防衛研究所 新領域研究会
「サイバー脅威インテリジェンス（CTI）をめぐる内外動向と産官学連携」

脅威インテリジェンスの歴史的・理論的視座

2024.03.01

Tomohisa Ishikawa, Ph.D., CISSP, CSSLP, CCSP, CISA, CISM, CFE, PMP

本日お伝えしたいこと

本日は、脅威インテリジェンスの政策的論点を抽出するため、民間企業で利用されている
脅威インテリジェンスが持つ機能的視座と歴史的視座をお話させていただきます。

- 以下の３部構成でお話をさせていただきます。
  - ***Part I　　：CTIの機能的視座***
    - 民間企業にとって脅威インテリジェンスがどのような役割を持つのか、脅威インテリジェンスのステークホルダーを洗い出し、各ステークホルダーが持つ目的、エコシステムの鳥観図を示し、脅威インテリジェンスの取り扱い、どのようなインセンティブに基づいてエコシステムが成立しているか、解説します。
  - ***Part II　　：CTIの歴史的視座***
    - *CTI*は、伝統的なインテリジェンスの考え方を借りつつ、独自の進化を遂げています。こうした変化について、サイバー脅威インテリジェンスの歴史を簡単に紐解き、現在の脅威インテリジェンスがどのような変遷をたどりどの位置にいるのか、解説します。
  - ***Part III　　：Wrap-Up***
    - 機能軸・歴史軸の両面から、まとめと今後の示唆について話します。

注意：本内容は、全て講演者個人の見解であり、所属企業、部門、その他所属組織の見解を代表するものではありません。

自己紹介：石川　朝久（いしかわ　ともひさ）

- **所属 ：Lead Cyber Security Architect @ グローバル金融機関**
- **資格 ：**
  - 博士（工学）, CISSP, CISSP-ISSMP, CSSLP, CCSP, CISA, CISM, CDPSE, CFE, PMP, 情報処理安全確保支援士 etc.
- **経歴 ：**
  - セキュリティ専門会社にて、侵入テスト・インシデント対応・脆弱性管理・教育に従事した後、2019年度より現職。
  - 現在は、グローバルセキュリティ戦略の企画立案、セキュリティアーキテクチャ検討、グローバルセキュリティ戦略・国内外のグループ企業のセキュリティ支援・TMHD-CSIRT運用・脅威インテリジェンス分析などに従事。
- **対外活動（抜粋）：**
  - **講演・講師：**
    - DEFCON 24 SE Village Speaker (2016)
    - Internet Week Speaker (2018-2020, 2022)
    - FIRSTCON23 Speaker（2023）
    - セキュリティ・キャンプ 全国大会 講師（2023）
    - セキュリティ・ミニキャンプ in 石川 講師（2023）
    - Global Security Camp 2024 Instructor (2024)
  - **委員会活動：**
    - IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）
    - IPA 「10大脅威執筆者会」メンバー（2010～2014, 2019~）
  - **執筆・翻訳・監訳：**
    - 複数の本を執筆・翻訳・監訳しています。
  - **調査・研究：**
    - 情報処理学会・電子情報通信学会で研究発表をしています。

Part Ⅰ：CTIの機能的視座

脅威インテリジェンスとは？

- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス = 脅威 + インテリジェンス

- **要素１：脅威とは？**
  - 要すれば、「**攻撃者・攻撃グループ**」のこと。
  - 「**意図 × 能力 × 機会**」という３要素（*）で特徴づけることができる（by SANS Institute）
  - 脅威インテリジェンスとは、「この３要素に関連する情報を集めること」と定義できる。

- 各要素の説明
  - 意図（Intent・Motivation）
    - 攻撃対象組織を狙う目的・動機を意味する。
  - 能力（Capability・Method）
    - 目的を達成するために必要な攻撃者の能力・攻撃手法を意味する。
  - 機会（Opportunity）
    - 攻撃の実行を可能とする環境・条件を意味する（脆弱性の有無 etc.）

（*）Motivation・Opportunity・Methodという頭文字をとってMOMモデルと呼ばれるケースもある。

脅威インテリジェンスとは？

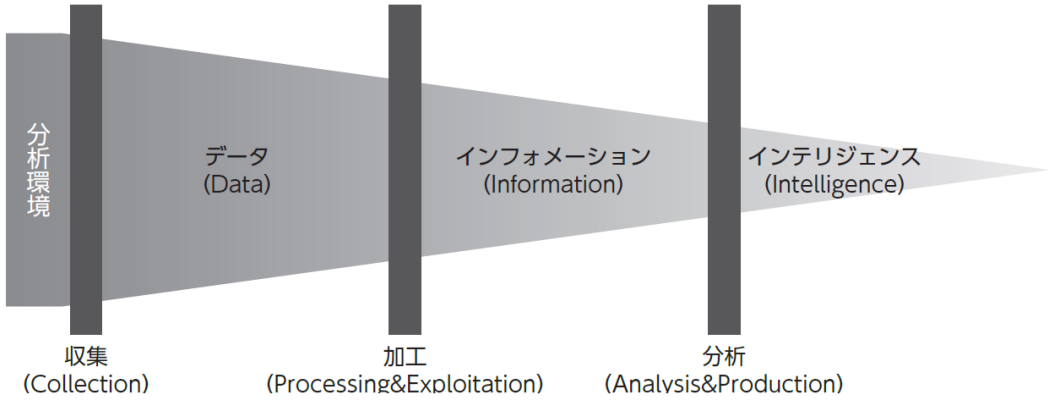
- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

- **要素２：インテリジェンスとは？**
  - 「歴史的経緯」から大きく２種類の捉え方があります。
  - 要すれば、**①方針に基づき、②データを収集・加工・分析してできた成果物**を「インテリジェンス」と呼びます。

