令和2年度 総務省「サイバー攻撃の被害に関する情報の望ましい外部への提供のあり方に係る調査・検討の請負」事業報告書

資料33- 3

サイバー攻撃被害情報の共有と公表のあり方について（公開版）＜概要＞

2021年3月

JPCERTコーディネーションセンター

問題意識と原因（仮説）

現状の問題

なぜサイバー攻撃被害の公表がうまくいかないのか

- 公表／報道された被害組織への批判
  - 「公表が遅いのではないか」
  - 「情報共有のために詳細な情報を公表すべき」
- “テンプレ”的な公表が目的化してしまう

相互連関

なぜサイバー攻撃情報の共有がうまくいかないのか

- 適切なタイミングで情報共有が行われない
- 公表はされても技術情報が共有されない

原因（仮説）

「どんな情報をいつ出してよいのか関係者間の共通理解がない」

情報の「特性」への理解不足

- 「社内」にしかない情報と「社外」にも存在する情報の区分について
- 外部に提供しても自社が特定されず他組織の防護に役立つ情報の性質について

※上記の問題により下記の問題を引き起こしている？

情報を組織外に出すべき「タイミング」への理解不足

- 情報共有、公表、ノウハウ共有のそれぞれの時間軸の理解不足
- 必要なタイミングを逃すと情報共有の効果がなくなることへの理解不足

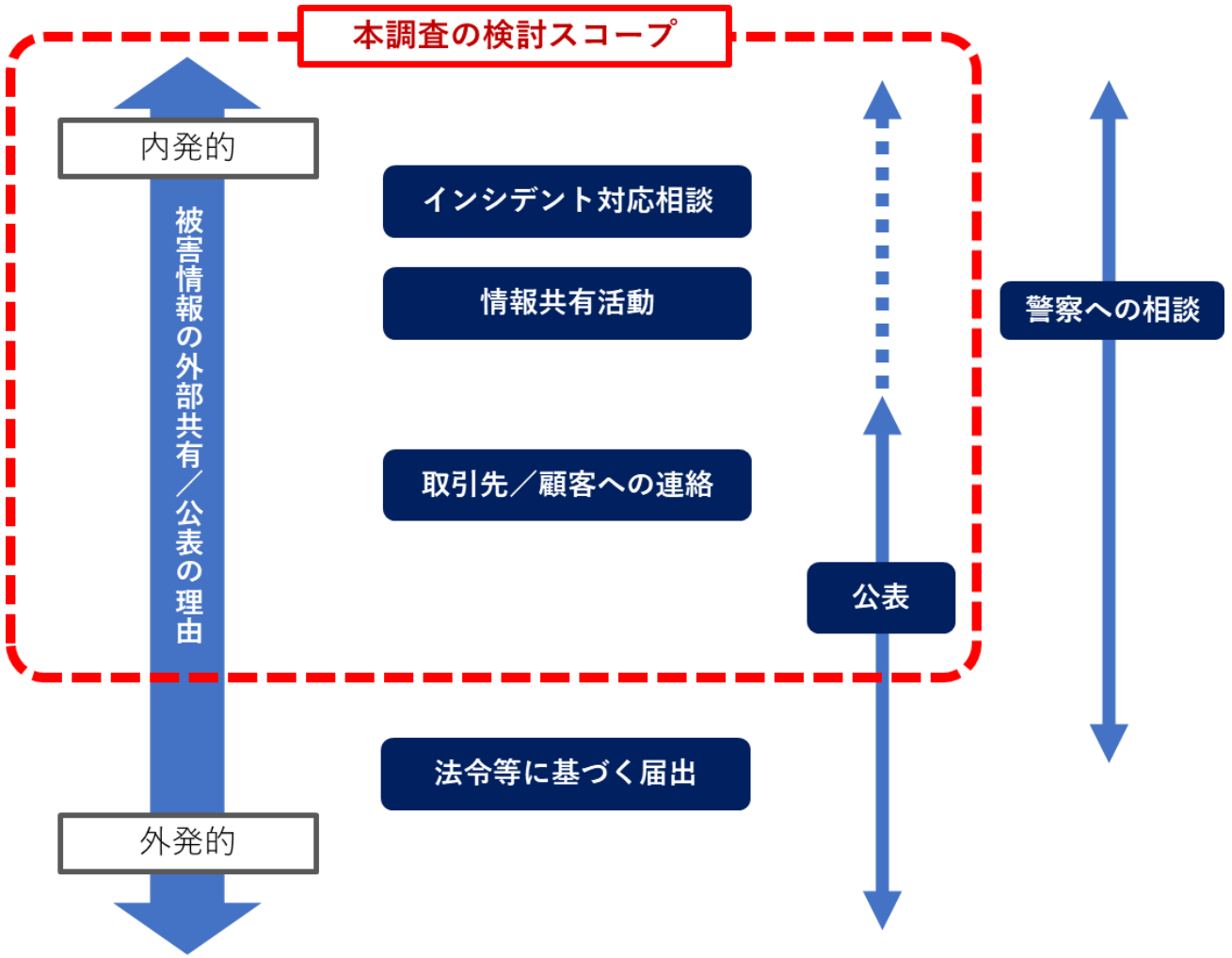
情報の出し入れを判断する部署の権限や理解度の問題

- 上記の理解を持つ部門と対外的に情報の“出し入れ”を判断・権限を持つ部門とのギャップが存在することについて

※今回は検討対象外

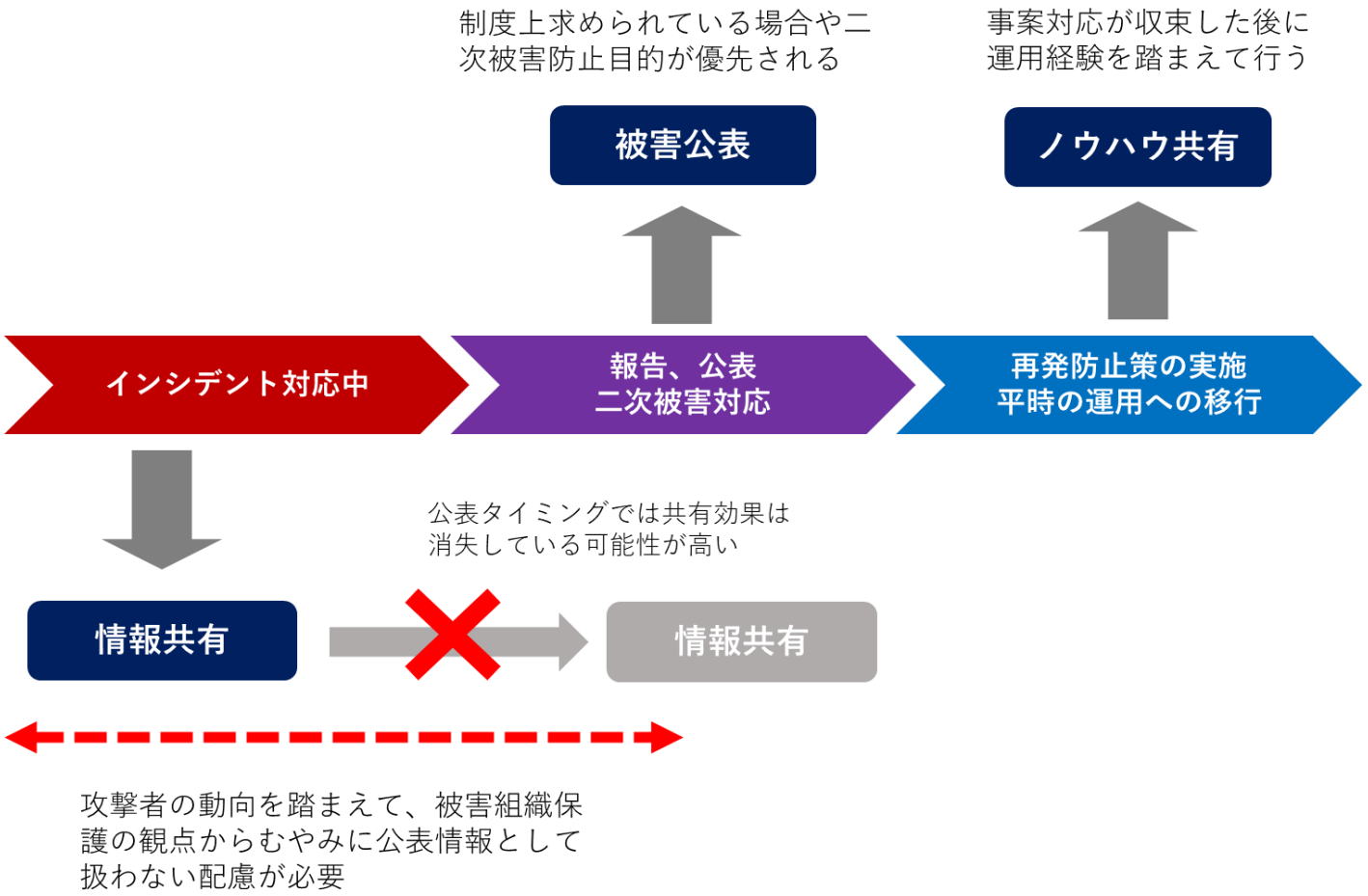
本調査・検討のスコープ

