第百八十六回国会　衆議院　内閣委員会議録　第二十三号

平成二十六年六月十一日（水曜日）

午前十時開議

出席委員

委員長　柴山　昌彦君

理事　関　芳弘君　理事　平　将明君

理事　橘　慶一郎君　理事　西川　公也君

理事　平井たくや君　理事　近藤　洋介君

理事　松田　学君　理事　高木美智代君

青山　周平君　秋本　真利君

大岡　敏孝君　鬼木　誠君

川田　隆君　小島　敏文君

小松　裕君　新谷　正義君

田所　嘉徳君　田中　英之君

高木　宏壽君　豊田真由子君

中谷　真一君　中山　展宏君

長島　忠美君　福山　守君

宮崎　謙介君　宮下　一郎君

盛山　正仁君　山田　美樹君

湯川　一行君　吉川　赳君

小川　淳也君　津村　啓介君

原口　一博君　吉田　泉君

浦野　靖人君　遠藤　敬君

杉田　水脈君　中丸　啓君

山之内　毅君　遠山　清彦君

濱村　進君　大熊　利昭君

赤嶺　政賢君　村上　史好君

国務大臣（内閣官房長官）　菅　義偉君

内閣官房副長官　加藤　勝信君

政府参考人（内閣官房内閣審議官）　武藤　義哉君

政府参考人（内閣官房内閣審議官）　谷脇　康彦君

政府参考人（内閣官房内閣審議官）　山崎　重孝君

政府参考人（総務省大臣官房審議官）　冨田　浩司君

政府参考人（外務省北米局長）　石川　正樹君

政府参考人（経済産業省大臣官房審議官）　鈴木　敦夫君

政府参考人（防衛省大臣官房審議官）　室井　純子君

内閣委員会専門員

委員の異動

六月十一日

辞任

青山　周平君　宮下　一郎君

秋葉　賢也君　秋本　真利君

勝俣　孝明君　湯川　一行君

川田　隆君　小島　敏文君

福山　守君　小川　淳也君

大島　敦君　原口　一博君

後藤　祐一君　吉田　泉君

若井　康彦君　浦野　靖人君

遠藤　敬君　遠山　清彦君

輿水　恵一君　濱村　進君

濵地　雅一君

補欠選任

宮崎　謙介君

同日

辞任

秋本　真利君　盛山　正仁君

小島　敏文君　福山　守君

宮崎　謙介君　青山　周平君

宮下　一郎君　秋葉　賢也君

湯川　一行君　川田　隆君

小川　淳也君　大島　敦君

原口　一博君　後藤　祐一君

吉田　泉君　若井　康彦君

浦野　靖人君　遠藤　敬君

遠山　清彦君　輿水　恵一君

濱村　進君　濵地　雅一君

補欠選任

盛山　正仁君

同日

辞任

盛山　正仁君

補欠選任

勝俣　孝明君

六月五日

ＴＰＰ交渉から撤退することに関する請願（塩川鉄也君紹介）（第一二〇五号）

特定秘密保護法の廃止に関する請願（塩川鉄也君紹介）（第一二〇六号）

特定秘密保護法の撤廃に関する請願（佐々木憲昭君紹介）（第一二一七号）

パチンコ店における出玉の換金行為を完全に違法化し、カジノ法の創設とカジノ特別区域の整備を求めることに関する請願（田沼隆志君紹介）（第一二一八号）

韓国・朝鮮人元ＢＣ級戦犯者と遺族に対する立法措置に関する請願（近藤昭一君紹介）（第一二九四号）

同月十一日

韓国・朝鮮人元ＢＣ級戦犯者と遺族に対する立法措置に関する請願（横路孝弘君紹介）（第一三二九号）

関東大震災時の朝鮮人虐殺の真相究明を求めることに関する請願（横路孝弘君紹介）（第一三三〇号）

特定秘密保護法の撤廃に関する請願（高橋千鶴子君紹介）（第一三六八号）

同（佐々木憲昭君紹介）（第一四二四号）

同（佐々木憲昭君紹介）（第一五七六号）

ＴＰＰ交渉から撤退することに関する請願（高橋千鶴子君紹介）（第一三六九号）

全ての子どもの権利が保障される保育制度・子育て支援策の実現に関する請願（高橋千鶴子君紹介）（第一三七〇号）

憲法違反の特定秘密保護法の撤廃に関する請願（笠井亮君紹介）（第一四二三号）

秘密保護法の廃止に関する請願（小宮山泰子君紹介）（第一五〇〇号）

戦時慰安婦問題の最終解決を求めることに関する請願（赤嶺政賢君紹介）（第一五六七号）

同（笠井亮君紹介）（第一五六八号）

同（穀田恵二君紹介）（第一五六九号）

同（佐々木憲昭君紹介）（第一五七〇号）

同（志位和夫君紹介）（第一五七一号）

同（塩川鉄也君紹介）（第一五七二号）

同（高橋千鶴子君紹介）（第一五七三号）

同（宮本岳志君紹介）（第一五七四号）

特定秘密保護法の廃止を求めることに関する請願（吉川元君紹介）（第一五七五号）

特定秘密保護法の廃止に関する請願（佐々木憲昭君紹介）（第一五七七号）

は本委員会に付託された。

本日の会議に付した案件

政府参考人出頭要求に関する件

内閣の重要政策に関する件

サイバーセキュリティ基本法案起草の件

サイバーセキュリティの確保に関する件

○柴山委員長　これより会議を開きます。

内閣の重要政策に関する件について調査を進めます。

この際、お諮りいたします。

本件調査のため、本日、政府参考人として内閣官房内閣審議官武藤義哉君、内閣官房内閣審議官谷脇康彦君、総務省大臣官房審議官山崎重孝君、外務省北米局長冨田浩司君、経済産業省大臣官房審議官石川正樹君、防衛省大臣官房審議官鈴木敦夫君の出席を求め、説明を聴取いたしたいと存じ

ますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○柴山委員長　御異議なしと認めます。よって、そのように決しました。

○柴山委員長　サイバーセキュリティ基本法案起草の件について議事を進めます。

本件につきましては、平井たくや君外五名から、自由民主党、民主党・無所属クラブ、日本維新の会、公明党、みんなの党及び生活の党の共同提案により、お手元に配付いたしておりますとおりのサイバーセキュリティ基本法案の起草案を成案とし、本委員会提出の法律案として決定すべしとの動議が提出されております。

提出者から趣旨の説明を求めます。平井たくや君。

○平井委員　サイバーセキュリティ基本法案の起草案につきまして、提案者を代表して、その趣旨及び内容について御説明申し上げます。

まず、本起草案の趣旨について御説明申し上げます。

現在、我が国におけるインターネットの人口普及率は約八割に達しており、社会経済活動に不可欠の存在となっています。また、スマートフォンの世帯普及率も五割を突破し、いつでも、どこでも、誰とでもインターネットを介してつながる、インターネット前提社会ともいうべき時代を迎えています。そして、我が国が今後持続的に発展していくためには、社会経済活動のあらゆる領域において、ＩＴ利活用の推進が必要不可欠であります。

しかし、インターネット等をめぐる状況は、ＩＴ基本法が制定された平成十三年当時と比べて大きく変わりました。国境を越えたサイバー攻撃などにより、政府や企業の機微情報や技術情報の窃取や、金融、電力、交通等の重要インフラ分野への攻撃といった脅威の深刻化はますます進んでいます。まさに我が国は、待ったなしの危機に直面している状況にあります。

また、平成三十二年には、東京オリンピック・パラリンピックが開催されます。さきのロンドン大会においては約二億回ものサイバー攻撃があったと言われており、東京大会においても、サイバーセキュリティーの確保は最重要課題の一つとなります。

こうした課題に対応するためには、我が国のサイバーセキュリティー対策の推進体制を抜本的に強化する必要があります。具体的には、政府において司令塔的な役割を担う情報セキュリティ政策会議の機能を強化し、各府省の情報共有、迅速な対応、連携を図るとともに、重要インフラ事業者等との連携強化を図る必要があります。

また、サイバーセキュリティー対策を支える人材の育成や技術力の強化を急ぐとともに、地方公共団体、民間企業を含む多様な主体の連携や国による支援を強化し、サイバーセキュリティーを守るための我が国の総合力を高めていくことが求められています。

そこで、我が国のサイバーセキュリティーに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティーに関し基本理念を定め、また、国の責務等を明らかにし、かつ、国として取り組むべき基本的施策を示すとともに、これらの施策を推進するための体制の整備等を行うことが焦眉の急であります。

以上が、本法案を提案するに至った理由であります。

次に、本起草案の主な内容について御説明申し上げます。

第一に、サイバーセキュリティーという概念を初めて法文として定義したほか、サイバーセキュリティーに関する施策の推進に当たっては、まず、情報の自由な流通の確保が経済社会の活力向上等にとって重要であることに鑑み、多様な主体の連携により積極的に対応すること、次に、国民一人一人のサイバーセキュリティーに関する認識を深め、自発的対応を促すとともに、被害から迅速に復旧できる強靱な体制を構築するための取り組みを積極的に推進すること、さらに、ＩＴ利活用による活力ある経済社会の構築のための取り組みを積極的に推進すること、また、国際的な連携促進のために我が国が先導的な役割を担うべく、国際協調のもとに行われるべきこと、加えて、民間主導というＩＴ基本法の理念に配慮すべきことの五点を基本理念として規定しております。

第二に、国、地方公共団体、重要インフラ事業者、サイバー関連事業者等の責務等を規定しております。

第三に、サイバーセキュリティーに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティ戦略を策定し、その実施に必要な資金等の確保を図るため、政府は必要な措置を講ずるよう努めること等を規定しております。

第四に、国が講ずるべき基本的施策として、国の行政機関等や重要インフラ事業者におけるサイバーセキュリティーの確保、国民一人一人、また中小企業者等の民間事業者や大学等の教育機関が自発的に行う取り組みの促進のための情報提供や相談に応じること等を規定しております。

第五に、サイバーセキュリティーに関する施策を総合的かつ効果的に進めるため、我が国における司令塔となるサイバーセキュリティ戦略本部を設置すること、同本部の事務として、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等について規定するほか、同本部は、ＩＴ戦略本部及び国家安全保障会議と緊密に連携すること、関係行政機関からの同本部への資料提供義務等を規定しております。

その他、附則において、政府に対して、サイバーセキュリティ戦略本部に関する事務の処理を適切に内閣官房に行わせるため、内閣官房情報セキュリティセンターの法制化を含む必要な法制整備を行うこと等を規定しております。

以上が、本起草案の主な内容であります。

我が国におけるサイバーセキュリティーを確保していくことの重要性及び緊急性に鑑み、何とぞ速やかに御賛同くださいますようお願いを申し上げます。

サイバーセキュリティ基本法案

〔本号末尾に掲載〕

○柴山委員長　これにて趣旨の説明は終わりました。

本件について発言を求められておりますので、順次これを許します。関芳弘君。

○関委員　自由民主党の関芳弘でございます。

それでは、どんどんとたくさんの質問をさせていただきたいと思います。

まず第一問でございますが、昨今、国内におきますインターネットバンキングにかかわる不正送金による被害額が過去最高となりますなど、サイバー犯罪が国民の財産を大きく毀損しております。銀行では、ワンタイムパスワードを生成する機器の発行、フィッシングサイトに関する注意喚起、管理するシステム及びネットワークの増強等の対策に追われているのが現状でございます。

また、政府機関からの情報の流出事案や独立行政法人、衆議院等での標的型攻撃によるウイルス感染事案など、サイバーセキュリティーにかかわる事件が増加しておりまして、攻撃の巧妙化や国家の関与が疑われるサイバー攻撃事案が世界で発生していることなどに鑑みますと、サイバーセキュリティ基本法を制定しようとすることは時に非常にかなったものだと考えます。

国民一人一人がその重要性を理解し、また国として対応を強化することが必要でありますが、今回の基本法案の中で特に強調すべき点は何か、御提案者にお伺いしたいと思います。

○平井委員　関議員にお答えさせていただきます。

まずは、「サイバーセキュリティ」という言葉を法律上の用語として定義したこと、この意味は非常に大きいと思っています。サイバー空間が実社会と一体となった現状において、インターネット

