第百八十七回国会 参議院内閣委員会会議録第四号

平成二十六年十月二十三日（木曜日）

午前十時開会

委員の異動

十月二十一日

辞任　大野　泰正君　尾立　源幸君

補欠選任　世耕　弘成君　蓮　舫君

十月二十二日

辞任　世耕　弘成君　森屋　宏君

補欠選任　堀井　巌君　岡田　直樹君

出席者は左のとおり。

委員長　大島九州男君

理事　石井　準一君　上月　良祐君　藤本　祐司君　山下　芳生君

委員　上野　通子君　岡田　直樹君　岡田　広君　鴻池　祥肇君　山東　昭子君　堀井　巌君　松下　新平君　山崎　力君　相原久美子君　芝　博一君　蓮　舫君　若松　謙維君　井上　義行君　浜田　和幸君

衆議院議員　山本　太郎君

内閣委員長代理　平井たくや君

内閣委員長代理　近藤　洋介君

内閣委員長代理　遠山　清彦君

国務大臣　国務大臣　上川　陽子君

国務大臣　山口　俊一君

事務局側　常任委員会専門員　藤田　昌三君

政府参考人　内閣官房内閣審議官　谷脇　康彦君

内閣官房内閣審議官　向井　治紀君

総務省総合通信基盤局電気通信事業部長　吉田　眞人君

外務大臣官房審議官　下川眞樹太君

経済産業大臣官房審議官　石川　正樹君

本日の会議に付した案件

○政府参考人の出席要求に関する件

○サイバーセキュリティ基本法案（第百八十六回国会衆議院提出）（継続案件）

○委員長（大島九州男君）　ただいまから内閣委員会を開会いたします。

委員の異動について御報告いたします。

昨日までに、尾立源幸君、大野泰正君及び森屋宏君が委員を辞任され、その補欠として蓮舫君、堀井巌君及び岡田直樹君が選任されました。

○委員長（大島九州男君）　政府参考人の出席要求に関する件についてお諮りいたします。

サイバーセキュリティ基本法案の審査のため、本日の委員会に、理事会協議のとおり、政府参考人として内閣官房内閣審議官谷脇康彦君外四名の出席を求め、その説明を聴取することに御異議ございませんか。

〔「異議なし」と呼ぶ者あり〕

○委員長（大島九州男君）　御異議ないと認め、さよう決定いたします。

○委員長（大島九州男君）　サイバーセキュリティ基本法案を議題といたします。

本案の趣旨説明は既に聴取しておりますので、これより質疑に入ります。

質疑のある方は順次御発言願います。

○藤本祐司君　おはようございます。

サイバーセキュリティ基本法案につきまして、前国会でこの参議院で継続審議になっておりまして、それの審議について今日は皆さんの御意見をいただきたいというふうに思っておるんですが、現代社会、もう皆さん御承知のとおり、我々が好むと好まざるとにかかわらず、我々の身の回りの生活でもＩＣＴの影響というのはもう多分に受けている。本当に生活も便利になっている部分がありますし、会社あるいは政府の方でも、事務効率を上げるためにもかなりのＩＣＴが普及されてきているんだろうということは認識をしているところです。

ここ昨今、ここ昨今という日本語は変ですね、今日のニュースもちょっと見たところ、アメリカなんかでもかなり大手小売で個人情報が流出しているとか、そういう問題がほとんど毎日のようにいろんなところで、大きい事件、小さなこと、流れてきているという。そういう意味では、プラスの側面が大きいのと同時に、やはり気を付けなければいけないマイナスの側面というのもあるんだろうというふうに思います。

具体的に言えば、例えばネットバンキングの不正送金などの犯罪なども頻発をしておりますし、被害も増加しているということで、政府機関においても不正アクセス攻撃が頻発しているというふうに認識しています。

法案の中に入る前に、政府の方にちょっとお尋ねしたいんですけれども、大臣の方にお尋ねしたいんですが、このサイバー攻撃というのはいろんな理由があってサイバー攻撃する方々がいらっしゃるんでしょうが、これが最近の傾向として、どういう理由といいますか、どういう意図を持ってやられているかということの分析がなされているのかどうかということと、もう一点は、量的な問題で、いつぐらいからどういう推移でこのサイバー攻撃、特に政府機関に対するサイバー攻撃が増えてきているのか、その現状についてお答えいただきたいと思います。

○国務大臣（山口俊一君）　どういう理由でというふうなことですが、我々としては、一つには情報を窃取するというふうなことがあるんだろうと思います。さらにはまた、いわゆる政府機関への攻撃というのは、ある意味でシステムの脆弱性を探っておるというふうな部分もあるんだろうと思います。さらには、最近特に問題になっております個人情報を取ったり、あるいは企業の特許に絡む大事な情報を盗み取る等々、いろんな目的があってやっておるんだろうと。かつては愉快犯が多いんじゃないかと言われておりましたが、最近は明らかにこういった傾向が変わってきておるというふうに考えております。

また、お尋ねの政府機関への実際のサイバー攻撃への対応としては、もう先生も御案内のＧＳＯＣですね、政府機関情報セキュリティ横断監視・

即応調整チーム、ここでいろいろやっておりますが、そのＧＳＯＣにおいて平成二十五年度に政府機関への脅威と認知された件数は約五百八万件ございました。その中でも、ＧＳＯＣによる監視活動によって不正アクセスを検知をして、特にこれ、非常にそういった危険性が高いというふうな情報については通報しておりまして、平成二十五年度においては百三十九件の通報を行っております。

さらに、ＧＳＯＣにおきましては、政府機関が受信をする不審メールですね、それぞれが受信をする不審メールについて情報の集約と注意喚起を行っておりまして、平成二十五年度におきましては三百八十一件の喚起文書を発出をさせていただきました。

いろいろあるんですが、例えば二十四年の十二月には、日本原子力研究開発機構の方に、これはメールからＰＣ三台がウイルスに感染をしまして、二台のＰＣから情報が漏えいをした、あるいは二十五年五月には、日本貿易振興機構の方でサーバーが何らかの理由によって意図せざる外部との連絡を勝手に行っておった等々、そういった事例が多々ございます。

○藤本祐司君　ありがとうございます。

基本法案、衆議院で議論をされて、一部修正をされたというふうに認識をしておるんですが、続いてちょっと法案提出者にお聞きしたいんですけど、このようなサイバー攻撃が非常に激しくなってきている中で、この基本法案の中では政府に対してこうしたサイバー攻撃への対処、どのような対応を求めているのか、それについてお答えいただきたいと思います。

○衆議院議員（近藤洋介君）　お答えいたします。

委員御指摘のとおり、政府機関に対する攻撃は、平成二十五年度一年間で約五百八万件、六秒に一回行われておると、こういうことでありますし、ネットバンキングの不正送金被害額が今年上半期だけで昨年度の被害額を超えているといった、過去最悪のペースになっておるわけであります。

また、警察庁の発表によれば、我が国において発見された不正プログラムの通信の接続先が大半が海外であると、こういうことであり、国境を越えたグローバルな対応も極めて喫緊の課題であります。

こうしたサイバー攻撃への対処については、警察庁、外務省、防衛省、さらには総務省、経済産業省といった関係機関がまたがることから、これらの政府機関がきちんと連携をして、そして司令塔機能を政府内に持って対応する必要があると、こういうことであります。

本法案においては、こうした問題意識に基づき、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について、関係機関における体制の充実並びに関係機関相互の連携強化、役割分担の明確化を図るための必要な措置と、その趣旨を明確化しております。きちんと役割を明確化した上で連携を強化してもらう、その上で迅速な、スピーディーな対応を取ってもらうと、こういうことであります。

○藤本祐司君　分かりました。

確かに、今後ますますサイバーセキュリティー確保の重要性というのは高まっていくということは認識をしておるんです。ただ、一方で、国民側の立場から見ると、国民の権利が侵害されてしまうんではないか、簡単に言えば本法案が成立して、国がサイバー空間上の国民の活動を監視するんではないかという、そういう一方のやっぱり懸念はあるんだろうというふうに思っております。

当然、我々としては国民の権利、侵害されてはいけないんだろうというふうに思っていますので、これに対する何か配慮はこの基本法案の中でどのようにされているのでしょうか。

○衆議院議員（近藤洋介君）　お答えいたします。

ここの点、非常に大事な御指摘であります。したがいまして、この法案の協議に当たって我々民主党もこの点を強く主張し、自民党、公明党、各党合意に至った経緯がございました。

本法案は、もとより国民が安全で安心して暮らせる社会の実現を目的と一条でしており、情報の自由な流通の確保を基本理念として定めております。サイバーセキュリティーを名目に政府が国民や企業一般に対する情報収集活動、監視活動を行うといったことはあってはいけないことであります。こうしたことから、第三条に、基本理念に国民の権利を不当に侵害しないように留意することと規定をしたところでございます。

