資料2-4

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2回

第1回検討会での議論に関連する論点の振り返り

一般社団法人
JPCERTコーディネーションセンター

【再掲】本検討のスコープについて

サイバー攻撃被害に係る情報の共有・公表ガイダンス（イメージ）

■ サイバー攻撃被害を受けた組織がサイバーセキュリティ関係組織（例：NISC、警察、所管省庁、JPCERT、ISACなど）と被害に係る情報を共有することは、被害組織自身にとっても社会全体にとっても有益。一方、被害組織においては、どのような情報を、どのタイミングで、どのような主体と共有すべきかについて、必ずしも十分な理解が進んでいない。

■ このため、被害組織の担当部門（例：システム運用部門、法務・リスク管理部門等）を想定読者として、被害組織の立場にも配慮しつつ、サイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス文書を策定し、普及を図ることで、円滑かつ効果的な情報共有を促進していく。

● **どのような情報を？**（様々な種類・性質の情報が存在）

● **どのタイミングで？**（サイバー攻撃への対処の時系列を意識）

● **どのような主体と？**（様々なサイバーセキュリティ関係組織が存在）

● **想定読者**（被害組織）

CSIRT
システム運用部門

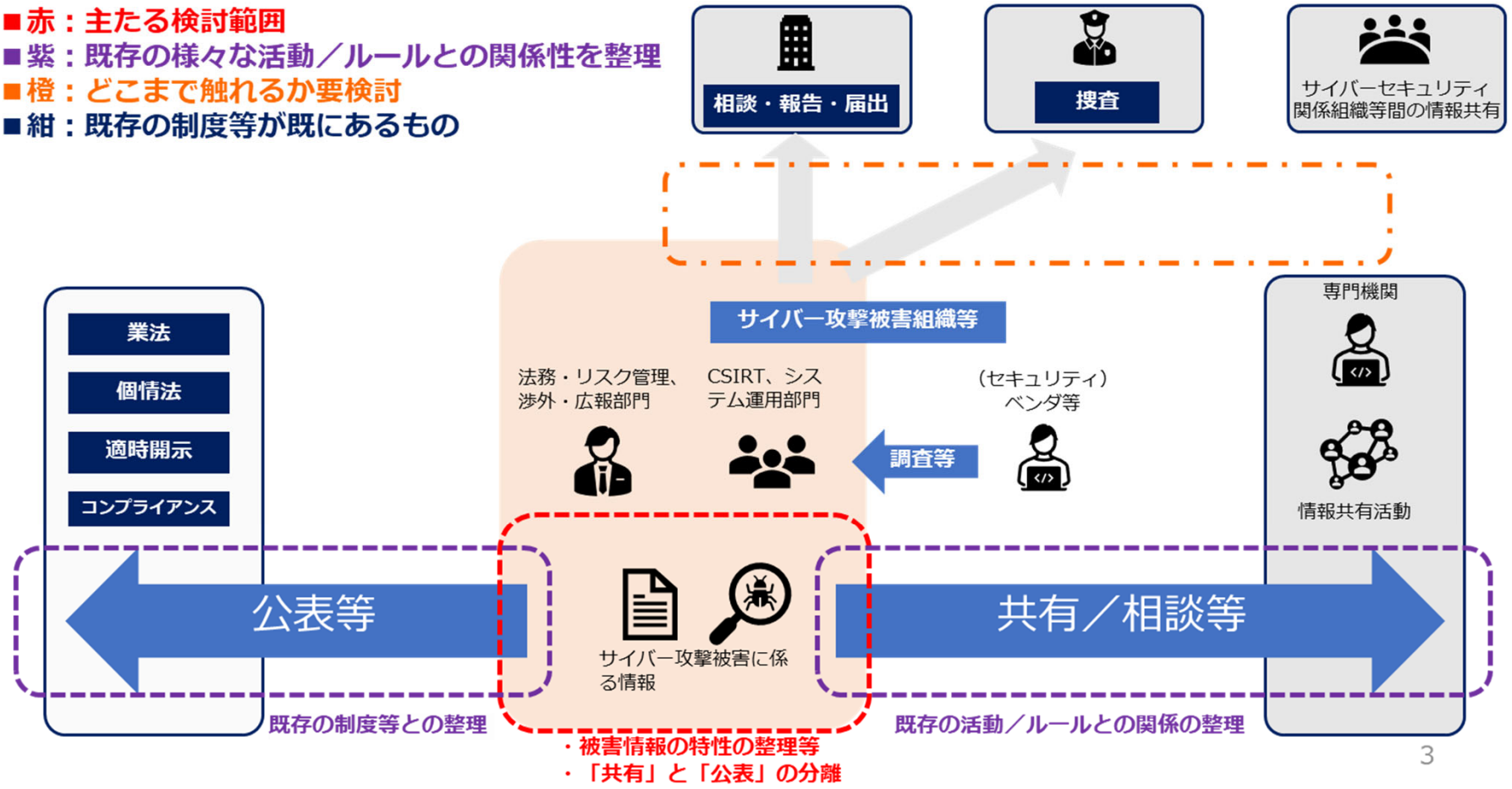
法務・リスク管理・
企画・渉外・広報部門

【再掲】本検討のスコープについて

成果物の対象範囲

- 共有・公表対象である被害情報の**各要素毎の特性**や**共有による効果**、**取り扱い上の注意点**を整理し、**「共有」と「公表」は分離して捉えることが出来るものであること**を解説するもの
- 被害組織が、情報の共有や公表を検討するにあたって、わかりやすい形にするため、既存の枠組みも含めた包括的なガイダンスとすることが望ましい。ただし、例えば、 ア）業法や個情報等の法令・告示に基づく公的機関への報告・届出、イ）警察等への届出・相談など、既存の枠組みが確立されているものについて新たな考えを整理するのではなく、①外部専門機関や情報共有の枠組みへの任意の情報共有、②一般への事実の公表、③ステークホルダーへの連絡などについて中心に検討を行う。

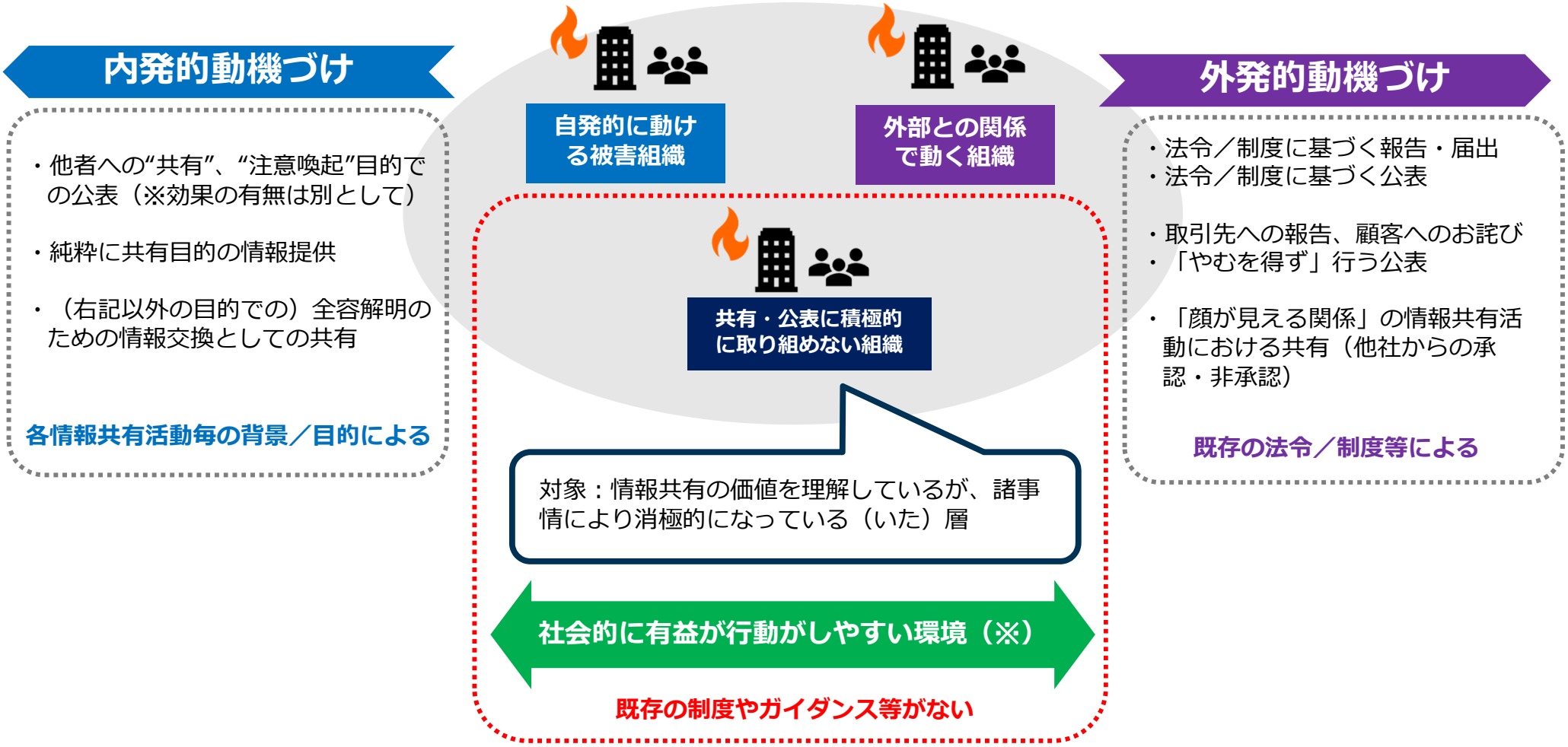
■赤：主たる検討範囲
■紫：既存の様々な活動／ルールとの関係性を整理
■橙：どこまで触れるか要検討
■紺：既存の制度等が既にあるもの