等を経由した不正プログラムの混入など、いわゆるサイバー攻撃への対応はまさに喫緊の課題であります。その防御の重要性を強く意識したこと、これが大きいと思います。

また、「サイバーセキュリティ」という言葉が広く国民、企業、政府、自治体等の中で浸透することによって意識が高まること、それを我々は期待しているところであります。

そして、次に、関係する多様な主体それぞれの役割を明確にしました。国や地方公共団体、重要インフラ事業者等のほか、国民一人一人の努力についても規定しています。

これは、スマートフォンの普及が五〇％を超えて、個人情報を詰め込んだ小さなパソコンを持ち歩いていると国民が理解というか意識しているかどうかです。今のスマートフォンは、一九九七年のディープブルーというチェスのチャンピオンを破ったスパコンよりも機能が上なんですね。そういうものを国民が皆さん持ち歩いている、そういう意識を、どのようにこれから多くの皆さんに意識してもらうか、これは非常に重要だと思います。

そして、自分は悪いことをするつもりがなくても、それぞれの小さなパソコン、いわばスマートフォンは踏み台にされる可能性が十分にあります。そういう意味で、国民の意識というものを高めていかなければならないと思います。

そして、私も、五月の連休に、アメリカの方、ワシントンで、ＤＨＳ、国土安全保障省、国務省、サイバーセキュリティーのいろいろな幹部の議員の先生方、またホワイトハウスにある大統領特別補佐官やシンクタンクと議論をさせていただきましたけれども、まさに戦略本部や各省庁や独立行政法人等々の情報共有の枠組みを法律で規定するというのは、アメリカでもそういう法案をつくりたいということで、下院で議論して、可決はしているんですけれども、なかなか成案を得ないというような状況です。

そういう意味で、日本が一歩先に出て、法律的な整備をするということの意味は大きいと思っています。

○関委員　今回の法案の重要性が非常によくわかりました。

一刻も早い成立が課題だと感じる次第でございますが、この基本法を整備しましても、魂が入らなければ意味がないと思います。政府が着実にサイバーセキュリティー対策を実施していくためには、現在、政府において情報セキュリティー対策を担っておりますＮＩＳＣの体制を強化すべきではないのかと私は思う次第でございます。また、着実に実施するための予算の大幅な充実を、これは私は避けて通れないことだと考えますが、この点、どのように思われますでしょうか。

○平井委員　この法案は、先ほど趣旨を説明させていただいたとおり、政府に対して必要な措置を講ずるように依頼をするという形になっています。

この法案は、立法府の意思、国会がピッチャーとして球を投げて、それを政府がキャッチャーとして受けとめていただき、体制強化をするところを含んでいるわけであります。そういう意味で、まさにＮＩＳＣが明確な権限とともに、法的な、法令に根拠を持つことになるように、いち早く、できるだけ早く政府に体制の整備の法律を出していただかなければならぬというふうに思います。

そして、法律的には、今回、日本の方が一歩先に出るというふうに思うんですが、予算に関して言うと、これはちょっと、各国と議論をしていて、本当なのかなと思われるレベルで少ないわけです。

例えば、日本のサイバーセキュリティー関連予算は、研究開発費を除いて約三百七十億なんですね。アメリカが六千二百四十億ですから、何倍になるんですかね、単純に数字の比較だけではないんですが。研究開発を除くと、まあ、平成二十六年の研究開発の費用、これも全部精査したわけではありませんが、ぱっと見ただけで、アメリカの方が十倍以上であることは間違いありません。そういう意味で、各国とも、法的整備はないものの、研究開発や組織に対しては予算を確保しているということだと思います。

そういう意味で、我々も、予算を含めて考え直さなければならない時期に来ていると考えています。

○関委員　世界に冠たるサイバーセキュリティーを構築していこうということでございますので、予算の点、十二分にこれから配備していただきたいと思います。

三つ目の質問でございます。

平井議員が趣旨説明の中でも触れられていましたが、一昨年のロンドン・オリンピックでは大規模なサイバー攻撃が行われたと伺いました。同大会では、セキュリティー対策に多くの人員、費用が割かれたと聞いておりますが、二〇二〇年の我々の東京オリンピック・パラリンピックの競技大会に当たりましても、万全の体制で大会を開催する必要があると思います。

本法案は、サイバーセキュリティーの分野において対策を加速化させていくものと承知しておりますが、その点につきまして、御提案者の御説明をお伺いいたしたいと思います。

○平井委員　趣旨説明でも申し上げたとおり、二〇一二年夏に開催されたロンドン・オリンピックでは、二週間の開催期間中、公式サイトに約二億回を超えるサイバー攻撃を受けました。東京大会の場合も、恐らくその最大の標的になることは間違いないわけで、例えばスタジアムの電力系の制御システムがハッキングされた場合は、これが開会式だったとしたら、全世界の注目を集める開会式の最中にブラックアウトするという可能性も十分あるわけです。ロンドンは、ぎりぎりになって電力系をマニュアル操作に切りかえて何とか事なきを得たという事実もあります。

そういう意味で、目的が何かはわかりませんが、日本の威信を大きくおとしめるようなことが仕掛けられることは間違いない。それと、東京の二〇二〇年は標的に既になっているということでございます。

そして、そういうことを考えたとき、そういう対策は一朝一夕に整うものではなくて、イギリスのケースもヒアリングをしてまいりましたが、やはりこれは六年前から準備を始めている。というのも、スタジアムの設計段階からサイバーセキュリティーを考慮した仕様、また、関係機関とも連携して体制整備等を図っていく必要があるわけですね。

そういう意味では、日本も、来年が体制強化のキックオフの年としてちょうどぎりぎり間に合うのではないかというふうに思います。六年の間に攻撃側の力もさらに強くなると思いますので、我々はすぐ取りかからなければならぬと考えています。

○関委員　二億回という桁外れの、また想像を絶するようなサイバー攻撃があるというのに本当に私も驚いた次第でございますが、ぜひ万全の体制で日本の東京オリンピック・パラリンピックが成功しますように、心から祈る次第でございます。

四つ目の質問でございます。

大規模なサイバー攻撃は、先ほど述べましたように、オリンピック等のイベントが開催されるときに脅威として強く意識されますけれども、ＩＴの利活用が進んだ国におきましては、日常的な脅威でございまして、常に対処の方策、体制を考えておかなければならないと思います。

例えば、ネットバンキング等の普及が顕著なＩＴ先進国であるエストニアは、二〇〇七年に世界各地からのＤＤｏＳ攻撃を受けまして、オンラインバンキングサービスが閉鎖される事態に陥ってしまいました。また、国連の電子政府ランキングで一位の評価を得ております韓国では、多数の大規模なサイバー攻撃を受けておりまして、昨年は、金融機関に対する攻撃により国内のＡＴＭサービスが利用できなくなったことがありました。ＩＴの利活用を進める我が国におきましても、これらは他人事ではございません。エストニ

ア、韓国における事案では、いずれも、海外のサーバーを経由して攻撃が行われていたと伺いました。

そこで、お伺いしたいのですが、銀行などの重要インフラ事業者等が海外からサイバー攻撃を受けた場合、どのようなスキームで対処するように考えていらっしゃるのか、教えてください。

○平井委員　委員と私、全く同じ考えで、二億回を超えるオリンピックへの攻撃、それだけではなくて、今霞が関も一分間に二回の攻撃を二十四時間三百六十五日受けています。そういうように、サイバーの脅威というものが日々増しているという状況の中で、これから、重要インフラ事業者に対する攻撃もふえると思います。

そして、お尋ねの、銀行などの重要インフラ事業者が海外からサイバー攻撃を受けた場合、この場合は、まず、民間ベースで状況を把握するというところから始まります。その当該事業者は、ＪＰＣＥＲＴ／ＣＣ、コンピューター・エマージェンシー・レスポンス・チーム・コーディネーション・センターというんですが、これは海外どこでも同じような形になっているんですが、ＪＰＣＥＲＴ／ＣＣという、インシデントへの即応対処等を行う組織へまず連絡をする、次に警察へ通報する、そして所管省庁への連絡をするということになります。

ＪＰＣＥＲＴ／ＣＣは、海外のＣＥＲＴ、同じような組織を通じて、攻撃元のＩＳＰ、インターネットサービスプロバイダーへのサーバー停止依頼等を行う。そして、サイバーセキュリティ戦略本部は、情報のハブとして、こうした関係者間のスムーズな連携を促進する調整役となるということになります。また、海外からの攻撃であっても、サイバー攻撃は一義的には警察権により対処する分野ということでありますので、日本の警察が海外の警察に捜査共助要請を行うことになります。

我が国は、サイバー犯罪に関する捜査の協力や犯罪者引き渡しを内容とするブダペスト条約を、これは実は、アジアで唯一批准している国なんですね。こうした国際的な枠組みを積極的に活用していきたいというふうに考えています。

また、こうした点に加えて、今回の法案では、サイバーセキュリティ戦略本部を中心に、関係府省の情報共有体制の強化を図ることとしており、これにより国としての対処能力の向上が図られると考えています。

○関委員　二十四時間三百六十五日、一分間に二回も霞が関が攻撃を受け続けていると。もう本当に驚きの実態でございますし、このことを国民みんなが知ることが大事だと思う次第でございます。

五つ目の質問でございます。

二〇一一年に起こりました三菱重工業や政府機関を標的とするサイバー攻撃につきまして、警視庁公安部の捜査によりますと、中国の特定の組織が関与した疑いがあることが判明した旨、先般報道されておりました。海外からのサイバー攻撃は、金銭目的の犯罪者によるものだけではなくて、中には機密情報の窃取を目的とした外国機関の関与が疑われるものもありまして、その場合には、安全保障の問題としても捉えなければならないと思います。

昨年末に策定されました国家安全保障戦略においても、サイバーセキュリティーの防護がその対象に入っていましたが、今回の法案によりまして設置されますサイバーセキュリティ戦略本部はＮＳＣとどのような役割分担、連携を行うのか、教えてください。

○平井委員　海外からのサイバー攻撃が行われた段階では、攻撃の主体が判明しない。したがいまして、一義的には警察権による対応となります。しかしながら、その捜査の結果、サイバー攻撃が国家機関が関与している疑いが生じた場合、これは安全保障上の問題として対応することになると考えています。

この法案では、サイバーセキュリティ戦略本部はＮＳＣと緊密な連携を図ることとされています。これにより、例えば本部が原因究明調査など、その所掌事務を遂行する中で安全保障にかかわるサイバーセキュリティー関連情報を取得した場合には、ＮＳＣに逐次情報提供をするといったことが想定されています。

○関委員　役割分担、この連携が円滑に行われることを心から祈る次第でございます。

六つ目の質問に参ります。

これまでに述べてきましたように、サイバーセキュリティーは、世界最先端のＩＴ国家実現といった成長戦略の礎でありますとともに、また、オリンピック・パラリンピック大会の成功や国家安全保障にもかかわりまして、今後の日本にとって極めて重要なテーマであります。

これにつきまして、民間に任せるのではなくて、ぜひ私は国に主導的役割を担ってもらいたいと思いますが、いかがでしょうか。

○平井委員　私も、そういう思いがありまして、今回の法律を提出するということに至りました。

ＩＴ社会の形成については、基本法として、高度情報ネットワーク社会形成基本法、ＩＴ基本法ですね、これは二〇〇一年に施行されて、私、国会議員として初めてこの議論に参加をした思い出深い法律ですけれども、この法律では、ブロードバンドの整備等は民間が主導的な役割を担うということが基本理念になっています。この基本理念にのっとって、日本のブロードバンドの環境というものは、本当にちゃんと安全に、速やかに整ったと思います。

サイバーセキュリティーに関しては、国家の安全保障、危機管理にも関する分野であり、国と民間の役割を明確化した上で、国が主導的立場を果たしながら、官民の緊密な連携により取り組みを着実に進めていかなければならないと考えています。

そこで、今回の基本法案は、ＩＴ基本法を補完する、要するに、時代に対応し切れなくなったＩＴ基本法を補完するものとして、各省庁、地方公共団体、重要インフラ事業者等、多様な主体が連携し、野球でいいますと、内野と外野が緊密に連携して、できるだけぽてんヒットを打たれないようにする、そのために国がリーダーシップを発揮するための体制を整備しようということであります。

この分野は、完全試合で食いとめることは無理ですので、できるだけヒットを打たれないようにする、そして、ヒットを打たれても点をとられないようにするというような感覚が私は当てはまるのではないかと思っています。

