経済産業省

事務局説明資料

（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）

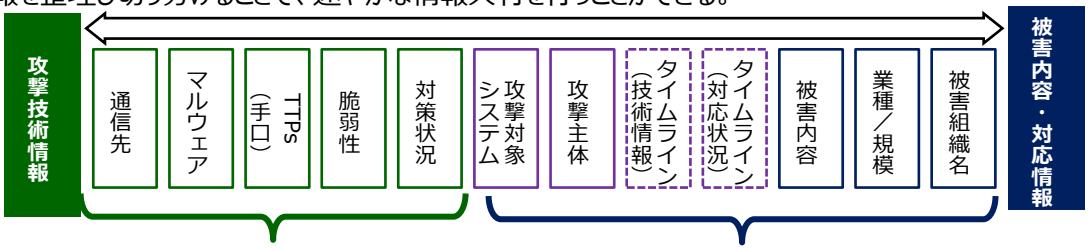
経済産業省
サイバーセキュリティ課

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

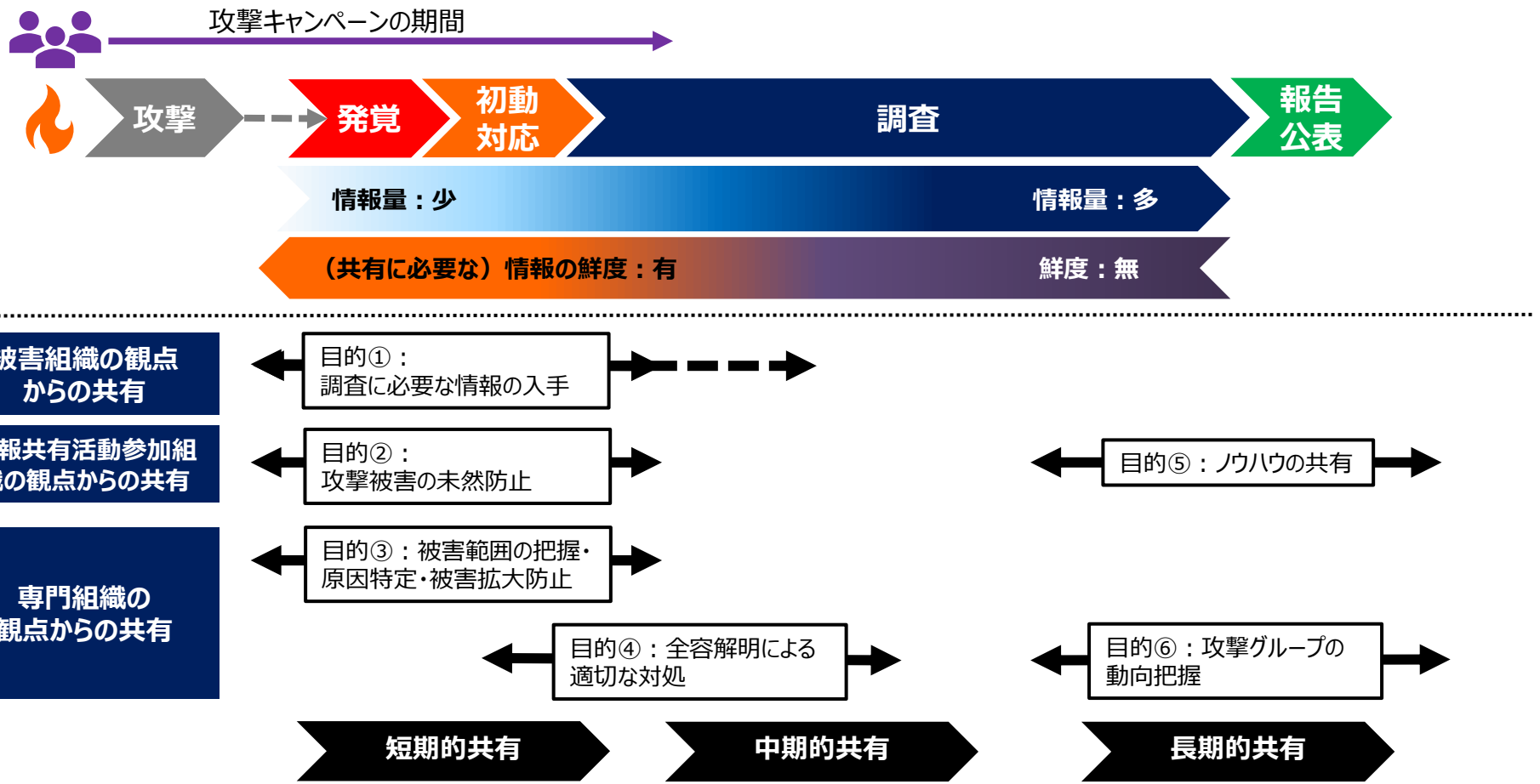
どのタイミングで？（サイバー攻撃への対処の時系列を意識）

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）