3

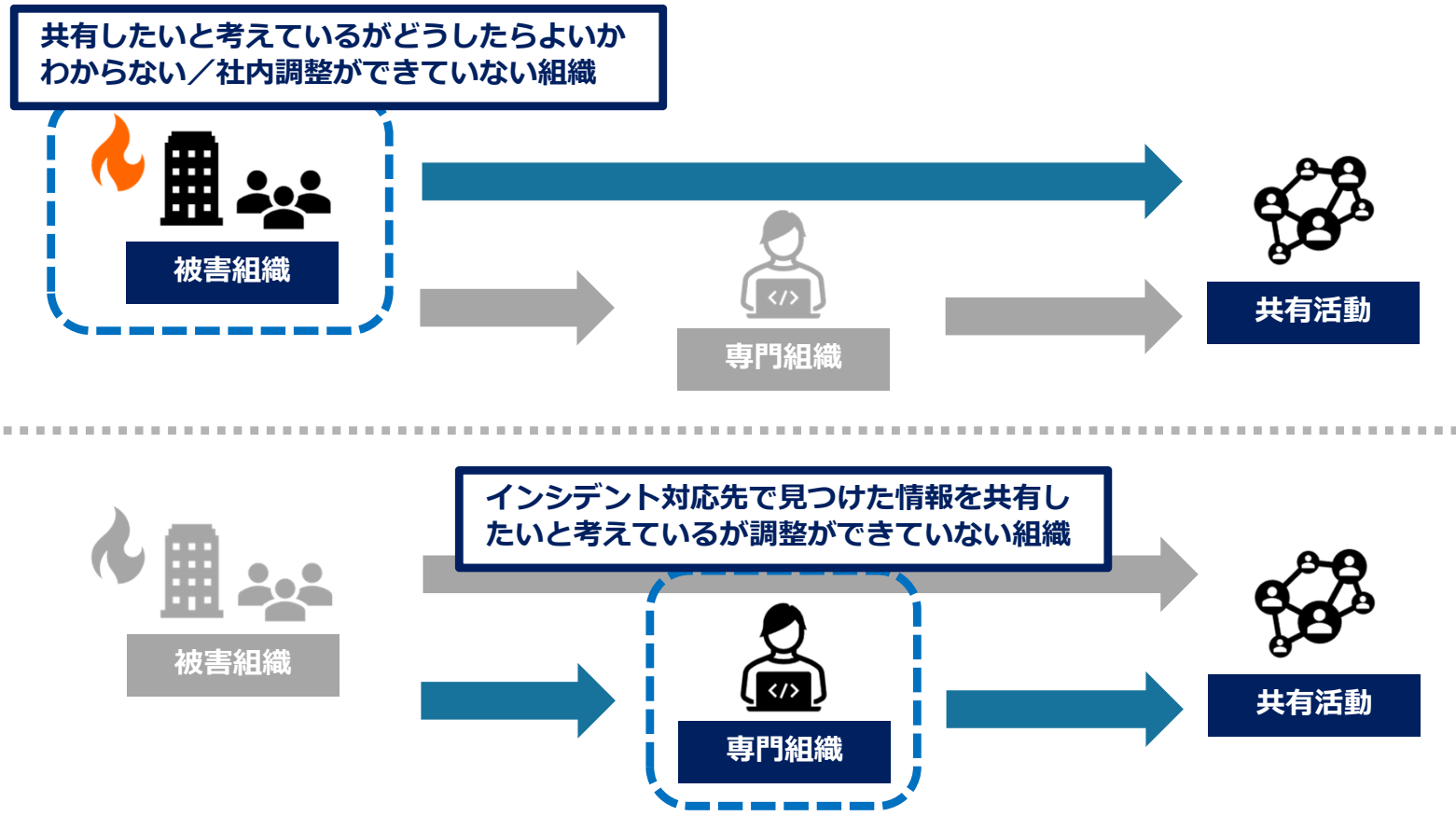
本検討のスコープについて：ガイダンスの主な対象

- 各組織の内発的動機（モチベーション）や、いわゆる一般的なインセンティブ（≒外発的動機付け）だけでは限界があることが問題の根底にあり、「共有／公表しやすい」環境づくりが必要ではないか

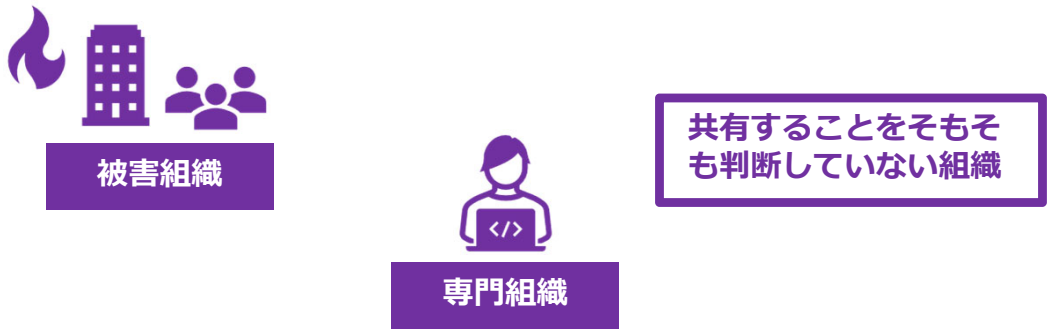


（※）参考：飯田高「法と社会科学をつなぐ」（2016年）78頁

本検討のスコープについて：「共有」の観点から



「どのような情報を、どのタイミングで、どのような主体と共有することが適当なのか等を検討するための実務上の参考」のニーズがある対象



共有を行うための「仕掛け」が必要な対象
⇒既存の仕組み、制度では不足しているものの検討が必要

【参考】共有活動の現状について

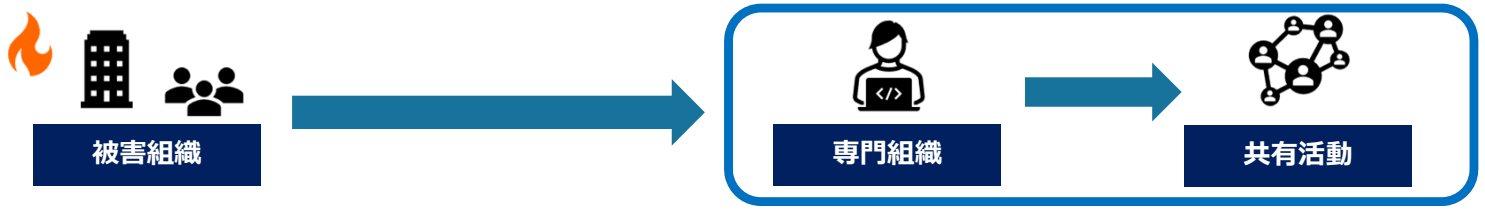
被害組織自身が判断／準備し、自ら共有活動に展開するもの

一部のISAC等

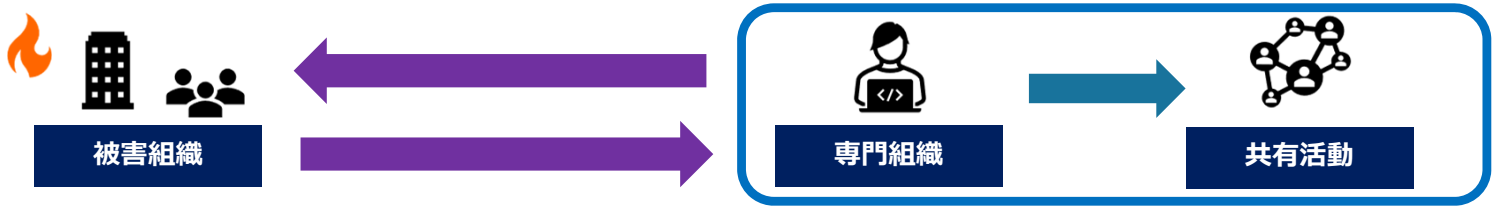
被害組織自身が判断し、ハブ組織が準備・展開するもの

・CISTA（早期警戒情報）
・J-CSIP

被害組織自身が判断し専門組織から間接的に共有されるもの



専門組織の案内／説得により専門組織経由で共有されるもの



感覚的にはこれらの割合が多いのではないか

本検討のスコープについて：「公表」の観点から

法令や制度上、公表が必要な対象事案

→ 既存の法令／制度の案内

（上記以外で）二次被害防止のために公表が望ましい事案

→ 

→ どのようなケースの場合、公表が望ましいのか示す

公表によって広く知られることに社会的意義のある事案

→ 

→ どのようなケースの場合、公表が望ましいのか示す

→ 

→ 専門組織のレポート公表等による“間接的”な公表（※）の効果を示す

※被害組織名は匿名のものを想定

その他

→ 上記以外で公表の必要性や効果を示すケースがあるがどうか要検討

第1回検討会での主なご意見

■ **「目的」の観点**
- 攻撃の種類によって、共有の目的／価値はわかるので、目的別（方法別）の整理が必要
- 「何のための公表を行うのか」の整理
- 公表することで個別問い合わせを交通整理でき、“避雷針”の役割がある
- 被害組織と専門家間、または専門家同士だけの共有だけでなく、公表や取材による社会一般の理解、問題意識が惹起される社会的意義についても言及すべき

■ **「時間」の観点**
- せっかく情報提供を受けても1年以上前のものなど“賞味期限”が過ぎている場合がある
- 公表タイミングの問題。共有と公表の間が間延びする問題

■ **「理解促進」の観点**
- 経営層や広報等に「どんな情報なら外部に共有しても問題ないか」「共有によるどのような効果があるのか」示せるとよい
- 情報提供する側の（共有活動に対する）理解を高めたい
- 「公表しないことのリスク」を示すことも重要
- 指針などにより、被害組織と専門組織側が安定してやりとりでき、共有活動が継続して行えることが重要
- 共有／公表に関わる各プレイヤーの様々に異なる立場／役割を示すべき