- インシデント対応フェーズを中心に検討し、企業のリスク情報開示や刑事捜査、法令等に基づく届出制度は対象外とする



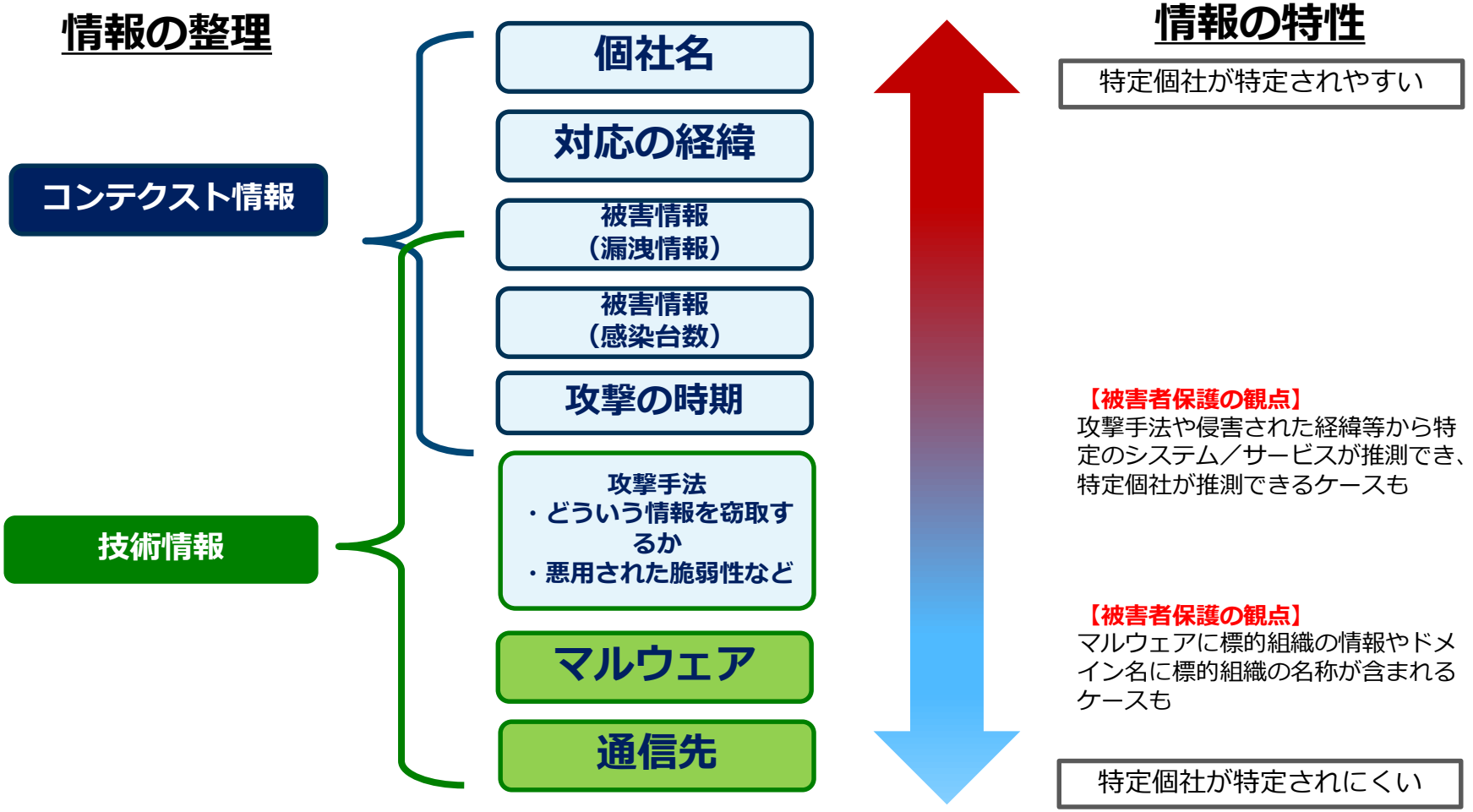
【調査のアプローチ】情報の「共有」と「公表」の分離

- 情報の「共有」と「公表」そして「（対応）ノウハウ共有」はそれぞれ目的が異なるため、適切なタイミングもいることから、それらの概念を整理／区分する



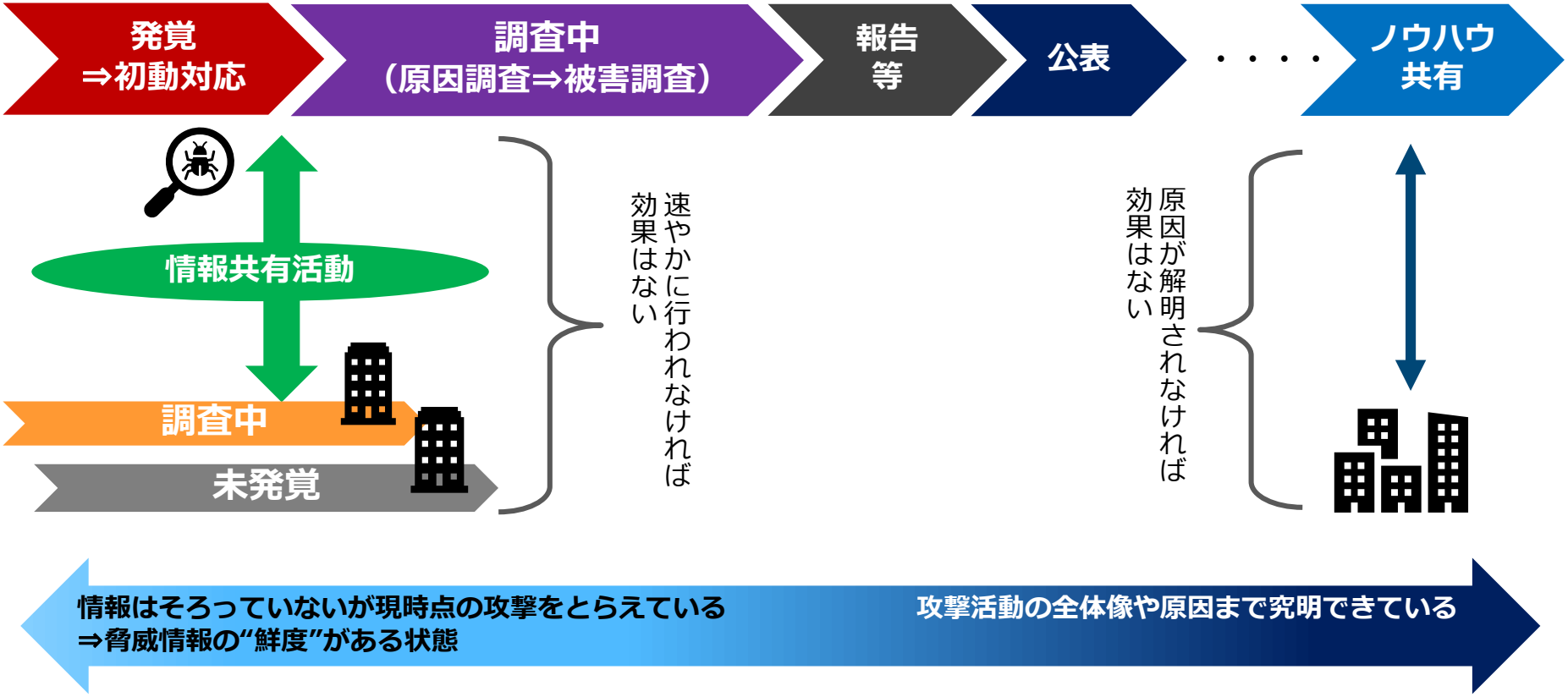
【調査のアプローチ】技術情報とコンテクスト情報の分離

