資料2-2

JPCERT CC®

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 第1回

JPCERT/CCからの論点提示

一般社団法人
JPCERTコーディネーションセンター

本資料の構成

【参考】パート（スライド3～6）

議論の前提となるポイントや本資料における各用語／概念について最小限まとめたもの

【抜粋資料】パート（ライド7～15）

右記「参考資料」を抜粋・編集したもの

- 【情報共有の課題】タイミングのミスマッチ（スライ7）
- 【情報共有の課題】共有内容のミスマッチ（スライ8）
- 【情報共有の課題】専門組織間共有の障壁（スライド9）
- 【公表の課題】公表までに一定の時間を要するケース（スライド10）
- 【公表の課題】公表内容に納得感がないケース（スライド11）
- 【公表の課題】他組織の公表等により未公表の事実が判明するケース（スライド12）
- 【公表の課題】被害が未公表であることの影響（スライド13）
- 【被害組織保護】未公表被害が公開情報となる場合（スライド14）
- 【共有と公表】注意喚起／ノウハウ共有目的の公表（スライド15）

【参考資料】パート

※事前説明会及び検討会で説明しない資料

インシデント対応における情報共有の課題について（スライド18～45）
- 「タイミング」のミスマッチが起きるケース
- 「情報の内容」のミスマッチが起きるケース
- （セキュリティ）ベンダが情報共有できないケース

インシデント対応における公表の課題について（スライド46～59）
- 公表までに一定の時間を要するケース
- 公表内容に“納得感”を得られないケース
- 他組織の公表等により未公表の事実が判明するケース
- 脆弱性悪用有無の情報の取り扱いで揉めるケース

被害組織保護の観点から（スライド60～64）
- 検体解析情報から被害組織が推測されるケース
- 攻撃インフラの調査から被害組織が推測されるケース
- 公開情報から被害原因が推測されるケース

各情報の性質・留意すべき点について（スライド65～72）

「共有」と「公表」について（スライド73～78）

【参考】用語の定義

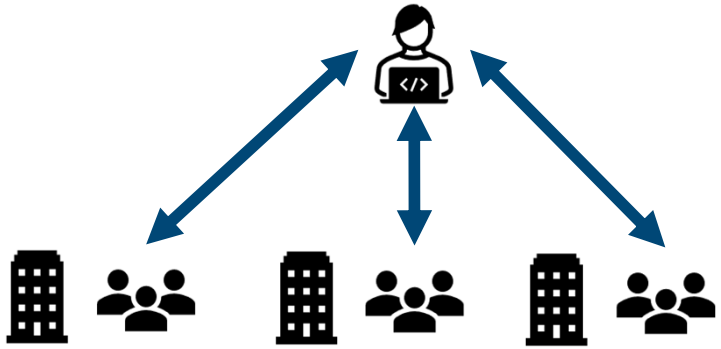
攻撃（情報）	攻撃に成功したもの（に関する情報）
攻撃試行	攻撃を試みるために行われたアクセス等
攻撃キャンペーン	一定期間内において特定の組織／分野に対して特定の攻撃手法／攻撃インフラを用いて行われる攻撃活動
マルウェア情報	マルウェアを解析した情報（※表層解析程度のものも含む）
マルウェア検体	マルウェア検体そのもの
攻撃インフラ	主にC2サーバ等の通信先や踏み台としたサーバ
TTP	攻撃者が用いた攻撃手法に関する情報 「Tactics（戦術）、Techniques（技術）、Procedures（手順）」の略
攻撃グループ	攻撃を行った者を便宜上グルーピングし、またそれを呼称するもの
被害情報	サイバー攻撃の発生により被害組織にて確認される、技術情報とコンテクスト情報を含む情報
技術情報	マルウェア情報や攻撃インフラ、TTP情報など攻撃者による攻撃活動やまたはその痕跡を示すもの
コンテクスト情報	攻撃活動によって発生した被害や攻撃被害発生に対して取った被害組織の対処内容を示す情報
全容解明／把握	攻撃に用いられた手法や攻撃インフラを明らかにすることや、攻撃キャンペーン全体を明らかにすること
フィードバック（情報）	情報共有（提供）に対して、何らかの返答をすること（とその返答時の情報）
専門組織	専門機関やセキュリティベンダ
専門機関	非営利でサイバー攻撃対処や分析、情報共有活動を行う組織
セキュリティベンダ	セキュリティ製品・サービスを提供することを主たる事業としている企業
ベンダ	いわゆるSierや運用保守ベンダ
（製造）メーカー	ソフトウェア等の製造元
（情報共有活動の）ハブ組織	情報共有活動で参加者間の情報伝達の仲介や、一部の分析、他の共有活動や専門組織との窓口を担う組織

【参考】情報共有活動の類型

ハブ・スポーク型

・専門組織等がハブ組織を務めているもの
・匿名で情報が共有されることが大半

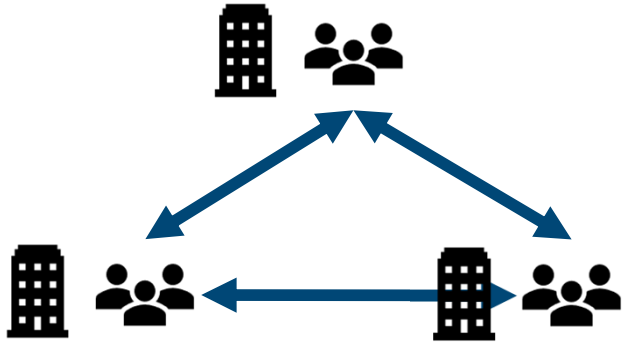
例：CS協議会、CISTA（JPCERT/CC）、J-CSIP



n対n型

・基本的にはお互い顔の見える形でおこなっているもの。特定の共有ハブはない。

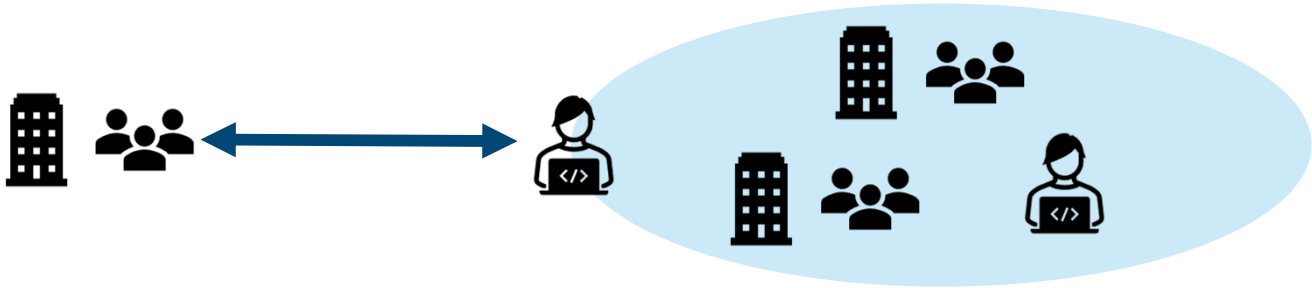
例：NCA（日本シーサート協議会）、各ISAC
※個人単位の「コミュニティ」活動もこのタイプ



間接／代理型

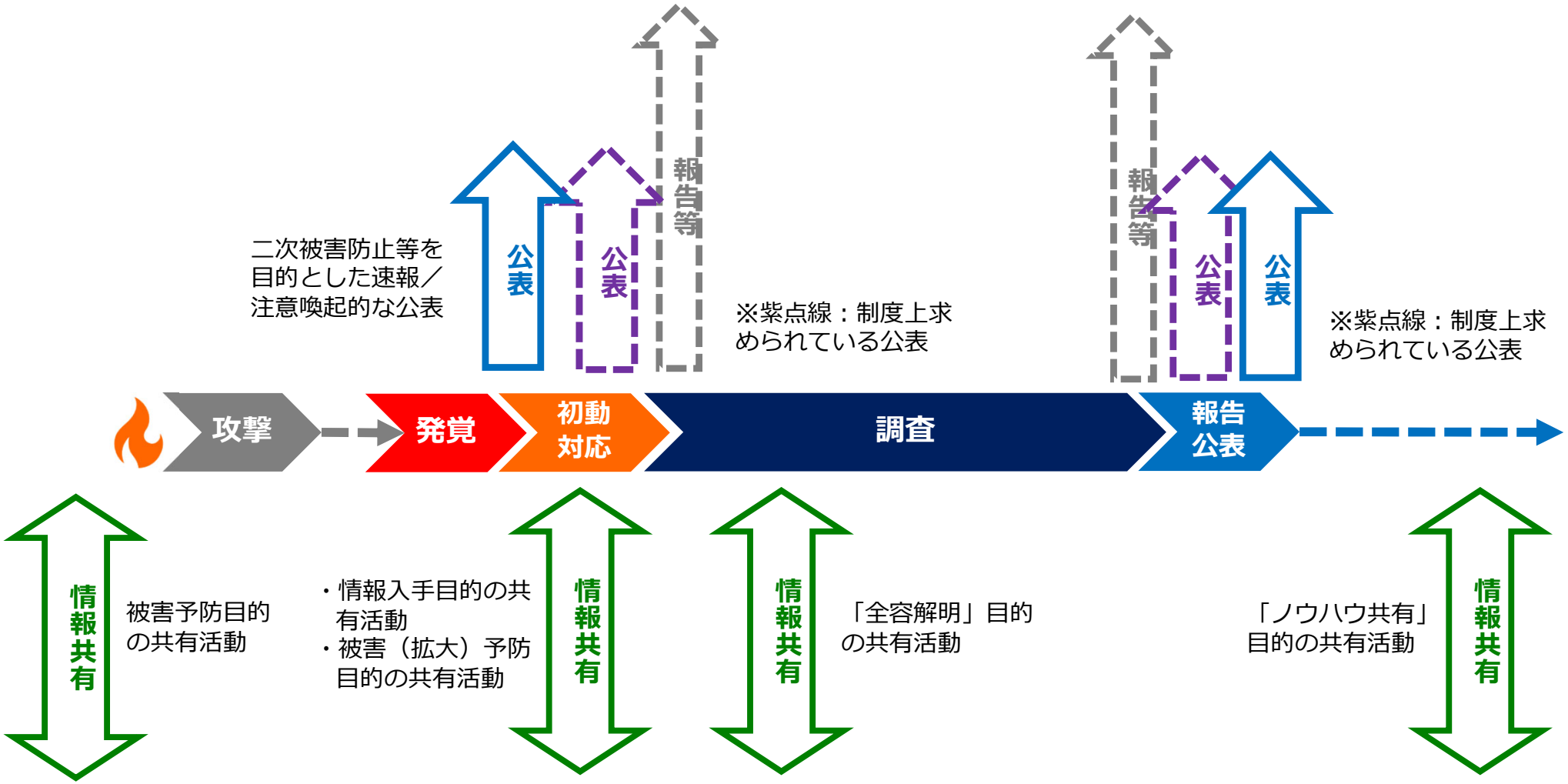
・情報共有活動に参加していない組織と情報共有活動参加組織間の共有をハブ組織等が担うもの

例：CS協議会、CISTA（JPCERT/CC）



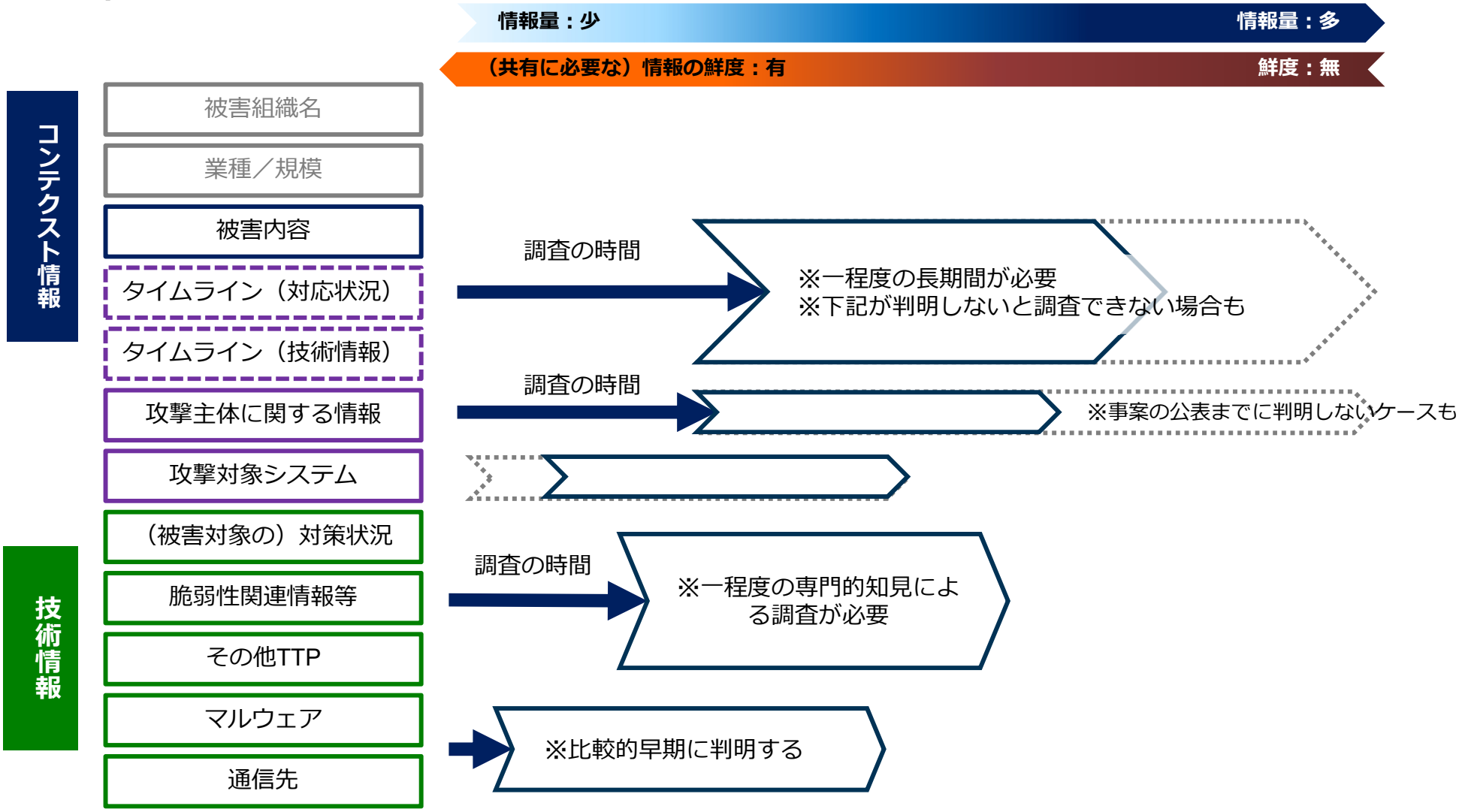
【参考】情報共有と公表

- 一言に「共有」「目的」といっても、それぞれの目的に応じて実施されるタイミングが異なる



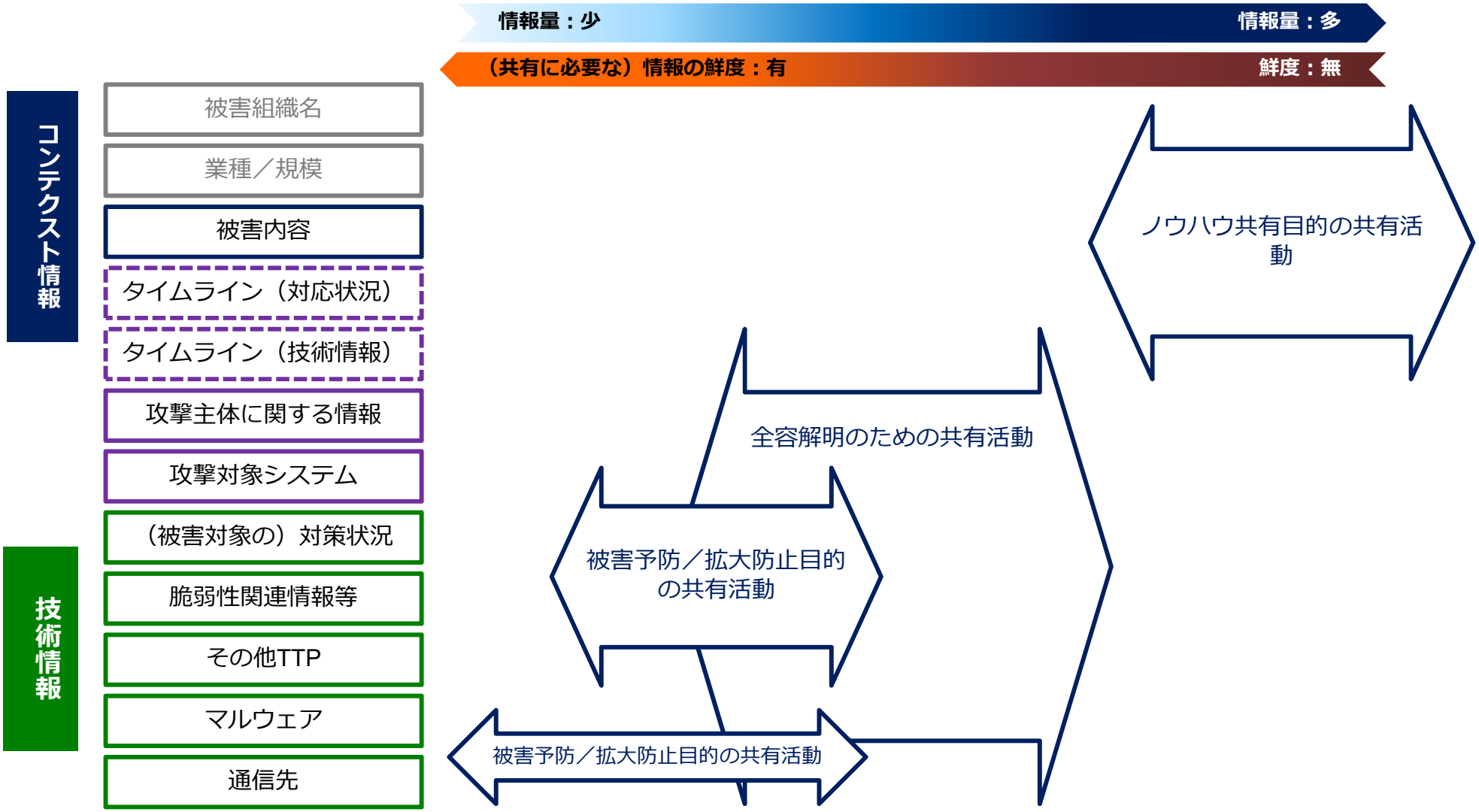
【参考】調査により各情報が判明するタイムライン

- 一程度の調査時間が経過しなければ判明しない情報もある



【参考】各共有活動が主に扱う情報

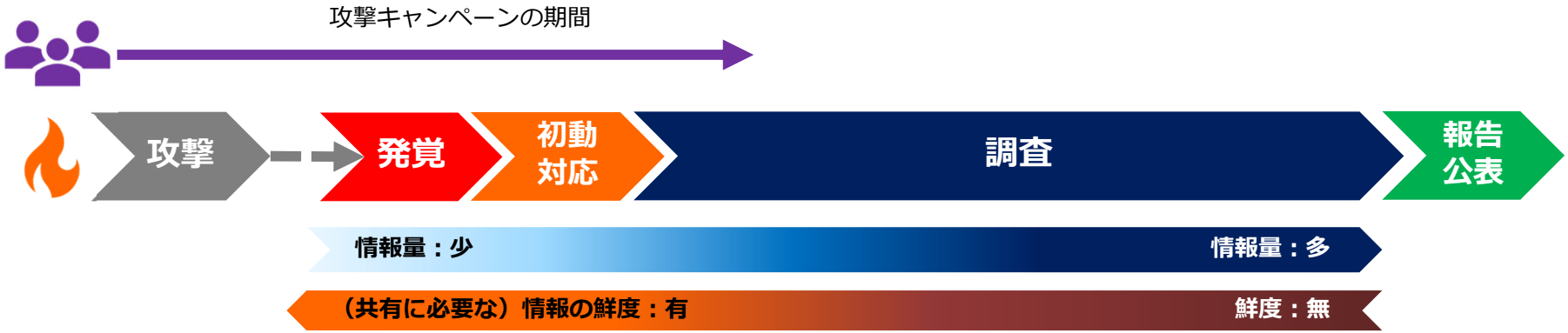
- 共有活動の目的に応じて特定のタイミングで主に扱う情報の種類は異なる

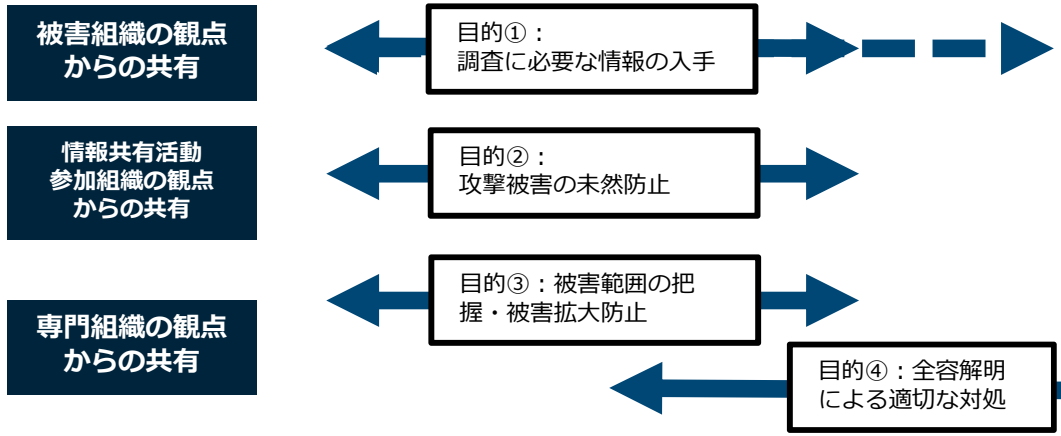


【情報共有の課題】タイミングのミスマッチ

参考資料：
18～25ページ参照

- 「情報共有」とひとくくりになっているが、各組織の目的毎に適切なタイミングは異なっている
- 一方で、どの組織の目的に適したタイミングにも間に合っていない情報共有が多数行われてしまっている

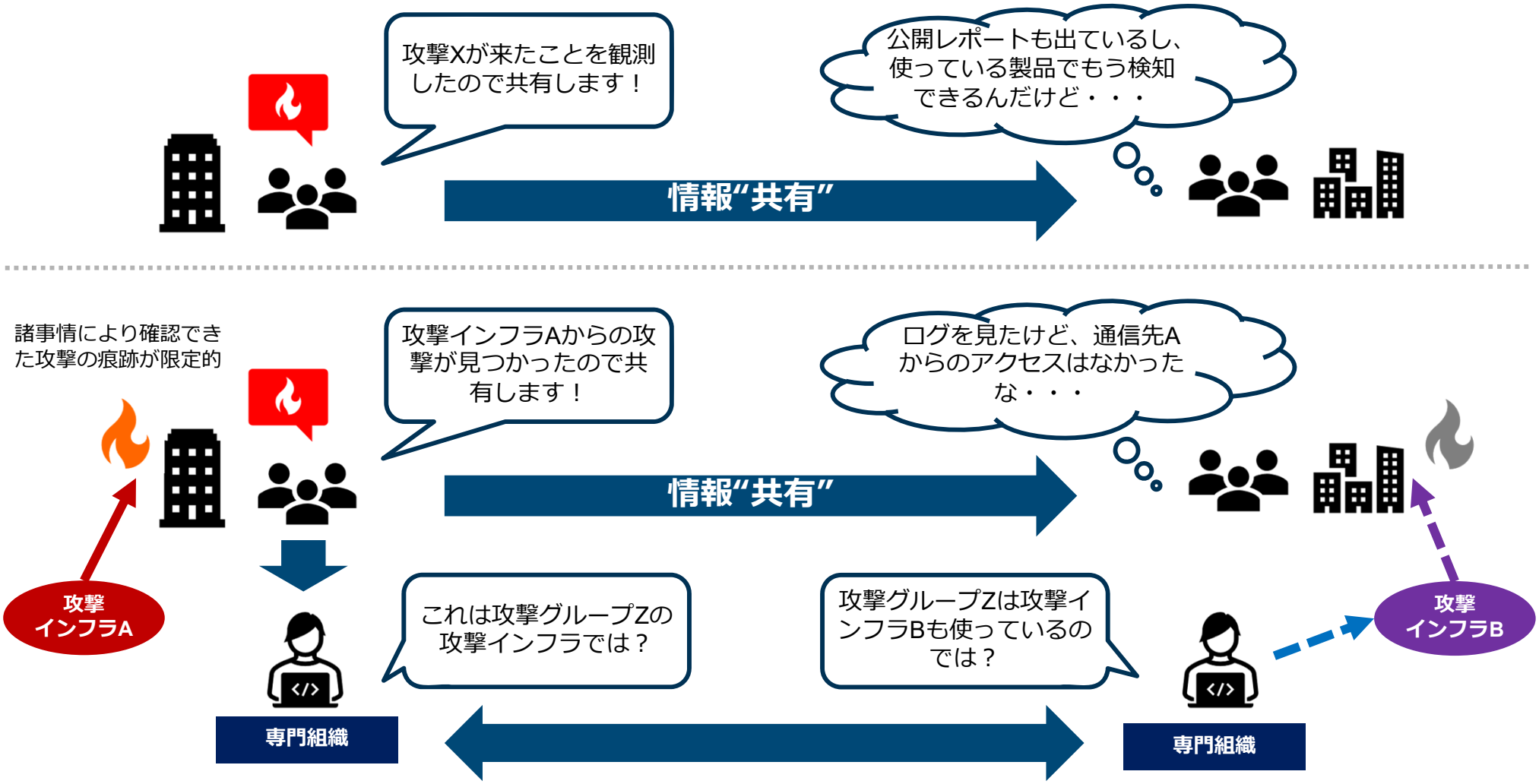




【情報共有の課題】共有内容のミスマッチ

参考資料：
26～34ページ参照

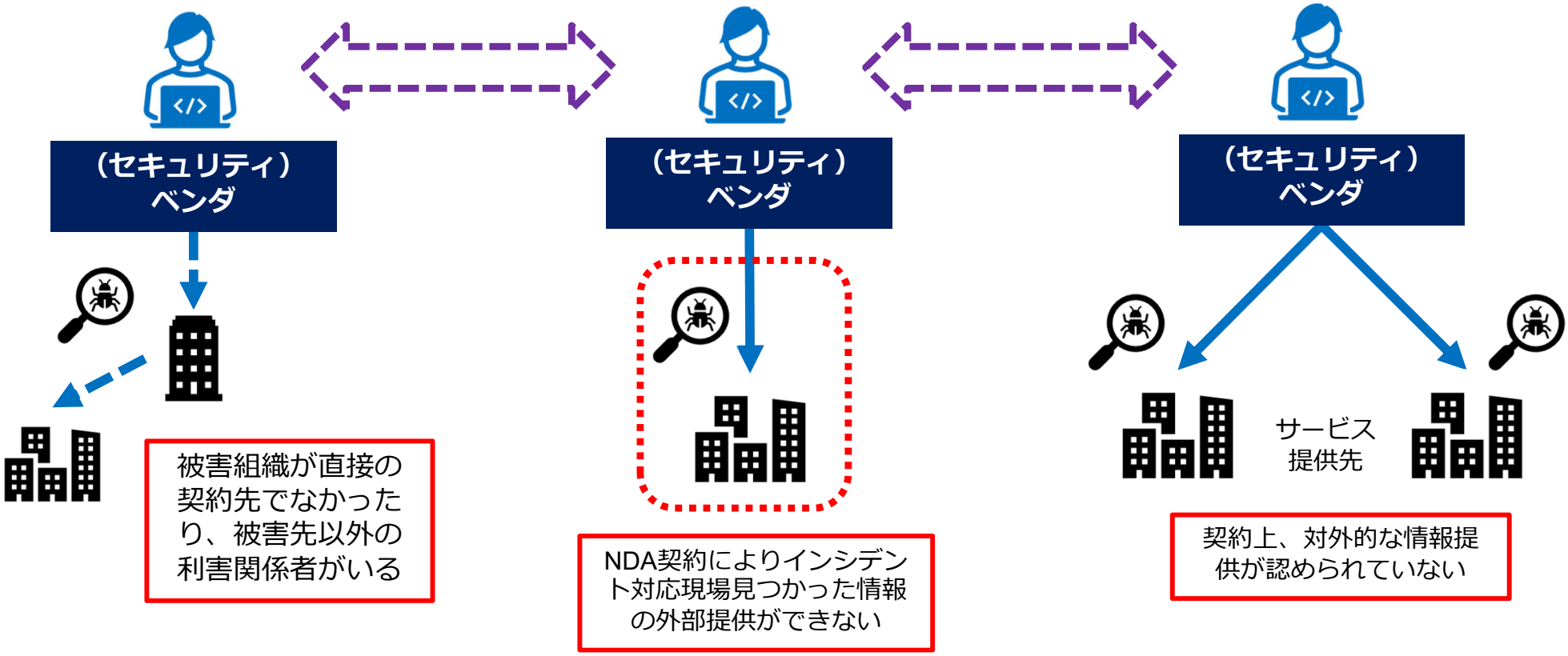
- 必ずしも情報共有に適さない種類の情報もある
- 調査の進捗次第により共有活動に提供できる情報が限定的な場合、専門組織のサポートがないと情報共有効果が発生しない場合がある