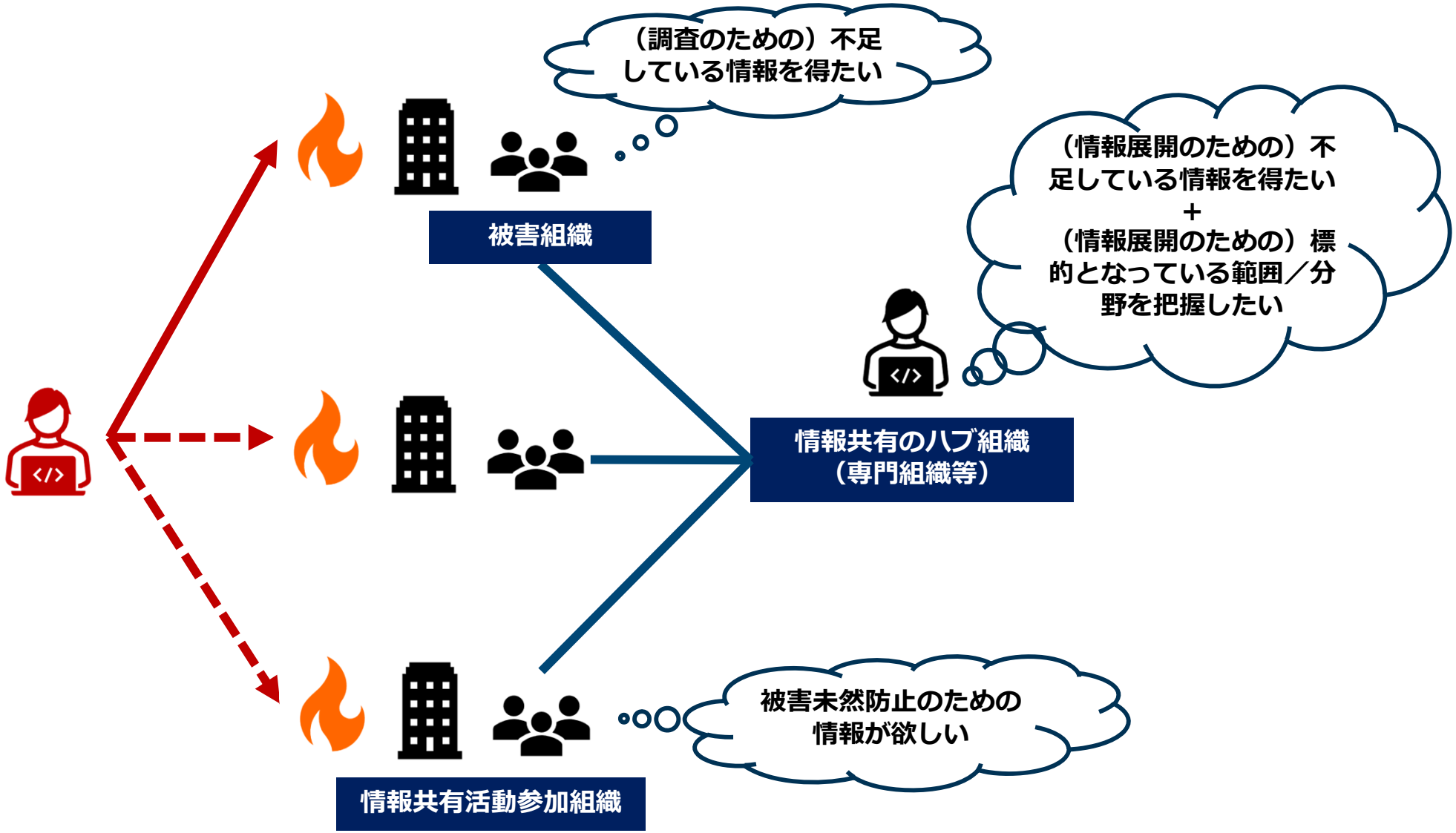
■ **「信頼性」の観点**
- 機微な情報が共有（提供）情報に含まれる場合のクリアランス
- 受け取った情報を適切に活用できるかなど共有活動参加者の資質も重要なポイント

■ **「契約との関係」の観点**
- セキュリティベンダの活動上の制約を緩和するような契約上の措置やそのメリットの解説の必要性

■ **「外部組織との連携」の観点**
- 被害組織の判断のみで100点の共有・公表判断ができるものではない
- 専門機関への相談スキームや様々な届出窓口の周知／案内が必要
- 警察への相談・通報の促進を示すべき

【再掲】情報共有の目的

■ 各立場によって共有の目的は（多少）異なる



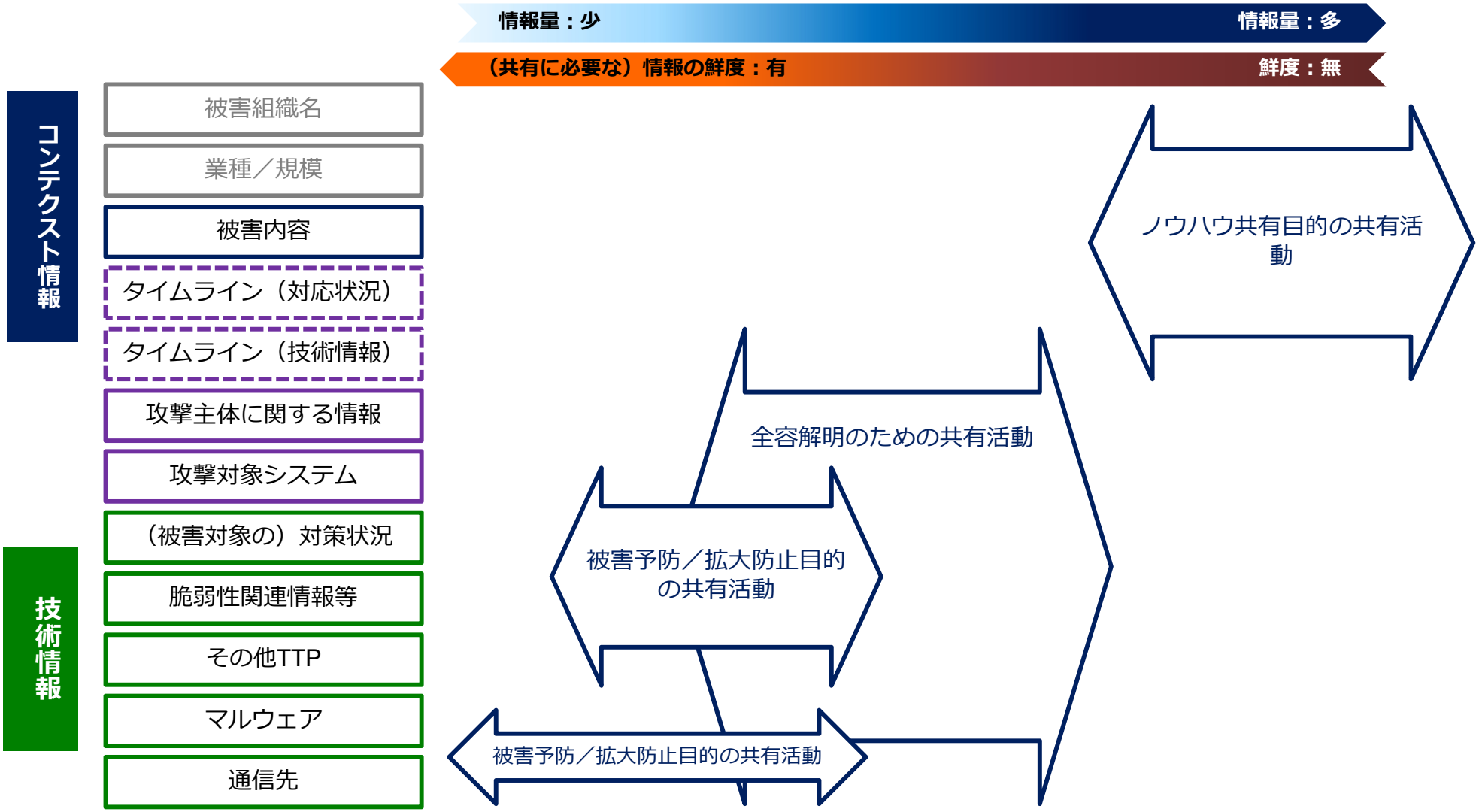
【再掲】「共有」の異なるタイミング／目的

■ 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

【再掲】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



【再掲】どういう情報の共有が共有効果があるのか

第1回目資料2-2
スライド32

- 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

【再掲】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

公表の目的

義務的

「やらざるを得ない」

積極的理由

- 法令／制度上義務または求められているもの

（例）

– 各業法
– 個人情報保護法
– 適時開示

- （上記以外で）二次被害防止のために公表を行うもの

– 顧客情報漏えいの場合（※個情報）
– 対外向けサービス停止に係るアナウンス

- 被害事実／推測される情報が外部に知られた場合／知られる可能性が高い場合に行うもの

– 従業員や利用者のSNS上の情報発信
– 未公表情報に関する報道
– （主に海外の）セキュリティベンダのレポート公表や報道等から未公表情報が明らかになるもの
– ステークホルダーへの個別連絡を進める中で第三者に情報が伝わる可能性がある場合