- 情報の特性に応じてサイバー攻撃被害に関する情報整理し、公表前に対外提供しやすい情報とそうでない情報を区別する



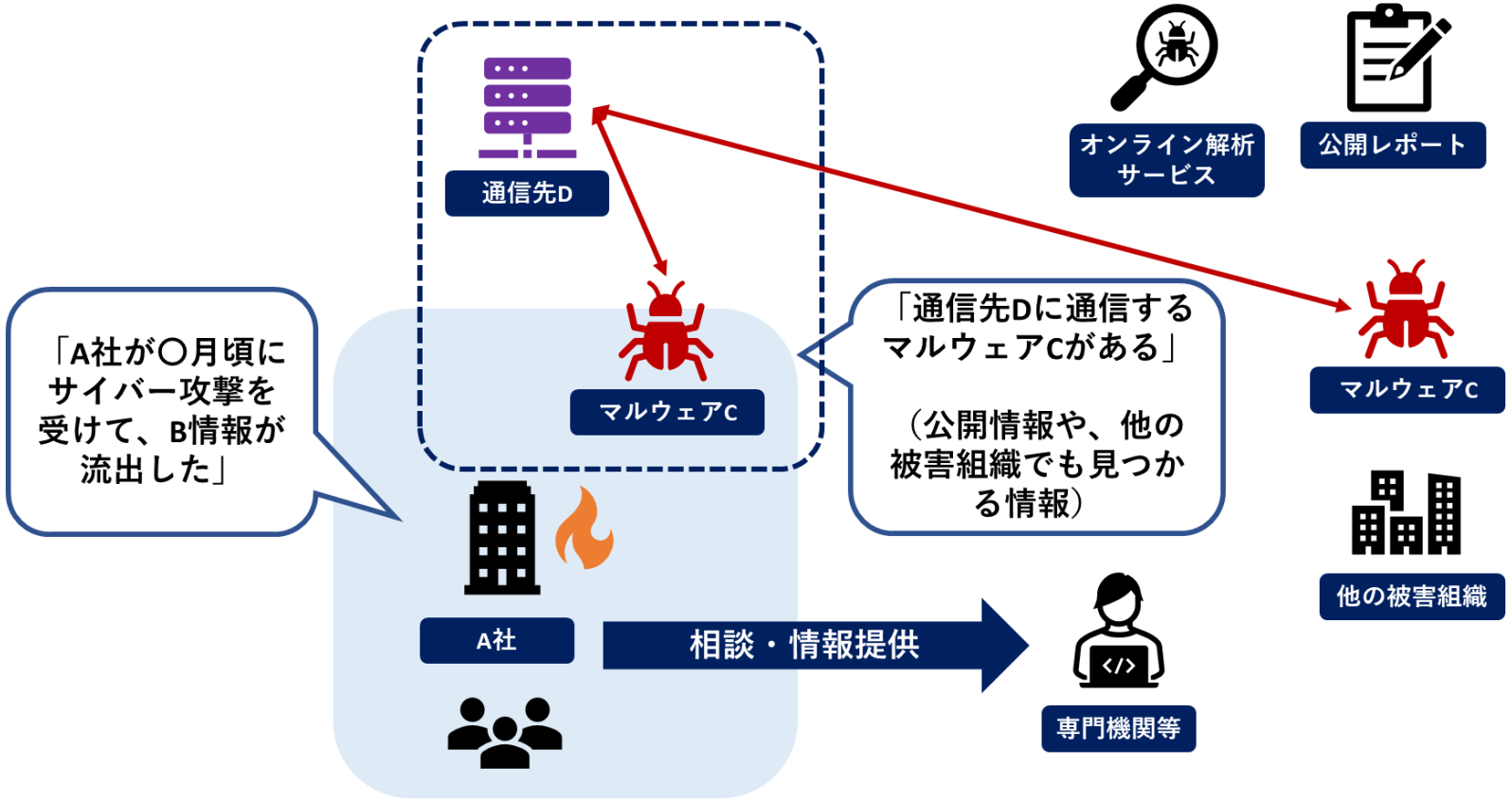
【調査のアプローチ】情報の共有から公表までのタイミング

- 原因特定や被害特定を行わなければ公表やノウハウ共有は困難
- コンテクスト情報（個社名、被害状況）ではなく、技術情報（マルウェア、通信先等）は（攻撃活動の最中に）速やかに共有されなければ効果がない
- “鮮度”を失った技術情報は（相互の）共有効果が薄くなる