【情報共有の課題】専門組織間共有の障壁

参考資料：
35～45ページ参照

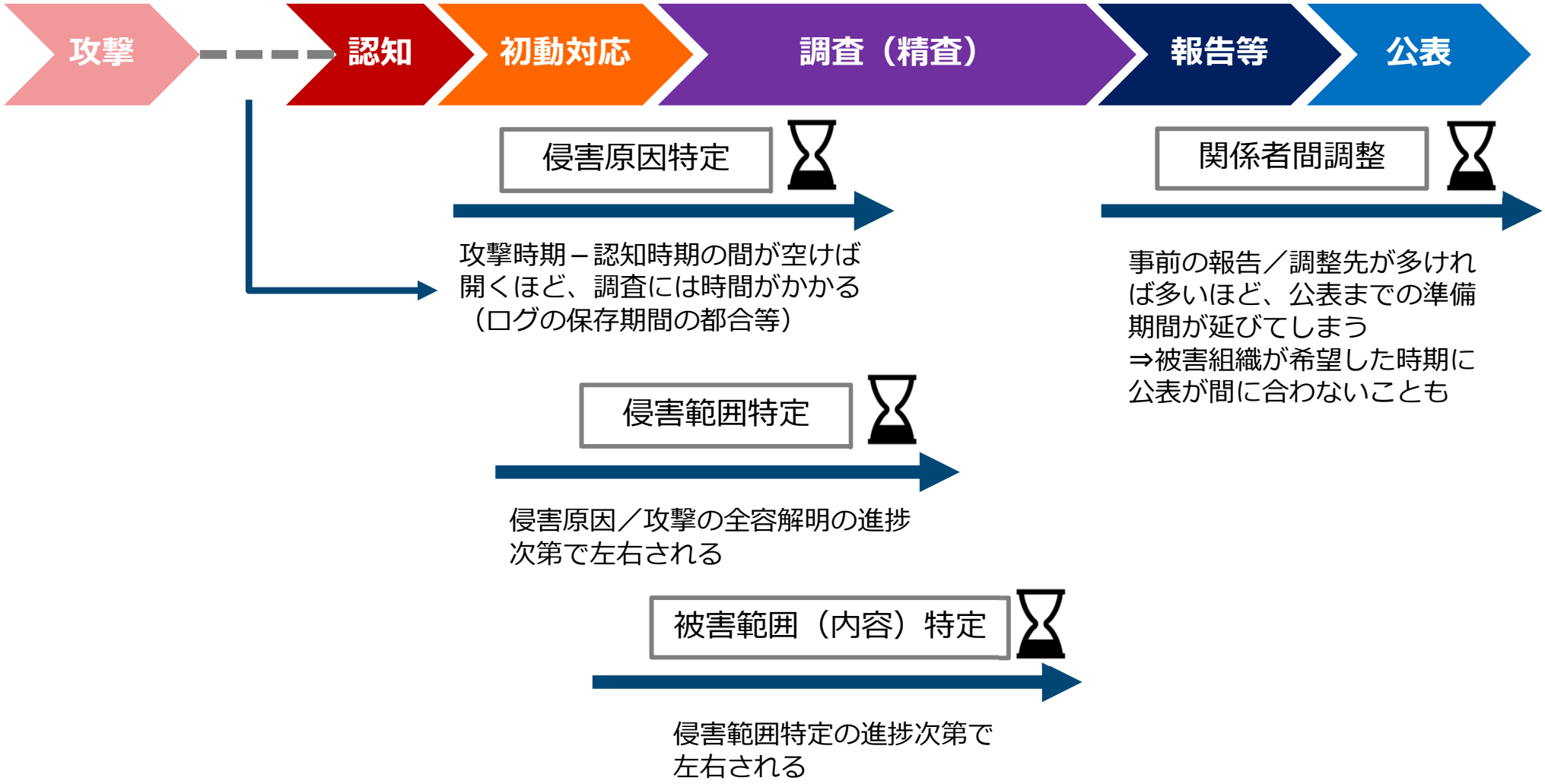
- 被害組織の支援にあたる（セキュリティ）ベンダはそれぞれ様々なサービス形態、契約形態の下で事案にタッチしているため、それぞれ外部に共有できる情報に差がある。あるいは、外部への情報共有自体ができない状況にある



【公表の課題】公表までに一定の時間を要するケース

参考資料：
47～48ページ参照

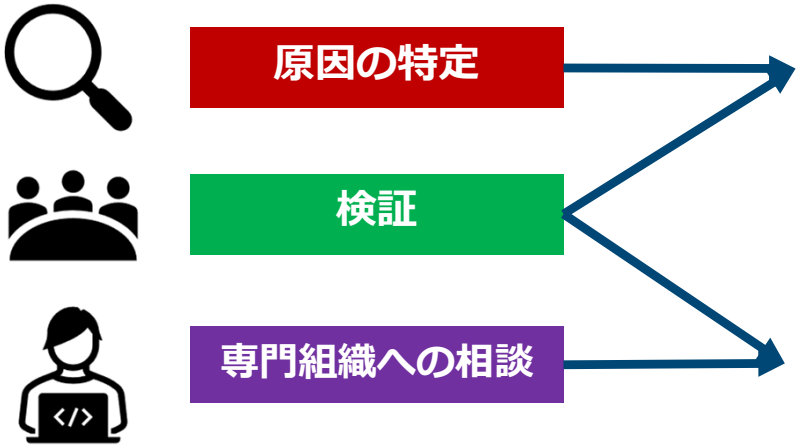
- 被害組織が「早期に公表したい」と考えていたとしても、調査進捗や関係者間調整により、公表時期は後ろ倒しになりがちである



【公表の課題】公表内容に納得感がないケース

参考資料：
49～50ページ参照

- インシデント対応に並行して、速報的な第1報～第n報～最終報と複数回にわたってが公表されるも、厳しい反応が見受けられるケース



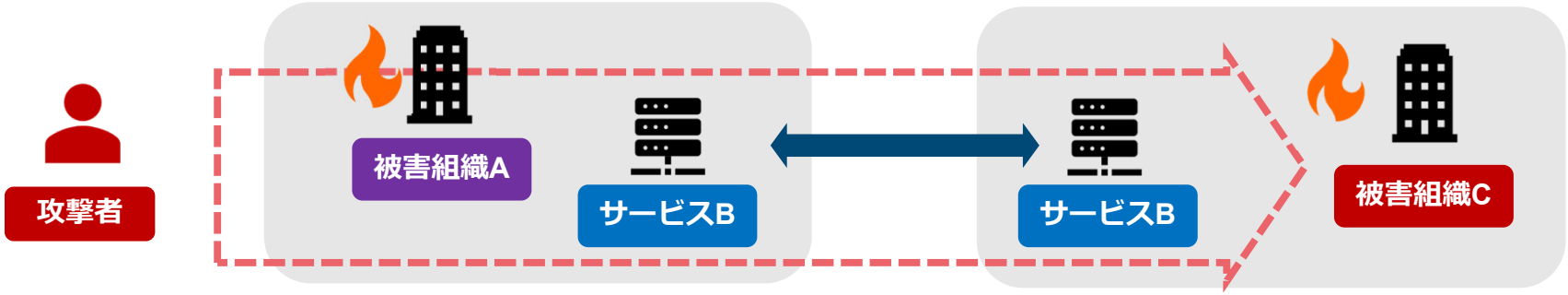
【評価が低かったポイント】
原因調査が芳しくない状況で、「検証委員会」や再発防止策等が並行／先行して発表されている

【評価が低かったポイント】
・原因調査が芳しくない状況で、外部専門知見を投入しているのか不明
・検証委員会は「検証」を行っているのか、原因調査に必要な知見提供をしているのか不明瞭

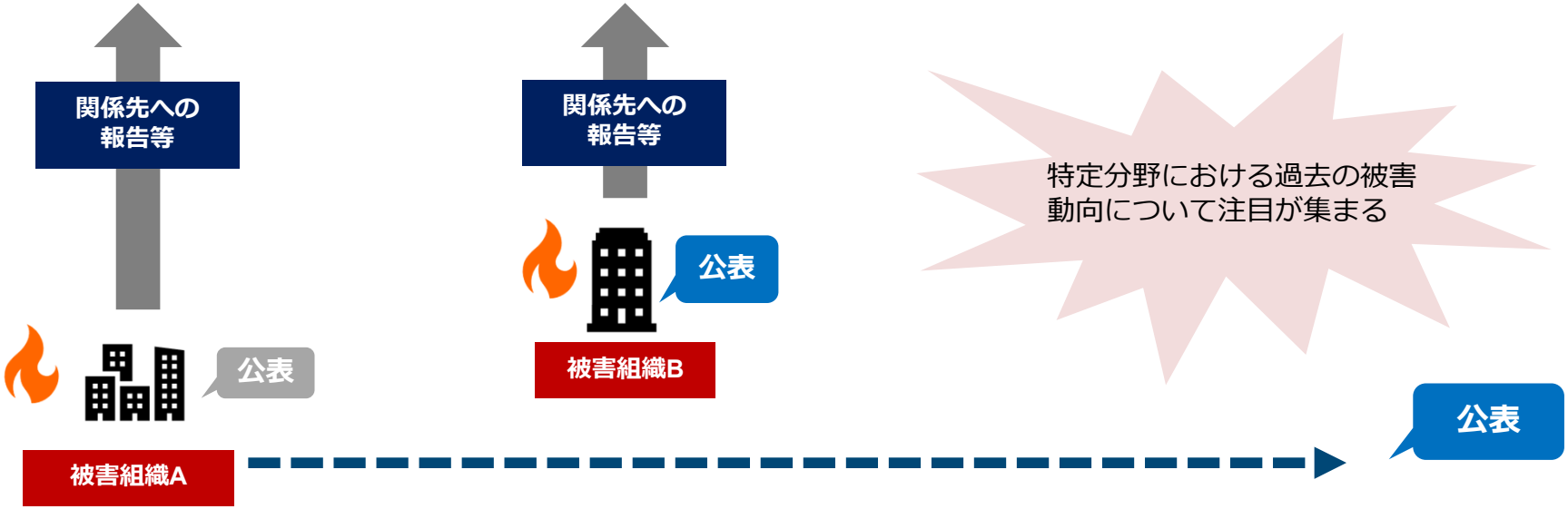
【ケース】の公表等により未公表の事実が判明するケース

参考資料：
51～54ページ参照

- 先行する被害組織Ａからの公表では詳細が明かされなかったところ、その後の取材や、二次被害先からの発表／二次被害先への取材等により、被害組織Ａからの公表内容以上の情報が後日明らかになるケース



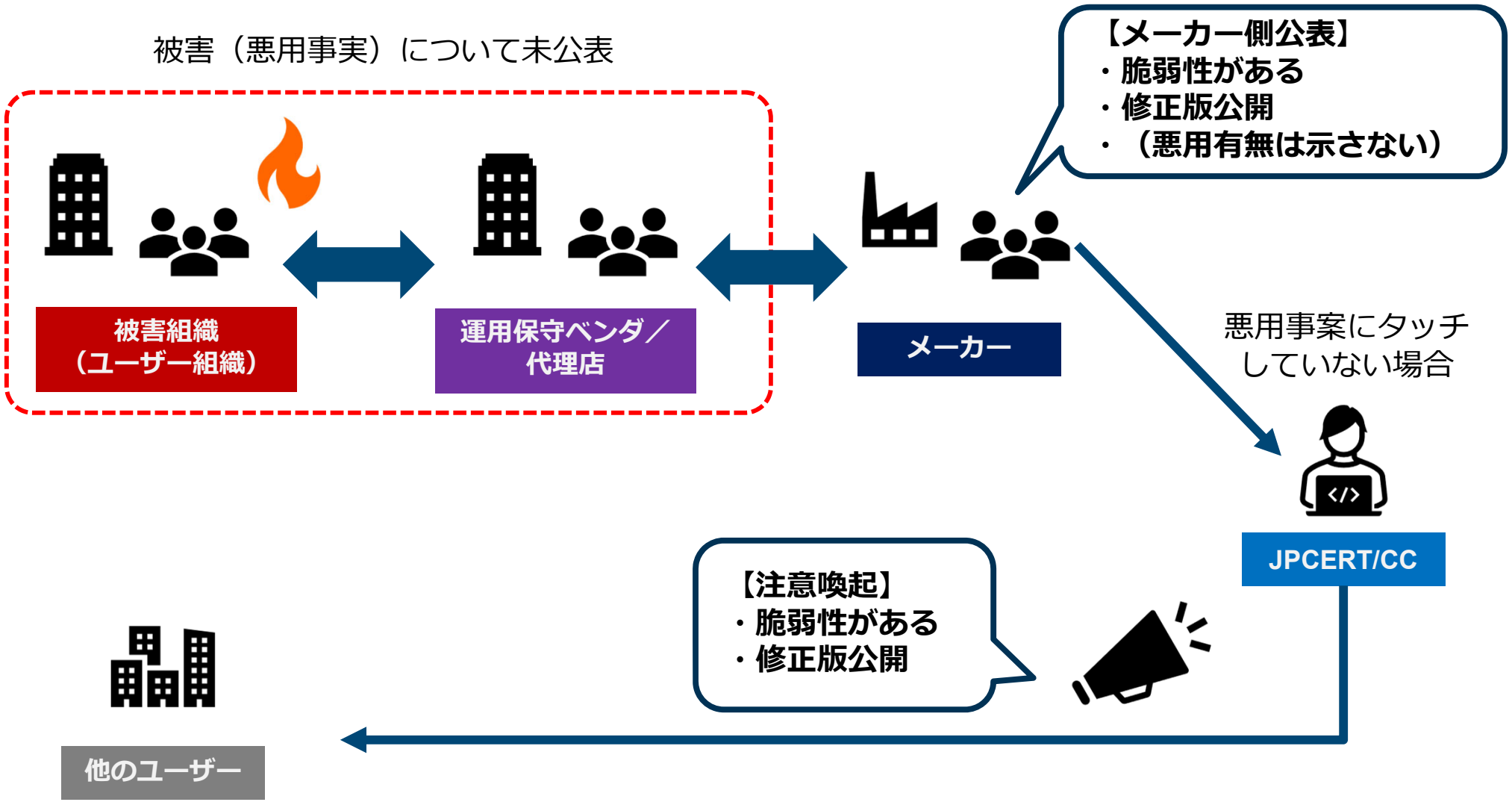
- 被害組織側が、対応当時には非公表と判断していたとしても、その後の状況の変化により過去の攻撃動向／被害状況について注目が集まるなどして、公表せざるを得なくなるケース



【公表の課題】被害が未公表であることの影響

参考資料：
57～59ページ参照

- 既に脆弱性の悪用被害があるにも関わらず、被害組織から未公表であるため、脆弱性公表時に「悪用情報」が含まれないケース



【被害組織保護】未公表被害が公開情報となる場合

参考資料：
61～64ページ参照

- 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）

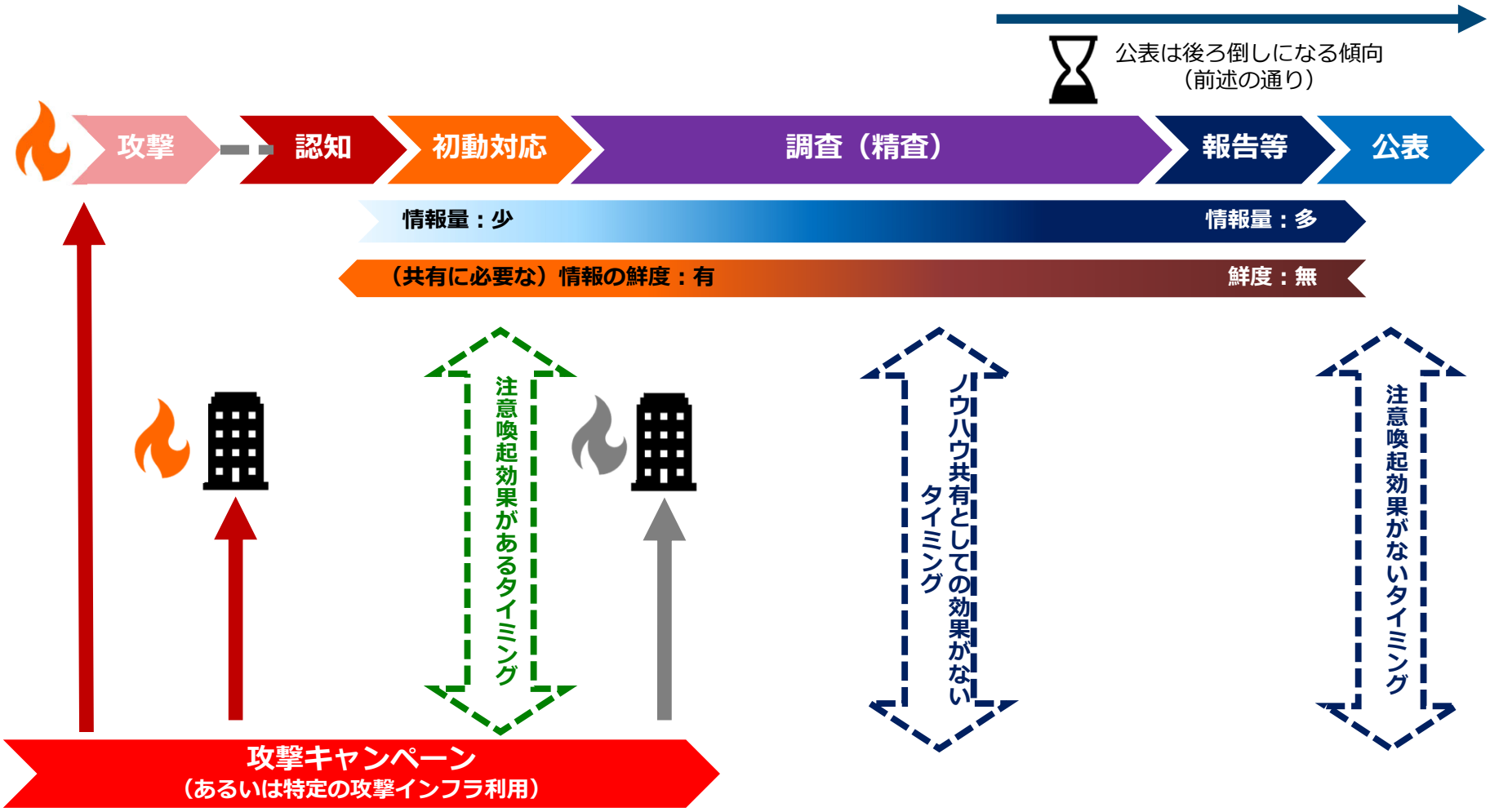
被害を観測しているもの → **被害（事実）を推測しているもの** → **被害の可能性の推測**

外形上攻撃被害が確認できる場合	漏えい情報の公開や犯行声明	（内部）関係者による情報発信	解析結果からの被害の推測	OSINTによるインフラ調査
例： Webサイト改ざん、Webサーバ等へのマルウェア設置	例： 第三者による漏えいデータの発見 リークサイト掲載	例： 従業員／顧客／取引先関係者によるSNS発信	例： 公開解析サービス上の検体解析結果からの推測	例： SHODAN,Censys等による脆弱なホストの調査

【共有と公表】注意喚起／ノウハウ共有目的の公表

参考資料：
75ページ参照

- （速報的な公表を除き）被害組織による公表は基本的に後ろ倒しになる傾向があるため、“注意喚起”目的の公表は、その喚起による効果をそもそも見込むことができない場合が多い
- 一方で対応「ノウハウ」の共有をするためには十分な調査と再発防止策が定まらなければならない

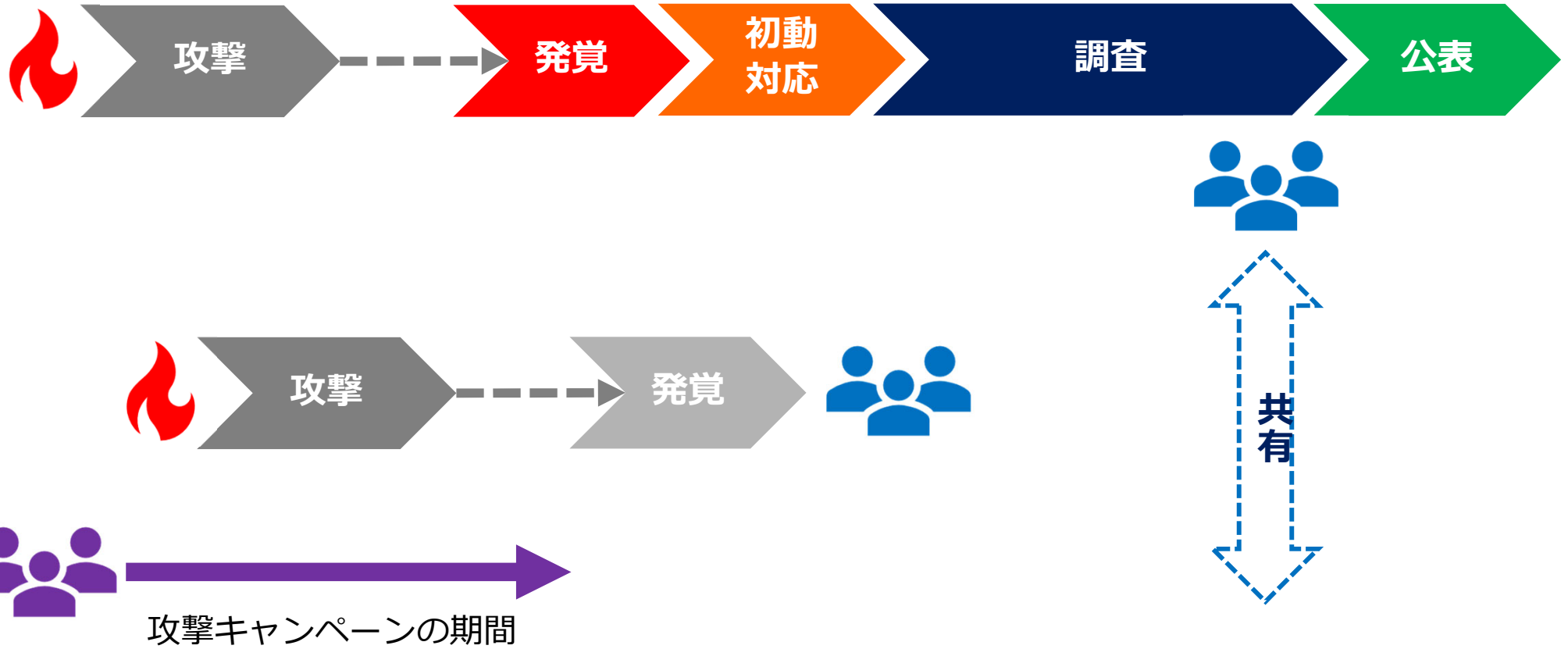


以下、参考資料

インシデント対応における情報共有の課題について

【ケース】「タイミング」のミスマッチが起きるケース

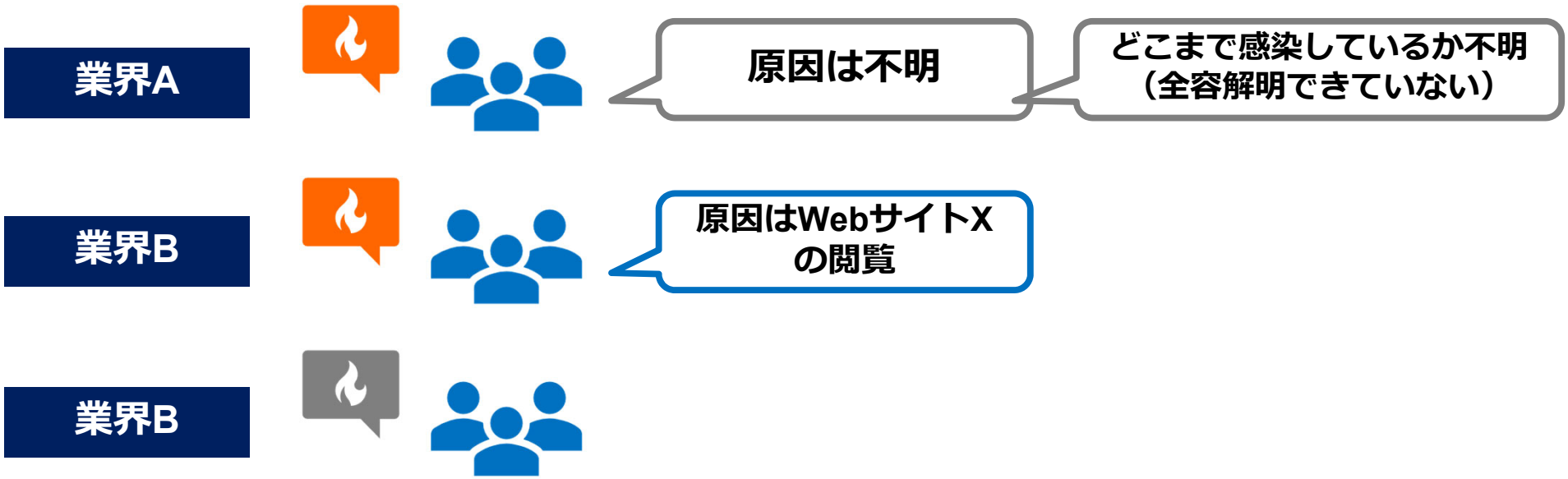
- 情報共有時点では既に攻撃キャンペーンが終了しており、共有効果（※）を得ることができない
- 必ずしも「早期に共有」できたとしても、共有効果が得られない場合もある（後述）



