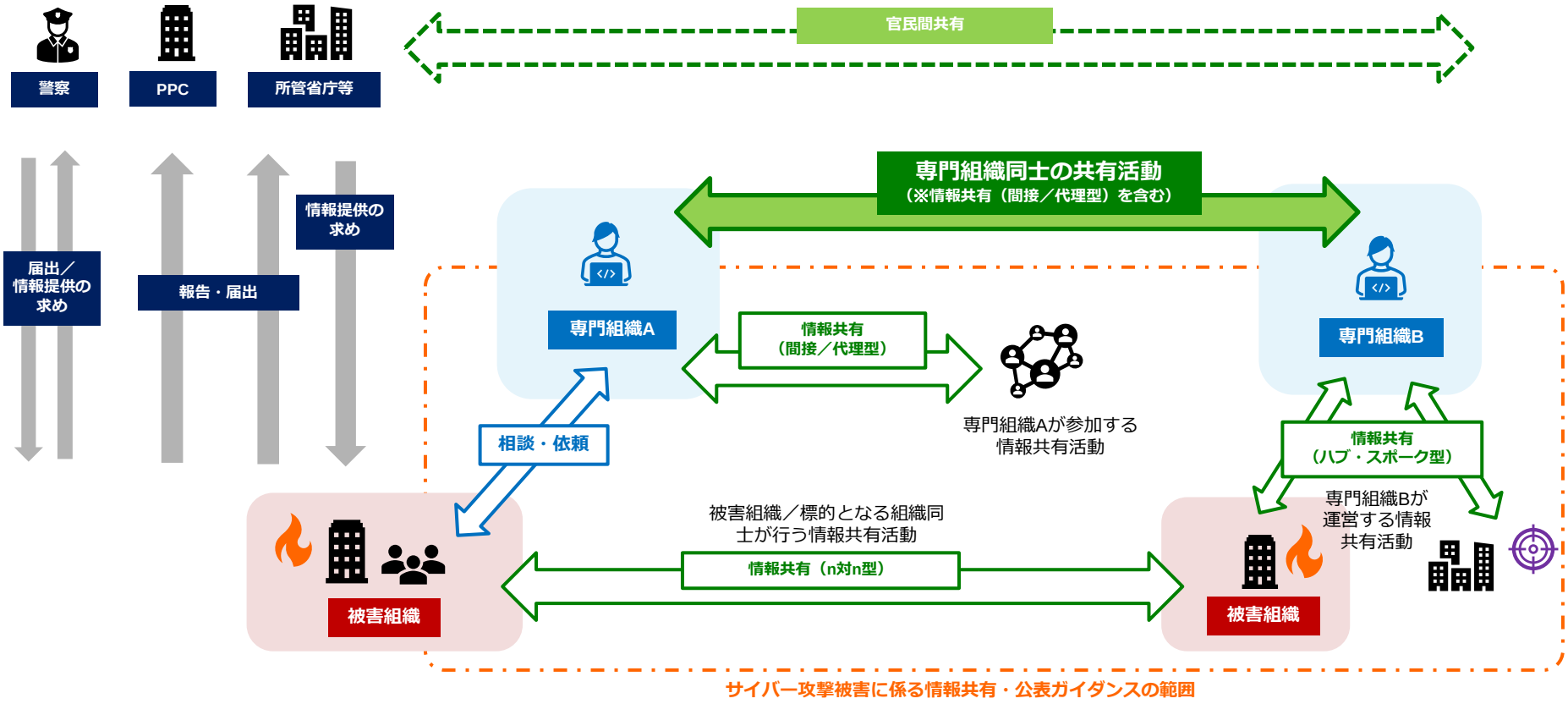
情報共有活動とNDAや専門組織間の競争性の諸論点

2023年5月15日

JPCERTコーディネーションセンター

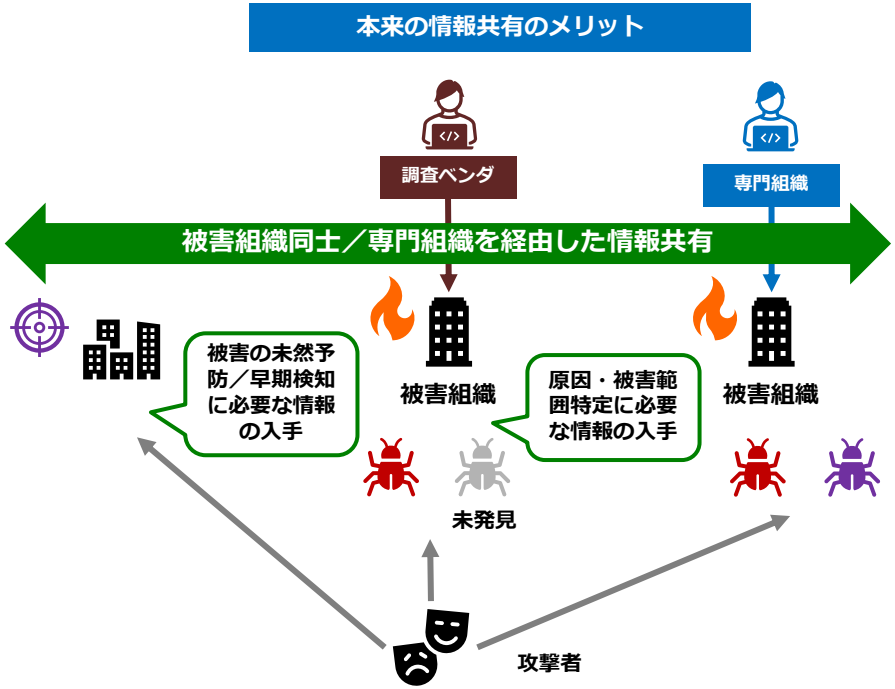
各「情報共有」の全体像

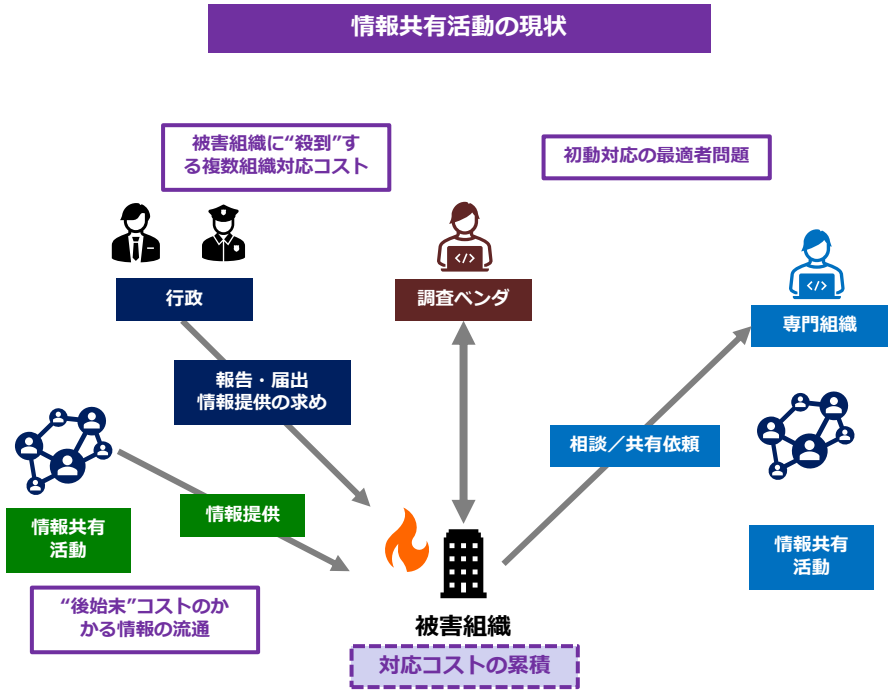
【用語に関する補足】
専門組織：専門機関やセキュリティベンダ（「サイバー攻撃被害に係る情報の共有・公表ガイダンス」における用語定義を準用）



被害組織から見た情報共有メリットと問題点

- 本来、情報共有により様々なメリットを得られるところ、現状は被害組織（あるいは標的となり得る組織）側の対応コスト／調整コストの負担が大きいため、情報共有活動そのものへのハードルが高い状態になっている



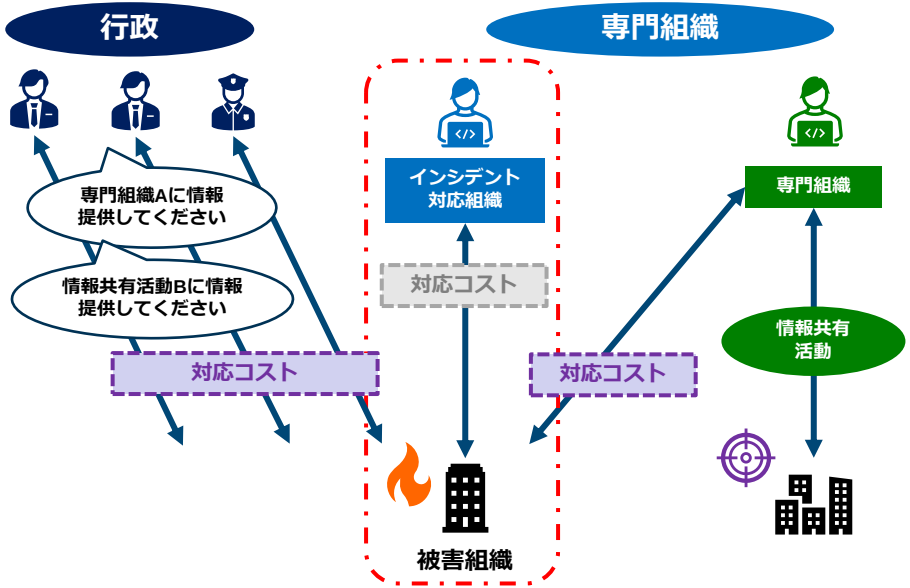


問題①：被害組織側の調整コスト負担

- 被害組織が（社会全体の）情報共有のための調整コストを負担している状況にある
- 被害組織自身の情報共有メリット ＜ 公益目的の負担（他の組織のメリットのための負担） ＋ 情報共有コスト
  となってしまっている。

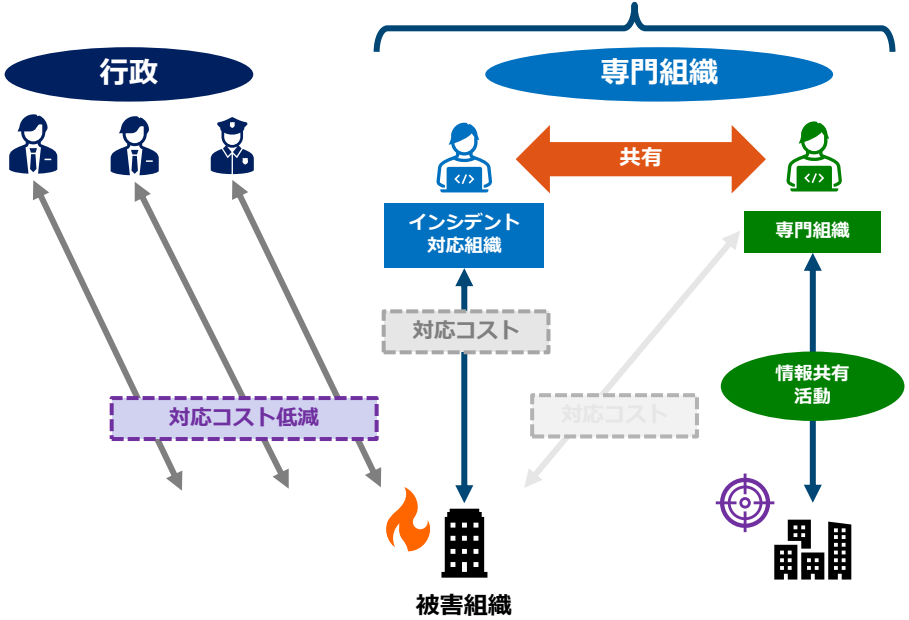
被害組織が調整コストを負担している現状

情報の共有に係る調整コストを被害者側が負担している状況



被害組織の調整コスト削減案

少なくとも攻撃技術情報の共有コスト負担は軽減可能



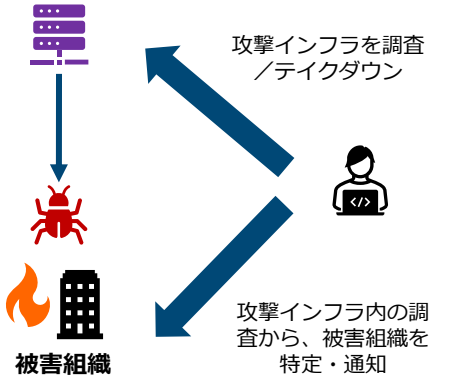
問題②：事案対応の最適者が調整／修正されない問題

- ファーストレスポンダー（「最初に被害組織から相談を受けた組織」や「最初に被害組織にコンタクトした組織」）が当該攻撃に十分な知見を有する事案対処の最適組織とは限らない
- ファーストレスポンダーは自組織に知見が不足しているかどうか知ることが難しい（他組織と共有して初めて知ることができる）
- 事案対処にあたる組織間の情報共有により知見が”補充”されるか、最適な対処組織に“交代”するかの調整／修正が必要

事案対処の最適者である例

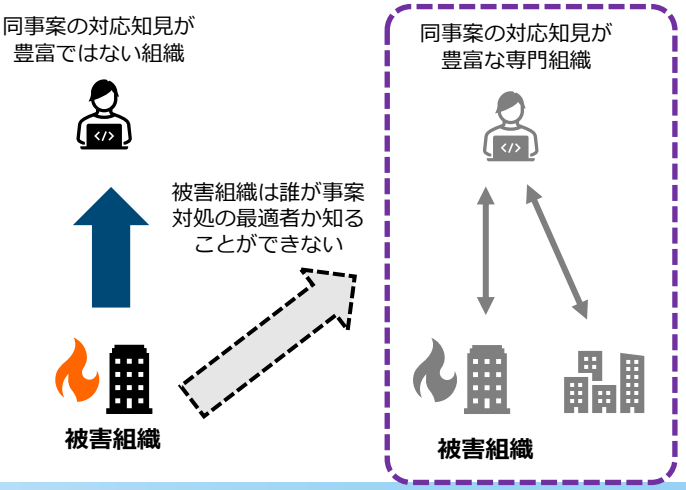
・攻撃インフラを調査／テイクダウンした組織が被害組織に通知するケース
・対処組織は当該攻撃に関する十分な情報／知見を有しているので、個別被害組織の支援に十分対応できる

※ただし、当該組織も「テイクダウンした別の組織から断片的な情報提供を受けただけ」であれば最適者とは限らない



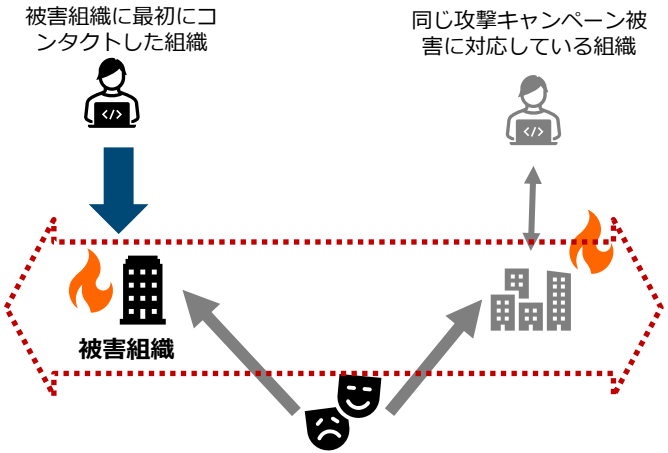
事案対処の最適者でないケース

・相談窓口を設けているからといって、あらゆる事案対応の知見をすべて有しているとは限らない
・被害組織から最も“近い”相談先組織（（セキュリティ）ベンダ、専門機関等）が事案対応の最適者とは限らない



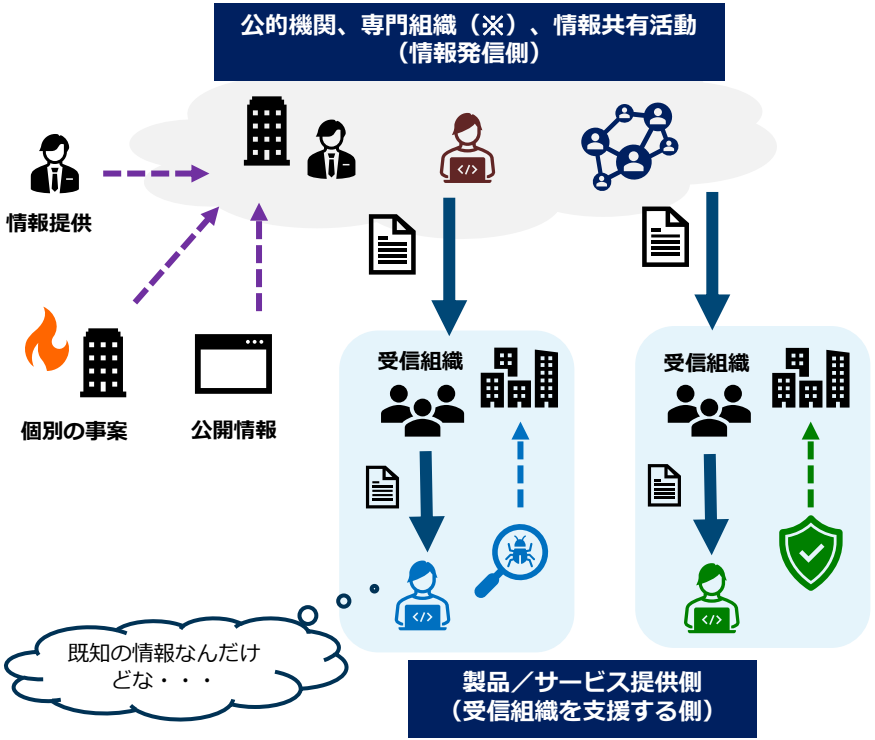
事案対処の最適者でないケース

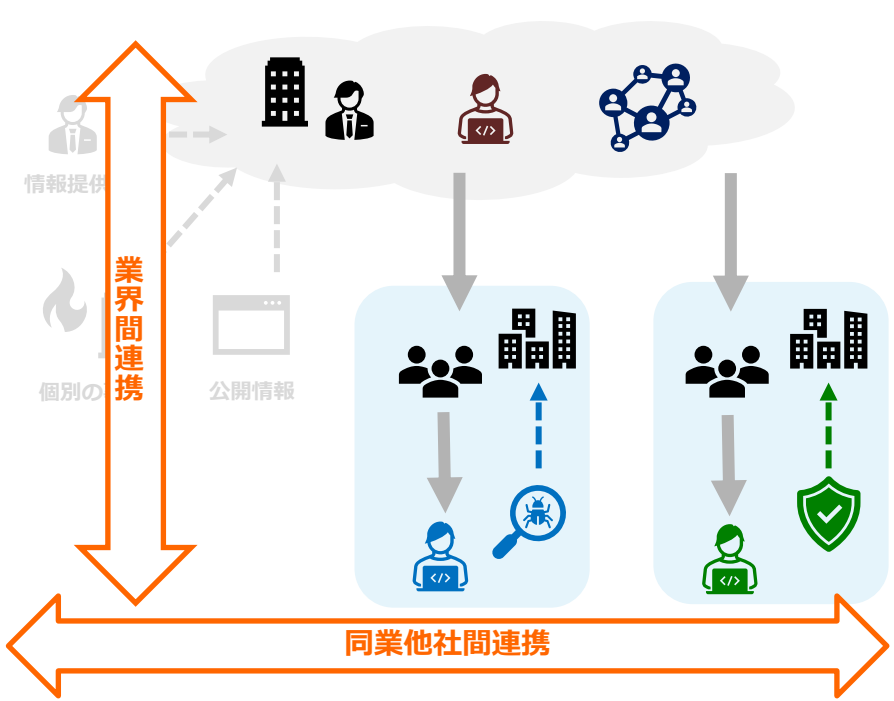
・単独の専門組織だけでは、攻撃キャンペーン全体の範囲を知ることは困難なため、そもそも十分な知見を持っているのかどうか知ることができない