- その他組織の判断として行われるもの

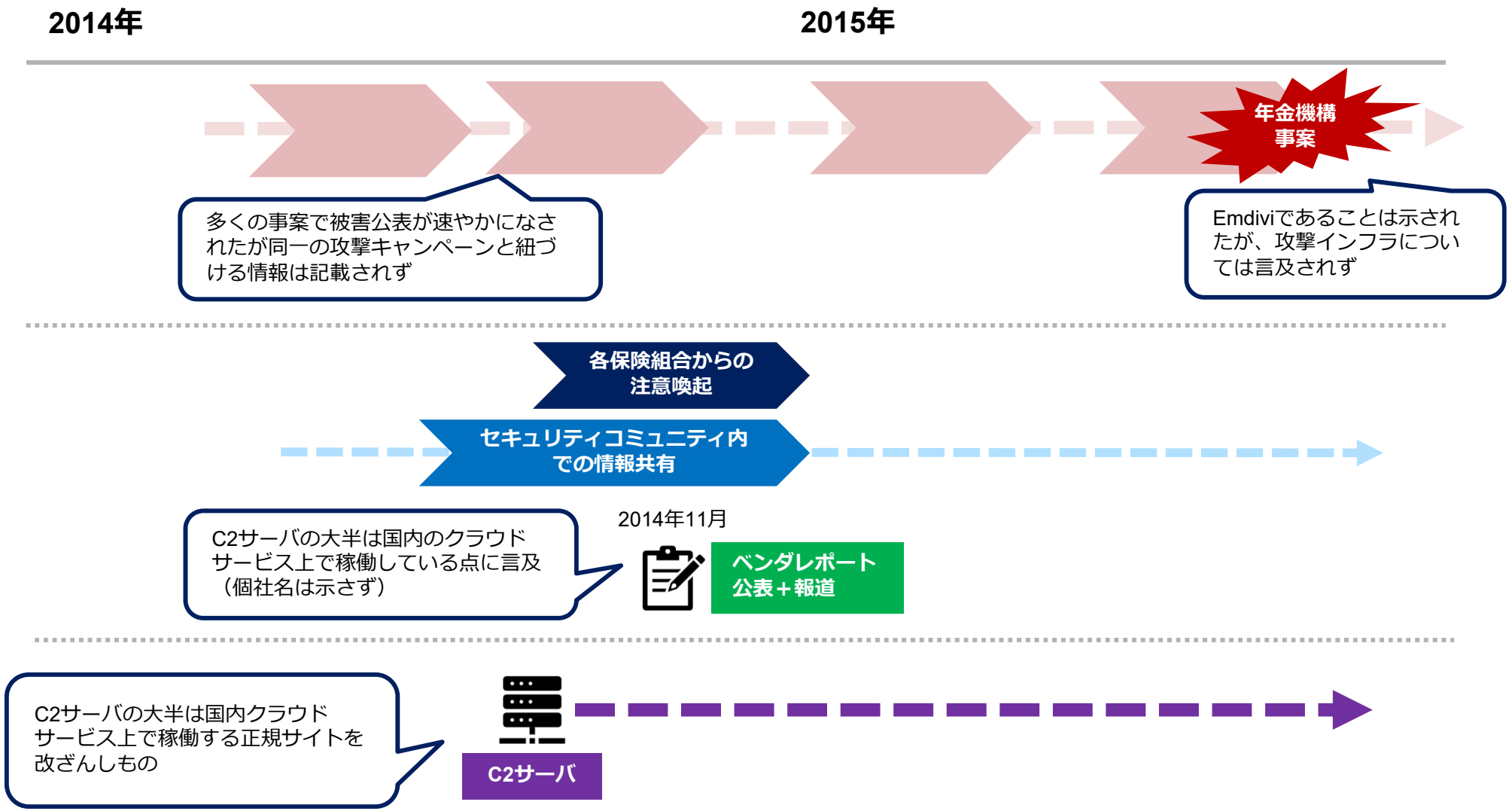
公表の社会的意義

- 広く脅威（※個別の被害ではない）が認知されることの効果があるのではないか？

- 脅威が認知されることで対策の必要性が理解されるようになる
  - 各企業等での対策実施、製品導入が進む
  - 国の施策等への理解が進む
- 脅威が認知されることで、根本的原因への対処がすすむ
  - 潜在的な被害組織の外部にある原因（特定の攻撃インフラの悪用など）に対する措置が進む

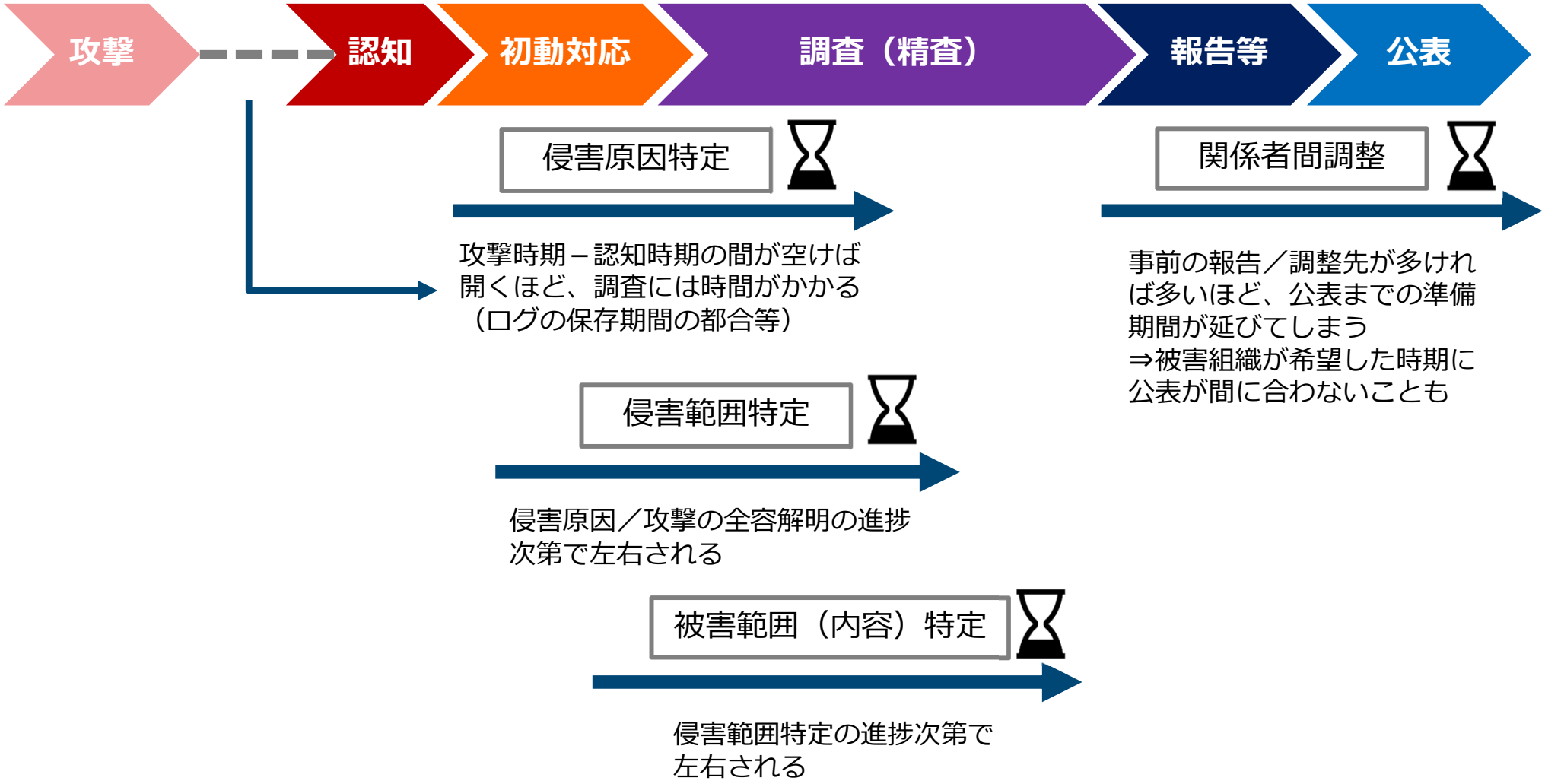
公表の社会的意義

- ケーススタディ：2014年～2015年 Emdivi事案（Operation CloudyOmega）
- 公表情報や報道から、攻撃インフラの問題には注目が向かなかったケース