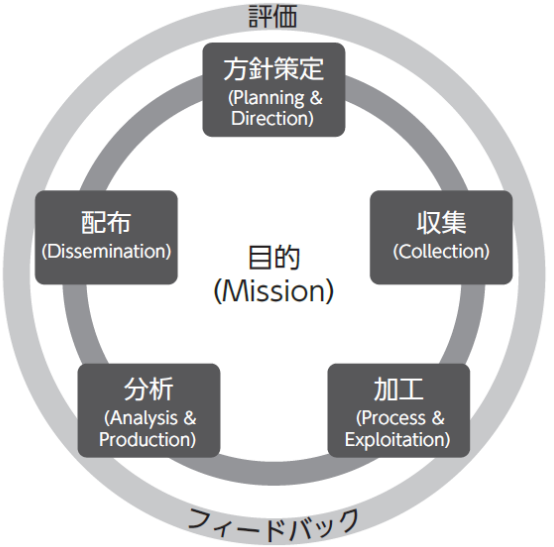
タイプ１：データ形式としてのインテリジェンス

インテリジェンスを「情報の収集・加工」してできるデータ形式としてとらえる定義方法



タイプ２：プロセスとしてのインテリジェンス

インテリジェンス作成過程を継続的な活動プロセスとしてとらえる定義方法

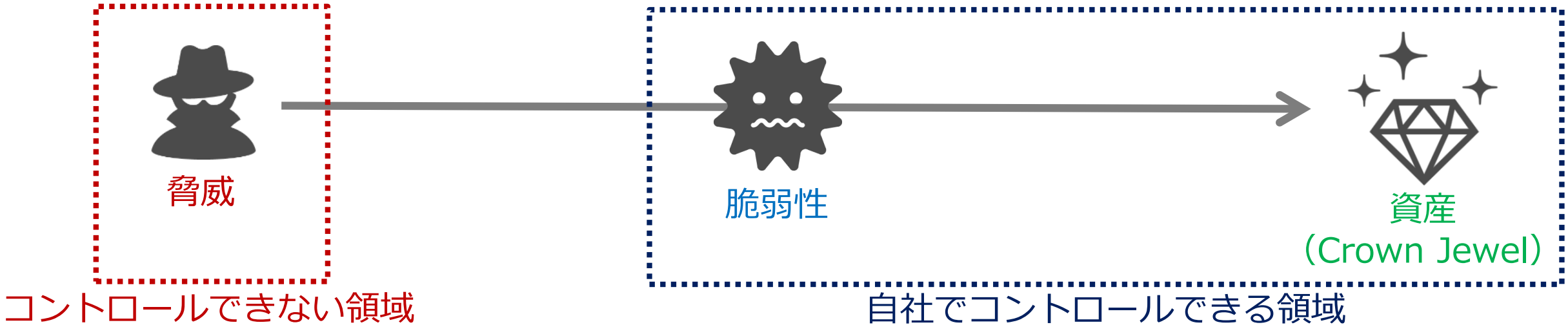


※ 図は、『脅威インテリジェンスの教科書』 より引用

脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - リスクは３要素で定義されるが、（防御側の組織が）コントロールできる要素は、「脆弱性」と「資産」である。そのため、**伝統的なリスク管理手法**では、できる限り「脆弱性」をつぶし、安全な場所に「資産」を保有することが重要であると言われていた。
  - 注意：「脆弱性」は技術的脆弱性だけでなく、設定不備・内部プロセスの不備なども含む。



脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - しかし、現在は各要素に大きな変化が生まれている。
  - **変化①：資産の変化**
    - ***“Data is the new oil”***
      - 2017年の『The Economist』の記事タイトル。リスクの観点から言えば、資産が膨れあがり、守るべき「領域」が拡充し続けている。
        - » 技術の進歩により、取得可能なデータ量が増加（＝ビッグデータ）
        - » 当該取得したデータを継続的に学習・分析可能な機械学習・AI技術の台頭
    - **分散化**
      - データの利用者（Subject）とデータ自体（Object）の分散化傾向にあり、攻撃対象領域（Attack Surface）が増大し続けている。
        - » データ利用者の多様化（API連携、リモートワーク etc.）
        - » クラウド利用によるデータの分散化

脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - しかし、現在は各要素に大きな変化が生まれている。
  - **変化②：脆弱性の変化**
    - **管理労力の増加：**
      - 技術的負債、膨大なサーバ群、利用製品の多様化などにより、膨大な管理労力がかかる
    - **継続的な変化：**
      - アジャイル開発に代表される常に変化するシステム開発手法の登場
    - **リスクの取り扱いが難しい領域：**
      - クラウド・サプライチェーンなどの既存の管理手法の応用が難しい領域も存在し、リスクの引き受け方が難しくなっている

脅威インテリジェンスの目的・必要性

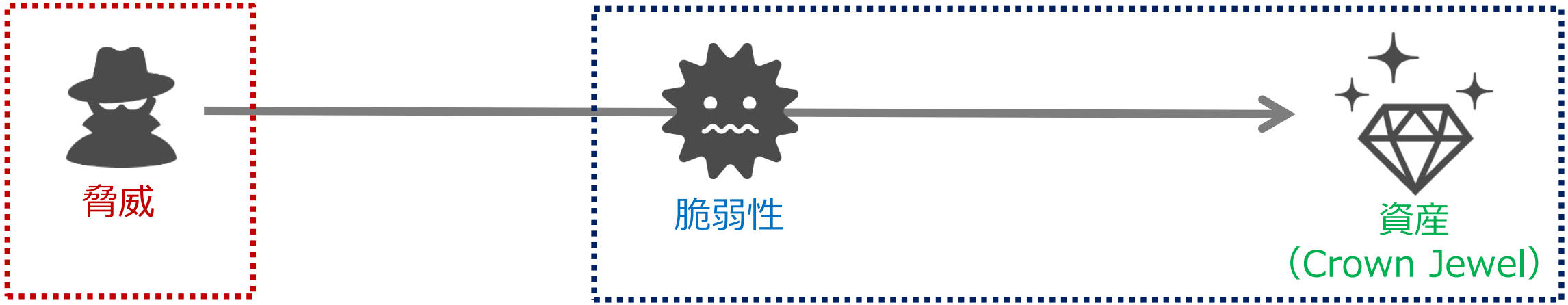
- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - しかし、現在は各要素に大きな変化が生まれている。
  - **変化③：脅威の変化**
    - **「汎用」型から「個別」型へ：**
      - 汎用的なマルウェアの配布から、個社・業種に特化した攻撃手法の台頭
      - 攻撃グループ（Threat Group）の種類により目的が異なるため、行われる攻撃も多様化
    - **攻撃の「分業化」：**
      - 攻撃の「分業化」が進み、マルウェア開発や、「初期侵入」に特化したInitial Access Brokerなど、攻撃手法も多様化している。

脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - **「リスク管理」の優先度をつけるため、「脅威」へ注目する。（＝敵を知る）**
  - サイバーリスクのドライバー（起点）となるのは、「脅威」であり、セキュリティリソース（人・モノ・金・時間）は限られるため、全方位に十分な対策を行うことが難しい。
  - そのため、具体的な脅威へ対応することを優先する。

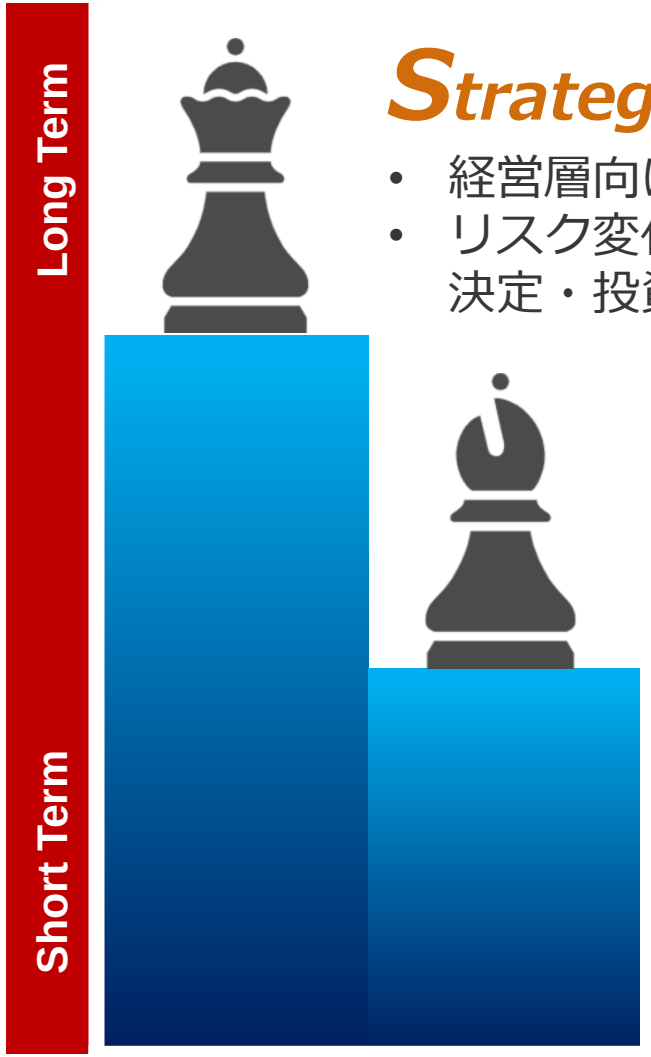


「リスク管理」の優先度をつけるため、「脅威」に注目する。（＝敵を知る）

→ 具体的な「脅威」に対応する形で対策を行うことが「**脅威インテリジェンス**」が役立つ理由！

脅威インテリジェンスの分類

- 脅威インテリジェンス活用は、種類・目的を理解することが重要（誰に価値を提供するか？）
  - 脅威インテリジェンス自体では価値をもたらさず、提供して初めて価値をもたらす。



Strategic Intelligence

- 経営層向け
- リスク変化に対するハイレベルな情報を提供することで、セキュリティに関する適切な意思決定・投資判断のインプットとする。

Operational Intelligence

- セキュリティアーキテクト・管理者・SOC担当者向け
- 攻撃者のプロファイル、攻撃手法（TTPs）など攻撃者の手法を理解し、短期～中期的なセキュリティ改善活動に活用する。

Tactical Intelligence

- SOC担当者向け
- 日々のセキュリティ運用において、攻撃シグニチャ（IOC）を取得・設定することでインシデントを未然に防ぐ。

良い脅威インテリジェンスの４条件

- **良い脅威インテリジェンスの４要件：**
  - 当該４要件を満たして、初めて有効活用が可能となる

Accurate

正確性：技術的に誤った情報や未精査な情報を流通しないこと
不確実性を扱うため「真の意味」で正しいというわけでなく、「確度」が重要となる

Audience Focused

利用者目線である：誰のために脅威インテリジェンスを提供しているか
利用者のニーズに合致した情報でなければ、脅威インテリジェンスの「価値」がでない

Actionable

アクショナブル：次に取ってほしい行動が何か明示されていること
具体的かつ現実的な対応が提示されていること

Adequate Timing

適切なタイミング：鮮度が保たれた情報を提供すること
古い情報を提供されても困るので、現在の脅威に即した情報を提示すること

民間企業における独自のインテリジェンス進化

「脅威」への分析手法を高度化するため、”伝統的な”インテリジェンス技術を応用してきた！

- 国のインテリジェンス機関の思考法を借りつつ、北米の産業界/セキュリティコミュニティのなかで、サイバー領域へ応用してきた経緯がある。
- 例）インテリジェンスサイクル・ACH（競合仮説分析）・Critical Thinking（批判的思考）…

- 例）APT1 Report
  - （元米国空軍士官であるKevin Mandia氏が創業した）Mandiant社が2013年に発表したレポート
    - 中国人民解放軍が、米国のサイバー攻撃に関与しているAPT-1に関するレポートを発表
    - “伝統的な”インテリジェンス技法が有効に活用できることを実証した事例
    - https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units

- 「脅威」に最も携わるDFIR専門家(*)の多くが米軍経験者・警察経験者であることも、伝統的なインテリジェンスの思考法を受け入れる上で、大きな下地になっていたと考えられる。

一方で、CTIは民間企業で独自の活用を遂げてきた。その理由として、以下が挙げる。

- ① 目的の相違（＝異なるニーズの違い）
- ② 調査主体 + 調査対象の違い（＝データの所有者の違い）
- ③ 共有におけるインセンティブの違い

(*)：Digital Forensics & Incident Response

民間企業における独自のインテリジェンス進化 - ① 目的の相違

① 目的の相違（＝ニーズによる相違）

While traditional intelligence focuses on securing nations,
CTI focuses on securing organizations and critical infrastructure
from breaches, attacks, and compromises.