問題③：処理コストのかかる情報の流通状態

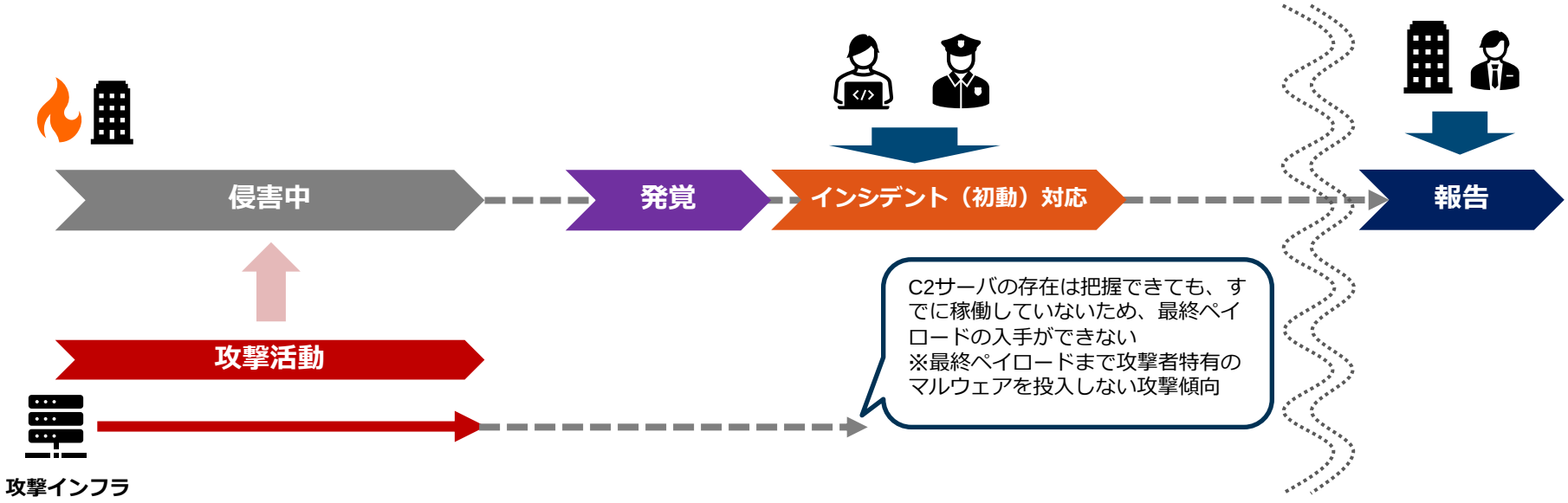
- 本来、情報共有活動に必ずしも流さなくてもよい情報も流れることによる受信組織側の対応コストが発生しているのではないか？（セキュリティ製品／サービス側で対応できている状況を情報発信側が把握できていない）





問題④：「被害現場」依存からの脱却の必要性

- 高度な攻撃の大半は攻撃活動後に認知されるため、その後のタイミングで専門組織や警察等が被害現場に情報を取りに行っても、攻撃インフラの全容や攻撃の全容（※最終ペイロードなど）が判明しないケースが多い
- かつ、インシデント対応の初動段階で複数の組織が現場に“殺到”することで、被害組織の対外対応コスト負担が増えてしまい、被害組織自身の調査が進まなかったり、各組織との連携による調査・分析が進まず、全体として非効率化する。
- （製品）検知情報やファーストレスポンダーが得た技術情報の複数（専門）組織間での共有の活用が必要



なぜ専門組織同士／ベンダ同士の共有が必要なのか

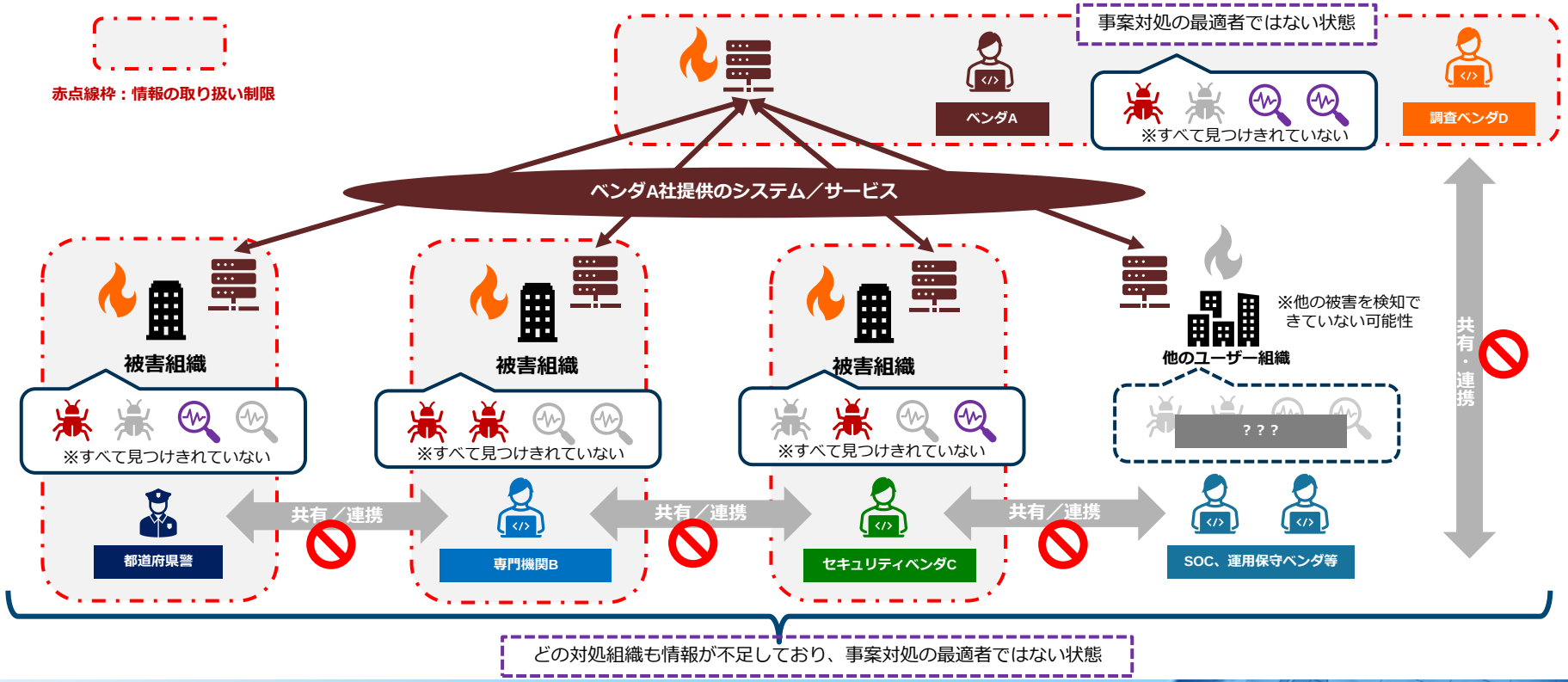
- 問題①：被害組織側で情報共有に必要な調整コストを負担している
- 問題②：「事案対応の最適者」が調整／修正されないことで被害組織が不利益を被っている
- 問題③：情報共有に適さない情報の流通による“後始末”コストが発生している
- 問題④：あらゆる組織が被害組織に情報をもとめて「殺到」する

⇒情報の流通に不必要なコスト／過大なコストが必要なため情報が流れない

⇒情報が流れないことで各プレイヤー間に情報の非対称性が発生し、各プレイヤーの活動・知見が修正されず、また、全体最適化もされない

専門組織同士の共有ができず事案対処に難航するケース

- 事案対処にあたる各組織間の情報共有がないため、各対処組織の情報（知見）が限定的であり、どの組織も事案対処の最適者でない状況にあり、個別のインシデント対応も不十分であり、事案全体の対処も不十分



NDAにおける情報共有活動との“摩擦”点

秘密情報に含まれない情報

（1） 開示又は知得の時点で、既に公知となっていた情報。
（2） 開示又は知得の後に、受領当事者の責めに帰すべき事由によらず公知となった情報。
（3） 開示又は知得の時点で、受領当事者が既に正当に保有し、且つ、開示当事者その他の者に対して秘密保持義務を負っていなかった情報。
（4） 受領当事者が、正当な権限を有する第三者から、秘密保持義務を負うことなく入手した情報。
（5） 開示当事者の秘密情報を利用することなく独自に開発した情報。

秘密保持義務の例外

法令の定めにより、官公庁等の政府機関又は裁判所等から秘密情報の開示を要求された場合で、かかる要求による開示が受領当事者の義務である場合には、受領当事者は、要求を行った政府機関又は裁判所等に対し、義務が課される範囲内で秘密情報を開示することができるものとする。

①情報の「公知性」判断について

被害現場で見つかった情報（※）がすべて「秘密情報」として扱われているケースにおいて、情報受領側（（セキュリティ）ベンダ）が知り得た情報を外部に共有／提供することができない

※当該被害現場以外に同じ情報が存在していることを「公知」と解釈するかどうか、という論点がある

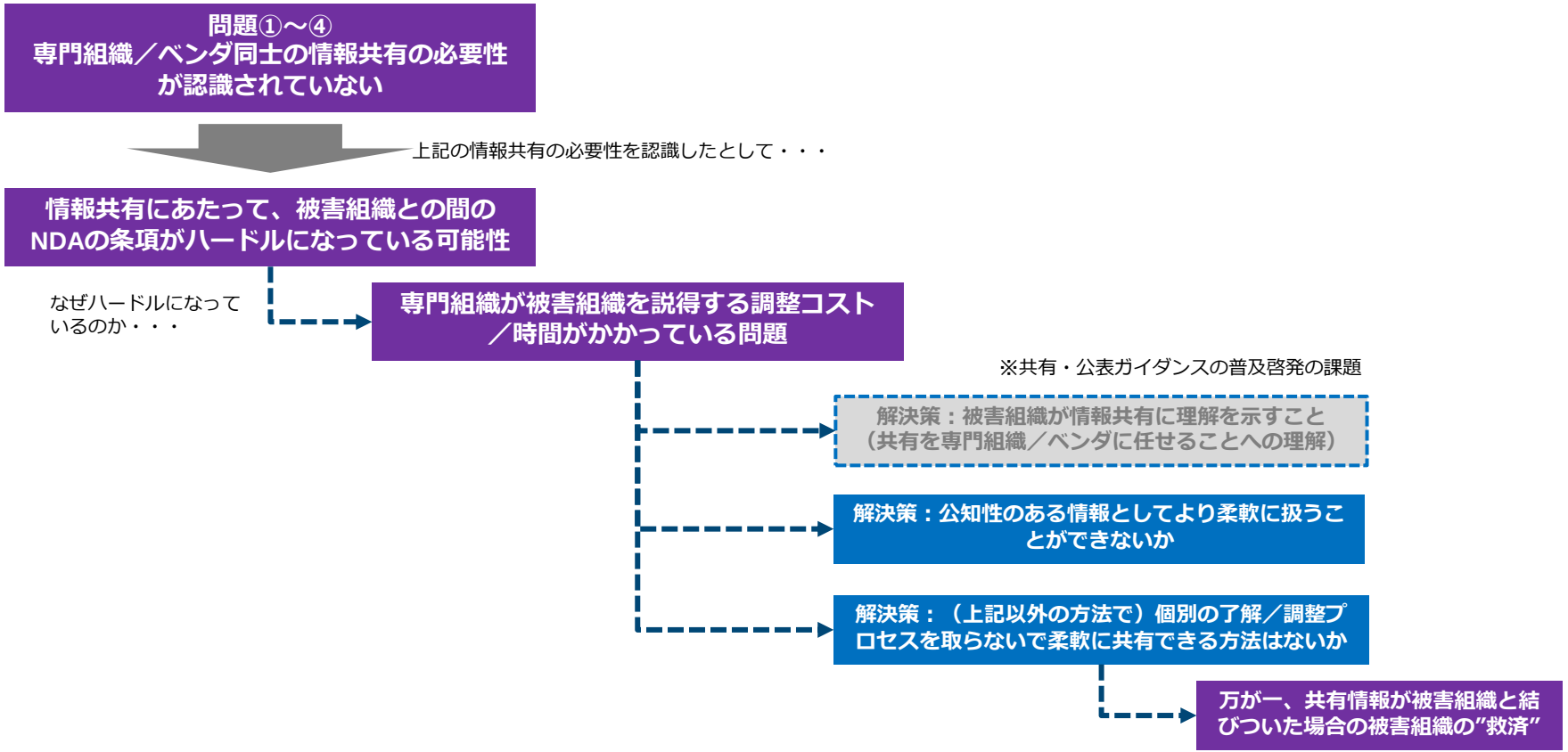
②個別の調整により秘密情報から除外、あるいは第三者提供を認めた場合

③法令の定めによる開示要求について

行政機関等からの法令に基づく秘密情報開示の求めに対して、契約相手方（開示当事者）の同意なく情報開示ができるのか

※左記はJPCERT/CCがインシデント対応時等に用いているNDAのひな型（の類型のうちの一類型）の一部を抜粋・加工したもの

問題と検討したい解決策の構造



議論の前提：脅威情報の流通について

- 脅威情報を取引可能な「財」として捉えることができるのではないか
- 社会全体でみると、公共財のように見えるが、情報を供給する側から見ると、競合性／排除可能性がある、共有資源のように見える

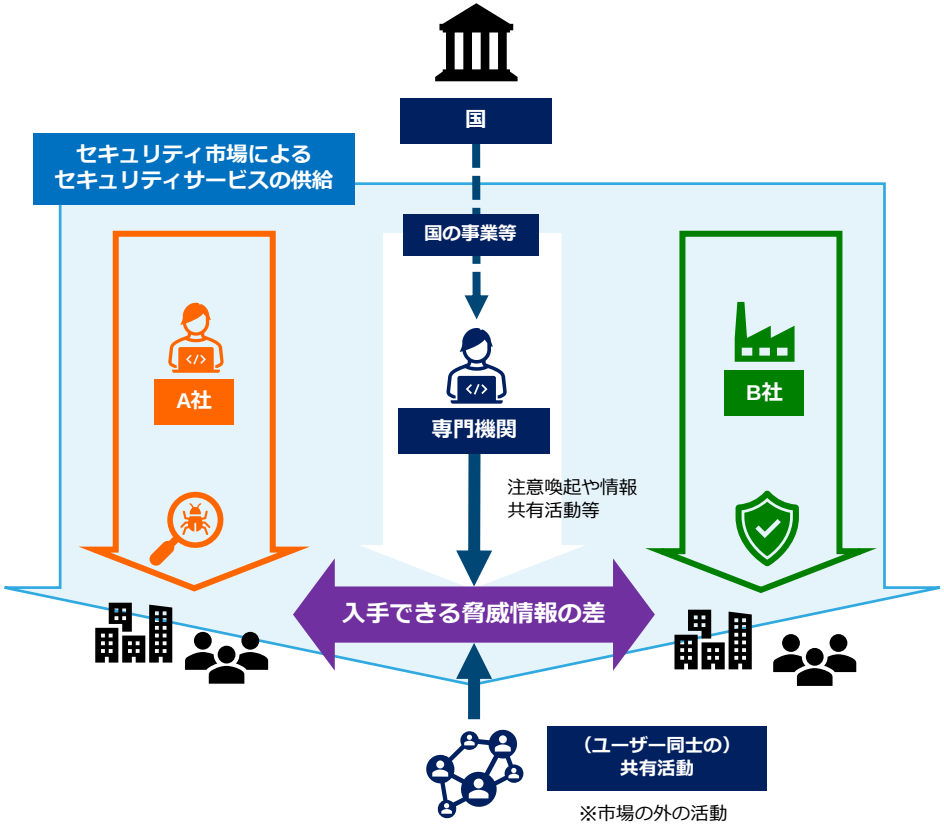
  ⇒いわゆる「メリット財」（医療や教育サービスなど、競合性／排除性があるが、公益性がある（正の外部性がある）に近いのではないか？

		消費において競合的か	
		競合する	競合しない
排除可能か	可能	**【私的財】** ・食品、衣服等	**【クラブ財】** ・消防
	不可能	**【共有資源】** ・漁業資源 ・環境 **＜資本財（セキュリティ企業側）として見ると・・・＞** **脅威情報**　⇒　排除可能であり、（基本的に）共有されると価値／受益が変化してしまう	**【公共財】** ・国家防衛、警察 **＜消費財（受信組織側）として見ると・・・＞** **脅威情報**　⇒多くの組織間で共有してもその価値／受益は変わらない

脅威情報は
メリット財？

「マンキュー経済学Ⅰミクロ編（第4版）」や松村良之「財としての情報とその法的保護－「法と経済学」からのアプローチ」（田村善之編「情報・秩序・ネットワーク」収録）などから筆者作成

議論の前提：脅威情報の流通について



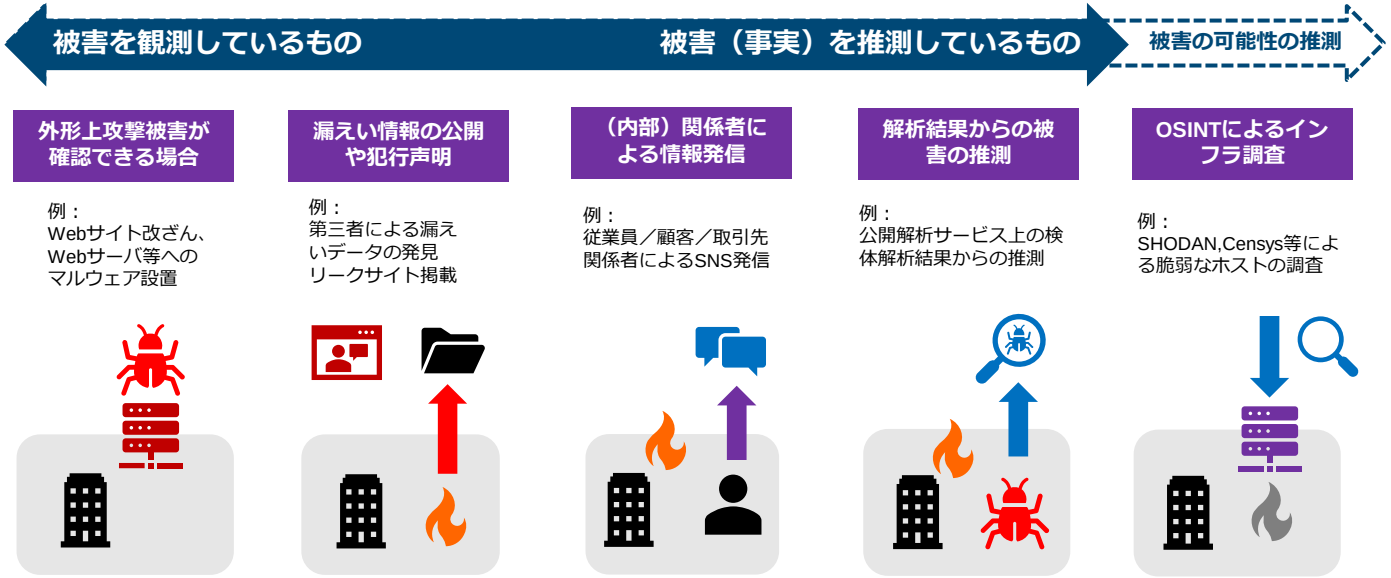
- 基本的にセキュリティサービスは民間事業者により市場を通じて供給されており、企業間の競争があることでよりよいサービスが適切な価格で提供される
- 脅威情報の供給も大半は私的財として供給されているところ、特定の攻撃においては、情報の不均衡が発生し、ユーザー間で不利益が発生する（“市場の失敗”への是正措置として情報共有活動が必要になるケース）
- 脅威情報の流通にはメリット財的な性質があるため、その流通は企業だけでなく、公的機関による提供も混在した、混合的市場となっている（※市場の失敗を是正する効果も兼ねている）
- セキュリティサービスを供給する企業間の競争性も維持しながら、メリット財としての脅威情報の流通（情報共有活動）を効率的に行うために、現在存在している過剰／不要な取引コスト（※前述の問題①～④）を軽減しなければならない