【再掲】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

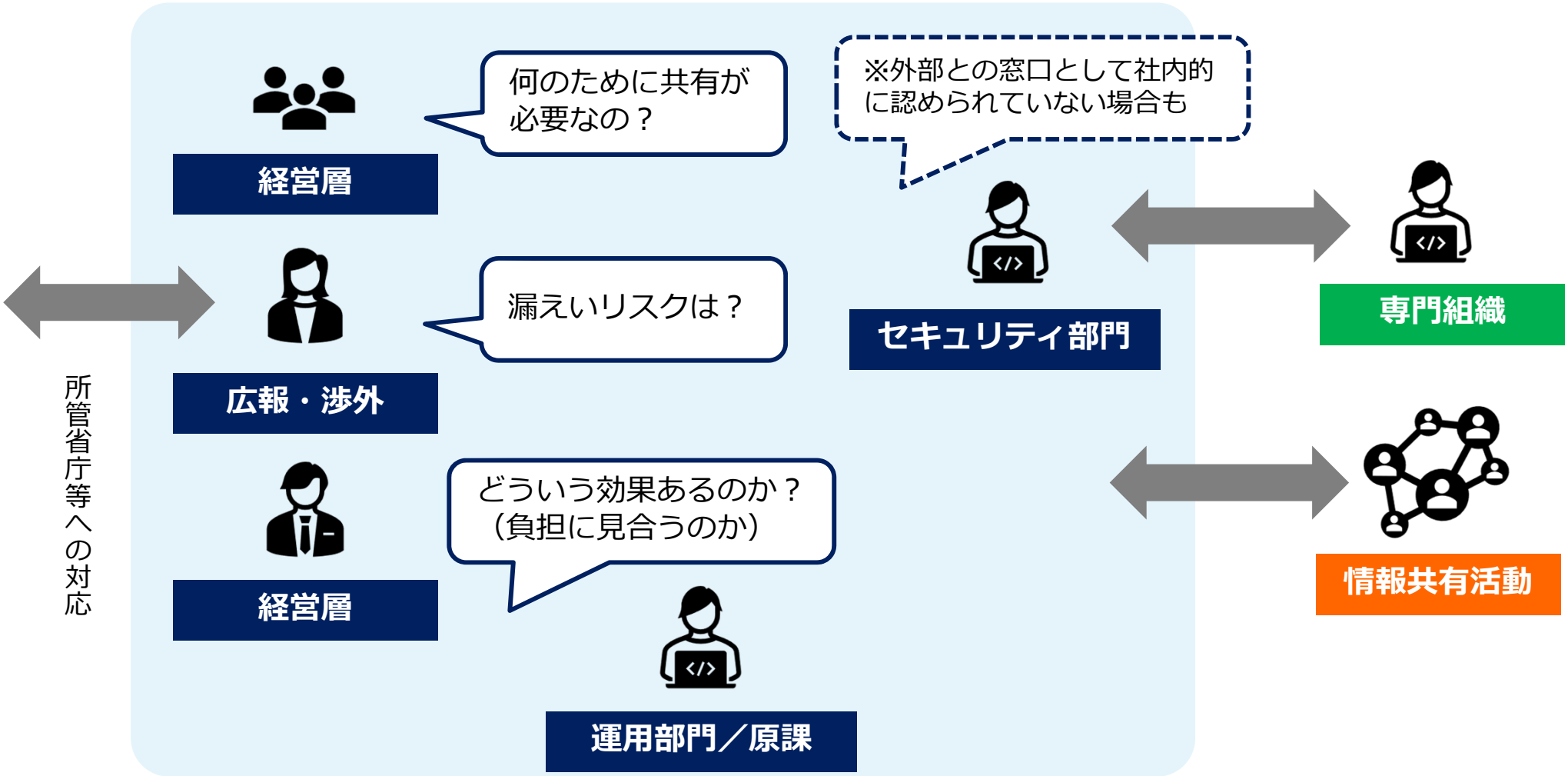


各制度の整理

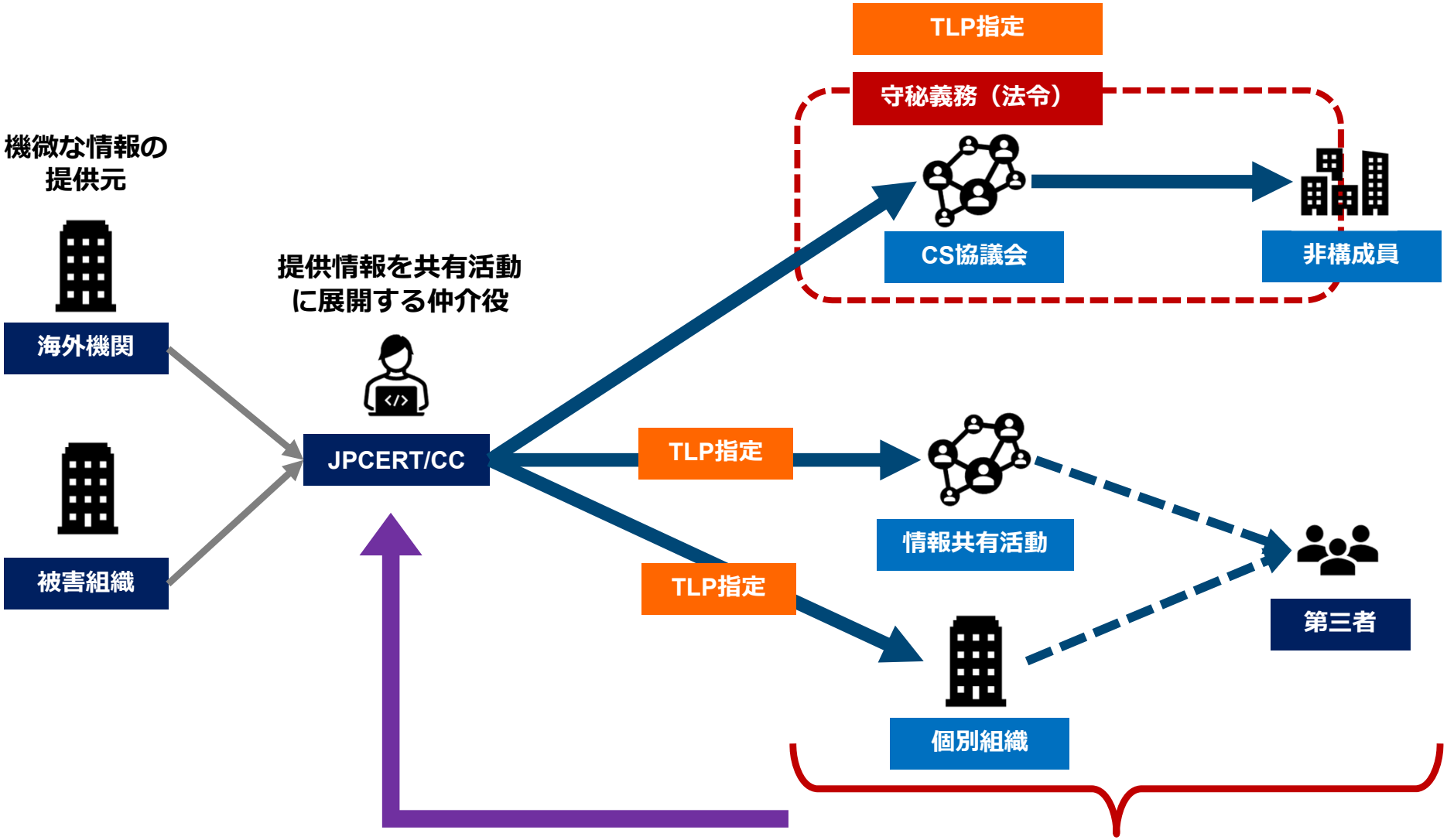
- （蔦委員説明で対応を想定）

理解促進の観点

- ガイダンスの効果として、部門間調整のための共通理解の促進につながるのではないか



信頼性の観点



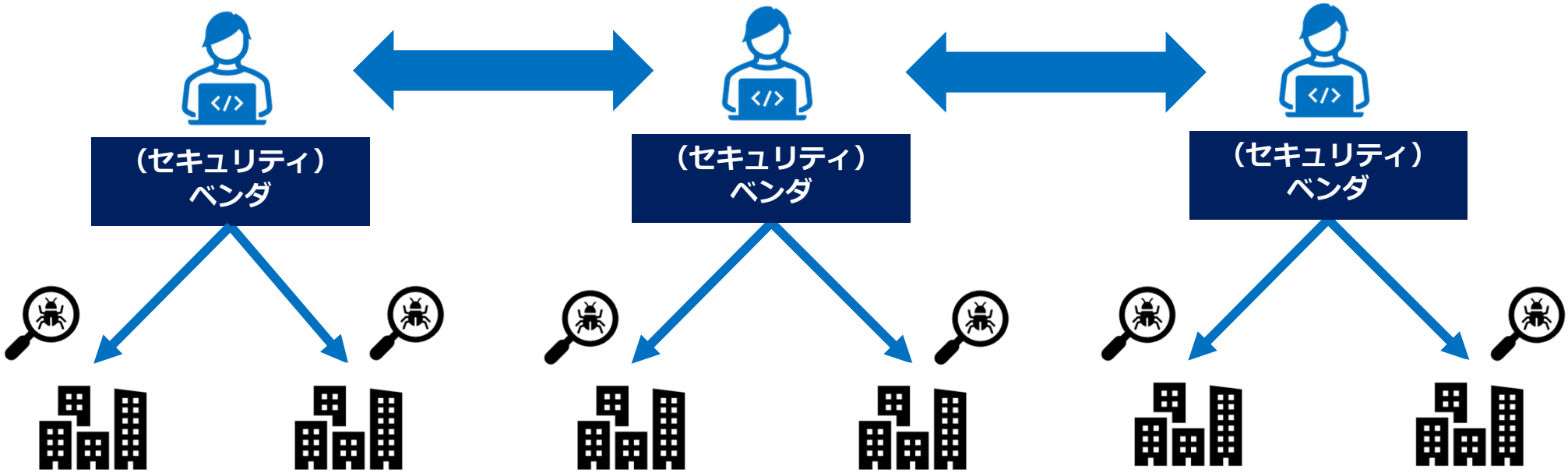
法的に強制力のない範疇の不適切な取り扱いにおいて、情報の提供元に対しては仲介組織が責任を負うことになる？

契約との関係の観点

- 主な論点は第1回目資料の参考資料に掲載済み
- 以後のスライドをご参考

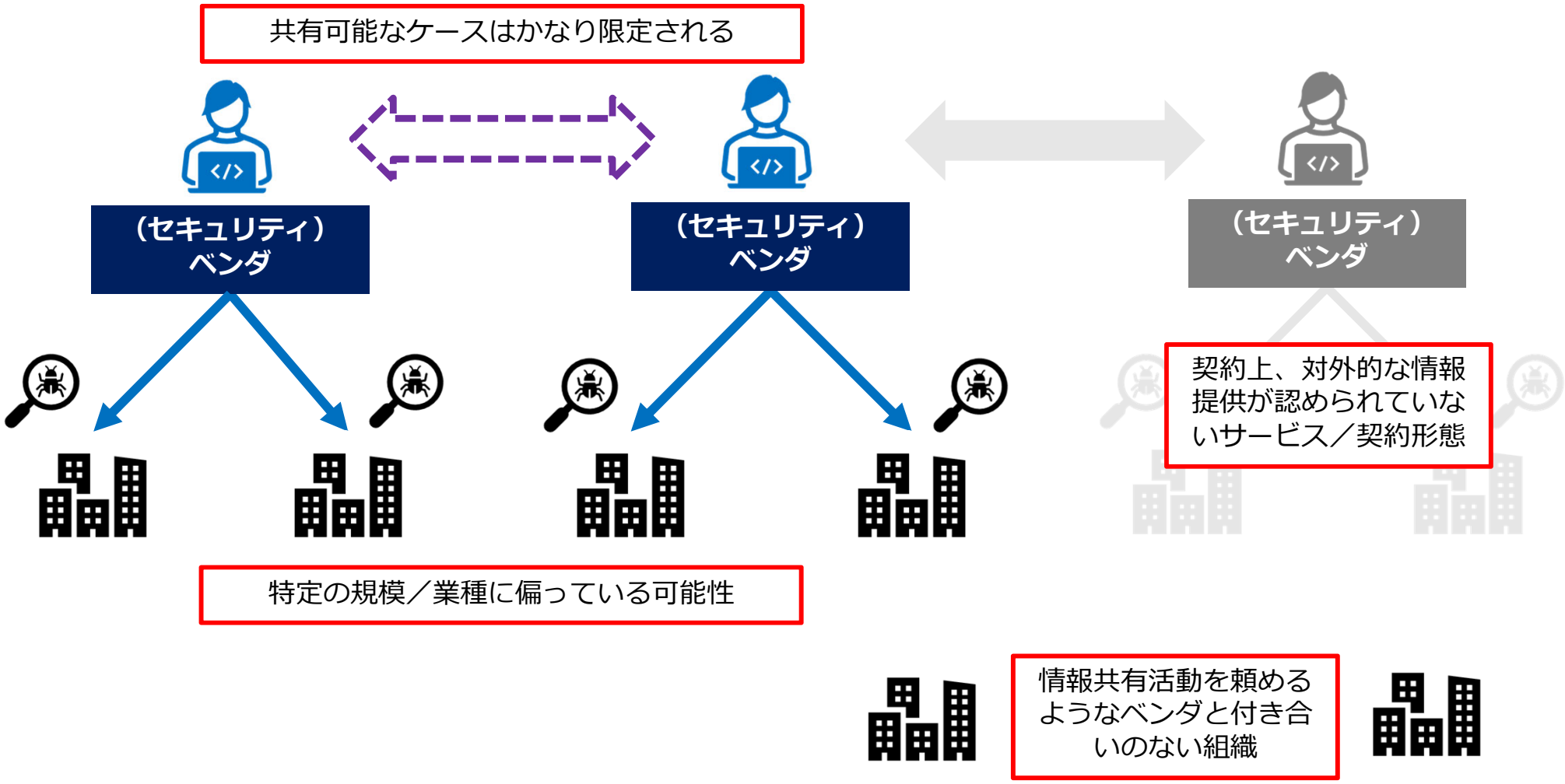
【再掲】情報共有の理屈上の“理想”