○藤本祐司君　その点非常に重要だというふうに私は思っておりまして、国民の権利保護というのは十分に配慮されていくべきだと思うんですが、これは、行政側はそういうことでサイバーセキュリティーを確保するためにいろいろ見ながら連携を取りながらやると、国民側は国民側としてやはり重要な、自分たちも自分たちのことは自分たちで守るというような部分も当然出てくるんだろうと思うんですが、じゃ、国会として、我々として、これは法案ができましたよと、あとは行政側と企業であるとかそれぞれの政府機関であるとか個人での話であって、国会はもうタッチしませんよという話には多分ならないんだろうと思うんですね。

ですから、そこのところを我々国会側として、もうやはり常にこのサイバーセキュリティーの施策については、その動向と結果と成果というのは見守っていかないといけないんだろうというふうに思っておりますけど、その点についてどのようにお考えになっていらっしゃるでしょうか。

○衆議院議員（近藤洋介君）　お答えいたします。

この点も極めて重要でありまして、御案内のとおり、本法案ではサイバーセキュリティー戦略本部を政府において設置をし、我が国におけるサイバーセキュリティーの司令塔としての役割を担わせることになっております。

この政府の取組に対して国会が適切にチェック機能を果たしていくことが極めて重要であります。こうした問題意識に基づいて、サイバーセキュリティ戦略本部が、政府が、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ることを法案に盛り込んでいるところでございます。

今後とも、サイバーセキュリティーに関する政府の取組については、法案の目的や基本理念に沿って適切に実施されているかどうか、衆議院、参議院両院において立法府として注視をしていくべきだと、こう考えているところでございます。

○藤本祐司君　大分イタチごっこ的なところがあって、かなり複雑怪奇にいろいろなことをやってくるんだろうと思うので、国会も非常に、我々の知識も上げていかないと難しいという、そういう非常にこの問題というのは難しい問題なんだろうなというふうには思っております。

そして、このサイバーについても、この主体者というのは、先ほど国民側というふうに一般的に言ってしまいましたけれども、これ企業という点で考えたときに、経済の持続的発展、あるいは国際競争力を日本の企業が付けていかなければならない、その中で、大企業よりも数としては圧倒的に中小企業、個人事業者という方が多いわけで、そこの企業なんかも知的財産を保護していかないといけないという、そういう側面があると思うんですね。

ただ、この問題というのは、ある意味専門的な知識がないとなかなか理解しにくいところがありまして、中小企業というのは大企業と違ってＩＣＴの知識や関心というのが必ずしも高くはないんだろうというところがあって、そういう意味では、このサイバーセキュリティー確保に対する対応への知見というのも、大手企業なんかと比べたりするとまだまだ高くなっていないというところがあるんだろう、これは現実なんだろうと思うんですね。

そこのところの、要するに中小企業のこうした関心あるいは知見をどうやって高めていくのか。これを高めていくことによって、知的財産保護という点では大変重要なんだと思うんですが、この課題、これかなり、私、現実的には難しい課題なんだろうと思うんですが、この課題についてはどのような配慮をこの法案の中ではされているんで

しょうか。

○衆議院議員（近藤洋介君）　お答えいたします。

委員御指摘の点、これまた大事な点でありまして、世の中の九九％が中小企業と、これが実態であります。こうしたことから、法案の第十五条又は第二十一条において、国は、中小企業者を始めとする民間事業者のサイバーセキュリティーに関する相談に応じて、必要な情報提供及び助言を行うなどの施策を講ずることとしておりますし、またさらには、若年技術者の養成等必要な施策を講ずることと規定をしております。

ただ、実際にこれが中小企業事業者にとってきちんとした施策が行われているかどうかということについては、先ほど御答弁申し上げたとおり、国会においてもきちんとチェックをし促さなければいけないと、こう考えておるところでございます。

○藤本祐司君　今の質問とそれとお答えと非常に重なるところがあると思うんですが、要するに、国民を挙げてということになる、国を挙げてということになると思うんですが、このサイバーセキュリティー確保に関しては官民の人材育成ですね、これはやっぱり大きな今後の課題になってくるんだろうと思います。

政府に対して、法案提出者として、いわゆる官民の人材育成という側面から政府はどのような対応が必要だと法案提出者としてお考えになっていらっしゃるのか、お答えいただければと思いますが。

○衆議院議員（近藤洋介君）　お答えいたします。

国内において、まず情報セキュリティーに従事する技術者は約二十六・五万人と、こう言われていますけど、そのうち約十六万人が必要なスキルを満たしておらず、さらに約八万人の情報セキュリティー人材が不足していると、こう指摘をされております。人材の不足は深刻な状況でございます。

そのため、政府においては、企業の経営者層がサイバーセキュリティーに対する意識を深めて、情報セキュリティーを経営の戦略の重要な一部であるとまず認識してもらうこと、さらには、高度な能力を持つ人材や突出した能力を有する若年技術者の養成や資格制度の活用等、こういった政策の推進を政府に求めていきたいと、こう思います。

また、本法案の附則においては、内閣官房における専門人材の任用を政府に対して求めており、まず隗より始めろと、こういうことで政府においても人材育成や確保について民間からの積極的な登用を求めてまいりたいと、こう考えております。

○藤本祐司君　時間も大分なくなってきましたので政府の方にちょっとお聞きしたいんですが、この問題が出るたびに私いつもいつも不思議だなと思うことがありまして、これ、政府の対応が不思議だなというのではなくて、我々、私も含めて、国民の行動が非常に不思議だなというようなことがよくあるんですね。

これ何かというと、もう割と余り考えずに、平気でネットで自分の個人情報をわあっと発信したり、あるいは、お店に行って何かポイントカードを作るとか何だとかというときに平気で個人情報をわあっと書いて提出をすると。そういう情報が流れたときには問題になるんでしょうけど、割とその辺りは安易に皆さんやっているのではないかなというふうには思うんです。その一方で、個人情報保護という点が非常にがちがちでありまして、要するに意識としてがちがちで、これは個人情報だから出さないとかということ、出せないとか、そういうのがあるのと物すごくギャップを私感じるんですよ。

ですから、このサイバーセキュリティーに関する知識と関心というのを、政府機関であるとか大企業はそういう知的財産守らなきゃいけないというところについては問題意識が非常に高いので、ふだんから高いので、それに対してどう対応しようかとか、割とセンシティブな問題だというふうに感じるというのはよく分かるんですね。ただ、それを一般の国民の皆さんにその関心と知識をどうやって意識付けていくんだろうかというのがなかなか私の頭では正解が見出せない。

実際に、この法案の二十二条に、教育及び学習の振興、普及啓発というのは、書かれていることは書かれているんですが、法文としては非常によく分かるし、そういうのをちゃんと書いて進めていかなければならないということは分かるんですが、これ具体的に、その辺りの意識啓発というんでしょうか、それを行動に結び付けていくというのはなかなか難しいなというふうに思っているんですが、政府としては、それをどういう方向性でどういうような対応ができると今お考えになっていらっしゃるのか、これを最後の質問とさせていただきます。

○国務大臣（山口俊一君）　御指摘のとおりで、リアルとバーチャルで、リアルの世界では結構個人情報に敏感な方々多いんですが、バーチャルの世界になるとつい出してしまうという事例も数多くございます。

ただ、様々な事件等が起こる中でじわじわと意識も高まってきておるんだろうと思いますが、この普及啓発に関しましては、これまでも実は国民の皆さん方を対象としたリテラシーの向上を継続的に図っていくために、関係省庁とも連携をして、一つが情報セキュリティ月間、これ二月でありますが、この実施とか、この二月の最初のワーキングデーで、サイバーセキュリティの日ということでシンポジウム等々を実施をしております。あるいは、情報セキュリティ国際キャンペーン、これは十月でありますが、これもやっております。さらに、普及啓発のためのコンテンツを作って配布をしたりして見ていただく、情報セキュリティーに関する教育の推進とか企業の意識向上等々に取り組んでおります。

しかし、そういった様々な問題がやっぱり増えこそすれなかなか減っていかないという中で、国及び国民全体の情報セキュリティーへの関心とか理解度、対応力の強化、増進を図ることを基本的な考え方として、実は本年の七月に情報セキュリティ政策会議におきまして、新たな情報セキュリティ普及啓発プログラムを策定をいたしました。これが今後、これまでの産学官民、各主体の取組状況等を踏まえながら、一つは情報セキュリティー普及啓発の推進体制の強化、総合的、集中的な普及啓発施策の更なる推進、そしてまた、地域ですね、地域における取組を推進をしていく、そして青少年等、特に注力が必要な層に対するきめ細やかな普及啓発活動の推進等の観点から、関係府省とも協力をして、とりわけ法律の方でも御指摘をいただいておりますので、しっかり取り組んでまいりたいと思います。

○藤本祐司君　終わります。

○委員長（大島九州男君）　この際、上川国務大臣から発言を求められておりますので、これを許します。上川国務大臣。

○国務大臣（上川陽子君）　特定秘密の保護に関する制度に関する事務を担当する国務大臣として、一言御挨拶を申し上げます。

特定秘密保護法について、先般、関係政令や運用基準を閣議決定いたしましたが、特定秘密保護法の施行日である本年十二月十日に向けて、今後も国民の皆様の御理解をいただくよう努めるとともに、その施行準備に万全を期してまいります。