○関委員　今回は、このサイバーセキュリティーに関しましては、国家安全保障とかかわるからこそ、国がしっかりとその分野を担当し、民間との役割分担をするという意味、よくわかりました。

それでは、最後の質問でございます。

多様な主体が連携しつつ、国全体でサイバーセキュリティーを確保するのはまさにそのとおりでございます。その前提としまして、サイバーセキュリティーに関する人材の質及び量の確保が大事ではないかと思う次第でございますが、この人材確保につきまして何か方策はあるのか、お伺いしたいと思います。

○平井委員　委員おっしゃるとおり、人材は、サイバーセキュリティー強化のまさにキーポイントであると考えています。

実は、日本の子供たちの中にもこの分野に非常に向いている子供たちはたくさんいます。しかし、なかなかキャリアパスが描けていないがために、そっちの道に進むという子供たちが多いようには思いません。

そういう意味で、本法案には、国は処遇面を含めてサイバーセキュリティー分野の仕事が魅力的になるような施策を講ずべきと明記をしています。今回の基本法の制定により、国民の意識を深め、人材の必要性を感じてもらい、どのような教育が必要かを考えてもらうなど、自発的な取り組みを大いに刺激したいと考えています。

また、本法案の附則において、内閣官房におけ

る専門的人材の採用を政府に対して求めており、まずは隗より始めるということで、政府部内にも人材育成のための場を設けたいと考えています。

今、セキュリティー人材というのが二十六・五万人と言われていますが、質的に十六万人足りない、量的に八万人足りないということですから、もうまさに人材の確保や育成というものは、国家的な、本当にダイナミックな取り組みが必要なときが来ていると考えています。

○関委員　以上で質問を終わります。ありがとうございました。

○柴山委員長　次に、高木美智代さん。

○高木(美)委員　公明党の高木美智代でございます。

今、集団的自衛権につきましては、目に見える安全保障ということで、議論は広く行われている最中でございます。一方で、コンピューターネットワークのいわゆる仮想的空間、サイバー空間における安全保障も急務でございます。

昨今の報道によりますと、米中間におきましても、中国の一方的な海洋進出をめぐる対立の激化に加えまして、サイバー空間におきましても、中国軍所属の五人が米企業に対してサイバー攻撃を仕掛けた、それによりまして起訴されたという事例も伝えられております。我が国におきましても、こうしたサイバーセキュリティ基本法成立は急務であると考えております。

我が党の遠山議員におかれましては、サイバー攻撃対処検討委員会の委員長として活躍をいただきまして、また、先般は平井座長を中心に、与党サイバーセキュリティ体制強化に関するワーキングチームということで、約四回議論を重ねまして、野党にも働きかけ、本日、委員長提案の運びとなったことを私は高く評価させていただきたいと思います。私もワーキングチームの一員に加えさせていただきました。

まず、遠山議員にお伺いいたします。

本法案を閣法ではなくて議員立法とした趣旨につきまして、その立法意思、また主なポイント等を含めまして、国民の皆様によくおわかりになりますように、説明をお願いしたいと思います。

〔委員長退席、橘委員長代理着席〕

○遠山委員　高木議員におかれましては、先ほど御自身でもおっしゃっておりましたとおり、与党のワーキングチームで一緒に議論をしながら本法案をつくり上げたわけでございまして、私からも感謝を申し上げたいと思います。

また、当委員会の与野党の理事を初め委員の皆様から御理解をいただきまして、本日、提案に至りましたこと、大変感無量に思っているところでございます。

ただいま御質問ございました、今回なぜ議員立法なのかということでございますが、先ほど来、平井議員からるる御答弁がありましたとおり、我が国は現在大変なサイバー攻撃にさらされておりまして、これは、国家の政府機関に対するもの、あるいは国会そのものに対するもの、また重要インフラを担う事業者に対するもの、さまざまございます。危機は相当深刻な状況にあるというふうに認識をしております。

また、先ほども御答弁ありました、スマートフォンの急速な普及、あるいは自動車とか家電製品がインターネットに接続されるようになってきておりまして、こうしたものもサイバー攻撃の対象になっているという状況から、脅威が拡散しているというふうに思っております。

私も、公明党内の先ほどおっしゃっていただいた立場上、さまざまな調査研究、ヒアリングをしてまいりました。

私が個人的に一番驚いたのは、スマートフォンをウイルスに感染させまして、持ち主が知らない間にスマートフォンの録音機能をオンにして、例えば、一時間ひそかにそれを録音して、ファイルにして、さらに御丁寧にその添付ファイルをウイルスが指定する電子メールの宛先に送る。まさに、昔でいいますと007の映画の中で出てくる秘密兵器のようなことが現在行われている、現実に。持ち主は気づかないそうでございます。ですから、私たちの個人的な会話を一時間とられて、知らないところの電子メールに送られて、それでも本人は気づかないという、攻撃というか、ツールが既にあるということも専門家から伺いました。

また、これは有名な話でございますが、昨年だったと思いますけれども、アメリカのハッキングの公開実験の場で、ネットにつながったトヨタのプリウスがハッキングされて、ドライバーが右折しようとしているときに左折させるということを実際に実演したということも報道されているわけでございます。

このような状況に鑑みまして、サイバーセキュリティーに関する基本理念あるいは基本的施策、それらを強い政治的なリーダーシップのもとで推進するための基本的枠組みを立法府が明確化することによって、政府のみならず、民間も含めて、関係者が一丸となって、スピード感を持って対策に取り組むことが必要であるというふうに思っております。

そのためにも、今回、サイバーセキュリティーに関する施策を総合的かつ効果的に推進するための法律を議員立法として制定することは大変な意義があると思っておりますし、また喫緊の課題でありまして、ぜひ、本日の審議を経て、参議院に送付をしていただいて、今国会で成立をさせていただきたいと心から期待をしているところでございます。

以上です。

○高木(美)委員　ありがとうございました。

今お話を伺いながら、我が国でも、最近、治安のための監視カメラが数万台、もっと大きな規模かもしれませんが、配備されておりますが、その監視カメラを踏み台にしたり、あと、パソコンのルーターを持ち歩いている方も多くいらっしゃいますが、そこからマルウエアが拡散されたり、本当にさまざまな事例が伝えられているところでございます。

こういう問題意識を含めまして、昨年、内閣委員会の代表メンバーで、平井議員を先頭にエストニアを訪問いたしまして、そこでの説明が、やはり私は立法化への確信となりました。世界一のＩＴ国家であるエストニアは、国政レベルの電子投票、デジタル署名、医療のＩＤカード、ｅ－Ｐｏｌｉｃｅなどを実現しております。ＩＴを活用することによって、国民にとっても企業にとっても、社会がより便利になり、効率的になるからという説明でした。

二〇〇七年、先ほどもお話ありましたとおり、大規模なサイバー攻撃を受けまして、政府のシステムはダウンしなかったけれども怖かったということを政府関係者は異口同音に語っておりました。そこで結論としておっしゃっていたことは、セキュリティーを確保するためには、開発デザインの段階から機密性を考慮すること、また、一〇〇％のセキュリティーはあり得ないので、リスクマネジメントを考えることが重要、こうしたお話を伺いました。

我が国におけるサイバー空間の信頼性と安全性を確保するためには、この法案の第二条にありますが、「サイバーセキュリティ」の定義に、「必要な措置が講じられ、その状態が適切に維持管理されていることをいう。」このようにありますように、サイバー空間の衛生を確保する、安全性と信頼性、クリーンな状態で感染をしない、また、そのような機器を推奨する、心配なものは輸入しないというような、こういう衛生を確保することが基本であると考えます。

このために本法律案にはどのようなことが定められているのか、遠山議員に伺います。

○遠山委員　お答え申し上げます。

本法案では、サイバーセキュリティーの確保のために、国や地方公共団体、また、先ほども申し上げました重要インフラ事業者、サイバー関連事業者あるいは教育機関等の関係者の責務、そして、国民については努力について定めるとともに、これらのおのおのの主体者が責務を果たせるよう、国が行うべき基本的な施策について定めて

おります。

少し具体的に申し上げますと、例えば、地方公共団体、地方の自治体やあるいは中小企業がもちろん自主的にサイバーセキュリティーの確保に努めていただくことを責務として規定をする一方で、国がこれらの主体の各種相談に応じ、必要な情報の提供や助言を行う旨も規定をしているわけでございます。

この点につきましては、与党の協議の中でも、私ども公明党の方から、もちろん、国やあるいは大手企業も、必ずしもサイバーセキュリティーについての十分な人材が確保されているとは言いがたい面もございますが、そうは言っても、高木議員の御指摘でもあったわけですけれども、日本の企業の九十数％を占める中小零細企業の皆様方は、日進月歩でどんどん技術が高度化をしているサイバー空間の事柄について、必ずしも十分に対応していくことができないという状況でございますので、やはり大事なことは、国がしっかりと、中小零細企業の皆さんでサイバーセキュリティーを確保したいという意向を持っておられる方々に丁寧に相談に応じ、必要な、そして適切かつ専門的なアドバイスを提供していくということが大事なのではないかというふうに思っております。

なお、国民につきましては、サイバーセキュリティーの確保に必要な注意を払うように努める旨が規定されているわけでございますが、この点につきましても、国がサイバーセキュリティーに関する教育及び学習の振興を図る努力、また、啓発及び知識の普及、こういったことに取り組む、その他の必要な施策もしっかりと講じていくことが大事だと思っております。

最後に、個人的に付言をさせていただければ、先ほどの平井委員の答弁にもありましたように、サイバーセキュリティーに関する人材の育成と確保に、やはり予算もしっかり増額をして、日本全体として取り組むことが重要ではないかというふうに考えておりまして、ぜひとも、今回の法律、これは基本法案でございますから、基本法に基づいてできることをしながら、また、それぞれの専門的な分野においてとるべき必要な施策については官民一体となってしっかりと取り組むべきである、このように考えております。

以上です。

○高木(美)委員　ありがとうございました。

それでは、この法案に規定しております地方公共団体、重要社会基盤事業者、サイバー関連事業者、また中小企業者等々、順次、時間の許す限り伺ってまいりたいと思います。

まず、地方公共団体の責務につきましては、これは、今マイナンバー制度を進めておりますが、この対応にも相当苦労しているというのが自治体の状況でございまして、私は、果たしてこのサイバーセキュリティーに対して十分取り組めるのか、懸念を持っております。相当な支援が必要なのではないかと思います。

そこで、まずＮＩＳＣの谷脇審議官にお伺いたしますが、今、地方公共団体向けに安全指針等を策定されております。自治体ごとに当然対応に差があると思います。十分に普及をしていないのではないか、また、安全指針とはどのようなもので、地方公共団体による対応状況がどうなっているのか、また今後どうされるのか、お伺いをしたいと思います。

あわせまして、総務省におきましては、マイナンバー制度を踏まえた支援、またＪ－ＬＩＳ、地方公共団体情報システム機構を通じた支援、同様の質問でございますので、ＮＩＳＣと総務省から順次答弁をお願いしたいと思います。

○谷脇政府参考人　お答え申し上げます。

私ども内閣官房情報セキュリティセンター、ＮＩＳＣでございますけれども、におきましては、地方公共団体を含みますいわゆる重要インフラ分野におけるＩＴの障害が国民生活等に重大な影響を及ぼさないよう、ＩＴ障害の未然防止及び再発防止の双方の観点から必要な情報セキュリティー対策を盛り込みました安全基準の整備、浸透を図るため、分野横断的に必要度の高い対策項目を収録いたしましたガイドラインを策定しているところでございます。

そして、これを踏まえまして、総務省におきましては、地方公共団体向けのガイドラインを策定しておりまして、各地方公共団体におきましては、これらを参考といたしまして、情報セキュリティーポリシーの策定や、あるいは組織、体制の整備等を図っているところでございます。

また、ＮＩＳＣにおきましては、所管省庁と連携をいたしまして、重要インフラ各分野の安全基準につきまして、その浸透状況等を毎年調査しております。そして、重要インフラ事業者等の情報セキュリティー水準の向上に努めているところでございます。

そして、この調査結果によりますと、地方公共団体によっては残念ながら対応が十分ではないというところもあるところでございまして、私どもＮＩＳＣといたしましては、総務省と連携しつつ、引き続き、地方公共団体の情報セキュリティー水準の一層の向上に向けて取り組んでまいりたいと考えております。