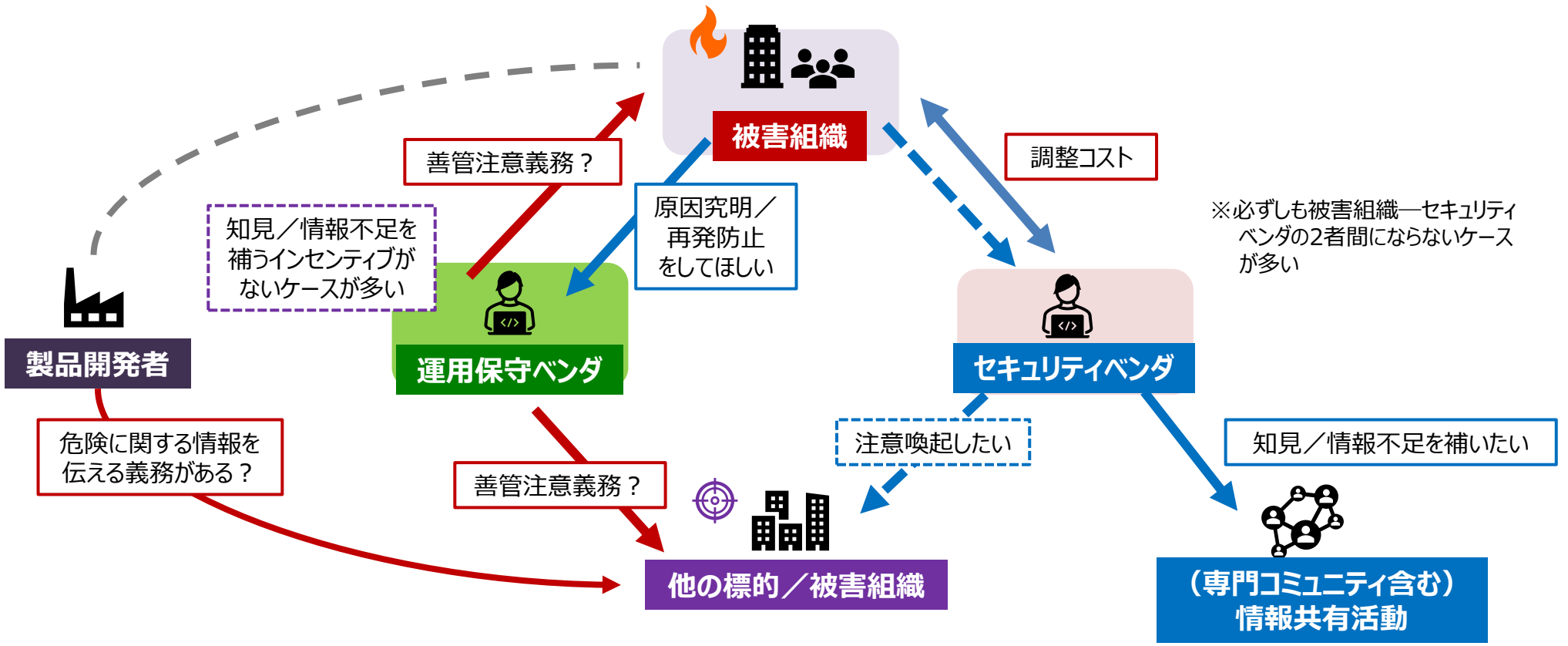
サイバー被害に係る情報共有の目的

- 情報共有については、短期的には①一つの機関だけでは情報量が少ない間に、②情報の鮮度がある早期に行うことで効果を最大化することが可能になるが、中期的、長期的な共有も重要であり、いつ、どのような情報を共有するかが重要である。
- 情報共有の実施により、①被害組織の観点からは原因究明調査に必要な情報の入手【短期】、②情報共有活動参加組織の観点からは攻撃被害の未然防止【短期】やノウハウの共有【長期】、③専門組織の観点からは被害範囲の把握・原因特定・被害拡大防止【短期】、全容解明による適切な対処【中期】、攻撃グループの動向把握【長期】といったことが可能になる。



