経済産業省

サイバー攻撃の情報共有にかかる取組について

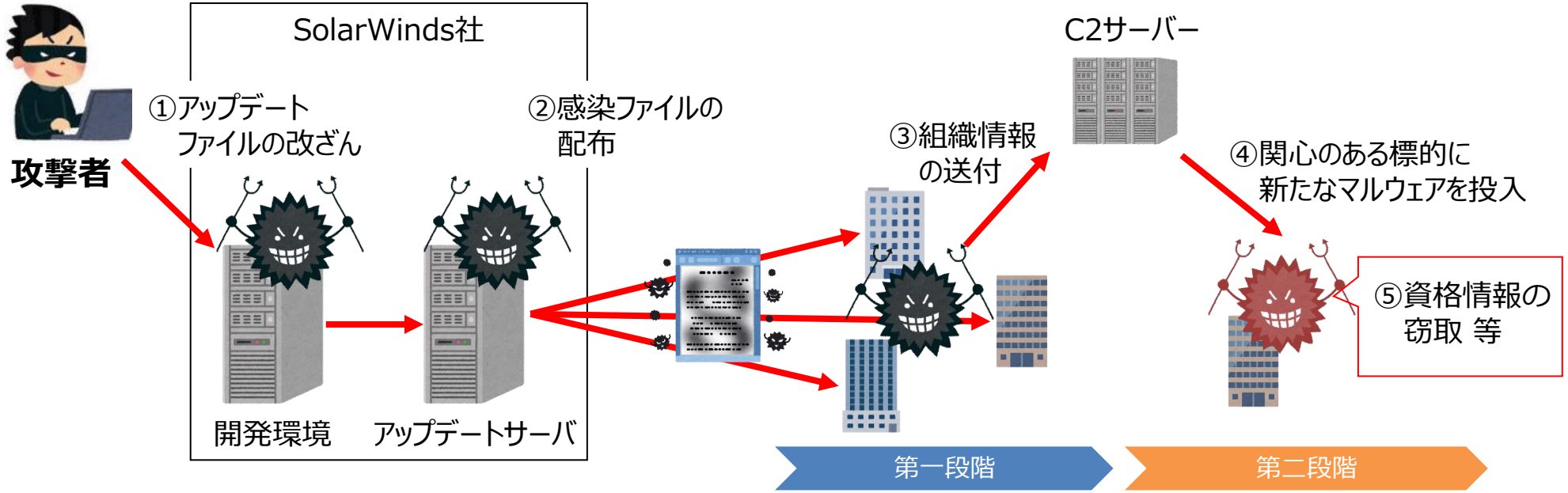
令和６年２月８日

経済産業省サイバーセキュリティ課

インシデント対応時における情報共有に関する課題例

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、正規のアップデートを通じてマルウェアが仕込まれたことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む最大約18,000組織が影響を受けたとされる。
- 事案発覚の半年前に米司法省が（自組織への）侵害に気付いており、またいくつかの事案に複数のセキュリティベンダが事案調査を始めていたが、**全体としての連携・共有が行われていなかったのではないかとの指摘あり**。

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

インシデント対応時における情報共有の重要性

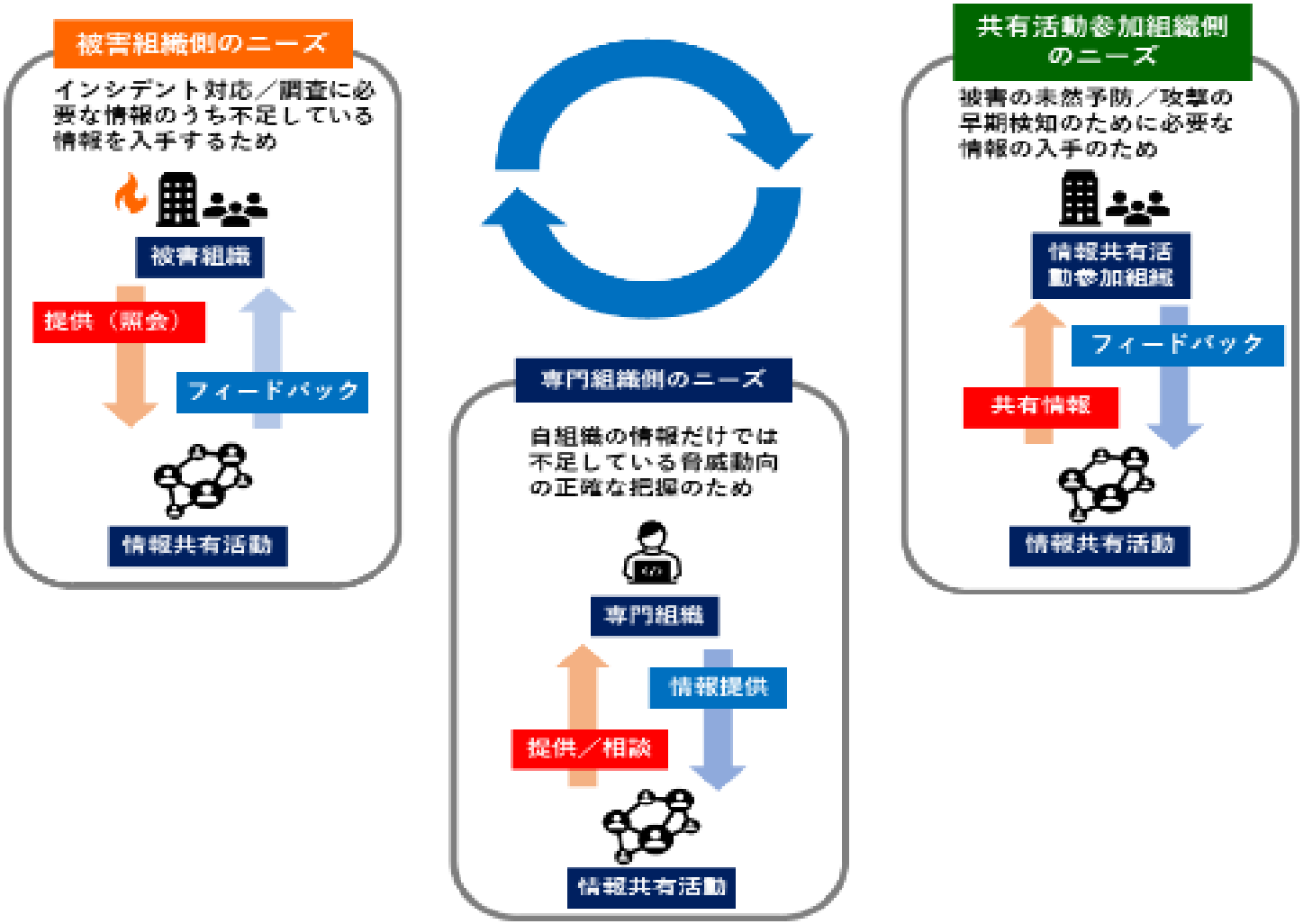
- 原因特定や被害範囲の特定、被害拡大防止や適切な再発防止策の実施につながるなど、情報共有活動を通じて「自組織だけでは見つけられなかった情報」を得ることは重要。

