脅威インテリジェンスガイドライン　～全体概要～

ガイドラインの背景・目的

- **背景**
  - ✓ 産業活動におけるIT・OTシステムの重要性が増大し、同時にサイバー攻撃の脅威が高まっている。
  - ✓ フレームワークや法規制をベースとした網羅的な成熟度評価とセキュリティ対策では現実で発生している脅威にプロアクティブな対応が困難であり、脅威をベースとしたアプローチである**脅威インテリジェンスが注目されている。**
  - ✓ 脅威インテリジェンスという概念は取り扱う組織によって定義・目的が異なるため、具体的な実施内容や事例の取り扱いが少なく、導入の障壁があることが分かっている。
- **目的**
  - ✓ 本ガイドラインにて脅威インテリジェンスの具体的な導入・運用方法とケーススタディを紹介し、**脅威インテリジェンスの普及と組織のセキュリティ強化**につなげる。

対象読者

- 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と組織
  - ✓ 脅威インテリジェンスを知らない組織
  - ✓ 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
- **活用方法**
  - ✓ 経営層への脅威インテリジェンスについての説明、提案
  - ✓ 脅威インテリジェンス運用部門への具体的な実施手順の提供

脅威インテリジェンスの意義

- **セキュリティ対応の優先順位付け**
  - ✓ 脅威を分析し、自組織への影響と攻撃可能性、発生頻度、対策状況を確認することで**脅威ベースのリスクアセスメントが可能**となり、対応優先度が分かる。
- **プロアクティブなセキュリティ対応**
  - ✓ **タイムリーな攻撃観測情報の収集・分析**により、自組織に攻撃が到達する前に準備・対応することが可能。
- **インシデントレスポンス能力の向上**
  - ✓ インシデント発生時の攻撃の痕跡をもとに、関連する脅威情報を分析し、**痕跡以外の侵害の有無を確認**できる。

脅威インテリジェンスの概要[1]

定義

※定義は取り扱う組織、媒体によって異なる

- **脅威インテリジェンス**
  - ✓ 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。
- **脅威**
  - ✓ 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。
  - ✓ 意図×機会×能力の３要素から構成される。
    - 意図：脅威アクターの動機
    - 機会：攻撃実行を可能にする環境、条件
    - 能力：攻撃を実現するためのリソース
- **インテリジェンス**
  - ✓ 収集した脅威情報をベースに、リスクアセスメントの実施結果などを加えて自組織の活動に活用可能なコンテキスト（付帯情報）を追加したもの

インテリジェンスの分類

- **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
    - （利用者）経営層、セキュリティ責任者
    - （アウトプット）経営層向けレポートなど
- **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
    - （利用者）セキュリティ責任者、SIRT部門
    - （アウトプット）攻撃シナリオなど
- **戦術的インテリジェンス**
  - ✓ 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
    - （利用者）SOC
    - （アウトプット）IoC情報など

実施ライフサイクル

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。
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。
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。
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。
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。

脅威インテリジェンスの背景・動向

- 組織の脅威となる環境や技術背景は常に変化を続けており、観測し対処するために脅威インテリジェンス技術が有効である。国内組織においても、多方面から見た様々な要因から注目が高まっている。

政治的要因（Political）

- **米中間の技術デカップリング**[2]

✓ 両国は産業技術戦略において互いの影響を排除した、それぞれ独立的な政策をとっている。

✓ 米国と中国を隔てるのサプライチェーン二極化の中で、日本はその両方から影響を受ける境遇に位置しており、互いへの牽制のためのサイバー攻撃を受けることが考えられる。

✓ 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。

経済的要因（Economic）

- **ランサムウェアの身代金、復旧額の増加**

✓ 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、国家的組織や大規模な犯罪組織のような、高度で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て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。

社会的要因（Sociological）

- **脅威インテリジェンスの導入状況**[3]

✓ 脅威インテリジェンスは、世界中で事業規模に関わらず活用されている。

✓ 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名未満の小規模組織が28%を占めているというSANSの調査結果もある。

✓ 本年我々が行った国内組織向けのアンケート調査では、**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への注目度が高まっていることが伺える。

技術的要因（Technological）

- **IT技術革新に伴う脅威の複雑化**[4]

✓ 生成AIやローコードプログラムなどの技術革新を背景に脅威の多様化が進んでいるが、それらの脅威に対処する技術が追い付いていない。

✓ 守るべき資産の数も増加しており、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、**重要資産への対応すべき脅威にフォーカスを充てて**自組織でのセキュリティ戦略へ適用することが重要である。

法的要因（Legal）

- **セキュリティクリアランス制度**[5]

✓ 政府の安全保障上重要な情報にアクセスする者に対して、調査を実施し信頼性を確認した上でアクセスを認める制度のことをセキュリティクリアランス制度と呼ぶ。

✓ 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。制度の具体的内容は本書執筆時点では決定していないが、**今後クリアランス認定を活用した脅威情報の共有が実施されると想定**。

✓ 国家をまたいだ共同研究はもちろん、脅威情報の共有においても効力を発揮することが期待されており、脅威インテリジェンスが業界全体のセキュリティを強化する効果が期待されている。

環境的要因（Environmental）

- **脅威アクターの動向と攻撃手口の変化**

✓ 検知が難しい攻撃が増加しており、脅威アクターとその攻撃手法を把握し、対策を講じる必要性が高まっている.

