資料29－３

# サイバー攻撃被害情報の共有と公表のあり方について

2021年3月9日

JPCERTコーディネーションセンター

# 現在実施中の委託調査について

- 総務省委託調査「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」にて、これまでのインシデント対応知見を踏まえた考察や有識者ヒアリングなどを踏まえた提案を報告予定。
- 各情報の「特性の整理」と共有・公表の望ましい「タイミング」の考察を踏まえて、積極的な情報共有（情報提供）を目指しつつ、被害組織保護の観点が盛り込まれたチェックリスト（案）などの提案を予定。
- 各組織のルール・体制整備や、情報共有活動、ガイドライン策定などで活用いただくことを想定

**初動対応** → **情報共有** → **公表準備** → **公表**

**情報共有・公表タイミングの解説**

被害にあった組織が目安とするもの

**情報共有時のチェックリスト**

積極的な情報提供を前提としつつ、被害組織保護の注意点をまとめたチェックリスト

**公表準備時のチェックリスト**

対外応答の観点も踏まえた準備時の確認リスト

# 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わからない（知らない）」**

**情報の「特性」への理解不足**

- 「社内」情報と「社外」にも存在する情報の区分について
- 外部提供しても自社が特定されない情報の性質について

※上記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**

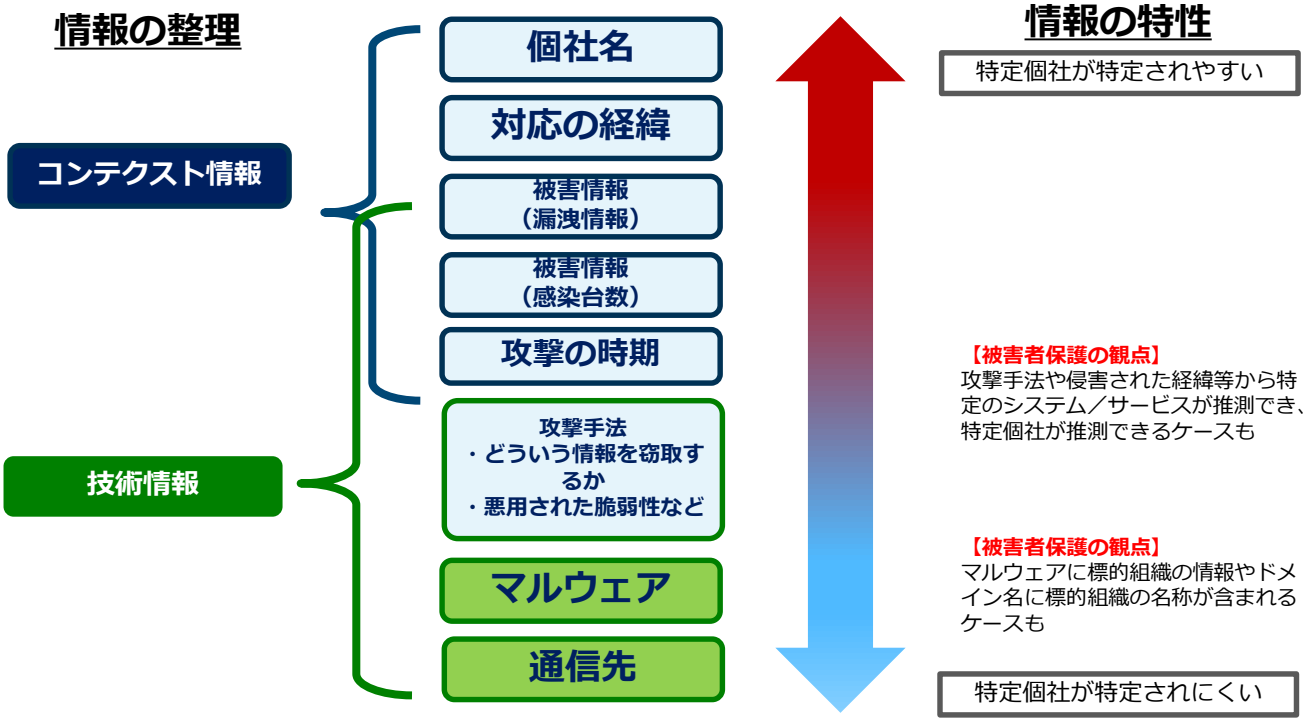
- 情報共有、公表、ノウハウ共有のそれぞれの時間軸の理解不足
- 必要なタイミングを逃すと情報共有の効果がなくなることへの理解不足

