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のスコープ及びスケジュール

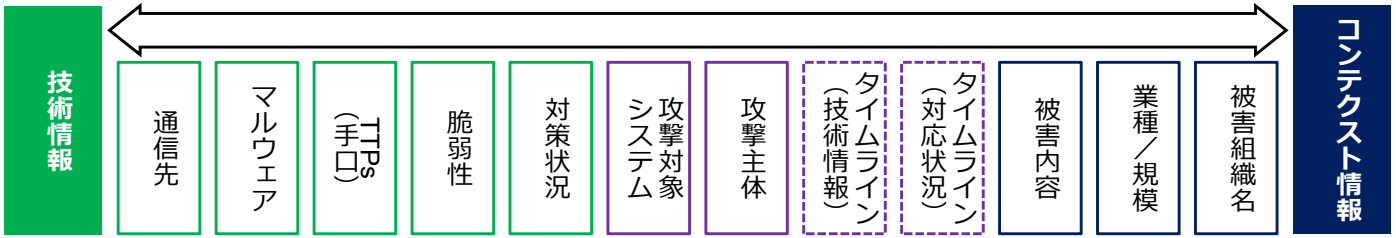
事務局

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）

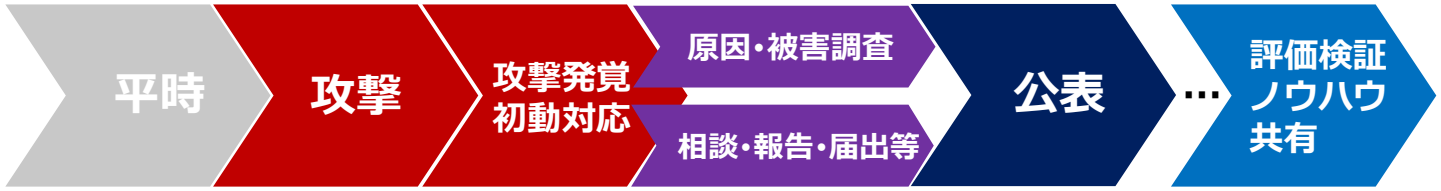
■ サイバー攻撃被害を受けた組織がサイバーセキュリティ関係組織（例: NISC、警察、所管省庁、JPCERT、ISACなど）と被害に係る情報を共有することは、被害組織自身にとっても社会全体にとっても有益。一方、被害組織においては、どのような情報を、どのタイミングで、どのような主体と共有すべきかについて、必ずしも十分な理解が進んでいない。

■ 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

今後のスケジュールについて（案）

■ **第1回（５月３０日（月））**
- ○ 座長の互選、手続の決定
- ○ 論点提示①
  - • サイバー攻撃への対処の観点からの論点提示
- ○ 議論

■ **第2回（６月２０日（月））**
- ○ 論点提示②
  - • サイバー攻撃への対処の観点からの論点提示（前回の議論が残っている場合）
  - • サイバーセキュリティ関連法令・制度の観点からの説明
  - • 行政活動／警察活動の観点の説明
- ○ 議論

（以下は想定。第2回までの議論を踏まえ、必要に応じて、論点に係る議論を継続。）

■ **第3回（７月）**
- ○ ガイダンス骨子案提示
- ○ 議論

■ **第4回（秋頃）**
- ○ ガイダンス原案提示
- ○ 議論

■ **年内**
- ○ ガイダンス案のセット・公表

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