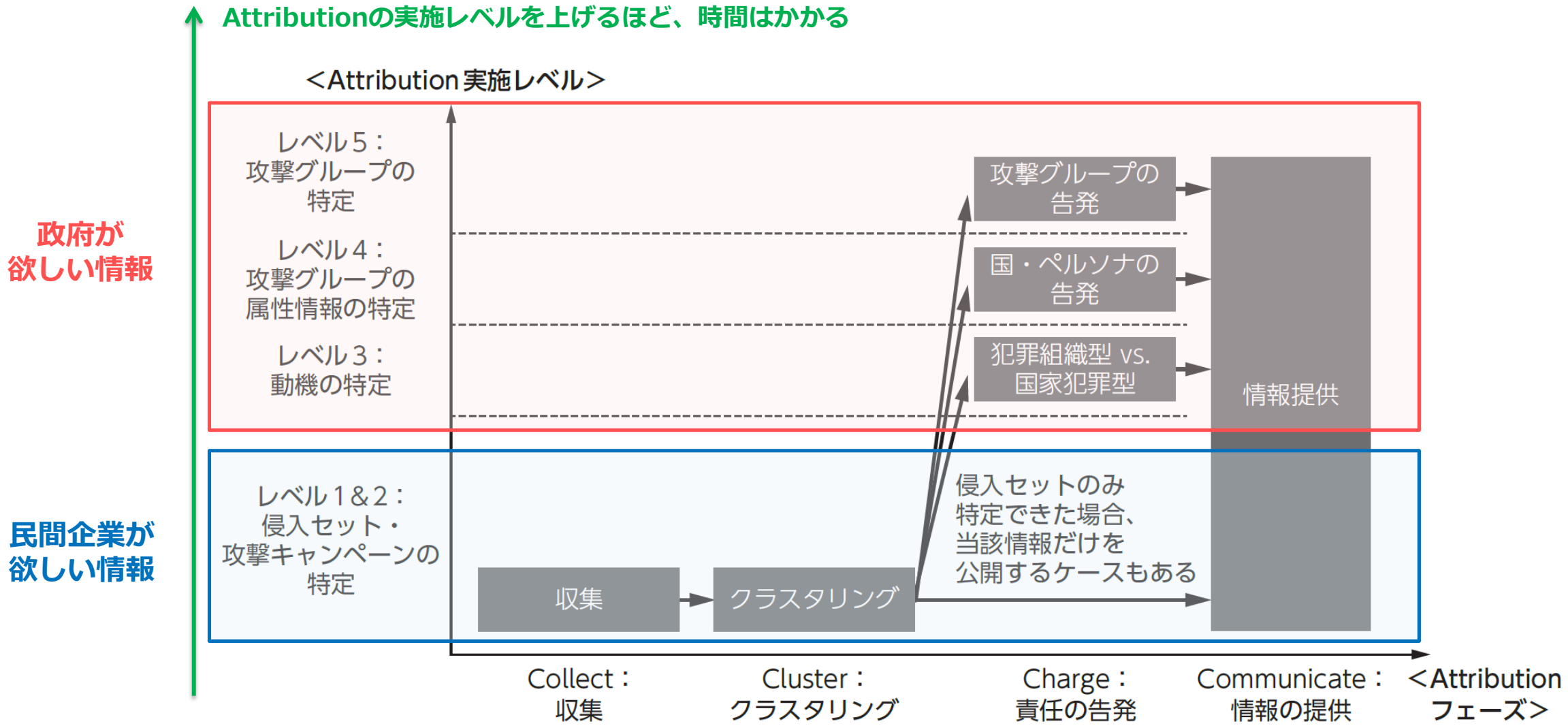
What is Cyber Threat Intelligence? (https://gca.isa.org/blog/what-is-cyber-threat-intelligence)

- 「伝統的なインテリジェンス」は国防のためである一方、CTIの「脅威」の分析理由はあくまで「リスク管理」、言い換えれば漏洩・攻撃・侵害を防げることが主眼であると捉えられている。
- **「脅威の排除」の捉え方の違い**
  - 民間企業にとって「脅威の排除」とは、攻撃グループに攻撃させない（予防） or 最小化すること（検知・対応）
  - では、政府機関にとって「脅威の排除」とは何か？

- サイバー攻撃も国防としても重要な課題だが、（政府機関が直接狙われた場合を除き）民間企業が狙われた場合、対応は民間企業に大きく依存する。
  - 参考）アトリビューション（攻撃グループを特定する技術）
  - 参考）Active Cyber Defense（積極的サイバー防衛）

民間企業における独自のインテリジェンス進化 - ① 目的の相違

- 例）Attributionプロセスモデル（C4モデル）における目的の相違



※ 図は、『脅威インテリジェンスの教科書』 より引用

民間企業における独自のインテリジェンス進化 - ② 調査主体 + 調査対象の違い

② 調査主体 + 調査対象の違い

- 伝統的な犯罪・攻撃と違い、調査主体は民間企業（+セキュリティベンダー）となるケースも多く、調査対象となる端末・サーバの調査も民間で可能となる（逆に、犯罪捜査における取り調べの権限・鑑識技術については、法的・技術的制約から国家の独占事項と考えられる）