○山﨑政府参考人　お答え申し上げます。

平成二十七年十月に予定されておりますマイナンバー制度の導入に向けました各地方公共団体の支援につきましては、これまで、全国説明会をいたしまして、さらに四十七都道府県で現地説明会等を実施しております。番号制度の概要、それからスケジュール、必要な作業のほか、肝心でございますが、マイナンバー制度に対応した個人情報保護措置として地方公共団体に求められる制度面、技術面、体制面で講ずべき措置などについて説明し、適切な対応を支援してきたところでございます。

引き続き、現地説明会等をさらに実施いたしまして、必要な情報提供を行うとともに、各省庁と連携いたしまして、きめ細やかな対応をしてまいりたいと思います。

総務省といたしましては、先ほどＮＩＳＣの方からお話がありましたが、地方公共団体の情報セキュリティー対策全般を支援するために、情報セキュリティポリシーガイドラインの提示をしております。それから、サイバー攻撃等の注意喚起情報の提供、情報セキュリティーに関する人材育成などの支援を行っておりまして、今御指摘のありました地方公共団体情報システム機構とも緊密に連携した上で実施しております。

今後も引き続き、地方公共団体に対しまして、情報セキュリティー対策の向上に資するよう必要な支援を行うとともに、セキュリティーポリシー遵守の徹底など、セキュリティー対策に万全を期すように促してまいりたいと思います。

○高木(美)委員　恐らく、そういう情報、ガイドライン等を出されますと、多分それがベンダーに行く、地方公共団体はそこに丸投げをするというところもあるようです。ですので、ベンダーロックインという今の状況を踏まえまして、地方自治体がどのように人材を確保しながら、そこで自分たちのシステム、また自治体クラウド等々活用を含めまして進められるか。

当然、そこには、先ほど来、本法案に規定されておりますサイバーセキュリティー、また個人情報保護の問題等々あると思いますので、そうした総合的な相談に、しっかりと自治体の相談に乗っていただきますように重ねて要請をさせていただきたいと思います。

それでは、中小企業者による自発的なサイバーセキュリティーに対する取り組みを促進するためにも、国による具体的な支援が必要と考えます。経済産業省の対応を伺います。

○石川政府参考人　お答えさせていただきます。

中小企業でございますけれども、御指摘のとおり、やはり非常に難しい問題がございまして、例えば、専門人材を雇用する余裕がないために、セキュリティー対策についての情報やノウハウが不足しているというようなこと、また、セキュリティー対策に必要な機器やソフトの購入などのために資金上の制約があるといったような問題があ

るというふうに考えております。

このため、私どもの方といたしましても、例えば、中小企業の情報セキュリティ対策ガイドラインというものをつくらせていただきまして、平成二十一年三月から、全国の商工会議所、自治体などと連携しまして、約六百五十回のセミナーや説明会を開催させていただきまして、きめ細かく御説明を申し上げております。

また、平成二十二年十月からは、情報セキュリティ安心相談窓口というものを専門機関に設置いたしておりまして、それぞれの細かい一般ユーザーの方からの御相談も含めまして、約五万四千件の御相談に対応させていただいてきております。

また、資金面でございますけれども、中小企業投資促進税制の中でセキュリティーのソフトウエアなどの購入も対象としておりまして、税額控除などが受けられるようにさせていただいております。

また、平成十二年度からは、日本政策金融公庫によりまして、ＩＴ活用促進資金という低利融資制度をつくらせていただいておりますが、こちらでもまた、セキュリティーなどの関係機器などにも低利融資をお使いいただけるようにさせていただいております。

今後とも、こういった中小企業の対応につきまして、積極的に支援をさせていただきたいと考えております。

以上でございます。

○高木(美)委員　相談窓口の設置等、取り組みにつきまして、さらに本法案の成立を機に強化をお願いしたいと思います。

最後に、国民に対して、このサイバーセキュリティーの確保に努めるために、普及啓発、具体的な対策等々、また相談に応じたり助言することなどが必要かと思います。三月十八日がサイバーの日というお話だったでしょうか。そういうことも含めまして、政府の対応につきまして谷脇審議官に答弁を求めます。

○谷脇政府参考人　お答え申し上げます。

委員御指摘のとおり、国民に対するサイバーセキュリティーの普及啓発につきまして、私どもＮＩＳＣは、関係省庁等と連携をいたしまして、イベントの実施、パンフレットの作成、あるいはインターネットを通じた情報提供等を行っているところでございます。特に、毎年二月を情報セキュリティ月間といたしまして、産学官民が連携をいたしまして、これらの取り組みを集中的に実施しているところでございます。

各府省等におきましても、例えば、都道府県警察におきましては、企業、団体や教育機関等との連携による講演の実施等の取り組みを通じたサイバー犯罪の手口等の周知、また、総務省におきましては、インターネットサービスプロバイダー等と連携した、一般の利用者がウイルスサイトにアクセスしようとした際に注意喚起を発するプロジェクトであるＡＣＴＩＶＥの実施、さらに、経済産業省におきましては、ＩＰＡによる情報セキュリティ安心相談窓口の設置や、小中高校生を対象としたセキュリティーに係るポスター、標語コンクールの実施等が行われているところでございます。

また、委員御指摘のとおり、ことしの三月十八日、サイバー訓練の日ということで、関係者が集まって情報共有訓練なども実施したところでございます。

政府といたしましては、本法案を踏まえまして、国民全体のサイバーセキュリティーへの関心の一層の増進を図る観点から、本年の夏ごろをめどに、新たな普及啓発プログラムの策定を進めているところでございます。

具体的には、多様な関係者が参画する協議会を通じまして、普及啓発活動を積極的に推進することのほか、情報セキュリティ月間の有効活用など、新たな施策の実施を含め、積極的に対応してまいりたいと考えているところでございます。

○高木(美)委員　さらに、国とそれから議員と一体となりまして、このプロモーション活動といいますか、普及啓発活動を強く進めてまいりたいと思います。

ありがとうございました。

○橘委員長代理　次に、近藤洋介君。

○近藤(洋)委員　おはようございます。民主党の近藤洋介であります。

近年、急激に増加をしているサイバー攻撃に対応するための基本法案、サイバーセキュリティ基本法案が議員提案の形で、内閣委員会でこうやって議論をされ、そして、採決を経て、委員会提案をされる見通しになりつつあることに、私も作業にかかわった一人として大変うれしく思います。

また、民主党としても、本法案に対して自公側から御提案があり、これに対して、条文の修正並びに新たな提案、相当な提案をさせていただきました。短い期間ではございましたけれども、こうした提案について、ほとんどというか全て受けとめ、そして、共同してつくり上げてきていただいたことに、まずもって、各党、とりわけ自民党、公明党さんに敬意を表したい、こう思います。

もとより国会は唯一の立法機関であり、国権の最高機関であります。各党各会派全ての思いが全部一致するということはなかなか難しいわけではありますけれども、こういった基本法といった性質のものについて、やはり各党各会派が、政府提案というのも一つかもしれませんが、あえて申し上げると、基本法のようなものは議員提案のような形でよい法律をつくる、よりベターなものを目指す、解を目指すという姿勢は非常に重要ではないか、私はこう思うわけであります。

平成二十年に、実は当内閣委員会で、こうした同様の形で宇宙基本法が制定をされております。これもこうした形で制定をされております。まさにこうした基本法のような性質のものは議会において提案をされ、そしてその議会の意思を受けて政府がさまざまな施策を講じていくというのは、議会制民主主義の一つの基本形であろうと思います。

今後、この基本法を受けて、政府において、政府提出法案なり、さまざまなことが予想されるわけでありますが、ぜひ、政府においては、本法案のこうした議論の経緯、経過を十二分に踏まえて、今後の行動に反映させてもらいたい、まずもって、冒頭、強く申し上げたいと思います。

まず冒頭、民主党提出者の原口一博議員にお伺いをします。

民主党は、政権担当当時からサイバーセキュリティーの確保の重要性を認識し、特に世界の動きに着目をして、国際連携の分野においてもさまざまな取り組みを進めてまいりました。とりわけ原口議員は総務大臣としてでもさまざまな活動をされてきたと認識をしております。今後ますますサイバーセキュリティーの分野で国際連携の必要性が高まる、こう思うわけでありますが、原口提出者のお考えをまずお伺いしたい、こう思います。

○原口委員　お答えいたします。

近藤委員におかれましては、内閣委員会で、またＩＣＴの専門家として、このサイバーセキュリティー法案を主導してくださいまして、本当にありがとうございます。また、政権時代からさまざまな御支援をくださっていることをあわせてお礼を申し上げたいと思います。

今お話しのように、サイバーアタックの状況はますます大規模化、深刻化しています。ちょっと前は、まあ、ミサイルに例えるのが適切かどうかわかりませんけれども、大規模なミサイルでどんと、量と破壊力でもってやってくるという例もありました。しかし、今では、ステルス型といいますか、先ほど答弁にもありましたように、それが入ったことさえ気づかないという状況が進んでいます。我が国の安全保障にとりましても、自由な社会を守り、人間の尊厳を守るためにも大変大事な分野でございます。

そこで、今御指摘ありましたように、私たちは国内の防御の仕組みをつくるために、例えば独立行政法人情報通信研究機構、これはＮＩＣＴといいますけれども、このＮＩＣＴでｎｉｃｔｅｒと

いうものを開発しまして、サイバーアタックの状況をビジュアル化しています。ぜひ、これは委員の皆様を初め国民の皆様にごらんになっていただきたいと思います。いかに深刻であるか。

そして、そのためには、何といっても、今委員が御指摘のように、国際連携が必要です。サイバーは、どこか一つの穴があれば、そこから無限に、ダムの一穴と同じで、大きな危機が広がっていきます。

そこで、私は、二〇〇九年九月、ちょうど政権交代直後でございましたけれども、アメリカを訪れまして、当時のＦＣＣ委員長に対して、サイバーセキュリティーを含む四つの分野についてタスクフォースを立ち上げようじゃないか、そして、日米が主導して世界のルールづくりをしようじゃないかということをやってきました。

このタスクフォースを基礎に、二〇一〇年十一月からインターネットエコノミーに関する日米の政策協力対話が開始されて、二〇一二年の三月、第三回目の会合では、総務省と米国国土安全保障省との間でサイバーセキュリティーに関する連携についても合意を得たところでございます。具体的には、サイバー攻撃を早期に検知する技術、これの研究協力を行うことについても、現在、連携が継続をしています。

今後の国際連携についてですけれども、ちょうど二〇一一年でしたか、当時のジェナカウスキー委員長、それから国務省のバービーア大使と数次にわたってやってきましたけれども、「サイバー空間における外国スパイによる米国経済機密の不正取得について」というこのペーパーを手交してくれました。ここには何が書いてあるか、ちょっと時間をいただいて。こう書いてあります。

中国とロシアについて。中国については、執拗な情報収集者であると指摘して、二〇一〇年の産業スパイ法の検挙者七名中の六名が何と中国関係者であった、そして、標的攻撃と呼ばれるコンピューターネットワークへの不正侵入のアクセス元が中国国内のＩＰアドレスであるとサイバーセキュリティーの専門家が報告していることを例示しています。ただし、それらの攻撃に国家の関与があるかどうかは断定できていないんですね。ロシアについては、ロシアの経済成長と安全保障のために、ヒューミント、サイバーその他の広範に洗練された手段を使って産業技術情報を収集していると指摘。

一国が、一つのインテリジェンスが他国を名指しでやるというのはなかなかないことです。これは、中国、ロシアをここで責めているんじゃなくて、むしろ、そういう国々も含めてやはり大きな連携をつくり、そして日米の同盟国が中心となって世界的なサイバー上のルールをつくっていく、これが必要だというふうに考えておりまして、与野党を超えた、こういう基本法的な仕組みを、ここで、議院、国権の最高機関でお示しいただいたことは、まことに時機を得たことである、そのように考えております。

〔橘委員長代理退席、委員長着席〕

○近藤（洋）委員　ありがとうございます。

あわせて原口議員にお伺いしたいんですが、サイバーセキュリティーの確保というのは、これは非常に重要であります。ただ同時に、押さえておかなければいけないのは、今基本法案でも基本理念を示しているわけですけれども、サイバーセキュリティーが重要だからといって、国民の権利というものを不当に侵害してはいけないんだろう、こう思うわけですね。ここはきちっと押さえていかなければいけない、守らなければいけない、これは大事なところだと思うのですね。