情報共有の目的

① インシデント対応に必要な情報を得る
② 被害防止のための情報を得る

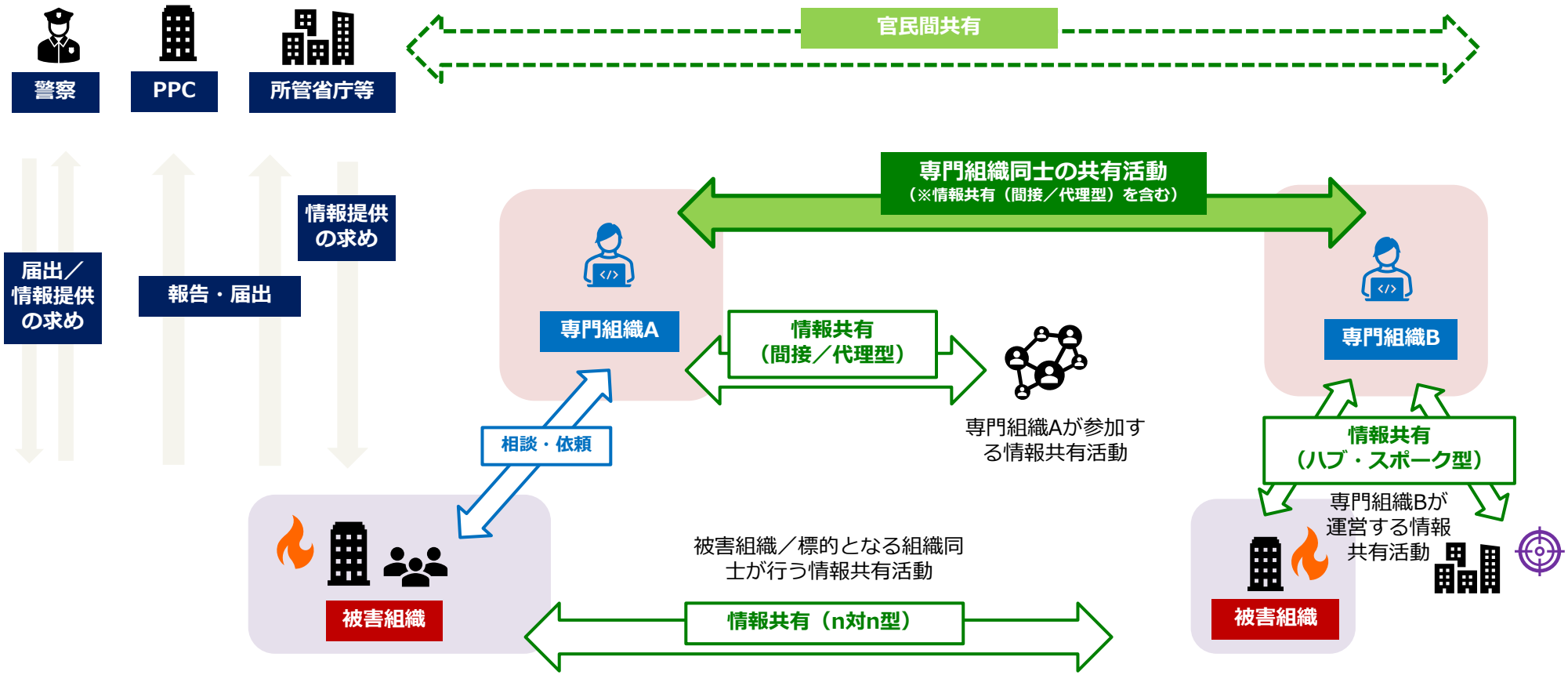
情報共有の効果

情報共有活動により「自組織だけでは見つけられなかった情報」を得ることを通じて、原因特定や被害範囲の特定、被害拡大防止や適切な再発防止策を行う



各組織間での情報共有の全体像

- 情報共有については、主に①被害組織／標的となる組織同士が行う共有、②被害組織と専門組織（専門機関やセキュリティベンダ）間での共有、③専門組織同士で行われる共有、さらには④官民間での共有などが挙げられる。