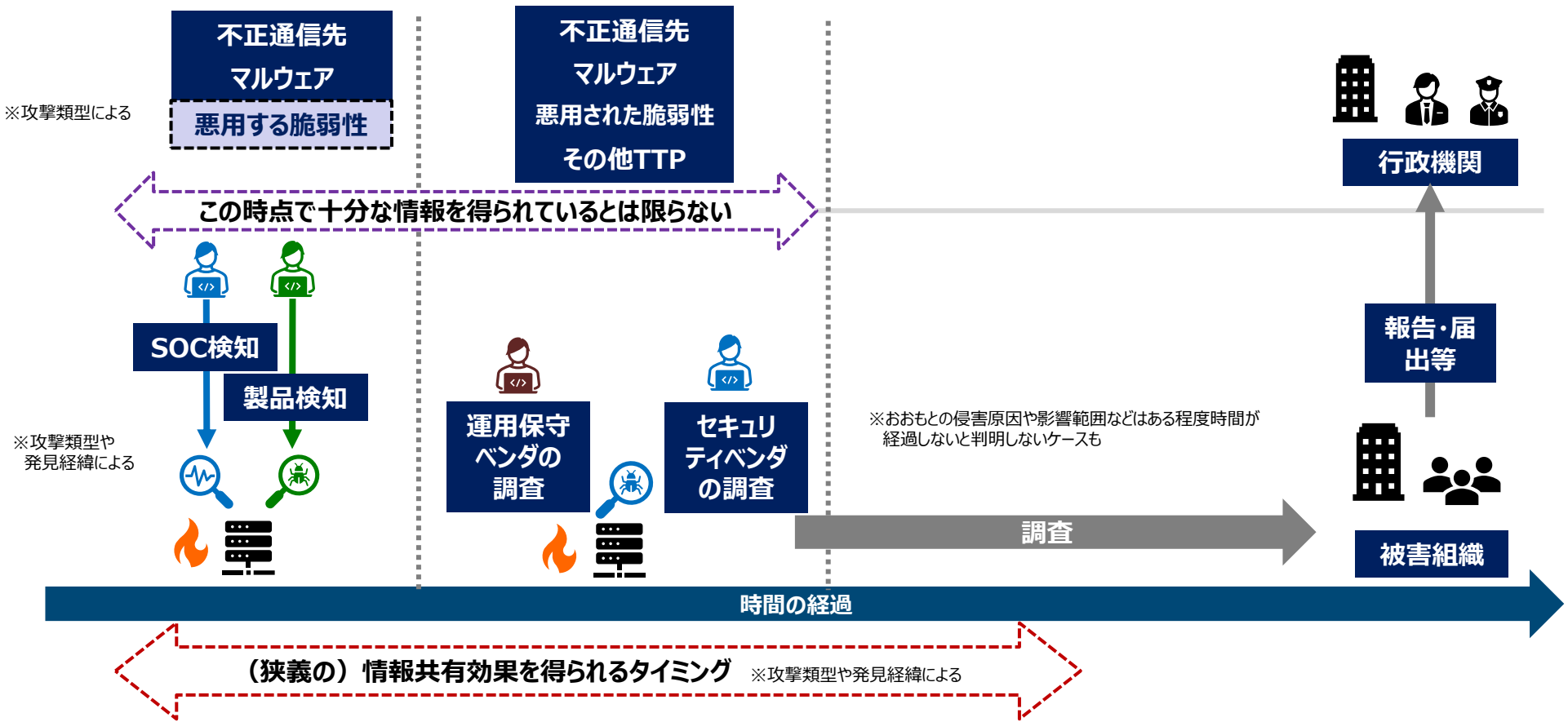
サイバー被害を受けた被害組織と被害対応を支援する組織の関係

- ユーザー企業で使用する情報システムについては、運用保守ベンダorセキュリティベンダにセキュリティ監視（SOC：Security Operation Center）を委託し、事案発生時にはセキュリティベンダと部分的にフォレンジック等のインシデント対応を委託するケースが一般的になっている。
- サイバー攻撃の被害の最小化・拡大防止のためには速やかかつ効果的な情報共有が重要であるが、被害組織に加えて、対応を支援する、①機器等の製品開発者、②運用保守ベンダ、③セキュリティベンダの役割についても検討を行うことが必要ではないか。



