を立てる前に、明らかにしておくべきことがある。最初に現地点を把握し、次に合理的な出発点として1年～1年半後までに到達していたい地点を設定することが重要である。各利害関係者は、インテリジェンス機能で達成したい成熟度のレベルについて合意する必要がある。
世界中の脅威インテリジェンスチームと協力した経験から推奨するのは、各機能の成熟度を、5段階評価中2点以下で毎年上げるように目指すことである。改善後のレベルでの運用に十分な時間を確保するために、結果を測定する時間と、それに応じて再調整し、計画を立てる時間を見越しておく。

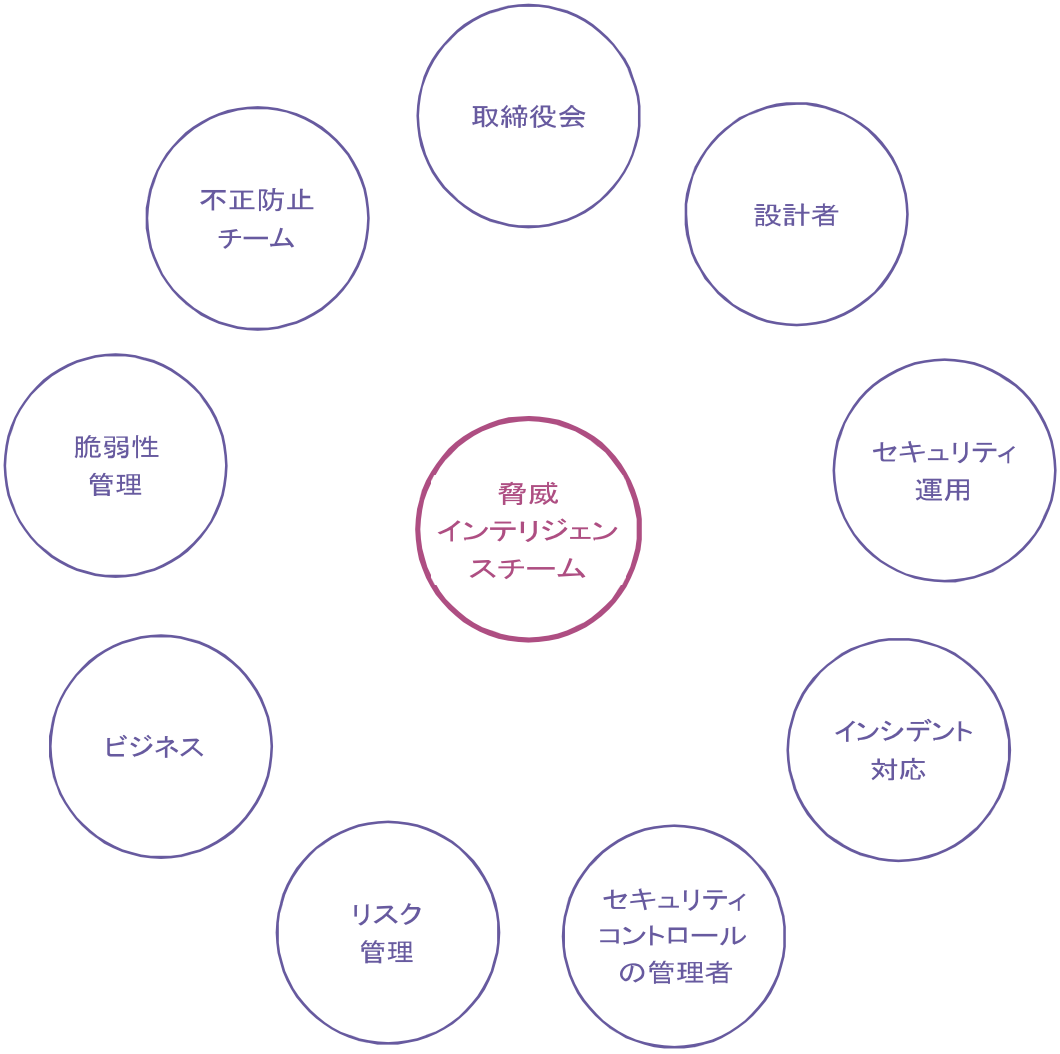
望ましい状態を基準として現況を可視化できるようにグラフ化する。



企業の脅威インテリジェンス機能を構築するベストプラクティス

1 利害関係者向けの構築

脅威インテリジェンスから事業価値を生み出すには、組織内の主要な利害関係者の情報ニーズと要件を理解する能力が必要となる。これらの利害関係者が最終的に、サイバー脅威の抑止、打破、防止の責任を負う。最初に、主要な利害関係者と、これが好むインテリジェンス利用形態と周期、必要となる主なインテリジェンス要件を理解する。