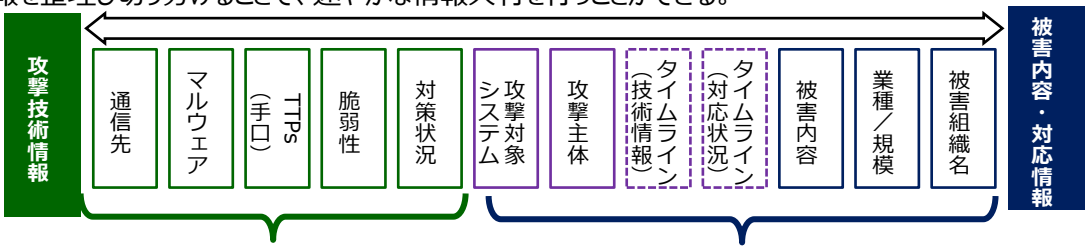


サイバー被害に係る情報共有ガイダンスの策定

- 攻撃手法が高度化する中で、単独組織による攻撃の全容解明はより困難になっている。他方で、被害組織はお互いに「他にどのような情報が存在するかを知ることができない」ため、情報共有がなかなか行われにくく、また、共有タイミングも遅いケースが多い。
- 第三者との関係などサイバー攻撃被害が複雑化する中で、被害組織のインシデント対応が適切になされているかどうかが外部から確認できず、また、被害組織も被害公表を通じた情報の開示に消極的なため、被害組織によるインシデント対応（結果）に不安や警戒を募らせるような状況になっている。
- ガイダンスでは、被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、被害組織を保護しながら、いかに速やかな情報共有や目的に沿ったスムーズな被害公表が行えるのか、実務上の参考となるポイントFAQ形式で整理。

どのような情報を？（様々な種類・性質の情報が存在）

情報を整理し切り分けることで、速やかな情報共有を行うことができる。



基本的に個別の被害組織には紐づかず、対応初期で見つかりやすく、早期に情報共有しなければ効果を得られない情報

ある程度調査期間を経なければ判明しない情報や、ステークホルダー等との調整が必要な機微な情報などが含まれるため、公表までに時間がかかる情報

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（被害組織等）

サイバー攻撃被害に係る情報の共有・公表ガイダンス
～情報共有・被害公表のポイント～

本ガイダンスは、被害組織で見つかった情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理したものです。

1.情報共有

- **(1)目的：**被害調査に必要な情報の提供や被害の未然防止に資する
- **(2)タイミング：**情報共有と被害公表を分離し、迅速な情報共有を図る
- **(3)情報の整理：**攻撃に関する情報（攻撃技術情報）と被害に関する情報（被害内容・対応情報）を分離し、

  迅速な攻撃技術情報の共有を図る

2.被害公表

- **(1)目的：**レピュテーションリスク低下やインシデント対応上の混乱の回避に資する
- **(2)タイミング：**攻撃の種類や被害の状況から、効果的な公表タイミングを選ぶ
- **(3)情報の整理：**専門組織との連携や情報共有活動の状況など対応の経緯等を含めて示すことで、

  ステークホルダーの不安等を解消することができる

3.外部組織との連携

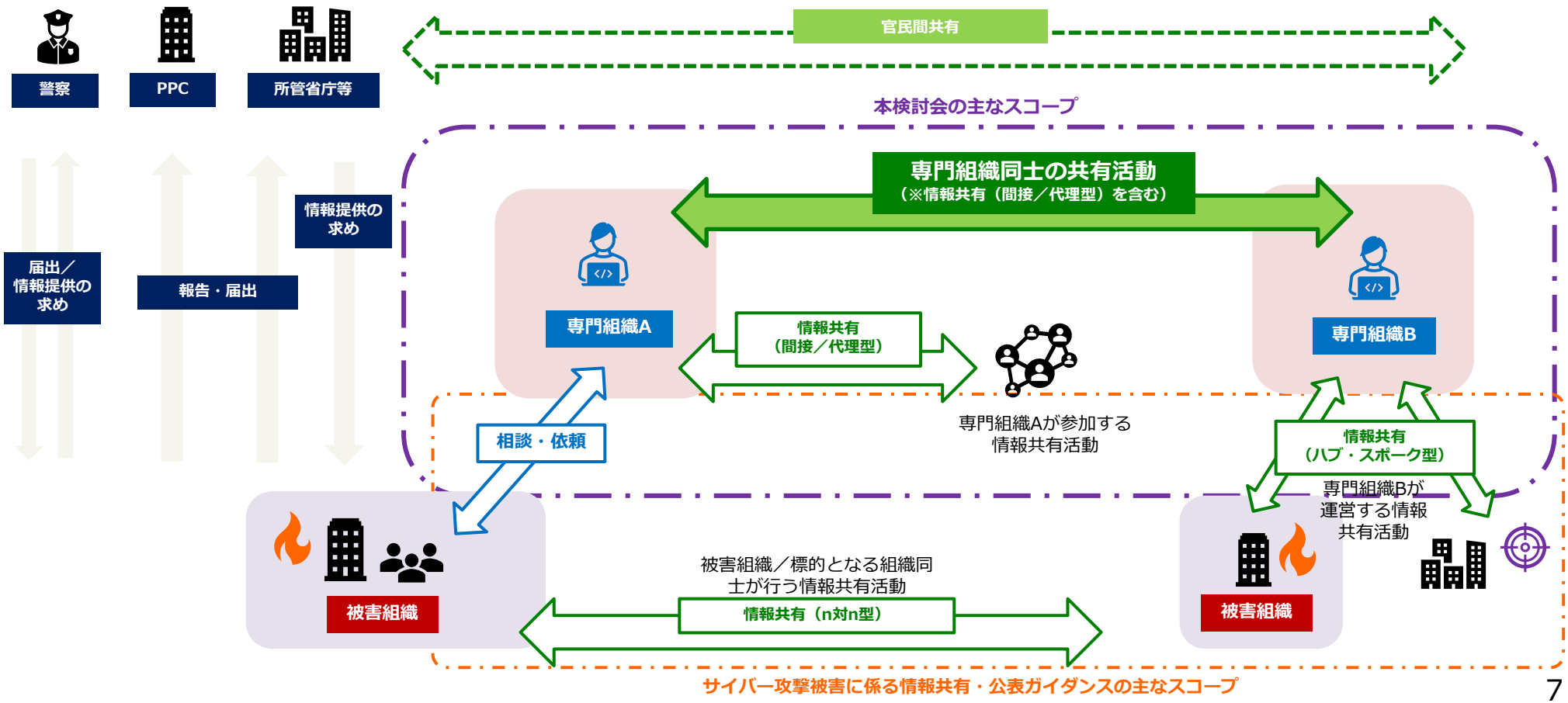
- 専門組織との連携、警察への通報・相談、所管官庁への報告等を実施することで、正確な情報共有や注意喚起、捜査を通じた犯罪抑止や広く国民に影響する事案への対処等につなげることができる

