「重要電子計算機に対する不正な行為による被害の防止の報告等に関する様式案（案）」に対する意見案

2026年8月7日

一般社団法人　日本貿易会
情報システム委員会

内閣府政策統括官（サイバー安全保障担当）が2026年7月13日、「重要電子計算機に対する不正な行為による被害の防止の報告等に関する様式案（案）」に関するパブリックコメントを募集したことを受け、商社自体は「特別社会基盤事業者」に該当しないが、商社も事業者へ重要設備を納入する中間業者（サプライヤー）として介在し、事前審査や届出の対象となり影響が想定されることから、情報システム委員会は2026年8月7日付で意見を提出した。

	意見内容	理由
1	本様式案の方向性に賛成します。DDoS攻撃、ランサムウェア、その他サイバー攻撃等について共通様式を用い、又は別途法令等で定める様式に添付する形で報告できる取扱いは、被害組織の報告負担軽減と政府側の対応迅速化に資するため、制度化を進めるべきです。	申合せ案では、報告先となる官公署が多いこと等により被害組織に過度な報告負担がかかっているとした上で、報告先や様式の一元化、簡素化を進める趣旨が示されています。また、告示案・概要では、DDoS攻撃事案、ランサムウェア事案、その他事案の区分ごとに関係省庁申合せ別添様式1～3を用いることが示されています。
2	具体的な提出先、提出方法、追加的な報告事項の有無について、施行前に、事業者が実務で参照できる一覧表、Q&A又はフローチャートとして公表いただきたいです。特に、複数の法令・ガイドライン、警察相談、所管省庁への報告等が重なる場合に、共通様式を提出した後の別途報告の要否、提出先の優先順位、同一内容の再提出が不要となる範囲を明確にしていただきたいです。	様式案では、具体的な提出先や提出方法、追加的な報告事項の有無は、各法令、ガイドライン、各省庁が公表する方法に従うものとされています。この記載のままでは、平時の準備やインシデント初動時に、どの窓口へ、どの様式で、どの範囲まで報告すべきかを事業者側で判断しにくく、結果として重複報告や報告遅延につながる懸念があります。
3	速報提出時の記載負担を抑えるため、各様式について「必須項目」「任意項目」「不明又は調査中でも差し支えない項目」を記載要領上で明示いただきたいです。また、IPアドレス、ログ情報、IoC、システム構成図、フォレンジック結果等を別ファイルで提出する場合のファイル形式、容量、暗号化・送付方法も明確にしていただきたいです。	様式案では「報告をしようとする時点で把握している範囲」で記載すること、ランサムウェア及びその他サイバー攻撃等の技術情報については不明箇所は空白でよいこと、IPアドレスやログ情報など記載内容が多数になる場合は別ファイルで提出することが示されています。一方、速やかな初動対応中は未確定情報が多いため、運用上の許容範囲を明示することで、報告品質の確保と初動対応への支障回避を両立できます。
4	報告内容の内閣官房国家サイバー統括室等への共有、匿名化された注意喚起等への活用、及び「共有等を希望しない」場合の取扱いについて、営業秘密、技術情報、個人情報、取引先情報が含まれる場合の保護措置と共有範囲を具体化いただきたいです。特に、法令に基づき共有される場合と、任意報告・同意に基づく共有の場合の違いを明確にしていただきたいです。	様式案では、報告内容が報告先機関から内閣官房国家サイバー統括室に共有され、被害者が分からないようにした上で注意喚起等に活用される旨が記載されています。また、共有等を希望しない場合でも、重要電子計算機に対する不正な行為による被害の防止に関する法律第5条に基づく報告や重要インフラのサイバーセキュリティに係る行動計画に基づき、共有されることがある旨も示されています。提出側が安心して正確な情報を出せるよう、共有範囲と保護措置の明確化が必要です。