**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

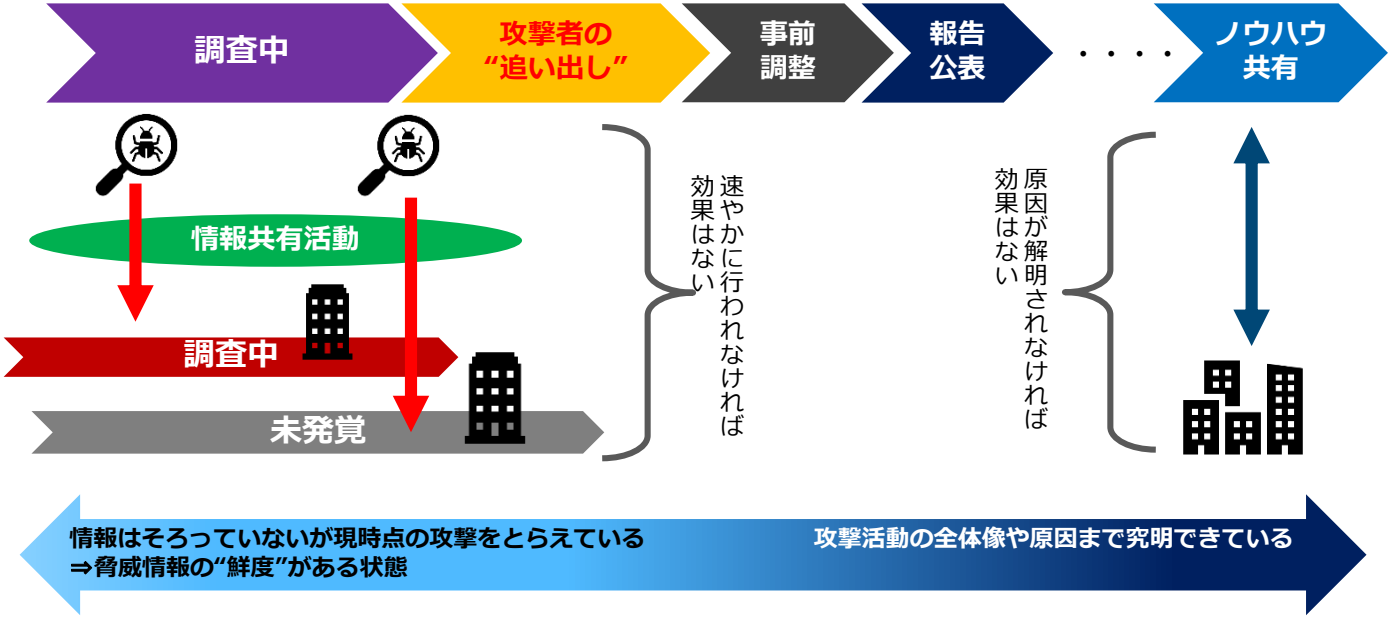
# 【概念の整理①】コンテクスト情報と技術情報

- サイバー攻撃被害情報を要素分解すると、被害組織外にも存在する情報か、被害個社が一意に特定されうる情報か、その特性が整理できる



# 【概念の整理②】情報の共有・公表・ノウハウ共有の時系列

- おおよその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／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<br>  <br>技術情報 | 対応の経緯 | △<br>特段の事情がない限り不要<br>ただし検知に資する情報であれば有効 | ◎<br>（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の説明 |
| | 被害内容 | ×<br>特段の事情がない限り不要 | ○<br>※詳細は取引先等関係者への報告が優先<br>※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） | ◎ | ○<br>対応策とのセットであればノウハウ共有に効果がある |
| | 攻撃手法（悪用された脆弱性や踏み台となったサービス） | ◎<br>※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<br>※被害者情報が特定されうる可能性への配慮が必要 | △<br>既に攻撃活動が終了して一定期間が経っている場合、効果は低い |
| | マルウェア通信先（IoC） | ◎<br>※被害組織を示す情報の有無の確認が必要 | △<br>既に攻撃活動が終了して一定期間が経っている場合、効果は低い |

# 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。