攻撃技術情報の性質と公知性

未公表被害が公開情報となる場合

共有・公表ガイダンス検討会
資料から

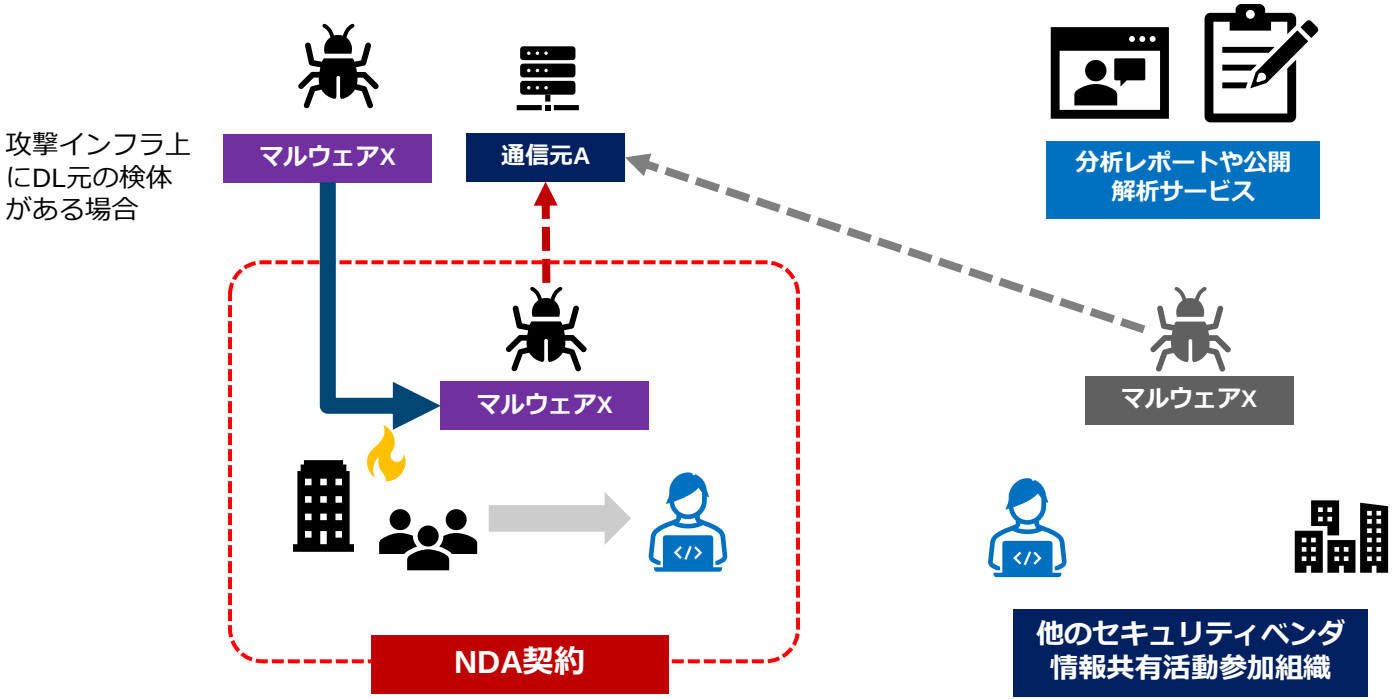
- 攻撃被害を示す情報（漏洩情報、犯行声明等）が意図せず、被害認知前や公表前に公開情報となって拡散する場合がある
- 公表前の被害について第三者が推測可能な情報が公開情報として存在する場合がある
- 被害が今後発生する、あるいは発生しているかもしれない、と推測できる情報が公開情報として存在している場合がある（※実際に被害が発生しているかどうかは別）



「公開情報」とは何か

共有・公表ガイダンス検討会
資料から

- 「非公開」情報というのは、対世的秘密（Confidential）なのか、絶対的秘密（Secret）なのか



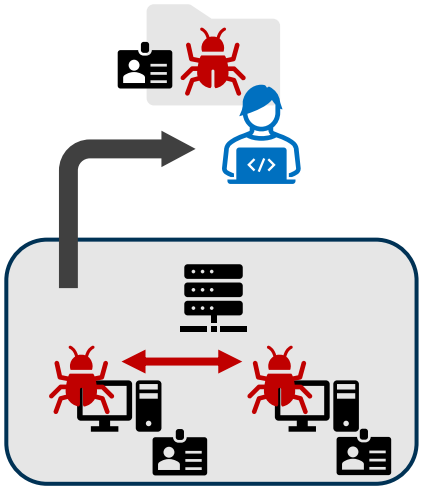
検体解析情報から被害組織が推測されるケース

共有・公表ガイダンス検討会
資料から

ケース①

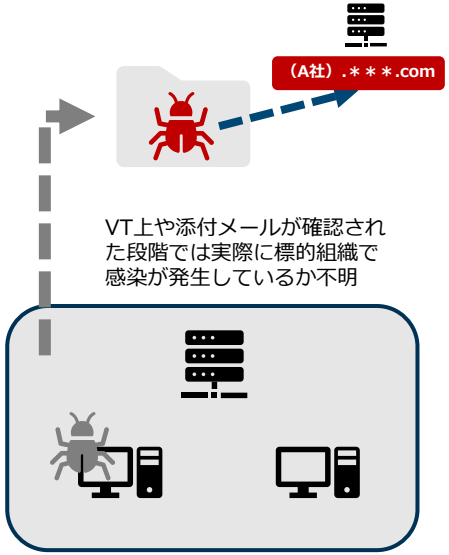
感染時に収集したクレデンシャル情報を含むケース
⇒ID＝メールアドレスのドメインから被害組織が推測されうる

【例】　Olympic Destroyer
のVT上にあがった検体



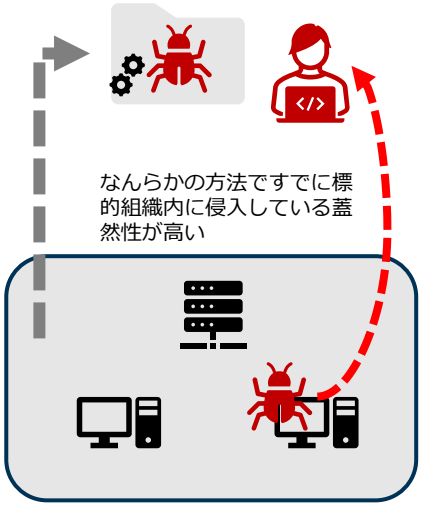
ケース②

検体内部やハードコードされたC2のドメイン名内に標的組織の略称（ドメイン名など）を含むケース
※検体だけでなく通信先情報だけでも推測できる場合もある



ケース③

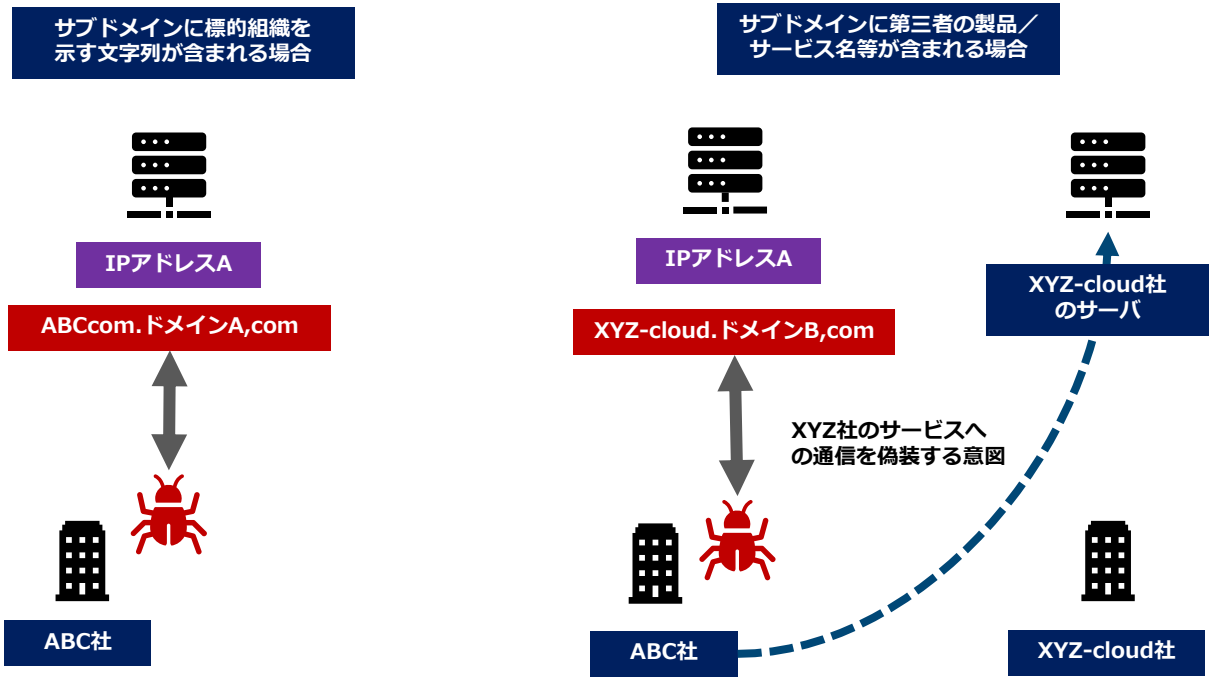
標的組織のプロキシサーバなどNW内部の設定情報を検体内に含むケース



攻撃インフラの調査から被害組織が推測されるケース

共有・公表ガイダンス検討会
資料から

- 被害組織を推測させる情報を含む場合がある

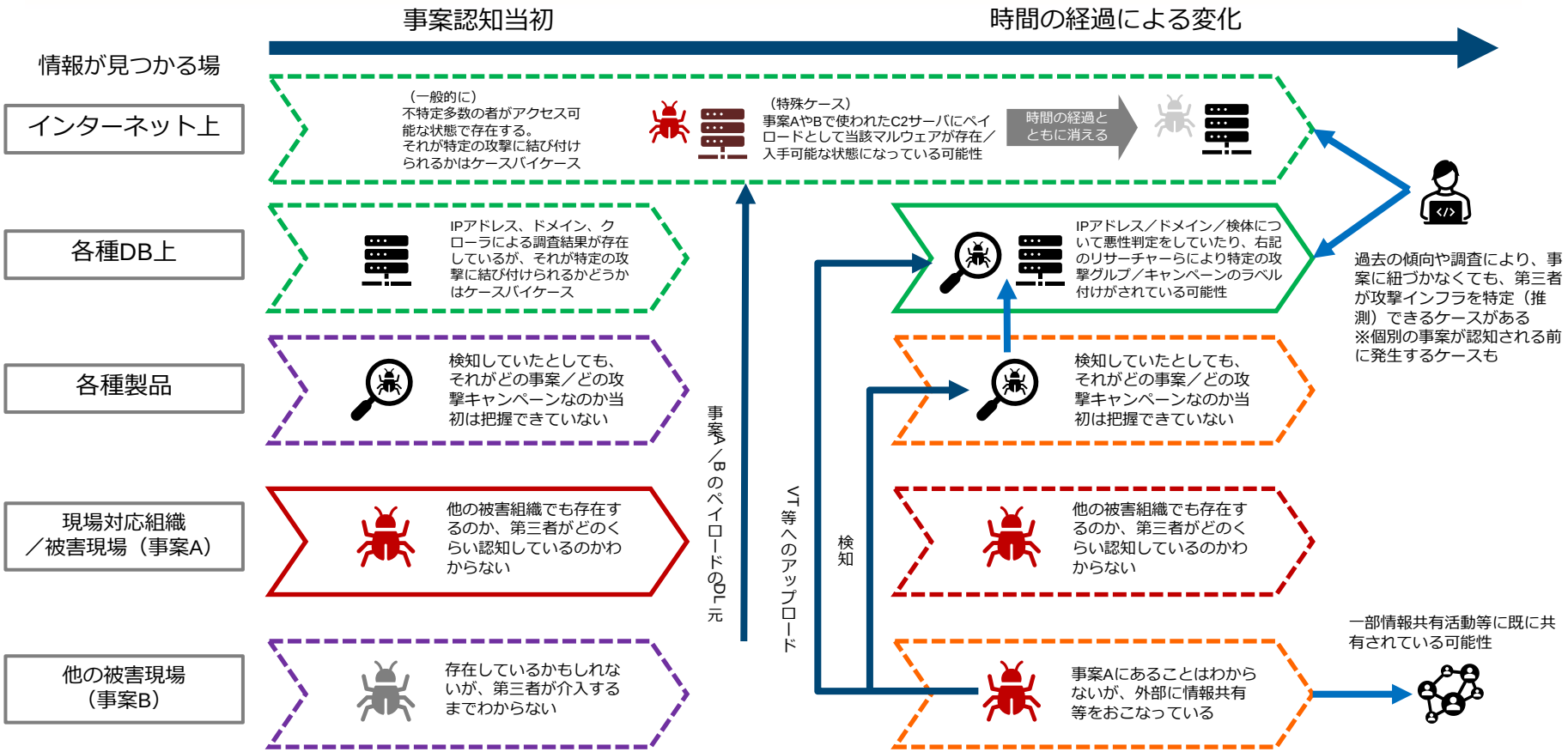


技術情報の公知性に係る時間軸上の変化

時間の経過

	情報収集サービスで無差別に収集される情報か	左記収集において、悪性情報（悪用されていることを示す情報）と紐づくか	第三者が悪性情報と紐づけることが可能か	被害発覚時点で第三者が同じ情報を入手している可能性	他の被害先で同じ情報が確認されている可能性	時間の経過とともに情報が公知になる可能性
通信先のIPアドレス／ドメインに関する情報	○ WHOIS情報、Passive DNSなど	△ ※（公開）マルウェア情報と紐づいたり、攻撃者のドメインの命名傾向や稼働しているサービスなどか悪性と推測できるケースはある		△ ※個別事案には紐づかないが、同じ技術情報を第三者が入手している場合がある	○ 基本的にほとんどのケースで想定されうる	○ レポート公表等を通じて
サーバに関する情報	○ Shodan/Censys等の検索エンジン	△ （同上）				
検体	△ ※基本的に被害者等がサービスにアップロードが必要	△ ※マルウェア判定程度	○	△ ※同様の攻撃による他の被害組織からアップロードされた場合		
TTP	×	—	—			
事案の存在に関する情報	△ アンチウィルス製品による検知などで被害発生の可能性が推測可能		—	—	—	○ 被害組織による公表等を通じて

技術情報の公知性に係る時間軸上の変化



「秘密」情報の整理について

- 地方公務員法第三十四条1項、国家公務員法第百条、「職員は、職務上知り得た秘密を漏らしてはならない。」
- 最高裁昭和48年（あ）第2716号

  ―国家公務員法一〇〇条一項にいう「秘密」とは、非公知の事項であつて、実質的にもそれを秘密として保護するに価すると認められるものをいい、国家機関が単にある事項につき形式的に秘扱の指定をしただけでは足りない。

形式秘

秘密の取扱いをすると指定された事項

実質秘

その性質上、非公知性と要保護（秘匿）性を有する事項

Secret

・いかなる状況でも秘匿すべきもの
・例：特定秘密、営業秘密、投票の秘密、入札情報、インサイダー情報、公益通報情報、通信の秘密のうち通信内容

Confidential

・情報の授受当事者間の関係性に依存するもの
・プライバシー関連情報、通信の秘密のうちログなどのメタ情報

引用：林紘一郎「情報法のリーガル・マインド」92頁

「秘密」とは何か

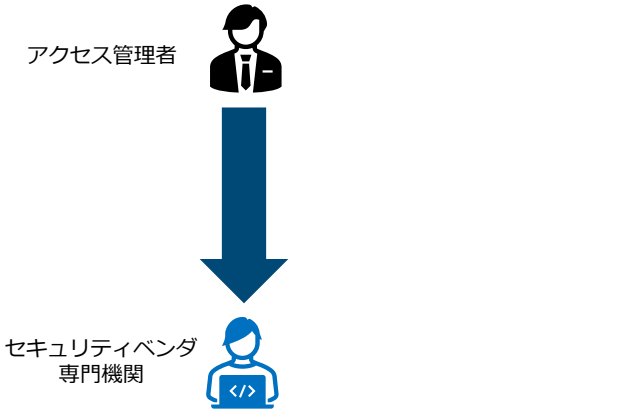
- 「一般に知られていない事実であって、かつ、知られていないことにつき利益があると客観的に認められるものをいう」（有斐閣「法律用語辞典　第5版」）
- 刑法134条（秘密漏示罪）：「少数者にしか知られていない事実で、他人に知らせることが本人の不利益となるもんである」（前田雅英「刑法各論講義（第7版）」125頁）

不正アクセス禁止法 第九条に係る「秘密」情報

一般的なインシデント対応相談

自ら／委託により専門的知識、技術を有している場合

不正アクセス行為によるものが判然としない場合

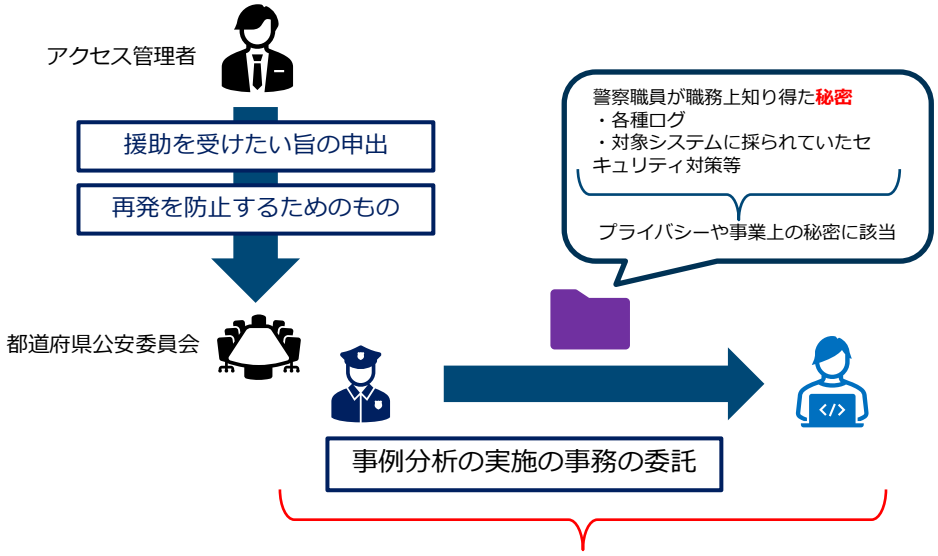


アクセス管理者の私的な被害回復？や原因特定を目的としたもの

不正アクセス禁止法9条に基づく場合

再発防止策を講じようとしても、そのための専門的知識、技術を有していない場合

不正アクセス行為が行われたと認められる場合



秘密保持義務の対象には「事例分析の結果判明した不正アクセス行為の具体的な手口等」が含まれる

犯罪の防止の観点から都道府県公安委員会に一定の責務を課したもの

「公知性」「秘密」の定義

- 営業秘密の「公知」性（不正競争防止法）
  - ○「公知」：一般的に知られた状態、または容易に知ることができる状態
  - ○ある情報を知った特定の者が当該情報について事実上秘密を維持していれば、なお非公知と考えることができる場合もある（経済産業省「営業秘密管理指針」17頁等）

- 特定秘密（特定秘密保護法）
  - ・別表該当性
  - ・非公知性
  - ・特段の秘匿の必要性

- 職務上知ることのできた秘密（国家公務員法第100条）

「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。」

※地方公務員法34条（秘密を守る義務）

※ほか刑法134条（秘密漏示）

医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、六月以下の懲役又は十万円以下の罰金に処する。

- サイバーセキュリティ協議会における「秘密」（サイバーセキュリティ基本法第17条4項）

「協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない。」

【参考】特定秘密保護法

■ 「公になっていないもの」（逐条解説（内閣官房））

特定秘密の指定の要件の１つである非公知性、つまり、不特定多数の人に知られていない状態であることを規定するものである。「公になっていないもの」との概念は、公にされたか否かとは別個の概念と解すべきであり、例えば、特定秘密に該当する情報を壁新聞に掲載して公道の傍らの掲示板に掲示する行為は、特定秘密を公にした行為であるが、たまたま警察官がこれを早期に発見して撤去し、誰の目にも触れなかった場合には、当該情報は「公にされた」ものの、いまだ「公になっていないもの」として、非公知性の要件は失われないものと解される。他方、例えば、当該情報と同一性を有する情報が、報道機関、外国の政府その他のものにより公表されていると認定する場合には、たとえ我が国の政府により公表されていなくても、「公になっていないもの」との要件を満たさず、特定秘密の指定は解除されることとなる