サイバーセキュリティーが大事だからといって、では、ある捜査機関が全て国民のパソコンを閲覧していいのか、これはとんでもないことになるわけでありますし、そうしたことも含めて、国民の権利の尊重とあわせて、国会への報告といったこともしっかりと図るべきだと考えますが、提出者の見解をお伺いしたいのですが。

○原口委員　まさに御指摘のとおりだと思います。今回の与野党の協議の中でも、今御指摘のところが一番大きな柱の一つになりました。

本基本法を受けてサイバーセキュリティーに関する施策が具体化される場合、サイバーセキュリティーの確保のために、個人所有のパソコンや通信記録あるいは一定の個人情報などを公的機関に対して提供することが一方的に求められるんじゃないか、まさに抑圧の仕組みになってはならない、そういうおそれを取り除かなきゃいけないという御議論がございました。

そこで、本基本法では、このようなおそれが生ずることがないように、サイバーセキュリティーに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意すべきこと、それから、サイバーセキュリティーに関する施策について定めるサイバーセキュリティ戦略が閣議決定された場合には、遅滞なく国会に報告すべきと。

まさに、国権の最高機関である国会が常に監視をして、そして、本来、委員も御指摘のように、インターネットの世界というのは、自由で、オープンで、人々をつなげる、そういうものであるはずであります。ですから、管理の仕組みをつくるのではなくて、むしろ自由で、一人一人を保障する仕組みをつくる。

それは、私たちが政権時代に、この内閣委員会でも皆さんに大変お世話になりましたけれども、マイナンバー制度、これを仕上げていただきました。

マイナンバーについては、一昔前は大変なアレルギーがありました。国民に番号をつけるのかと。そうではないんだ、私たちは、国民の権利を守るための番号である、あるいは、みずからの情報を不正に利用、ストックされずに確認、修正が可能な、いわゆる自己情報のコントロール権、こういったことをしっかりと担保する仕組みであること、こういう五原則を出させていただいて、マイナンバーについて、皆様の御英断で今実施がされているわけであります。

今回のサイバーセキュリティーの問題についても、国民の権利の保障といったところで、自由なインターネット社会を守るため、あるいは自由な社会を守るための、そのための法案であるということを強調しておきたいというふうに思います。

ありがとうございます。

○近藤（洋）委員　ありがとうございます。

今、原口提案者のおっしゃった点は極めて重要な点だ、こう認識するわけであります。

やはり、インターネット社会というのは基本的に自由であるべきである、そして個人の権利も守る、この原則に立ちながら、そして同時にサイバーセキュリティーを確保していく、こういう仕組みということだろうと思いますし、その基本法に基づいて、これから閣法ができる。

宇宙基本法のときもそうでありましたが、宇宙基本法は、自民党では河村建夫先生なり、民主党では野田佳彦元総理、公明党では西先生等々が御活躍をされました。その後も、フォローアップ議員協議会というものをつくってチェックをしております。サイバー基本法においても、やはりそうした枠組みをつくりながら、政府、もちろん、当内閣委員会、国会においての機能も必要でありますし、そうした形でしっかりとチェックをすることが大事だ、そして推進することが大事だということを申し上げておきたい、こう思います。

官房副長官、お忙しいところ来ていただいております。

先ほど、平井議員の方からも、国会がピッチャー役として基本法の形で方針をつくりました、キャッチャーが政府です、こういう御発言がございました。

やはり、東京オリンピックというものに対してきちんと対処しなければいけない、我々もそう思っております。大事な一つのエポックメーキングのことであるし、これが大変なことになってはいけないということもありますし、また、それに限らず、サイバーセキュリティー確保のためには、体制整備及び一定の予算確保が肝要かと思いますが、こうした体制、予算確保について、きちんとした、恒常的にある程度手当てが充てられる

必要があろうかと思いますが、情報セキュリティセンター、ＮＩＳＣを所管する副長官としてどのように対応するお考えか、基本法成立後、成立すると仮定して、どうするおつもりか御答弁いただけますでしょうか。

○加藤内閣官房副長官　まず、サイバー攻撃への対応については、国家の安全保障、危機管理という大変重要な課題でありまして、本法案はまさに時機を得たものということで、この法案の取りまとめに当たっていただきました近藤委員初め関係の委員の方々、また、提案をしていただいた六会派の皆さんに改めて敬意を表させていただきたいと思います。

　その上で、今、政府としての取り組みということでございますが、今申し上げた情報セキュリティーの確保というのは、国家安全保障、危機管理のみならず、今私どもが取り組む成長戦略の重要な柱であります、世界最高水準のＩＴ社会の実現のためにも大変必要不可欠なものだというふうに認識をしております。

　そうした観点から、昨年六月に、情報セキュリティ政策会議においてサイバーセキュリティ戦略を策定し、政府機関や重要インフラの情報セキュリティー水準の向上、また、サイバー攻撃への対処体制の充実強化、人材育成をこれまでも推進してきたところでありますが、さはさりながら、今、さまざまな手口が大変複雑、巧妙化しているということ、あるいは、スマートフォン等サイバー攻撃の対象となり得る情報通信機器の範囲が拡大するなど、我が国のサイバー空間を取り巻くリスクはまさに拡大している、深刻化している、こういうふうに考えております。

　そういう意味で、この法案をこれから御審議いただき、成立していただいた中で、政府としても、サイバー攻撃の対処体制の充実強化、すなわち、必要な人材、予算の確保にしっかり努めていきたい、こう思っております。

○近藤（洋）委員　あわせて副長官にお伺いします。

　今回、行政機関との関係においては、我々民主党側の提案をさせていただき、一つは、関係府省がサイバーアタックを受けた場合、なかなかきちんとした情報をＮＩＳＣに開示しないケースもある。恥ずかしいとは言いませんけれども、なかなか表に出さない。それによって対処がおくれるケースもあると。したがって、今後はきちんと情報を提供しなければいけないという形で、与党提出の法律に対して、さらに強い権限をＮＩＳＣに持たせるような形で我々は提案をし、そして、共同提案で受けとめていただきました。

　これは、政府の、行政の中の話なんですが、さらに伺いたいのは、この立法機関及び司法機関のサイバーセキュリティーの確保なんですね。これは、行政の中はそういう形でいいんですが、司法機関と立法府、ここはやや微妙な関係になるわけであります。ここについて、しかしながら、行政、司法及び立法府についてもサイバーアタックが行われるわけでありまして、これに対してどう協力体制を整えていくのか、この点に限って、副長官、お答えいただけますでしょうか。

○加藤内閣官房副長官　今お話ありましたサイバーセキュリティーの確保において、関係省庁の連携は大変重要でありますし、この法案で関係行政機関の資料提出義務等が規定されたということは、一層そういう方向に進んでいけるもの、こういうふうに考えます。

　その上で、今、立法府と司法府との関係がございます。これも大変重大な、またよく連携をしていかなきゃいけないテーマであります。私どもの方も体制をしっかり強化する中で、情報共有により得られる知見、技術、私どもの中でのこういったものを、立法府また司法府とよく情報交換しながら、お互いの対策の向上を図っていくように努めていきたいと思っております。

○近藤（洋）委員　ぜひ、ここは大事な点なので、もちろんそれぞれ、立法府の独立性、司法の独立性に十分配慮をしつつ連携をしていただきたい、こう思うわけであります。

　また、副長官にお伺いをします。

　国の機関だけではなくて、やはり民間、サイバー攻撃に対応するためには、民間企業も含めたオール・ジャパンの取り組みが必要かと思います。第一点には、その民間からの人材登用を含めたＮＩＳＣとの人材交流が重要かと、こうも思いますし、これの必要性についてどうか。また、民間との共同開発も含めた技術の開発について、こうした民間との協力体制を一層深めるべきと、このように考えますが、この二点について、いかがお考えでしょうか。

○加藤内閣官房副長官　先ほど申し上げましたように、サイバーセキュリティ戦略にのっとって、いろいろ推進させていただいておりますけれども、特に人材育成や技術開発というのは、大変、このサイバーセキュリティー確保における基盤でありますし、官民挙げての体制強化はまさに急務であるというふうに認識しておりまして、民間との人事交流、あるいは技術の共同開発など、これまでも進めてきているところでありますけれども、さらに積極的に推進していきたい、こういうふうに考えております。

○近藤（洋）委員　時間が参りましたので、ここは要請だけに終わりたいと思いますが、副長官、特に民間のインフラ分野、私、ちょっと心配しているのは電力なんですね。

　電力システム改革、我々、民主党政権下で提案をし、今の政権で具体的な電力システム改革の第一弾の法案、第二弾の法案が成立をいたしました。発電と送電の分離、これは、これ自体、我々は正しいことだと思っています。ただ、同時に、これによってスマートメーターが急速に普及をいたします。これまでは、閉じた発送一貫の中で、閉じたシステムですから、サイバー攻撃にはある意味では強かった、こう想像されるわけですけれども、これからスマートメーターが急速に普及して、そして発送電が分離した中で、我が国が、この電力システムにおいて、サイバー攻撃についてどう対処するか。これは非常に大事なテーマになると思いますし、これに対する対処は相当腰を据えてやっていかなければならない。

　これまでは電力業界も力がありましたから、ある程度のことができたとは思うんですけれども、なかなかそうはならなくなってくる、こう思いますので、この分野、電力システム改革の中でサイバーセキュリティーをどう確保するかということについて、特に配慮してシステムを開発していただきたい、協力をしていただきたいということを要請して、時間ですので、私の質問を終えたいと思います。

○柴山委員長　次に、中丸啓君。

○中丸委員　中丸啓でございます。よろしくお願いいたします。

　質問に入る前に、一つ申し上げておきたいことがあります。

　何事にも侵されることのないセキュリティーの環境を実現することを考える上で、究極の目的、何事にも侵されない、これが究極目的でございます。その中で、絶対にあってはならないのは、外部からの不正侵入、それから情報の改ざん、それから情報漏えい、大きく分ければこの三つだろうと思います。

　その部分に近づけていくには、完全独立というのが一つのキーワードになると思います。それに近づけること、これが、ネットワークを考える上での、一種の矛盾する、ネットワークというのは広がりですけれども、セキュリティーというのは究極は完全独立です。この二つの相対するものを考えることがまず一つ重要だろうということをお伝えしたいと思います。

　そのためには、情報というのは、当然、オープンにするものとクローズにするものが出るわけで、まず、その情報をセグメント化する作業、これが非常に重要になります。

　大きく分けて二つに分かれます。極論を言えば、多少攻撃に遭っても致命的な被害にならない情報と、絶対に攻撃されてはいけない情報、大きく分けるとこの二つに分けます。前者にあっては

パソコンのネットワーク、後者は大型汎用機のネットワーク、こういうふうに考えていただければよろしい。前者はオープンＯＳを使ったネットワークであり、後者はクローズドＯＳの大型汎用機だというふうに理解をしていただきたいと思います。

海外、国内を問わず、サイバー攻撃の脅威にさらされているネットワーク環境と、その環境から完全独立の汎用ネットワーク環境の二重ネットワーク環境が、これから実現していくセキュリティーを考えた上でのネットワークです。当然のことながら、データベースに関しても、オープンデータベースとクローズドデータベース、この二つを実装すべきであろうと思います。

そのためにも、全てが閉ざされたシステム環境と一対一の専用回線、これで結ばれるネットワーク網が必要条件であり、それを実現できるシステムは、大型汎用機で構成されたネットワークシステムしか基本的に現状では考えられないと思います。

どんなウイルスチェックソフトを使っても、先に攻撃を受けるのは間違いなく、後手に回るわけです。その後のウイルス対策にならざるを得ない。受けた後の対策では、どれほどの負荷がかかるかを想像するのも恐ろしいことであります。攻撃を受けない環境をつくることが絶対に必要であり、後悔のないシステム運営とセキュリティー対策を実現していただきたいということを初めに申し上げておきます。

本日付の産経新聞の朝刊に載っていましたが、サイバー攻撃の九割が中国サイトへ接続したものであり、中央省庁や防衛関連企業など三十余りが平成二十一年以降攻撃を受けた問題で、コンピューターウイルスに感染したパソコンは国内で百台以上に上り、うち九割が中国のサーバーやサイトに強制接続されていたことが捜査関係者への取材でわかったというのがあります。中国が意図的にやっているかどうかという証明にはなりませんが、中国のサイトを九割が経由しているというのは事実であろうということが読み取れると思います。