利害関係者とその要件は一般的に次のようなものがある。

- **経営幹部と意思決定者**は、組織が主要な脅威にどのようにさらされているかを理解する必要がある。
- **IT設計者およびその他のIT意思決定者**は、サイバー脅威の現実を念頭に置くITインフラストラクチャの構成に見合うように、一般的なITセキュリティのシステムおよび概念に対する主要な脅威を、常に最新の状況で理解する必要がある。
- **セキュリティオペレーションセンター（SOC）**は、主要な脅威に関連する技術的な構造化指標と警告信号を要求する。
  通常は利用可能になり次第、機械で読み取り可能な構造化フォーマットで要求する。
- **インシデント対応および運用（IR）チーム**が頻繁に要求するのは、臨時で特注のインテリジェンスである。これらは注目すべきITセキュリティインシデントの発生中および発生後のフォレンジック時に発見された侵害のツール、手口、該当キャンペーン、実行犯の意図と属性、その他の発見された技術的指標の状況に関係する。
- **セキュリティコントロールの管理者**は、コントロール構成を適応させて脅威を阻止するために、敵対者の戦術、ツール、および手法に関する情報を要求する。
- **リスク管理**では、主な
  事業達成目標をめぐる不確実性の見込みを評価するために、組織が直面している脅威に関するビジネスリスクを完全に理解する必要がある。
- **ビジネスの利害関係者**には、主要な脅威と、それぞれの責任範囲における事業運営への潜在的影響について、定期的な情報更新が必要である。
- **脆弱性管理チーム**が要求するのは、新興で影響力大のITシステムの脆弱性と既知の悪用ベクトルを説明した、インテリジェンスの文書である。
- **不正防止チーム**は、サイバー脅威に関する情報を使用して、電子バンキングや小売など、組織の顧客向けプラットフォームでの潜在的な不正行為を検出して対応する。

2 サイバー脅威に対する組織の認識を加速化

脅威インテリジェンスを適用できる範囲は幅広く、即時対処と長期計画の両方が求められる運用上、戦術上、および戦略上の諸問題に及ぶ。利害関係者は、脅威インテリジェンスの適用範囲と、それが変化する脅威に対する危険の制御にどのように役立つかを認識しなければならない。脅威管理機能の実施を成功させるには、意思決定者による賛同が必要であり、投資に対する彼らの意欲は、内部の利害関係者が脅威インテリジェンスの価値をどれだけよく理解しているかに比例する。