大島委員長を始め、理事、委員各位の御理解と御協力をよろしくお願い申し上げます。

○山下芳生君　日本共産党の山下芳生です。

既に国民の八割がインターネットを使っており、スマートフォン、携帯電話の普及、所有台数は一億数千万人の規模に上っております。提案者の皆さんがおっしゃるように、インターネット前提社会とも言うべき時代を迎えていると思います。そのネット空間、サイバー空間を含むこうした空間で、安心、安全な空間にいかにしていくのかと、それをどう国民に保障するのかというのは非常に重要な課題だと思います。

まず、提案者に伺いますが、サイバー攻撃とは何か、その対策とはどういうことか、簡潔にお答

えください。

○衆議院議員（平井たくや君）　認識は全く先生と同じでありまして、そのサイバー空間の安全、安心をいかに確保していくかというところがこの法案の元々の発想でございます。

今回、議員立法で我々対策を急いだということの中に、一つ、やっぱりサイバーセキュリティーという言葉をまず定義したいというのがありました。二〇一年にＩＴ基本法というものが制定されましたけれども、当時のＩＴ基本法の中にはセキュリティーの概念が全くありませんでした。あの法文を全部チェックしても安全という言葉が一回出てくる。私は、今回、これだけ、先ほどおっしゃったとおり、インターネット前提社会、あらゆるものがインターネットなしでは成り立たないような社会になっている以上、そのセキュリティーという概念をまずちゃんと定義をするということが一番重要だと考えました。

そして、その概念を法文として定義した上で、その事態を脅かすようなものをサイバー攻撃ということで、具体的には、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を通じた電子計算機に対する不正な活動であると規定しました。例えば、ネットワークを通じて不正に電子データを改ざんするような行為はこれに含まれるということです。

ですから、攻撃というものの規定ということは先ほどお話ししたとおりの考え方ですが、その内容は巧妙化、複雑化、大規模化しておりますので、その対策が急がれると考えています。

○山下芳生君　安全、安心なネット空間、サイバー空間という場合に、私は市民的自由の問題、プライバシーの問題というのは重要な要素となると思います。

そもそもコンピューターの開発というのはミサイルの弾道計算と密接な関係があって、また、半導体産業というのはペンタゴンの国防高等研究計画局の支援によって生まれました。インターネットも、その起源は軍事目的であったということはよく知られていることであります。

そういう下で、アメリカでは、ＩＴ企業とＮＳＡ、国家安全保障局の諜報活動が特別な関係にあることが明らかとなっています。エコノミスト誌、今年一月十四日付けに次のような記事がありました。強力な暗号特許を保有していたＲＳＡ社がＮＳＡに協力するという密約が結ばれていた、スノーデンは、米国の主要検索サービス企業やＳＮＳ関連企業がＮＳＡに情報提供していた事実も明らかにしていた、さらに、当局に情報提供していたネット企業として、グーグル、マイクロソフト、アップル、フェイスブック、ヤフー、ユーチューブ、スカイプ、ＡＯＬ、パルトークの九社の名前もさらされた、アメリカ市民の中に、個人情報を盗み見られていることに震撼、市民のプライベートを侵害する行為であるとの激しい批判が起こったという記事でありました。

これは、あながち勝手なでっち上げではないと思われます。ＮＳＡ、アメリカ国家安全保障局の諜報活動というのは、ＩＴ企業からの情報提供によって成り立っているということが実態なんですね。

インターネットというのは、市民に、先ほど提案者が言われたように、豊かで便利な生活を提供する一方で、こういう問題も生んでいると。その下で、どう市民のプライバシーを守るのか、市民的自由を守るのかということが問われているわけですが、提案者に伺いますが、この法案においては具体的な担保をどう取られているでしょうか。

○衆議院議員（近藤洋介君）　山下先生にお答えいたします。

一般論でありますけれども、技術開発は軍事技術と重なる部分があると、軍事技術によって技術開発が進むという、一般論でありますけれども、面もあるということは認識しておるわけであります。

とりわけ、ただし、委員御指摘のとおり、サイバーの分野に、セキュリティーにおいて、そのサイバーセキュリティーに名を借りて、その施策が具体化された場合に、サイバーセキュリティー確保のために個人所有のパソコンや通信記録、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といったおそれがあるのではないか、自由なインターネット空間が阻害されるのではないかと、こういうおそれ、懸念があることは私どもも十分承知をしておるところでございます。

そこで、本法案では、このようなおそれが生ずることがないよう、まずは基本理念として、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留意すべきことを第三条第六項に基本理念として明定し、さらに、サイバーセキュリティーに関する施策に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ること、第十二条第四項を特に明記したところであります。国会への報告義務、そして国会のチェックといったことを明定しているわけでございます。

こうした基本理念の規定を踏まえ、個別具体策の施策の中できっちりと措置されるものと考えております。

○山下芳生君　これはまた後でもう少し具体的にやり取りしたいと思うんですが、もう一つ、角度を変えて、国民は、ネット空間のそういった危険性や脆弱性をいろいろ知らされる中で、パソコンを買い換えたりウイルス撃退ソフトを買ったり、かなり大変な負担を強いられている面があるんですね。

日経新聞が昨日付けでネットバンキング記事を、先ほど近藤さんがちょっと紹介されたことにも通じておりますけれども、インターネットバンキングの機能を悪用し他人の口座から不正に送金する犯罪が増えている、ネットバンキングはＡＴＭに比べて好きなときに手続できるのが魅力だ、一方で、犯人がパスワードを盗むなどして他人の預金口座から自分の口座にお金を振り込むということが起こっている、そのネットバンキングによる個人の不正送金被害が、全国銀行協会の調べでは、二〇一四年、今年の四―六月期に四百十三件と前年同期比の三・四倍に急増しているということがありました。

この記事の中で、私、これ何とか対策しなければならないなということは感じたわけですが、同時に、大手銀行が今、個人顧客にやたらとこのネットバンキングを勧めているんですよ。こっちの方が手軽ですよ、便利ですとやたら勧めています。やたらネットバンキングを勧めながら、この不正送金などの被害に遭った場合は、例えば利用者側に落ち度があったんじゃないかと、パソコンのソフトを更新していなかったじゃないかとか、パスワードの管理がずさんだったなどとして補償額を減額しているというケースもこの記事でも指摘されておりました。

一部の銀行では不正送金に対応するソフトを無料で配付していることもあるようですが、しかし多くは利用者負担による自衛、自己責任に任せられていて、こういう被害に遭っても、あなたが悪いんやと言って補償が余り十分されないということもあるようなんですね。

私は、安心、安全なネット空間をつくるためには、個人ではなくて、事業者の側にどう責任を持たせるのかというのは大きな課題だと思いますが、この点で、提案者と山口ＩＣＴ担当大臣の認識を伺いたいと思います。

○衆議院議員（平井たくや君）　安全で安心なインターネットの空間をつくるというのは、国民だけでもできない、企業だけでもできない、政府だけでもできない、全てが協力をしながら、それぞれが努力をしながらそういう空間をつくっていくということが宿命付けられているのではないかというふうに私は思います。

本法案は、そういうために、サイバーセキュリティーに関する施策を総合的に推進するための基本法ということになっていますので、先ほどお話しになったような事例に当てはまる具体的な措置は書いていません。それと、今、全てのどのようなことが起きるかということを想定できないとい

う問題もあります。何が起きるか正直言って分からない、それに対して今後やっぱり国と企業と国民が協力しながら対応していくということが望ましいと思います。

法案の中には、サイバー関連事業者の責務に規定をしているのが第七条、民間事業者の自発的な取組を促進するのが第十五条、そしてサイバー関連事業者が国を始めとする多様な主体と相互に連携してサイバーセキュリティーに関する施策に取り組むことができるような施策を講ずるものとするのが第十六条ということで規定をさせていただいております。

これは、官民一体となった政策をこれから進めていくということが非常に重要であり、私は、認識として、今まさに第三次産業革命のもう真っただ中にいるんだというふうに思います。それは、コンピューターとネットワークによって約一九八〇年ぐらいからスタートをしたもので、ちょうど我々、その折り返し点をちょっと過ぎた辺りにいるというふうに思うんです。これは私の認識ですけれども。

そうなると、これから先の話はもう全く想定外の事態というのも十分あり得ると思うんですね。ですから、基本的には、国、そして民間のいろいろなセクター、そして国民が協力し合いながらつくっていくという体制が望ましいと思っています。

○国務大臣（山口俊一君）　今、提案者の方からお答えがございましたように、やはり国も民間もあるいは国民の皆さん方も、それぞれが共々にやっぱり努力をしていくということが必要なんだろうと思います。