情報共有の「効果」とは？

- よくある説明
  - （他の組織における）被害防止
  - （次の）攻撃抑止
- これまで言及されてこなったポイント
  - 攻撃の解明
  - 攻撃の「規模」の把握

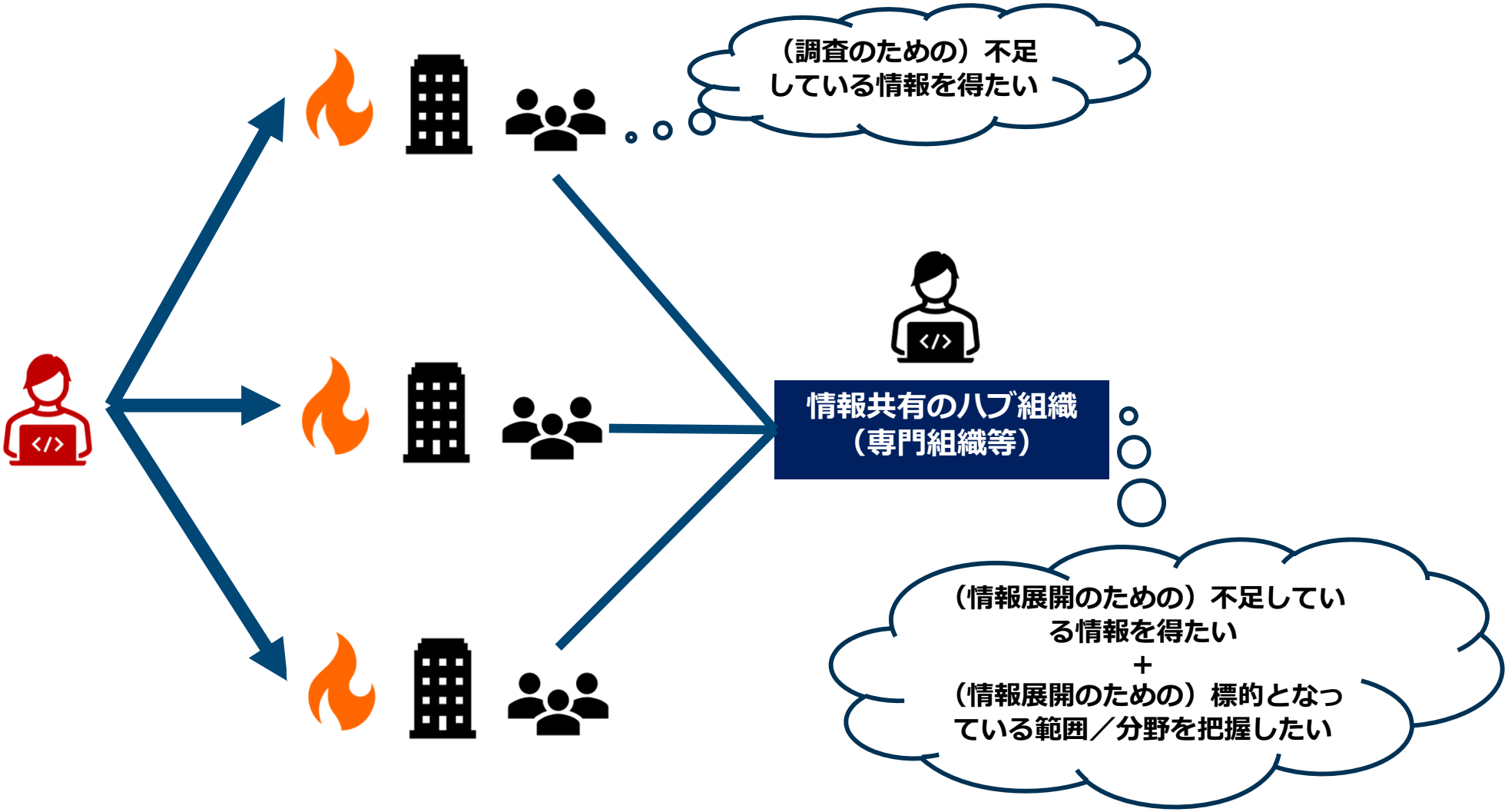
被害組織側、専門組織（共有ハブ組織）側、双方の目的が混在している



⇒特定の業界や固有のシステムを狙ったものではなく、Webサイトを閲覧した組織が感染

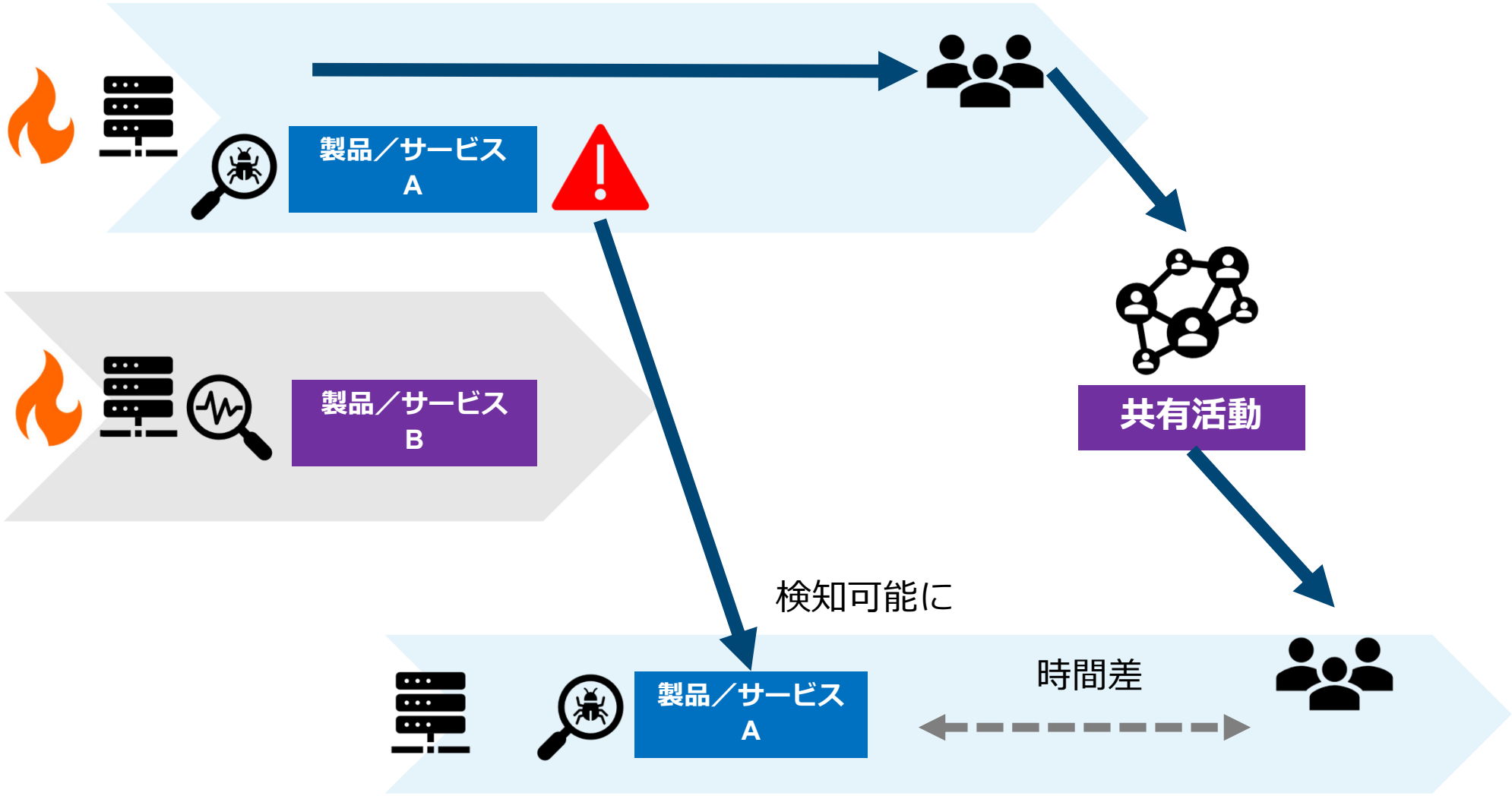
情報共有の「効果」とは？

■ 各立場によって共有の目的は（多少）異なる



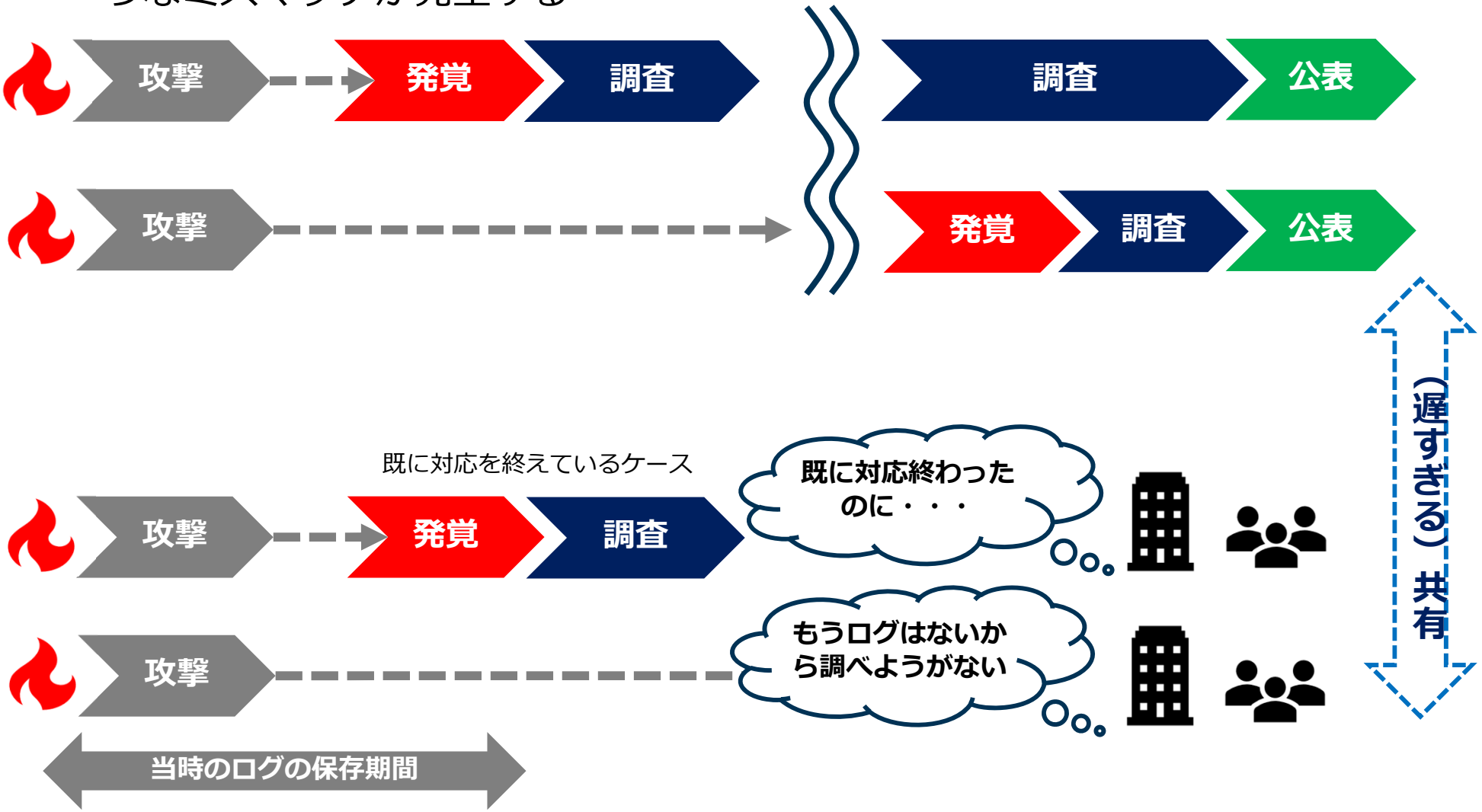
情報共有活動が本当に被害予防をしているのか？

- （セキュリティ）ベンダの製品／サービスなど見えないところで“情報共有”はなされている



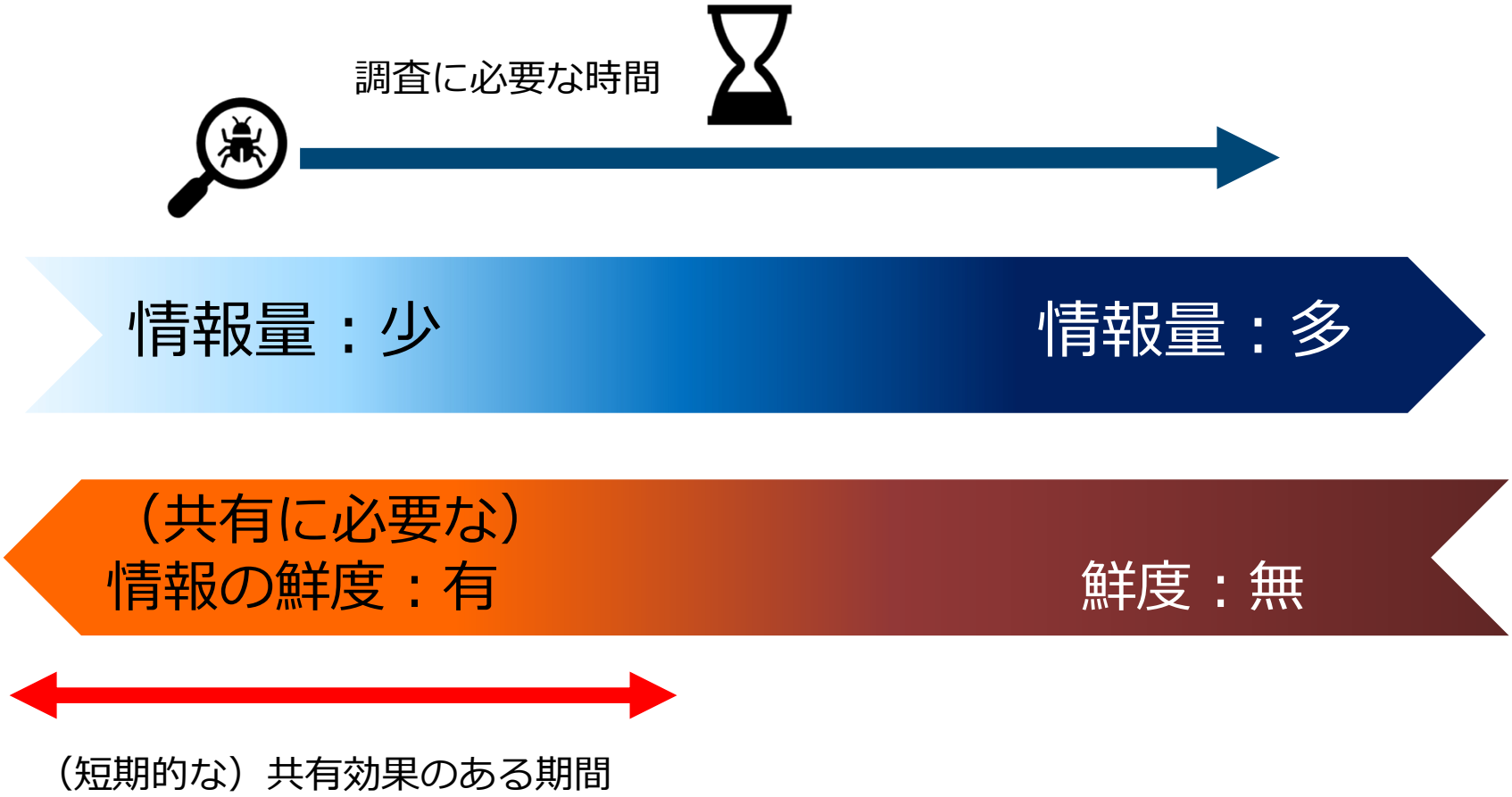
事案の「掘り返し」

- 相当期間経過した事案に関する情報が“共有”されてもフィードバックすら難しい場合がある
- 情報の展開元が、攻撃活動に対する時間軸的認識が不足している場合、このようなミスマッチが発生する



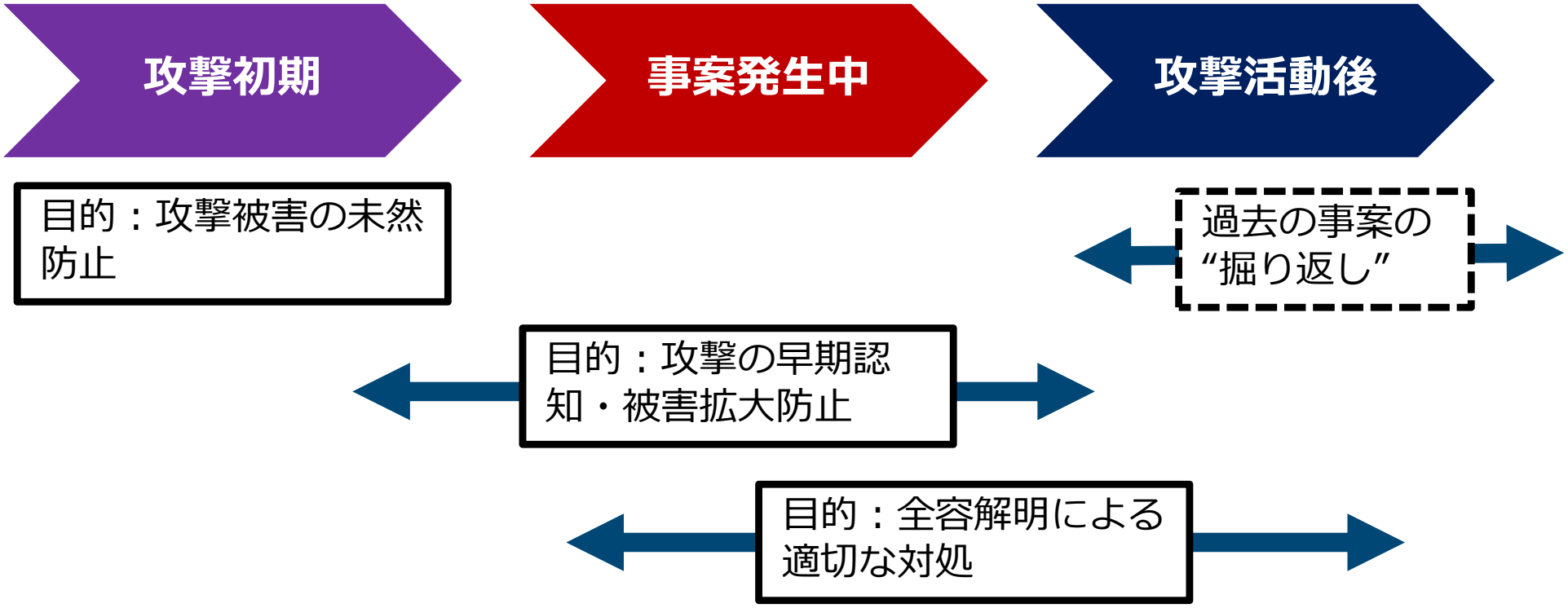
調査に必要な「時間」

- 全容が判明するまである程度の時間がかかる
- 断片的な情報であっても、ある程度判明した段階で外部に共有することが効果的



情報共有の現況と定義について

- 「情報共有」とひとくくりになっているが、実際には目的／効果の異なる情報共有活動が分野毎／目的毎に設置・活動している



「共有」の異なるタイミング／目的

■ いつ行う「共有」活動かによって目的／効果は異なる

	短期的共有	中期的共有	長期的共有
被害組織 （個別組織）	被害未然防止 早期検知	（被害の）全容解明 （原因特定、被害範囲特定）	
情報共有活動 （参加組織側全体）	被害拡大防止	※個社対応フェーズに移る	ノウハウ共有
情報共有活動 （ハブ組織側）	攻撃範囲把握	※個社対応フェーズに移る	
専門組織	原因特定	（攻撃の）全容解明	攻撃グループの動向把握

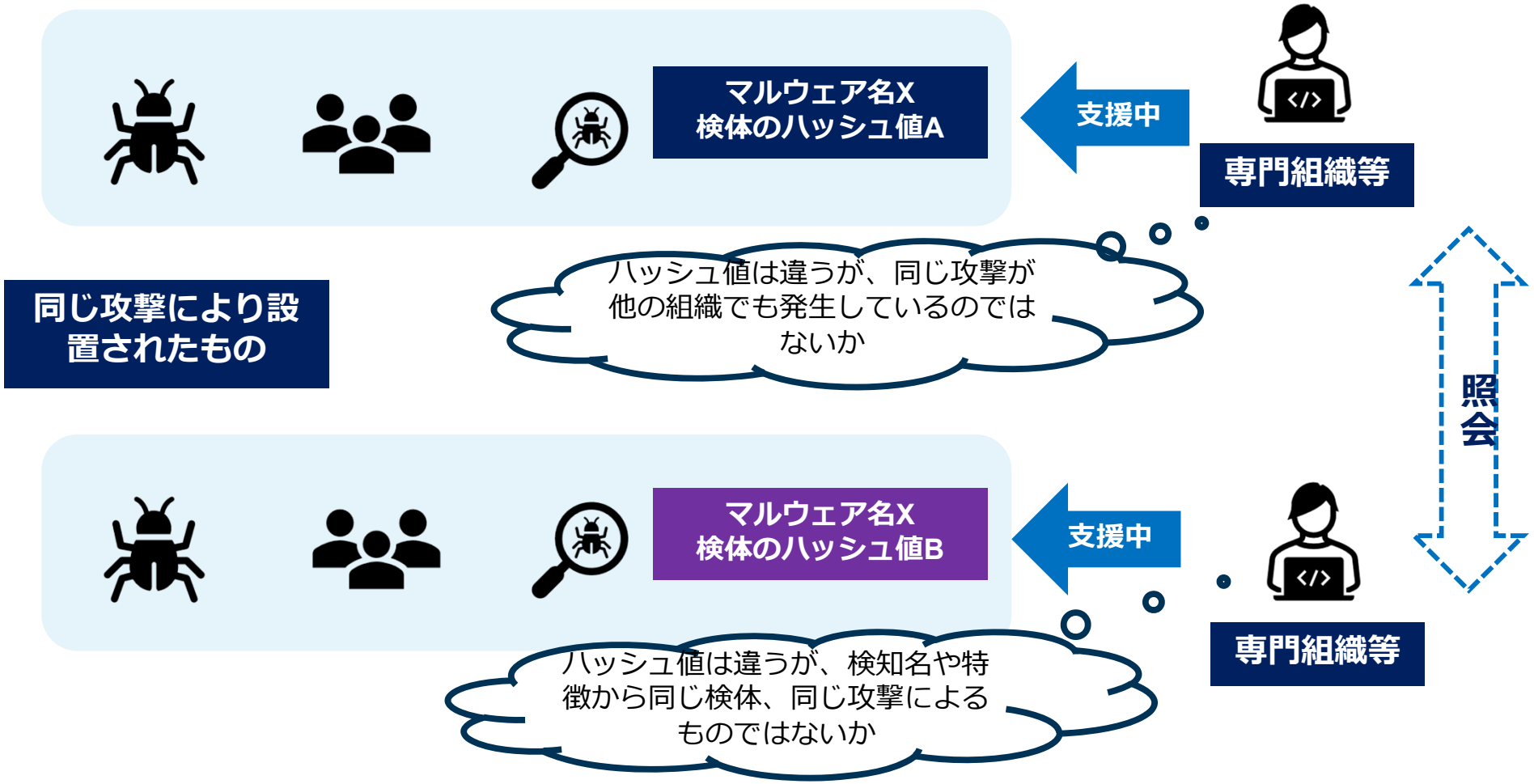
【ケース】情報の内容のミスマッチが起きているケース

- 様々な理由で、検体のハッシュ値や検知名しか共有活動に提供できないケース

違うハッシュの可能性もあれば、そもそもハッシュ値で検索できない可能性もある

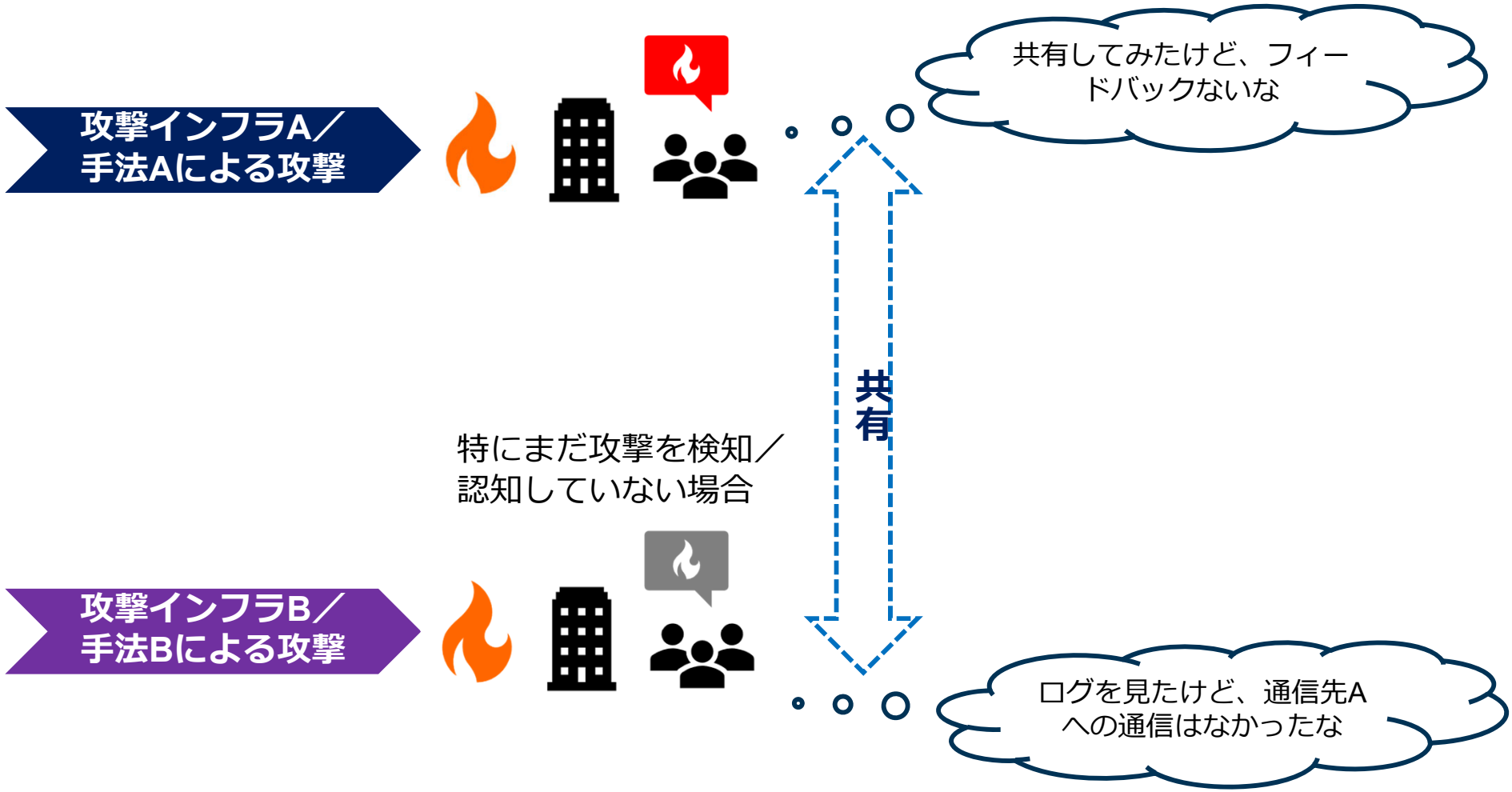
どのような扱い方が適切か

- 各事案対応にはいっている専門組織同士が「照会」を行うための「キー」情報として用いる
- ハッシュ値以外のTTP情報等、「同じ攻撃活動ではないか」と推測させる他の情報とセットで用いて初めて効果があるのではないか