✓ 匿名性の高い環境が攻撃者が追跡されるリスクを低減し、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ている。

✓ 攻撃観測数の多い脅威アクターは変遷し続けている。**現在注目すべき脅威アクターや攻撃手法、および環境の変化を迅速に把握する必要がある**。

脅威インテリジェンスの課題・留意事項

国際的な課題

課題①：戦術的インテリジェンス（IoCの検知・遮断）に注目されがち

✓ 戦術インテリジェンス（リアルタイムの脅威に対応）を活用する組織が多いが、戦略的・運用インテリジェンス（脅威インテリジェンスを用いたセキュリティ戦略策定やペネトレーションテストなど）は**定義に関する明確なコンセンサスがないなどの障壁がある**。戦略的・運用インテリジェンスの実績や評価、活用ケースを展開していく必要がある。

課題②：脅威インテリジェンス分野における専任人材の不足

✓ 脅威インテリジェンスを有効活用するには専任人材の配置が望ましいが、脅威インテリジェンス分野が**未だ発展途上の分野である**と同時にセキュリティの中でも**専門性が高い領域である**ため、人材が不足している実態がある。

日本固有の課題

課題①：業界単位や組織での活用そのものが成熟していない

✓ 業界、公的機関においては脅威インテリジェンスの重要性が注目され始めている。事業会社では**大手事業会社が取り組みを始めてる段階であり、かつ専任人材も不足しており**、各組織手探りで進めている状況である。

課題②：インシデント情報などの共有を拒む文化的な障壁

✓ 米国などと比較すると**インシデント情報の共有・報告義務化が進んでいない**状況であり、かつインシデントの報告・公表が**自組織のセキュリティ対策不足を露呈するという考えが強く**、脅威情報の共有に課題がある。情報共有の概念やポリシーを定め、報告・公表内容を分類し、浸透させていく必要がある。

留意事項

留意事項①：脅威インテリジェンスは取り組み自体を意味するもので、特定のツールやサービスを指すものではない

✓ 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。**脅威インテリジェンスの開始時点でツールやサービスの選定を実施することは推奨されない**。

留意事項②：脅威アクターを特定することやIoCを遮断することのみが脅威インテリジェンスではない

✓ IoCを用いて、検知・遮断することもインシデント予防の短期的対策として有効である。また、脅威アクターの分析も脅威自体の防止観点において重要ではあるが事業会社として分析することは困難である。事業会社においては、フレームワークを用いた成熟度評価だけではなく、**脅威動向をベースにセキュリティ戦略を検討する第一歩として脅威インテリジェンスという概念を導入すべき**である。

留意事項③：脅威インテリジェンスを活用するうえで、一定のセキュリティ成熟度が要求される

✓ どの組織においても脅威インテリジェンスが活用できるものではなく、収集した脅威情報を**自組織の状況から分析するリソース（内部/外部）**や組織状況を確認するための**分析基盤**、セキュリティ戦略に**セキュリティリスク項目を含める組織体制**などが必要となる

留意事項④：組織単独で実施することは困難である

✓ 脅威インテリジェンスは、信頼できるグループで情報共有することでその効果を発揮することができる。組織単独での活用は困難であり、**公的機関との連携や組織間でのインシデントの情報共有を実施することで、自組織に影響ある脅威に対してプロアクティブに対応することができる**。

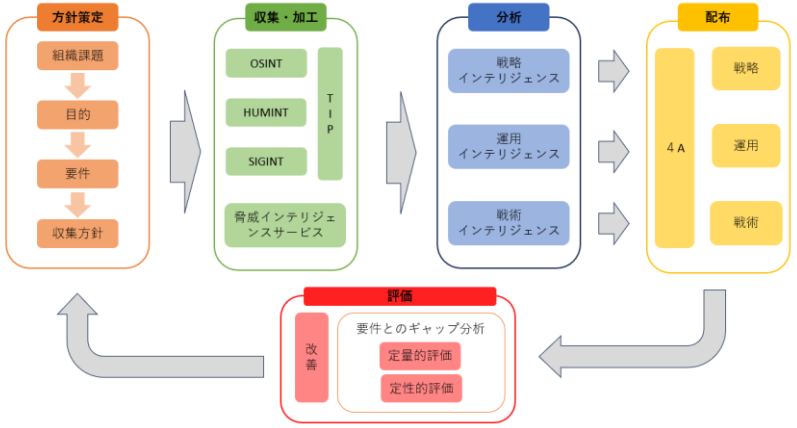
脅威インテリジェンスの全体像

- 脅威インテリジェンスは5つのフェーズのライフサイクルで構成され、ライフサイクルを開始するにあたり、脅威情報を収集し自組織のテレメトリー情報を分析できる基盤などが必要となる。

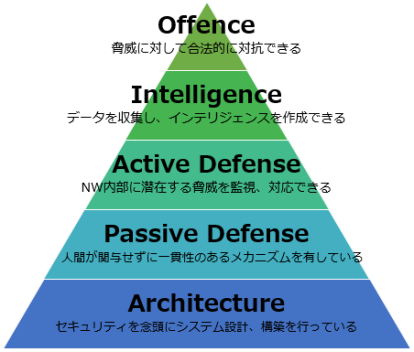
全体像

- ✓ 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い。
- ✓ 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**。
- ✓ 組織がインテリジェンスを活用する目的と必要な要件を定め、要件に必要な情報を様々なソースから収集し、自組織の意思決定に必要なインテリジェンスを作成・配布し、要件を達成しているか評価する。