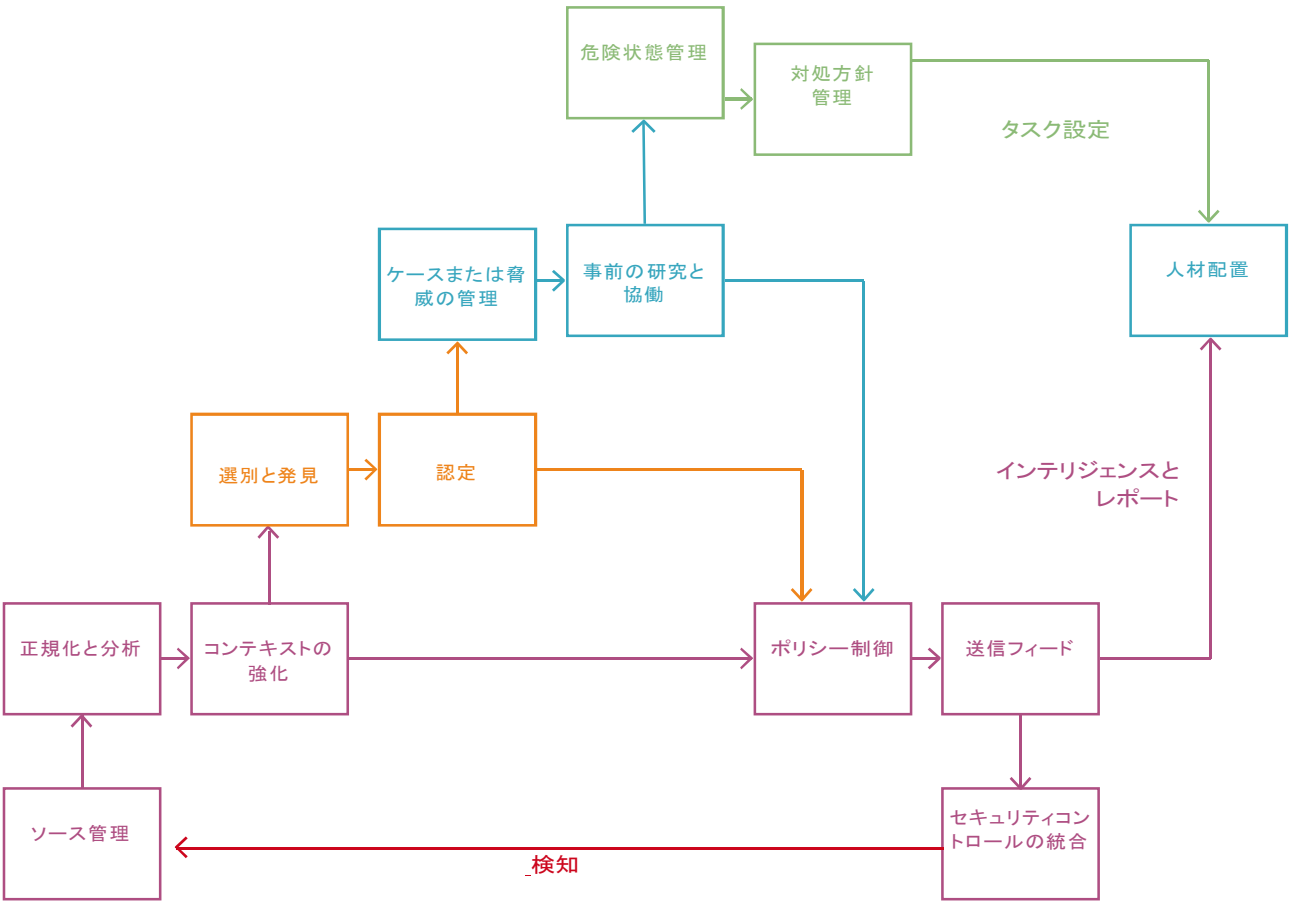
3 組織の賛同を得る

すべての利害関係者は、共有ビジョン、段階的な展開のタイミング、既知の制約、期待される測定可能な結果など、脅威インテリジェンスの計画に満足しているものとする。プロジェクトを成功させる秘訣は、タイミング、リソース、その他の要因のいずれにしても、どの程度、どのようなペースとステップで、どのような事業上の制約において達成したいかという理解を深めることである。大小にかかわらず、組織に対して実現可能な約束をする。

4 ITセキュリティとは別の脅威管理の実践を明確化

脅威管理の実践には脅威インテリジェンスプロセスを導入する。そのような実践をうまく計画、導入、運用するには、特定のインテリジェンス能力が要求される。

脅威インテリジェンスはITセキュリティに密接に関係しているが、明確な境界線が引かれた別の機能である。さらに別の脅威管理の実施によって、脅威インテリジェンスフィードの取得と分析を含む脅威インテリジェンスのプロセスや手順の設計、計画、および導入に必要な関連機能の可用性を確保できる。
ITセキュリティチームと脅威管理チームは、既存の新しいプロセスと手順への変更を展開する際に、バランスの取れた機能横断的なチームとして協力するものとする。あるいは、それぞれのチームが別個の責任を持つものとする。



5 分析と作成の機能を強化

脅威インテリジェンスでは、分析と作成がサイバー脅威を理解する上で重要な要素となる。

分析と作成に関する脅威インテリジェンスのベストプラクティスは、成熟度のいくつかのレベルで確認できる。組織は、レベルを上げながら機能を向上させるように努めるものとする。

- **認定**は、自動化されたシステムと脅威アナリストがソースから受け取ったインテリジェンスを認可して、組織との関連性を理解し、
  確信と近接性を判断し、対処を定義することを、確実に行う事後対応プロセスである。

- **IOC管理**によってさらに、組織に対してサイバー脅威が有効であると示す該当の技術的警告信号
  （侵害指標（IOC）、攻撃指標（IOA）、または観察可能特性と呼ぶことが多い）が十分な質を備え、組織の検出、防止、および対応機能に適することが保証される。