【情報共有のための視点】被害者保護の観点から（分析から一部抜粋）

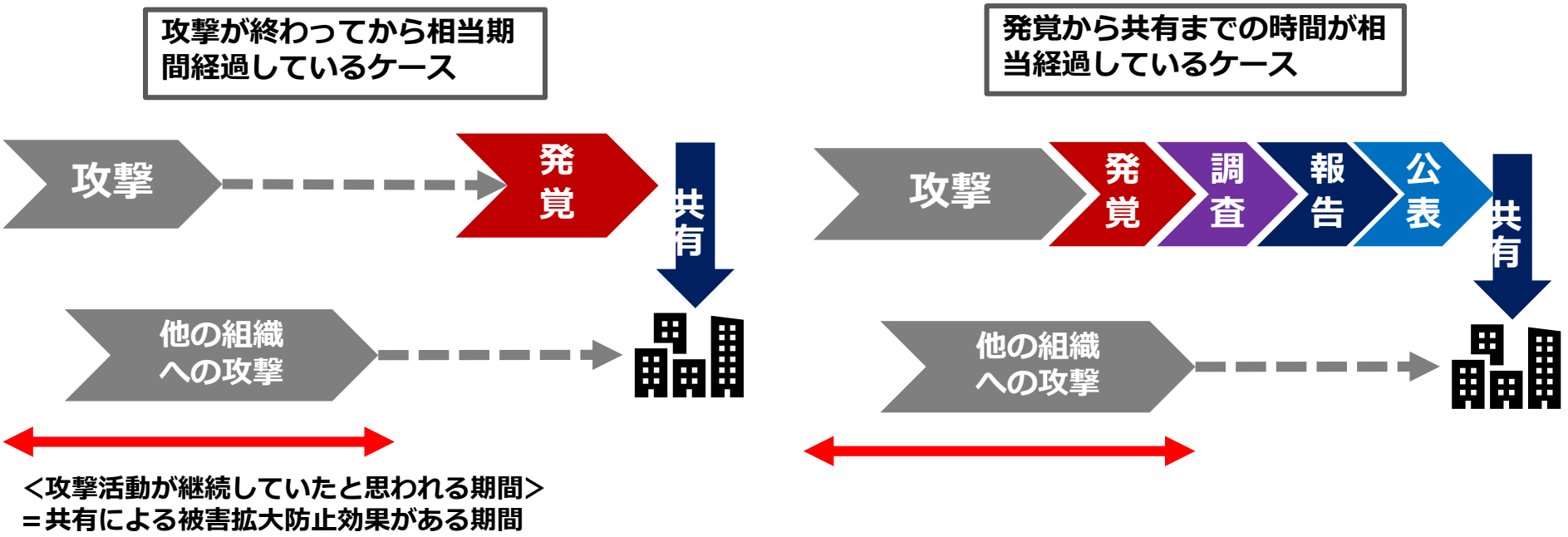
- サイバー攻撃被害に関する情報：被害組織の内部だけに存在し外部に秘匿したい自組織固有の事情を含む情報もあれば、公知になっている情報や他の被害組織でも見つかる情報もある
- その情報が技術情報かコンテクスト情報かという情報の性質や、情報を秘匿する利益と共有する利益を比較考量しつつ、外部への共有や公表を検討することが必要