4.機微な情報への配慮

- 被害者への保護や機微な情報への配慮が必要な情報の取扱いを知ることで、スムーズな情報共有、被害公表を行うことができる

(参考)各組織間の情報共有の全体像と本検討会の主なスコープ

- 被害組織を直接支援する専門組織を主体とした情報共有により、被害組織も含め他の組織における被害の拡大防止や、被害組織にとっての情報共有に必要な社内調整コスト等の軽減につながり、また、事案対応の最適者が調整され得るといった利点が見込まれる。
- そのため、**本検討会では**、情報共有公表ガイダンスで主なスコープとしていた被害組織自身による情報共有ではなく、**被害組織を直接支援する専門組織間での情報共有の促進を主なスコープとして、情報共有を促進するための必要事項を検討**。
- 専門組織が被害者組織との間において事前に共有可能な情報について共通の認識を持ち、共有した情報の取扱いについて、事後に不要なトラブル等を防ぐことが可能となる。



サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書概要

１．情報共有の重要性と現状の課題

- サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。そのため、**攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要**。他方で、被害組織自らが情報共有を行うことについては、①被害組織側の調整コスト負担、②最適者が事案対応を行わない懸念、③処理コストのかかる情報共有、④被害現場依存の脱却の必要性などの課題が存在。

２．本検討会における提言

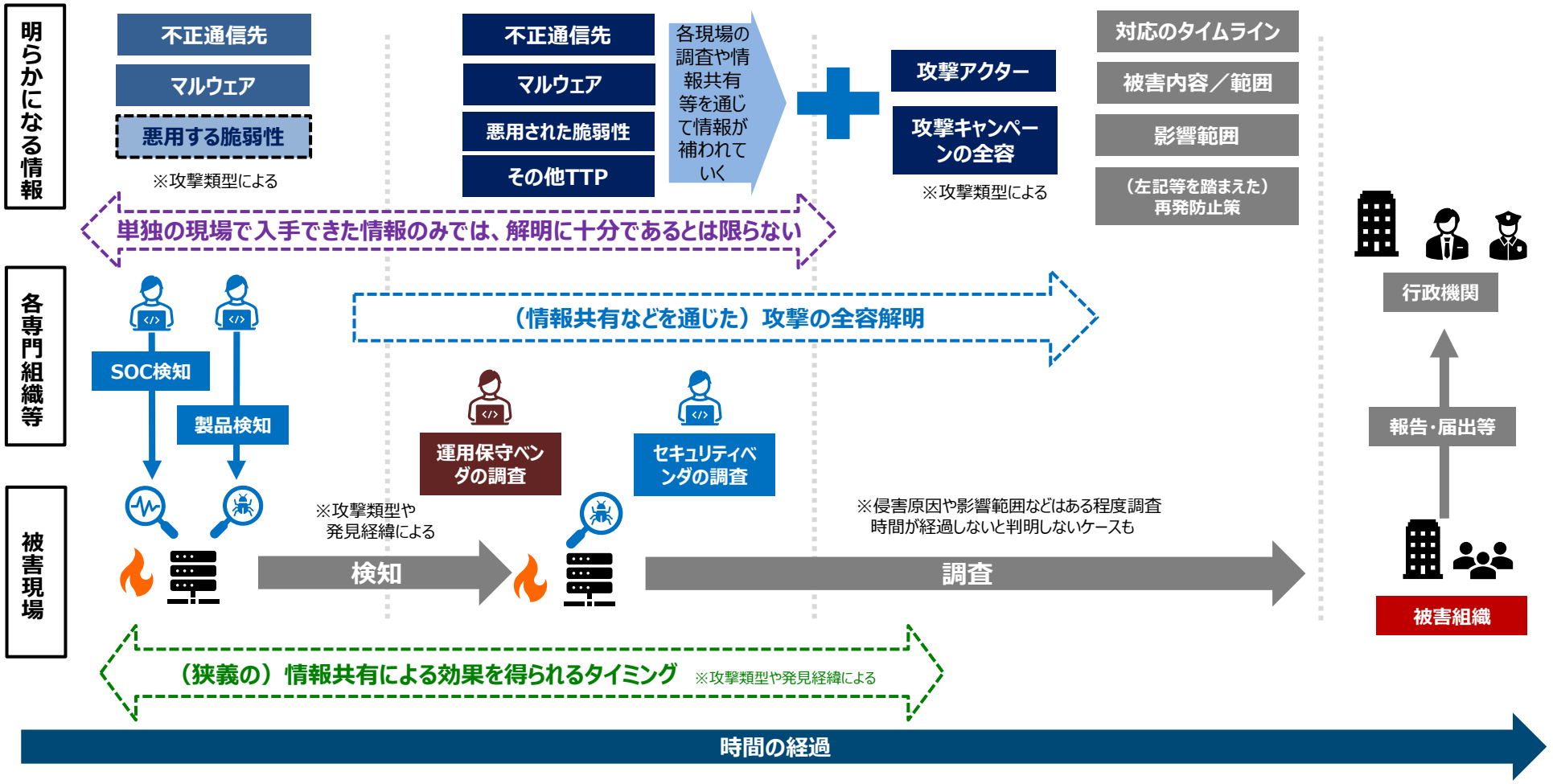
- **被害組織を直接支援する専門組織を通じた速やかな情報共有の促進が重要。**これにより、①全体像の解明による被害拡大の防止や②被害組織のコスト低減などが実現できる。
- 他方で、専門組織を通じた情報共有を促進するためには、**①秘密保持契約による情報共有への制約、②非秘密情報からの被害組織の特定/推測の可能性の課題に対応をする必要がある。**
- このため、本検討会では、これらの課題を乗り越え、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有を可能とするために、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の**「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得る**と整理。
- さらに、本報告書の提言を補完する観点から、**「攻撃技術情報の取扱い・活用手引き（案）」についてもとりまとめ**。本手引きでは、専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えばよいか、またどのように情報共有をおこなえばよいのかなど**専門組織として取るべき具体的な方針について整理**。
- 加えて、円滑な情報共有を促進すべく、上記考え方について**ユーザー組織と専門組織が共通の認識**を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく**法的責任を原則として負わないことを合意するため**の**秘密保持契約に盛り込むべきモデル条文案を提示。**今後、本検討会の成果の**周知・啓発に取り組む**。