そういった中で、総則にもありましたように、目的に、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。」というふうに記載されておりますけれども、まさにこの一文が重要と、我々、いわゆる石原新党では考えております。

そういう意味では、もう既に、先ほどのアタックも含めて、サイバーセキュリティーというか、サイバー戦争が既に行われているというまず前提を持ち、そういう認識のもとで理念を構築し、システム、法案を考えていかないといけないと思うんですけれども、松田提出者にお伺いします。今回はどのような理念で構築されましたでしょうか。

○松田委員　お答えいたします。

中丸委員御指摘のように、この問題は、まさにサイバー戦争、安全保障の最も重要な問題であろうと思っております。

先ほど平井先生からも御答弁がありましたように、政府機関への脅威件数だけでも、一分当たり二回の頻度、二〇一二年度は約百八万回。民間も含めて、情報通信だけでなく、金融、航空あるいは鉄道、電力、医療、物流、日本の重要インフラがやられてしまいますと、社会の機能が麻痺してしまう。まさに、国民の生命と安全、財産を守るという安全保障の基本というところの基本にこのサイバー攻撃対策があろうかと思っております。

冷戦体制後、安全保障の概念、いわゆる国家間の戦争から、戦争脅威というものも非常に広がっている、任意の民間集団でありますテロリストもそうであります。この情報化時代には、サイバーということも問題になってまいりました。とりわけ日本では、これからマイナンバー制度というのが導入されることになります。そうなりますと、このマイナンバー制度で、生活がいろいろな面で個人番号なしには成り立たなくなっていく、これがサイバー攻撃を受けると大変な事態になっていくということでございまして、社会の利便性の向上と、一方で脅威も増大しているという状況にあると思います。

本基本法案でも、御指摘のように、目的規定のところに安全保障への寄与ということが明確にうたわれているところでございます。

今、石原新党というお言葉がございましたが、この私も石原新党のグループの方に属する立場として申し上げますと、やはり国家機能の強化といいますか、これは強い国家基盤なくしては維新が標榜してきた自立ということもあり得ない。マイナンバー制度もサイバーセキュリティー対策も国家基盤の重要インフラである、これは車の両輪であると思っております。

平時の行政はどんどん地方に移していく、その受け皿として道州制ということを考える一方で、国家は、やはり有事を想定した日ごろの対応というところに集中、特化して国家機能を強化していくということが、これが維新が当初から掲げてきた、強く、賢く、したたかな国づくり。私どもは、石原グループは、こういった維新の会が有権者と約束をした理念、原点を継続、発展、進化させるというグループであると思っておりますので、本法案もその中核の一つになるものだと考えております。

以上です。

○中丸委員　ありがとうございます。

続きまして、提出者平井議員にお伺いします。

今、松田委員の答えにもありましたけれども、これは安全保障であるという観点が非常に必要だと思います。そういう意味では、国民の一人一人の認識を深め、自発的に対応というふうに起案されていると思うんですけれども、これは非常に大切なんですが、言葉で書くと簡単なんですけれども、これは実際、国民一人一人の認識を深め、自発的に対応できるようにするには、非常に難しい課題でもあると思います。

今後それについての取り組みをどのように進めていくか、教えていただければと思います。

○平井委員　私も委員と問題意識は全く同じであって、今回この法案で「サイバーセキュリティ」という言葉を定義するということが非常に重要だと思いました。

というのも、やはりサイバーセキュリティーというと、一般の方々は、他人事で、自分が巻き込まれるような世界じゃないと思っている方々が実は多いと思うんですね。しかし、意識してもせずとも、今や全てのものがインターネットを使うことが前提で動く社会になってしまっている。

私は、時代認識として、一九八〇年ぐらいから始まったコンピューターとネットワークによる革命といいますか、産業革命、第三次産業革命と言ってもいいものの真っただ中にいて、つまり、これはデジタル化とグローバル化に全ての国民がもう巻き込まれてしまっていて、恐らくこれはもうやめられない、とまらないんだと思います。そういう状況の中で、やはり国民の一人一人の認識を深めるということは非常に重要だと思っています。

そして、この法文の中にいろいろ書かせていただいています。

まず、第九条において、サイバーセキュリティーの確保は基本的には国民一人一人が行うことであるため、スマートフォンの普及等に伴いリスクが拡散する中、各自が広くサイバーセキュリティーに関する関心と理解を深め、サイバーセキュリティーの確保に必要な注意を払うよう努めることが必要であるという旨の条文を規定しました。

そして、他方、実際には、サイバーセキュリティーの確保に関して、国民の自発的対応では限界があることから、本法案において、国が国民一人一人からのサイバーセキュリティーに関する相談に応じ、情報提供、助言を行う旨の規定も入れました。これが第十五条第二項です。

加えて、国民一人一人のサイバーセキュリティーに関する理解や関心の増進等のため、国

は、サイバーセキュリティーに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるよう規定しているのが第二十二条第一項です。

具体的には、こうした施策の推進のため、国は、重点的かつ効果的にサイバーセキュリティーに対する取り組みを推進するための期間の指定、先ほども話がありましたが、情報セキュリティ月間や、サイバー訓練の日、三月十八日等の必要な施策を講ずることを規定しています。それが第二十二条第二項です。

それだけではまだ十分ではなくて、やはり、我々国会議員一人一人も、こういう問題、今までなかなか政治的な対話集会では出てこなかったんですが、スマートフォンというのは電話じゃないよ、皆さんはスーパーコンピューターを持ち歩いているんだよというようなことから、我々自身も広く国民に対して情報発信していく必要があろうかと考えています。

○中丸委員　それでは次に、結局、我が国の法案をこれから組み立てていくわけですけれども、実は、インターネットには国境はありません。そういった意味では、国際社会のルール構築というのが非常に重要になります。ただ、このルール構築には一つの大前提が必要だと私は思っています。

具体的に言いますと、相手が信頼できる国である、信頼に足る者である。というのは、お互いに、情報交換、さまざまなことをやっていかないといけないですから、かといって我が国一つでできることではなくて、連携が必要ですが、信頼できるというキーワード、これは非常に大事だと思います。また、アジアの中で我が国がリーダーシップをとっていく必要があると思いますが、提出者松田議員、いかがでしょうか。

○松田委員　中丸委員御指摘のとおりだと思います。

現在の国際社会の課題全体を考えてみましても、ルールを守らない国々が一部にある。そして、それに対抗して、ルールを守るという価値観を持った国々がどうやって連携、協調をして対応していくかということが、経済面においても安全保障面においても、両面において大きな課題になっていると思っております。

経済面においては、その一環として、同盟国である米国と一緒にＴＰＰというものを推進している。安全保障面においても、日本は、世界の中でも最も緊密な同盟国であります米国と連携しながらアジアのルールをつくっていくということは、いろいろな面で、日本は、その中でもアジアを先導する国になっていくということが肝要であろうと思っております。

なお、この基本法案におきましても、二十三条で、「国際的な規範の策定への主体的な参画」、あるいは三条で、「国際的な秩序の形成及び発展のために先導的な役割を担う」ということは規定しておりますし、また、二十三条では、「開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力」ということが書いてございます。

ただ、アジアの国々との連携をするに当たっては、委員おっしゃるように、サイバーというものの特殊性に鑑みまして、信頼関係が構築できる、まさに、ルールを守る、そして、市場経済、自由主義という価値観も含めて共通の基盤を持った国々との間でまずは連携関係を結んでいくべきだろうと思っています。

なお、日本は、サイバーに関して見ますと、必ずしも最先進国ではありません。二〇〇七年に、先ほどもありました、エストニアが、サイバー攻撃、人類史上初の大規模な攻撃を受けて、翌二〇〇八年にＮＡＴＯサイバーセキュリティセンターというのが設けられております。例えばこういったサイバーの先進国とも協調しながら、アジアに新しいルールをつくっていくことを先導していくことが大事だろうと思っております。

以上でございます。

○中丸委員　ありがとうございます。

今、ルールを守らない国、要は、信頼できない国というのはルールを守らない国でございます。

逆に、今エストニアのことも出ましたけれども、米国、それからセキュリティーで非常に最先端を行っているイスラエル、それからイギリス、こういった国々と協調していくことが非常に大事だと思いますけれども、また、逆に、信頼できない国というのも認識しておく必要があると思うんですけれども、両提出者にお伺いします。

信頼できない国、今わかるところがあれば教えてください。

○平井委員　信頼できない国はどこかということに関して、私、今すぐに明確な答弁をできる立場にはございませんが、ただ、グローバル化とデジタル化というお話をさせていただきましたが、一体、どこから攻撃を受けているのかというのが実は本当になかなか解明できないんですね。

先ほど中国のサーバー経由の事象が多いという話がありました。確かに、今霞が関を攻撃しているいろいろな攻撃の約五割は中国のサーバー経由ということになります。その理由はいろいろあるとは思うんですけれども、まず一つには、世界で一番サーバーの数が多いんですね。急激にインターネットが普及している。それぞれのサーバーのデータセンターの要するにセキュリティーレベルが必ずしも高くないんですね。ですから、そういう意味で、国だけの問題ではなく、いろいろな、グローバルな社会の中において我々が対処しなきゃいけない相手はたくさんいるんだというふうに思っています。

そして、先ほども私、一度、お話をさせていただきましたが、サイバーセキュリティーに関する国際的な枠組みというのは、実は、あるようで余りないんですね。平成十三年にブダペストで署名式典が行われたサイバー犯罪条約が今のところ唯一なんです。これはヨーロッパ、アメリカ、日本など約四十カ国が署名していますが、中国とロシアは署名していないんです。そういうふうなこともあります。

そのほかに、我々が信頼できる国というようなことで、当然、同盟国の日米サイバー対話、また、英国との二国間協議を今積極的に進めていますし、先ほど委員がお話しになりましたエストニア。大統領が来日されたときに、安倍総理との会談の中で、サイバーに対する定期協議、これを立ち上げることにもなりました。

ですから、我々も、この法案を成立させた上で、国際的にサイバーのいろいろな協議に対して主導的な役割を担えるようになればよい、そのように願っております。

○松田委員　先ほど、ルールを守るという価値観を持った国々とそうでない国というふうに申し上げました。ルールを守っていない国というのは、最近の状況を見ましても、あえて申し上げなくてもおわかりのとおりかと思います。

それと、私、思いますに、やはり我々が連携、協調すべき相手というのは、これは聞いた話でございますけれども、サイバー対策が真にできる国は、サイバー攻撃を受けた経験のある国か、あるいはみずからサイバー攻撃を行うことができる能力を持った国であるというふうに聞いたことがあります。そういったところとも緊密な連携をとっていくことが必要であると思っております。

○中丸委員　ありがとうございます。

国名は挙げられないとは承知の上でお伺いしましたので、後は皆さん御想像いただければと思います。

あと、イスラエルとはぜひとも続けていただきたいと思いますし、十一月にイスラエルでそういう国防セキュリティーに関する国際会議、そういったものもあります。そういったところへの出席というのもぜひ考えていただきたいと思います。

それから、もう時間もなくなりましたので、最後にまとめてちょっと申し上げます。一問ずつお願いします。

平井提出者には、活力ある経済社会の構築に情報通信技術の活用というのは不可欠であります、

その中で、情報活用をすればするほど、セキュリティーというのは下がってくるわけです、このバランス感覚をどのように捉えられているかというのを平井議員にお伺いします。

そして松田議員には、最後は、それをやるのは人です、仕事は人なり、人材確保、育成というのは非常に大切なんですけれども、海外からの専門人材も含めて、報酬、それから雇用契約の体系、こういうものを考えなければいけないと思うんですけれども、それについての御所見を最後にお願いします。

○平井委員　委員の御指摘は非常に重要だと思います。

先ほど、私の時代認識が、まさに第三次産業革命の真っただ中にいて、その中で我々は成長戦略を組み立てていかなきゃいけないと考えたときに、当然、情報通信技術の活用とサイバーセキュリティーというもののバランス、これが一番難しいし、そこを何とか一番ベストな方法を考えなければならないというふうに考えています。

今回の法律の中で、ＩＴ総合戦略本部、サイバーセキュリティ戦略本部との連携というのは、まさにそこのところだと考えています。車の両輪として、やはりそこは補完し合わなければならないというふうに思っていますし、サイバーセキュリティーという概念だけではなく、例えば、パーソナルデータの扱いや個人情報保護法等、法律的な手当てというものも、当然これから取り組まなきゃいけないと思います。