- **ケース管理**は、受け取ったインテリジェンスに対してしきい値基準または関連性基準を適用して、さらなる調査と協力を保証する潜在的に価値のあるデータポイントを明らかにする。
  この「いいとこ取り」はアナリストが問題を深く理解するように促し、有意義な収集分析を行いやすくする。さらに、自動化されたケース管理によって、アナリストの能力が向上し、より長い期間にわたって脅威を評価できる。個々のケースは通常、短期や中期にわたる。したがって、受け取るインテリジェンスは通常、より広範な傾向や一般的な脅威を代表するものではない。ケース管理は、履歴データを現在の分析に組み込むことにより、アナリストにさらに包括的な視点を与える。

- **脅威管理**はケース管理の上に構築される。これには、キャンペーン、攻撃者、その他の分析トピックと構成など、一般的に発生する脅威カテゴリーの事前追跡と管理をともなう。
  拡張データセットを使用すると、組織は常に受信インテリジェンスを評価して、関連する「既知の未知」を発見し、事前調査によってそれらを「既知の既知」に変えることができる。 脅威管理は、サイバー脅威の全体像を提供し、脅威インテリジェンス機能がもたらす最高レベルの成熟度と複雑な分析の中でランク付けを行う。

- **危険状態管理**は新しいベストプラクティスで、組織が現在理解しているサイバー脅威を正常に制御した程度を測定する。
  危険状態管理プロセスは、既知の情報と、その情報を行動に移せる組織の能力との間のギャップを測定する。たとえば、組織は、それを元に利害関係者が行動に移せないようなさまざまな技術的指標を受け取る場合がある。検出システムと防止システムには、脅威インテリジェンスチームが管理する指標への互換性が必要であり、その逆も同様である。危険状態管理は、このような隠れた弱みを明らかにして軽減する。

6 脅威インテリジェンスプラットフォームの技術による立ち上げ

脅威インテリジェンスプラットフォーム（TIP）の各技術は、サイバー脅威インテリジェンス（CTI）の各機能の導入や改善の一般的課題に対応するために登場した。TIPによって、成功した脅威管理業務の一環として、コアワークフローとプロセスを立ち上げる簡単な方法が提供される。

組織のTIPを選択するときは、ワークフロー機能が利用できることを確認する。そうすることで、脅威インテリジェンスの集中化と統合、およびその後のインテリジェンスデータの分析、作成、配布、セキュリティコントロールへの統合、調整、その他の各主要プロセスがTIPによって確実に実現できる。

7 技術的指標をセキュリティコントロールに統合

組織は通常、インテリジェンスに関連する技術的指標を用いて、セキュリティコントロールの検出、防止、および対応機能を向上させる。これによって、脅威の検出と修復の応答時間が改善される。

インテリジェンスを組み込んだセキュリティコントロールには、次のものが含まれる（最も一般的な機能から最も一般的でない機能の順に挙げる）。

- ITインフラストラクチャおよびネットワークイベントからの履歴および現在のログ情報を保持する**セキュリティ情報イベント管理（SIEM）システム。**たとえば、Splunk、HP ArcSIGHT、IBM QRadar、Logrythmである。
- SIEMシステムと同様の情報を保持するHadoop、Elastic、Cassandraなどの**ビッグデータクラスタ。**通常、このデータの新しい適用範囲とサイズを取り扱うため社内で構築される。
- 既知の脅威指標に照らしてネットワークまたはホストアクティビティの実体を評価する**侵入またはエンドポイントの検出および防止システム**
- 検出やインシデント操作のシナリオを自動化する**セキュリティの自動化および調整**のツール利用

EclecticIQについて

EclecticIQは、応用サイバーインテリジェンステクノロジーのプロバイダーであり、企業のセキュリティプログラムや政府機関が脅威インテリジェンスを立ち上げできるようにします。アナリストが脅威の現実に対して制御を取り戻し、それに応じて危険度を軽減できるようにします。

EclecticIQが目指すのは、サイバー攻撃者との戦いにおけるバランスの回復です。その主力製品であるEclecticIQ脅威インテリジェンスプラットフォームは、セキュリティ情報交換の運用化を実現し、アナリスト共同ワークフローを強化し、確実にサイバー脅威インテリジェンスの検出、防止、および対応機能をタイムリーに統合します。

EclecticIQは、オランダのアムステルダムに本社を置く株式非公開企業で、ロンドンにオフィスを構えています。

2015年EU IPACSOサイバーセキュリティ賞を受賞し、NATO NCIエージェンシーセキュリティインキュベーターのパートナーです。

EclecticIQの詳細については、www.eclecticiq.comをご覧ください。

販売や製品のデモについては、sales@eclecticiq.comにお問い合わせください。または、電話+ 31（0）20 737 1063におかけください。

Twitterは@eclecticiqをフォローしてください。