「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案並びに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の施行に伴う関係法律の整備等に関する法律案（サイバー対処能力強化法案・サイバー対処能力強化法整備法案）」
に対する本会議質疑

国民民主党・無所属クラブ
衆議院議員　菊池　大二郎

国民民主党・無所属クラブの菊池大二郎です。

まず、冒頭、私の地元・山形県を始め、今冬は広い範囲で大雪に見舞われ、人身被害や家屋・農業用施設等の被害も多数発生いたしました。また、東北に身を置くものとして、先日発災いたしました、岩手県大船渡での大規模山林火災は、東日本大震災から１４年目を迎える折に発生した極めて悲惨なものであり、胸が締め付けられる思いです。お亡くなりになられた方々・ご遺族様に衷心よりお悔やみ申し上げますとともに、被害に遭われた方々へ心からお見舞いを申し上げます。政府に於かれましては、こうした東北の窮状にしっかりと目を向け、寄り添い、一日も早い復旧・復興に向けて全力で取り組まれるよう心からお願い申し上げます。

それでは、会派を代表して、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案並びに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の施行に伴う関係法律の整備等に関する法律案（サイバー対処能力強化法案・サイバー対処能力強化法整備法案）について、質問させていただきます。

国民民主党は、令和４年１２月に国家安全保障戦略が閣議決定される以前から、玉木雄一郎代表を中心に、サイバー安全保障の必要性について提唱するとともに、昨年４月には「サイバー安全保障法案」を国会に提出し、いわゆる能動的サイバー防御の重要性を力強く訴えてまいりました。

この分野において、大切なことは単純明快であります。サイバー攻撃は受けたら終わりということです。受けてから対処するでは、これから、ますます各分野でデジタル化・DX化を加速させ、通信なくして社会が成り立たない状況下において、国民生活を守り抜くことはできません。

この点、政府は、国家安全保障戦略において、特に、国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとして、能動的サイバー防御を導入することを明記しておりますが、今回の政府案においては、能動的なスタンスは読み取れません。

本法案が、政府全体としてサイバー防御能力を強化し、官民連携等を推進する仕組みを構築していく姿勢は評価いたしますが、サイバー安全保障分野における取組は世界的にみても後進国になっているのではないでしょうか。

そこで、この分野における我が国のレベルを総理はどのように認識されておりますか。また、我が党が掲げ、政府においても戦略と位置付ける能動的サイバー防御の必要性や今後の取組についてはどのようにお考えですか。欧米主要国と同等以上の対応能力を向上させるわけですから、そうした各国の水準と同様の措置を講じるべきと考えますが、総理のご見解をお伺いいたします。

次に、本法案では、政府と民間事業者の連携強化が重要な柱の一つとされていますが、大前提として、我が国へのサイバー攻撃の状況や対応の必要性について、民間事業者のみならず国民レベルで理解を醸成していくことが必要と考えます。

この点、先ほど紹介しましたように、重要インフラ等がひとたび機能不全に陥れば、国民生活への影響や経済的損失は計り知れませんし、国立研究開発法人「情報通信研究機構」が観測したサイバー攻撃関連の通信数は、平成２７年の年間約６３２億回から令和５年は約６１９７億回とほぼ１０倍に増加したとのことです。

そこで、近年の、サイバー攻撃による被害件数及び経済的損失は分野ごとにどのような実態にあるのでしょうか。また、そうした事態に対して、これまで政府としてどのような取組を実施されてきたのか、その成果と課題について、坂井大臣及び平大臣にお伺いいたします。

この点、サイバー攻撃によって被害に遭った民間事業者は、イメージダウンや防御レベル等について周知されることを懸念・警戒することも想定されるため、こうした企業心理を考慮した政府主導の官民連携が求められると考えます。また、インシデント報告等が事業者等にとって過度の負担にならぬように、窓口の一本化やフォーマットの統一、情報共有等に係るガイドラインを示すなど事業者等への相談体制の整備や配慮も重要です。加えて、大多数を占める中小企業等への支援も重要であり、企業のサイバー対策投資を促進するための税制上のインセンティブ、セキュリティクリアランス制度の活用に向けた制度設計をいかに図るかが問われているといえます。