■ パブリックコメントにおける解説

非公知性の要件は、特定秘密に限らず国家公務員法上の「秘密」等、秘密全般で共通の要件であり、これまでも、現に不特定多数の人に知られていないかにより判断されてきたところです。非公知性の判断は、個別具体的な状況を踏まえて行う必要がありますが、特定秘密と同一性を有する情報が現に不特定多数の人に知られるに至ったと認定する場合には、非公知性が失われたこととなるものと考えられます。 報道機関等が公表した情報がある場合、これが真に特定秘密と同一性を有するものであるか、特定秘密が非公知であるか否かを客観的に判断する（「認定する」）ことが必要となりますが、その主体は特定秘密を管理する行政機関の長が相応しいと考えます。特定秘密である情報を本来保有していた外国の政府が公表した場合は非公知性が失われますが、それ以外の外国の政府が公表する場合は、この判断が必要になります。 なお、内閣府独立公文書管理監が特定秘密の指定等の検証・監察を行う中で、御指摘の点についてもチェックを行うこととなります。

【参考】情報の「有効期限」

秘密の有効期限と管理責任

ところで秘密に関して世間一般にある誤解は，一旦秘密と指定されたら，その情報は永久に秘密扱いされるもの，という見方です．実態は全く逆で，秘匿には必ず管理限界や賞味期限（両者を合わせて「有効期限」）があるから，いずれは公開されざるをえません．つまり原則と例外が逆で，「情報はすべて公開の運命にあり，保有する主体が秘密を保つ努力する場合に，一定の期間に限り秘匿することができる」と考えるべきでしょう．先に挙げた，秘密を保護する前提としての３条件の中に，秘密管理性が入っているのは，このような意味に解するべきです．秘密として例示したものの中でも，入札情報やインサイダ情報には，このような「秘密の有限性」という特徴がよく現れています．

これを言い換えれば，図表 2-1 で示した「全体の中で法的な保護の対象になる情報は限られている」という理解が，秘密を扱う場合の原点でもあることを意味しています．また政府機関が保有する情報に関していえば，およそ税金で取得・加工・保存された情報は原則として国民のものであり，秘密として管理される期間を過ぎれば，国民には「知る権利」があると考えるのが妥当でしょう．現に，最も厳格な秘密管理システムを定める特定秘密保護法においても，以下のような規定が置かれていて，秘密の指定が時限的なものであることを明示しています．

①指定期間は，原則として５年である（同法４条１項）．

②延長は可能であるが，５年ごとに延長措置を講じなければならない（４条２

- 参照：林紘一郎『情報法のリーガルマインド』101頁
- 秘匿における
  「管理限界」
  「賞味期限」
  （※両者合わせて「有効期限」）

「コンフィデンシャリティ」の概念

- 脅威情報に秘密性があるのではなく、両者間の関係における「コンフィデンシャリティ」の問題なのではないか？

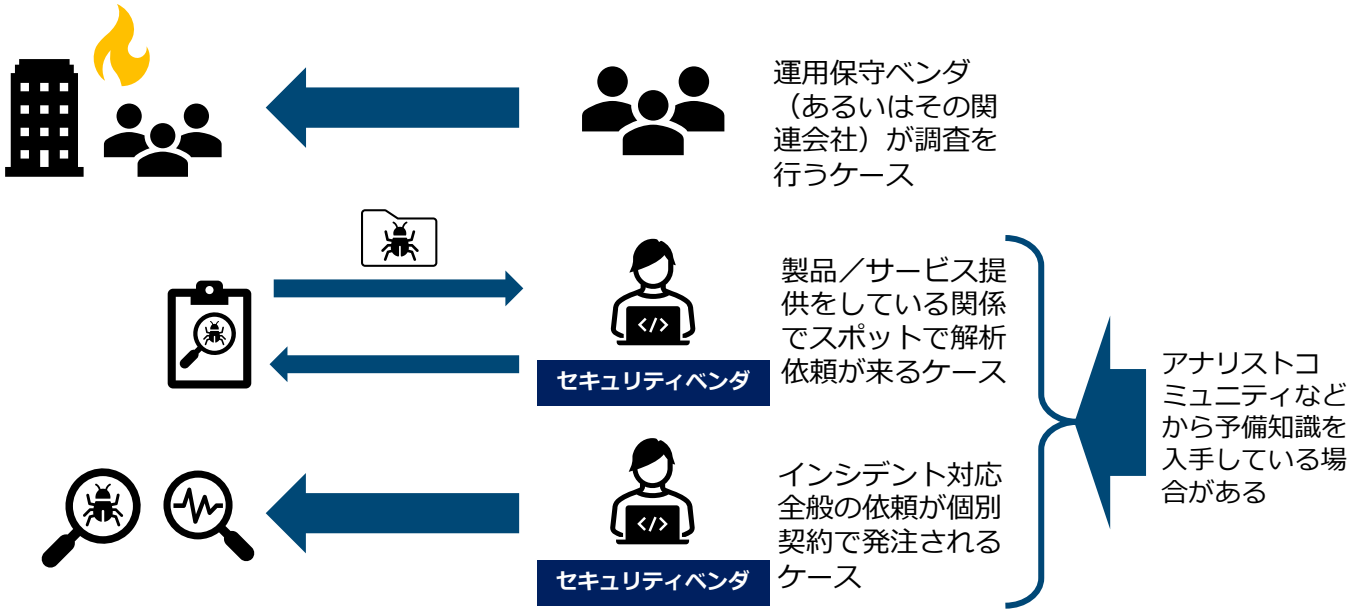
- 「コンフィデンシャリティの約束とはつまり、明示または黙示を問わず、情報およびその入手経路が開示されないという理解に基づいている」（池田公博『報道の自由と刑事手続き』243頁 ニューヨーク州法の適用について、Wolf v.People（ 329 N.Y.S.2d 291）の解説を紹介）

個別の了解／調整プロセスを取らないことによるリスクの問題

運用保守ベンダ、セキュリティベンダ

共有・公表ガイダンス検討会
資料から

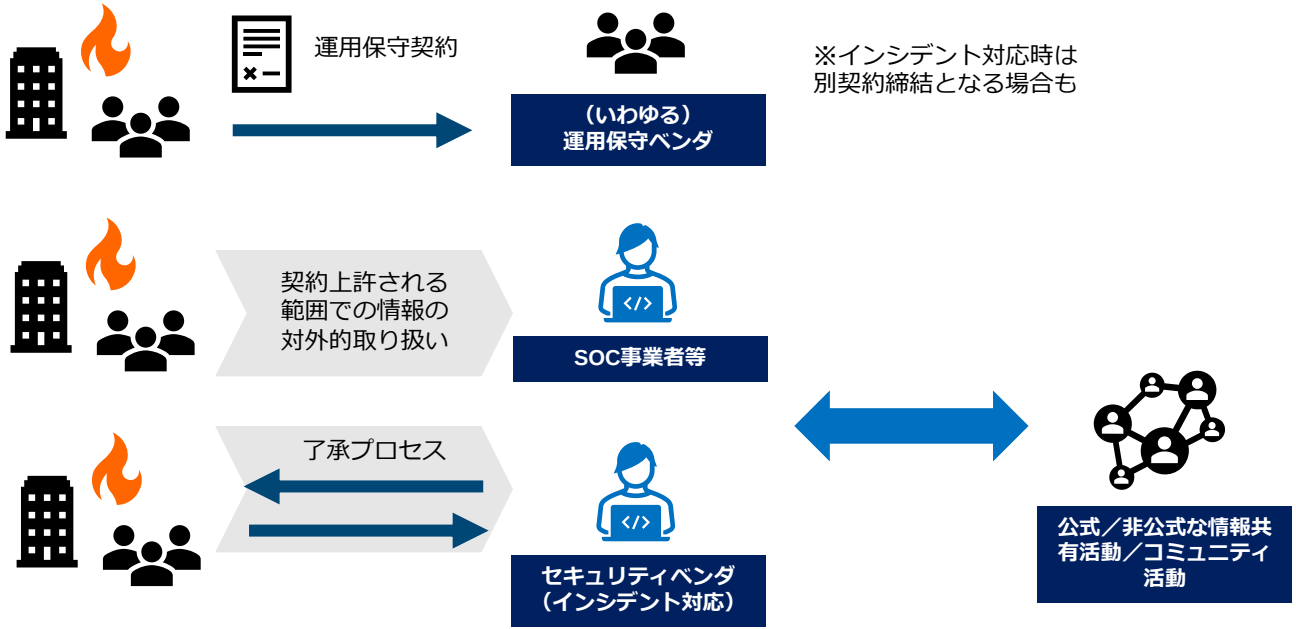
- ※あくまで弊センターから見たケース
- インシデント対応といっても、実際には異なるスタンスでの関与の仕方をしているため、「触れられる情報」「外部に共有／活用できる範囲」はケース毎に差が出る



（セキュリティ）ベンダの情報共有活動

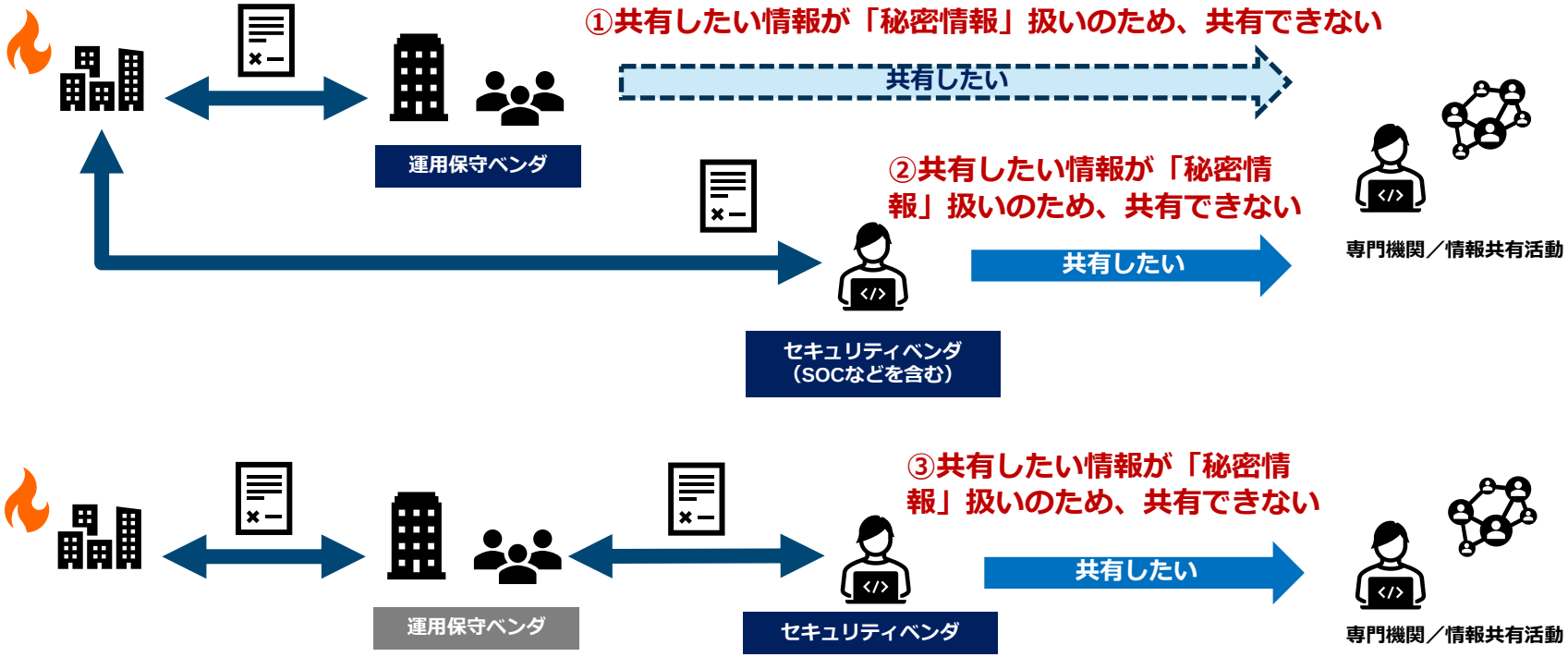
共有・公表ガイダンス検討会
資料から

- 主に事案対応にあたるセキュリティベンダ間で情報共有が行われる場合がある
- セキュリティベンダとして被害対応、全容解明に必要な情報を得る目的であったり、被害組織の“代理”として情報共有によるフィードバック情報を得ることが目的



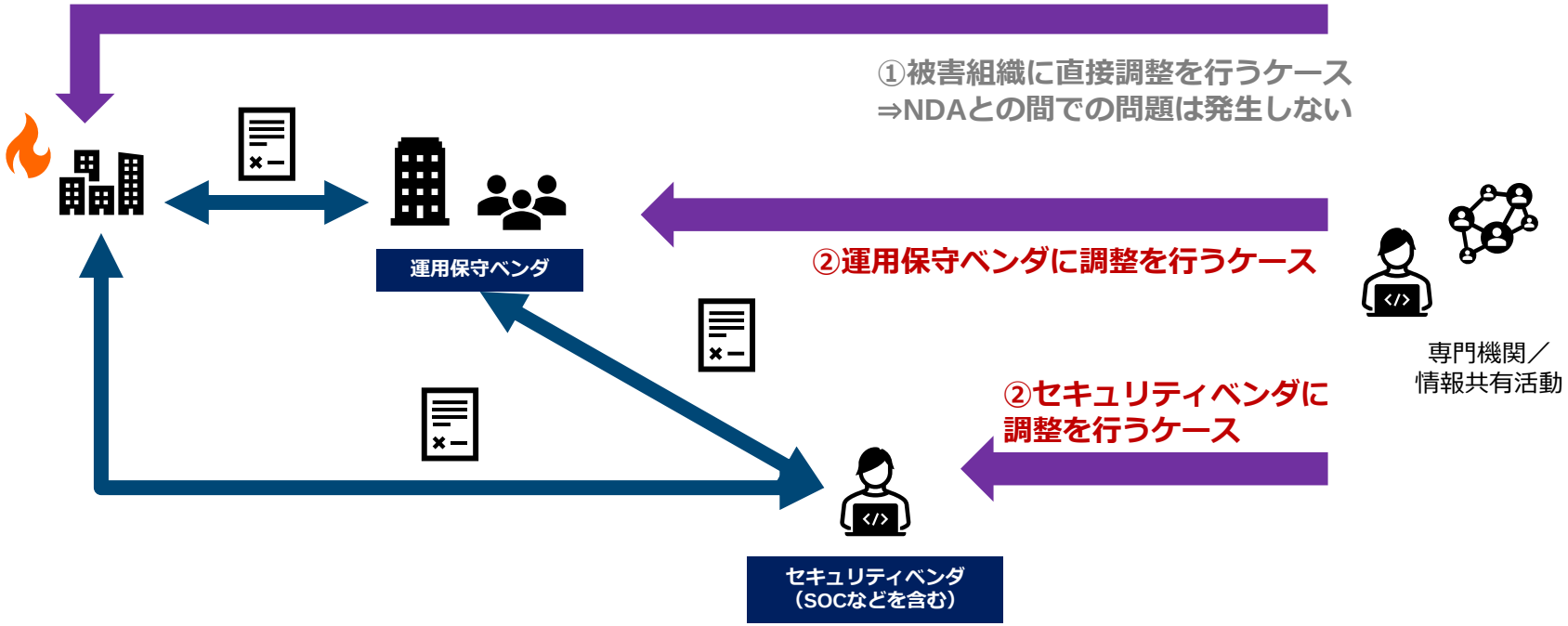
外部へ情報提供したいと考える事業者がNDA問題にぶつかるケース

■ 基本的に「共有して情報交換をしたい」動機を持つ②、③のケースが多く、①のケースは少ない。
（③のケースではセキュリティベンダは被害組織の運用保守ベンダのコントロール下にある）



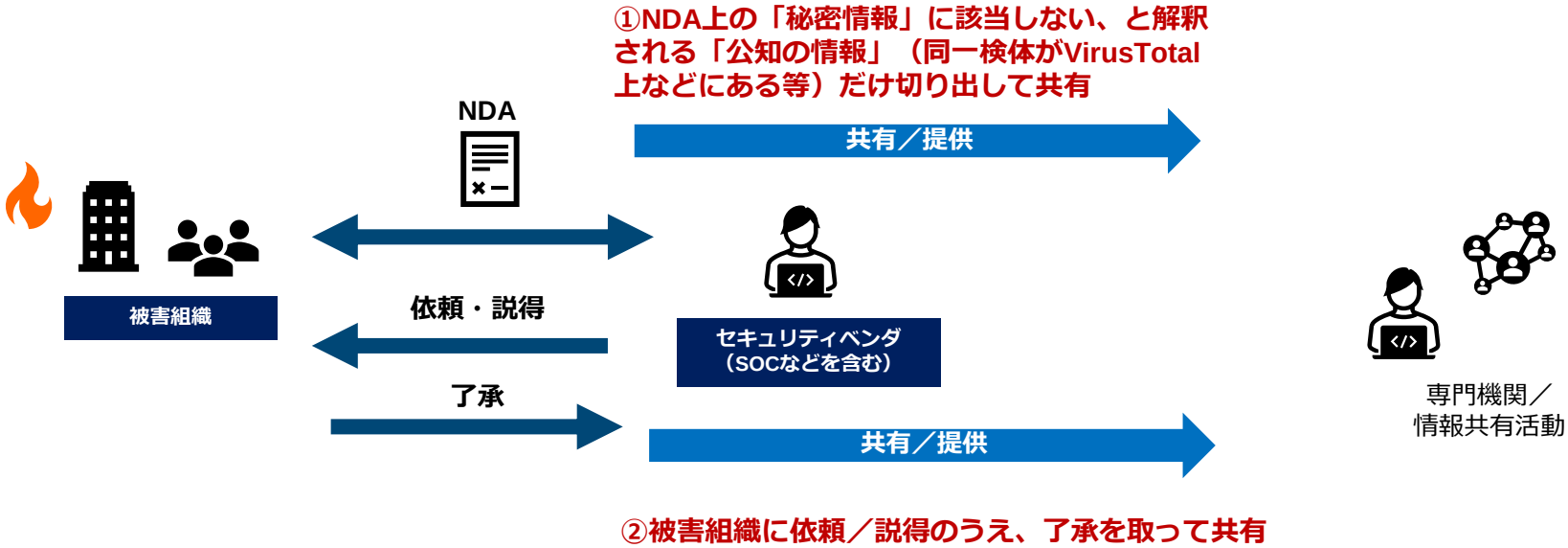
外部からの情報提供の求めに対してNDAが問題となるケース

- ②の場合、専門組織同士の情報共有活動などにおいて、「ある攻撃情報を匿名の被害現場で“見ている”」旨のメタ情報的情報？は共有できているケースが想定されるため、（セキュリティ）ベンダ側には「共有／提供しよう」という意思が既にある（前ページ③とほぼ同じ状況）