とりわけ、私も実はそうなんですが、ソフトウエア等の脆弱性で自らのパソコンがウイルスに感染をするおそれがある、これ、もうどうしようかなということで高いアンチウイルスソフトを買い込んだわけでありますが、また、最近というか、近年増えてきておりますのが、自らのＰＣが踏み台になって結局他人のいろんな皆さん方に迷惑を掛けるというふうなことがありまして、そういったときにどうしたらいいのかということで、国民の皆さん方お一人お一人が日頃からセキュリティー対策にそれこそ頭を悩ましておられるんだろうと思っております。

そういった状況の中で、国民のお一人お一人がより広くサイバーセキュリティーに関する関心と理解を広げていくということの重要性に鑑みまして、セキュリティーに必要な注意を払うよう努める旨が基本法案において、第九条ですか、規定をされておるというふうに承知をいたしております。

政府としましても、国民の皆さん方が何をしたらいいんだろうかといった疑問とか対策の負担を軽減をしていくというふうなことで、平成二十五年六月に情報セキュリティ政策会議で決定をしましたサイバーセキュリティ戦略におきまして、サイバー防犯ボランティアとか、あるいは情報セキュリティサポーターと呼ばれる地域の身近な相談相手の育成を支援をする取組を促進をするとともに、ウエブサイト等を通じて個人に対して情報提供も行っておりますし、また、ＩＰＡ、これは独立行政法人の情報処理推進機構でありますが、安心相談窓口、これを設置をして国民の皆さん方のサイバーセキュリティーの確保の応援をさせていただいておるというふうなことでございまして、この法案が成立をした場合には、同法を踏まえて、引き続き政府としてもしっかりと必要な支援を実施をしてまいりたいと考えております。

○山下芳生君　国民にいろいろ啓発していただくのはいいんですが、私が一番問題提起したかったのは、事業者がちゃんとやるべきことをもっとやるべきだと。インターネットバンキングというのは、それは利用者にとってもいつでもどこでもという便利さはありますけど、銀行側にとったって、設備がなくて済むとか人件費をうんと抑制できるとか、いっぱいメリットあるわけですよね。だから推奨をしているんですよ。それで被害に遭ったら自己責任だと利用者が責任を負わされるというのは、これはやっぱりフェアじゃないと思うんですよね。そういうところももう少し目配りをして、事業者の側へのやるべきことはこういうことだということを提起することも、私は政府の責任として大事だと思っております。

次に、ちょっと角度を変えて、アメリカのこの分野での戦略について見てみたいと思います。

ホワイトハウスや国防総省の戦略を見ますと、アメリカはサイバー空間というものを、陸、海、空、宇宙に次ぐ第五の戦闘領域と位置付けているということが分かります。ホワイトハウスが二〇一一年に制定したサイバー空間に対する国際戦略という戦略文書を分析された防衛省統合幕僚監部指揮通信システム部の佐々木孝博一等海佐が、「ディフェンス」二〇一二という書物の中で次の二つの特徴に注目されています、アメリカのサイバー戦略ですけれども。

第一に、米国は、サイバー空間を海、空と同様に自由な空間と捉え、かつ米国が主導して同空間における国際規範を構築していくのだという姿勢を示した。

つまり、アメリカが自分でルールを作るんだという立場に立っているということです。

第二に、米国は、サイバー空間での戦い（敵対行為）に対しては他の物理的な脅威への対応を適用し、それによりサイバー攻撃に対しても自衛権の行使を適用する、そのためには軍事力の行使を含むあらゆる手段をとる可能性を留保することを明言している。

つまり、サイバー攻撃に対して軍事力の行使を含むあらゆる手段を行使するんだという立場にアメリカは立っているということであります。

山口大臣、アメリカのサイバー戦略はこういうものであるということを御認識されていますか。

○国務大臣（山口俊一君）　今先生の方からお話がございました、米国が二〇一一年五月に公表したサイバー空間国際戦略ですね、ここにおきまして、サイバー空間の原則として、基本的自由権、プライバシー、自由な情報の流通というのが示されました。また、世界が求めるべきサイバー空間の在り方が示されて、それに対して米国がどのような役割を果たすべきかというのも示されております。さらに、お話の国家からのサイバー攻撃、これについては、物理的な戦争をその対抗手段として取り得るというふうなことを記載をされているということは承知をしております。

○山下芳生君　承知をされているということですが、さっきのまとめは私がまとめたんじゃなくて防衛省の担当者がまとめたものですから、共通の認識になり得ると思います。

アメリカは、この戦略に基づいて実際にどんな活動をしているのか。これは、先ほども述べました元ＣＩＡ職員エドワード・スノーデン氏による米国家安全保障局、ＮＳＡのグローバル監視プログラムに関する告発によってその実態が暴露されました。ＮＳＡの監視対象は全世界の市民に及んでおります。単なるテロリスト予備軍とか犯罪者ばかりではなくて、各国の首脳まで電話盗聴されていたということが分かりました。ドイツのメルケル首相への盗聴など、大きな外交問題になったことは記憶に新しいところであります。アメリカは、こういう無法なやり方をサイバー空間でも展開しようとしております。

山口大臣に伺いますが、ＩＣＴ空間、サイバー空間がこうした無法な諜報活動、監視活動の舞台となっていることをどう評価されますか。

○国務大臣（山口俊一君）　ただいまるる御指摘がございました様々な盗聴等の問題に関しては、私ももちろん報道等では存じ上げておりますし、スノーデン氏にまつわるいろんな話等々も報道等を通じて承知はしておりますが、しかし、それの実態が本当のところどうなのかということも、これはもう承知をしておりませんし、また、かつ、そのいわゆる情報、インテリジェンスの収集に関しては私の方の担当でもございませんし、そういったことでこれ以上のコメントはしかねるのかなと思っております。

○山下芳生君　今のコメントにも私、本当に心配

を覚えるんですね。さっき言ったアメリカのこのNSAの監視対象は日本にも向けられております。NHKのインタビューに対して、アメリカ政府当局者も、NSAが日本国内に通信傍受の施設を設けて活動しているということも明らかにしました。

ところが、今、山口さんおっしゃったように、日本の政府当局者はそれに対して余りにも鈍感過ぎるというか、あえて目と耳を塞ごうとしています。これ、小野寺前防衛相がこういうことがあるんじゃないかと問われたときに、報道は信じたくありませんと、これで終わっているんですよ。全く、真剣にそういうことに対して、だってメルケル首相は激怒してアメリカに抗議したじゃないですか。そういう姿勢が全くないということを本当に私危惧します。

アメリカはそういう下で今どんなことをやっているかといいますと、二〇一三年三月、米上院軍事委員会で、当時の米サイバー軍司令官キース・アレクサンダー大将、もう既にサイバー軍というものをアメリカは各軍の中に設けているんですね、そのサイバー攻撃を目的としたチーム編成を行っていることを議会の証言で明らかにしました。もうサイバー攻撃専門の部隊を各軍にアメリカはつくっております。

イギリスのガーディアン紙の報道によりますと、スノーデン元CIA職員が暴露した大統領政策指令20という文書の中には、サイバー攻撃についてこうあります。平時と戦時の双方で米国の国益に害悪を与える敵を抑止し打倒する不可欠な能力を持つんだと。要するに、戦時だけじゃなくて平時からそういうことをやっているんだということです。

それから、世界中の敵や標的に対して警告なしで深刻な損害を与え、米国の国家目標を前進させ得ると。要するに、サイバー攻撃やられる前に先制攻撃やるんだということもアメリカのサイバー戦略には位置付けられているんですね。さっきのように、単なるサイバー世界ではなくて、物理的な軍事力の行使もその中には含まれているということであります。

もう一度山口大臣に聞きますが、軍事力と一体となったアメリカのサイバー戦略についてどうお考えか、日本もそういう方向に進むべきかどうか、この御認識を伺いたいと思います。

○国務大臣（山口俊一君）　先ほど来お話がございましたメルケル首相の盗聴の話とか、あるいはドイツもやっておったんじゃないかという報道もありましたし、あるいは、かつてエシュロン云々というふうな話もございました。

しかし、それに対して、じゃどうなんだといった場合に、我々はもっと具体的事実を基にしてやっていく必要があろうかと思います。今のところはもう非常にコメントをしにくいとしか言いようがないわけでありますが。

同時に、米国のサイバー戦略ですね、お話がございましたが、これも私の方からはコメントは差し控えさせていただきたいと思いますが、我が国におきましては、サイバー空間の防御というのが国家安全保障上不可欠であろうということで、昨年十二月に閣議決定をしております国家安全保障戦略、あるいは昨年の六月に情報セキュリティ政策会議におきまして策定をしたサイバーセキュリティ戦略、これに基づいて、我が国は我が国として粛々と施策を遂行してまいるというふうなことだろうと思います。

○山下芳生君　アメリカについてはノーコメント、我が国は我が国として粛々ということでしたが、もうそれでは済まない状況になっております。

十月八日、政府は、日米防衛協力のための指針、ガイドライン見直しに関する中間報告をまとめました。この中間報告は、新たな戦略的領域における日米共同の対応として、宇宙及びサイバー空間について初めて明記をしております。