以上の点を踏まえ、官民連携の在り方について、総理にお伺いいたします。

さて、本法案の実効性を担保するうえで欠かせないのが、サイバー防御等に係る専門性の高い人材の育成と確保であり、まさに、人づくりは国づくりであります。

この点、昨年１２月、参議院における令和５年度決算に関する代表質問にて、我が党の浜口誠政調会長が、世界デジタル競争力ランキングによれば、日本が過去５年間で４ランク低下し、６７か国・地域中３１位になっていることを紹介し、デジタル人材の育成強化が喫緊の課題であることを指摘されました。総理からは、有識者会議における提言を踏まえ、サイバー攻撃への対処にあたる優れたデジタル人材の育成、確保に一層努めてまいりたいとの答弁がありましたが、具体的にサイバーセキュリティ分野への人材の流入や育成に向けてどのように取り組まれていかれるのでしょうか。

この点、同等以上の処理能力を目指す、いわば目標とも言える欧米所有国との連携を密にし、様々なノウハウを入手し共有する場の提供を日本側から呼び掛け、人材交流等を積極的に働きかけていくことで人材の育成を図っていくことも手法としてはあり得るのではないかと考えますし、現に、経団連は、英国の国家サイバー諮問委員会と情報交換や人材育成で協力していく合意を締結し、取組を進めています。

以上を踏まえ、人材の育成・確保に関する考え方について、総理にお伺いいたします。

次に、組織・人事の点からお伺いいたします。

本法案によれば、これまでのサイバーセキュリティ協議会を廃止し、新しく情報共有・対策のための協議会を設置するとのことですが、これまでの同協議会の取組をどのように検証をされているのか、また、新しく設置する協議会との違いは何か、どのような部分を強化していくのかお伺いいたします。

また、サイバー攻撃の実態を把握するため、通信情報を利用し分析する審査及び承認等の権限を新たに設置される独立機関であるサイバー通信情報管理委員会に付与し、委員長及び委員４人をもって組織するとのことですが、単なる政府の追認機関とならぬような人選や組織形成が不可欠と考えますが、どのような基準で選考し組織化を図るお考えでしょうか。

一方で、承認に過度な時間を要しては、即応性が求められる緊急事態においては被害が拡大してしまうおそれがあるため、事後通知という手法も想定されておりますが、具体的な運用方法はどのようなものでしょうか。

また、同委員会は所掌事務の処理状況について、国会に報告し、その概要を公表することとしておりますが、事前・事後の承認件数等を明確にするほか、事前承認が形骸化しないか、政府が取得した情報が目的外の使用に及んでいないかなどの調査等を含めて定期的に報告するなど、可能な限り国民の知る権利に応え、国民から信頼される制度が構築されるような運用が重要といえますがどのようにお考えでしょうか。

加えて、サイバーセキュリティ戦略本部を改組し、その機能強化を図っていくとのことですが、関係省庁や地方公共団体、有識者から構成されるサイバーセキュリティ推進専門会議に期待される役割や責任範囲につき不透明であり、新たに内閣官房に設置されるサイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官についても、国家安全保障局次長を兼務させることも含めた設置の狙いと具体的な権限、人事の考え方などについて示されるべきと考えますがいかがでしょうか。

また、各省庁におけるサイバー攻撃に関する高い専門性を有する人材の配置が叶うのかが懸念されますし、そもそも、我が国の公務員の人事制度は、定期的な部局異動が伝統である故、専門性を向上させる土壌があるとはいえず、こうした点を克服し、洗練された専門家集団をいかにして形成していけるかが鍵です。また、横断的なサイバーセキュリティ部局が物理的にも独立し、同一の場所で協働できるような環境やデータセンターといった