必ずしもフィードバックを得られるわけではない

- 攻撃インフラに重複がない攻撃類型や、展開した情報が限定的である場合、必ずしも情報共有活動でフィードバックを得られない場合がある



情報提供（照会）と情報共有のギャップ

- 最初から「情報共有」活動への展開を依頼してくるケースもあれば、専門機関／セキュリティベンダでの「情報提供」（※専門機関／ベンダへの照会）として連絡してくるケースも混在している。
- 元々被害組織が情報共有活動に「期待していること」と実際に共有活動で得られる可能性のある情報とのギャップが、攻撃類型毎、共有タイミング毎に発生してしまうところ、これを事前に被害組織側は知ること／予測することができていないため、情報共有側との間にミスマッチが発生する

どのような情報の共有が必要か

技術情報

- 侵入方法
- マルウェア／ツール
- 通信先

※被害組織Aでは見つからなかった情報

コンテキスト情報

- 対処内容、経緯
- 被害範囲、内容

・同じ攻撃方法に関する情報が見つかる可能性がある
・互いに足りない情報を補填し合える可能性がある

被害組織の規模、業態、システム構成や、保有情報によって異なる

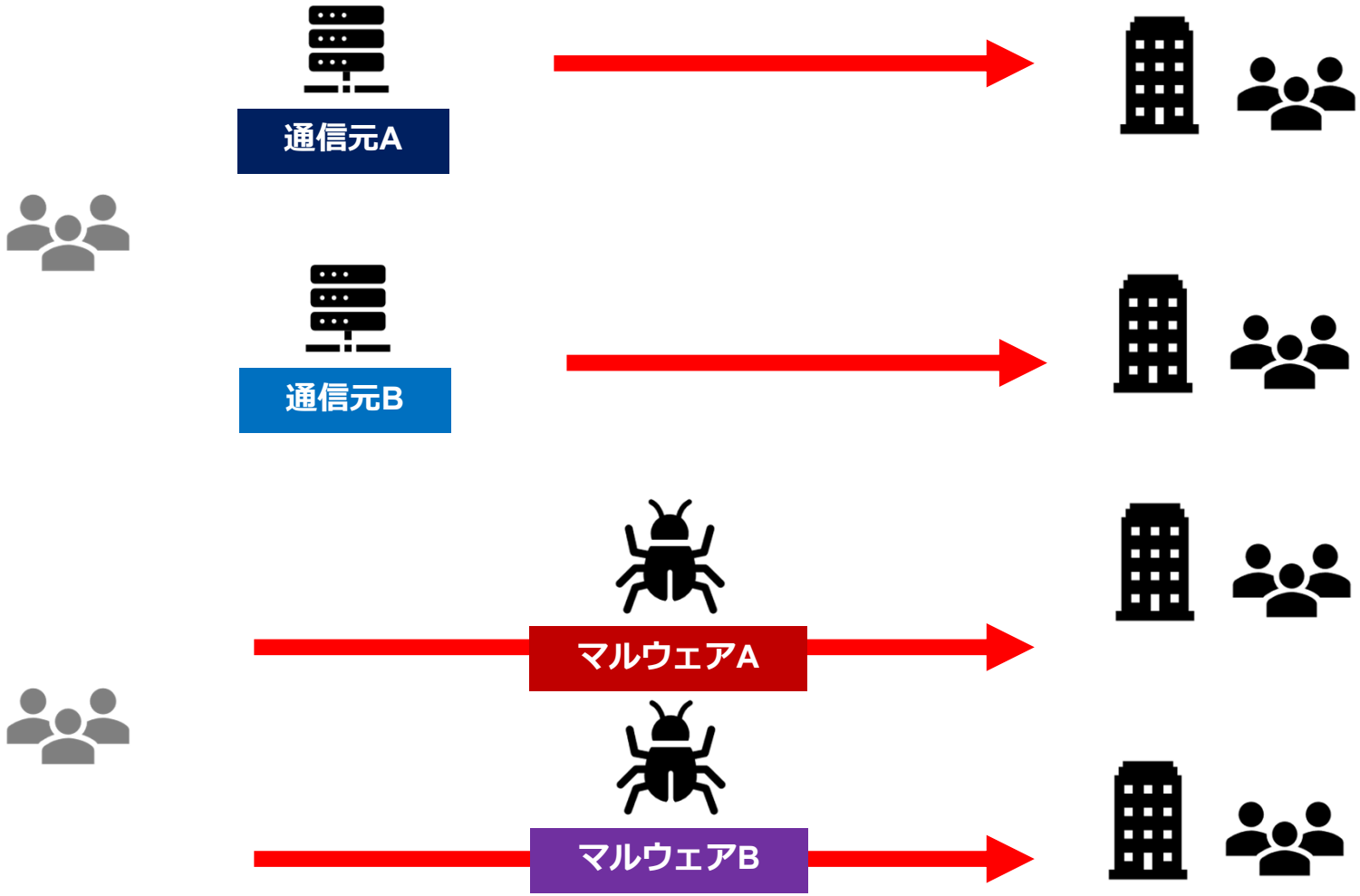
- 侵入方法
- マルウェア／ツール
- 通信先

※被害組織Bでは見つからなかった情報

- 対処内容、経緯
- 被害範囲、内容

「共有効果」が得られない攻撃類型があること

- 通信先が標的毎に異なる
- 使用されるマルウェアが標的毎に異なる



どういう情報の共有が共有効果があるのか

- ある程度の期間内において、複数の標的組織に対して同一の攻撃インフラを使いまわしている場合
- 同一ハッシュ値を持つマルウェア等を用いる場合
- 特定の初期侵害方法／特徴的なTTPが見られる場合

攻撃類型毎の共有効果

- あらゆる種類の攻撃類型において必ずしもユーザー組織間での情報共有が有効とは限らない
- ただし、専門組織間においては、攻撃類型を問わず、共有が有効なケースが多い
- 「共有してみないと、共有が有効がどうかわからない」ケースもあり得るが、専門組織が展開予定の情報をある程度精査・補強する必要がある

攻撃インフラ：使いまわし
TTP：ある程度一致
例）標的型サイバー攻撃

→ 共有効果あり

※標的型サイバー攻撃：いわゆる「Advanced Persistent Threat (APT) 」

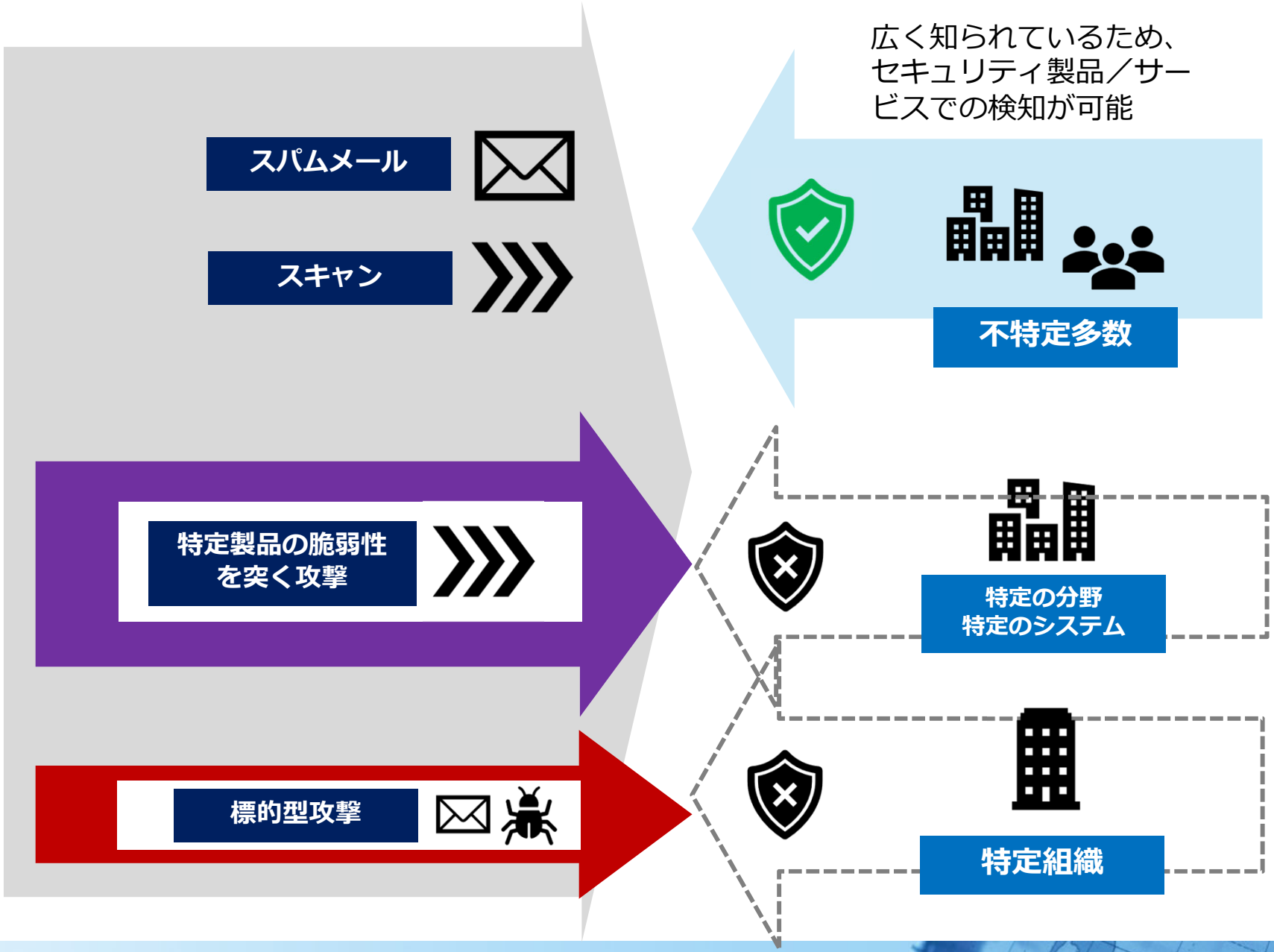
攻撃インフラ：バラバラ
TTP：ある程度一致
例）（いわゆる）標的型ランサム攻撃

→ 共有効果は限定的
※専門組織間では共有もなお有効

攻撃インフラ：バラバラ
TTP：バラバラ
※ただし、特定製品の脆弱性を悪用するケース
例）Webサーバの脆弱性を突く不正アクセス

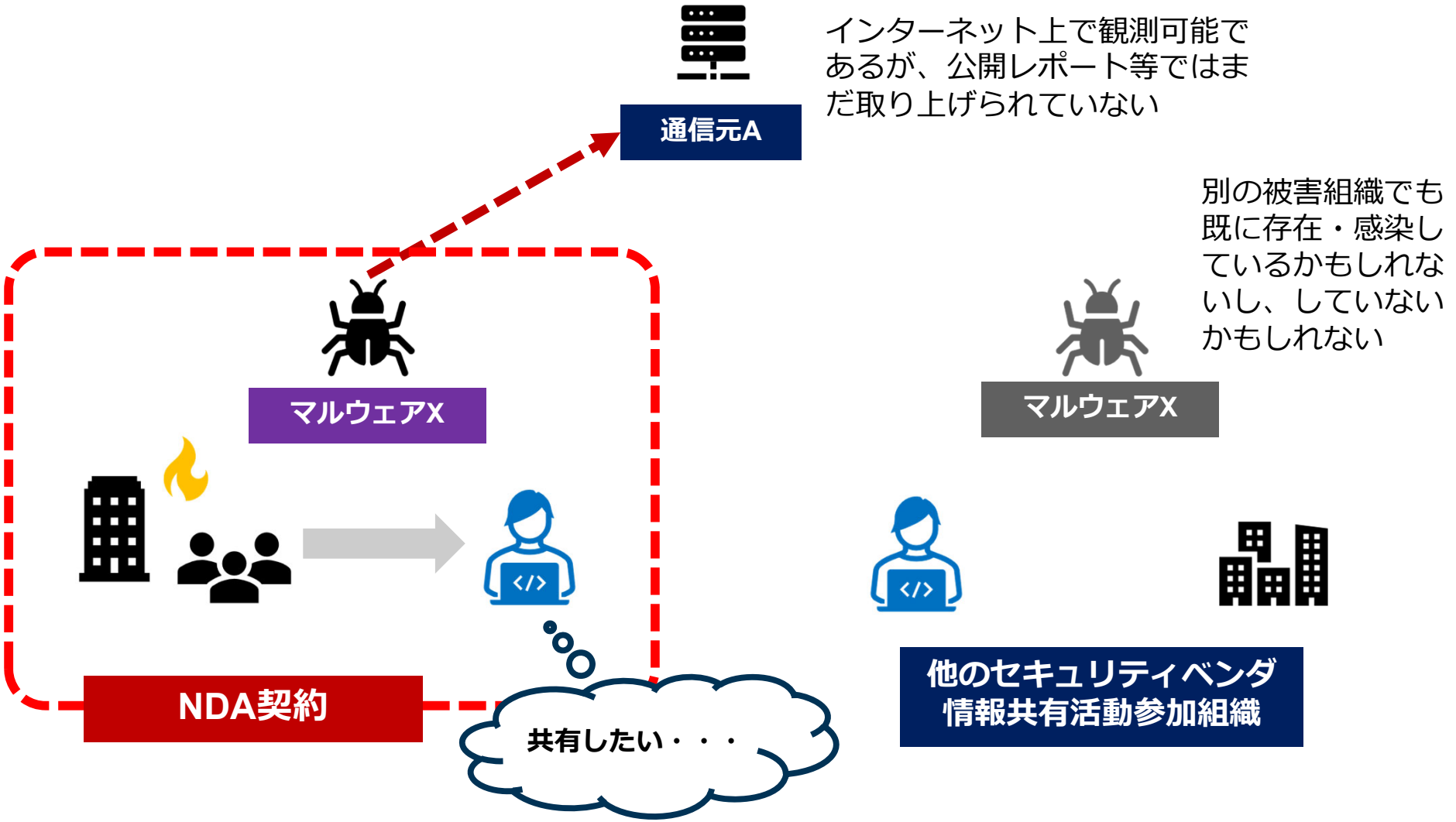
→ 共有よりも注意喚起が有効
※専門組織間では共有もなお有効

どのような攻撃類型は情報共有の対象に向いているか



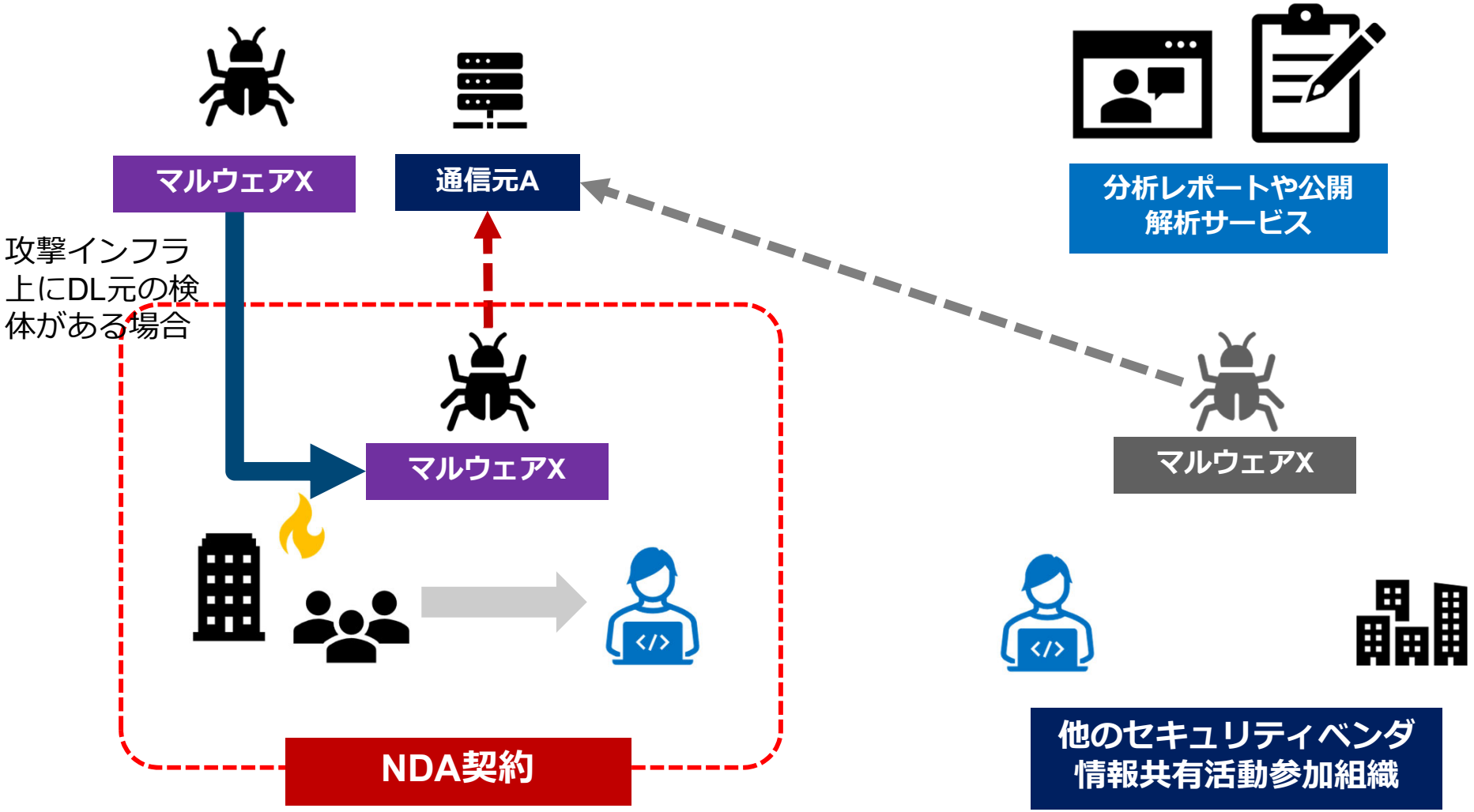
【ケース】インシデント対応組織における問題

- 被害組織とのNDA契約により、見つけたIoC情報を第三者に提供し情報共有できないケース



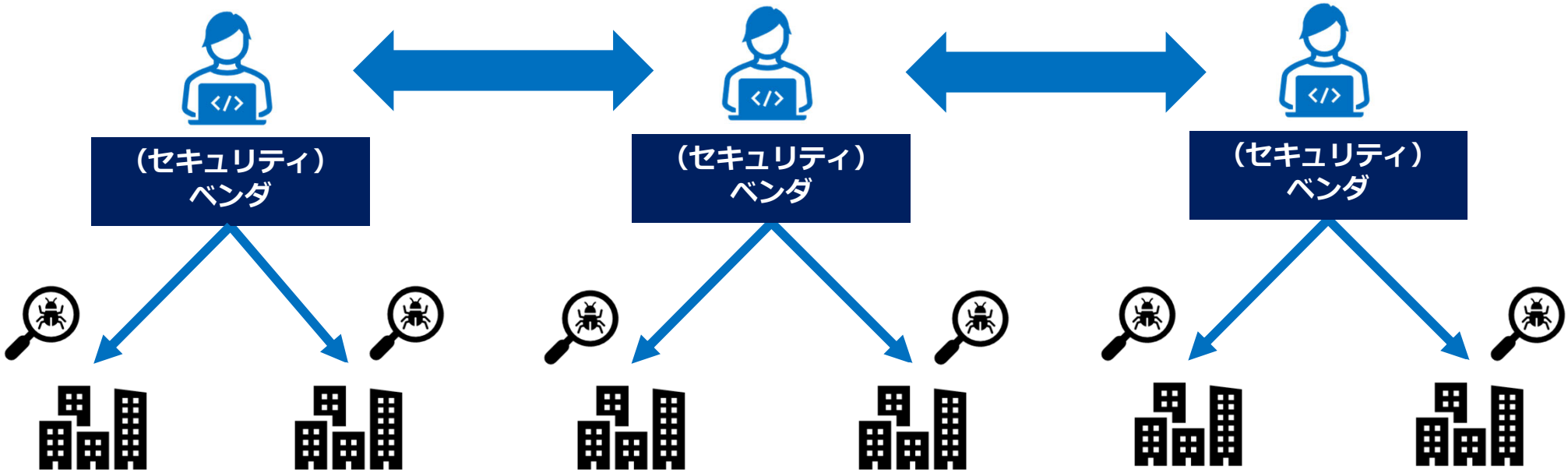
「公開情報」とは何か

- 「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



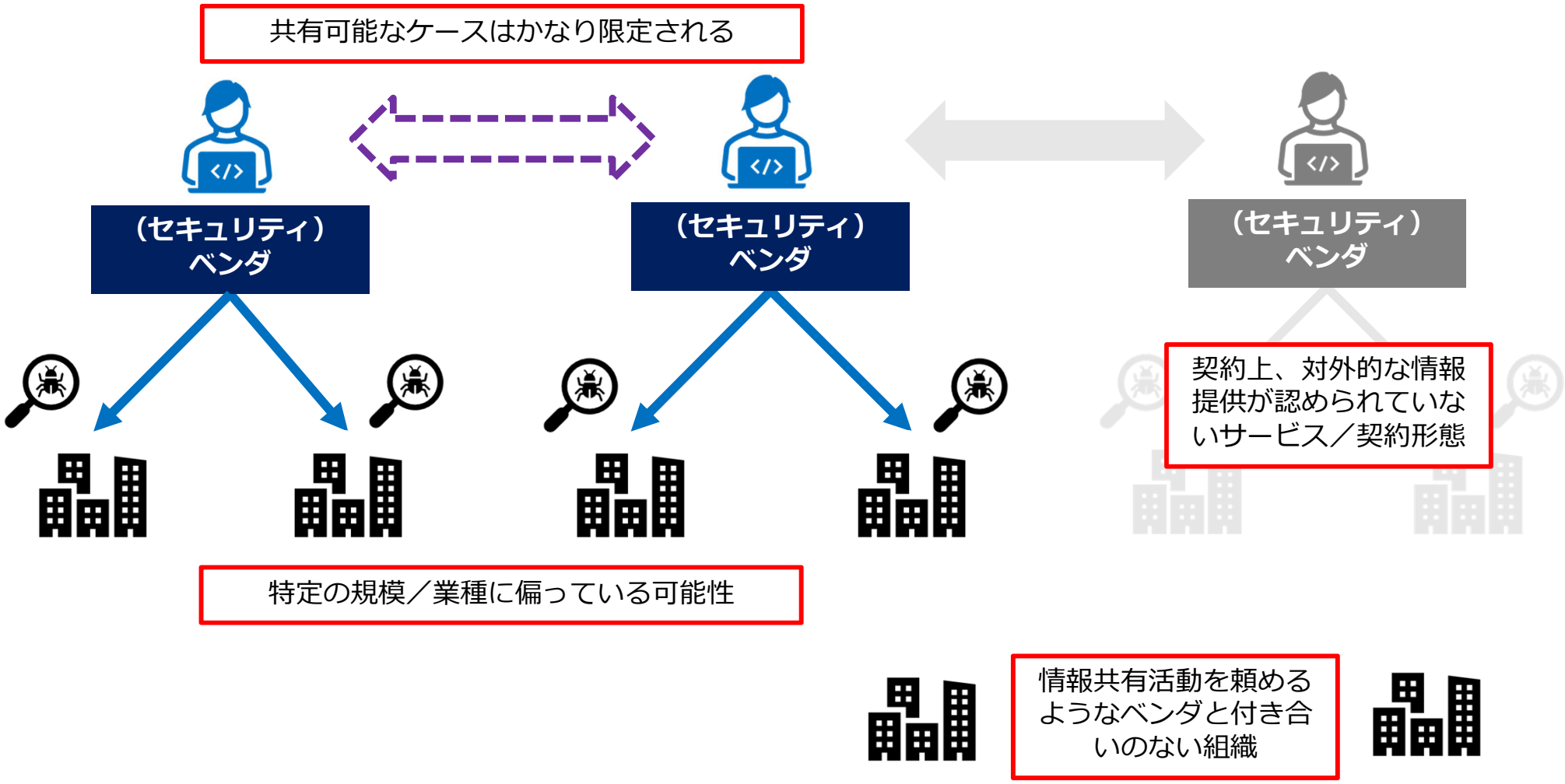
情報共有の理屈上の“理想”