３．今後の課題

- 専門組織同士の情報共有促進だけでは解消されない**今後の課題**としては、**（１）情報共有に向けた官民連携のあり方**（行政機関への相談・報告のあり方や政府と民間事業者間の情報の共有など）、**（２）サプライチェーンにおけるベンダ等の役割**を挙げた。

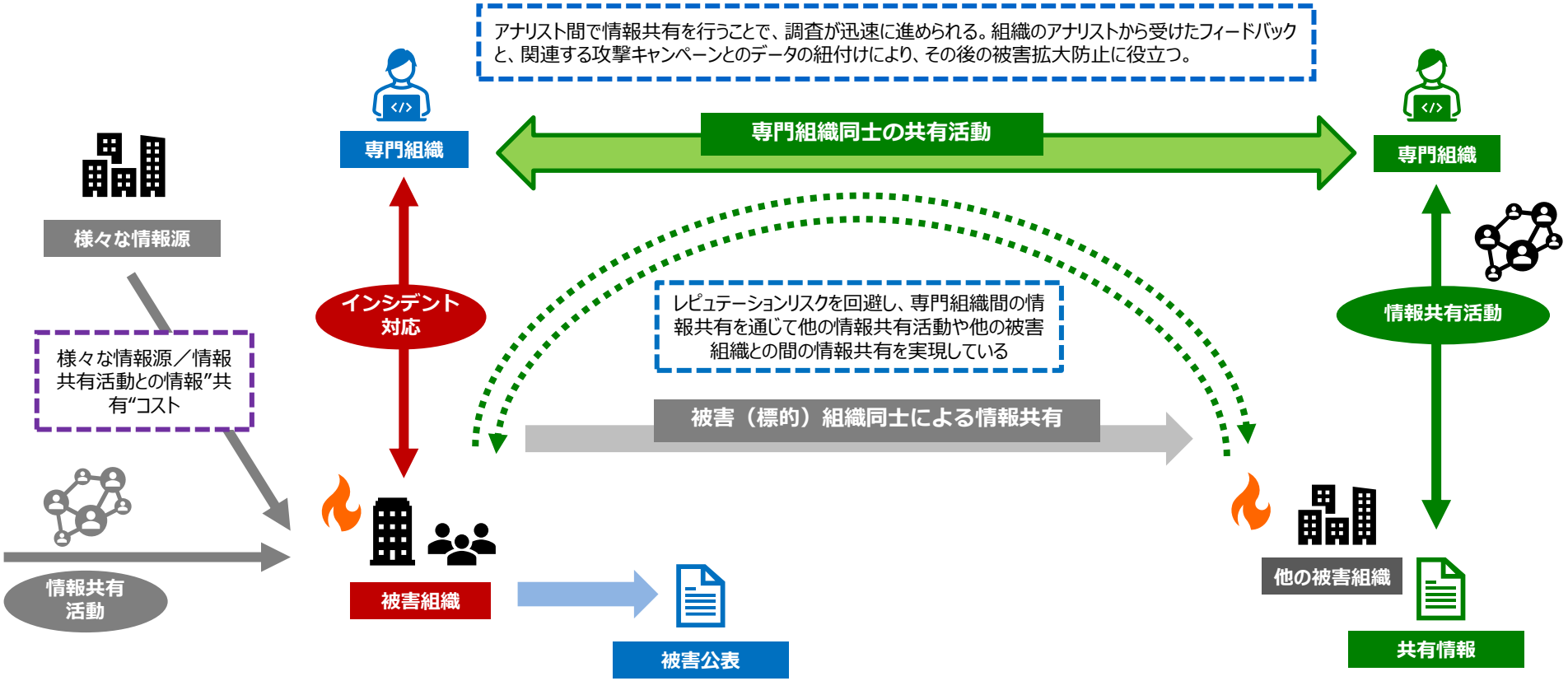
(参考)専門組織による情報共有活動の重要性①：全体像の解明

- 被害企業においては、セキュリティ監視をしている運用保守ベンダ等により不正通信先やマルウェア等が検知される、もしくは初動対応に当たった段階での調査で、悪用された脆弱性等が把握されることがある。
- しかし、それらの情報のみでは、被害の原因究明・再発防止に十分な情報を得られているとは限らず、専門組織による情報共有により、他者でも同様の攻撃が起きている状況を把握しながら、被害拡大防止と攻撃の全容が解明されていく必要がある。