セキュリティ専門組織が外部との共有を行う際の実際の対応

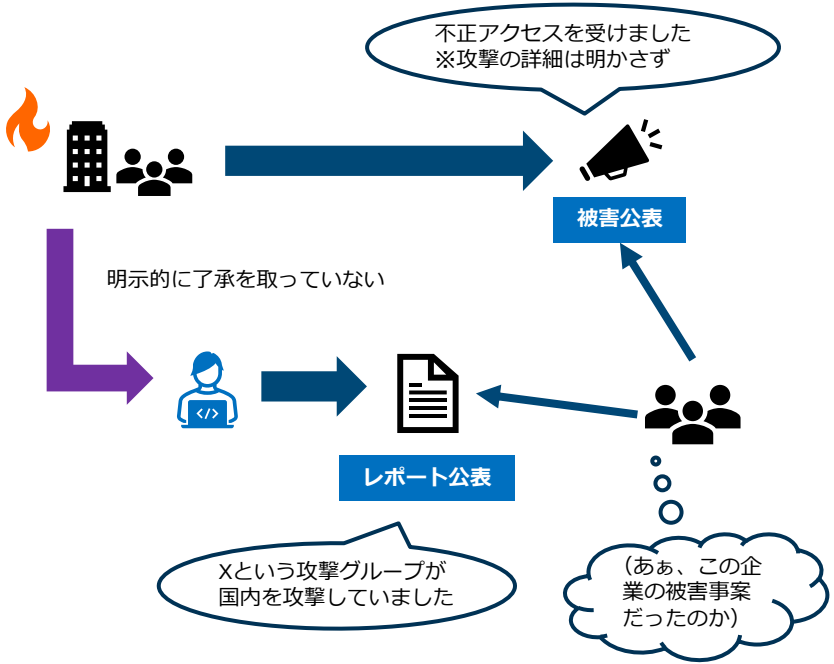
- ②が“正攻法”であるが、調整コストが高いことから、①が用いられるケースがある。
- ②には調整コスト／時間がかかり、かつ、了承を得られないケースも多い（※被害組織だけでなく、当該被害組織の委託先（運用保守ベンダ）の了承が得られないケースもある）ため、相対的に②で共有ができる件数が少なくなる。



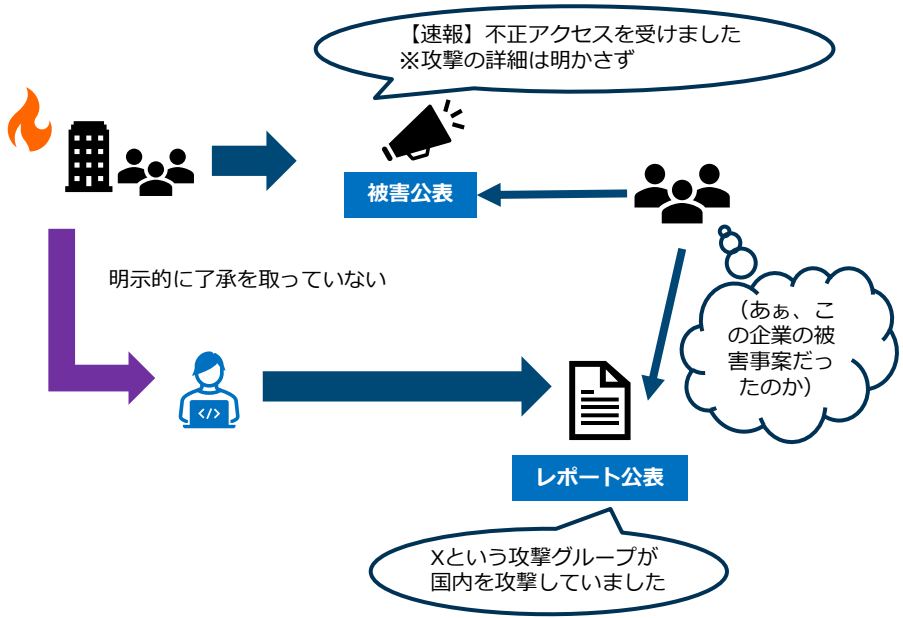
被害公表との関係

- 海外では比較的、以下のような問題は意識されていないように見受けられる

先行するレポート公表がその後の個別被害公表と結びつくケース



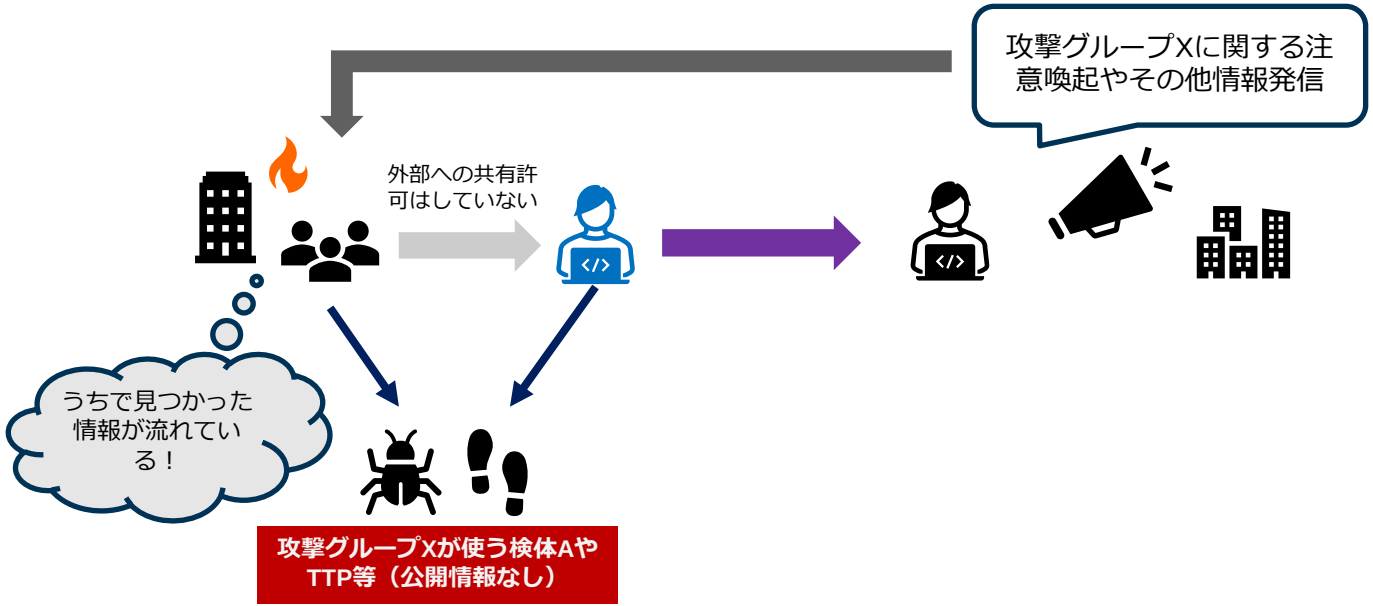
先行する被害公表により、その後のレポート公表がむずびついてしまうケース



情報共有の“滞留”ポイント

共有・公表ガイダンス検討会
資料から

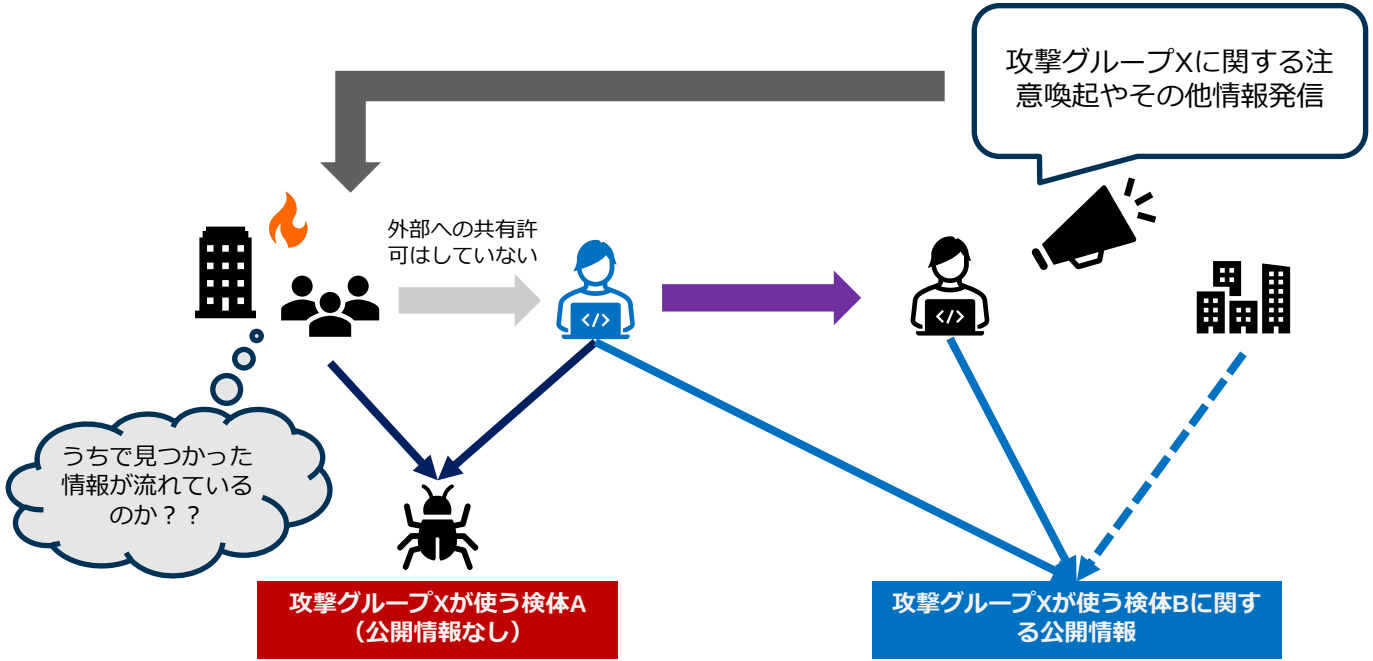
- 情報そのものは了承がなくとも「持ち出す」ことはできるが、情報が“逆流”したときに、「持ち出したこと」自体を責められてしまう恐れ
- また、場合によっては、（セキュリティ）ベンダ側の不注意により外部展開された技術情報から被害組織が推測／特定されてしまう場合も想定される
- 結果として、基本的に被害組織の意向次第となる



情報共有の“滞留”ポイント

共有・公表ガイダンス検討会
資料から

- 仮に、特定の被害組織だけで見つかった（と当該時点では思われた）情報は外部に共有していなかったとしても、被害組織から「自社だけで見つかった（と当該時点では思われた）情報を外部に無断で提供したのではないか」と疑われる可能性がある



各事業者においてNDA上の情報の扱いがハードルとなるケースの分類

<table>
<tr><th></th><th>セキュリティベンダ</th><th>SOC／製品ベンダ</th><th>運用保守ベンダ</th></tr>
<tr><td rowspan="2">右記事業者自体が情報共有活動／専門機関へ共有／提供したいと考える場合</td><td>A：NDA上の「秘密情報」に該当するために情報を出せない
B：被害組織に調整をしても外部への共有／提供について了解を得られない</td><td>左記に加えて、

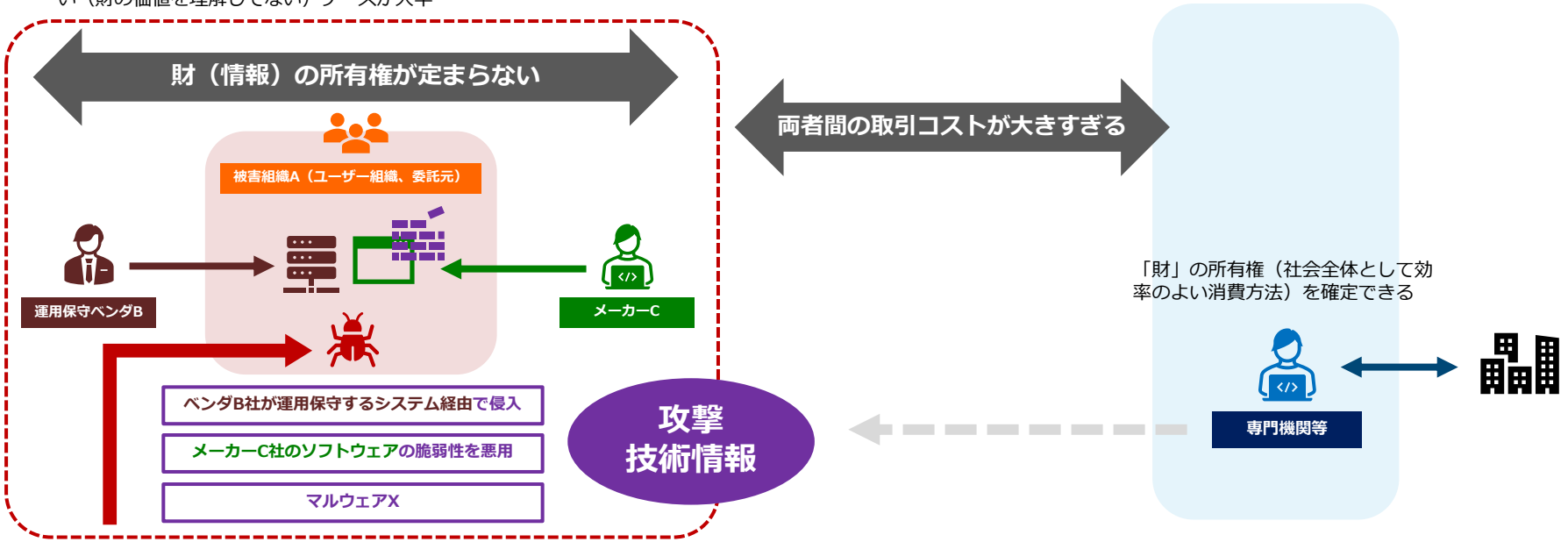
C：製品／サービスの利用契約上、研究目的以外の情報の活用が認められていないケース</td><td>A：NDA上の「秘密情報」に該当するために情報を出せない
B：被害組織に調整をしても外部への共有／提供について了解を得られない</td></tr>
<tr><td colspan="3">D：Bについて社内＋社外の調整コスト（“取引コスト”）が高いために実施されないケース</td></tr>
<tr><td rowspan="2">共有活動（事務局）／専門機関側が共有／提供を求める場合</td><td colspan="3">※上記に同じ</td></tr>
<tr><td colspan="3">※専門機関等は被害者に直接提供を求めることが多い</td></tr>
<tr><td>行政機関が提供を求める場合</td><td colspan="3">（各法令／手続きに基づく）</td></tr>
</table>

脆弱性問題、”踏み台“ベンダ問題

脆弱性悪用事案／“踏み台”ベンダ事案で情報共有がなされない背景

- 攻撃技術情報（マルウェア、通信先、その他TTP）を経済学上の「財」と定義した場合、自社（や顧客）が侵害された運用保守ベンダや被害組織（行政機関などの委託元も含む）は当該「財」の価値（※本来は共有することで社会全体で効率的に消費できる）が理解できなかったり、「財」の移転（※外部への共有）のための「取引コスト」（※社内外の調整コスト）が高すぎるため、「財」の所有権を確定できないことから、「あいまいなまま放置する」ことが合理的選択肢として選ばれてしまう（所有権理論）

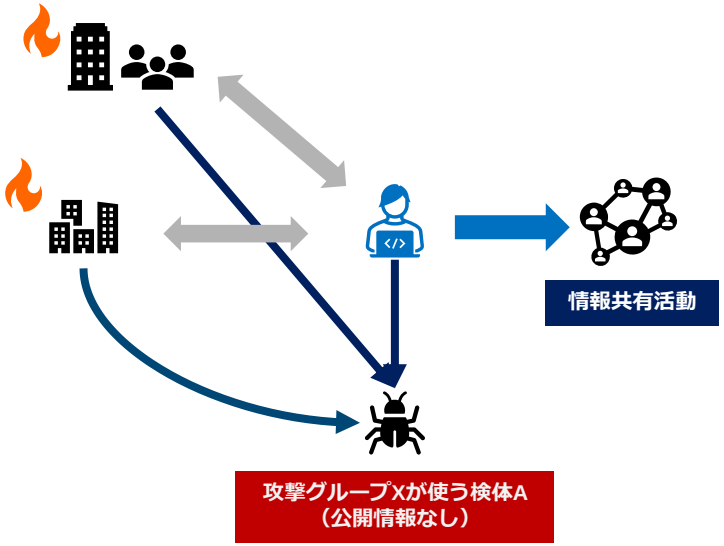
※そもそも情報を外部に共有しようというインセンティブを持つ者がいない（財の価値を理解してない）ケースが大半



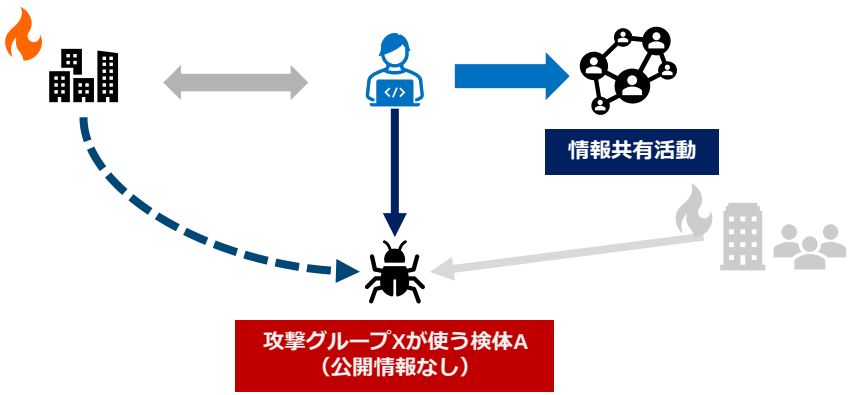
インシデント対応現場における実際の対応

被害組織から「了解」を取らないケース

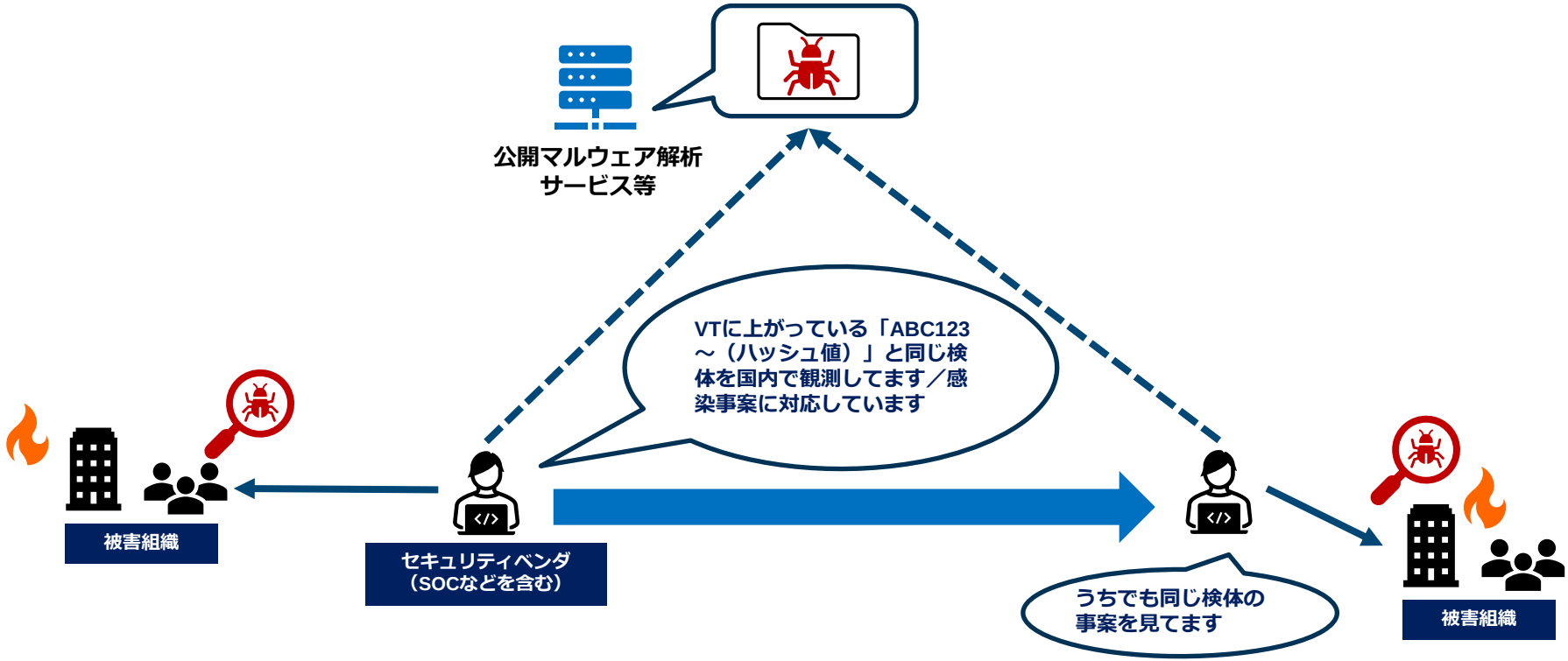
- ①複数組織で既に同一検体／通信（左記）が見つかっている場合は前述の懸念がなくなるため、個別に了承は取らずに情報共有を行う