そこには、日米両政府は、「安全保障上の課題に切れ目なく、実効的かつ適時に対処することによって、宇宙及びサイバー空間の安定及び安全を強化する決意を共有する。」と、こうあるんですね。アメリカのサイバー戦略は知りませんではもう済まないんですよ。日米がサイバー空間の安全保障問題で決意を共有するとまでガイドラインではうたっているわけですから。

その中には、中間報告、特に自衛隊及び米軍は、「宇宙及びサイバー空間の安全かつ安定的な利用を確保するための政府一体となっての取組に寄与しつつ、」と、こうあります。自衛隊と米軍が政府と一体となって取り組むということでありまして、提案者にも伺いたいと思いますが、この日米のサイバーセキュリティーの連携の中で、提案者が提案されている法案の中にあるセキュリティ戦略本部は一体どういう役割を担うんでしょうか。

○衆議院議員（遠山清彦君）　山下委員にお答えいたします。

まず、この法案の内容に即して、サイバーセキュリティ本部と関係機関の連携について申し上げたいと思いますが、ポイントは二つございます。

まず一つは、このサイバーセキュリティ戦略本部は、サイバーセキュリティーに関する基本的な計画であるサイバーセキュリティ戦略の案を作成をしなければならないわけですが、その際に国家安全保障会議、NSCの意見を聴かなければならないと規定をされております。これが一点目でございます。

二つ目は、サイバーセキュリティ戦略本部は、我が国の安全保障に係るサイバーセキュリティー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ということも規定をされているわけでございます。

ですから、この法案で規定されている範囲で申し上げれば、この二つだけでございます。

先生御指摘の米軍と自衛隊がどういう連携をするかということにつきましては、象徴的に言えば、アメリカの国防総省と防衛省の協議がなされた上で具体的に決まっていくんだろうと思います。

その内容につきましては、当然のことながら国家安全保障会議が今政府にございますので、そこが司令塔になって政府全体の取組の中での位置付けというのがなされると。今回、この法案で規定をされておりますサイバーセキュリティ戦略本部というのはNSCと連携をしていくわけですから、あくまでもNSC、国家安全保障戦略会議を基軸にしながら、政府全体のものが調整を図られていくんだと私どもも理解をしております。

しかし、自衛隊と米軍の連携のサイバーについての中身については、これは私どもの立場でお答えする立場にございませんし、是非政府の関係省庁にまた別の機会に聞いていただきたいと、こう思います。

○山下芳生君　今、遠山さん、提案者として答弁できるぎりぎりの答弁だったと思います。今、正確な答弁でした。

サイバーセキュリティ戦略本部と国家安全保障会議、NSCが、二つの点で協議をし、緊密連携するということが書かれてあるんですね。その中で、遠山さんおっしゃったように、国家安全保障会議というのは、もう安全保障問題についての最高の司令塔ですから、当然自衛隊と米軍との間でサイバー戦略についての共有化がされるときには当然司令塔の役割を果たします。どちらも官房長官が、安全保障会議でも重要な役割を担っておりますし、セキュリティ戦略本部でも担うことになっております。これ、一体になるわけですよ、当然ながら。そのときに、そうなってきますと、先ほどからある説明していますように、アメリカのサイバー戦略と日本のサイバー戦略がリンクしていくことになるとどういうことが心配されるか。私、二点心配されることがあるんです。

第一に、日本のサイバーセキュリティー体制が軍事化することになる危険。二つ目に、日本のIT企業などが持つ情報がこうした体制を通じてアメリカ側に流される危険があるんじゃないかと。先ほど言ったように、アメリカはIT企業を全部もう情報活動、監視活動の傘下に収めているんですから、そことリンクしたら日本のIT企業が持つ情報がアメリカ側に流されるんじゃないか、日本の国民や市民がアメリカによって監視される危

険が生じるんじゃないか。

この二点について、山口大臣、そうならない保証はありますか。

○国務大臣（山口俊一君）　先ほど提案者の方からも御答弁がございました。

確かに、法案ではＮＳＣの意見を聴いたり、あるいは連携をしていくというふうなことになっておりますが、一方、基本法に関しましては、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をしていくと。いわゆる経済社会活力の向上とかあるいは持続的発展とか国民が安全で安心して暮らせる社会の実現、これを図っていくとともに、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しておるというふうに承知をしておりますので、サイバーセキュリティ戦略本部としては、そういった方向に沿って国民の皆さん方が安全で安心で暮らせるような社会の実現を図っていくというふうなことでございまして、直接リンクすることはないんだろうと。

ただ、お話しのように、ＮＳＣはＮＳＣの考え方等もあるかも分かりませんが、そこら辺はまた担当の方にお聞きをいただきたいと思います。

○山下芳生君　山口大臣にこれ以上この問題を突っ込んで聞くという点では、お立場が違いますからまた別の機会にしたいと思うんですが、そういう方向になり得る道を開こうとしているわけですね。

もうちょっと時間ないので、せっかく上川さんに来ていただいていますから、この法案では、サイバーセキュリティ法案では、各府省に対してセキュリティ本部が資料提供義務を課しているんですよ。秘密保護法では、この間、運用指針が決められましたけれども、どうなっているかといいますと、内閣府に独立公文書管理監を置いて秘密保護指定が妥当なものか検証、監察、是正をさせるとしていますが、必要なときは、行政機関の長に対して特定秘密である情報を含む資料の提出若しくは説明を求め、実地調査をすることができるとなっていまして、こちらはできる規定で義務を課していないんですね。

これは、行政機関の長がそれは出せませんと言ったら、独立公文書管理監に情報を出さなくていいんですか。

○国務大臣（上川陽子君）　ただいま御質問がございました特定秘密保護法の運用基準における規定ぶりということでございますが、運用基準におきましては、行政機関の長は、独立公文書管理監による求めがあったときは、特定秘密保護法第十条第一項の規定により、独立公文書管理監に特定秘密を提供するものとするという規定をしているところであります。

これは、特定秘密保護法第十条の規定でございまして、行政機関の長は、公益上特に必要があると認められる場合において特定秘密を提供するものとすると規定をしておりまして、この規定を受けての運用基準ということでございますので、この特定秘密保護法における規定ぶりに合わせた表現を用いるということであるというふうに承知をしております。

○山下芳生君　だから、情報提供を要請されたらしなければならないんですか。拒否はしてはならないんですね、じゃ。

○委員長（大島九州男君）　上川国務大臣、時間ですので簡潔にお答えください。

○国務大臣（上川陽子君）　はい。

この特定秘密保護法の第十条の第一項に基づきまして、行政機関の長が、我が国の安全保障に著しい支障を及ぼすおそれがないと認められないときに内閣府独立公文書管理監等に特定秘密が提供されないことはあり得るということでございます。

○山下芳生君　一言だけ。

結局、行政機関の長が駄目だと言ったら出さなくていいんですよ。何のチェックにもならないんですよ。そういう下でこのサイバーセキュリティーが米国とリンクするようなことになったら、何がリンクしているか、国民は知ることができません。極めて危険な状況になり得るということを指摘して、終わります。

○浜田和幸君　新党改革・無所属の会を代表して、提案者並びに政府参考人に幾つか質問をと考えております。

まず最初に、これまでずっと議論をしてきましたように、今、日本はサイバーセキュリティー立国、これを内外にＰＲしているわけですよね。要するに、サイバーセキュリティーを頑丈なものをつくって、外国から投資家や研究者がどんどんやってきても安心して日本で研究開発ができる。また、これは新しい成長産業という位置付けも、この基本法案の中に述べられています。そういうことを実現するに当たって、やはり全体像ですよね、この基本法の中で一体日本をどういうセキュリティー立国として位置付けるのか。

今、インターネットの世界で、どんどんサイバー空間で軍事化、様々な問題が起こっているという指摘がありました。しかし、もう今インターネットをめぐる環境はどんどん日々進化しているわけですね。もうインターネットの時代は時代遅れと言われているぐらいで、今年六月からは、アメリカが主導するアウターネット、要するに、もう通信衛星から個別のＰＣに全部情報ができる、途中で情報が抜かれたりそういうことがないような全く新しいネット空間さえ今生まれつつあるわけなんですよね。ですから、インターネットの中のセキュリティーをどう確保するのかという議論そのものが、ある意味では時代から相当遅れているという見方もできるんではないかと思っているんです。

そういう観点で、今回のサイバーセキュリティ法案、サイバーセキュリティー立国としての、国家戦略の中に位置付けられているんですけれども、そういう新しい時代の動きに対応するような柔軟性があるのかどうか、その点についてまず提案者にお伺いしたいと思います。

○衆議院議員（平井たくや君）　先ほど、インターネット前提社会という話とインターネットはもう時代遅れだという話、その両方とも理解できる話なんですが、私はデジタル化とグローバル化という見方をさせていただいています。このデジタル化とグローバル化というのは、もう動きが止めようがない、ボーダーレスになっている。これからインターネット以外の通信手段が出てくる可能性も十分あると思いますし、しかしながら、やっぱりそういうものを使う、ネットワークを使う以上、そのセキュリティーを担保していくというのは永遠の課題ということで、ありとあらゆることに我々対応していかなきゃいけないんだというふうに思います。