全体ライフサイクル

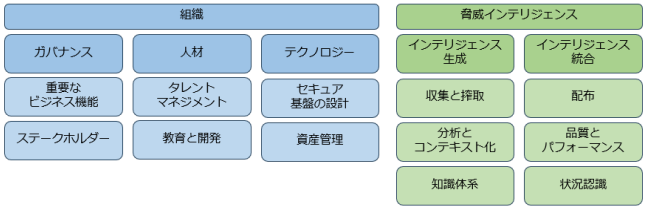


必要なセキュリティ成熟度



- **The Sliding Scale of Cyber Security（M.Lee）**[6]
  - ✓ 組織のセキュリティ成熟度を5段階で評価する成熟度モデル。
  - ✓ 活用するインテリジェンスに合わせ、組織・人・技術面での成熟度が必要である。
  - ✓ 一般的には、脅威インテリジェンスを活用するうえで、Passive Defenseまでの成熟度が要求される。

脅威インテリジェンスの成熟度評価



- **Cyber Threat Intelligence Maturity Platform（TU Delft）**[7]
  - ✓ 組織の脅威インテリジェンス成熟度を12のカテゴリーを250の質問に細分化し6段階で評価する指標。
    - ✓レベル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
    - ✓レベル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
    - ✓レベル2（整理）：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
    - ✓レベル3（管理されている）：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
    - ✓レベル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
    - ✓レベル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

必要なセキュリティ成熟度

- 組織が脅威インテリジェンスを開始するにあたり、ライフサイクルに必要なレベルの成熟度を確立しておく必要があり、未達の組織はまず全体の成熟度の向上を実施する必要がある。

ステップ	人・体制・運用	プロセス	技術
成熟度 1 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
成熟度 2 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
成熟度 3 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

①方針策定フェーズ

- 方針策定フェーズでは、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。

ステップ	実施事項	ポイント
1．課題抽出 自組織の課題を明確にする	□ 自組織に取り巻く資産を把握する □ 自組織における機器類の構成を把握する □ 各プロセスにおける手順書が作成され、また運用に使用されている	● 資産に対し全てを守ることはリソース負荷がかかります。守りべき資産は何か、優先度はどうかと特定資産に限定した重要資産の把握が重要。 ● 重要資産を特定しても誰が所有しどこにあるのかを把握することが重要。 ● 手順を起こすことはプロセスの見直しに必要な要素である。手順書がないとどこが悪かったのかと改善に活用できない。
2．目的の設定 脅威インテリジェンスを活用する目的を定める	□ 課題が抽出され優先順位付けを行う □ 戦略的・運用・戦術的インテリジェンスに応じた目的を設定する	● 課題の優先順位付けは簡単なもの難しいものといった基準で決定するのではなく、脅威動向をキャッチし事業継続に影響を及ぼすリスク度から順位付けを行う。 ● 戦略的・運用・戦術的インテリジェンスに対し、どれかではなくそれぞれに対し目的を設定する必要がある。言い換えれば利用者目線に合わせ目的を設定する。
3．要件の策定 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	□ アウトプットのイメージ化がされている □ インプットすべき情報が決定され、それに対する収集元が特定できる	● 目的に対し成果物としての内容、形式、活用方法がアウトプットイメージされることが重要。これには次のフェーズの収集も含まれる。
4．収集方法の検討 要件を達成するための情報収集・分析手段を定める	□ 要件を元に分析の基礎となるデータを収集先、収集方法、収集技法を確定する □ 情報源が適切なタイミングで提供されている □ OSINT、HUMINT、SIGINTの3種の情報源を活用する	● 分析の結果次第ではこのフェーズに戻り別の情報取集をする必要がある。 ● 情報源へ直接アクセスすることは自社へ跳ね返ってこないか注意が必要なため推奨しない。

②収集・加工フェーズ

- 収集・加工フェーズでは、方針策定フェーズで検討した収集方針に従って情報収集を実施する。
- 収集に際して組織のリソースや収集ソースに応じて、TIPやベンダーサービスを利用することを検討する。

情報収集技法

分類	実施事項	ポイント
OSINT Open Source Intelligence	◘ 公的機関による公開情報、ソーシャルメディア、有償無償の脅威インテリジェンスベンダー（OSINTツール）といった外部ソースからの情報収集 ◘ 情報源：技術的、外部	● OSINTツールによる情報の正確性について考慮する必要がある。 ● OSINTにおける情報収集の種類 ・公的資産の把握と確認　・情報漏洩の有無確認 ・マルウェア情報の調査　・ゼロディやエクスプロイトの調査 ・脆弱性情報の収集　・IPアドレスやドメインの情報収集 ・フィッシングサイトの調査
HUMINT Human Intelligence	◘ 非営利団体（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 ◘ 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 ◘ 情報源：人的、外部・内部	● 団体コミュニティとしてはISACが代表例 ● ダークウェブは誰でもアクセス可能。アンダーグランドフォーラムとしてはTelegramが活用されている。
SIGINT Signal Intelligence	◘ 自組織のテレメトリー（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、アラート情報など）による情報収集。 ◘ 情報源：技術的、外部	● IoC情報やTTPsを検証する場合、複数のテレメトリー情報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。 ● 脅威インテリジェンスを活用するにあたり、テレメトリー情報を収集できる機器とSIEMの導入は必要な要件となる。