検体そのものやサーバ、その他第三者が入手しうる関連する情報からは被害組織が特定されない場合

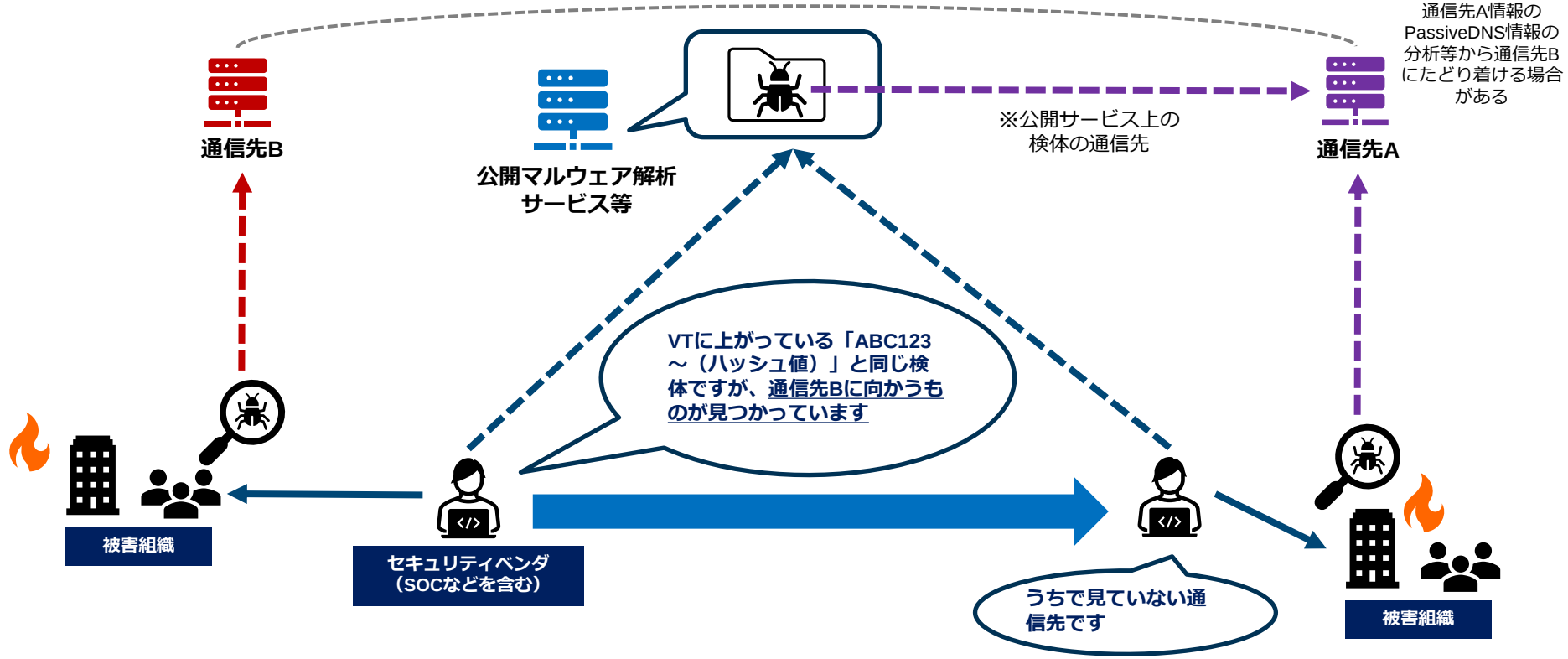


「公知の情報」を使った専門組織間の“共有”事例①



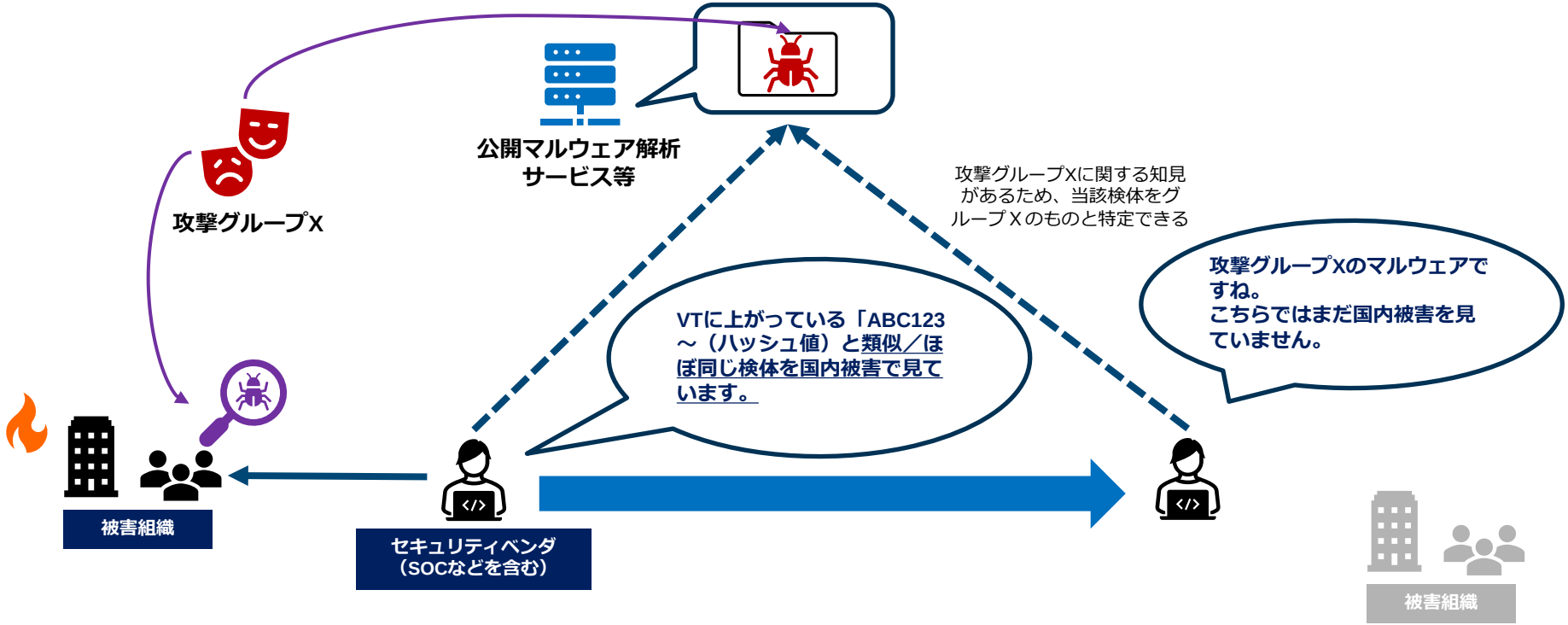
「公知の情報」を使った専門組織間の“共有”事例②

■ 公開サービス上では明示されていない「通信先B」の情報を共有



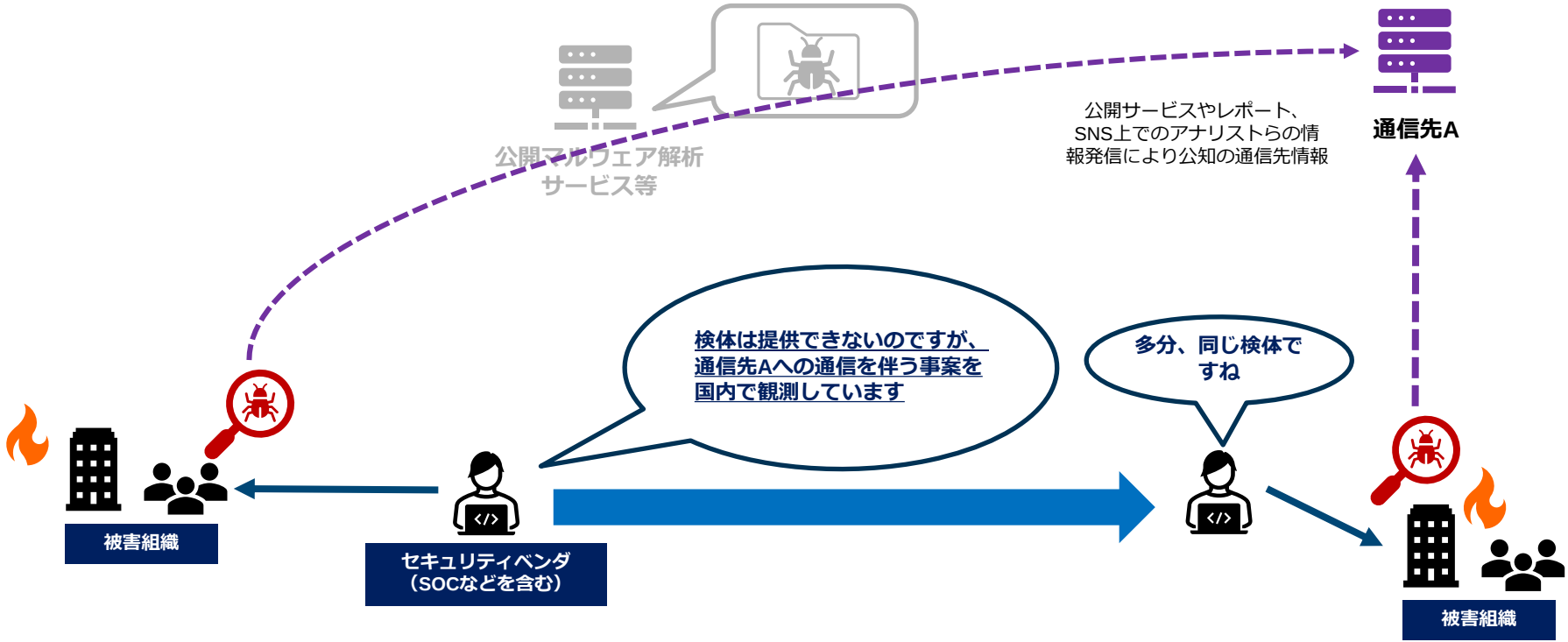
「公知の情報」を使った専門組織間の“共有”事例③

- 現場で見つかった検体情報は交換できないが、当該検体を用いる攻撃活動の動向（の把握状況）等を伝えることはできる



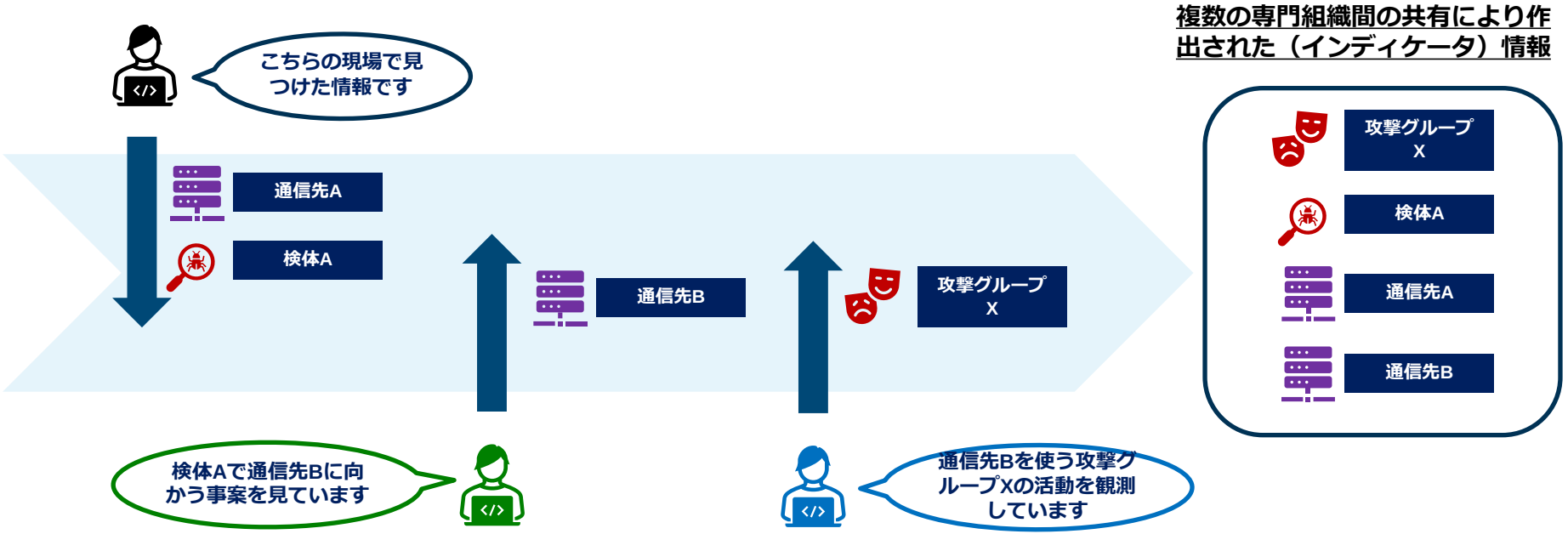
「公知の情報」を使った専門組織間の“共有”事例④

- 検体はお互いに共有できないが、通信先Aの情報を共有



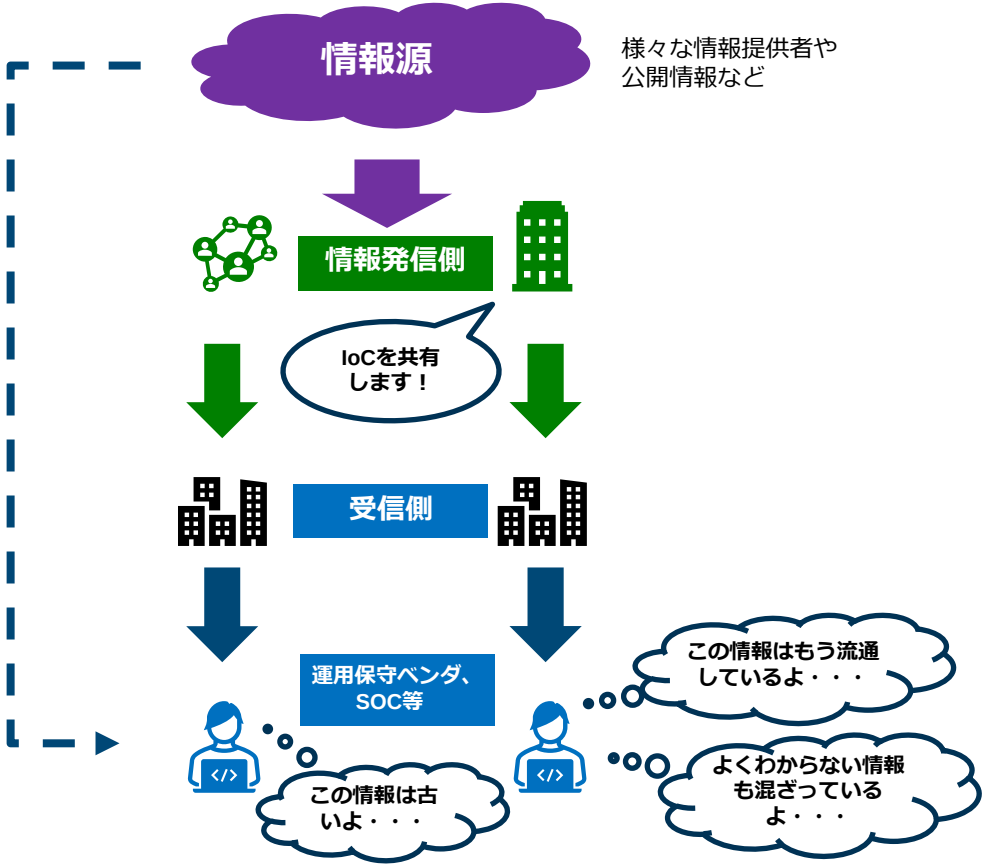
公知の情報を活用したインディケータ作出例

- 各専門組織が個別の現場で把握している情報には限界があり、かつ、各専門組織が共有許可を得た情報の範囲も限定的であるため、専門組織が情報を持ち寄って、インディケータを作出したり、攻撃の全容把握に必要な情報を交換し合うことが行われている



処理コストのかかる情報の流通状態

情報があふれている問題



- 必ずしも情報共有活動を通じて流す必然性がない情報や、未精査の情報が手動で流れるケースがある（製品・サービス上で十分に情報が流通している or ある程度時間が経てば十分に流通する）
- （自動／手動であれ）むしろ、”共有活動“を通じて未精査の情報や断片的情報が混在した情報が流通することで、その処理コストを発生させてしまったり、”誤爆“事故のリスクを増やしている
- 「情報を出すこと」自体が自己目的化している

情報共有効果が高い情報を流すための専門組織同士の共有の必要性

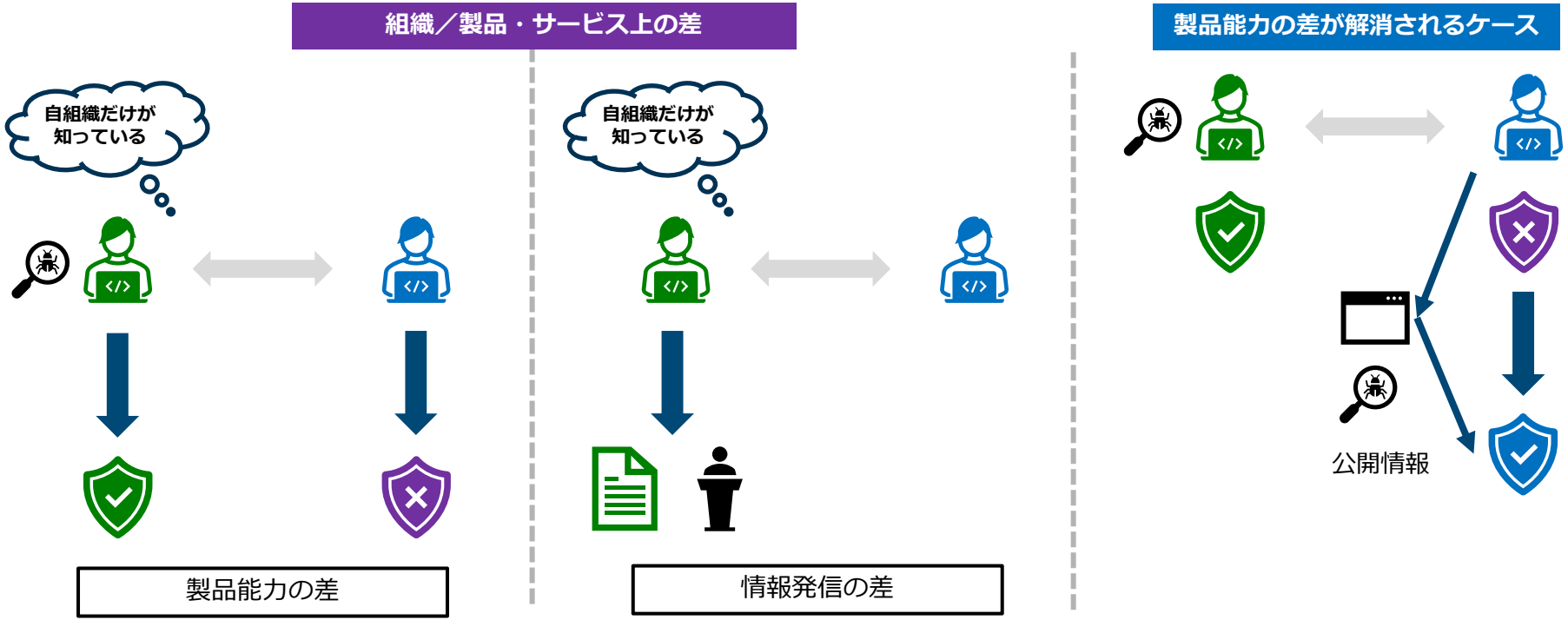
- 「情報共有に適した情報（攻撃類型、タイミング）」がある⇒サイバー攻撃被害に係る共有・公表ガイダンスQ6等で解説
- 情報発信者（専門組織、情報共有活動のハブ組織）側が「これから展開しようとしているその情報は情報共有活動に展開する情報として最適か」「その情報はどこに展開すれば効果的か」把握してない場合がある

  ⇒そもそも限定された“守備範囲”しか有しない情報発信者側の各組織が自らそれを知ることはできない
- そもそもそういう推測をすることには限界があるため（情報の非対称性）、専門組織同士の情報共有（シグナリング）が必要ではないか