インフラを整備していくことも必要ではないかと考えますがいかがでしょうか。

以上の点を踏まえ、組織・人事に関する総理の見解をお伺いいたします。

なお、アクセス・無害化措置において実施主体となる警察庁長官が指名するサイバー危害防止措置執行官の選定や各都道府県警察本部も踏まえた体制の構築、並びに、自衛隊における専門部隊の強化について、坂井大臣及び中谷大臣にそれぞれお伺いいたします。

次に、通信情報の利用及びアクセス・無害化措置について、本法案によれば、国内を経由し伝送される国外から国外への通信（いわゆる外外通信）、国外から国内への通信（いわゆる外内通信）、国内から国外への通信（いわゆる内外通信）について、基幹インフラ事業者等の同意によらずして、前述のサイバー通信情報管理委員会の承認を受けることを要件に、内閣総理大臣は、自動的な方法による機械的情報（例えば、総受信日時やＩＰアドレス、指令情報等の意思疎通の本質的な内容ではない情報）を選別・取得し、それ以外のものは直ちに消去されるとのことですが、具体的にどのような態様でなされるのでしょうか。

この点、近年、攻撃の高度化に伴い、前述の単純なインディケータ情報の共有では検知や対策が困難であるため、実効性のある運用となり得るのかという懐疑的な意見もありますがどうお考えでしょうか。

また、内閣総理大臣は、必要がある場合には、外国の政府等に対して、分析情報を提供することができるとしておりますが、片務的な印象もあり、その真意は何でしょうか。

加えて、サイバー攻撃による重大な危害を防止するため、警察・自衛隊による措置等を可能とし、その際の適正性を確保するための新しい手続きとして、攻撃元へのアクセスは原則警察が行い、高度に組織的かつ計画的な行為については自衛隊が共同で対処にあたるとしておりますが、警察と自衛隊の組織間連携をどのように図っていかれるのでしょうか。

一方で、国家安全保障の観点から整合性のとれた形で実施される必要性から、内閣官房が国家安全保障局とも連携しつつ司令塔機能を発揮するとのことですが、緊急事態時における指揮命令系統をどのように整理し、即応性を確保するのでしょうか。

以上の点につき、総理にお伺いいたします。

次に、いわゆる能動的サイバー防御を導入する場合、憲法２１条に規定される通信の秘密との整合性の確保、刑法及び不正アクセス禁止法や電気通信事業法等の改正も必要であると考えます。同様に、サイバー攻撃の監視・特定・対抗措置を行うためには、国外でのサイバー活動が必要となりますが、その許容性や課題につき、国際法上の観点も踏まえて、どのように認識されておられるか、また、本法案における通信の秘密に対する配慮についての評価や能動的サイバー防御に対する国民の理解と協力の観点も併せて、総理にお伺いいたします。

さて、サイバー攻撃は国際的な問題かつ我が国単独での対処には限界があり、各国との連携強化が不可欠ですが、本法案では国際協力等に関する具体策や考え方について十分な記載がありません。

そこで、攻撃元へのアクセス・無害化につき、相互理解が得られるような関係性の構築、サイバー演習等の実践等を視野に入れた同盟国や同志国との連携を深めるための戦略をどのようにお考えなのか、総理にお伺いいたします。

結びに、本法案は、我が国のサイバーセキュリティを強化する重要な一歩であります。

一方で、我が党が掲げる能動的サイバー防御の導入や緊急事態における迅速的な対応を可能とする体制の確立と強化、アメリカやＮＡＴＯとの協力体制の構築、虚偽情報の拡散が国家・国民の安全に及ぼす影響についての調査・研究及び必要的措置の実施等の政策実現に向けては道半ばでありますので、引き続き、積極的に議論を展開していく覚悟です。

政府に於かれましては、本法案の提出を機に、関係法令も含めて不断の見直しと改善に努められますよう、心からお願い申し上げ、会派を代表しての質疑とさせていただきます。

ご清聴ありがとうございました。

以上