そういう社会の中において、我々日本というのは、今いろいろな問題抱えています。少子高齢化とか、やっぱり地方都市の人口減少の問題とか、財政の問題とかでいろいろある中で、問題を解決するためにはそういうものも使っていかなきゃいけないという宿命もあります。そうすると、そういう社会、グローバル化とデジタル化の社会というのは必ず光と影があって、我々は、光のところを大きくして影の部分を小さくするために、常にありとあらゆることにチャレンジするということが必要なんだと思います。この法案の思想はそうなんです。ですから、そのための研究開発とかそういうものを進めていかなきゃいけないし、そういうグローバル化とデジタル化の中で企業活動とか社会活動をするということになりますと、我々自身も物の考え方からやっぱり変えていかなきゃいけない部分があるんではないかと思います。

産業化できるかどうかというのはこれからの取組次第だと思うんですが、今まで日本の企業というと、どちらかというとＩＴ投資はコストと見ていました。セキュリティーはコストの一部分。ところが、多くのグローバル化とかデジタル化の中で先行している企業は、戦略的投資と見ているわけです。ですから、単なるサイバーセキュリティーに対する対処のお金を用意するのではなくて、それを企業戦略の中に位置付けて、言わば一種の企業コンプライアンスの中の非常に重要な部分と位

置付けている、そこがちょっと我々出遅れたところがあるのではないかと。

今回、この基本法案を制定することによってサイバーセキュリティーという言葉を定義をする、法文の中で定義する初めての国家になると思うんです。そこがやっぱりパラダイムの一つの転換であって、それに対応する、安全な状態をつくるために対応するいろいろな方法はこれからやっぱり我々考えていかなきゃいけないし、そのために予算も使っていかなければならないのではないかと、そのように思っております。

○浜田和幸君　是非、パラダイムシフトの時代に日本が世界に先駆けてこういうサイバーセキュリティ基本法を制定する意味はとても大きいと思うんですね。そういう観点で、昨日の新聞報道で、初めての試みで、日本、中国、韓国、この三か国の外務省担当者によるサイバー協議が開かれた、北京でですね、そういう報道がありました。

御承知のように、中国というとまさに世界のサイバー攻撃の大本という評価が定着しているぐらいでありまして、アメリカからも、中国の人民解放軍将校五人をサイバー攻撃の元凶、犯人として訴追するということも行われているぐらいでありますね。中国の有名なハッカー集団、コメント・クルー、ここなんかは、中国政府から委託を受けてアメリカや世界の軍需産業や航空宇宙産業にどんどんハッカー攻撃を仕掛けて情報を盗み取っている。

そういう、言ってみれば国際的な基準を作ろうとしているときに、無法者、違反者と思われるような国、中国、まあ韓国は日本と同じようにそういう脅威にさらされていると思うんですけれども、しかし、日中韓のこのサイバー協議、一体どのような目的でどのような成果があったのか、これが今後の日本のサイバーセキュリティー立国の推進にどのような位置付けがされるのか、その辺り、外務省の方に説明を願います。

○政府参考人（下川眞樹太君）　お答え申し上げます。

二十一日に、中国北京におきまして初めての日中韓サイバー協議が開催されました。日本から河野章外務省総合外交政策局審議官兼サイバー政策担当大使が出席いたしましたが、外交当局だけではございませんで、内閣官房情報セキュリティセンター、総務省、経産省、防衛省の関係者の方々の参加も得て実施されたところでございます。

今回のサイバー協議は、最初の協議ということもございましたので、最近のサイバー環境やサイバー分野における三か国のそれぞれの施策ですとか戦略ですとか、そういったようなことについて意見交換、協議を行いますと同時に、それぞれの国が、国連サイバー政府専門家会合、ＵＮＧＧＥ、ないしはＡＳＥＡＮ地域フォーラム、ＡＲＦ、そういった国際的なプロセスにおいてサイバー問題についてどういうふうに取り組んでいるかと、そういったようなことについて意見交換を行ったところでございます。

今回の会合の目的でございますけれども、こういう協力を通じまして、今後どういう分野で協力ができるのか、そういったようなことについて協議をすると。それから、何よりも各国がそれぞれどういう考え方を持っているのかという、その辺の基本的な考え方を共有するということには意義があるところでございますので、今後どういうところで具体的な協力があり得るのか探求していこうということになったところでございます。今後も対話を継続するということで、サイバー政策に関する外交当局間でのやり取りも続けていくということを確認したところでございます。

したがいまして、本件対話は継続はしていくということでございますけれども、今後どういうふうにしていくかということについてはまだ何も決まっておりませんで、その辺につきましては、今後外交ルートを通じて調整していく予定でございます。

○浜田和幸君　やはり中国にとっても国際的な批判とかいうことは大変敏感になっていると思うんですね、来月はＡＰＥＣの総会が北京でありますから。ですから、国際的な安全なネット空間ということは彼らも今は真剣に対応せざるを得ない状況だと思いますので、是非こういう対話を続けて、やはり日本からサイバーセキュリティーの規範を作っていく、それにやっぱり無法な行為を取り締まる、場合によっては強制的な方向転換を促すような、そういう外交努力も是非続けていただきたいと思います。

それで、北朝鮮もこのサイバー攻撃に関しては大変物議を醸しておりますよね。この過去四年間見ても、ダーク・ソウル・ギャング、これは北朝鮮のハッカー集団ですけれども、四年間にわたってＤＤｏＳ攻撃を韓国に集中的に行っています。当然、それは日本にも影響してくる。そういうことは今回の北京での会合の中では共通の危機問題として共有されたんでしょうか。

○政府参考人（下川眞樹太君）　今回の協議の具体的な中身については、事、事案の性質もあり差し控えたいというふうに思いますが、やはりこのサイバーの話をいたしますときに、サイバー犯罪の問題ですとか、サイバーテロの問題ですとか、それに対してどういう規範が、国際法上の規範が適用できるのかとか、それから各国がそれに対してどういうふうに対応しているのか、そういったようないろいろな側面から意見交換をしたというのは事実でございまして、それぞれの国が抱える問題について率直にいろいろと意見交換をしたということでございます。

○浜田和幸君　中国も韓国もこの国連ＧＧＥには加盟しているわけですから、そういう国際的な圧力、国際的な基準の中で違法行為というものを取り締まるということで、是非積極的に動いていただきたいと思います。

次に、サイバーセキュリティ基本法そのものについて質問をしたいと思いますが、基本法の第十五条二項に相談に応じて必要な情報の提供及び助言ということが述べられているんですが、一体誰がどのような制度をつくるのか。先ほど山口大臣の答弁の中でサイバーボランティアというようなことも言及ありました。相談業務に一体誰がどういう形で応じるのか、今どういうことが考えられていて、必要な人材育成、どういう形で取り組もうとされているのか、その点について説明をお願いします。

○政府参考人（谷脇康彦君）　お答え申し上げます。

情報セキュリティー人材の育成でございますけれども、これは政府といたしましても極めて重要な課題であるというふうに認識をしております。昨年の六月に情報セキュリティ政策会議で決定をいたしましたサイバーセキュリティ戦略を受けまして、政府としても人材の発掘、育成、活用を進めているところでございます。サイバーセキュリティーに関する相談に応じ、必要な情報の提供や助言を行う人材の育成につきましては、サイバーセキュリティ戦略を踏まえて、先ほど山口大臣から御答弁を申し上げましたようなサイバー防犯ボランティアですとか、情報セキュリティサポーターと呼ばれる地域の身近な相談相手の育成を支援する取組を政府としても促進をしているところでございます。

今後とも引き続き、官民の適切な役割分担の下、こうした人材の育成が進むよう政府として積極的かつ必要な支援を実施してまいりたいというふうに考えております。

○衆議院議員（遠山清彦君）　浜田委員の御質問に少し補足的に、議案提出者の立場からお答えをしたいと思います。

第十五条に相談に応じて必要な情報の提供及び助言を政府がせよということを書かせていただいているわけでありますが、この意味は、従来、サイバー攻撃といいますと政府機関などが対象とされていたわけでございますが、最近は国民のスマートフォン保有率が五〇％を超えておりますし、今日の審議の中でもネットバンクの不正送金被害の問題が指摘されたりしておりますが、要するに、国民一人一人が、あるいは企業がサイバー攻撃の被害を受ける可能性が高まっております

し、実際に既に受けていると、こういう認識を我々持っておるわけでございます。

法文を読んでいただきますと、例えば御指摘のあった第十五条の一項のところには、国は中小企業その他の民間事業者やあるいは大学、教育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ということに鑑みて、これらの者が自発的に行うサイバーセキュリティー対策、ですから、自発的というところが大事でございまして、国は国民一人一人や企業が自発的に自らを守るための取組を支援をしていくという意味で、しかし、これは非常に専門的な知識とか技術が要求されますし、日進月歩で技術も革新をされていくエリアでございますので、ですから、政府としてあるいは地方公共団体としてできる限りの支援はしていきましょうと。しかし、考え方は、自発的という表現が何度もこの法文の中に出てまいりますとおり、個々の国民や企業の自助努力というものも重要であるという考え方が入っているという御認識を持っていただければと、こう思っております。

