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。