効果的な収集方法の活用

分類	実施事項	ポイント
TIP Threat Intelligence Platform	◘ 自組織に関連する情報を重点的に収集 ◘ 共有プラットフォームとして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 ◘ 脅威情報を収集し，分析，共有を一元的に行える	● 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。
脅威インテリジェンスベンダー	◘ 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 ◘ 自組織のインテリジェンス要件としてFRIを制定する ◘ 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できる	● RFI 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。

③分析フェーズ

- 分析フェーズでは、収集した脅威情報をもとに事業影響や自組織の対策状況、資産状況と照らし合わせてリスクアセスメントを実施したり、外部評価ツールによって確度をあげるなど、意思決定に必要な情報を分析することが含まれる。

分類	実施事項	ポイント
戦略的インテリジェンス	◘ 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	● 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)を作成することが該当する。
運用インテリジェンス	◘ 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	● 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」などのフレームワークの利用を検討する。 ● システム開発・運用開始時期に行う侵入テストとして脅威ベースでテストを行うTLPT（Threat-Led Penetration Testing）が注目を集めている。
戦術的インテリジェンス	◘ 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実施する	● 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される。 ● 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。

- 分析フェーズでは自組織への影響や攻撃可能性を検討するために、インテリジェンス運用部門以外の関係個所との連携が必要になる。
- そのため、組織の役割分担の状況に応じて事前にインテリジェンス活動についての協力を依頼する必要がある。
  - ✓ **<u>システム開発・維持運用部門</u>**：資産管理状況の確認、侵入テストの実施
  - ✓ **<u>事業部門</u>**：攻撃の影響による事業影響の確認
  - ✓ **<u>SIRT部門</u>**：意思決定判断に必要な情報の追加提供支援、脆弱性対応方針・状況の確認
  - ✓ **<u>SOC部門</u>**：遮断・検知実施における連携内容の調整

④配布フェーズ

- 配布フェーズでは、インテリジェンスとして必要な４Ａ（正確性、利用者目線、アクショナブル、タイミング）[8]を念頭に、インテリジェンスを利用する組織、部門へ提供することが含まれる。

分類	戦略的インテリジェンス	運用インテリジェンス	戦術インテリジェンス
インテリジェンス例	セキュリティ方針	ペネトレーションテスト	検知・防御ルール
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化	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（Actinable）	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細心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

⑤評価フェーズ

- 評価フェーズでは、提供したインテリジェンスが方針策定フェーズで定義したインテリジェンス要件を満たしているか評価し、組織課題や目的の更新、その他各フェーズの改善を実施する。

実施事項	分類	ポイント
要件とのギャップ分析	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

実施事項	分類	改善のヒント・問いかけ
改善	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？
	収集・加工フェーズ	✓ 収集基盤 　✓ 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、自動化の検討） 　✓ 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	✓ 分析技法 　✓ 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	✓ 正確性 ✓ 利用者目線 ✓ 次のアクション ✓ タイミング

方針策定フェーズへ

ケーススタディ①：流行の脅威

インシデント対応 ― プロアクティブ

- ランサムウェアや標的型メールなど、公的機関やセキュリティベンダーが分析した昨今活動的、重大な脅威情報をもとに、自組織への影響や攻撃可能性、対策状況をアセスメントし、今後の戦略を策定する。

インテリジェンスの目的

- **セキュリティ対策の優先順位付け**
  - ✓ 攻撃観測情報から、流行となっている脅威動向・攻撃手法を把握し、脅威がもたらす自組織への影響と攻撃対象の有無、攻撃の頻度、対策の実施状況をリスクアセスメントし、対策の要否と優先度を判断する。
- **経営層のセキュリティ意識の向上とリスク管理**
  - ✓ 世の中の脅威動向をレポートし、セキュリティ担当役員が動向を把握できるようにする。
  - ✓ 経営層がリアルタイムのセキュリティ動向に関心を持つように向ける。

インテリジェンスのアウトプット

- **戦略的インテリジェンス（経営層向け）**
  - ✓ 経営層への脅威動向のレポート
  - ✓ 流行の脅威に関する自組織の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