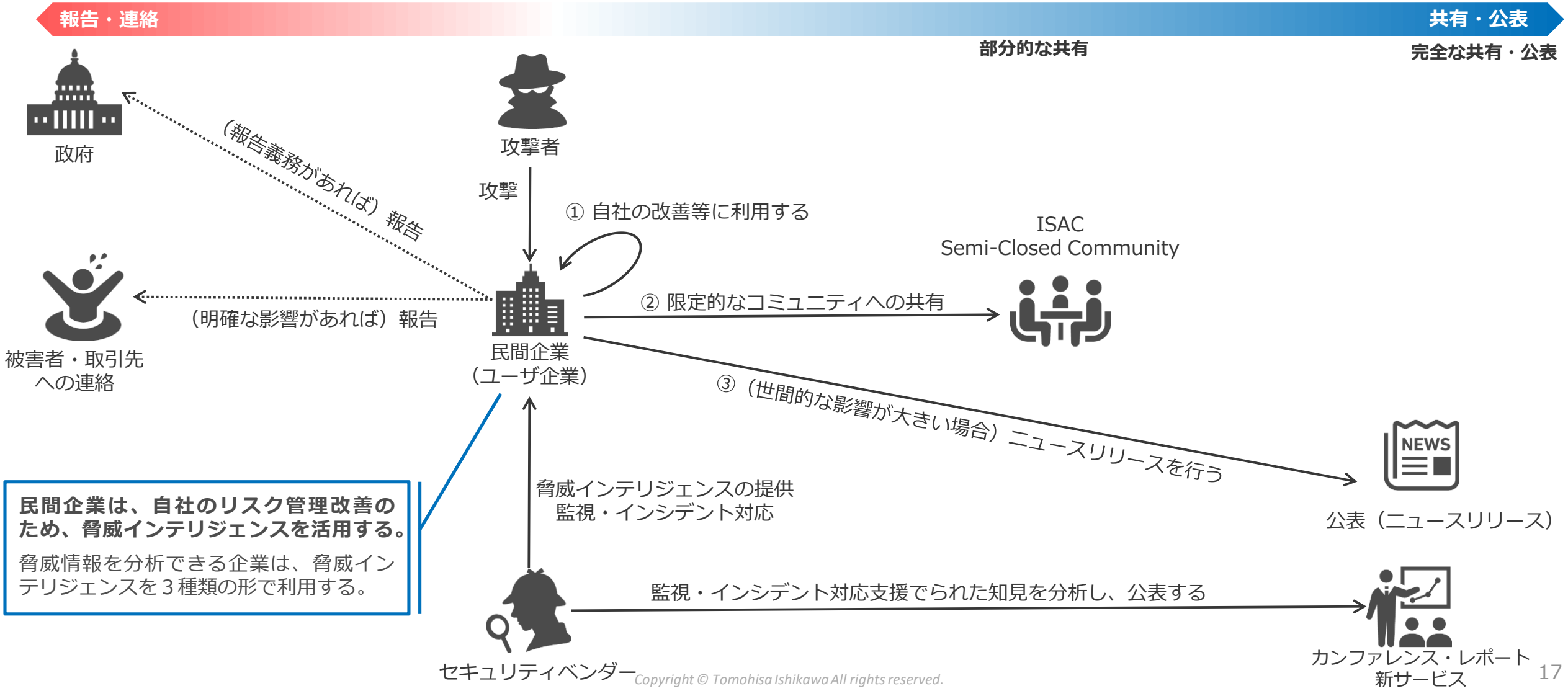
- 民間企業が予防・検知・対応を行う観点から、分析も独自で行うようになった経緯がある。

	民間への伝統的犯罪の場合		民間へのサイバー攻撃の場合	
	調査主体（例）	調査対象（例）	調査主体（例）	調査対象（例）
金銭的被害（泥棒）	警察	人・犯行現場	民間企業	コンピュータ
エスピオナージ	警察・諜報機関	人・犯行現場	民間企業	コンピュータ
重要インフラへの攻撃	自衛隊	衛星写真	民間企業	コンピュータ
テロ活動	警察・諜報機関	人	民間企業	コンピュータ

民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

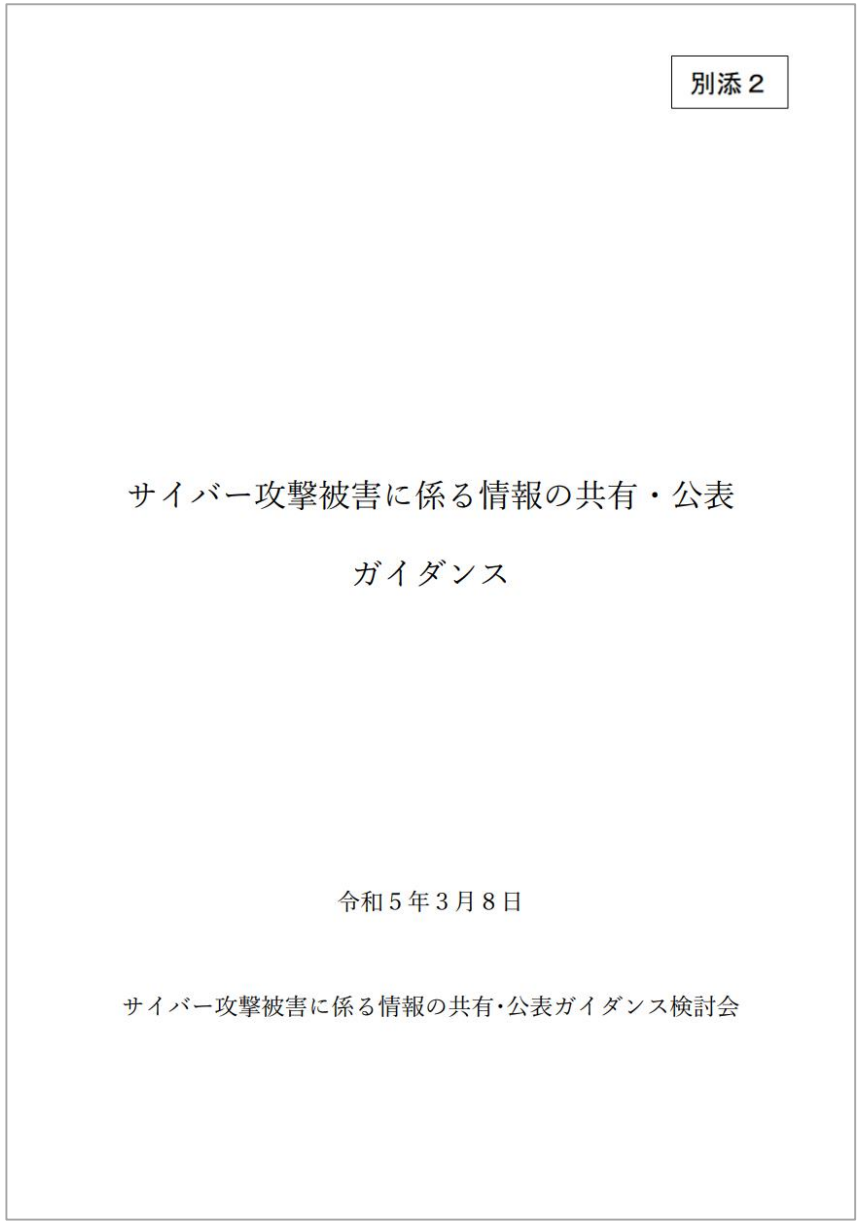
民間企業は、「自助・共助・公助」のために共有する。但し、背後にあるインセンティブが大きく影響する。