○浜田和幸君　もちろん、個々人あるいは個別の企業、自治体が自発的な取組というのは大前提だと思うんですけれども、御指摘あったように、なかなか個人ではそういうサイバー攻撃には十分な対処ができない。そういうことで、国が、第十四条でも、サイバーセキュリティーに関しては、基準の策定、演習及び訓練、情報の共有に必要な施策を講じるとありますよね。

また、同じ基本法の第十九条では、サイバーセキュリティーに関連する産業、これは成長産業なんだと。おっしゃったように、個々人が自分の情報を守るためには、しかるべきそのソフトを導入したり、あるいはそういうアドバイスを受ける、これは成長産業になり得るわけですよね。ですから、それは企業にとっては新しいビジネスチャンスでもあるわけですね。

国が応援するという立場と、その問題があるから企業の側はそのサービスを提供することでビジネス、成長産業に結び付けよう。ですから、国が大きな方針でサポートするんだけれども、個別の企業のビジネスチャンス、これは、取捨選択するような場合には、どの企業のソフトを推奨するのか、あるいはどの企業の研究開発に支援をするのかによってかなり、この自主的なということを強調すればするほど個別の企業からすると、必要な情報なんかは出さないでそれを、大事な虎の子の情報ですから、それでビジネスに結び付けようとしますよね。そうすると、国がこの自発的な動きを応援するといってもやっぱりバッティングする部分が出てくると思うんですが。

そこで、国と企業との、民間との役割、そこで、基準の策定、演習などをやる場合にどういうような協力体制を想定されているのか、その点について、提案者及び政府の方から、現在考えておられる計画があればお示しいただきたいと思います。

○政府参考人（谷脇康彦君）　お答え申し上げます。

基本法案の第十四条でございますけれども、これは、重要社会基盤事業者等、いわゆる重要インフラ事業者等に関する情報セキュリティーの確保の規定でございます。

政府におきましては、昨年六月に策定をいたしましたサイバーセキュリティ戦略等に基づきまして、この重要インフラ事業者等に関する必要な施策を実施をしているところでございます。

具体的には、重要インフラ分野におけるＩＴ障害が国民生活等に重大な影響を及ぼさないよう、重要インフラ所管省庁等とも密接な連携を図りつつ、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んだ安全基準の整備、浸透、あるいはＩＴ障害発生時における対応能力向上のための分野合同での演習、あるいは官民の情報共有体制の強化等の諸施策を推進しているところでございます。

加えて、本年五月、情報セキュリティ政策会議におきましてこの重要インフラの情報セキュリティー対策に係る第三次の行動計画を策定をいたしまして、社会・技術面での環境変化を踏まえた個別施策の改善、補強を行うこととしたところでございます。

引き続き、このサイバーセキュリティー対策に関しまして、重要インフラ事業者等に対しまして必要な施策を積極的に推進してまいりたいと、かよう考えているところでございます。

○衆議院議員（平井たくや君）　サイバーセキュリティー対策というのは、やっぱりＲアンドＤなんかのハイレベルの話と社会のボトムアップをする話、両方やらなきゃいけないと思っています。

委員の問題意識も恐らくそうだと思うんですが、中小企業のサイバーセキュリティー対策というのは恐らく今の多くの経営者の頭の中にはない話だと思います。そこを新しく、コストに見合ったセキュリティー対策ができるようなものが進むような、これは我々これから考えていきますが、政府に対して、税制による支援であったり、また研究開発の成果を生かした支援であったり、そういうものをこれから政府にお願いをしていきたいと考えています。

○浜田和幸君　是非、そういう自発的な動きを応援していただきたいと思います。

最後に、第二十条に、技術力の自立的な保持という言及がありますね。これは恐らく暗号ソフトのことを言及されている部分があると思うんですけれども、我が国ではクリプトレックが暗号の評価を行っておりますが、やはりその中で、アメリカのソフトを使うとか、国産のソフトは必ずしも十分使われてない面があるので、ここのところをしっかり押さえておかないと、山下委員がおっしゃったような、アメリカに全部筒抜けになってしまう、バックドアでアメリカのソフトを使っていれば全部、ＴＰＰの交渉内容までアメリカに盗まれてしまうという現状があるわけですから、その辺りの暗号技術に関する自国製、日本製の開発について、最後に、どういう方針で、現在どうなっているのか、お答えいただければと思います。

○委員長（大島九州男君）　谷脇内閣審議官、簡潔にお願いします。

○政府参考人（谷脇康彦君）　はい。

サイバー攻撃が複雑巧妙化する中で、海外の技術あるいはサービスや製品への依存度が現在高いという点は今委員御指摘のとおりでございまして、暗号技術を含めた研究開発等を通じて国際競争力を強化をするということが大変重要だというふうに考えております。

政府といたしましては、本年七月に情報セキュリティ研究開発戦略改定版を決定したところでございまして、委員御指摘の暗号技術の件も含めまして、日本としての独自技術の開発を含めてこれからも積極的に推進をしてまいりたいと、かように考えているところでございます。

○浜田和幸君　以上で終わります。ありがとうございました。

○山本太郎君　よろしくお願いします。新党ひとりひとり、山本太郎と申します。

いまだに携帯はガラケー、しかもパソコンはキーボード、右手一本、左手一本で打つという僕なんですけれども、このサイバーセキュリティーのことについて、中学生でも、あっ、中学生の方が詳しいですかね、お年寄りでも山本太郎でも分かるように教えていただけると幸いです。よろしくお願いします。

このサイバーセキュリティ法、ＩＴ基本法の中にはなかったもの、先ほど提出者の先生方が言われていました。要は、安全という部分が抜け落ちていたものに対して、そこを補完していかなきゃいけないんだというようなお話、趣旨のことを言われていたと思うんですけれども、この件に関して、サイバーセキュリティ法に関して、基本法に関して、どれぐらいの期間の話合い、どれぐらい前から準備というものが行われていたんでしょうか、教えてください。

○衆議院議員（平井たくや君）　先ほどお話ししたとおり、ＩＴ基本法、正確にはもっと長い法案ですけど、これが二〇〇一年に制定されて、このサイバーセキュリティーの問題は二〇〇四年、二〇〇

五年辺りから、まあ体制がつくられたのは二〇〇五年ということになると思いますが、それからも、その時点でももう既に幾つかのセキュリティーに関する心配事というのはありました。

これは自民党政権のときも、また民主党政権のときも、そのサイバーセキュリティーに対応していかなきゃいかぬという問題意識はずうっとありながら個別対応ということだったんですが、そういう長年の議論を積み重ねた上で、もういよいよ社会が大きく変わったと、これから先は更に加速度を付けて変わる中でいかに社会全体を守るかということで、もう一回、そのＩＴ基本法の目的に照らして、その次の社会の進化、発展、国民の幸福ということを考えたときに、このタイミングで出さなければならぬということで、実はそういう長い年月の間の議論が積み重なってここに基本法になったということでございます。

○山本太郎君　まさに十年越しぐらいですよね。今日やっとこの日を迎えられたと、もう練りに練った法案なんだということだと思います。

サイバー攻撃、これ、定義って何なんですかね。誰がどのように判断して決めていくのかということを教えていただけますか。

○衆議院議員（平井たくや君）　この法案の中ではサイバー攻撃というものを明示して定義しているわけではないんですが、サイバーセキュリティーという言葉を法文の中で定義しました。ですから、その状態を壊されるものが攻撃ということになろうかと思います。具体的には、いわゆる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を通じた電子計算機に対する不正な活動であると規定しており、ネットワークを通じて不正に電子データを改ざんするような行為はこれに含まれる。

しかし、非常にややこしいのは、企業にとって、また個人にとってのリスクは必ずしもネットワークにつなげていなくても起きるんですね、今は。だから、そういうことを考えると、今の安全な状態が壊されるものは全てその攻撃の一つの形だろうというふうに我々考えています。

○山本太郎君　この法案に対して不安がある部分というのは、やはり個人情報という部分がどんどん吸い上げられちゃうんじゃないかなと。それが本当に、今までであれば、例えば令状を取ってきて、それに対して対応するとかというような形がありましたけれども、それもサイバーセキュリティーという部分、犯罪という部分を防ぐためにも、そういうのを取っ払って全て吸い上げられるような状況にされちゃうとすごく怖いなと思うんですけれども。

基本法の全文を読みますと、国民の権利については、三条六項に留意しなくてはならない、これしか書いてないようなんですけれども、これ、留意って弱くないですか、表現として。これ、辞書で調べたんです。そしたら、気に掛けるって出てきたんですよね。これ、人々の権利に対して留意、気に掛けるって、結構上から目線かなって思っちゃうんですよね。本当にこの法律で人々の権利が奪われるようなことがないならば、保障するって書いてもいいんじゃないかなって思うんですけれども。