インテリジェンス要件

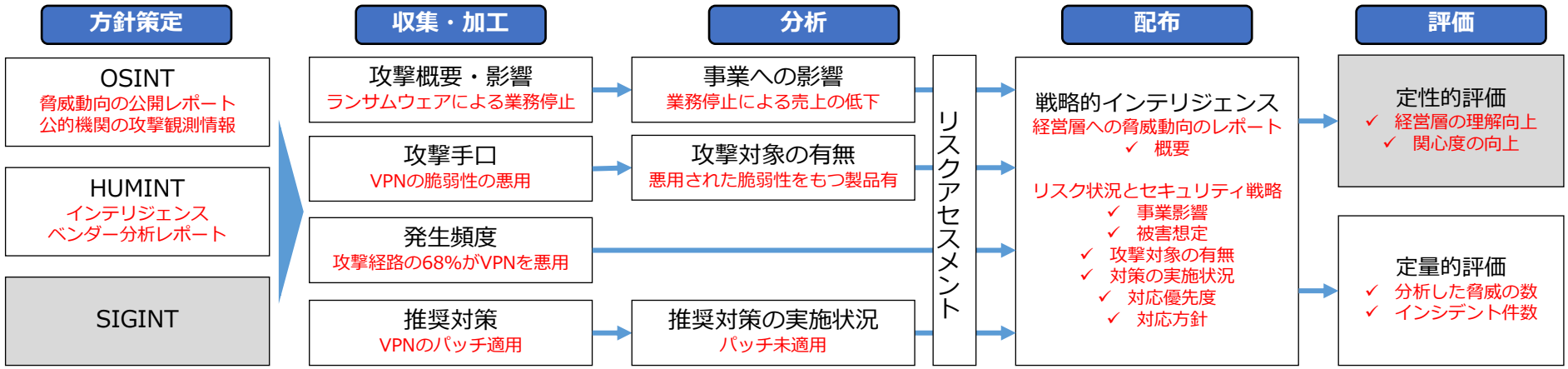
- ✓ 脅威情報とその攻撃概要、影響、攻撃手口、発生頻度、推奨対策情報
- ✓ 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況
- ✓ 推奨対策の自組織の実施状況

求められるセキュリティ成熟度

- **人・体制・運用**
  - ✓ 脅威動向を定期的に収集し、自組織の環境を確認する運用が可能であり、リスクアセスメントが実施できる閑居
- **プロセス**
  - ✓ 経営層へセキュリティリスクに関する報告を実施する機会がある
- **技術**
  - ✓ （推奨）複数の情報源から収集、集約するツール（TIP）
  - ✓ （推奨）アタックサーフェスマネジメント（ASM）

実施フローとケーススタディ

※グレーハッチングはケーススタディ紹介範囲外



ケーススタディ②：自社・特定業界への警戒情報

インシデント対応 ― プロアクティブ

- 業界コミュニティや公的機関、ベンダーレポートから収集した攻撃観測情報や注意喚起情報、攻撃キャンペーン情報をもとに、自組織に攻撃が到達する前に技術的なセキュリティ対応を実施する。

インテリジェンスの目的

- **プロアクティブなセキュリティ対応**
  - ✓ 連携される攻撃観測情報、侵害情報をもとに自組織での侵害有無の確認と、セキュリティ製品での検知・遮断ルールの設定を実施し、自組織に到達する前に対応を行う。

インテリジェンスのアウトプット

- **戦術的インテリジェンス（SOC向け）**
  - ✓ 侵害情報をもとにした検知・遮断判断に必要なインテリジェンス情報

インテリジェンス要件

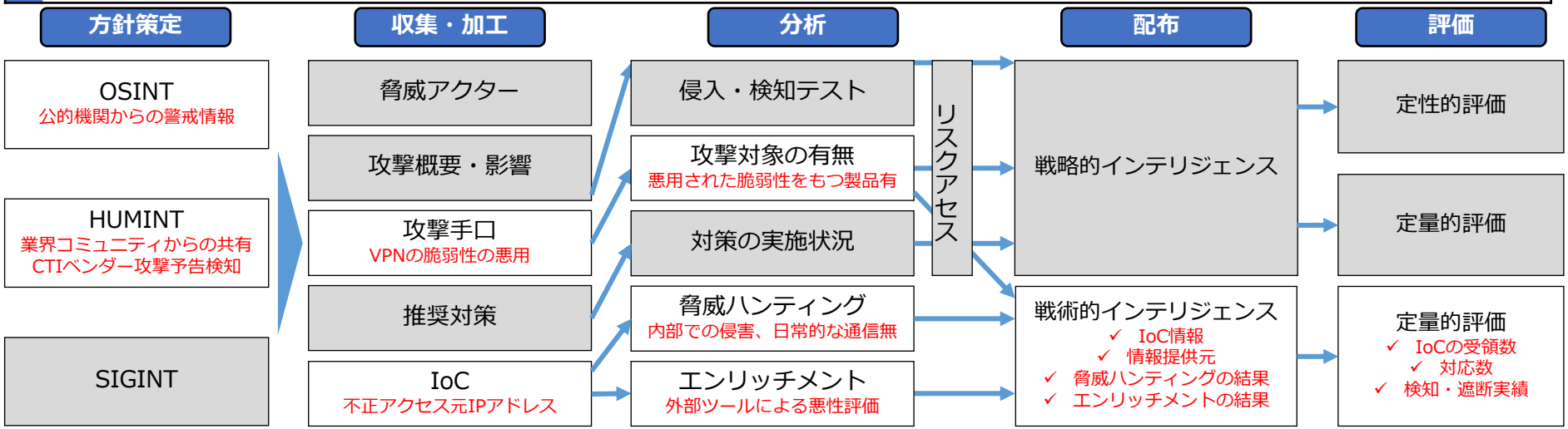
- ✓ 攻撃キャンペーンに利用されるIoC情報とIoCの遮断判断に必要な情報（IoCの外部評価結果、内部評価結果）

求められるセキュリティ成熟度

- **人・体制・運用**
  - ✓ IoC情報をもとに内部・外部評価を実施する人
  - ✓ IoCに関する検知・遮断判断する組織、体制
- **プロセス**
  - ✓ IoCに関する検知・遮断判断の基準
- **技術**
  - ✓ 警戒情報提供元から情報収集する基盤、契約
  - ✓ エンドポイント、NWログの集約・分析基盤