【現状】情報共有がうまく行われない背景（分析から一部抜粋）

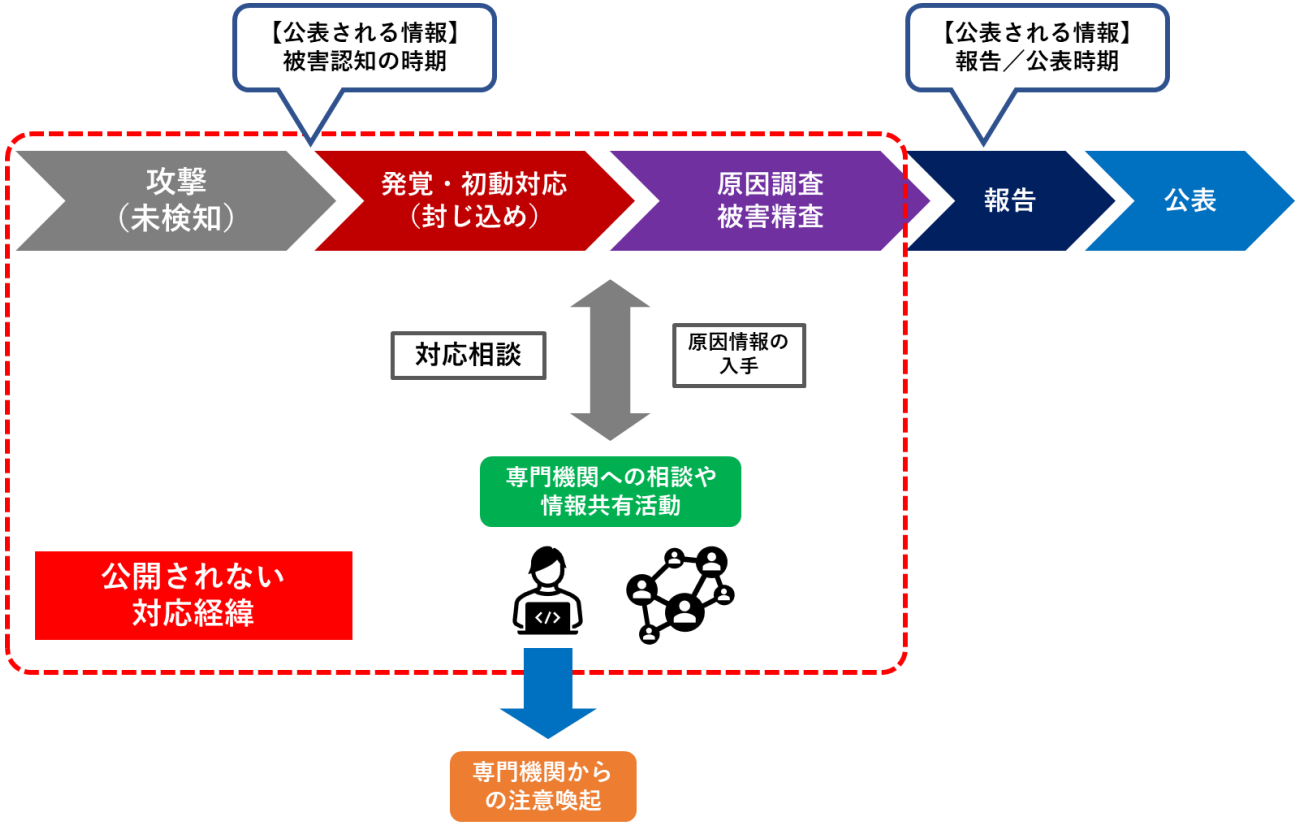
すでに攻撃から長期間経過し「共有効果」が乏しい情報が共有されている

- 理屈上は、攻撃活動全体が継続されている最中に情報が共有されることで、被害拡大防止の効果が見込めるが、実際には適切な共有タイミングよりも後に情報が共有されている。
- 情報共有タイミングが遅くなると、共有効果がないだけでなく、「過去の攻撃被害の“掘り返し”」が発生し、受信組織が調査や情報提供に対するインセンティブも失ってしまう



【現状】公表が遅くなる合理的事情（分析から一部抜粋）

- 事案の公表に至るまでの必要なプロセスが理解／評価されていないため、「公表の遅れ」ばかり指摘される
- 実際は必要な対応（専門機関への相談・情報提供等）は行っているが、利害関係者への通知や一般への公表は、情報の精査の都合上遅れがちになる