- 被害組織／ユーザー組織側が個別に情報共有“コスト”を負担するのではなく、これらの組織をフォローしている（セキュリティ）ベンダ同士で見えている情報を共有すれば済むのではないか、と考えられがち（※とある情報共有活動立ち上げ時に関係省庁から出た意見）



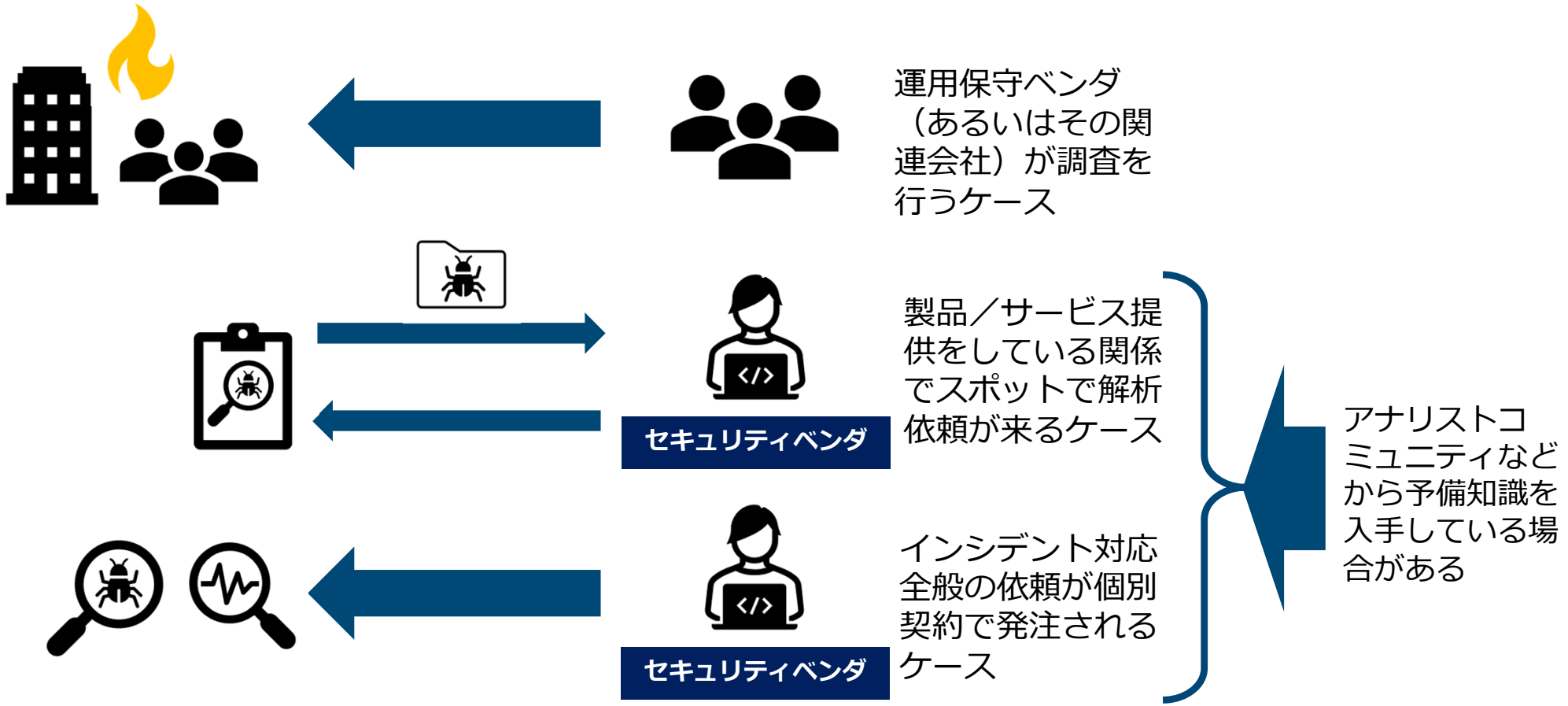
理屈上の“理想”と“現実”

- 実際の（セキュリティ）ベンダ間の情報共有は後述の要因により、かなり限定的なものにとどまっている（※サイバーセキュリティ協議会等、JPCERT/CCがセキュリティベンダ等と情報共有を行っている現状から）



