2025.04.18
国民民主党　竹詰仁

サイバー対処能力強化法案及び同整備法案　本会議質問

国民民主党・新緑風会の竹詰仁です。

会派を代表し、ただいま議題となりましたサイバー対処能力強化法案及び同整備法案について質問をいたします。

令和４年12月に策定した「国民民主党の安全保障政策2022」の中では、アクティブ・サイバー・ディフェンスの早期導入を提唱し、サイバー対処能力の強化を訴えました。

一方その後も、アクティブ・サイバー・ディフェンス、能動的サイバー防御の導入は実現には至らず、令和５年７月には、名古屋港のターミナルシステムが大規模なサイバー攻撃を受け、名古屋港は３日間機能停止に陥った事案が発生してしまいました。

こうした重大事案を踏まえ、令和６年４月、我が党は、議員立法で、「サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案」を提出いたしました。また、同月、いわゆる経済安全保障版セキュリティ・クリアランス法案の参議院本会議質問で、私自身が質問に立ち、その際にも「アクティブ・サイバー・ディフェンスは待ったなしで、すぐにでも法整備が必要である」旨を訴えました。

今回の政府案は法案提出までにかなりの時間を要しましたが、その方向性は従前から我が党が主張してきたことと合致しており、責任ある国家安全保障体制の構築に向けた大きな一歩と評価したうえで石破総理に質問をさせていただきます。

まず、現状の日本のサイバー防御能力が本法案によりどれだけ強化されるかについての展望、あるいは目標についてお伺いします。

各国のサイバー防御能力についての国際的な比較を行うため、一つの参考として米国のハーバードケネディスクールが実施した「国家サイバー・パワー・インデックス」調査があります。この調査によると、日本のサイバー防御能力の順位は2020年の９位から2022年は16位まで落ちています。また、アメリカの元国家情報長官であるデニス・ブレア氏が2022年、そして2024年にも「日本のサイバー防御能力はマイナーリーグレベル」と酷評しています。

石破総理は３月18日の衆議院本会議で「今回の立法措置により、既に欧米主要国で取組が進められている官民連携の強化や、通信情報の利用、アクセス・無害化のための権限付与などを通じ、サイバー攻撃に関連する情報収集、分析能力や、重大なサイバー攻撃への対処能力の大幅な強化が可能となります」と答弁していますが、真にサイバー対処能力を欧米主要国と同等以上に向上させるためには、その制度を効果的に運用するとともに、日本が弱いとされるインテリジェンス能力を高める必要があります。「日本

のサイバー防御能力はマイナーリーグレベル」などと評価されないために、具体的にどのようなことに取り組んでいくのか、石破総理の見解と決意を伺います。

次に、官民連携の強化、そして目指すべき成果について、伺います。

官民の協議体について、例えば米国では2021年にＪＣＤＣ[1]（Joint Cyber Defense Collaborative）が設置され、政府機関とセキュリティベンダ、グーグルのようなビッグテック等が連携し、情報共有が行われてきています。そしてＪＣＤＣでは、未公開情報を官民で共有し、起こり得る危機のシナリオを共同で研究しているとされています。

今回の法案では、米国のＪＣＤＣなども参考にして、協議会を設置するとの規定が盛り込まれると思いますが、民間企業が協議会に参加するインセンティブとして、政府はどのようなことを考えているのでしょうか。それによってどれぐらいの数の民間企業が協議会に参加することを見込んでいるのでしょうか。また、基幹インフラ事業は現在15分野で、200を超える者が特定社会基盤事業者として指定されていますが、すべての者が協議会に参加することを想定しているのでしょうか。そして新たな協議会をどのように活用し、どのような成果を得ようとしているのか、石破総理の見解を伺います。さらに、衆議院本会議で、石破総理は「協議会においては、重要経済安保情報保護活用法のセキュリティ・クリアランス制度も活用して、適切な情報管理がなされるよう取り組んでいく」旨の答弁をしていますが、本年５月から始動する重要経済安保情報保護活用法のセキュリティ・クリアランス制度と今回のサイバー防御強化法案との関係、そして、これらの取組を産業競争力の強化につなげていくためのポイントや課題について総理に伺います。

次に、通信情報の利用について、伺います。

基幹インフラ事業者や電気通信事業者が政府に提供した通信情報について、仮に情報漏えいが発生した場合には、それらの企業の信用を毀損することにつながってしまう懸念があります。情報漏洩を回避するためにも、政府においては、厳格な安全管理措置を講じることが重要になると思いますが、具体的にどのような措置を講じることを考えているのでしょうか。また、今後、情報漏洩を回避する措置に伴う予算規模と確保について、総理の見解を伺います。

次に、アクセス・無害化措置について伺います。

有効なアクセス・無害化措置を実行するために、警察・自衛隊はどのようにしてそうした能力を身に付けるべく訓練等を実施しているのでしょうか、また、今後その能力をどのように強化していくのでしょうか。例えば、サイバーに係る共同演習等を通じ、アクセス・無害化措置を先に実施している米国や英国などの知見や技術を学んでいく必要もあるのではないのでしょうか。また、我が国が誤ってアクセス・無害化措置をとることは避けなければなりません。ミスを防ぐにも先行する国に学ぶべきことがあると思い

ます。誤ってアクセス・無害化措置をとることをどのようにして回避していくのでしょうか。「単にミスがないように留意する」というものではなく、具体的なミス防止策について伺います。

次に、サイバーセキュリティ人材の育成・確保について伺います。昨年 11 月末の有識者会議提言では「政府が官民の人材育成の取組をしっかり把握した上で、産学官の共通認識を醸成するため、政府主導で技術者に限らず、経営等に関わる者も含めたサイバーセキュリティに関わる人材の定義付けや資格の活用による可視化等を行う」とされています。こうした提言を踏まえ、政府はサイバー人材の育成・確保について、どのような取組を行っていく考えなのか、総理の見解を伺います。また、石破総理は防衛庁長官や防衛大臣を歴任されておりますが、特に自衛隊のサイバー能力についてはどのような認識を持ち、今後どう高めていく必要があると考えているのか伺います。

最後に、偽情報対策をサイバー防御能力の強化と併せて行う必要性についても伺います。サイバー攻撃と同時並行で偽情報によって国家を混乱に陥れるようなことも十分想定されることであり、偽情報対策についても可能な限り早期に法整備を行うべきではないでしょうか。国民民主党は令和６年４月に提出した議員立法の中で、偽情報対策について調査・研究を行い、その成果を踏まえ、偽情報の拡散が国家及び国民の安全を損なうことがないようにするための措置についても提言しています。偽情報対策はこれまで主に内閣官房や総務省が担当してきたと思いますが、これまでどのような取組を行い、どのような成果を挙げてきたのでしょうか。併せて、サイバー攻撃と偽情報により社会的混乱が発生している事案も踏まえ、偽情報対策について法整備を行う必要性についても総理の認識を伺います。

能動的サイバー防御を導入するという趣旨に賛成ではありますが、重要となるのは実効性の高い運用の確保だと考えます。本法案による能動的サイバー防御の制度について、どのようにして実効性の高い運用を行っていくのか、丁寧な説明と真摯な議論を求め、私の質問を終わります。（3,126 字）