- 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）



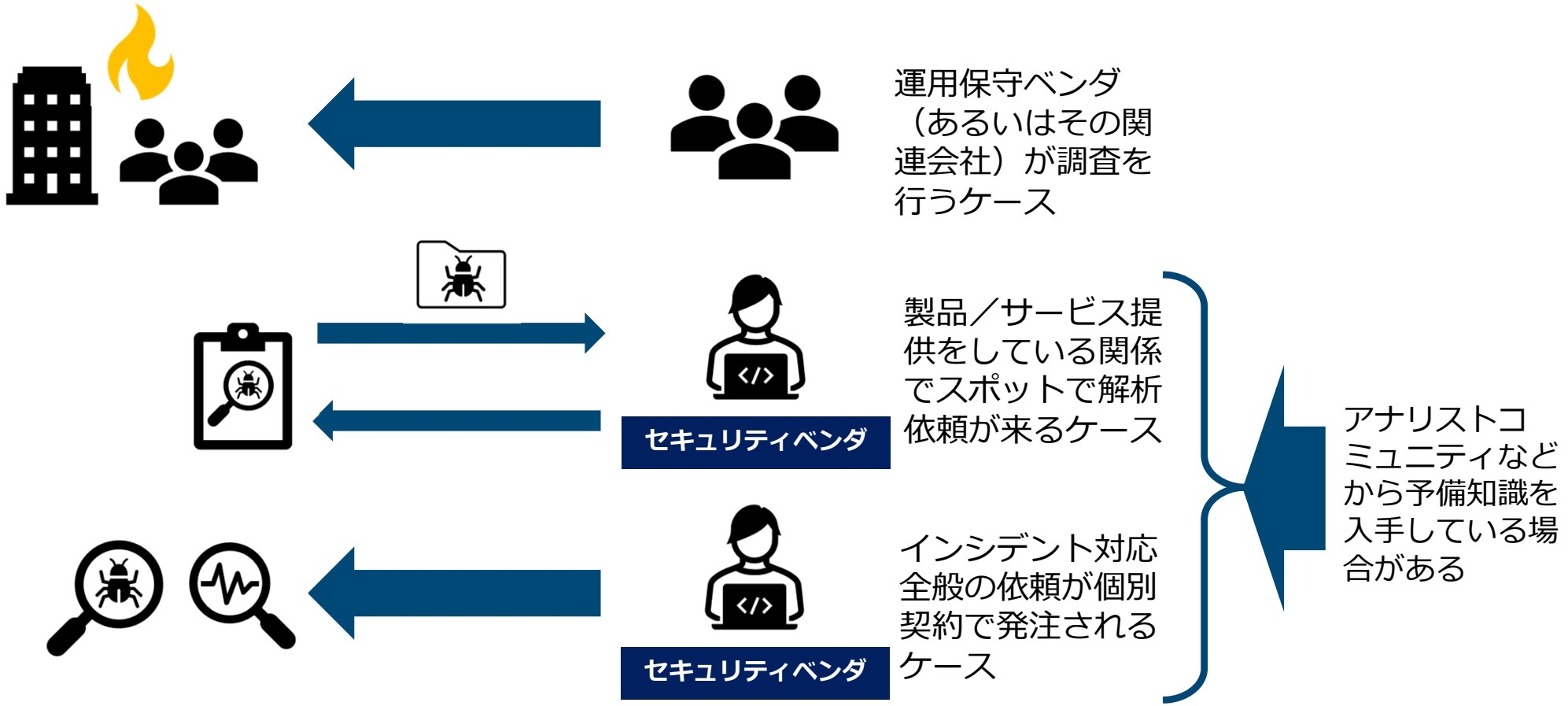
【再掲】理屈上の“理想”と“現実”