民間企業は、自社のリスク管理改善のため、脅威インテリジェンスを活用する。

脅威情報を分析できる企業は、脅威インテリジェンスを３種類の形で利用する。

補足：共有・公表・報告等の違いについて


別添２

サイバー攻撃被害に係る情報の共有・公表

ガイダンス

令和５年３月８日

サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会

＜共有＞

1. 自ら情報共有活動参加者に対して行うもの
2. 情報共有活動のハブ組織である専門組織や情報共有活動に参加している専門組織を介して情報共有活動に情報を共有し、仲介した専門組織の知見を含むフィードバックを得る方法

＜公表＞

- 法令／ガイドラインに基づく公表
- （法令等の定めはないが）被害組織自身の判断で行われる公表

＜報告・連絡＞

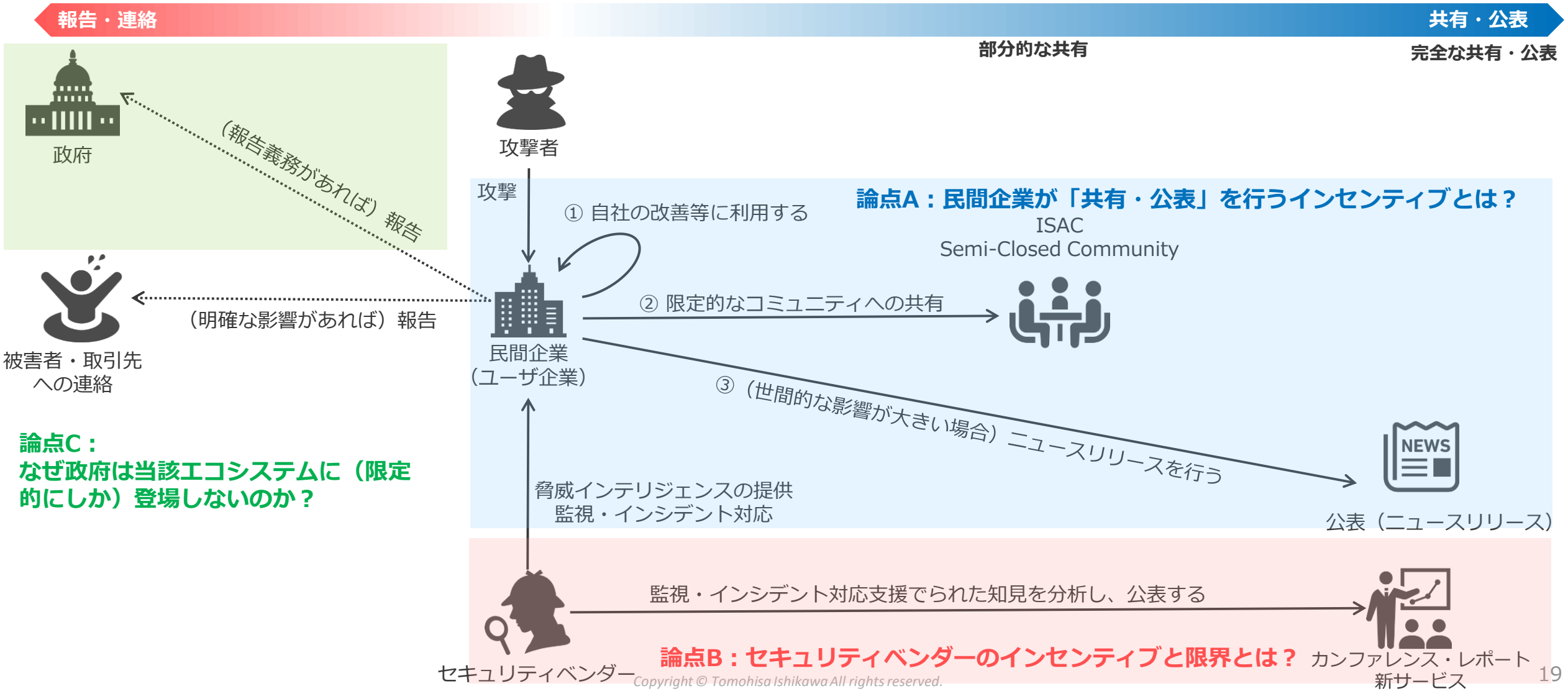
- 特定のステークホルダーへの通知（通知根拠は、法令に基づく場合と自組織の判断で行われる場合がある）

参考：サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会

民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

民間企業は、「自助・共助・公助」のために共有する。但し、背後にあるインセンティブが大きく影響する。



民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

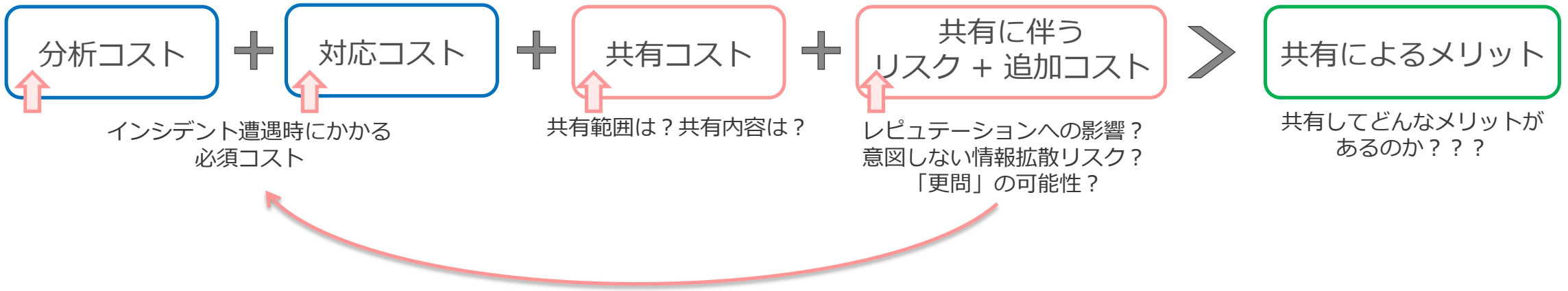
③ 共有のインセンティブの違い

論点A：民間企業が「共有・公表」を行うインセンティブとは？

- 民間企業は、予防コストのみならず、分析コスト + 対応コストも支払う必要がある

- 既に「コスト」がかかっている状況下において、さらに「共有コスト」 + 「共有に伴うリスク」を伴って共有するメリットが見えないため、（原則的には）民間企業は情報を出したくない。
  - 世論などの反応が大きくなり、公表したほうがメリットが大きくなれば公表する。
  - 参考）フリーランチ問題