実施フローとケーススタディ

※グレーハッチングはケーススタディ紹介範囲外



ケーススタディ③：他社インシデント

インシデント対応 ― プロアクティブ

- セキュリティニュースなどから収集した他社のインシデント事例をもとに、動向レポートとして経営層に報告を実施、分析結果が詳細に判明した場合は自組織の対策必要性の有無を検討する。

インテリジェンスの目的

- **セキュリティ対策の優先順位付け**
  - ✓ 攻撃観測情報から、流行となっている脅威動向・攻撃手法を把握し、脅威がもたらす自組織への影響と攻撃対象の有無、攻撃の頻度、対策の実施状況をリスクアセスメントし、対策の要否と優先度を判断する。
- **経営層のセキュリティ意識の向上とリスク管理**
  - ✓ 世の中の脅威動向をレポートし、セキュリティ担当役員が動向を把握できるようにする。
  - ✓ 経営層がリアルタイムのセキュリティ動向に関心を持つように向ける。

インテリジェンスのアウトプット

- **戦略的インテリジェンス（経営層向け）**
  - ✓ 経営層への脅威動向のレポート
  - ✓ 流行の脅威に関する自組織の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

インテリジェンス要件

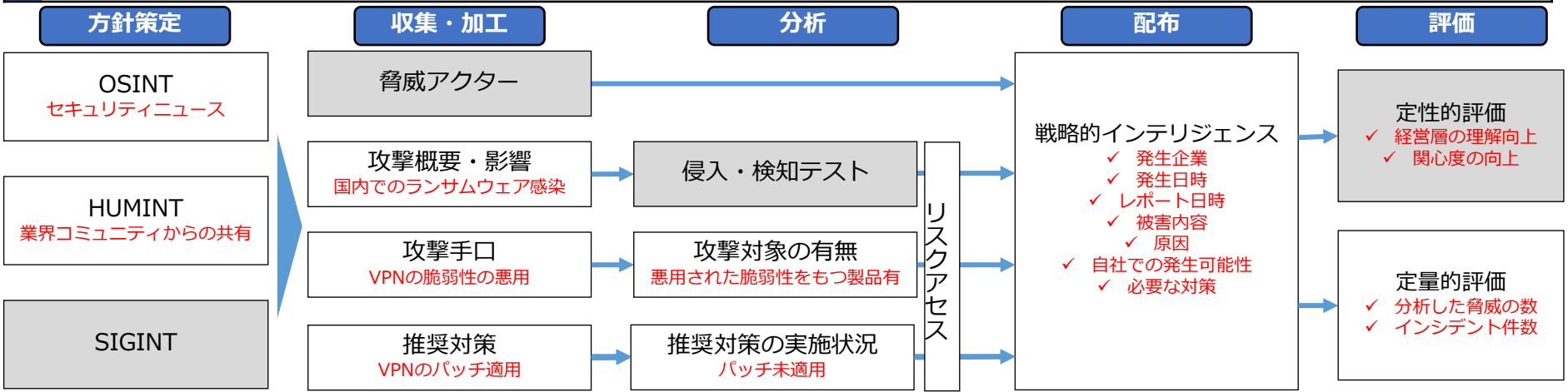
- ✓ 関連業界、地政学的関係のある他社のインシデント情報とその脅威アクター、攻撃概要、影響、攻撃手口、推奨対策
- ✓ 攻撃手口から想定される自組織における攻撃対象の有無、検知・防御状況
- ✓ 推奨対策の自組織の実施状況

求められるセキュリティ成熟度

- **人・体制・運用**
  - ✓ 脅威動向を定期的に収集し、自組織の環境を確認する運用が可能であり、リスクアセスメントが実施できる環境
- **プロセス**
  - ✓ 経営層へセキュリティリスクに関する報告を実施する機会がある
- **技術**
  - ✓ （推奨）複数の情報源から収集、集約するツール（TIP）
  - ✓ （推奨）アタックサーフェスマネジメント（ASM）

実施フローとケーススタディ

※グレーハッチングはケーススタディ紹介範囲外



ケーススタディ④：脅威アクターの動向・動機

インシデント対応 ― プロアクティブ

- 自組織、業界、地政学に関連する脅威アクターと、アクターの攻撃活動・攻撃手口の動向をもとに自組織での対策要否の検討や喫緊のアクターに対する技術的な対応を実施する。

インテリジェンスの目的

- **経営層のセキュリティ意識の向上とリスク管理**
  - ✓ 世の中の脅威動向をレポートし、セキュリティ担当役員が動向を把握できるようにする。
  - ✓ 経営層がリアルタイムのセキュリティ動向に関心を持つように向ける。
- **プロアクティブなセキュリティ対応**
  - ✓ 連携される攻撃観測情報、侵害情報をもとに自組織での侵害有無の確認と、セキュリティ製品での検知・遮断ルールの設定を実施し、自組織に到達する前に対応を行う。

インテリジェンスのアウトプット

- **戦略的インテリジェンス（経営層向け）**
  - ✓ 流行の脅威に関する自組織の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
- **戦術的インテリジェンス（SOC向け）**
  - ✓ 侵害情報をもとにした検知・遮断判断に必要なインテリジェンス情報