(参考)専門組織を通じた情報共有の重要性②：被害者組織のコスト低減

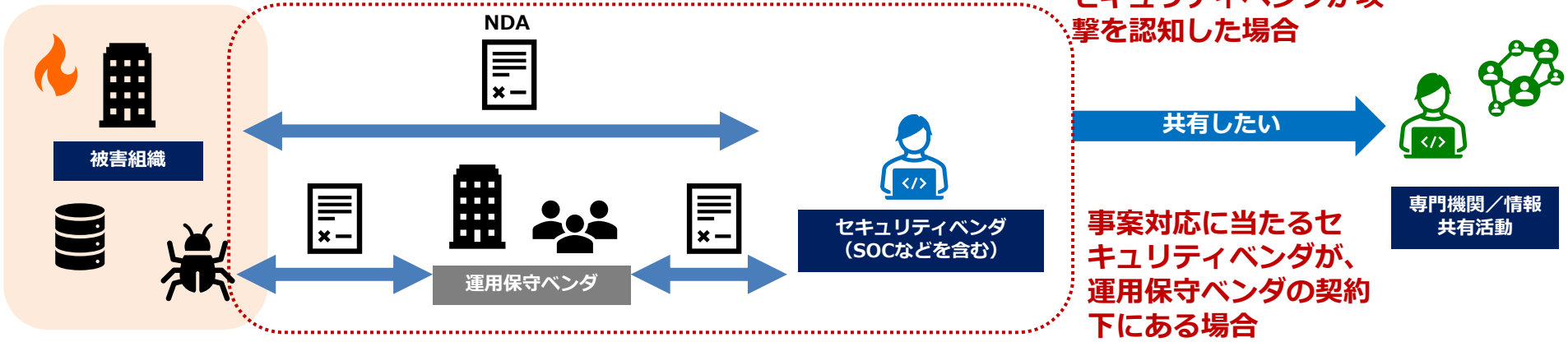
- 情報が必要に応じて「非特定化」され、専門組織を通じて他の情報共有活動に提供されることで、被害組織は、情報共有対応コストを軽減できるだけでなく、 レピュテーションリスクも低く保ちながらフィードバックを得ることができ、調査に資する情報を得ることができる。その結果、調査が迅速に進められる等、被害拡大防止につながる。



専門組織を通じた情報共有の課題：秘密保持契約（NDA）の関係、被害組織が推測されるおそれ

- 専門組織を通じた情報共有は重要であるが、**専門組織が共有したい情報が、秘密保持契約上の「秘密情報」扱いとされ、共有できない可能性**がある。
- また、マルウェアの検体には、**被害組織を特定や推測できる情報が含まれていることがある**ため、そのままでの情報共有は不適切な場合がある。

秘密保持契約（NDA)が問題となるケース



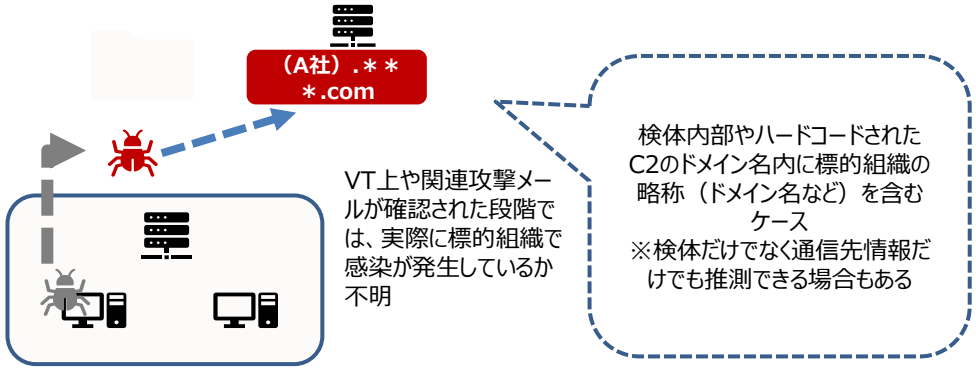
検体そのものが流通することで被害組織が特定／推測されるケース

参照：第1回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　資料2-2 JPCERT/CCからの論点提示資料