- 「更問」や公表による追加対応など、既存コストにも影響する可能性がある。

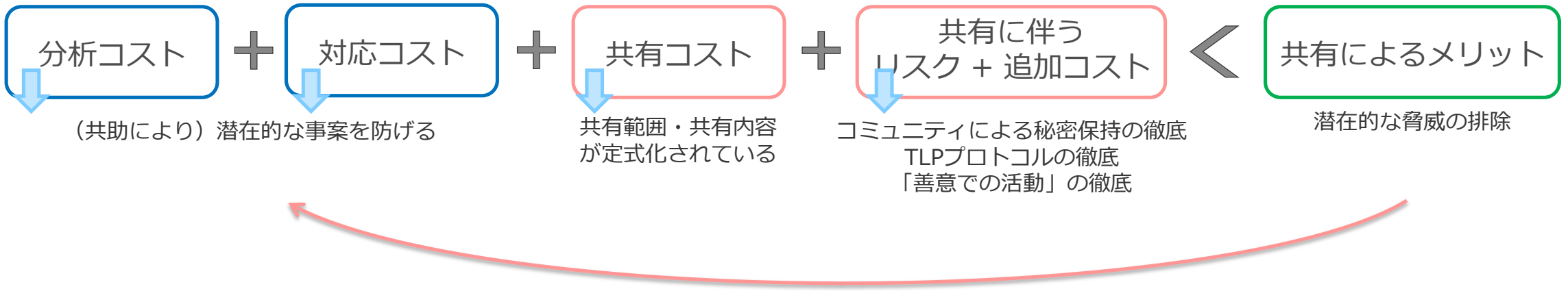


民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

論点A：民間企業が「共有・公表」を行うインセンティブとは？

- ISACなどのコミュニティが成り立っている背景には、「共助」を実践できるために成り立っている。
- その背後には、様々な施策によりインセンティブ設計が行われている。
- **「共助」のメリット：**
  - 同じ業界であれば、原則的に直面する脅威・攻撃グループ、利用される手口も同じである。
  - 一方、脅威情報を全て収集することには現実的には不可能である。お互いに情報を共有することで、潜在的な共通の脅威を排除することが可能となる。
  - アナロジー）保険によるリスク分散



民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

論点A：民間企業が「共有・公表」を行うインセンティブとは？

- ICでの共有のメリット：
  - **理論的観点：**
    - 脅威インテリジェンスの目的である「リスク管理」に必要な脅威情報を全て網羅的に収集することは不可能
      - » 異なるテレメトリ、リソース、キャパシティ、偶然性…
    - そのため、「共助」という形でお互いの情報を持ち寄ることで、脅威の全体像などを行うことができる。
    - アナロジー）クラウドソーシング

  - **参考）マタイ効果（Matthew Effect）**
    - 1968年に、科学社会学者ロバート・キング・マートンによって提唱された考え方
    - 「条件に恵まれた研究者は優れた業績を挙げることでさらに条件に恵まれる」という現象を説明した考え方
    - 「情報共有した人に、より多くの情報が集まる効果がある」とも考えられる。

  - **参考）「オープンソース」文化：**
    - ソースコードを使用、調査、再利用、修正、拡張、再配布することができるソフトウエアのこと
    - （実証はできないが）IT技術の発展に寄与したソースコードを「共有」する文化・習慣こそ、”伝統的な”インテリジェンス機関に見られる「インテリジェンスの独占・秘匿」とは異なり、情報共有を行う文化を形成したのでは？？

民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

論点B：セキュリティベンダーのインセンティブと限界とは？

- セキュリティベンダーは、①技術力の開示、②サービス開発への応用、③製品に対するシーズ構築など、共有には非常にポジティブである

- **セキュリティベンダーが提供するインテリジェンスの課題：**
  - **課題１：情報粒度**
    - ベンダー側が取得できる情報の多くは、技術的情報に限られるケースが多い。脅威の定義（**意図 × 能力 × 機会**）において、能力について分析できるが、意図・機会に関する十分な分析は難しいケースも多い。
    - 詳細情報を開示できないため、情報粒度は抽象化される。
  - **課題２：ベンダーが「見える」範囲に限定された分析**
    - ベンダーは複数企業の情報を保有している一方、ベンダー間での情報連携はほとんど行われないため、分析は当該ベンダーが取得できる情報に基づいて行われる（＝データセットの習得範囲の問題）
  - **課題３：情報の「正しさ」**
    - 公開された情報が本当に「正しい」情報なのか、検証する方法がない（＝ここでいう「正しさ」は、データセットが公開されない/できないため、情報の受け手として、自組織との関連性・影響度を自身で検証する術がないという意味）

民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

論点C：なぜ政府は当該エコシステムに（限定的にしか）登場しないのか？
→ インセンティブの不一致

- 報告へのハードル（監督官庁への「報告」と「情報提供」の違いとは？）

- 政府機関がCTIを必要とする理由　→　国防のため but…
  - 国防に必要なアトリビューションを含む情報は、民間企業が持つ脅威インテリジェンスをメタ分析する以外に現実的に取得する方法がない。
  - サイバー攻撃は民間企業に対しても行われるが、「第５の戦場」と呼ばれるサイバー空間において、「（国家が持つ）レーダー」が限定的となってしまうため、民間が所有するセンサーを活用する必要性が出てくる。

- 情報を提供しても、（政府として）意味のあるインテリジェンスを生成するには時間がかかる可能性があるため、共有するメリットがそこまで大きくない可能性がある（＝**インセンティブの不一致**）
  - 前述の**4A条件**を満たす情報を提供できるか？

