「重要インフラ統一基準（案）」に対する意見案

2026年5月14日

一般社団法人　日本貿易会
情報システム委員会

内閣官房国家サイバー統括室が2026年4月21日、「重要インフラ統一基準（案）」に関するパブリックコメントを募集したことを受け、商社自体は重要インフラ事業者に該当しないが、サプライヤーや外部委託先としての影響が想定されることから、情報システム委員会は2026年5月14日付で意見を提出した。

	意見内容	理由
1	本統一基準（案）は、重要インフラ事業者を主対象としているが、第3部においては「サプライチェーンに関わる事業者等」にも対応を求める構成となっている。 一方で、サプライヤーや外部委託先となる非重要インフラ事業者（例：商社、ITサービス提供事業者等）に求められる対応水準・責任範囲が必ずしも明確ではなく、結果として契約実務や対応コストの解釈にばらつきが生じる懸念がある。 欧米（EU NIS2 指令、米国 NIST SP800-53/CSF 等）では、重要事業者とサプライヤーの責任分界点や最低限求めるセキュリティ要件が明示されている事例が多い。 これを踏まえ、日本においても、安全基準等策定ガイドライン等において、 重要インフラ事業者 直接関与する主要サプライヤー 一般的な委託・調達先 といった区分ごとに、「最低限求められるセキュリティ対策の水準」や「契約で求めるべき主な要求事項（例：事故報告、脆弱性対応、監査協力）」を整理・明示することを検討いただきたい。	本統一基準（案）では、サプライチェーン・リスクマネジメントの重要性が明確に位置付けられており（第3部3.2.9等）、方向性としては国際的なベストプラクティスと整合している。 しかしながら、実務の現場では、重要インフラ事業者からサプライヤーへ要求される対応が過度に拡大解釈される可能性があり、特に中堅・中小事業者にとっては過剰な負担となる懸念がある。 EUのNIS2指令や米国NISTフレームワークでは、リスクベースの考え方を前提としつつも、責任主体の整理や要求事項の例示が行われており、契約実務における一定の予見可能性が確保されている。 日本においても、サプライチェーン全体の底上げを図りつつ、過度な萎縮や形式的対応を防ぐ観点から、事業者区分に応じた要求水準の整理・明確化が不可欠と考える。
2	【適用範囲】 複数事業を有する企業においては、事業ごとにIT・運用体制が異なる実態もあるため、統一基準の適用範囲について、事業単位・会社単位・グループ単位といった整理の考え方を明確に示していただきたい。 また、分野や事業特性を踏まえたリスクベースでの適用範囲の考え方についても、参考となる整理や例示があると、実務上の判断に役立つものと考える。	複数の事業領域を有する企業では、対象とするインフラ性やリスクの大きさが事業ごとに異なる場面がある。 例えば、エネルギー供給に関わるシステムと、一般的な商取引に係るシステムでは、求められるセキュリティ対応の優先度や水準の考え方が異なるケースがある。 このため、適用範囲の考え方が一定程度示されることで、各社における実務上の判断が行いやすくなると考える。 【統一基準（案）記載箇所】第1部1.2、第2部2.1.1（2）
3	【委託先設備の責任範囲】 委託先設備を活用する事業形態においては、自社で直接管理できない領域も生じるため、委託先管理に関して求められる対応範囲（契約、確認、努力義務等）の考え方について、一定の整理が示されるとよいと考える。 あわせて、供給者・委託先に対する基本的な対応水準や考え方についても、参考となる指針があると実務上有用と考える。	商社機能を有する企業では、自社設備に加え、取引先や委託先の設備・サービスを前提とした事業運営を行う場面がある。 例えば、物流や外部サービスの利用など、直接的な管理が及ばない領域も含まれるため、どの範囲まで対応すべきか判断が難しいケースも想定される。 このような点について一定の考え方が示されることで、各社における対応のばらつきを抑えることや、過度な対応負担の回避につながると考える。 【統一基準（案）記載箇所】第3部3.2.1②、第3部3.2.9③
4	【中小取引先への段階的対応】 サプライチェーン全体のセキュリティ確保にあたっては、中小規模の取引先を含めた実務負担にも一定の配慮が必要と考えられるため、規模やリスクに応じた段階的な対応の考え方について整理が示されると実務上有益と考える。 一律に同水準の対応を求めるのではなく、成熟度や影響度に応じた柔軟な考え方が整理されることが重要と考える。	当社の取引先には多様な規模・業態の事業者が含まれており、取引内容や重要性も一様ではない。 例えば、限定的な取引においても一律に高水準の対応を求める場合、取引先側の負担が大きくなることが考えられる。 このため、取引の重要性や影響度に応じた段階的な対応の考え方が示されることで、サプライチェーン全体として無理のない形でのセキュリティ確保につながると考える。 【統一基準（案）記載箇所】第3部3.2.9
5	【改定時の経過措置】 重要インフラに関連する設備は長期利用を前提とするものが多いため、基準改定時における既存設備への適用について、経過措置や優先順位の考え方が示されると実務上有益と考える。 また、新設設備と既存設備の取扱いの違いや、更新計画に応じた段階的対応の考え方についても整理が示されることで、実務上の判断に資するものと考える。	当社が関与するエネルギー関連設備や物流設備などは、長期間にわたり運用されるものが多く、短期間での全面的な対応が難しい場合がある。 例えば、供給設備や制御システムについては、更新サイクルや安全性の観点から一度に更新することが難しいケースもある。 このため、基準改定時における既存設備への適用の考え方が示されることで、現場での計画的な対応が進めやすくなると考える。 【統一基準（案）記載箇所】第1部1.5
6	クラウドサービスや外部委託先へデータを預ける際の確認事項として、ISMS等の国際規格認証の取得状況、SOC2等の監査レポート、ISMAP等の公的評価制度等、第三者性のある認証・監査・評価を活用することを明記してはどうか。	統一基準案においては、3.2.9節「サプライチェーン・リスクマネジメント」における「対策の状況の把握を行う」や、3.4.7節「クラウドサービス利用時の対策」における「仕様を確認し理解を深める」といった記載が、いずれも抽象的な表現にとどまっている。しかし、各事業者が自らサービス提供者の内部的な仕組みまで監査することは、現実的には困難である。 このため、客観的な第三者認証や監査レポートの活用を統一基準案の中で明示的に位置づけることで、各省庁が策定する基準の粒度を揃えるとともに、その実効性を高めることができるのではないかと考える。
7	バックアップデータの保護に関して、「バックアップ元と異なるセグメントやオフラインで保管する」ことに加え、「バックアップ取得用の通信を一方向のみに制限する」「世代管理を行う」など、より踏み込んだネットワーク分離やデータの不変性（イミュータビリティ）の確保を要件として明記するのはどうか。	統一基準案の3.4.3.3節「バックアップ」では、「バックアップデータをバックアップ元のシステムと異なるセグメントやオフラインで保管する等の対応を検討する」と記載されている。一方、近年のランサムウェア攻撃では、取得済みバックアップが狙われたり、バックアップ管理システムの脆弱性が悪用されたりする被害が報告されている。 この状況を踏まえると、現行の記載事項に加え、被害を未然に防ぐ予防的統制として「バックアップ環境への通信制限」や「バックアップシステム自体への継続的なセキュリティ対策（パッチ適用など）」を明記することが望ましい。さらに、確実な復旧のための是正的統制として「常時複数世代分のバックアップの保管」や「バックアップデータの改ざん防止（不変性の確保）」についても併記すべきと考える。