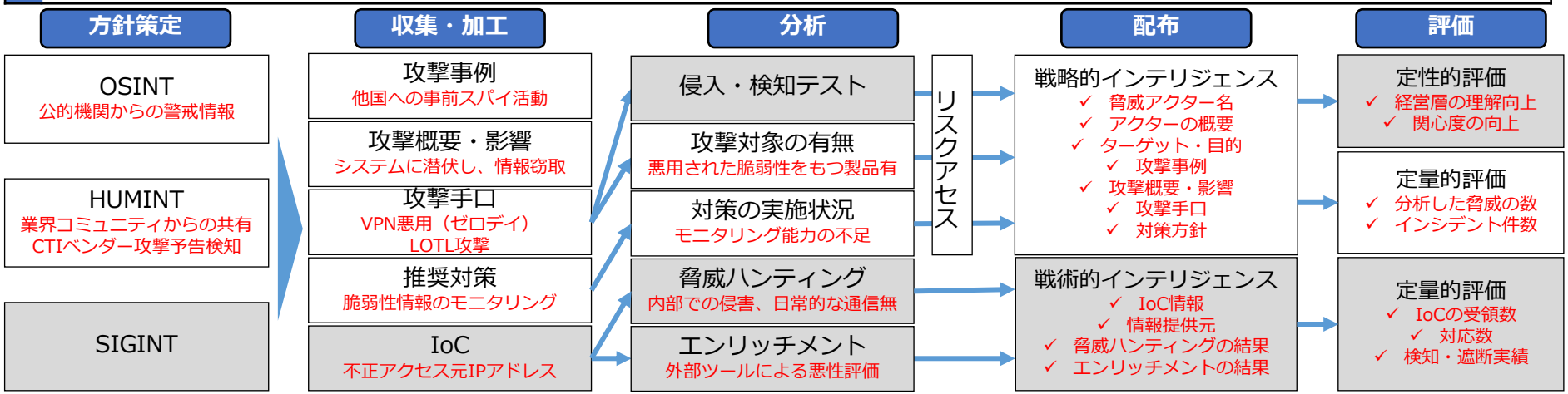
インテリジェンス要件

- ✓ 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
- ✓ 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）

求められるセキュリティ成熟度

- **人・体制・運用**
  - ✓ 脅威動向を定期的に収集し、自組織の環境を確認する運用が可能であり、リスクアセスメントが実施できる閑居
- **プロセス**
  - ✓ 経営層へセキュリティリスクに関する報告を実施する機会がある
- **技術**
  - ✓ （推奨）複数の情報源から収集、集約するツール（TIP）
  - ✓ （推奨）アタックサーフェスマネジメント（ASM）

実施フローとケーススタディ　※グレーハッチングはケーススタディ紹介範囲外



ケーススタディ⑤：自組織で観測された脅威

インシデント対応 ― プロアクティブ

- 従業員からのインシデント疑いの通報やセキュリティアラートをもとに侵害痕跡を調査し、攻撃経路や関連する脅威アクターのインフラストラクチャを特定し、網羅的な侵害情報に対する技術的対応を実施する。

インテリジェンスの目的

- **インシデントレスポンス能力の向上**
  - ✓ 従業員からの通報やセキュリティアラートをもとに、侵害有無を確認し侵害があれば分析、遮断を行う。
  - ✓ また、発見された侵害情報をもとにその攻撃経路やログを追跡し、潜伏している侵害情報を発見することで、網羅的な戦術的対応を実施でき、被害範囲の特定（インシデント除去）と再発防止が可能となる。

インテリジェンスのアウトプット

- **戦術的インテリジェンス（SOC向け）**
  - ✓ 侵害情報をもとにした検知・遮断判断に必要なインテリジェンス情報
  - ✓ インシデント対応要否の判断に必要なインテリジェンス情報

インテリジェンス要件

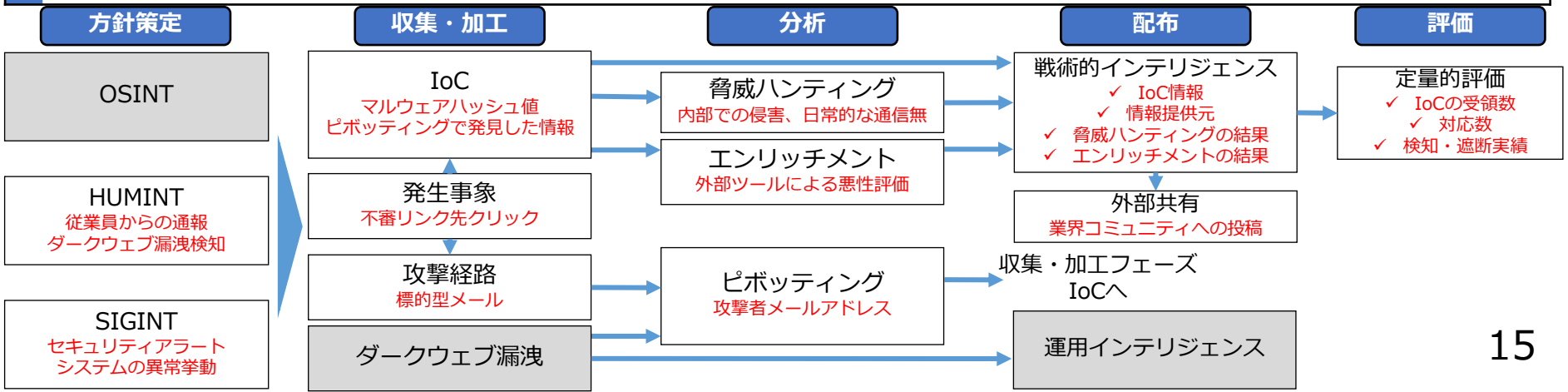
- ✓ ダークウェブでの組織機密情報、アカウント、メールアドレスの漏洩情報
- ✓ ランサムウェア脅迫の有無、自組織の侵害報告
- ✓ インシデントで検知したIoC情報、インシデント調査で発見、分析した追加のIoC情報