民間企業における独自のインテリジェンス進化 - ③ 共有のインセンティブの違い

③ 共有のインセンティブの違い

論点C：なぜ政府は当該エコシステムに（限定的にしか）登場しないのか？
→ インセンティブの不一致

- 例）InfraGard
  - 1996年にFBIのクリーブランド支局におけるローカルな取り組みとして始まり、その後全米の支局に拡大された組織。
  - 当初は、サイバー犯罪分野におけるFBI、地方の法執行機関及び企業や学術機関との連携、情報共有を目的としたプログラムであったが、現在では、テロ、インテリジェンス、犯罪及びセキュリティに関する諸問題にまで拡大されている。また、全米規模での分科会活動も行われている。
  - 「官のみの対応で重要インフラを防護することは困難である」ことへのアンチテーゼとして生まれた概念
  - 参加者を増やすことで情報を取れる「センサー」を拡大する活動だと捉えられる。
  - https://www.fbi.gov/news/stories/2010/march/infragard_030810

Part II：CTIの歴史的視座

サイバー脅威インテリジェンスの歴史

- （所説あるが…）世界で初めて行われたサイバー脅威インテリジェンス活動とは？
  - 『カッコウはコンピュータに卵を産む』（1989年）
    - 著者のClifford Stoll氏が、 1986年、ローレンス バークレー国立研究所の管理者として勤務していた際、当研究所サーバ経由で米軍各所のサーバに侵入していたクラッカーを発見し、状況を監視。最終的には警察当局と共同で捜査を進め、ハニーポットを設置して、 KGBに雇われたドイツ人ハッカーMarkus Hess氏を検挙に追い込んだ実話。

サイバー脅威インテリジェンスの歴史

簡単に脅威インテリジェンスの歴史を振り返ると…（※1）

- **~2010年頃：「脅威インテリジェンス = 脆弱性情報」という時代**
  - ゼロデイ攻撃を止めることを目的とした脅威インテリジェンスが中心

- **~2013年頃：脅威インテリジェンスに必要な概念が登場する**
  - IOC（Indicator of Compromise）の一般化（※2）
    - Mandiant社が、分析ツールOpenIOCを公開
  - MITRE ATT&CKフレームワークの登場
    - MITRE社により、攻撃手法（TTPs：Tactics, Techniques, and Procedures）の定式化
    - *“MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures…”*（※3）
  - NIST Cyber Security Frameworkの発表（※4）
    - セキュリティフレームワーク（特定・予防・検知・対応・復旧）を定式化
  - Mandiant社によるAPT1レポートの発表（※5）
    - 民間企業によるアトリビューション分析の実践
    - Pyramid of Pain (by David J Bianco) の提唱（※6）

（※1）大局的な流れを理解することを目的に作成
（※2）https://taosecurity.blogspot.com/2018/11/the-origin-of-term-indicators-of.html
（※3）https://attack.mitre.org/resources/faq/
（※4）https://www.nist.gov/cyberframework/history-and-creation-framework
（※5）https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units
（※6）https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

サイバー脅威インテリジェンスの歴史

- **~2017年頃：米国における 脅威インテリジェンスのブーム + 疲れ**
  - 2015年に、「Cybersecurity Information Sharing Act」が成立
  - SANSトレーニング（FOR578）+ 書籍などで、脅威インテリジェンスで何をすべきか、定式化され始める
  - （日本でも）ISACなどにおいて、脅威インテリジェンスの利用を開始し始めた時期
  - **Attributionに関する議論：**
    - DNC（Democratic National Committee）に対する攻撃が、APT28 + APT 29による攻撃だと発表される
      - *“Does a BEAR Leak in the Woods?”*
    - False Flagの可能性 + 民間企業は、アトリビューションをする必要がないという議論が行われる
      - *Leveraging Threat Intel Disinformation Campaigns*
      - *Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks*
    - こうした議論を経て、**政府 + メディア**と**民間企業**がやるべき内容の線引きがされたとともに、Attributionの有効性（False Flag + Disinformation）に対する懸念も醸成されてきた時期

サイバー脅威インテリジェンスの歴史

- **2018年以降～：**
  - CISA（Cybersecurity and Infrastructure Security Agency）の設立
    - https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency
    - 政府主導で様々な施策が開始される
      - KEV（Known Exploited Vulnerability）
      - Cybersecurity Alerts + Adversaries (YARAやThreat Actorに関するレポートを発表)
  - 各種政府機関も様々なガイドライン・ツールを公開開始
    - NSA Cybersecurity Advisories & Guidance
    - NASA Issues New Space Security Best Practices Guide
    - NSAが開発したマルウェア解析フレームワークGhidraの公開（2019年4月）
      - これ以前より、米軍ではオープンソースの活用に注目を置いており、2014年にはアメリカ陸軍研究所（ARL）が公表したインシデント対応フレームワークDshellなどがある。
        - » 参考）OPEN SOURCE ADVANTAGES ARE MAGNIFYING IN THE ARMY
        - » 参考）Open Source @ NSA

サイバー脅威インテリジェンスの歴史

- **歴史からの考察：**
  - 2013年頃までに、必要な概念が整理される
  - 2017年頃までに、民間企業がCTIとどう向き合うかが整理されてきた（＝「**共助**」の開始）
    - InfraGardなどでは、「草の根」レベルの官民連携が行われている
  - 2018年頃から、「**公助**」の開始
    - 米国政府の積極的な関与を開始（＝CISA設立）
    - 2018年度以降、FBI（” Cyber’s Most Wanted”）でも積極的にAPTグループを名指しし始める。
  - 米国でも、政府機関が主導的な役割を開始してから試行錯誤を重ね、CISAや各機関の役割が定まってきたと考えられる。

Part III : Wrap-Up

Wrap-Up

- **CTIの機能的視座：**
  - 民間企業が「リスク管理」という観点から、国のインテリジェンス機関が培ってきた技法をサイバー技術へ応用してきた経緯がある。
  - 脅威インテリジェンスのエコシステムにおいて、目的・対象範囲の違い、インセンティブの違いから「政府」が登場する機会がいままで限定的であり、民間の脅威インテリジェンスは独自の進化を遂げてきた経緯がある。
- **CTIの歴史的視座：**
  - 歴史的にみると、2017年度までに一通り脅威インテリジェンスの試行錯誤がされた後、2018年頃から政府主導による取り組みがなされてきた。
- **最後に：**
  - 制度設計・ガイダンスによるインセンティブ設計が重要！
    - 共有することにより、より情報が集まるインセンティブ（=マタイ効果）を生み出すような制度設計が重要
  - こうした現場での議論こそが、（真の意味で）有効な「脅威インテリジェンス」活用になるので、ぜひ皆様と様々な議論・情報交換をさせてください！

Thank You!