「サイバーセキュリティ戦略（案）」に対する意見

2025年11月21日

一般社団法人　日本貿易会
情報システム委員会

2025年5月、サイバー対処能力強化法が成立し、新たな体制となったサイバーセキュリティ戦略本部にて「サイバーセキュリティ戦略」の案が作成された。
内閣官房国家サイバー統括室が2025年11月7日、「サイバーセキュリティ戦略（案）」に関するパブリックコメントを募集したことを受け、情報システム委員会は11月21日付で意見を提出した。

意見内容	理由
P13③ アクセス・無害化措置をはじめとする能動的防御・抑止について 現状案では、アクセス・無害化措置などにより攻撃の影響を低減することが中心に記載されているが、これに加えて、「攻撃者を特定し、刑事捜査・逮捕・起訴にまでつなげること」を可能にする国際的な枠組みの整備方針も明記していただきたい。	多くのサイバー攻撃は海外から行われ、国内で通信を無害化するだけでは、抑止力が十分に働かないおそれがあると考える。攻撃者を実際に捜査・逮捕・起訴できる国際的枠組みを整備することは、能動的サイバー防御の実効性を高め、将来的な攻撃の抑止にもつながると考える。
P15(2) 官民連携エコシステムの強化について 官民連携の重要性が示されていますが、どの組織がどのような役割を担い、民間企業はどの窓口に連絡すればよいのかが分かりづらいと感じる。サイバーインシデント発生時・平時の情報共有時の「統一連絡窓口」（例：分野別CSIRT、ワンストップの相談窓口など）について、それぞれの窓口の担当範囲（相談内容／対象業種／緊急度など）を戦略の中で整理し、図表などで分かりやすく提示していただきたい。	窓口と役割分担が明確になれば、インシデント時の初動も速くなり、平時の情報共有や支援メニューの活用も進み、官民連携エコシステムの実効性向上につながると考える。
P17② 官民における脅威ハンティングの実施拡大について 脅威ハンティングの取組対象は、政府機関や独立行政法人、重要インフラ事業者等に重点が置かれていますが、これに加えて「一般の民間企業」に対しても段階的に拡大していく方針を明記していただきたい。また、日本政府主導の脅威インテリジェンス・プラットフォームを構築する等、規模や業種を問わず多くの企業が脅威情報を閲覧・共有できるようにすることを検討していただきたい。	多くの攻撃は、必ずしも重要インフラに直接向かうのではなく、一般企業やサプライチェーンの弱い部分を足掛かりにして広がるため、脅威ハンティングの考え方を広く普及させることが、社会全体のセキュリティ水準向上につながると考える。また、政府主導の脅威インテリジェンス・プラットフォームがあれば、個々の企業だけでは得られない情報を活用でき、限られたリソースでも効率的な防御が可能になると考える。
P18③ 演習の体系的実施 / P30(4) 全員参加によるサイバーセキュリティの向上について 現状の記載では、主な対象が政府機関や重要インフラ事業者に限定されている印象があるため、参加企業の業種・規模を問わず、インシデント対応能力の向上を図るための、段階別・レベル別の演習メニュー等を整備し、「官民・業種横断」で参加できる仕組みの構築を戦略に位置付けていただきたい。	より多くの一般企業が継続的に演習に参加できる仕組みを整えることで、「全員参加によるサイバーセキュリティ」の理念が具体的に実現していくと考える。
P18　32行目「同盟国・同志国等の関係機関との間で継続的な対話を行い、政策面でのベストプラクティスのみならず、脆弱性情報やIoC（Indicator of Compromise）情報、攻撃手法等のサイバー攻撃に関する技術情報やサイバー攻撃の背景・目的に関する情報等を的確に共有し、」の記述および36行目「必要な情報保全措置を徹底」の記述を踏まえ、NCOが被害組織や専門組織等から提供を受けた情報を同盟国・同志国等と共有する際の、同意取得や匿名性確保等の具体的な配慮事項や、運用指針が決まっているかご教示いただきたい。	被害組織の攻撃技術情報は匿名化が徹底されるものと認識するが、その匿名化の具体的な運用方法や管理体制について、明確化されることが被害組織の安心確保に資するため。
P22 ア 政府統一基準群の継続的見直しについて 日本国内には既に多くの団体（業界団体、学会、標準化団体など）が様々なセキュリティ基準やガイドラインを公開しており、現場では「どれを参照すべきか分かりにくい」という課題があると考える。政府主導で基準の統合・整理を進める方針を明記していただきたい。	基準が分散している状況では、どこから手を付けるべきか判断が難しいと考える。政府主導で基準の統合・整理により、企業や団体は自組織に必要な基準を選びやすくなり、対策の効率化とコストの低減につながると考える。
P21② 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上について 社会全体のレジリエンス向上のためには、「重大インシデントの情報が適切に共有されること」と、「各組織が定期的に自らのセキュリティレベルを確認すること」が重要だと考える。 そのために、以下の導入・検討を、戦略の中で打ち出していただきたい。 ・一定規模以上、または特定分野の企業・団体に対して、重大サイバーインシデントの政府機関への報告を「実質的に義務に近い形」で求める制度（報告対象・期限・報告先の明確化） ・定期的なセキュリティチェック（自己点検・外部監査など）の実施と、その結果を踏まえた改善計画策定を求める仕組み ・加えて、攻撃の手口や実施事項等の事例を政府主導でプラットフォーム上で日本企業に公開するような仕組み	報告とチェックを制度として定着させることで、政府は状況把握と支援策立案がしやすくなり、事業者側も継続的な改善サイクルを回しやすくなると考える。
P29 17行目「また、2026年度には（略）、重要インフラを含む業界団体と連携した普及を目指す」の記述は、経済産業省で検討中の「サプライチェーン強化に向けたセキュリティ対策評価制度」を指すものと推察する。本制度基準★4以上の構築・運用につき、以下の3点ご教示いただきたい。 1.【認定機関】当該制度に係る認定・評価を実施する主体はどの機関を想定されているか。政府機関、独立行政法人、民間の第三者認証機関、業界団体等のいずれか、または複数併存となるか。 2.【義務の有無】本制度の認定取得は原則任意との理解でよいか。あるいは、重要インフラ・重要産業や一定規模（例：従業員数・売上・資産規模等）以上の事業者に対して取得を義務付ける想定であるか。一定の義務付けが想定される場合は、義務付け対象の業界・条件等、また経過措置、適用開始時期、不適合時の対応（罰則・発注制限の有無）などの想定をご教示いただきたい。 3.【制度運用】当該基準・制度は、政府統一基準に規定の上、政府調達における入札参加資格・技術要件等として導入することを想定しているか。（要は政府案件の入札時には認定を必須とするなど） 他方、民民の取引・委託契約においては、本認定制度の活用を「義務」、「推奨」、「任意」のいずれに位置付けるのか、方針をご教示いただきたい。	本意見は、事業者の予見可能性を確保し、計画的な対応準備にあたり確認するもの。 認定主体や義務付け範囲、政府調達・民間契約での位置付けを早期に明確化いただくことが、各業界業種に応じた対策の促進、公正競争の確保、ひいてはサプライチェーン全体のセキュリティ水準の向上につながると考えるため。