- 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）



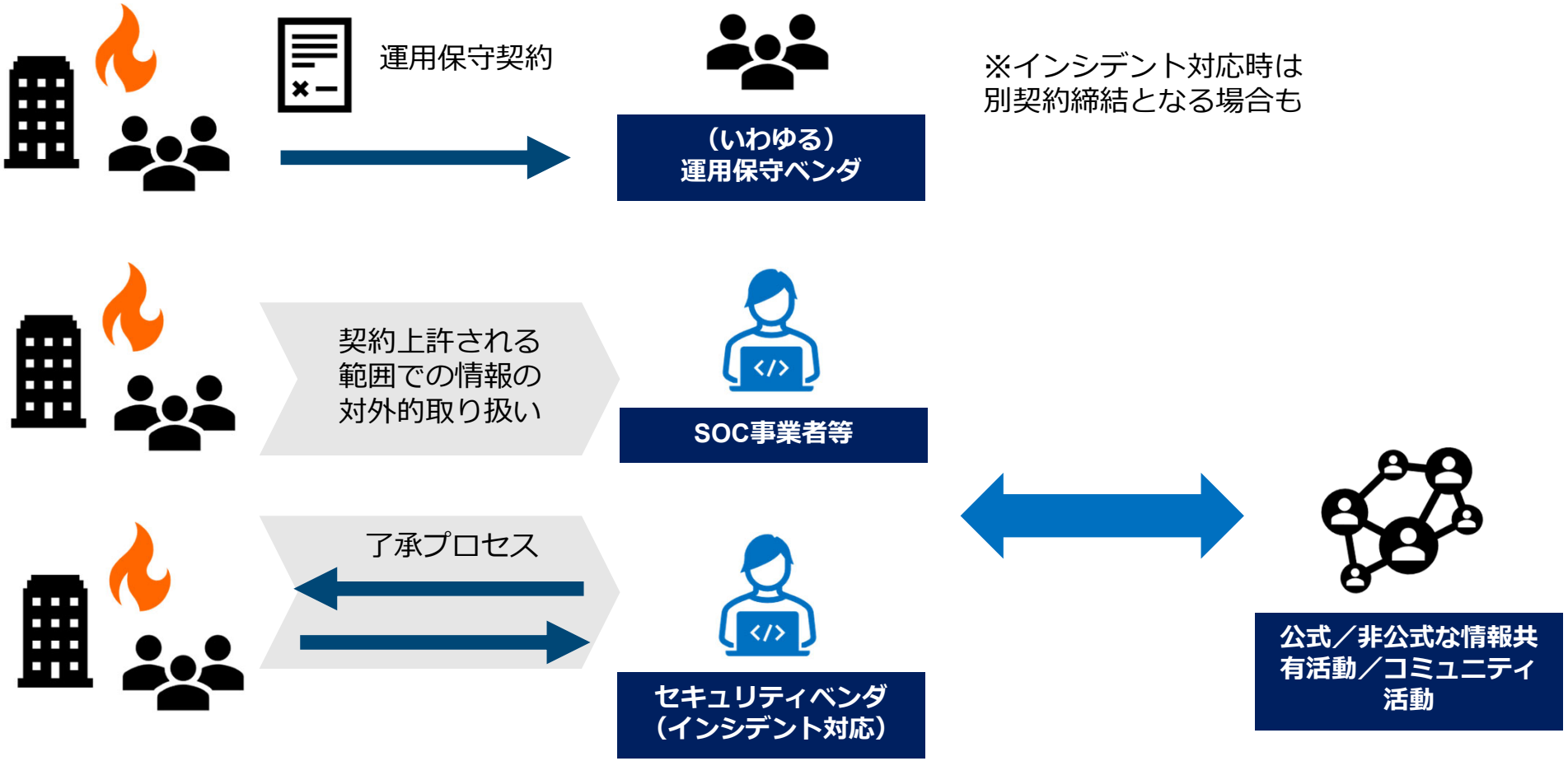
【再掲】運用保守ベンダ、セキュリティベンダ

- ※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



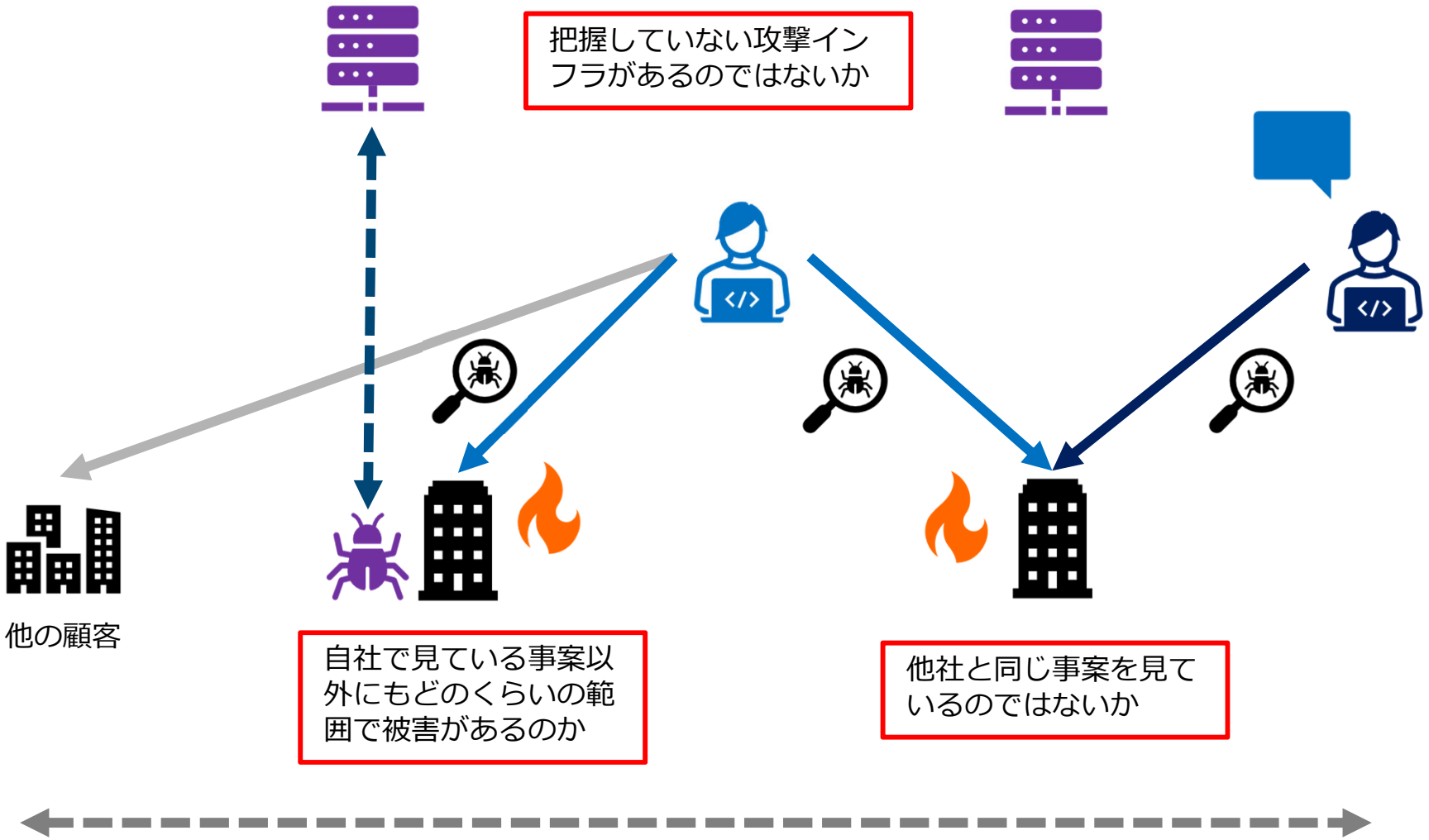
【再掲】（セキュリティ）ベンダの情報共有活動

- 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



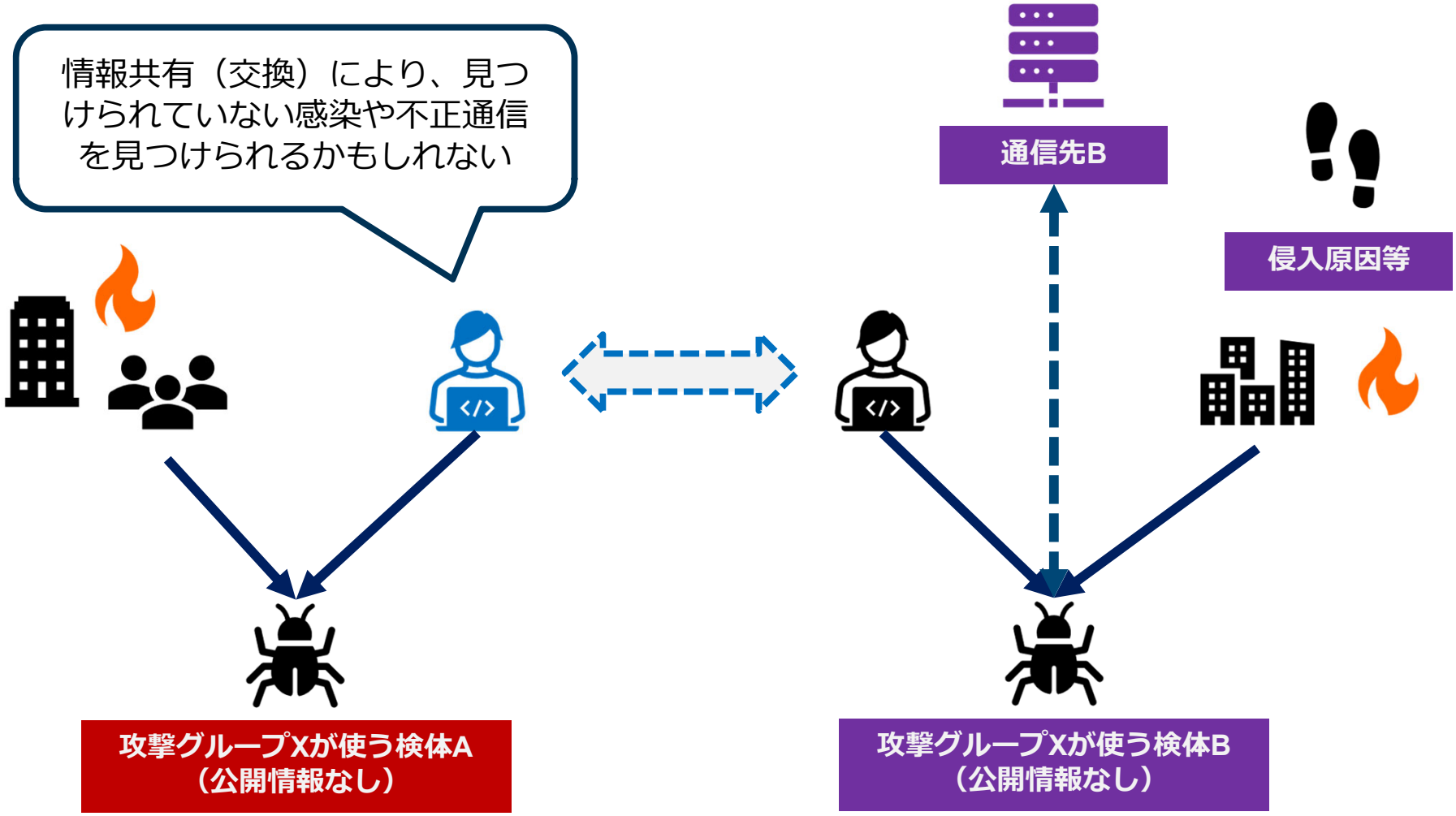
【再掲】（セキュリティ）ベンダとしての情報共有

全容把握のための情報共有のニーズ



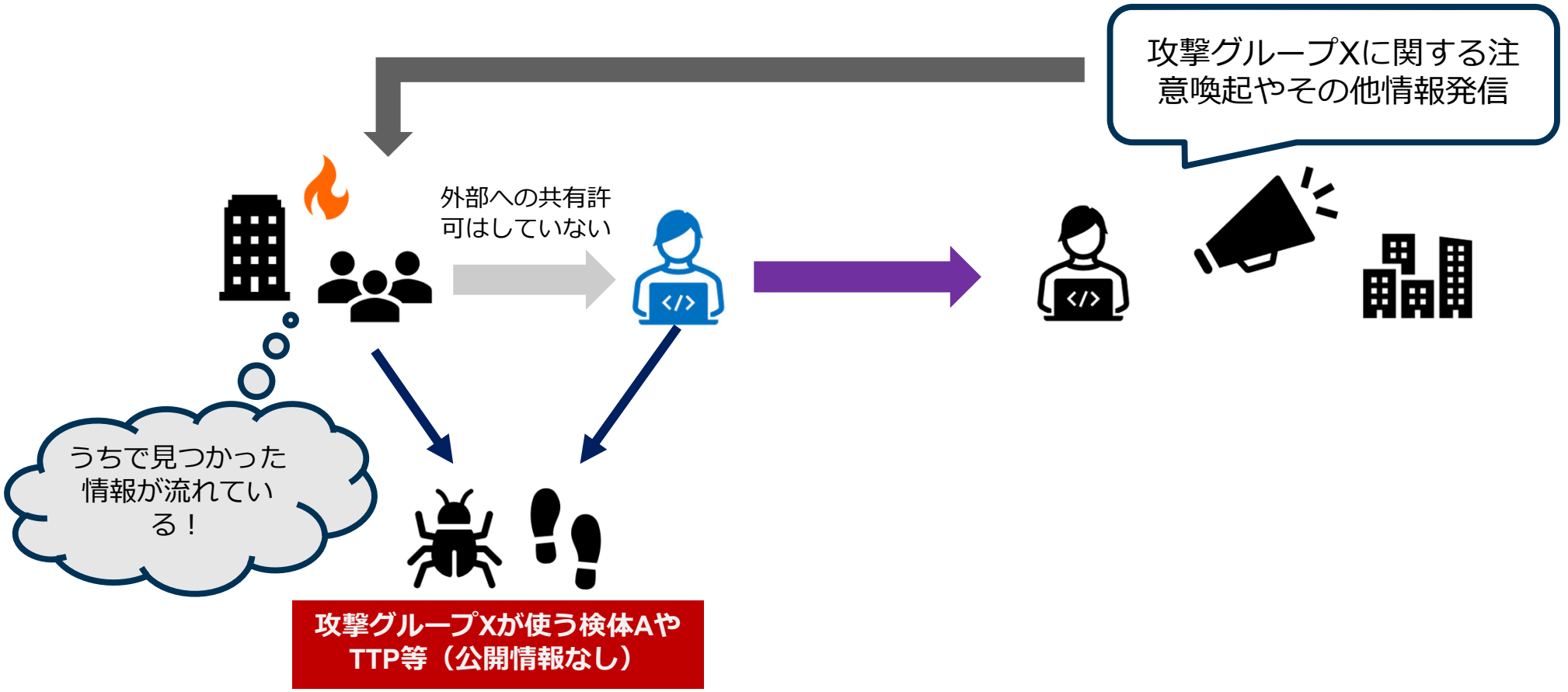
【再掲】被害組織からどのように「了解」してもらうか

- 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



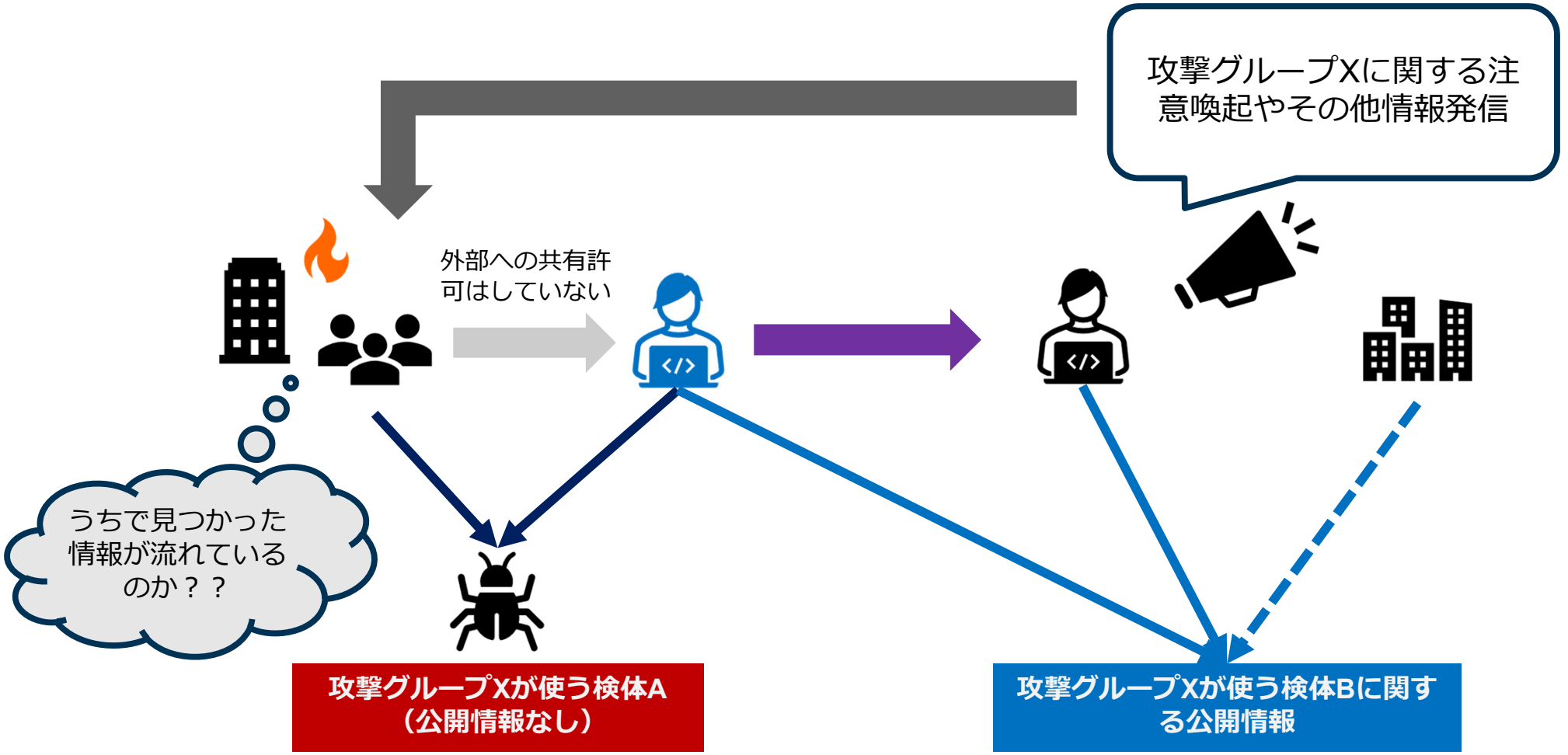
