資料３

官民連携の強化に向け
今後具体化が必要な論点

令和７年10月
内閣府政策統括官（サイバー安全保障担当）

今後具体化が必要な論点（1／2）

特定重要電子計算機の届出やインシデント報告の施行、新協議会の立ち上げに向けては、運用面/技術面で更なる深掘りが必要。この点、基本方針（案）の記載を踏まえ、今後以下のような論点につき、ステークホルダとも意見交換を行いつつ具体化を進める。

1. 特定重要電子計算機の考え方について

- 法第4条における届出や第5条におけるインシデント報告の対象となる特定重要電子計算機について、具体的にどのような機器を対象とすべきか。例えば、近年その脆弱性の悪用事例が多く確認されているVPN装置等のインターネットから直接接続可能な機器（アタックサーフェス）や、その他にどのような類型が必要か。
- 実際のシステム構成において、インターネットから接続可能な領域と、いわゆる制御系システムを物理的に分離（エアギャップ）している例が見られるが、このような場合の特定重要電子計算機の考え方。
- また近年、基幹インフラ事業者においても、その役務提供に当たってクラウドサービスが広く活用されているところ、特定重要電子計算機としてクラウドサービスを利用している場合に、どのように捉えるべきか。

2. 特定重要電子計算機の届出について

- 脆弱性の提供等における活用に当たって、具体的にどのような事項、粒度で届出を求めるべきか。
- 経済安全保障推進法における特定重要設備の全部又は大部分がクラウドサービスを活用している場合に、届出の対象をどのように考えるべきか。また、ゼロトラストのように、システムの機能保障上重要な機能がクラウドサービスを活用している場合はどうか。
- 大多数の事業者が通常利用していると考えられ、必ずしもその保有状況を把握せずとも、情報提供を行い得るようなソフトウェアについても届出を求めるか。
- 経済安全保障推進法の規定に基づく届出が必要な設備について、事業者の負担軽減の観点から、当該届出の内容と本法で届出を求める内容について整理してはどうか。

今後具体化が必要な論点（2／2）

3. インシデント報告について

- 法第5条において、「特定侵害事象の原因となり得る事象」についても報告を求めるとしているところ、例えば、具体的な事象の痕跡を認知した場合に報告を求めるといった対応としてはどうか。
- 報告期限について、インシデント発生時の事業者の対応負担も鑑み、例えば個人情報保護法といった関係法令における報告期限を参考に設定すべきか。
- 特定重要電子計算機がクラウドサービスを利用している場合、SaaS，PaaS，IaaSそれぞれの責任範囲に基づき、どの利用形態の場合にどのタイミングで報告を求めるか。

4. 新協議会について

- 協議会の組織及び運営に関し必要な事項は、協議会が定める（法第45条第8項）とされているが、今後、基本方針（案）の内容を踏まえて協議会の組織及び運営の具体化を図る上で、特に留意や配慮が必要な事項はあるか。
- 協議会の構成員は、政府から情報提供を受けることができる一方で、協議会で知り得た秘密を含む情報の適正な管理や資料の提出の求めがあった場合における対応が必要となるなど、一定の負担も生じ得る。構成員の協議会への参画意欲を高め、協議会が官民連携のエコシステムとして効果的に機能するために、運用面での工夫やルール整備等を行う上で、どのような事項を考慮すべきか。
- 基本方針（案）では、協議会の構成員以外の者に対しても、秘密を含まない情報の提供を行うことで、広く国内のサイバーセキュリティ強化を促し、重要電子計算機に対する特定不正行為による被害防止につなげていくとしている。協議会の活動において、どのように取り組むべきか。