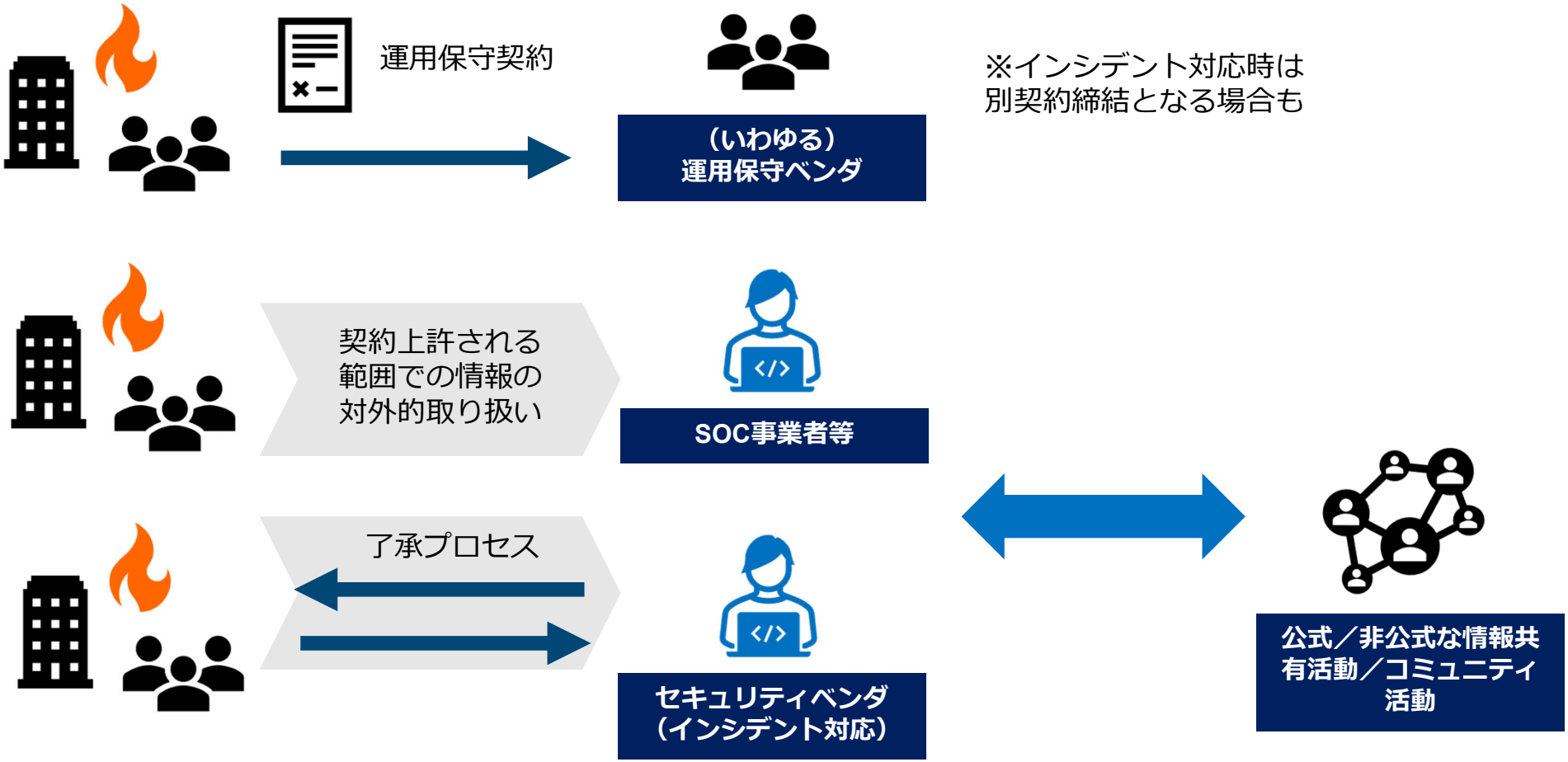
運用保守ベンダ、セキュリティベンダ

- ※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



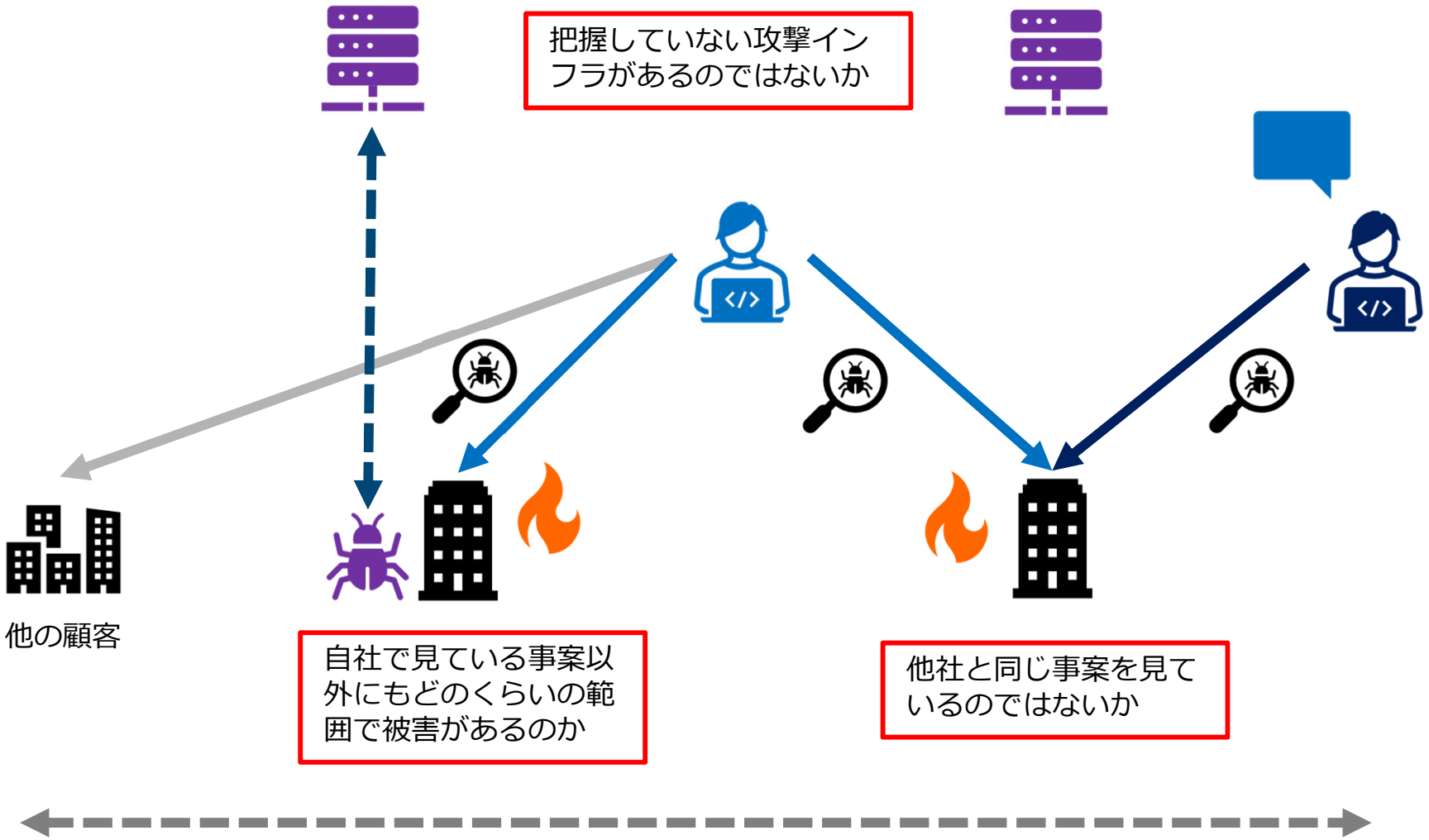
（セキュリティ）ベンダの情報共有活動

- 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



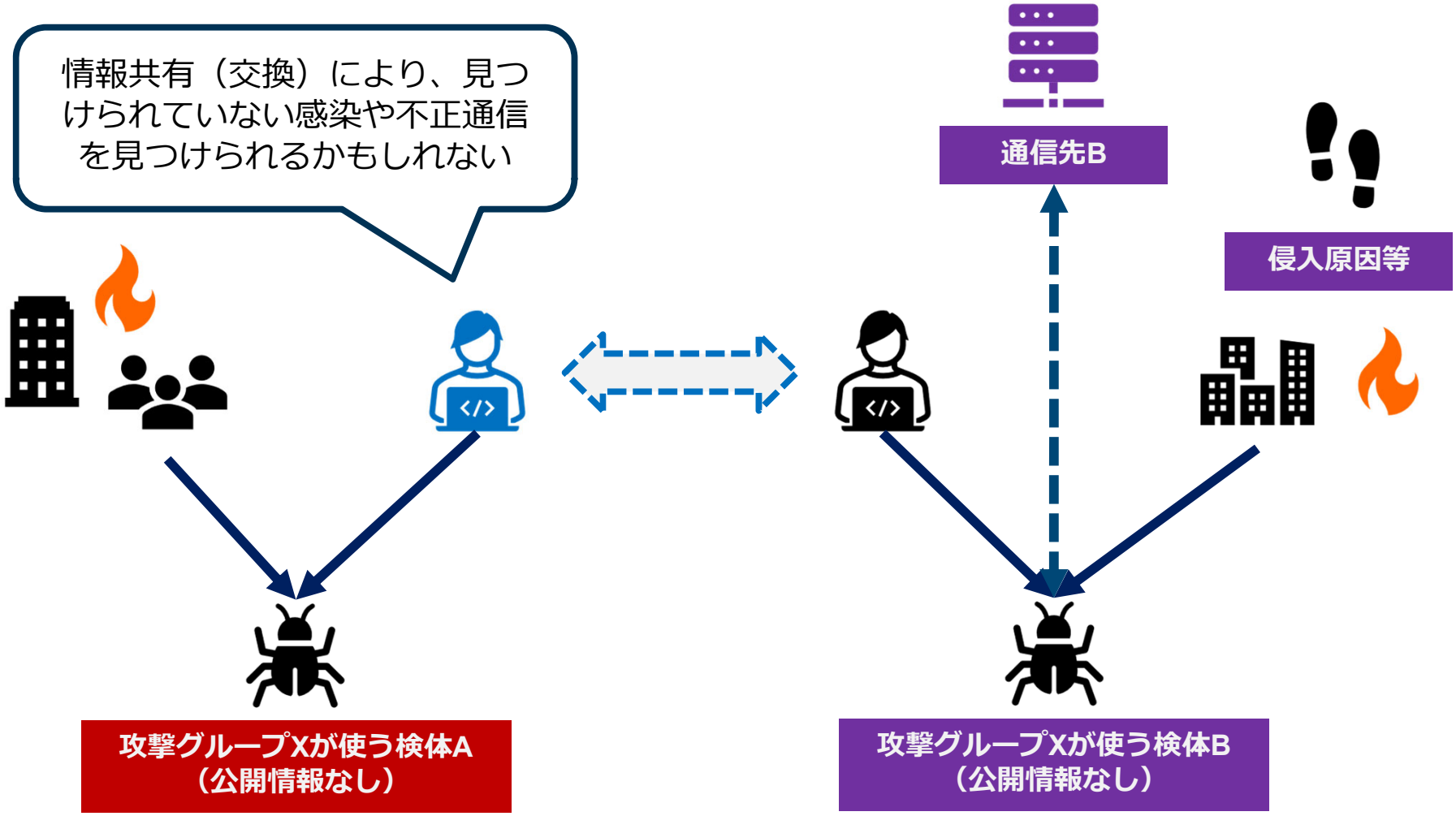
（セキュリティ）ベンダとしての情報共有

■全容把握のための情報共有のニーズ



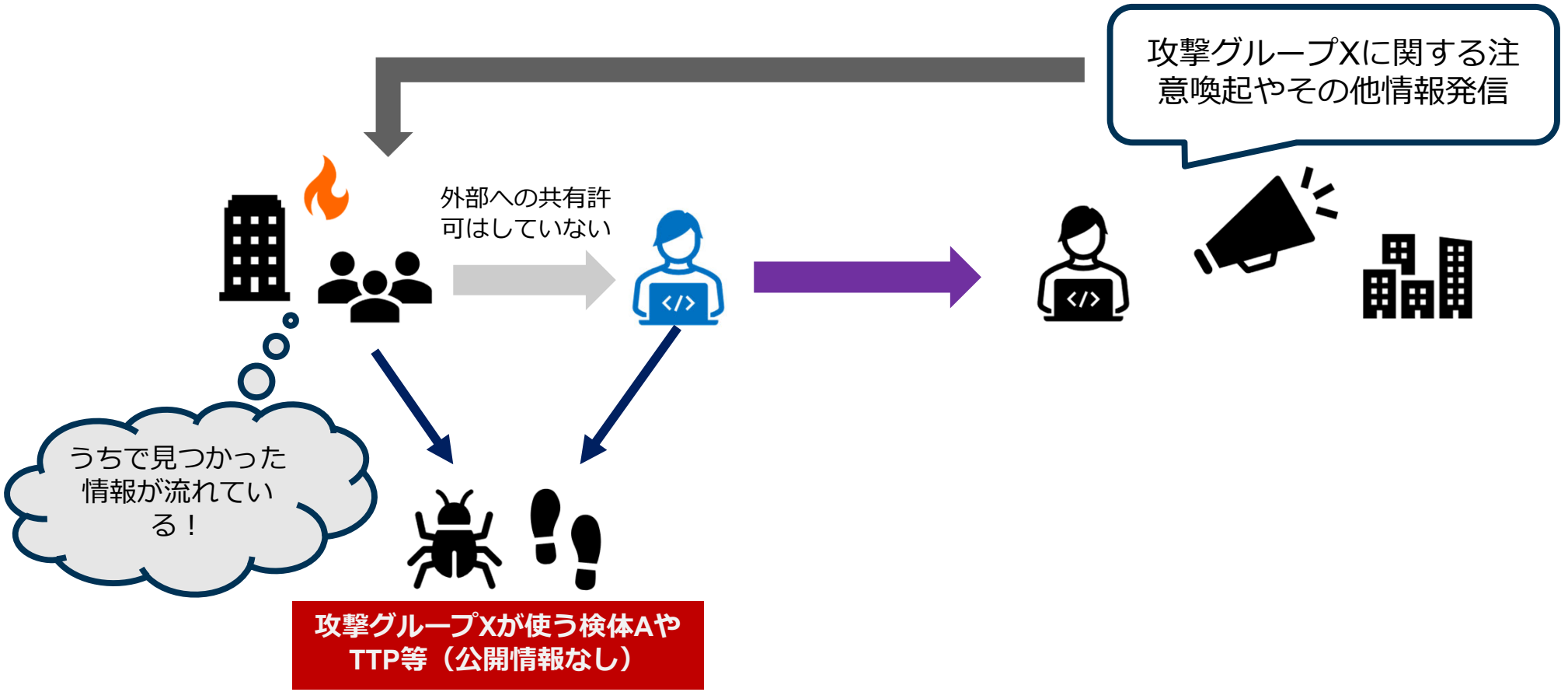
被害組織からどのように「了解」してもらうか

- 専門機関間、（セキュリティ）ベンダ間の情報共有が“詰まる”背景
- 基本的に被害組織の意向に左右される



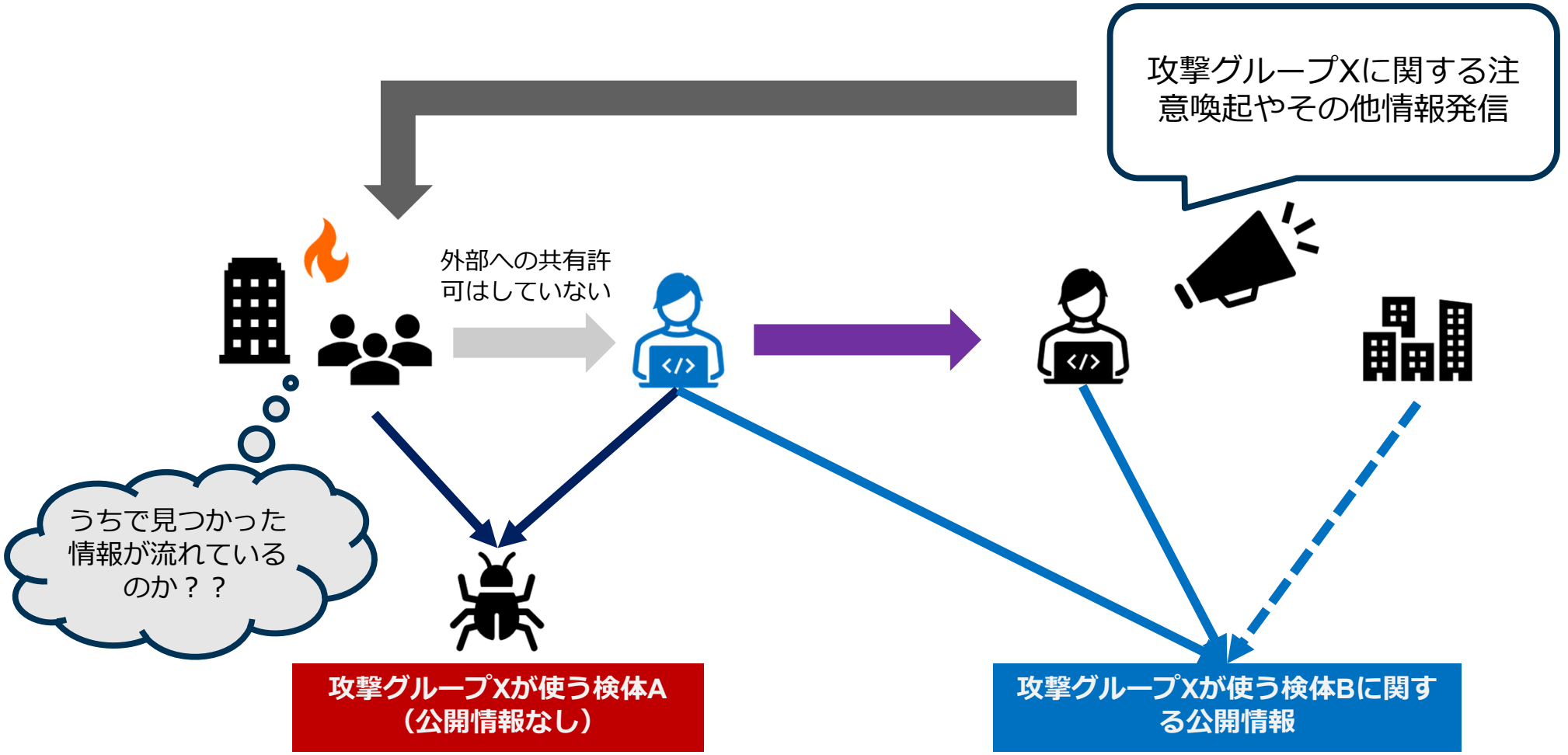
情報共有の“滞留”ポイント

- 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



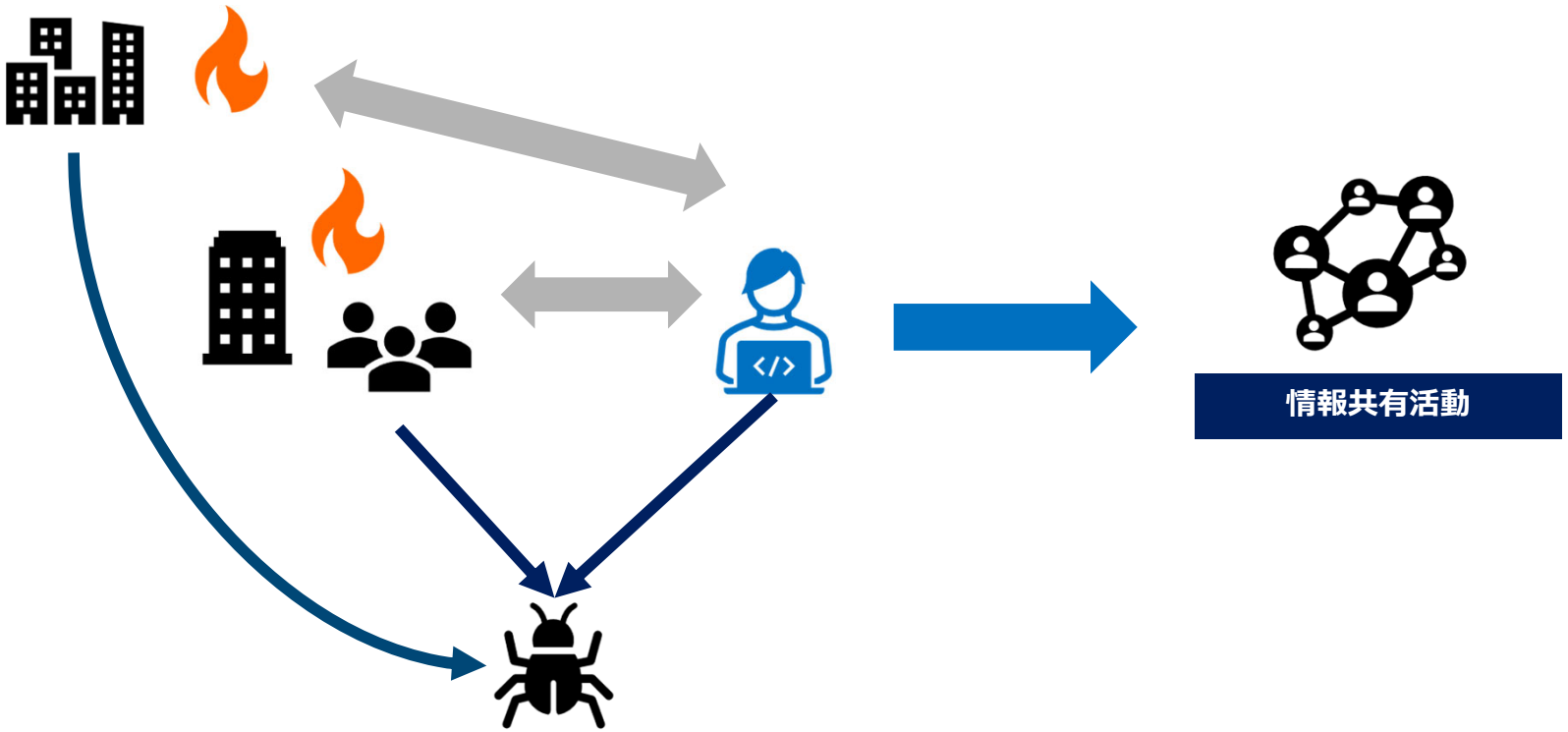
情報共有の“滞留”ポイント

- 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



被害組織からどのように「了解」してもらうか

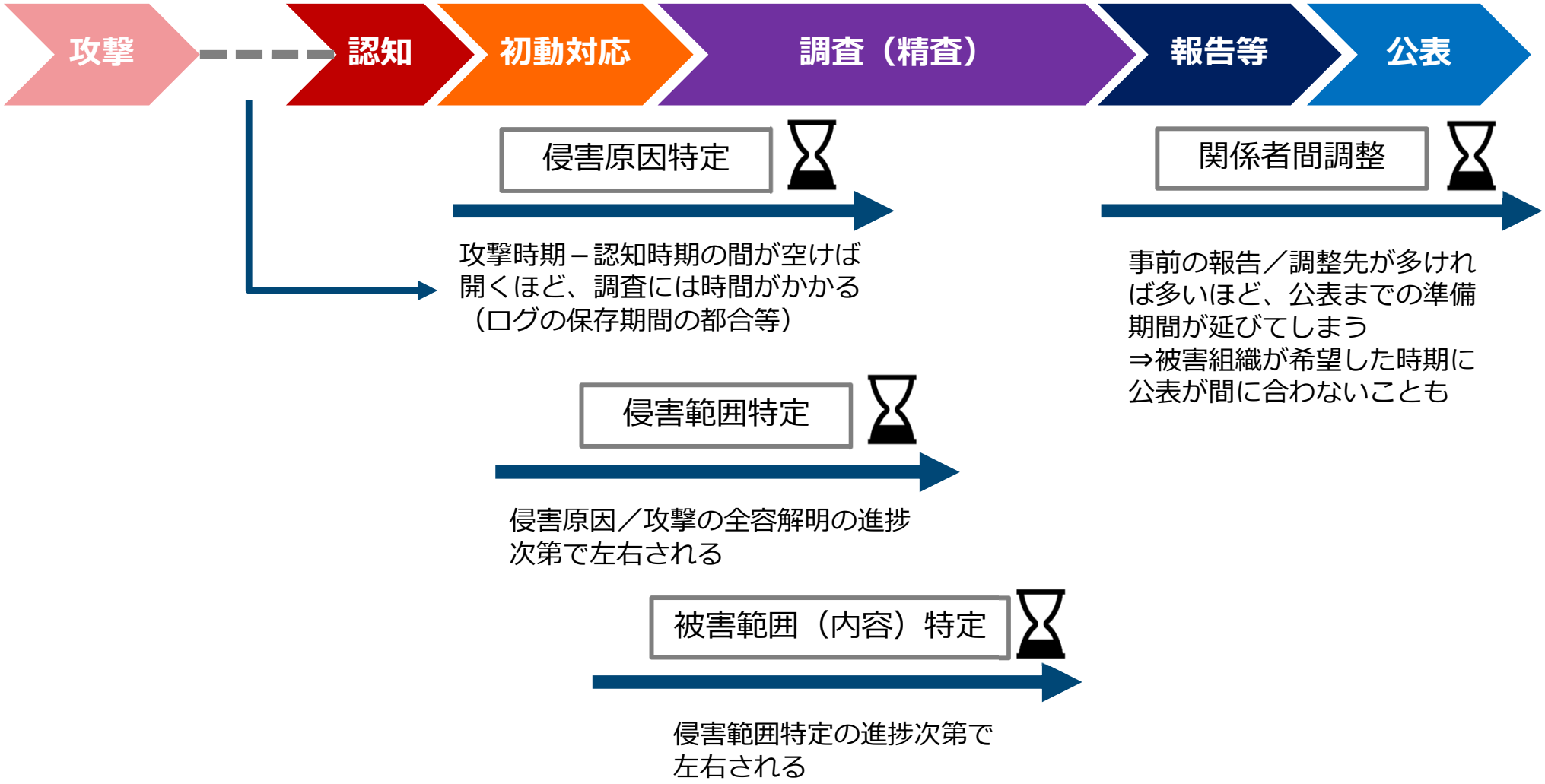
- 複数組織で既に同一検体／通信（左記）が見つかっている場合は前述の懸念がなくなるため、個別に了承は取らずに情報共有を行う



インシデント対応における公表の課題について

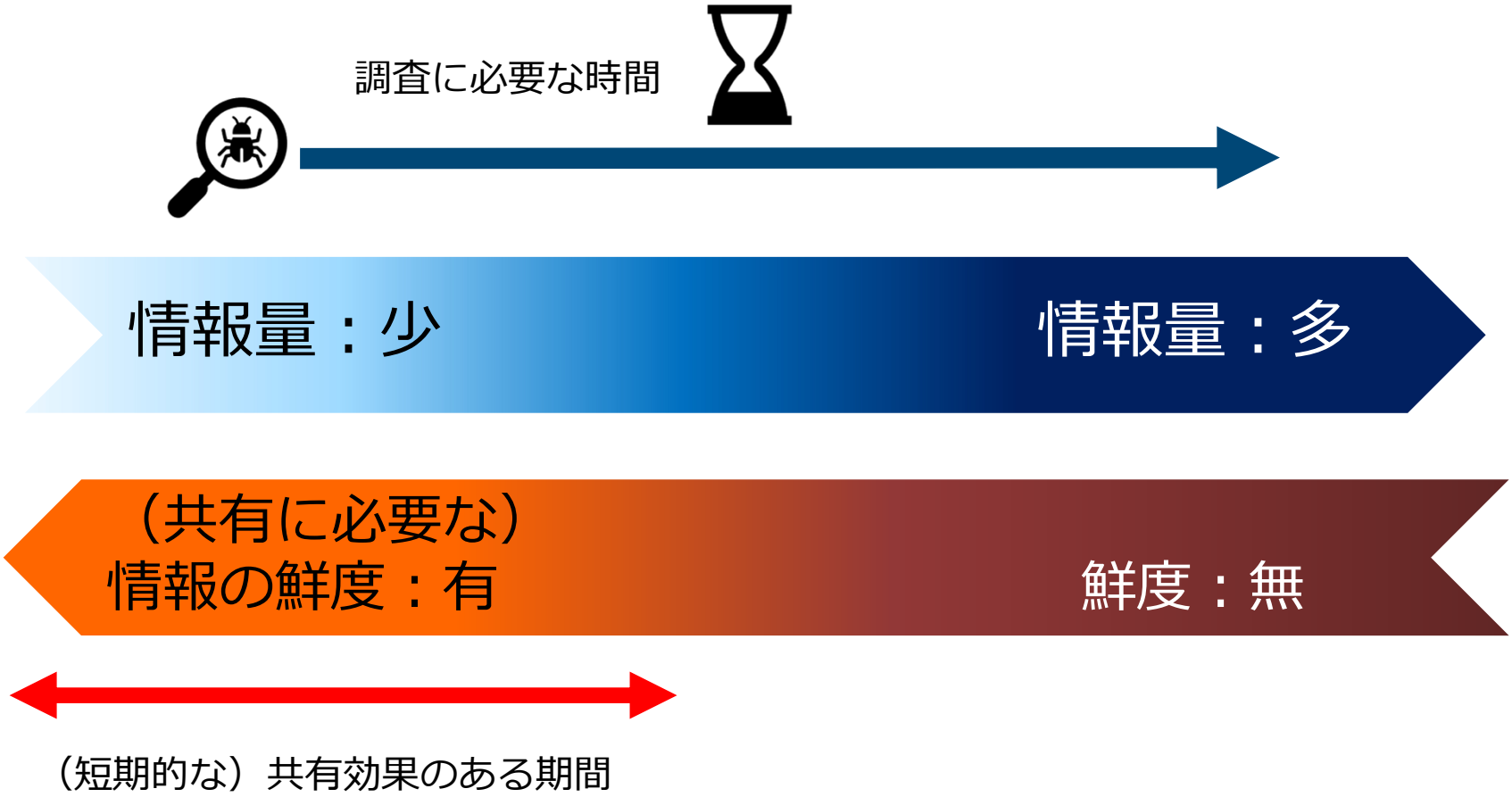
【ケース】公表までに一定の時間を要するケース

- 被害組織が「早期に公表したい」と考えていたとしても、調査進捗や関係者間調整により、公表時期は後ろ倒しになりがち



調査に必要な「時間」（再掲）

- 全容が判明するまである程度の時間がかかる
- 断片的な情報であっても、ある程度判明した段階で外部に共有することが効果的

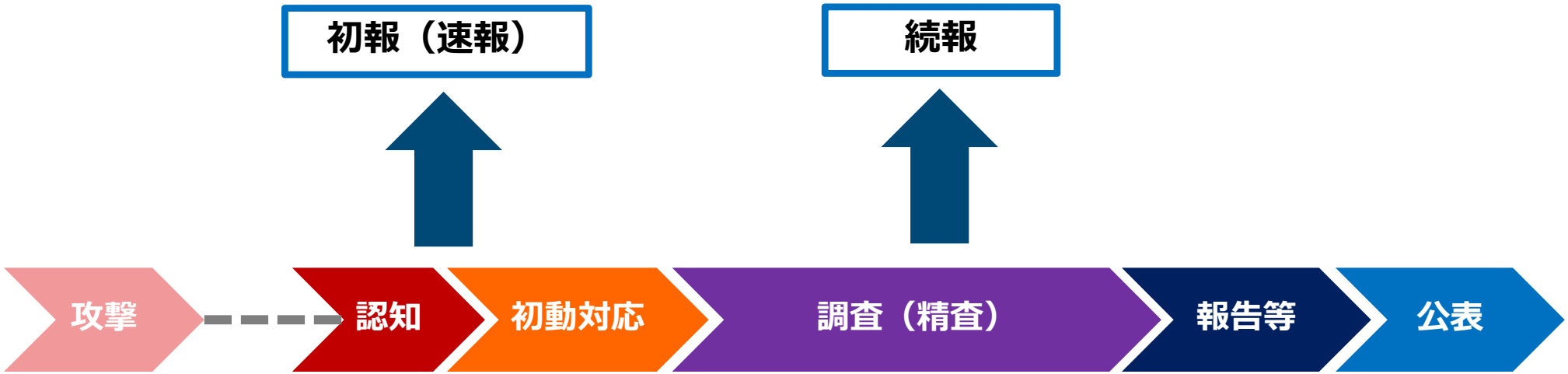


第一報と第n報（続報）について

- 公表は必ずしも単発ではなく、複数回にわたって行う場合もある。
- あるいは、調査がほとんど進んでいない段階でも速報的な第一報が必要になる場合がある

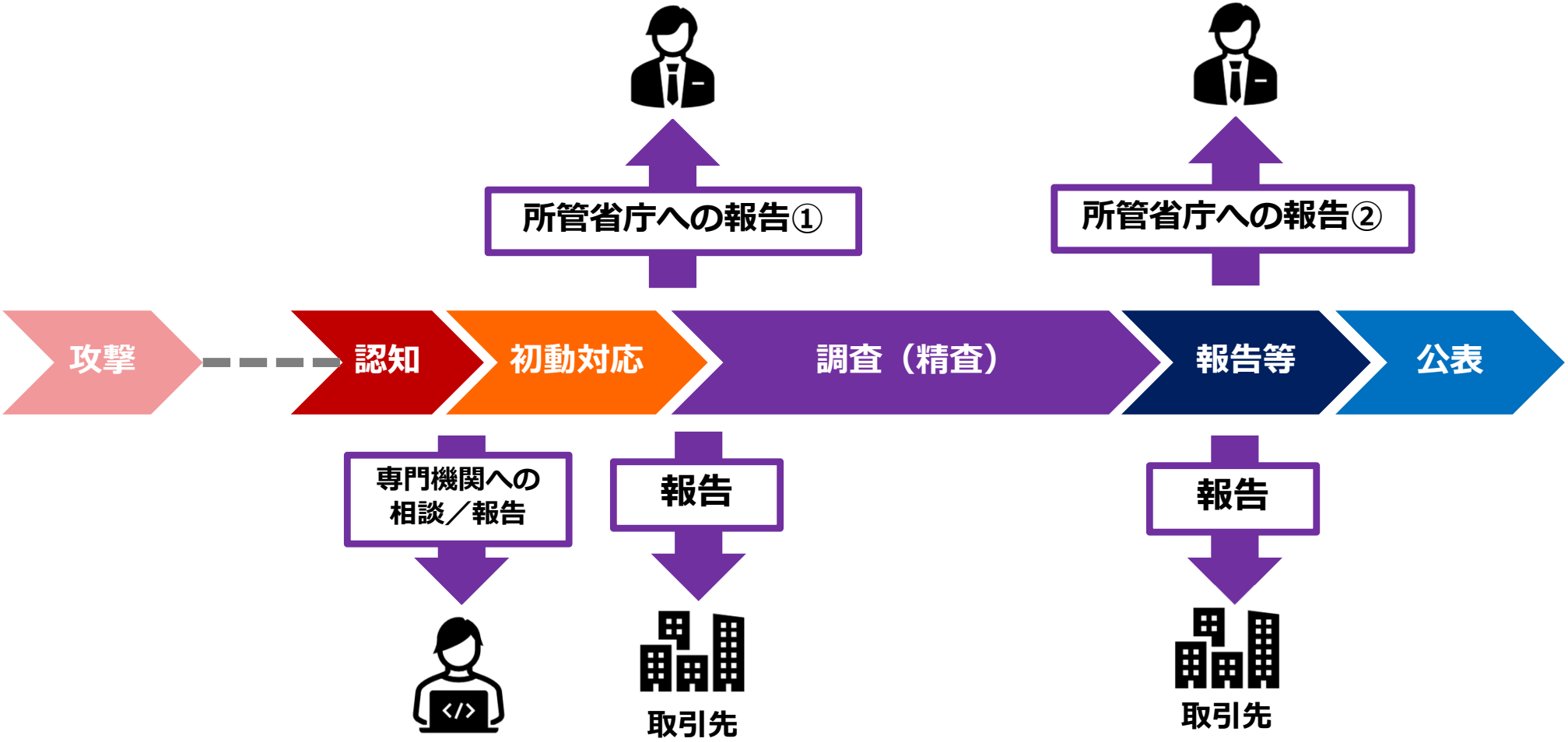
・対外サービス停止を伴う場合
・既に攻撃事実が公開情報となっている／なる蓋然性が高い場合
・二次被害防止のため
・法令等で求められている場合

・調査まで相当の期間がかかると見込まれる場合
・被害範囲調査とは別にサービスの再開を行う場合
・被害全容は解明されていないが、一部判明した被害に係る二次被害防止のため



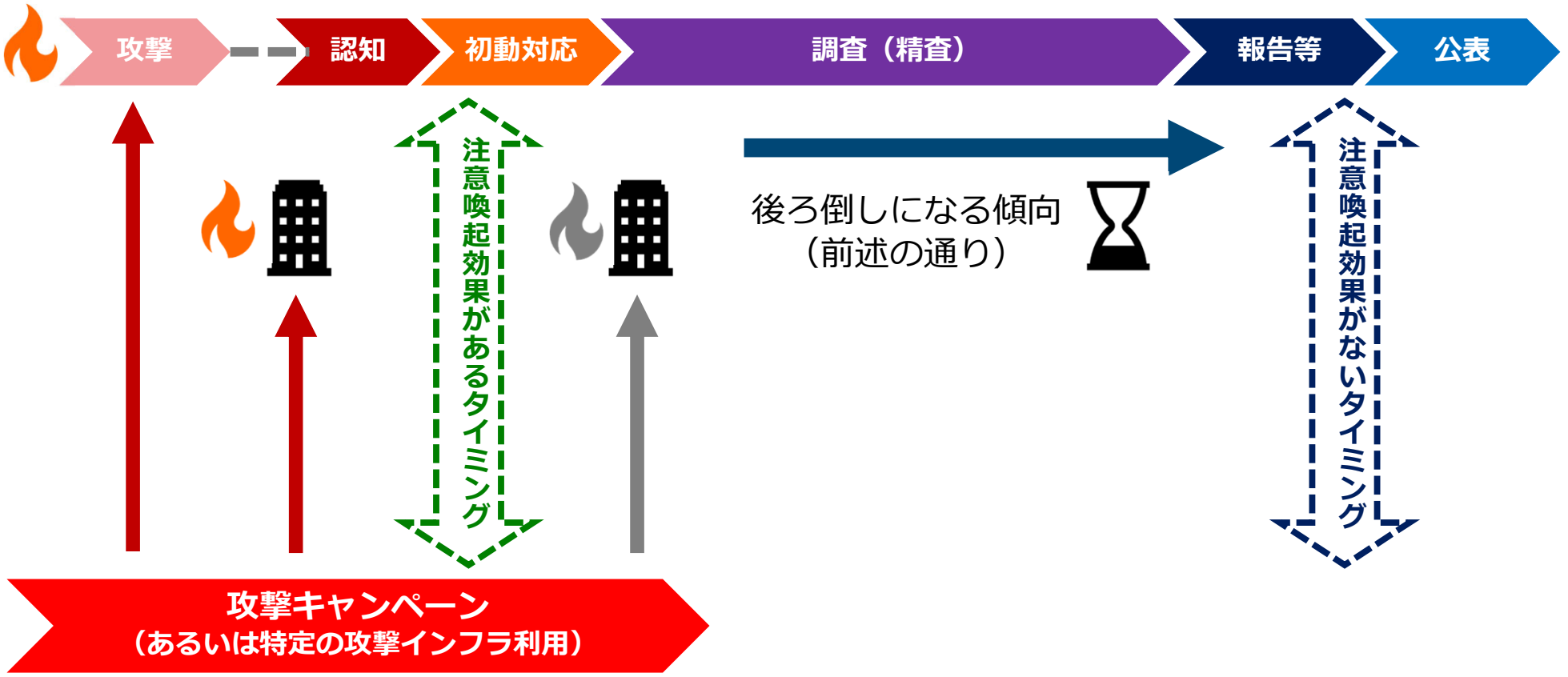
公表までに情報提供等を受けた第三者の対応

- 情報の共有先以外にも公表前に被害事実に関する情報が伝わる関係者が複数存在している
- 受け取った情報が各伝達先でどのように扱われるのか、（NDA契約を結ぶインシデント対応ベンダ等と比べて）必ずしも被害組織の意向でコントロールできない場合がある