競争優位性と情報共有との関係

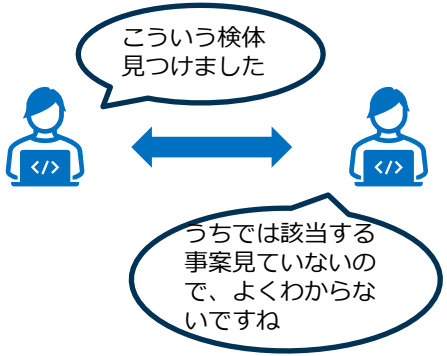
競争優位性と共有活動

- 必ずしも専門組織同士の共有がなされておらず、専門組織／アナリスト間で知見の偏りや、製品／サービス上の能力の差が放置され続けているわけではない

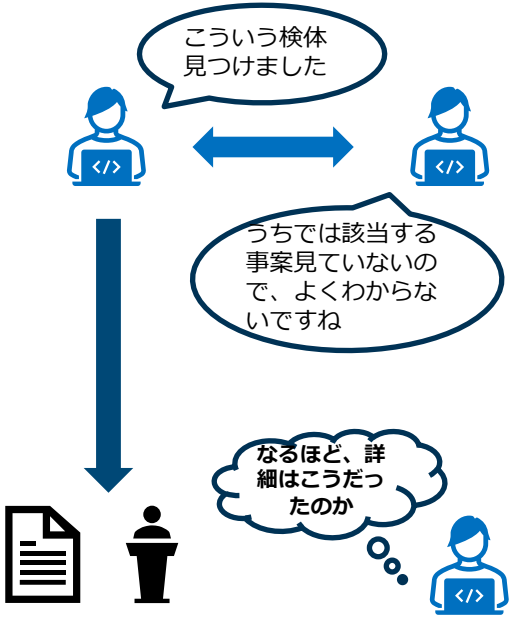


専門組織同士の情報共有と競争優位との調整

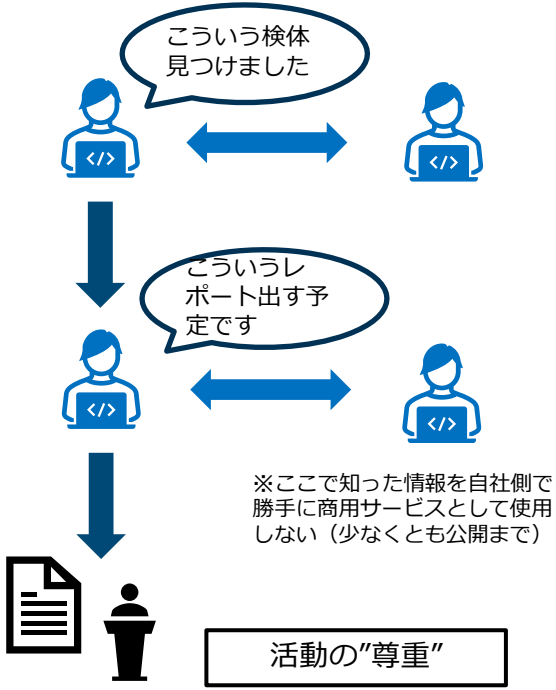
- 現状では専ら、アナリスト同士の共有活動や一部の情報共有活動（サイバーセキュリティ協議会第一類）に限られている



情報の非対称性の解消



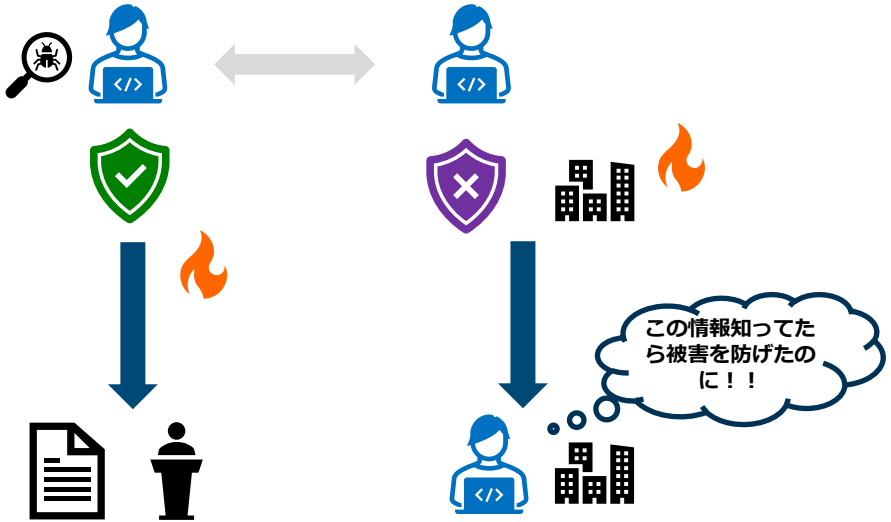
情報発信の差

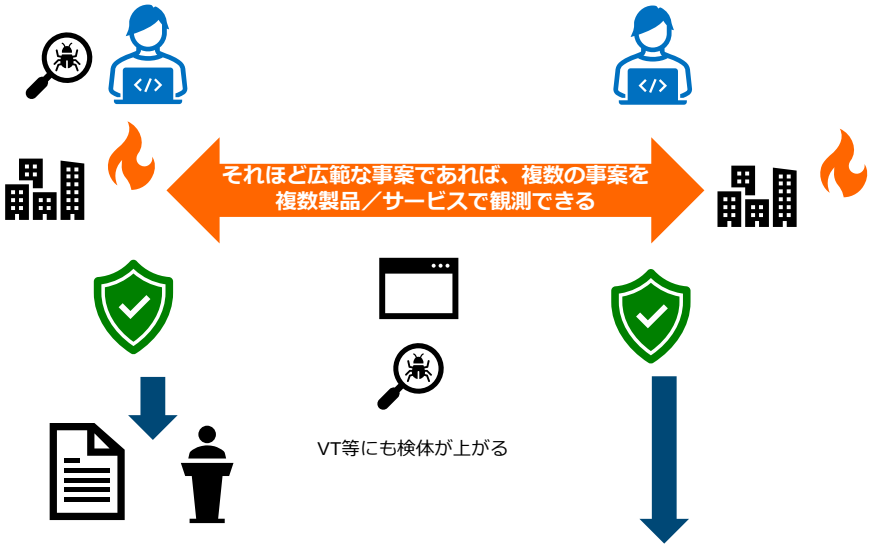


活動の”尊重”

共有しないことの不利益はどのように回避されているのか

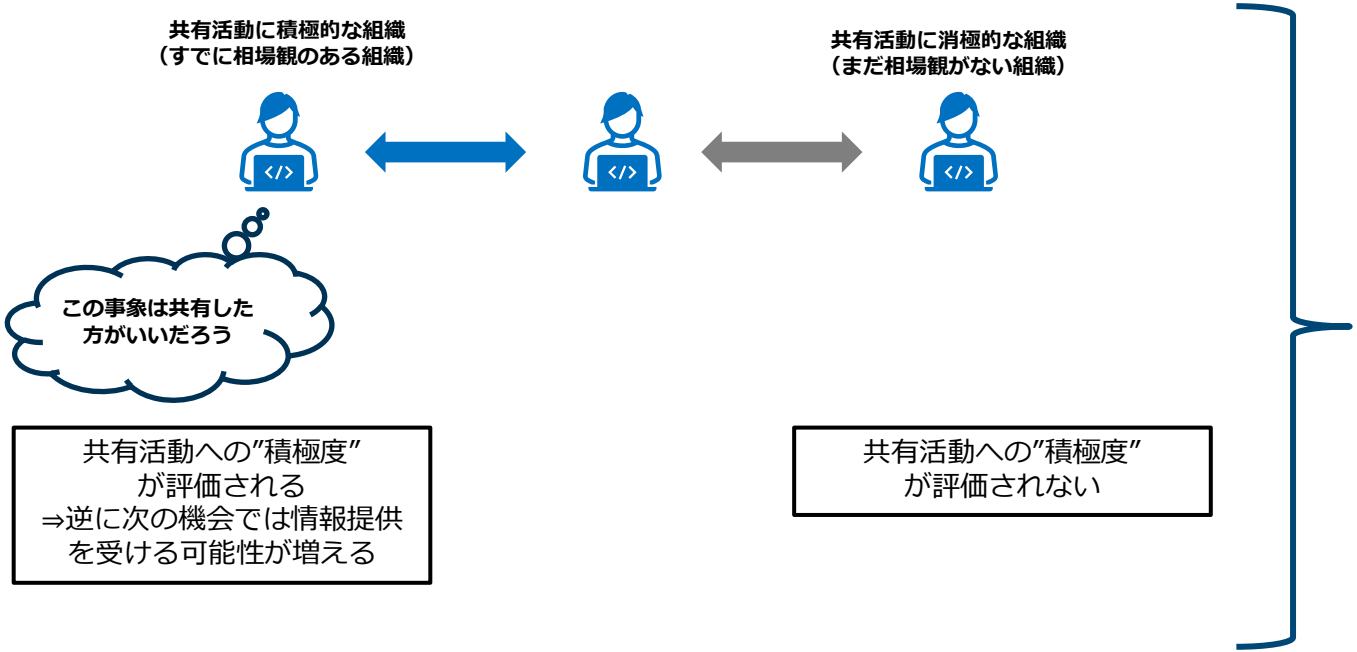
- 専門組織同士の共有がないことでユーザー組織側が著しく不利益を被るケースはあるのか？（※問題②「事案対応の最適者」が調整／修正されないことで被害組織が不利益を被っているケースを除く）
- 左記のようなケースは（すでに専門組織同士の共有を試みている関係者間では）ほとんどない
- 右記のような、ある程度の範囲観測されている攻撃の場合は、共有するまでもない





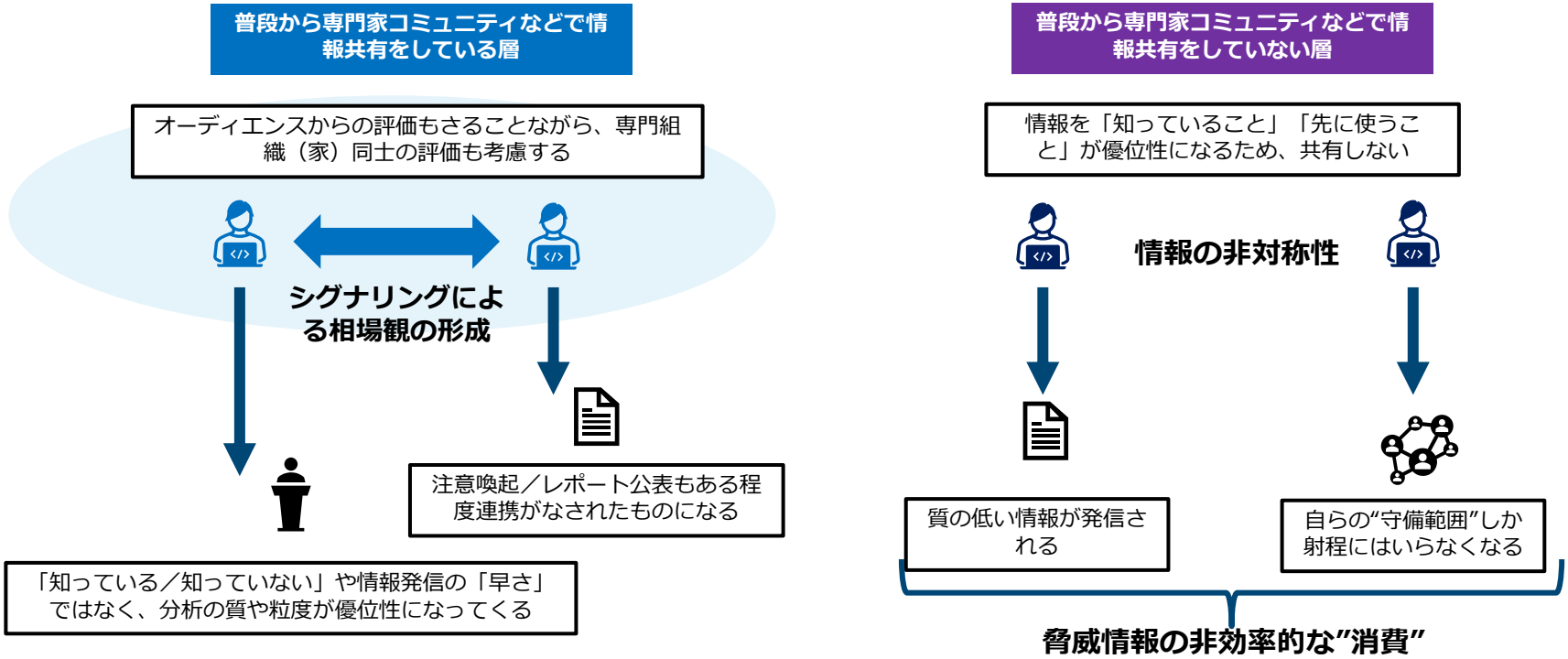
共有活動における調整機能

- 専門組織（家）同士の共有活動においては、下記のような「相場観」が形成されるため（シグナリング効果）、「共有しなかったことで他所での被害が拡大する事案」（前頁）への配慮もなされ、「これはここで共有しておいた方がよいだろう」という判断に基づく情報共有がなされる



専門組織（家）間の共有を通じた脅威情報の効率的な消費

- 「鶏が先か卵が先か」論であるが、普段から専門組織同士で情報共有しない層は「知っていること」「先に情報を使うこと」が優位性になったままであるため、共有を避け、情報を非効率的に“消費”してしまう



共有対象と競争優位性

- **広範囲／同時多発な事案**　⇒情報格差を埋めるまでもない。　⇒それでも発生する製品／サービス差は、もはや市場における競争として十分認められる範囲ではないか

中間の事案：
事案の広さで情報格差が埋まらないが、ある程度の範囲で被害が予想されるので、情報共有による格差解消が求められるもの
⇒情報共有効果が得られると見込まれるもの

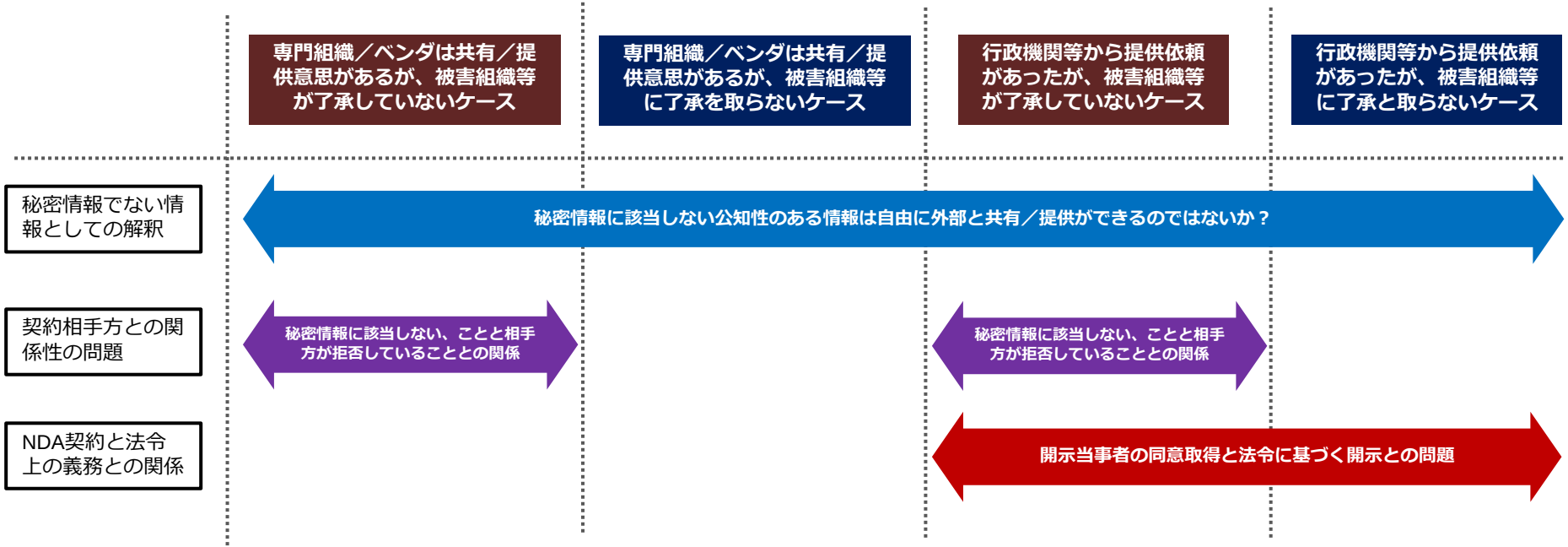
- **限定的な事案**　⇒必ずしも事案を見てない製品・サービスの提供先でも発生するとは限らないため、無理に情報格差を埋めなくてもよい

今後に向けて：
論点の整理

基本的な整理

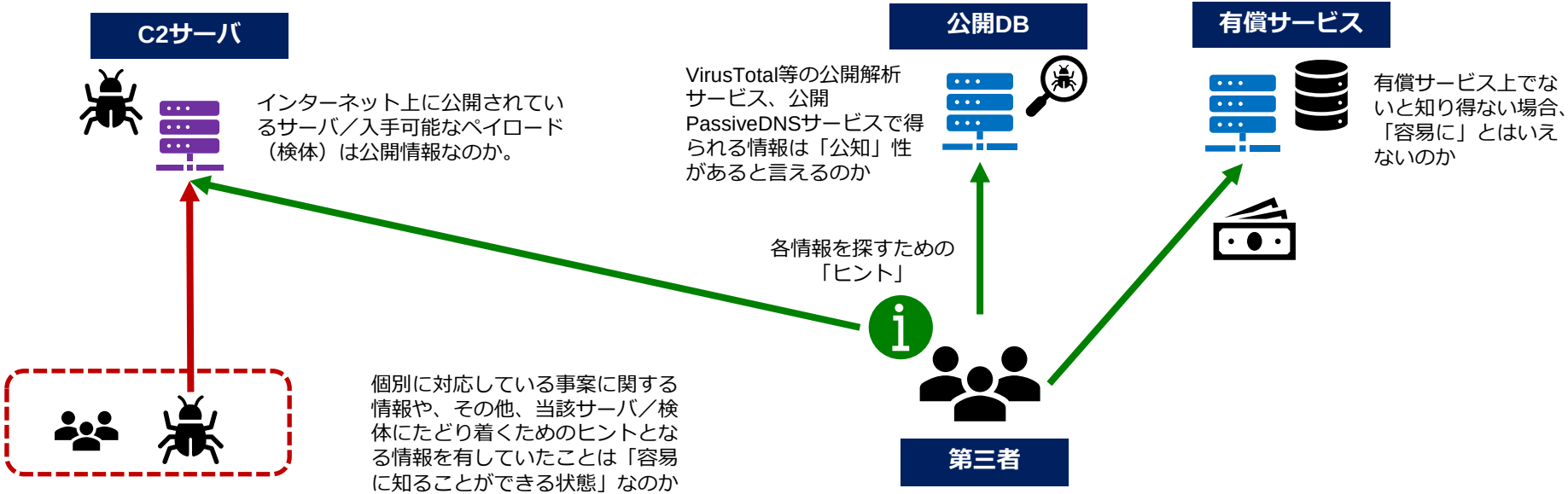
- 攻撃技術情報（の大半）についてその公知性が認められれば、外部との共有を行いやすくなるものの、公知性が認められ、旧来のNDA上における秘密情報の定義外になるとしたとしても、なお、契約相手方（開示当事者）との間の論点が残るのではないか

  ⇒NDAの変更や、攻撃技術情報（の大半）について秘密情報の定義外となることの「説明」が事前に必要になるのではないか



公知性の解釈について

- 「公知」：一般的に知られた状態、または容易に知ることができる状態（参考：営業秘密管理指針等）
- 何らかの専門的知見や、紐づける「ヒント」となる情報を有していなければ当該情報を知り得ない場合、「容易に知ること」になるのかどうか