ケース①

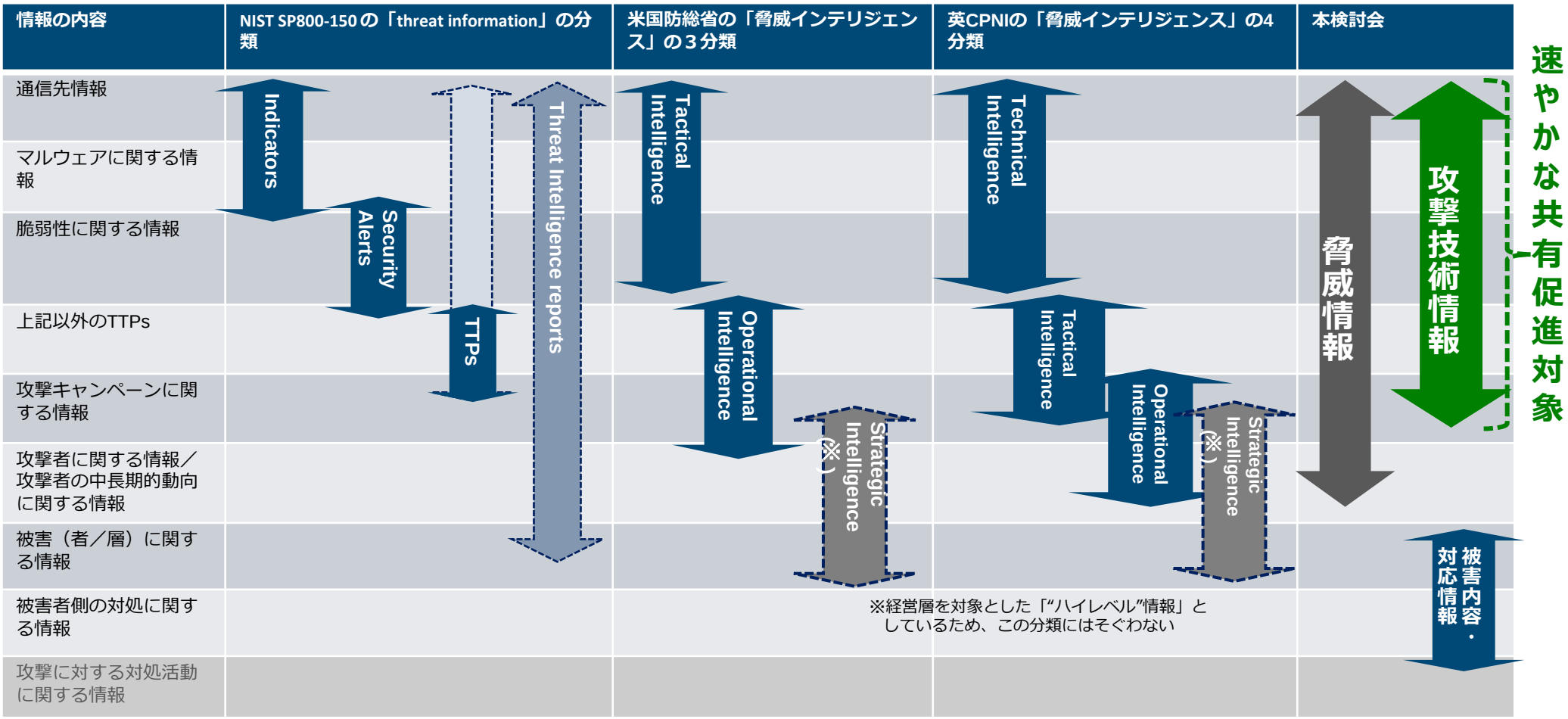
【例】 Olympic DestroyerのVT上にあがった検体

ケース②



速やかな共有促進の対象となる「攻撃技術情報」について

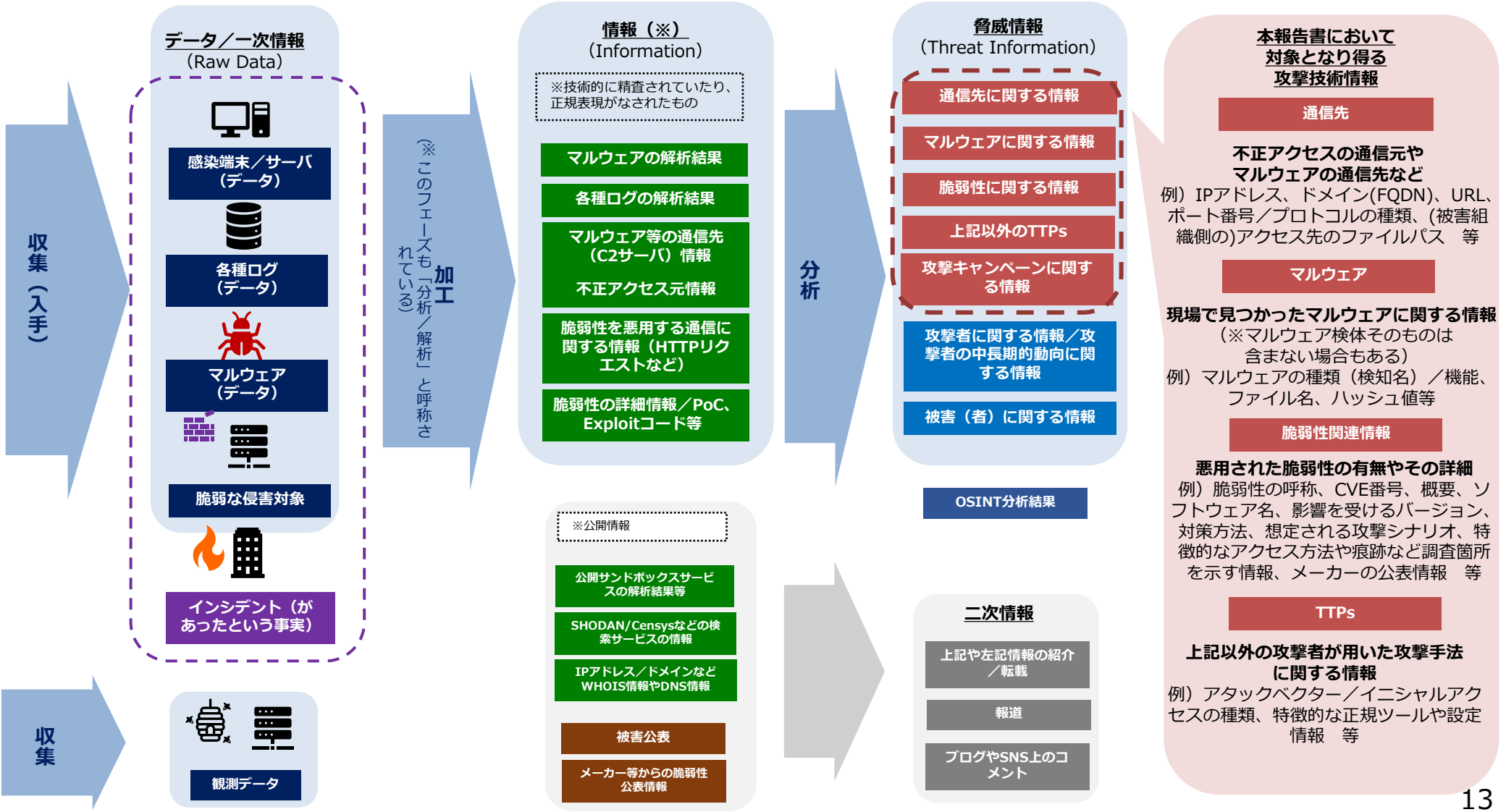
- 脅威情報のうち、**攻撃技術情報には基本的に被害組織が特定される情報は含まれないため、専門組織の判断で他の専門組織への速やかな情報共有が可能な対象となり得る**。ただし、場合によっては被害個社名等を推測可能なケースが想定されるため、留意が必要。