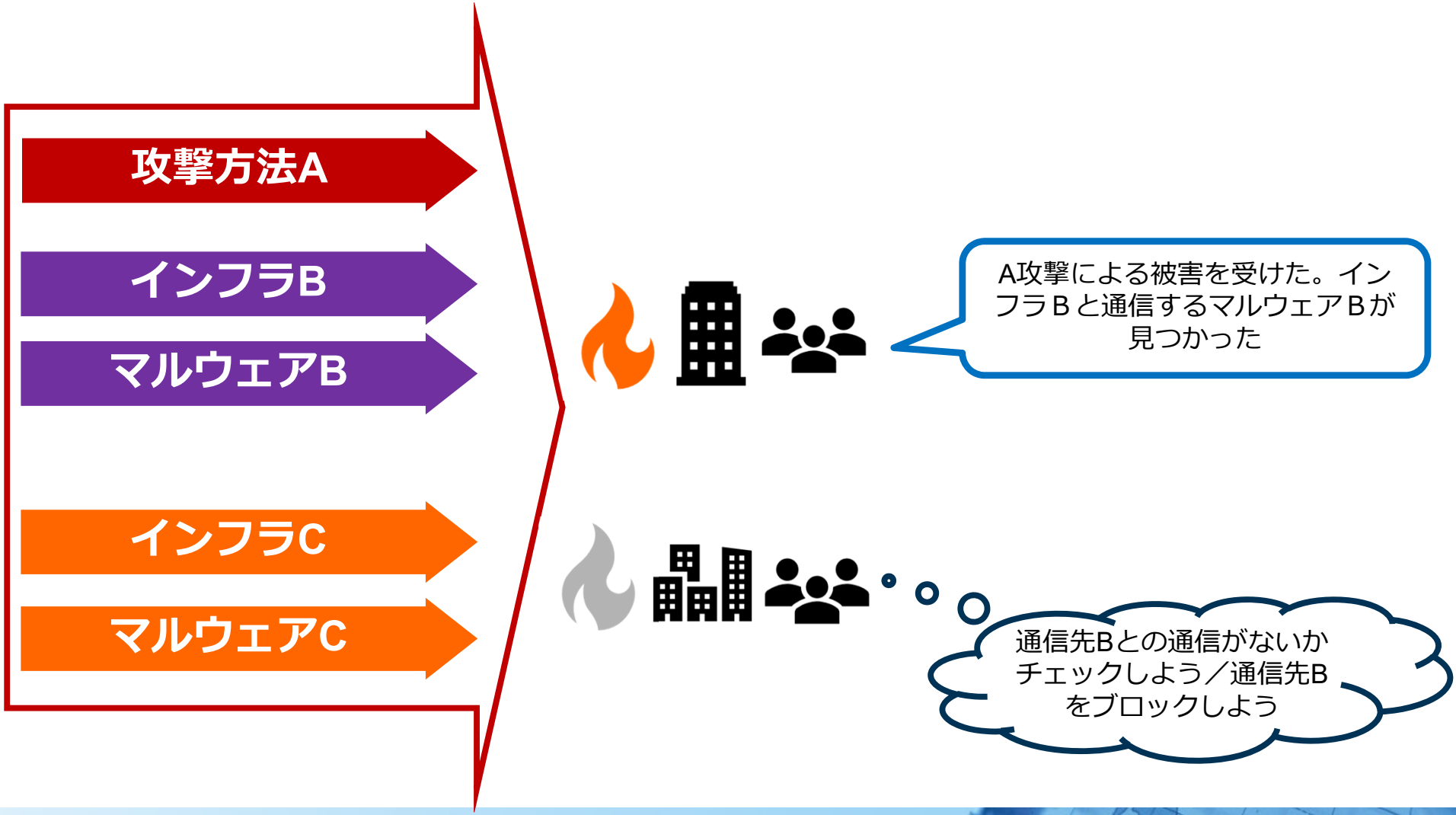
“注意喚起”目的の公表について

- （速報的な公表を除き）公表は基本的に後ろ倒しになる傾向があるため、“注意喚起”目的の公表は、その喚起による効果をそもそも見込むことができないのではないか



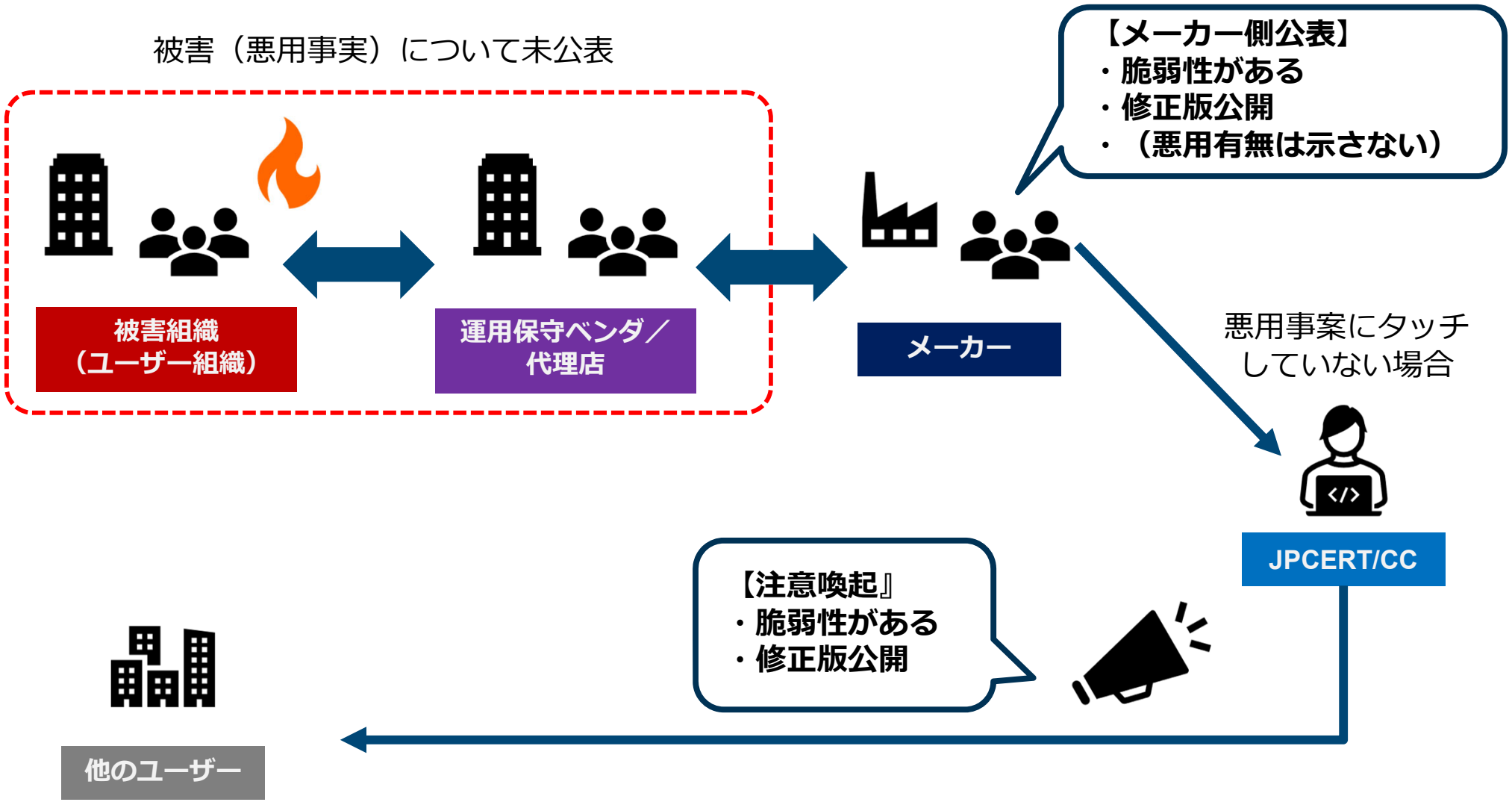
“注意喚起”目的の公表について

- 被害組織単独の判断による“注意喚起”目的の公表（情報発信）が技術的に妥当でない場合がある



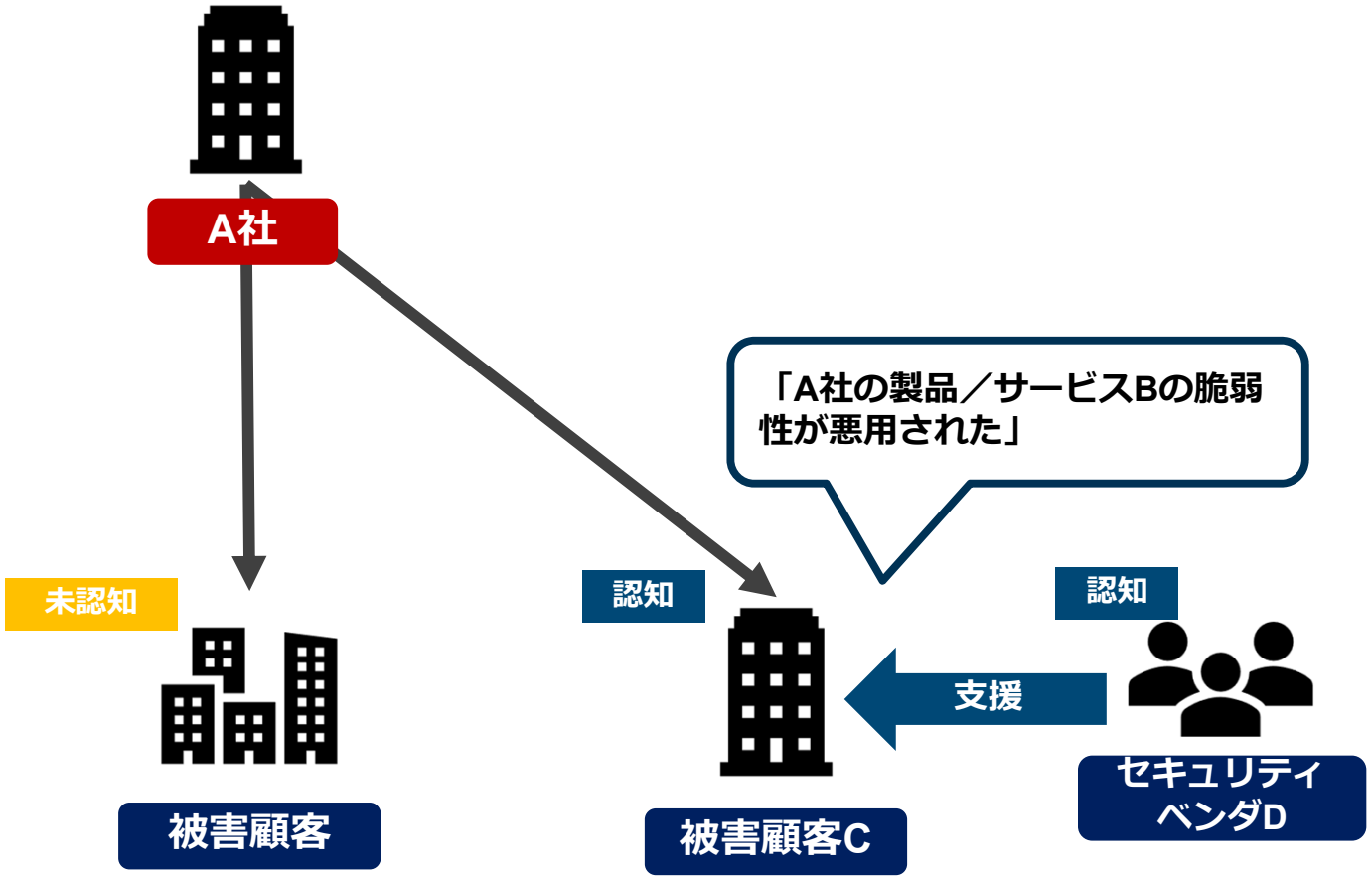
【ケース】未公表であることに「引きずられる」ケース

■ 既に脆弱性の悪用被害があるにも関わらず、注意喚起に「悪用情報」が含まれないケース



被害組織が脆弱性悪用有無について公表することの可否

- 既知の脆弱性が悪用された場合は被害組織の判断で公表可能



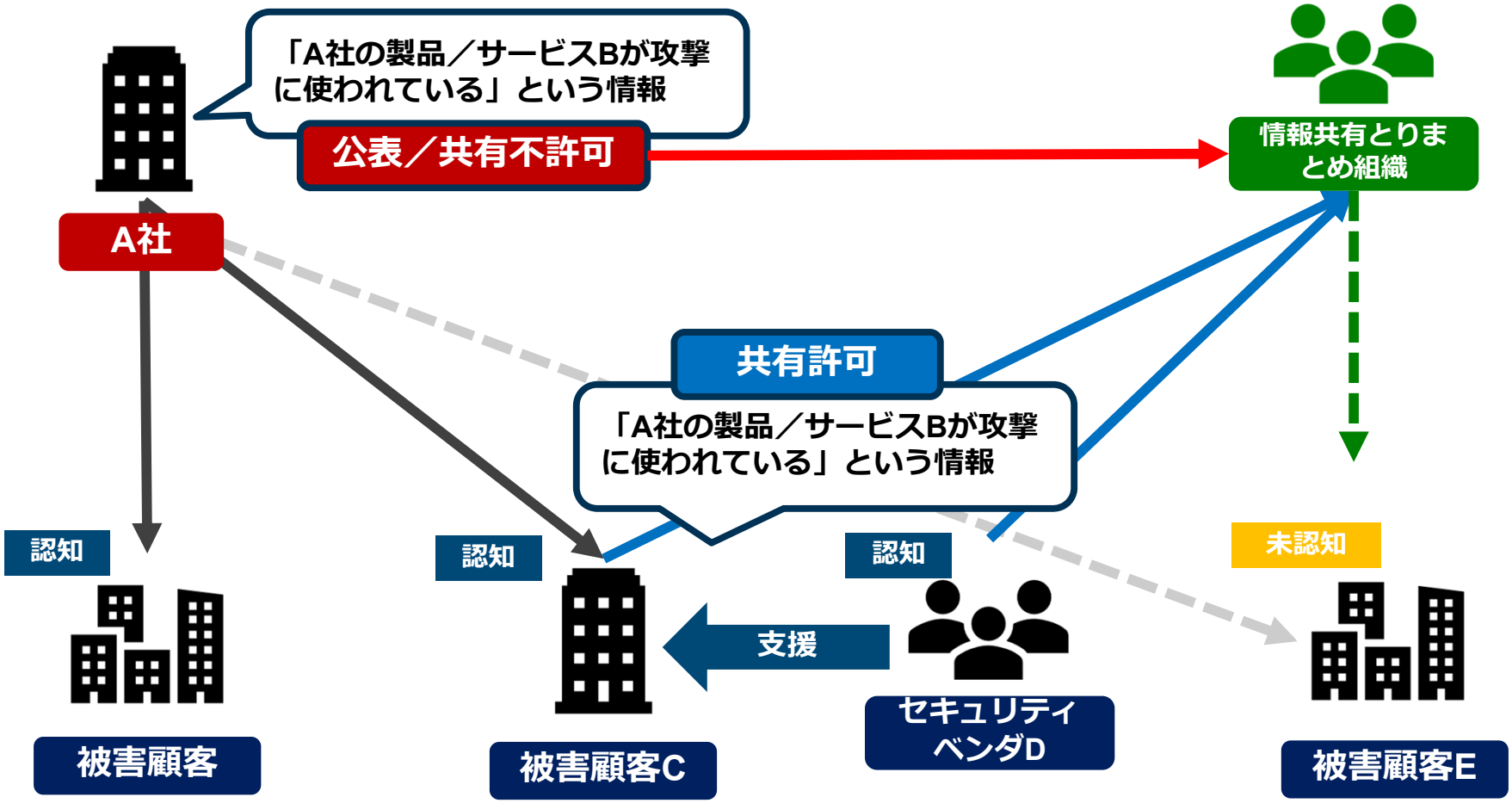
影響（可能性のある）範囲

未知の脆弱性の場合：
告示制度に基づく調整が望ましい

既知の脆弱性の場合：
※告示制度上特段の制約はない

脆弱性（悪用）情報のハンドリング問題

- 技術情報や攻撃手法について、既に第三者が認知している場合、「情報展開を許可する情報提供元」とは誰を指すのか



影響（可能のある）範囲

被害組織保護の観点から

未公表被害が公開情報となる場合

- 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）

被害を観測しているもの　←　被害（事実）を推測しているもの　→　被害の可能性の推測

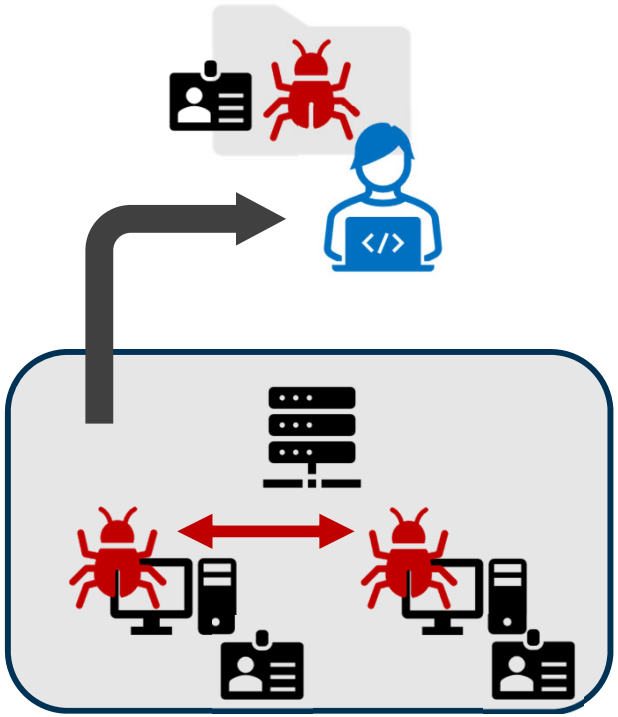
外形上攻撃被害が確認できる場合	漏えい情報の公開や犯行声明	（内部）関係者による情報発信	解析結果からの被害の推測	OSINTによるインフラ調査
例： Webサイト改ざん、 Webサーバ等への マルウェア設置	例： 第三者による漏えいデータの発見 リークサイト掲載	例： 従業員／顧客／取引先 関係者によるSNS発信	例： 公開解析サービス上の検体解析結果からの推測	例： SHODAN,Censys等による脆弱なホストの調査

検体解析情報から被害組織が推測されるケース

ケース①

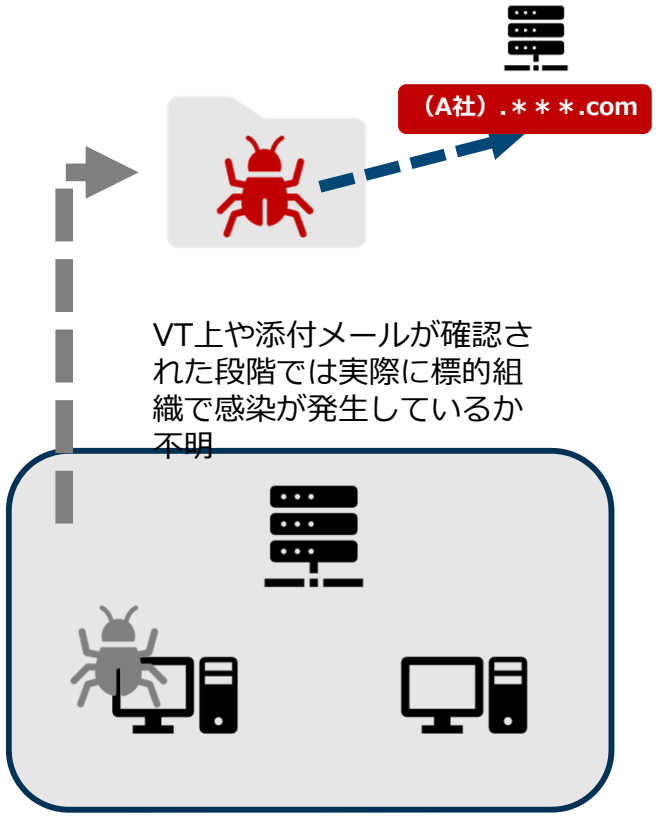
感染時に収集したクレデンシャル情報を含むケース
⇒ID＝メールアドレスのドメインから被害組織が推測されうる

【例】　Olympic Destroyer のVT上にあがった検体



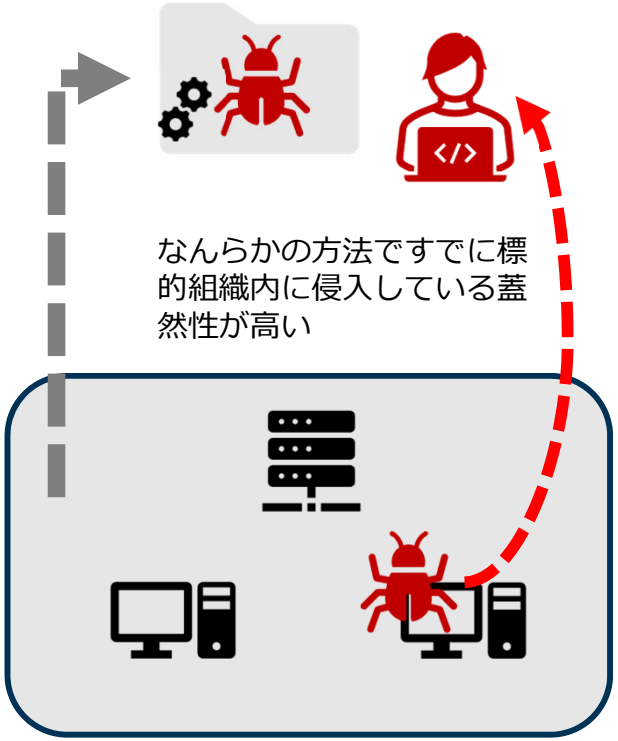
ケース②

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



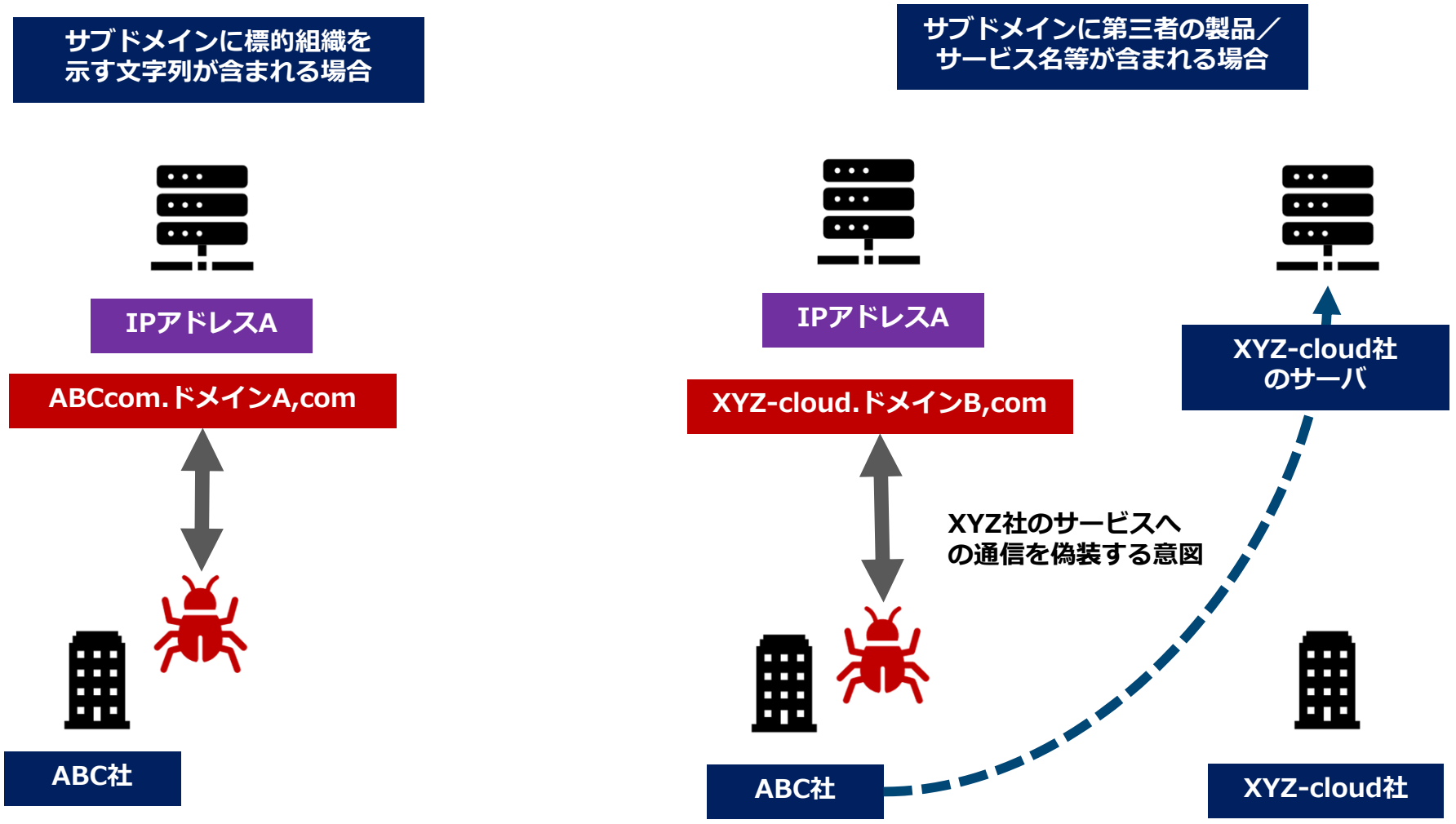
ケース③

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



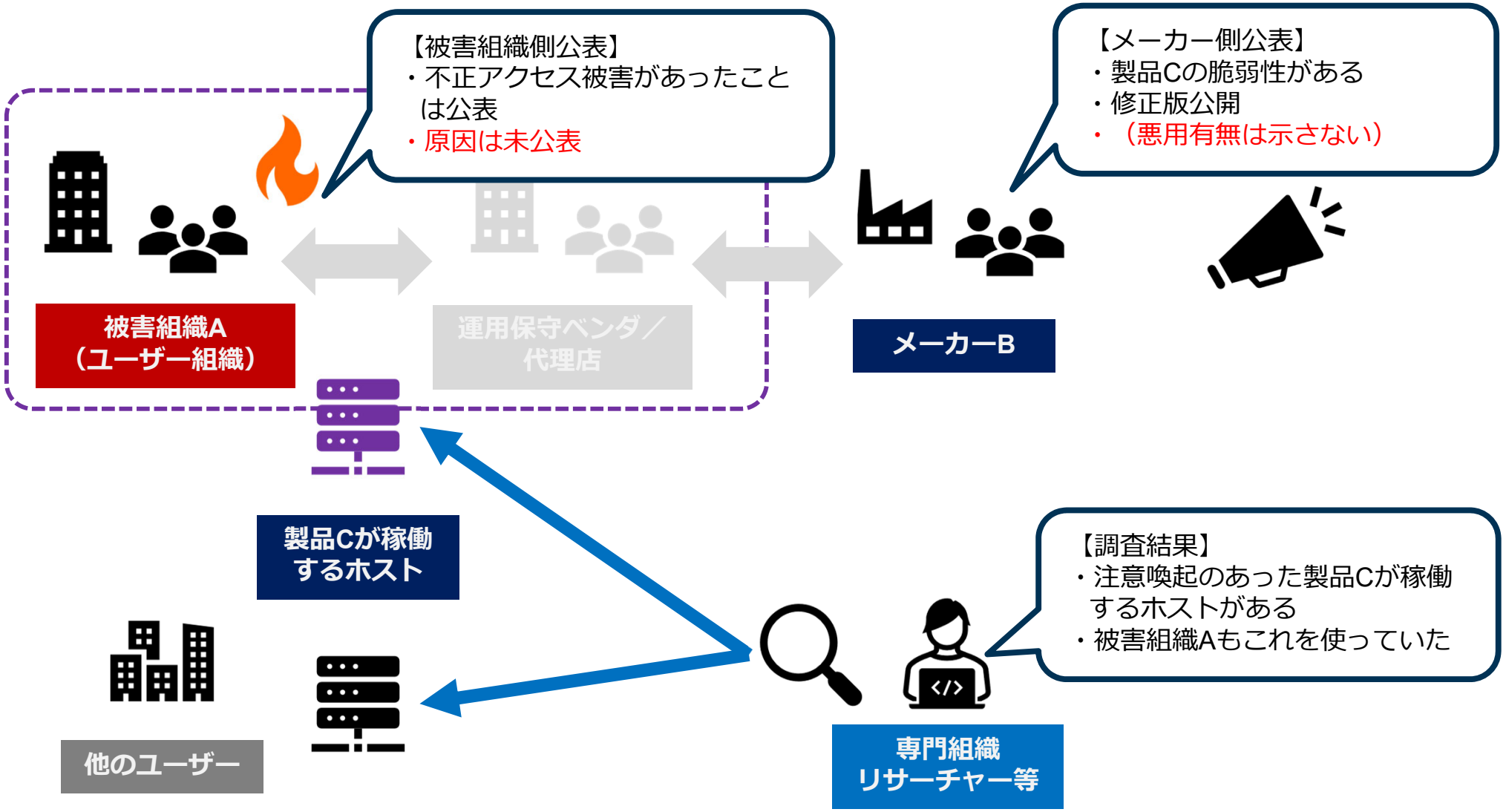
攻撃インフラの調査から被害組織が推測されるケース

- 被害組織等を推測させる情報を含む場合がある



公開情報から被害原因が推測されるケース

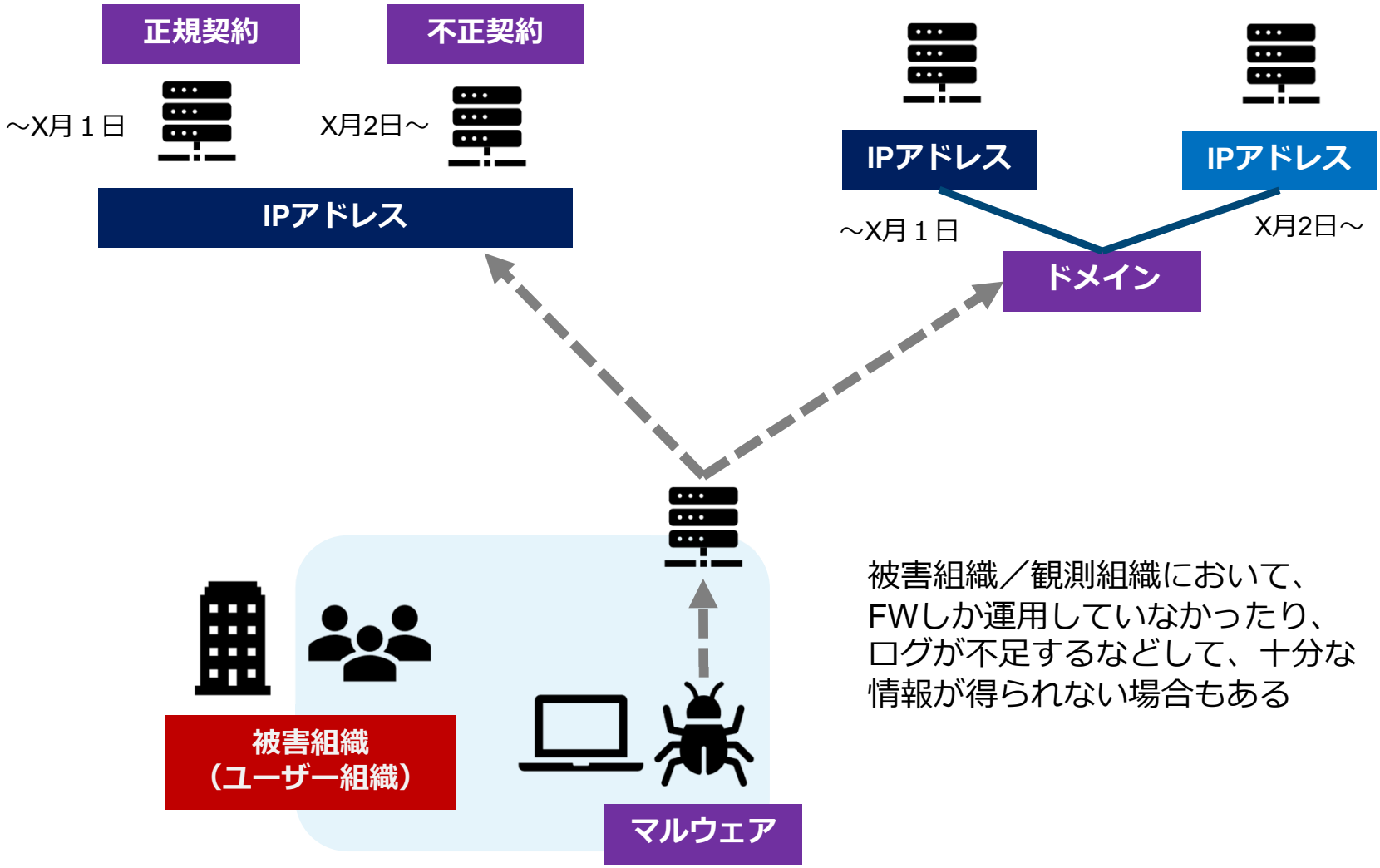
- 脆弱性の悪用について被害組織やメーカーから公表していなくても、OSINT調査等により「推測」はできるケース