また一方、成長戦略の柱の一つの中に入っているビッグデータの利活用というようなものも、これも、情報をどうやって流通しやすくするかという観点から、またいろいろ考えなきゃいけない。

しかし、その両方とも、その前提にサイバーセキュリティーというものが確保されていなければ意味がないんですね。そういう意味で、今回、やはり、両方のバランスを図っていくというのは、まさに我々立法府にいる人間、また行政にいる方々とも十分に議論をし、また民間の方々とも協力しながら、常にベターな方法を考えていくべきだと考えています。

○柴山委員長　松田君、質疑時間が終了しておりますので、簡潔にお願いします。

○松田委員　先ほど、攻撃を受けた経験のある国ということで、エストニアを申し上げました。

私も、昨年、内閣委員会で平井先生と一緒にエストニアを訪れまして、その経験の中で最も大事なものは何かという質問をさせていただきましたが、サイバー攻撃の対策を、単なる技術者のレベルの問題ではなく、政策決定のレベルできちっとそういう人材に活躍してもらうということが極めて重要であると。それから、特定のソリューションに頼らない、一旦つくられたソリューションも傷つきやすく脆弱なものであるという認識、つまり、不断にそういった政策決定のレベルでその人材が活躍する場を提供しなければいけないと。

また一方で、そういった人材はどういうところにあるかと。先ほど申し上げましたように、サイバー攻撃ができる能力のある国々というと、アメリカやイギリス、あるいはイスラエルといったようなところに限られるというふうに聞いております。

したがいまして、日本では人材がそもそも国内で不足しているわけでもございますし、何としてもこういった人材にそれなりの場で活躍していただくことが喫緊の課題だろうというふうに考えております。

その際に、日本のいろいろな意味での公務員制度の制約というものも、これは非常に、報酬も含めて弾力的に考えていく。まさに、この法案にもございますけれども、魅力ある職場にするということを、私は、公務員制度改革、先般成立いたしましたが、まさに、身分から職業へ、魅力ある職場にしていくというのが公務員制度改革の重要な論点であると、内閣委員会でも何度も質疑をさせていただいたところでございます。

まさに、サイバーセキュリティーの人材をどうやって有為な外国人を含めて確保していくかということが、こういった公務員制度改革の一つのかなえの軽重が問われてくるところになろうかと思っております。

以上でございます。

○柴山委員長　中丸君、質疑時間終了です。

○中丸委員　はい。ありがとうございました。

○柴山委員長　次に、赤嶺政賢君。

○赤嶺委員　日本共産党の赤嶺政賢です。

今回、委員会提出にしようと提出されている法案の草稿についてでありますが、我が国の安全保障にかかわる重要な内容を含んでいるものです。こうした重要な法案を国会の会期末に、しかも、わずか一時間四十分の審議でスピード成立を図る、これ自身はやはり言語道断だと我々は考えております。我が国の安全保障に責任を負う官房長官や外務大臣、防衛大臣に対する質疑もありません。

安全保障に関する法案の審議というのは、政府・与党とは反対の立場からではあれ、私も長くそういう審議にかかわってきました。そういう点では、これだけの重要な法案がこんな簡単に成立していいのかという点では、非常に大きな疑問であり、前代未聞のやり方だということを厳しく指摘しておきたいと思います。

そこで、まず提出者に伺いますが、今回の法案は、第一条の目的、ここには、「経済社会の活力の向上及び持続的発展並びに国民が」「安心して暮らせる社会の実現を図るとともに、」といたしまして、「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。」このようにしております。

一方、第十八条は、「国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化」と、その他の「必要な施策を講ずるものとする。」施策を明らかにしております。

「サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるもの」とは具体的にどういうものを想定しておられるのか。また、「関係機関における体制の充実強化」その他の「必要な施策を講ずるものとする。」ということは、どの機関のどのような体制を充実強化することを想定しているのですか。

○平井委員　冒頭、今回の法律の提出のやり方、そして審議のやり方が不十分だという御指摘をいただきました。その御指摘は真摯に受けとめたいとは思いますが、この法案が提出されるまでの長い経緯を考えますと、実は、もう各党の調整だけではなく、我々が野党の時代、民主党さんが政権与党の時代からこの問題提起をさせていただき、議論の積み上げの中で、今回、立法府の意思として出てきた法律というふうに思っています。

そこで、この法律そのものの基本的な考え方、確かに国家の安全保障というものにかかわる問題ですが、我々の基本的な認識は、二〇〇〇年に成立させたＩＴ基本法、その中にセキュリティーの概念というものがなかった。つまり、情報とネットワークを民間の力でどんどんつくっていくんだといったときに、言葉としては、民間によって安全なインフラをつくるという、その安全なという言葉、この言葉は実はサイバーセキュリティーのことを意味していたわけではありません。

その後、二〇〇五年あたりから、サイバーセキュリティーという問題に政府としても各政権がいろいろ取り組んできたんですけれども、もうここに来てＩＴ基本法のときとは全く時代が変わってしまったので、ＩＴ基本法を補完するような形で何とか立法府の意思を示せないかというところが原点にあった。ですから、「サイバーセキュリティ」という言葉の定義にもこだわったということでございまして、十分な審議がこの場でできなかったと言いますが、その背景にはそういう議論の積み上げがあってここに至っているということも御理解をいただければと思っています。

そして、先ほど御質問の第十八条の「我が国の安全に重大な影響を及ぼすおそれがあるもの」と

はということでございますが、これは、例えば大規模なサイバー攻撃による重大な緊急事態等が想定されるということであります。

そして、「関係機関」についてのお尋ねでございますが、「関係機関」とは、警察庁、外務省、防衛省等であり、「体制の充実強化」とは、これらの機関におけるサイバーセキュリティー確保のための必要な体制整備を示すものであります。

そして、「関係機関相互の連携強化及び役割分担」とは、近年サイバー攻撃が複雑化、巧妙化する中、引き続き政府が一体的かつ有効に大規模サイバー攻撃事態等に対処するため、関係府省の連携強化や役割分担の明確化を引き続き確保していくということを我々は考えているんですが、実はアメリカも、例えばイギリスも、要するに、情報共有と連携というものに関して、サイバーに関して、いろいろと議論があります。つまり、インフォメーションシェアリングという考え方がサイバー対策にはやはり一番重要だと。省庁の縦割りというものがやはり障害になっていたことも事実なんですね。そういう意味で、今回、立法府においてこのような法律の提案ということに至ったんだと思います。

○赤嶺委員　次は、国家安全保障会議との緊密な連携、これについて伺っていきます。

「国家安全保障会議との緊密な連携を図るもの」として、「我が国の安全保障に係るサイバーセキュリティに関する重要事項」、これはどのようなものですか。

○平井委員　ＮＳＣ、「国家安全保障会議との緊密な連携」については、本法案において、「我が国の安全保障に係るサイバーセキュリティに関する重要事項について」行うものとされています。

その「重要事項」の例としては、外国政府等が関与して我が国に対してサイバー攻撃が行われた場合を考えています。

具体的には、サイバーセキュリティ戦略本部がサイバー攻撃の端緒等を把握し、その分析等を行った結果、外国政府等が関与している可能性が高いと判断する場合等について、同本部が国家安全保障会議に対しその情報を提供すること等を行うということが考えられます。

○赤嶺委員　この法案の二十五条の第二項で、「本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。」としております。一方、二十五条四項では、「我が国の安全保障に係るサイバーセキュリティに関する重要事項」、このようになっておりますが、第二項は、「我が国の安全保障に係る」という限定が置かれておりません。

国家安全保障会議は、我が国の安全保障に係る問題に限らず、サイバーセキュリティー全般について意見を言うことが想定されているのですか。

○平井委員　法案の第二十五条第二項においては、本部がサイバーセキュリティ戦略の案を作成する際、ＩＴ総合戦略本部と国家安全保障会議にあらかじめ意見を聞くことを求めているのは、そのとおりでございます。

しかし、国家安全保障会議は、我が国の安全保障に関する重要事項を審議する機関であることから、その所掌の範囲において意見を言うことが可能になるという意味です。これはＩＴ総合戦略本部についても一緒でありまして、そのため、御指摘のように、これらの機関がいかなる事項でも意見を述べるわけではなくて、その所掌内において戦略の案を作成する際に意見をすることができるというふうに考えています。

○赤嶺委員　その国家安全保障会議についてもっと聞いていきたいんですが、国家安全保障戦略の中には、サイバーセキュリティーの強化、これはどのように位置づけられているのですか。これは政府に聞きたいと思います。

○武藤政府参考人　お答えいたします。

国家安全保障戦略におけるサイバーセキュリティーの位置づけということでございますけれども、サイバー空間は、国際公共財として、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっておりまして、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障の観点からも不可欠でございます。

国家安全保障戦略においては、そのような認識を示した上で、サイバーセキュリティーの強化として、まず、サイバー空間を守り、その自由かつ安全な利用を確保するとともに、サイバー攻撃から我が国の重要な社会システムを防護するため、国全体として、組織、分野横断的な取り組みを総合的に推進して、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図ることとしておりまして、そのための各種施策を掲げてございます。

政府としては、サイバーセキュリティー分野も含め、国家安全保障に関する政策を一層戦略的かつ体系的なものとして実施してまいりたいと思っております。

○赤嶺委員　平井議員に伺いますが、今のＮＳＣの中でのサイバーセキュリティーの強化についての位置づけは、政府と全く同じ認識であるというぐあいに理解してよろしいですか。

○平井委員　安全保障に対する考え方は、政府が考えることだと考えています。

我々は、先ほどもこのお話を冒頭させていただきましたとおり、今のＩＴ基本法によって、ここまで進んだこの社会の中において、サイバーセキュリティーというものが国民にとっても大きな脅威になっているということから、やはり安全に情報が流通し、その恩恵を享受できる社会をどうやってつくっていくかということが一番重要な問題だと思ってこの法案をつくっています。

その上で、サイバーというものは、国際的、グローバルに、そして国の枠を越えて、何が起きるかわからない、また、そういうサイバーの攻撃がリアルな社会と表裏一体になっているということに鑑みて、そこは当然、安全保障というところとつながってくるという理解であります。

ですから、今回、広く安全保障ということを言っているわけではなくて、我々は、サイバーに係る分野に関してはＮＩＳＣの方で情報をきっちり把握して、トータルとして安全保障に資するようにしたいということであり、ＮＳＣの判断というものはＮＳＣの判断であるというふうに考えています。

○赤嶺委員　法文の中にも、安全保障に資するという大きな目的がうたわれているわけですね。

そこで、政府にもうちょっと聞いていきたいんですが、ＮＳＣの中では、サイバー防衛協力を、関係国と情報共有の拡大を図る、そういう項目もあるわけですが、現在、アメリカとの間でサイバー防衛協力はどのような形で推進しているんですか。

○鈴木政府参考人　お答え申し上げます。

日米の防衛当局間におきましては、日米サイバー防衛政策作業部会というもの、ＣＤＰＷＧと申しますけれども、これが、小野寺防衛大臣とヘーゲル国防長官の指示に基づきまして、サイバーセキュリティー分野における日米防衛協力を一層促進するという観点から、昨年十月に設置されております。そして、本年二月に第一回会合を開催したというところでございます。

第一回会合におきましては、両国国防当局間のサイバー分野における各種の取り組みの現状などについて認識を共有するということとともに、今後の協力分野に関しまして、政策レベルも含めた日米の情報共有のあり方、人材育成における連携など、包括的な意見交換を行ったところでございます。

○赤嶺委員　去年の2プラス2の中での防衛協力の推進の方向が出ているわけですが、今回、年末にガイドラインもいろいろ予定されております。このガイドラインの変更の中では、サイバー空間についてどのように位置づけていますか。

○冨田政府参考人　お答えをいたします。

昨年の十月に行われました2プラス2におけるサイバーセキュリティーの位置づけでございます

けれども、この共同声明におきましては、新たな戦略的領域としてのサイバー空間の重要性について認識を共有したということでございます。その上で、先生今お話がございましたけれども、日米防衛協力のための指針の見直し作業を初めといたしまして、サイバー分野を含む幅広い分野での安保・防衛協力をさらに進め、安保体制の抑止力、対処力を強化していくことで一致したということでございます。