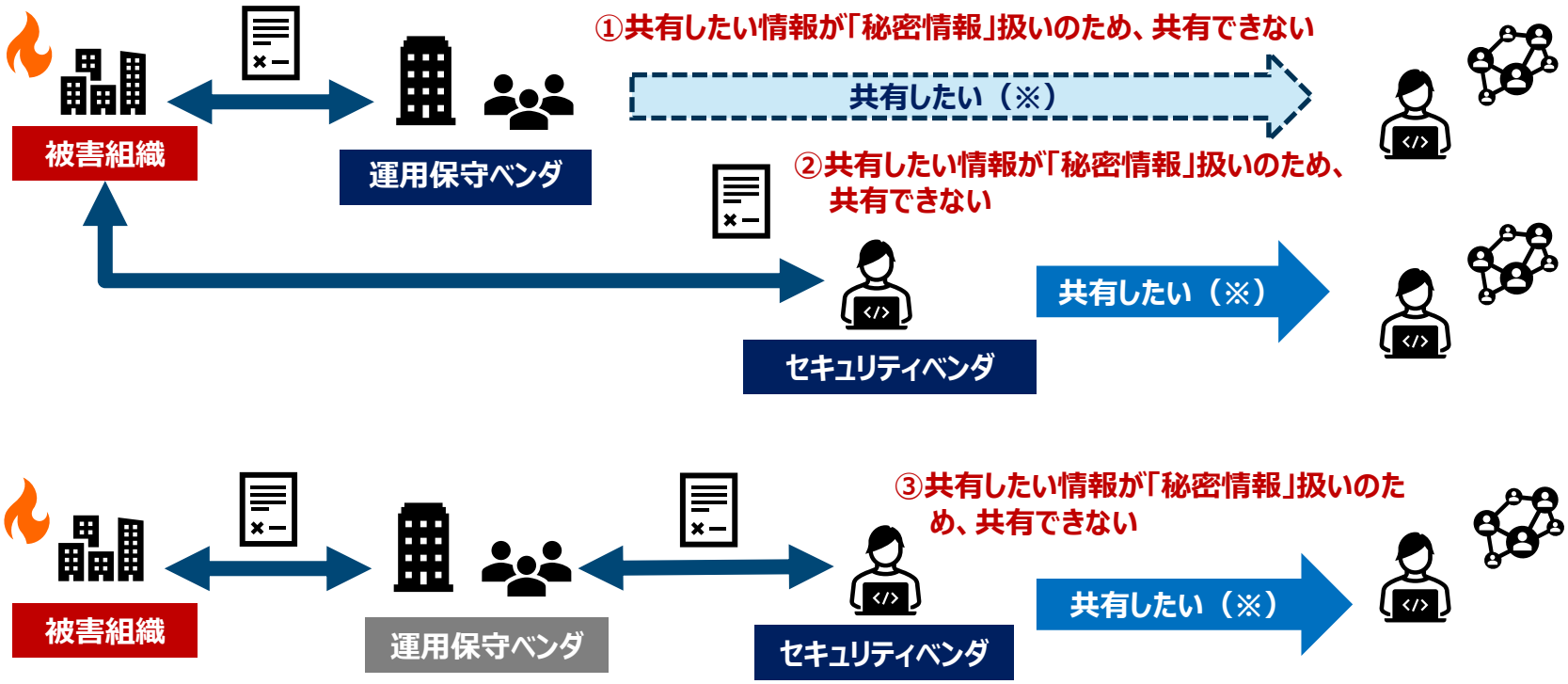
サイバー被害時には、誰が、どのような情報を把握しているか

- 攻撃類型にもよるが、被害企業では、最初に、セキュリティ監視をしている運用保守ベンダや、そこで使用されている製品の開発者において不正通信先やマルウェア等が検知される。
- 攻撃に気づかず、被害に遭った場合は、ユーザー企業側がシステムの異変に気づいた後、運用保守ベンダやセキュリティベンダがシステム分離等の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できることがある。
- 当該被害企業において、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、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することが必要であると考えられる。



NDAが情報共有の制約になると考えられるケース

- NDAが情報共有の制約になるケースとしては、①被害組織と運用保守ベンダとの契約で、運用保守ベンダが情報共有できないケース、②被害組織とセキュリティベンダとの契約で、セキュリティベンダが情報共有できないケース、③運用保守ベンダとセキュリティベンダとの契約で、セキュリティベンダが情報共有できないケースが考えられる。



（※）情報の種類や性質、企業の業態等にもよるが、共有したいと考えるベンダは一定数存在。

本検討会の検討事項（案）

１．サイバー攻撃による被害に関する情報の共有のメリット

２．サイバー攻撃による被害に関する情報の整理

- 対象とする脅威情報の種類と性質
- 被害現場で把握できる情報の種類と性質

３．被害組織を支援する専門組織における被害組織と結ぶ秘密保持契約のあり方

- 専門組織における情報の扱い
- 秘密となる情報と公知の情報の考え方
- 法令の定めによる開示要求の考え方

サイバー被害に係る情報共有ガイダンスの活用方法

- 本ガイダンスを活用することで、被害組織の担当部門が情報共有／被害公表を行うにあたっての参考とするだけでなく、情報共有／被害公表に関わる関係者間の共通理解促進のために活用することができる。