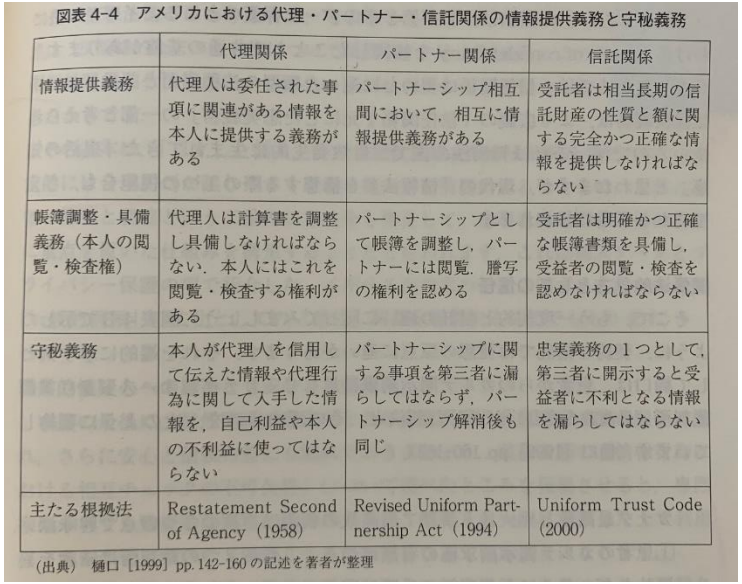
秘密（性）の解釈について

- 「情報：コンテンツ」と「保護対象者：帰属」との分離（林紘一郎『情報法のリーガル・マインド』259頁等
  - 類型①：客体たる情報そのものを保護する必要性がある場合の「秘密性」 ⇒帰属は公表できるが、コンテンツは公表できない（分離可能）
  - 類型②：情報の（当該時点での）利用権者を保護する必要性がある場合の「秘密性」 ⇒ コンテンツ・帰属両方とも公表できるが、分離はできない
  - 類型③：特定の人／組織を保護する必要性がある場合の「秘密性」 ⇒ コンテンツ・帰属いずれも勝手に公表できない（分離不可能）

- サイバー攻撃被害のうち技術情報は新たな類型④（コンテンツ・帰属の分離は可能であるが、元々の帰属の公表はできない）なのではないか？

個別の契約上の観点

- 善管注意義務として、自組織で不足する知見／情報を補うべく外部と情報共有することがそもそも求められるのではないか（※委託契約上の善管注意義務というより、専門家への請負契約や信託契約に近いのではないか）
- 委託者の不利益にならない範囲であれば、むしろ必要な情報を外部と交換して委託者の利益になる情報を積極的に集めることを求めるべき
- ↑（“にわとり・卵”だが）積極的な情報収集が委託先に求められるのであれば、事案発生時に委託先は「動かないといけなくなる」し、委託者はそのための権限／情報を与えなくてはならない



図表 4-4　アメリカにおける代理・パートナー・信託関係の情報提供義務と守秘義務

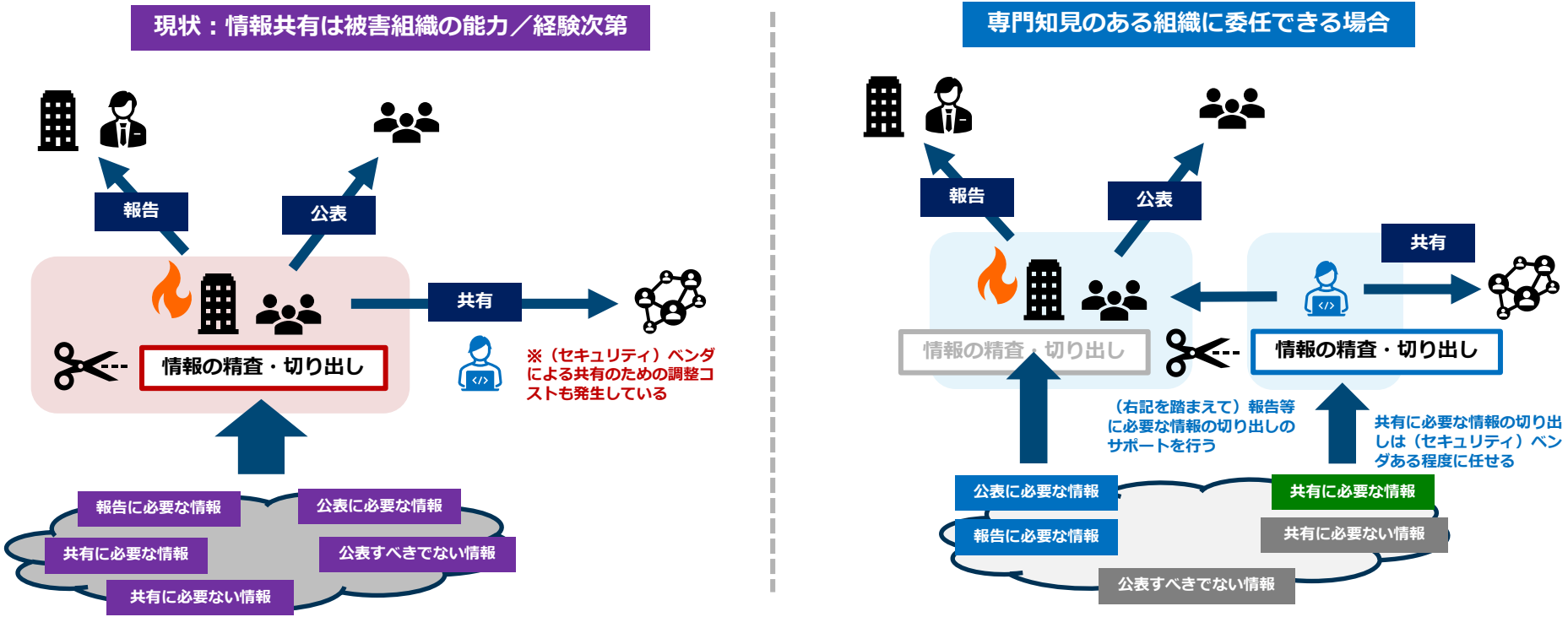
	代理関係	パートナー関係	信託関係
情報提供義務	代理人は委任された事項に関連がある情報を本人に提供する義務がある	パートナーシップ相互間において，相互に情報提供義務がある	受託者は相当長期の信託財産の性質と額に関する完全かつ正確な情報を提供しなければならない
帳簿調整・具備義務（本人の閲覧・検査権）	代理人は計算書を調整し具備しなければならない．本人にはこれを閲覧・検査する権利がある	パートナーシップとして帳簿を調整し，パートナーには閲覧，謄写の権利を認める	受託者は明確かつ正確な帳簿書類を具備し，受益者の閲覧・検査を認めなければならない
守秘義務	本人が代理人を信用して伝えた情報や代理行為に関して入手した情報を，自己利益や本人の不利益に使ってはならない	パートナーシップに関する事項を第三者に漏らしてはならず，パートナーシップ解消後も同じ	忠実義務の１つとして，第三者に開示すると受益者に不利となる情報を漏らしてはならない
主たる根拠法	Restatement Second of Agency（1958）	Revised Uniform Partnership Act（1994）	Uniform Trust Code（2000）

（出典）　樋口［1999］pp. 142-160 の記述を著者が整理

林紘一郎「情報法のリーガル・マインド」229頁

情報ハンドリングコストの解消に向けて

- 被害組織のみがすべてのコストを負うのではなく、ある程度専門知見を持つ委託先に任せることができれば、全体としてコストを減らせるのではないか



その他の論点

- NDA以外の個別サービス契約／約款との関係
  - アンチウィルス製品のテレメトリー情報やSOC監視情報の取扱い
  - 公知性の有無は関係なく、「検知した情報」をそもそもどう扱ってよいか、という問題なのではないか？
  - 契約／約款改訂対応コスト（ユーザーへの説明コスト）の負担が高いため、仮に法的解釈が解消しても、着手にはハードルがなお残るのではないか
- ~~そもそも情報共有／提供の意志がない組織の問題~~
  - ~~NDA問題以外の問題~~

今後に向けて：
「契約」と「情報」の整理

情報の整理

- 攻撃技術情報について、一部については共有・公表ガイダンスで整理・解説を行っているが、「（主に被害組織同士の）情報共有目的」の観点からの整理で終えている

- 上記のほかに

・情報共有効率化のための整理

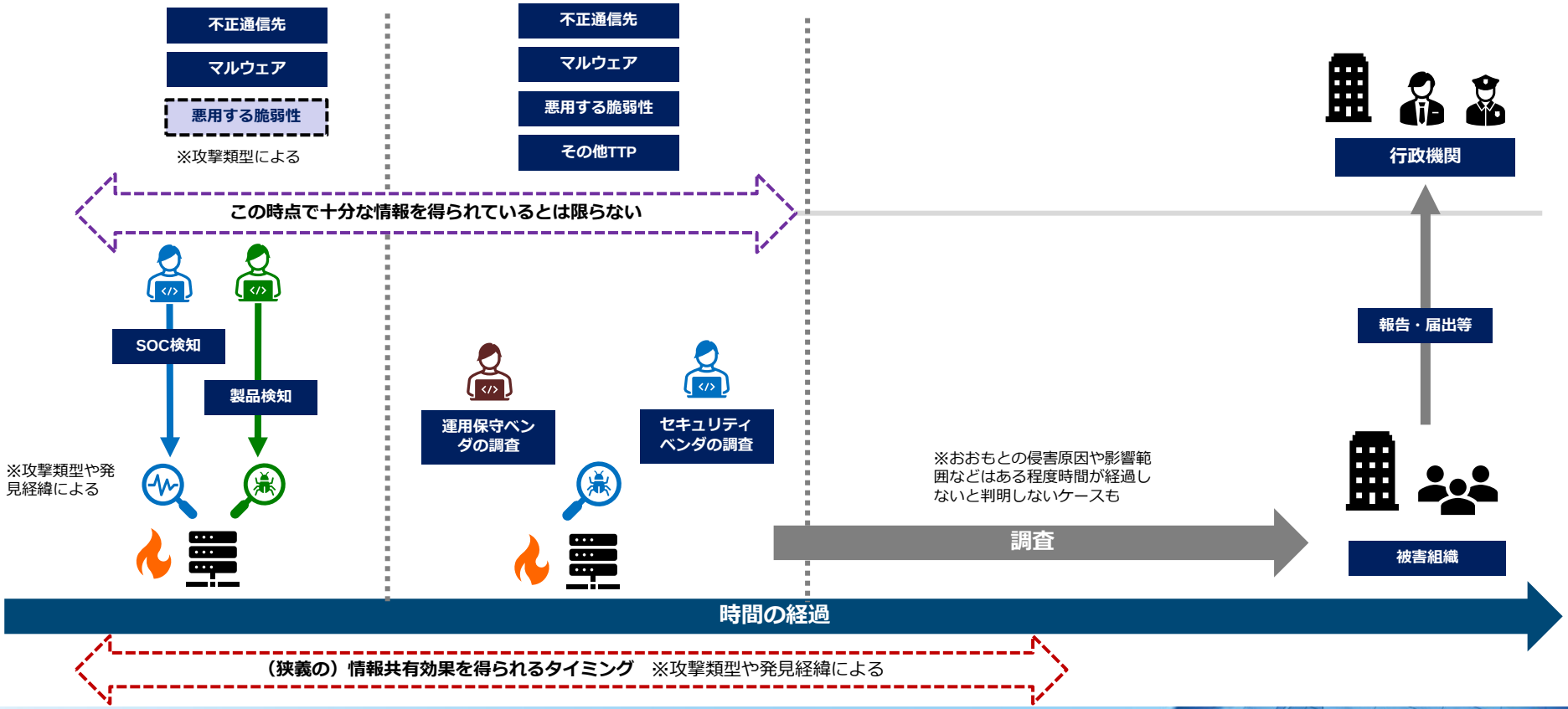
—「共有しなければならない情報」と「必ずしも共有しなくてよい情報（いずれ製品／サービスを通じて流通する情報）」の整理

—攻撃類型別の「共有すべき情報」と「共有効果のあるタイミング」の整理

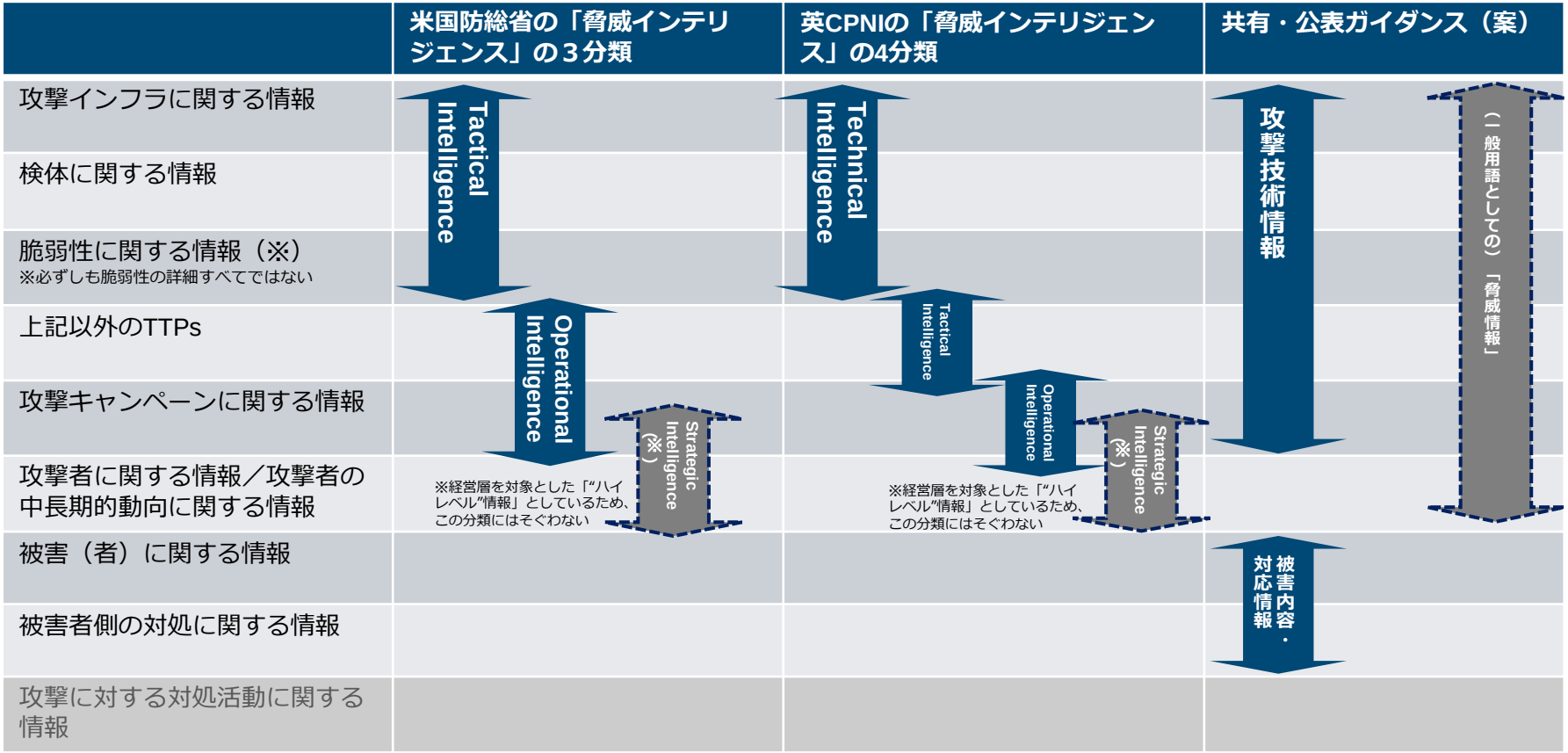
・様々な機関等が対抗措置を速やかに行うために必要な情報

の整理が必要ではないか

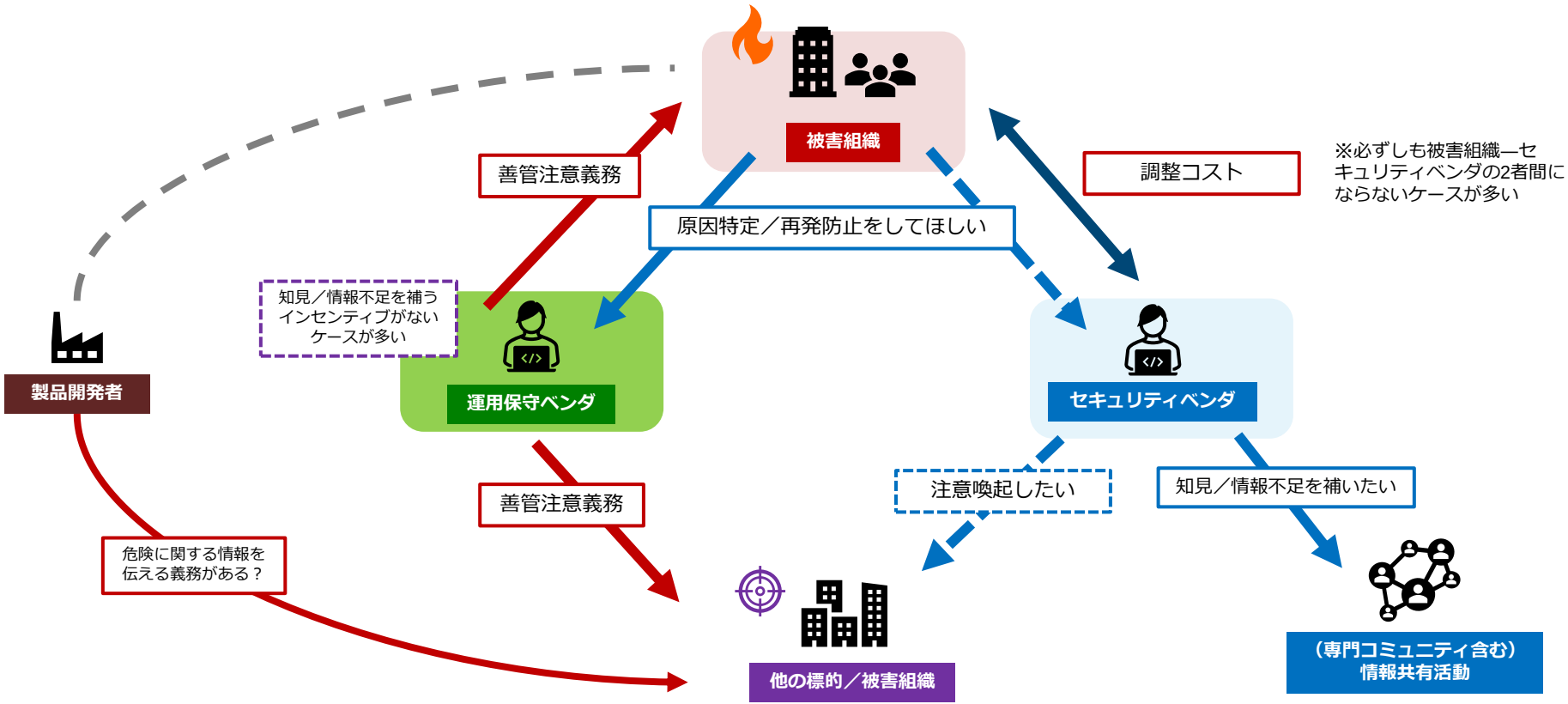
各タイミングでどのような関係者がどのような情報を見ているのか



対象とする「脅威情報」の整理



全体像：民側の各プレイヤーの動機と契約上の求め



公益目的の観点の整理

- 特定製品の脆弱性やその悪用事実に関する情報については、情報伝達の公益性が高いことから、速やかに必要な組織（影響を受けるユーザー、脆弱性告示制度上の調整機関等）に通知されるべきではないか
- 悪用に関する伝達手段を個別通知にするか専門機関からの注意喚起にするかは攻撃の状況等応じて製品開発者と調整機関が相談するとして、ただ、被害組織と運用保守ベンダとのNDA等に縛られてこれが阻害されるべき理由は見当たらない（※当該脆弱性に関する注意喚起を出すこと自体が当該被害者や他の組織への新たな攻撃を惹起する可能性があるとしても、それは情報発信の手段に関する問題であり、悪用事実が伝えられないことの理由にならない）

官民間の諸問題