【再掲】情報共有の“滞留”ポイント

- 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



【再掲】情報共有の“滞留”ポイント

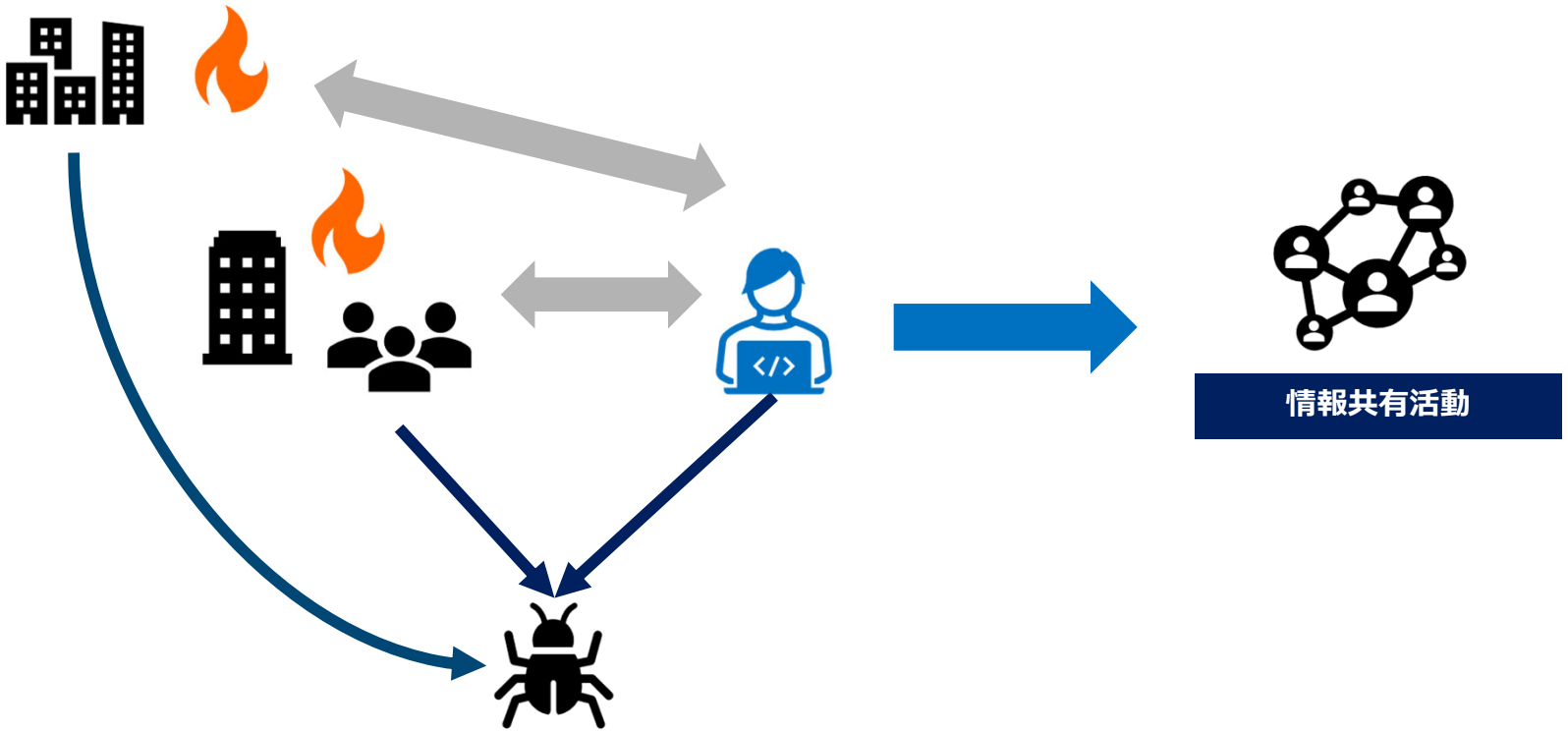
- 仮に、特定の被害組織だけで見つかった（と当該時点では思われた）情報は外部に共有していなかったとしても、被害組織から「自社だけで見つかった（と当該時点では思われた）情報を外部に無断で提供したのではないか」と疑われる可能性がある



【再掲】被害組織からどのように「了解」してもらうか

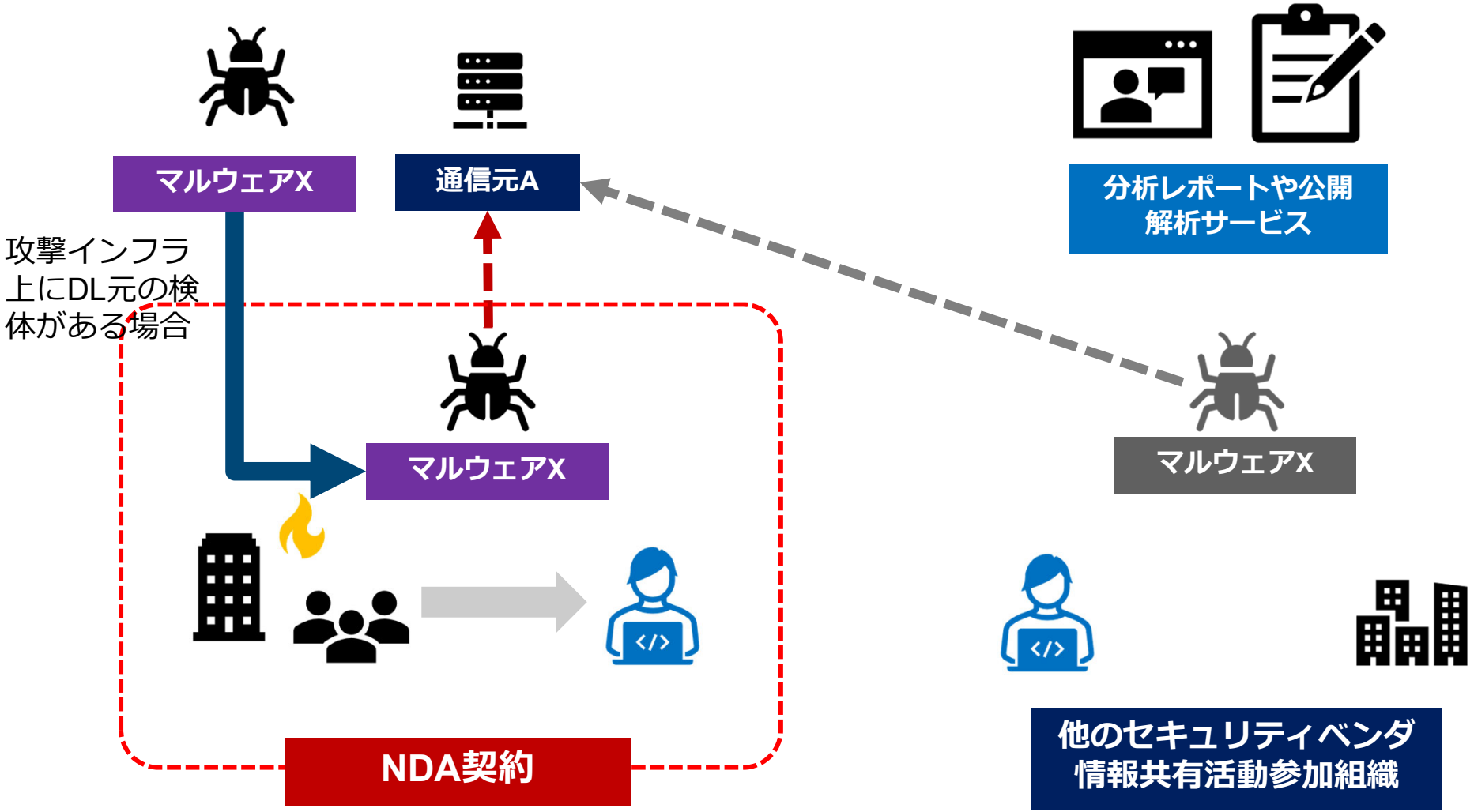
第1回目資料2-2
スライド45

- 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



【再掲】「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



「外部組織との連携」の観点

- JPCERT/CCで対応するインシデントでの事例
- 普段から何らかの情報共有活動に参加していない場合