具体的にガイドラインの中でこの問題をどう扱っていくかということについては、いまだに政府間で検討を進めているところでございますので、まだちょっとその結論をお話しするには時期尚早かというふうに考えております。

○赤嶺委員　この法案が国の安全保障についても重要な役割を果たすものであると同時に、NSCの中でもサイバーセキュリティーが位置づけられ、その中でアメリカとの関係も言われ、2プラス2でも緊密な連携を図ってきた。

そのアメリカのサイバー防衛の政策について確認をしていきたいんですが、アメリカでは、サイバー攻撃に対して自衛権を発動する、あるいはサイバー空間での攻撃を行う、いろいろな戦略が言われておりますが、アメリカのそういうサイバー戦略について、政府に、説明していただけますか。

○柴山委員長　冨田北米局長、質疑時間が終了しますので、簡潔に御答弁ください。

○冨田政府参考人　米国のサイバー戦略というお尋ねでございますけれども、外務省としてお答えできる範囲で申し上げますと、米国は、サイバーセキュリティーに対する脅威を、国家として直面する最も深刻な国家安全保障、公共の安全及び経済的課題の一つとして認識しているということでないかと思います。そういう認識のもとで、例えば二〇一〇年の国家安全保障戦略、それから本年の三月に発表された四年ごとの国防計画の見直し、QDR等でより具体的な政策が打ち出されているというふうに承知をしております。

○柴山委員長　赤嶺君、質疑時間終了です。

○赤嶺委員　かなり短い時間で、しかし、この法案が国の安全保障政策にも重要な関係を持っているということは明らかであります。

先ほど、サイバー攻撃をできる国との連携というお話もありましたが、平井議員は、積み上げてきた結果の今回の法案だというお話もありましたけれども、こんな大事な議論や中身が二十分で全然明らかにできるはずもないし、そういう審議のやり方、政府と全く同じ安全保障観を持っているわけですから、これは安易にそういう法律の提出がやれるようになったら非常に国の進路を間違うのではないかということを強く申し上げて、私の発言を終わります。

○柴山委員長　これにて発言は終わりました。

お諮りいたします。

本起草案を委員会の成案と決定し、これを委員会提出の法律案と決するに賛成の諸君の起立を求めます。

〔賛成者起立〕

○柴山委員長　起立多数。よって、そのように決しました。

なお、本法律案の提出手続等につきましては、委員長に御一任願いたいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○柴山委員長　御異議なしと認めます。よって、そのように決しました。

○柴山委員長　この際、平井たくや君外七名から、自由民主党、民主党・無所属クラブ、日本維新の会、公明党、みんなの党及び生活の党の共同提案によるサイバーセキュリティの確保に関する件について決議すべしとの動議が提出されております。

提出者から趣旨の説明を求めます。近藤洋介君。

○近藤(洋)委員　ただいま議題となりましたサイバーセキュリティの確保に関する件につきまして、提出者を代表して、その趣旨を御説明いたします。

その趣旨は案文に尽きておりますので、案文を朗読いたします。

サイバーセキュリティの確保に関する件（案）

政府は、サイバーセキュリティ基本法の施行に当たっては、次の諸点について法的措置も含めて検討を加え、その遺憾なきを期すべきである。

一　具体的な施策

1　サイバーセキュリティ戦略本部は、国家安全保障会議、高度情報通信ネットワーク社会推進戦略本部、内閣危機管理監等と緊密な連携を図ることとするほか、サイバーセキュリティに関する幅広い分野の有識者の意見を十分に取り入れ、施策に反映させるよう努めること。

2　サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するための演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンターを中心として総合的に実施すること。

3　内閣情報通信政策監と連携して、サイバーセキュリティに関する施策の評価を定期的に実施すること。

4　政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、総合的かつ有機的な視点から策定すること。

5　大規模サイバー攻撃への対応要領を作成し、関係者の協力の下に行われる定期的な演習及び訓練を通じて実効性のある対応策の構築に努めること。

6　サイバーセキュリティ確保のため、サイバーセキュリティに関する技術の向上のための研究開発予算の充実等の取組を積極的に推進すること。

7　中小企業者その他の民間事業者におけるサイバーセキュリティの確保のための自発的な取組を積極的に促進すること。

8　国民一人一人が自発的にサイバーセキュリティの確保に努めることができるよう、必要な情報の提供及び助言その他の施策を積極的に推進すること。

9　地方公共団体が自主的な施策の策定及びその実施を推進できるよう、積極的な支援を行うこと。

10　内閣官房情報セキュリティセンターについては、サイバーセキュリティ対策を着実に実施するために必要かつ十分な人員、予算を継続的に確保し、サイバーセキュリティ戦略を積極的に実施すること。

11　サイバーセキュリティ戦略本部の事務のうち、監査、原因究明のための調査、府省横断的な計画及び関係行政機関の経費の見積り方針等の作成等について、迅速かつ効果的に行う体制を整備すること。

二　人材の育成及び登用

1　サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

2　国の行政機関等でサイバーセキュリティに係る事務に従事する者の関係府省庁及び民間企業等との積極的な人事交流を推進するとともに、過去の人事慣行にとらわれない人事評価の在り方を検討すること。

三　連携体制の整備

1　サイバー攻撃のもたらす被害の重大性に鑑み、国家安全保障会議等との連携の下、安全保障上の観点から迅速かつ実効性のある措置を講ずることを検討した上で、必要

な措置を講ずること。その際には、平素から危機管理、安全保障までを連続的に対応できる体制を整備すること。

2　サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

四　サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

五　二〇二〇年オリンピック・パラリンピック東京大会におけるサイバーセキュリティに関する事象に対処するための国内外の関係機関との連絡調整等を行う組織の在り方について、将来の推進体制を見据えて検討した上で、必要な措置を講ずること。

六　国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

七　立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。

以上でございます。

何とぞ委員各位の御賛同をお願いいたします。

○柴山委員長　これにて趣旨の説明は終わりました。

採決いたします。

本動議に賛成の諸君の起立を求めます。

〔賛成者起立〕

○柴山委員長　起立多数。よって、本件は委員会の決議とすることに決しました。

この際、本決議に対し、政府から発言を求められておりますので、これを許します。菅内閣官房長官。

○菅国務大臣　ただいまの御決議につきましては、その趣旨を十分尊重し、サイバーセキュリティーの確保に努めてまいります。

○柴山委員長　お諮りいたします。

本決議の議長に対する報告及び関係政府当局への参考送付等の手続につきましては、委員長に御一任願いたいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○柴山委員長　御異議なしと認めます。よって、そのように決しました。

次回は、公報をもってお知らせすることとし、本日は、これにて散会いたします。

午後零時二分散会

サイバーセキュリティ基本法案

サイバーセキュリティ基本法

目次

第一章　総則

（目的）

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

（定義）

第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

（基本理念）

第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

2　サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。

3　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するための取組を積極的に推進することを旨として、行われなければならない。

4　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。

5　サイバーセキュリティに関する施策の推進は、高度情報通信ネットワーク社会形成基本法の基本理念に配慮して行われなければならない。

6　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。

（国の責務）

第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責

務を有する。
（地方公共団体の責務）
第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。
（重要社会基盤事業者の責務）
第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
（サイバー関連事業者その他の事業者の責務）
第七条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
（教育研究機関の責務）
第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
（国民の努力）
第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。
（法制上の措置等）
第十条　政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない。
（行政組織の整備等）
第十一条　国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。

第二章　サイバーセキュリティ戦略

第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。
2　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。
一　サイバーセキュリティに関する施策についての基本的な方針
二　国の行政機関等におけるサイバーセキュリティの確保に関する事項
三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項
四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項
3　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。
4　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。
5　前二項の規定は、サイバーセキュリティ戦略の変更について準用する。
6　政府は、サイバーセキュリティ戦略について、その実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない。

第三章　基本的施策

（国の行政機関等におけるサイバーセキュリティの確保）
第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析、国の行政機関におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。
（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）
第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。
（民間事業者及び教育研究機関等の自発的な取組の促進）
第十五条　国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。
2　国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。
（多様な主体の連携等）
第十六条　国は、関係府省相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする。
（犯罪の取締り及び被害の拡大の防止）
第十七条　国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする。
（我が国の安全に重大な影響を及ぼすおそれのある事象への対応）
第十八条　国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする。
（産業の振興及び国際競争力の強化）
第十九条　国は、サイバーセキュリティの確保を

自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため、サイバーセキュリティに関し、先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化及び新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。

（研究開発の推進等）

第二十条　国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。

（人材の確保等）

第二十一条　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする。

2　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。

（教育及び学習の振興、普及啓発等）

第二十二条　国は、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるものとする。

2　国は、前項の施策の推進に資するよう、サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策を講ずるものとする。

（国際協力の推進等）

第二十三条　国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し、国際的な規範の策定への主体的な参画、国際間における信頼関係の構築及び情報の共有の推進、開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力、犯罪の取締りその他の国際協力を推進するとともに、我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策を講ずるものとする。

第四章　サイバーセキュリティ戦略本部

（設置）

第二十四条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二　国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

三　国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）に関すること。

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

2　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。

3　本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。

4　本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

（組織）

第二十六条　本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

（サイバーセキュリティ戦略本部長）

第二十七条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。

2　本部長は、本部の事務を総括し、所部の職員を指揮監督する。

3　本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一条の規定により提供された資料、情報等に基づき、必要があると認めるときは、関係行政機関の長に対し、勧告することができる。

4　本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、その勧告に基づいてとった措置について報告を求めることができる。

5　本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、内閣総理大臣に対し、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう意見を具申することができる。

（サイバーセキュリティ戦略副本部長）

第二十八条　本部に、サイバーセキュリティ戦略副本部長（以下「副本部長」という。）を置き、国務大臣をもって充てる。

2　副本部長は、本部長の職務を助ける。

（サイバーセキュリティ戦略本部員）

第二十九条　本部に、サイバーセキュリティ戦略本部員（次項において「本部員」という。）を置く。

2　本部員は、次に掲げる者（第一号から第五号までに掲げる者にあっては、副本部長に充てられたものを除く。）をもって充てる。

一　国家公安委員会委員長

二　総務大臣

三　外務大臣

四　経済産業大臣

五　防衛大臣

六　前各号に掲げる者のほか、本部長及び副本部長以外の国務大臣のうちから、本部の所掌事務を遂行するために特に必要があると認める者として内閣総理大臣が指定する者

七　サイバーセキュリティに関し優れた識見を有する者のうちから、内閣総理大臣が任命する者

（資料提供等）

第三十条　関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない。

2　前項に定めるもののほか、関係行政機関の長

は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。

（資料の提出その他の協力）

第三十一条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の理事長、特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。）であって本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。

2　本部は、その所掌事務を遂行するため特に必要があると認めるときは、前項に規定する者以外の者に対しても、必要な協力を依頼することができる。

（地方公共団体への協力）

第三十二条　地方公共団体は、第五条に規定する施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を求めることができる。

2　本部は、前項の規定による協力を求められたときは、その求めに応じるよう努めるものとする。

（事務）

第三十三条　本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。

（主任の大臣）

第三十四条　本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣とする。

（政令への委任）

第三十五条　この法律に定めるもののほか、本部に関し必要な事項は、政令で定める。

附　則

（施行期日）

第一条　この法律は、公布の日から施行する。ただし、第二章及び第四章の規定並びに附則第四条の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

（本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等）

第二条　政府は、本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備（内閣総理大臣の決定により内閣官房に置かれる情報セキュリティセンターの法制化を含む。）その他の措置を講ずるものとする。

2　政府は、前項の措置を講ずるに当たっては、専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等について検討を加え、その結果に基づいて必要な措置を講ずるものとする。

（検討）

第三条　政府は、武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（平成十五年法律第七十九号）第二十四条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする。

（高度情報通信ネットワーク社会形成基本法の一部改正）

第四条　高度情報通信ネットワーク社会形成基本法の一部を次のように改正する。

第二十六条第一項中「事務」の下に「（サイバーセキュリティ基本法（平成二十六年法律第　号）第二十五条第一項に掲げる事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く。）」を加える。

理　由

サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、サイバーセキュリティに関し、基本理念を定め、国の責務等を明らかにし、及びサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置する等の必要がある。これが、この法律案を提出する理由である。

平成二十六年六月十九日印刷　平成二十六年六月二十日発行　衆議院事務局　印刷者　国立印刷局