求められるセキュリティ成熟度

- **人・体制・運用**
  - ✓ IoC情報をもとに内部・外部評価、内部調査を実施する人
  - ✓ IoCに関する検知・遮断判断する組織、体制
- **プロセス**
  - ✓ IoCに関する検知・遮断判断の基準
- **技術**
  - ✓ 警戒情報提供元から情報収集する基盤、契約
  - ✓ エンドポイント、NWログの集約・分析基盤

実施フローとケーススタディ

※グレーハッチングはケーススタディ紹介範囲外



ケーススタディ⑥：インテリジェンス活動の統合レポート

- ケーススタディ①～⑤の活動内容をもとに、一定期間のタイミングでインテリジェンス活動のサマリレポートとしてセキュリティリスクに関する報告と今後の重点取り組みを経営層に報告する。

インテリジェンスの目的

- **セキュリティ対策の優先順位付け**
  - ✓ 今年度の脅威動向をもとに、次年度以降必要なセキュリティ対策の優先項目を特定する。
  - ✓ 重点項目をもとに、自組織のセキュリティ戦略の意思決定を行う。
- **経営層のセキュリティリスク管理**
  - ✓ 世の中の脅威動向および自組織の対応状況をレポートし、セキュリティ担当役員が動向を把握できるようにする。

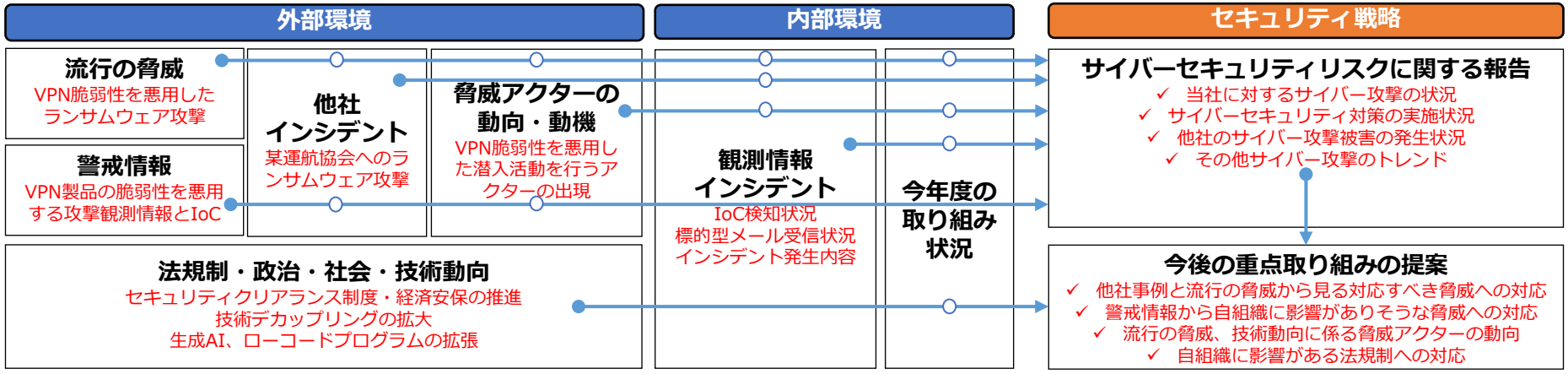
インテリジェンスのアウトプット

- **戦略的インテリジェンス（経営層向け）**
  - ✓ サイバーセキュリティリスクに関する報告レポート
  - ✓ 今後の重点取り組みの提案レポート

インテリジェンス要件

- **流行の脅威**
  - ✓ 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
- **自社・特定業界への警戒情報**
  - ✓ 警戒内容、対応数、検知・遮断件数
- **他社インシデント**
  - ✓ 発生企業、発生日時、被害内容、原因、自組織での発生可能性、必要な対策
- **脅威アクターの動向・動機**
  - ✓ 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、対策の実施状況
- **法規制・政治・社会・技術動向**
  - ✓ 国内外のセキュリティに関する法規制動向
  - ✓ 地政学上関連のある国家政府の動向（セキュリティ以外も含む）
  - ✓ セキュリティに関する業界、一般社会の動向

ケーススタディ



参考文献

[1] 石川朝久, 「脅威インテリジェンスの教科書」, 技術評論社, 2022年, P.2 P.17

[2] PwC, 「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」
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/geo-technology-and-cybersecurity.html

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

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

[5] 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

[6] Robert M. Lee, 「The Sliding Scale of Cyber Security」
https://www.sans.org/white-papers/36240/

[7] TU Delft, 「Cyber Threat Intelligence Maturity Platform」
https://www.cti-maturity.com/

[8] 石川朝久, 「脅威インテリジェンスの教科書」, 技術評論社, 2022年, P.7