脅威情報：被害組織から専門組織に提供等される調査対象の「データ」を加工し、技術的に精査等した「情報」を分析したもの。

（参考）「データ」、「情報」、「脅威情報」、「攻撃技術情報」について

- 脅威情報は、被害組織から専門組織に提供等される調査対象の「データ」を加工し、技術的に精査等した「情報」を分析したもの。
- 「攻撃技術情報」とは「脅威情報」のうち、通信先情報やマルウェア情報、TTP情報等、攻撃者による攻撃手法やその痕跡を示すもの。



(参考)攻撃技術情報の取扱い・活用手引き（案）

- どのような情報が速やかに専門組織同士で共有できるのか、そもそもどのような情報を共有すべきなのか、どのような情報は被害組織（情報提供元）が特定／推測されるおそれがあるのか、どのように非特定化加工すれば良いのか、どのように共有すれば良いのか、といった専門組織同士の情報共有における各論点や方法について解説。

目次構成

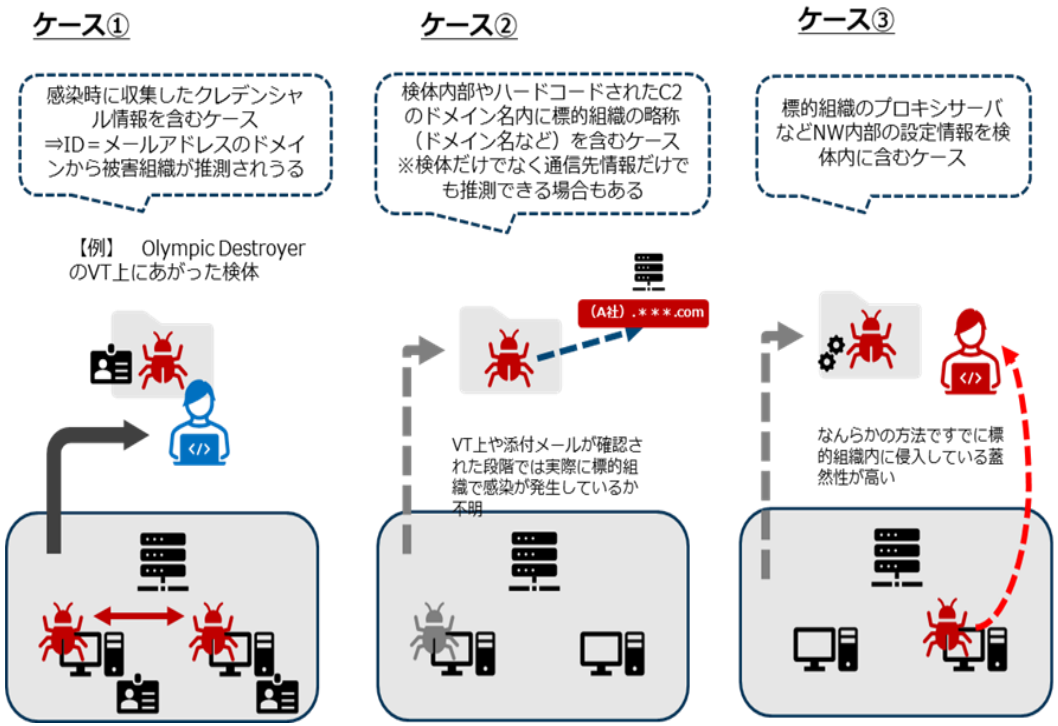
はじめに
・スコープとしている情報共有活動
・用語の定義
・本手引きの想定読者

第１章　専門組織間の情報共有について
・脅威情報を扱う大原則
・脅威情報と「攻撃技術情報」いついて
・どのような情報を共有するのか
・何のために専門組織は攻撃技術情報を共有するのか
・専門組織間の共有が有効な場合と有効でない場合
・どうやって共有するのか
・いつ共有するのか
・正確性を優先すべきか、スピードを優先すべきか
・情報受信側の対応コストを減らすためのポイント
・攻撃技術情報共有時の被害組織との間の問題点は何か
・NDAについて

第２章　各攻撃技術情報の解説
・通信先情報
—通信先情報について
—通信先情報の特性
—通信先情報の共有のポイント
—被害組織が特定されてしまうケース
・マルウェア情報
—専門組織同士のマルウェア情報の共有
—その情報を共有するのか：マルウェア解析情報
—被害組織が特定されてしまうケース
・脆弱性情報
—被害組織が特定されてしまうケース
・その他TTPs
—被害組織が特定されてしまうケース

第３章　ユースケース

解説例：検体に内包する情報から被害組織が特定／推測されるケースの解説



(参考)秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文案

- 専門組織を通じた情報共有を促進し、被害組織の被害に対する迅速な調査や被害拡大防止等を目的として、あらかじめ被害組織（ユーザー組織。甲）と専門組織（乙）間で合意しておく攻撃技術情報等の取扱いや円滑な情報共有のための関連事項（保有情報に対する安全管理措置や免責事項など）を示すもの。

１．乙は、本サービスの遂行過程において、乙の知見により得られたサイバー攻撃に関する通信先、マルウェア、脆弱性その他の情報（以下この条において「攻撃技術情報」という。）について、甲の被害に対する迅速な調査、被害拡大の防止及び甲乙以外の組織に対するサイバー攻撃の未然防止を目的としてこれを保有又は利用し、また、甲を識別及び特定できないように加工した攻撃技術情報（以下この条において「攻撃技術情報」及び「甲を識別及び特定できないように加工した攻撃技術情報」を合わせて「攻撃技術情報等」という。）を作成、保有、利用又はサイバーセキュリティに関する専門組織に対して開示することができる。

２．乙は、保有する攻撃技術情報等について、必要かつ適切な安全管理措置を講じなければならず、前項の目的を達成するために必要な範囲を超えて攻撃技術情報等を開示してはならない。

３．乙は、第１項及び第２項の攻撃技術情報等の利用又は開示に関連して、甲に生じた損害については一切の法的責任を負わないこととする。ただし、乙に故意又は重過失がある場合は、この限りでない。