各情報の性質／特性

情報の性質：通信先情報

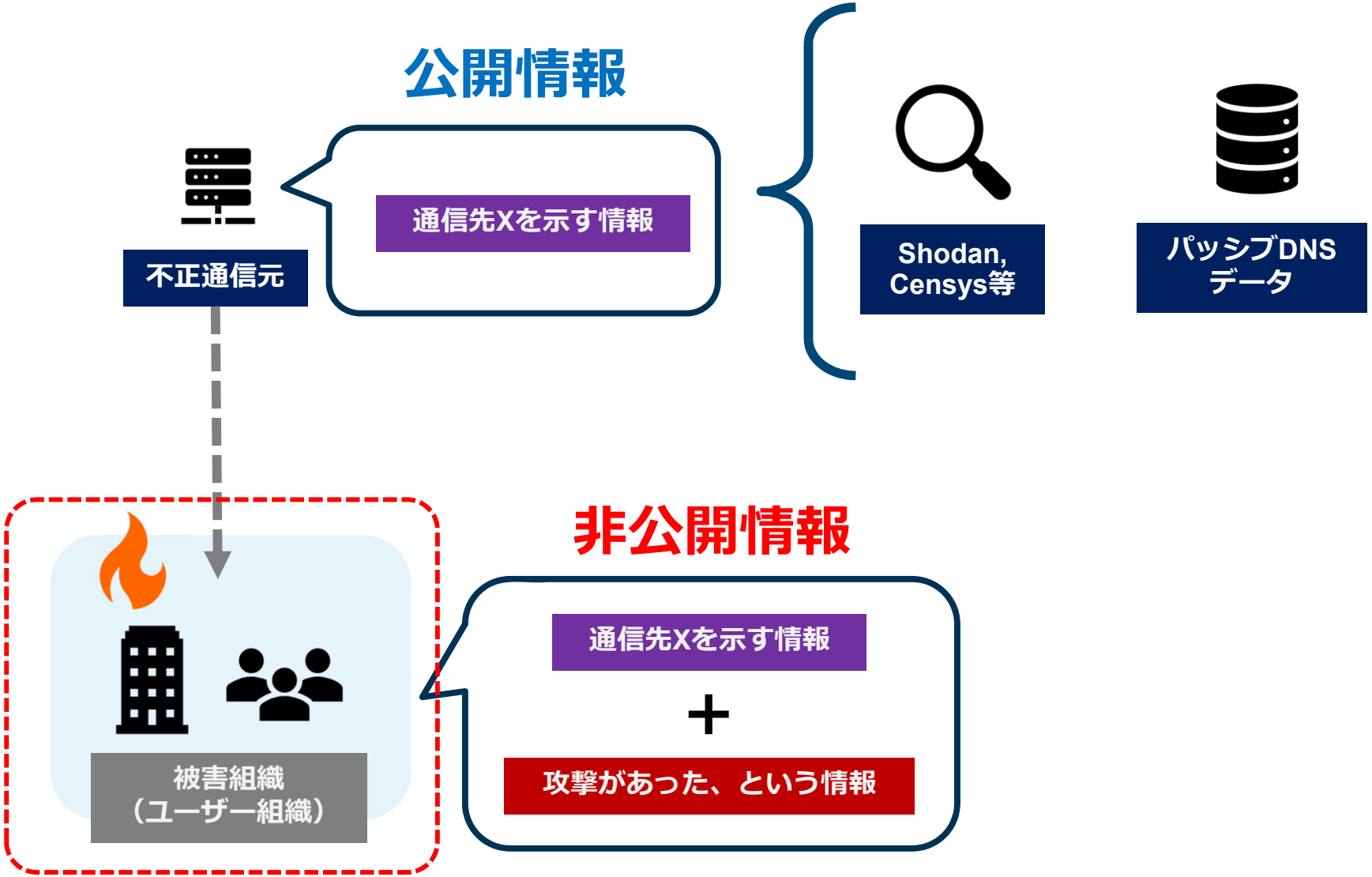
- 動的な情報であるため、（不正アクセスが行われた／確認された）「日時」とセットである必要がある



被害組織／観測組織において、FWしか運用していなかったり、ログが不足するなどして、十分な情報が得られない場合もある

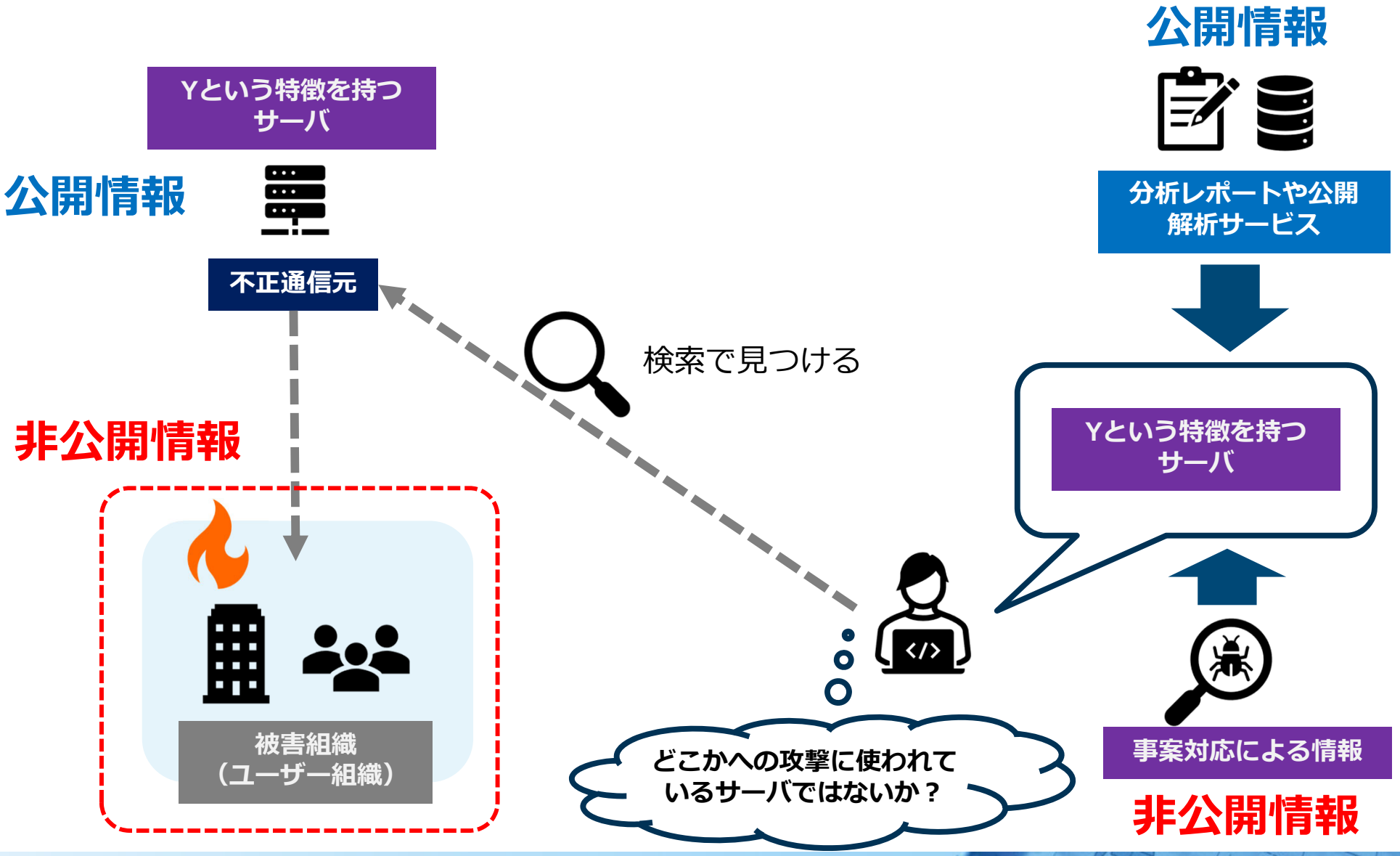
情報の性質：通信先情報

■ どこまでが「公開情報」なのか



情報の性質：通信先情報

■ 第三者が“たどり着く”場合がある



情報の性質：その他攻撃に関する情報

☑：共有効果が見込めるもの
△：効果が限定的と思われるもの

定性的な情報 ⟷ 定量的？な情報

各タイミングの共有活動における共有効果	攻撃者に関する情報	標的とする分野・地域に関する情報	TTP情報（右記のものを除く）	マルウェア／攻撃インフラに関する情報
短期的効果	※そもそも短期的な情報共有活動では絞り込めない可能性	※そもそも短期的な情報共有活動では絞り込めない可能性	△ 可能な限り右記情報とセットが望ましい	✓
中期的効果（攻撃キャンペーンの継続中）		✓	✓ 今後も継続／再活動しうる攻撃に対する対策情報として	△
長期的効果（攻撃キャンペーン終了後）	✓ 長期的な攻撃活動の捕捉・追跡	✓ 次の攻撃に備えた分野別の周知など		

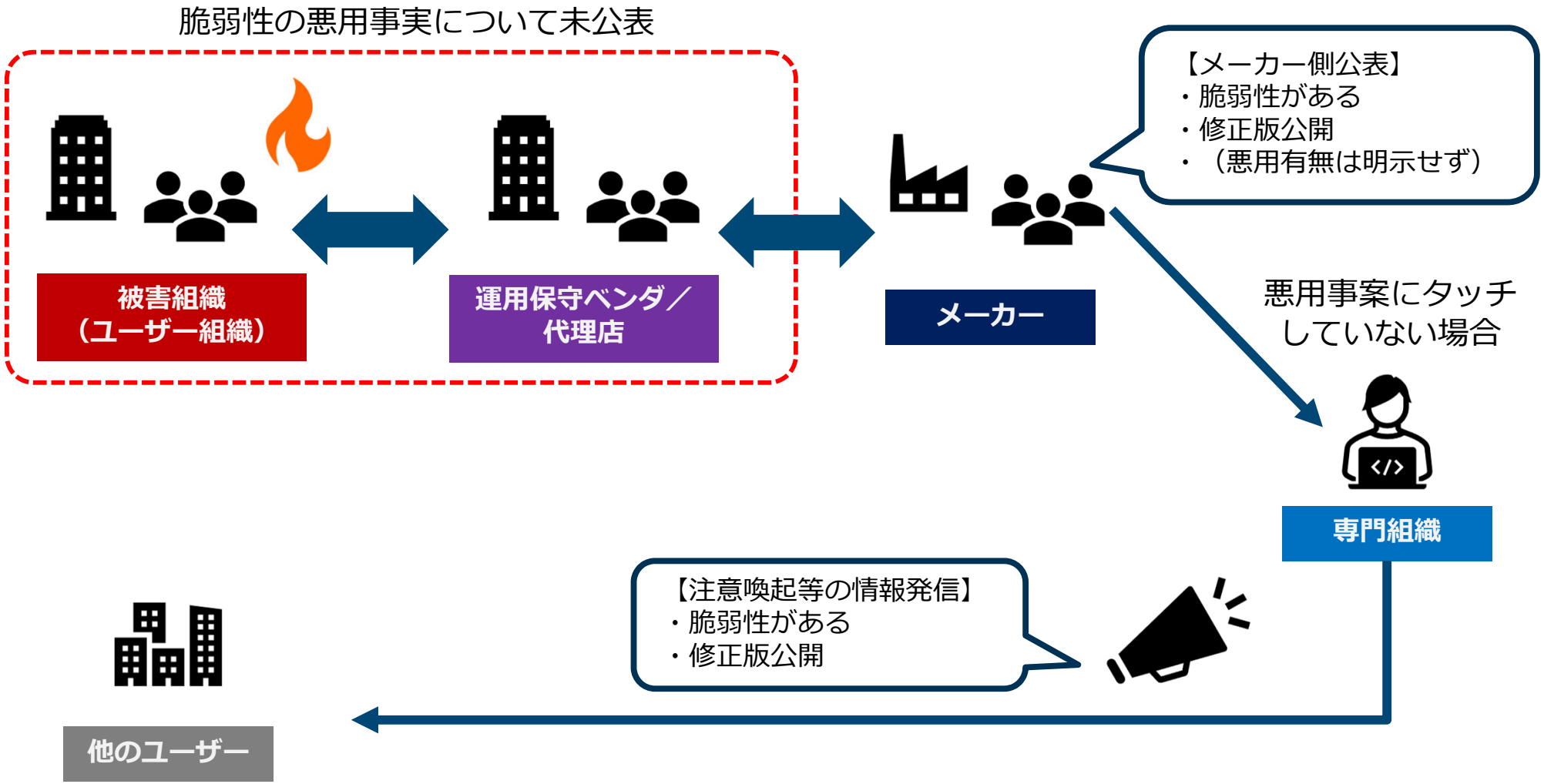
情報の性質：被害情報

Confidential ← → Secret

	被害事実（「被害があった」という情報）	個社名	被害内容（侵害期間や侵害範囲など）	漏えい情報
いずれ公表される可能性があるか	✓	✓	✓	
当該情報が第三者に関係するものである場合があるか			✓	✓
意図せず第三者が知り得る／推測する可能性があるか	✓ ※スライド61のケースを参照			

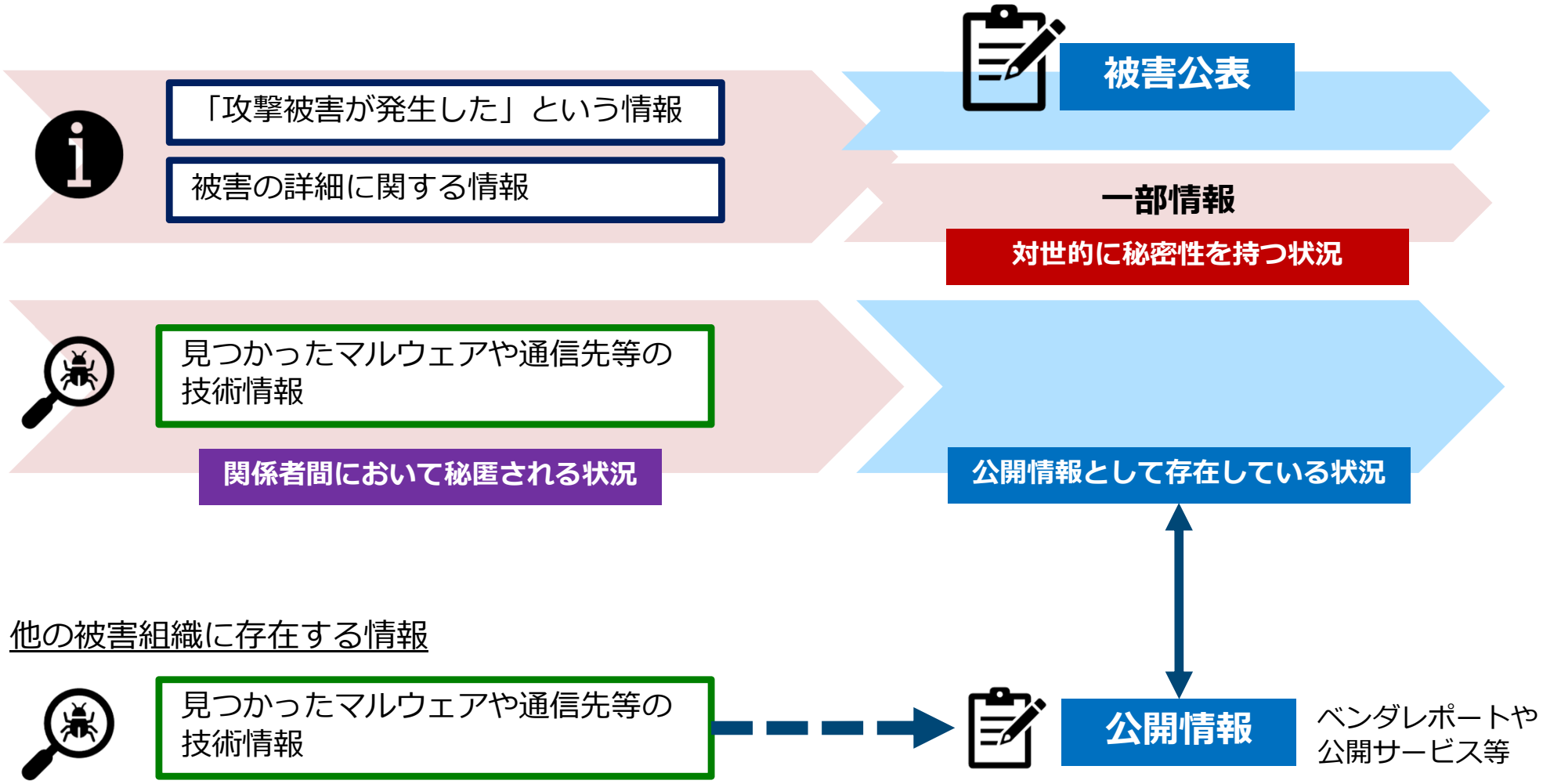
情報の性質：脆弱性関連情報（悪用有無情報）

- 脆弱性関連情報の取り扱いについては経済産業省告示やガイドラインで示されているところ、悪用有無を示す情報については明示的な記載がない
  ⇒参考：情報システム等の脆弱性情報の取り扱いに関する研究会2021年度報告書



ConfidentialとSecret

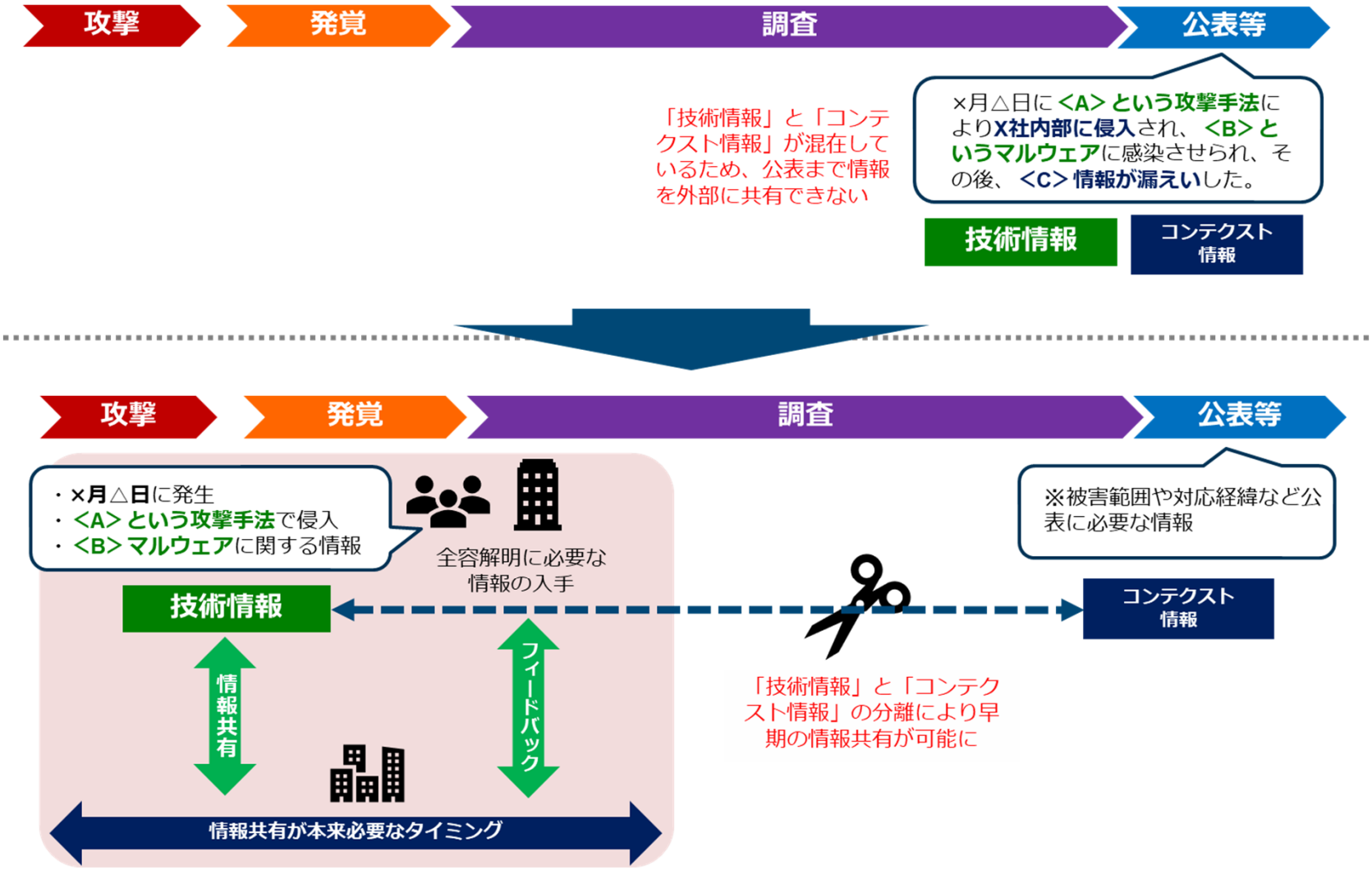
- （稀なケースを除き）基本的に同様の攻撃が同時多発的に発生している以上、時間の経過とともに、Confidential情報は（一部が）公開情報として存在するようになる



「共有」と「公表」について

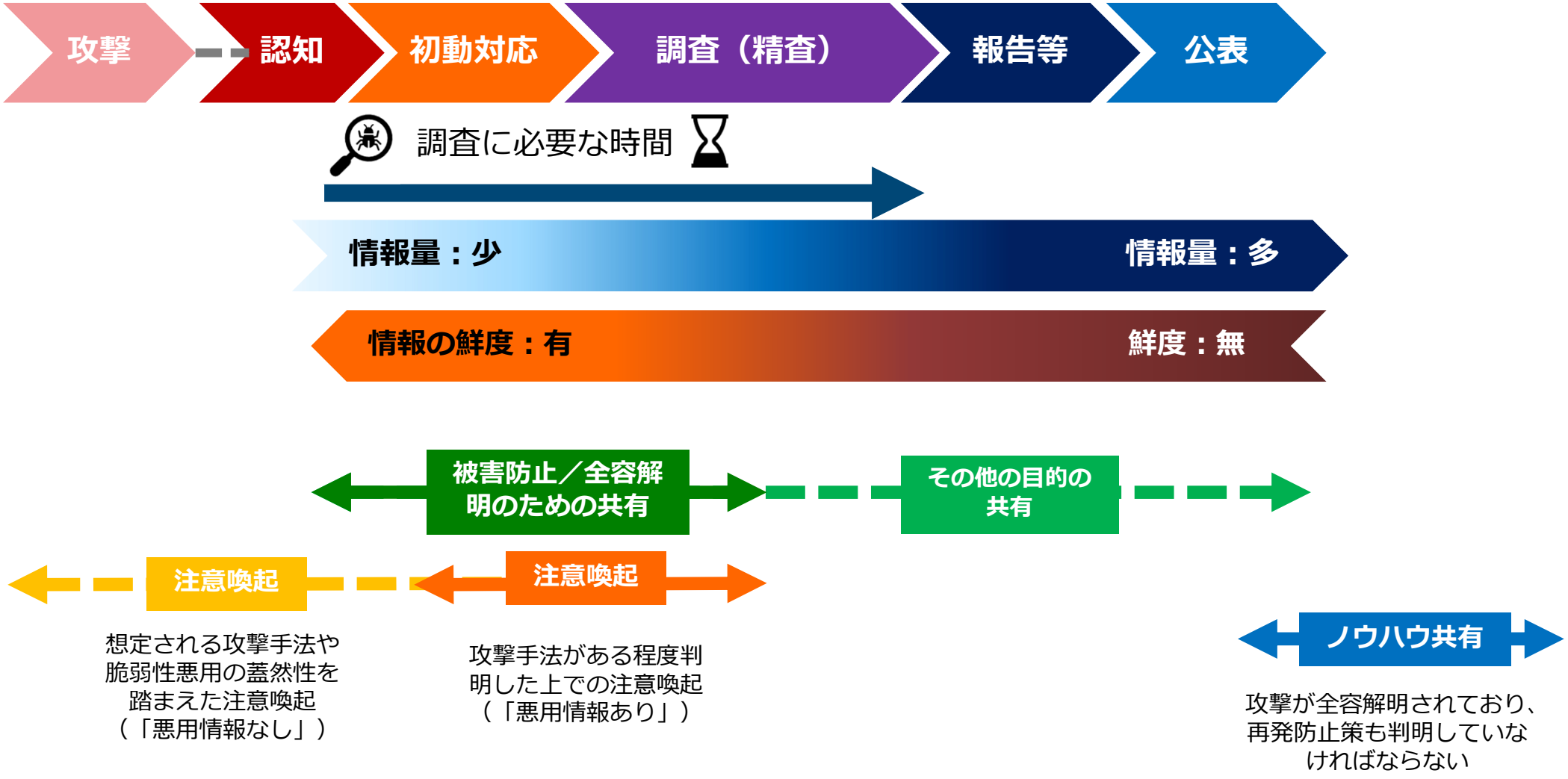
「共有」と「公表」の分離

- 2つの目的／方法／タイミングが混在すると、共有効果を得られなくなる



「情報共有」と「注意喚起」と「ノウハウ共有」の違い

- 効果的なタイミングと、それぞれ着手するために必要な情報が集まるまでの時間が存在する

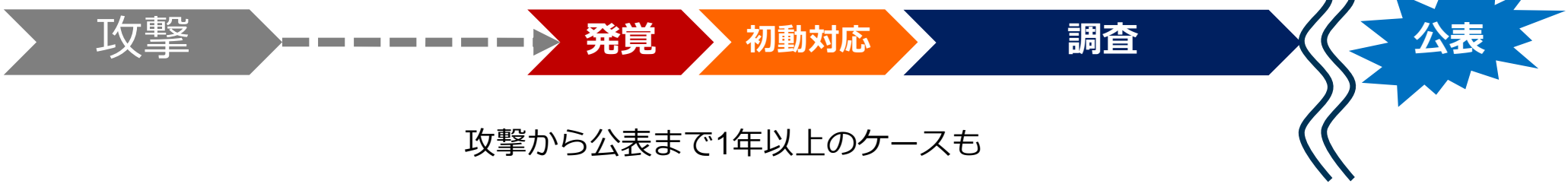


「共有」と「公表」を同時に行う必要があるケース

- ランサムウェア攻撃被害のように、対外サービス停止や予防措置的なシステム停止によるダウンタイム発生により、被害事実が直ちに公開情報となり、公表を迫られれるケース
- 情報漏洩系の他のインシデント対応とタイムラインが全く異なる

（情報窃取目的の）標的型攻撃等

“過去の攻撃”を時間をかけて対応できる



攻撃から公表まで1年以上のケースも

ランサムなどのリアルタイムインシデント

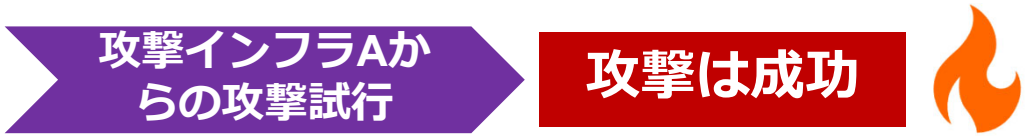
侵入からランサムウェア実行まで数日間～数時間という事案が多い

感染実行と同時にシステム障害や業務停止影響、リークサイト掲載等により被害が明るみに出る

被害は発生していない事案に関する情報の共有

- 必ずしも共有すべき情報は「攻撃被害に関する情報」だけではなく、攻撃の「試み」に関する情報の共有も有用である
- ただし、広く雑多な攻撃試行すべてを共有してしまうと、飽和状態になってしまう

設定等の運用状況により攻撃は失敗したケース



・
・
・

公開情報であっても共有効果のある情報

- 既にIoC情報等がレポート等で公開されている場合であっても、当該攻撃（試行）を観測した場合は情報共有することは有用である