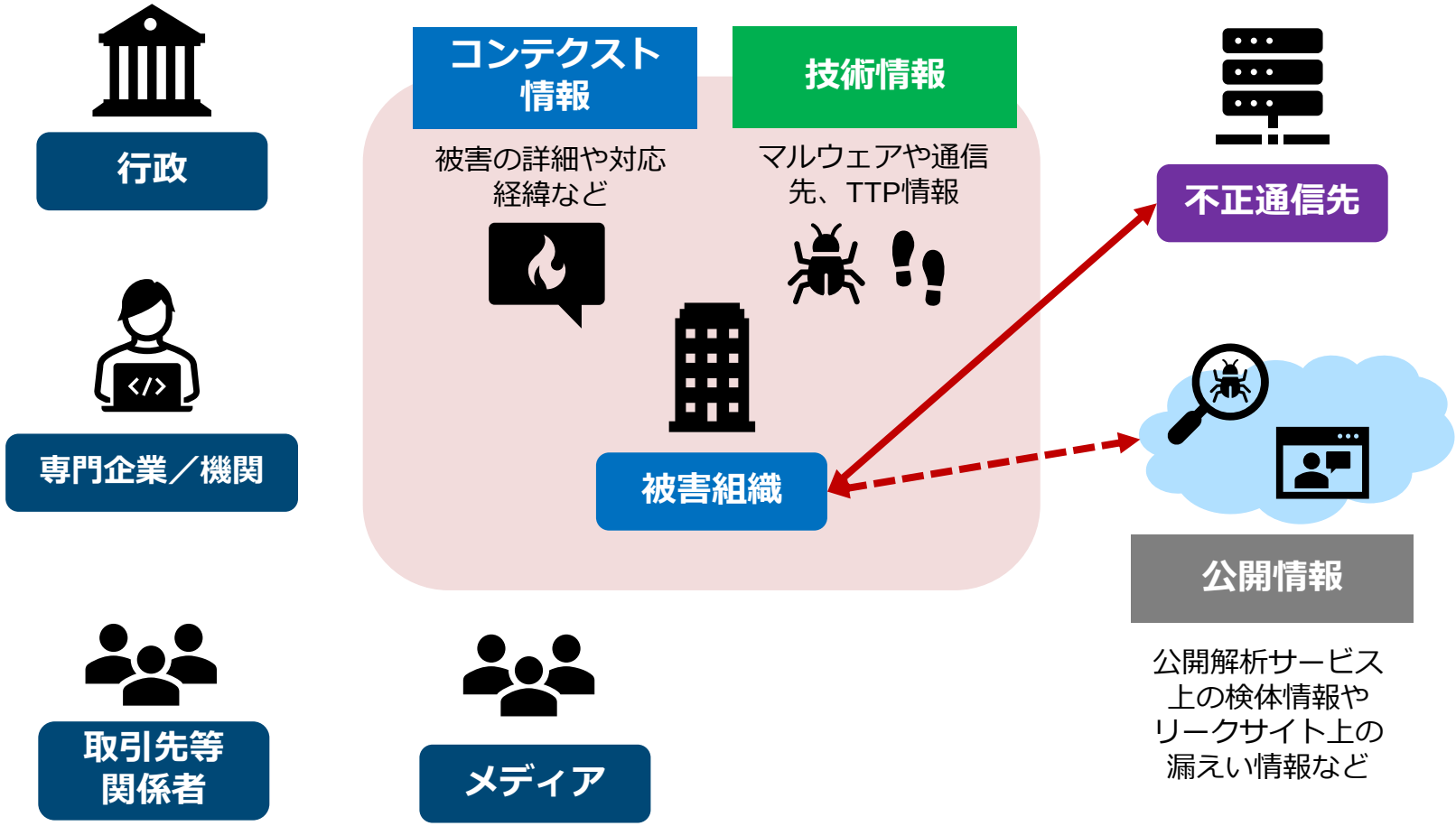
情報共有／公表時それぞれに望ましい情報の整理

■ それぞれの「タイミング」と各情報の「特性」を踏まえた有効性／注意点を整理

	情報の種類	情報共有時に望ましい情報	被害公表時に望ましい情報
コンテクスト情報  技術情報	対応の経緯	△ 特段の事情がない限り不要 ただし、早期の検知のために必要な情報であれば有効	◎ （公表前の）情報共有活動や専門機関等への相談など、公表までの時間で適切な対応が行われていたことを説明
	被害内容	× 特段の事情がない限り不要	○ ※詳細は取引先等関係者への報告が優先 ※その他法令等で定められている場合は必須
	攻撃時期	◎	○
	攻撃手法（TTP）	◎	○ 対策とのセットで示されればノウハウ共有としての効果はある
	攻撃手法（悪用された脆弱性や踏み台となったサービス）	◎ ※未修正の脆弱性の場合は脆弱性告示制度等での対応が優先	△ すでに攻撃活動が終了して一定期間が経過している場合、公表による効果は特にない
	マルウェア通信先（IoC）	◎ ※被害組織を示す情報の有無の確認が必要	△ すでに攻撃活動が終了して一定期間が経過している場合、公表による効果は特にない

【考察】ガイドラインの必要性

- 被害組織向けだけでなく、攻撃対応に関わる主要な関係者が、被害組織の保護や攻撃被害の拡大防止をすすめ、社会全体で攻撃に対抗するために、「被害情報」の取り扱いにおいて何を配慮すべきか示すガイドラインが必要ではないか



お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター（広報）

- **Email：pr@jpcert.or.jp**
- **https://www.jpcert.or.jp/**

インシデント報告

- **Email：info@jpcert.or.jp**
- **https://www.jpcert.or.jp/form/**

制御システムインシデントの報告

- **Email：icsr-ir@jpcert.or.jp**
- **https://www.jpcert.or.jp/ics/ics-form.html**

※資料に記載の社名、製品名は各社の商標または登録商標です。