先ほど、ＩＴ基本法では安全という言葉が一度しか出てこなかったんだよって先生方からお聞きしました。それぐらいセキュリティーが抜け落ちているものだと言えるというような表現があったと思うんですけれども、でも、この国民の権利について、この基本法は三条六項に留意という言葉しか出てこないという話なんですよね。ある意味で、これ、国民の権利について、ひょっとして抜け落ちてしまう可能性もありますよね。これ、留意っていうのは、先ほど言ったとおり、気に掛けると出てきたと。もっと強い言葉ではっきりと、この法案が、この基本法が、サイバーセキュリティーによって人々の権利が侵害されることがないんだ、それを保障するという言葉がないと、なかなかこの法案に対して安心しましたということは言えないかなと思うんですけど、いかがでしょうか。

○衆議院議員（遠山清彦君）　大変重要な御指摘、ありがとうございます。

国民の権利を不当に侵害しないように留意というところで、留意という表現が弱いのではないかという御指摘が中心の御質問だったと思いますが、私どもといたしましては、この法律を作る際に、他の過去の法案等も参照いたしましてこういった表現にさせていただきました。

ただ、先生の御懸念は私共有をいたしているわけでございますが、そもそも今回の法案が目指しておりますのは、国民あるいは企業あるいは地方自治体、それから政府の機能、こういったものを悪意を持ってサイバー空間によって多様な形態の攻撃をしてくるところから守るための政府の体制づくりや施策を促す法律になっているわけでございます。

よって、私が申し上げたいことは、今回のこの法案によって、何か国民の権利をそもそも制限しようとしているのではなくて、逆に言えば、分かりやすく言えば、インターネットというのは、今、国民が国民の知る権利を行使する際に極めて重要なツールになっております。山本委員もそうだと思いますし、私もそうですが、ぱっと分からないことがあったときに、今は、あっ、ガラケーだと難しいところもあるかもしれませんが、スマートフォンを持っている方々は、もう分からないことがあったらすぐぱっとスマートフォンでその事柄を調べるということをやっているわけでございます。

ですから、国民の知る権利を充実させていくための一つのツールにインターネットやスマートフォンがなっているというわけでございまして、ここが悪意を持っているサイバー攻撃によって損害を被らないように守る体制をどうしていくかという観点で今回の法律が作られているという、それが目的であるということでございますので、もちろん、冒頭に申し上げましたように、国民の権利がこの法案によっていかなる形でも不当に侵害されることはあってはならないということは、先生がおっしゃるとおりでございます。

○山本太郎君　ありがとうございます。

一番心配しているのは、例えばですよ、時の権力者が暴走し過ぎてしまったりということは、常々あるわけじゃないですか、歴史の中でも。（発言する者あり）済みません、ストレートに言わなかったことをお許しください。そのような状況が考えられるわけですね。

そのときに、この基本法というか、このサイバーセキュリティーという法律が、何というんですか、そのやいばが、やいばがといいますか、悪意を持って攻撃してくる人たちを取り締まるというものが、この情報を吸い上げられるということに関して国民にやいばが向いてしまうというような危険性もあるのかなというふうに思っちゃうんですよね。

サイバー空間の犯罪対策として、サイバーセキュリティ戦略三十二ページには、「サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。」とあります。

これ、私が一番心配しているのは個人情報に関して、そしてこの通信履歴、ログについてなんですよね。僕、ログってことさえも知らなかった。ログって何と言ったら、今までインターネットで検索したものがどんなものを検索してきたかという履歴が残るあれだよと。あっ、それはまずいなと思いませんか、皆さん。恥ずかしくないですか、自分の今まで検索してきたものが見られるって。ちょっと人には言いづらい、それがばれてしまったらぽっと頬を赤らめてしまうような検索、皆さん一度はしたことありますよね、一度どころか二度、三度も。それが表に出てしまう。誰かに知られてしまうなんて最低ですよ。

で、これ、ログに関してなんですけれども、どのような検討が行われていますか。

○政府参考人（谷脇康彦君）　お答え申し上げま

す。

サイバー攻撃への対応につきましては、国の治安あるいは安全保障、危機管理上、極めて重要であるというふうに認識をしております。一方、サイバー空間におきましては、国境を越えて攻撃を実行することが可能であり、他国に所在するサーバーを経由したり、ソフトウエアを用いて攻撃元を秘匿したりするなど巧妙な手段が用いられることもあり、攻撃者を特定することは必ずしも容易ではなく、また通信の秘密の観点から、制度面の検討は慎重に行うべきであるというふうに認識をしております。

こうした点を踏まえながら、昨年六月の情報セキュリティ政策会議で決定をいたしましたサイバーセキュリティ戦略や、昨年十二月に閣議決定をいたしました「世界一安全な日本」創造戦略におきまして、サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方について検討する旨盛り込まれているところでございます。

通信履歴の保存につきましては、通信の秘密との関係、セキュリティー上有効な通信履歴の種類、保存する通信事業者等における負担、こうした点を勘案した上でサイバー犯罪における捜査への利用の在り方について政府として検討を進めてまいりたいと考えております。

○山本太郎君　ちょっと余り意味が分からなかったというか、このログの保存に関してどのような検討が進んでいるかというのをもっと端的に、例えばここまでが制限されるとか、ここまでが勝手に吸い上げられるとかというような具体的なことって何かお聞きできないですか、短めに。

○政府参考人（谷脇康彦君）　具体的に検討すべき事項といたしましては、憲法が保障しております通信の秘密の観点からどのように理解すればいいのか、あるいはセキュリティー上有効などういう種類の通信履歴、通信ログがその対象となるのか、また、保存をする通信キャリアにおいてどの程度の財政的な、経営的な負担になるのか、こういった様々な点を総合的に勘案する必要があるだろうというふうに考えております。

○山本太郎君　結構、まだざっくりとしか決まってないんですか。結構、もうちょっと具体的に言えそうなものだと思うんですけれども。だって、もう十年ももんでいる話なんでしょう、これって。十年間、やっと今日という日が来たという話なのに、どういうことを話していますかということに対して、どういうような決まりになりそうですか、どういうことが盛り込まれそうですかということに対して、すごくざっくりとしか答えていただけてないという感じがするんですけど。

○政府参考人（谷脇康彦君）　現在、政府部内、関係省庁間におきまして協議を進めているところでございまして、現時点での明確な方向性についてはコメントを差し控えさせていただきたいと思っております。

○山本太郎君　協議をしている途中です、検討中です、差し控えさせていただきますって、これ結局、何のことかよく分からないということですよ。一体何なんだと、このやり取りはと。

この法案、いただいている法案にはもっともらしいことしかほとんど書いてないわけじゃないですか。何か聞いても検討中だ、審議中だ、詳しいことは言えないという話になるんだったら、ほとんど内容の分からないものに対して僕たち審議しているということになるんですかと。ちょっとぐらい情報をくれてもいいんじゃないかという話と思うんですけれども。

このログに関して、通信履歴ですよね、自分がどういうものを検索したとかという履歴だったり、あと、どういう人に手紙を送ったかとかというものに関して、現状では、現在では令状があれば後で差押えができますよというだけですよね。法的な義務はないと、そういう状況ですよね。これひょっとして取っ払われるという可能性もあるわけですよね。そういうことについてはお話しできない状態ですかね。

○衆議院議員（遠山清彦君）　山本委員の問題意識を理解、正確にしているかどうか分かりませんが、ここの、まず今日御審議をお願いをしているこの法案が成立をした後に、この法律に基づきましてサイバーセキュリティ戦略が策定されていきます、新たな。先ほど検討状況と政府側が答弁しておりましたのは、そのまさに、この法案の成立の後に作られるサイバーセキュリティ戦略の中で、もちろん委員にもはっきりと分かる形で、国民にも分かる形でこのログの保存の在り方等について策定がなされるという御理解を持っていただければと思います。

なお、一点だけ御指摘申し上げますが、このサイバーセキュリティ戦略の中で事後追跡可能性を確保するとなっている対象はサイバー犯罪でございますので、サイバー空間でネット検索する方々全ての人のログを追跡するわけではないということは、今の時点でもはっきりと書かれていると認識をしております。

○山本太郎君　ですから、先ほどから言っているとおり、その時の権力者であったりとかというものの使い方によっては、どこまでも網を張れるよという状況になるわけですよね。これ、そう思いませんか。だって、これ、サイバー犯罪という……（発言する者あり）法律というのはそういうものだと言われたってしようがないですよね、でも。もちろん、そういう意見もあると思いますよ。法律ってこういうものなんだよ、まず基本法を作るんだよ、その後に内容を決めていくんだよという話になりますけど、でも、もう既に後のものって準備されているでしょう、普通に考えて。

だって、これ、基本法を通った後にみんなで一緒に作っていきましょうと言ったら、何年掛かるんだよという話になりますよね。もう既に作られているというものがあるんだったら、この基本法、その後に作られているものがひょっとしてまずいんだったら、基本法の段階で止めたいじゃないですか。まず骨組みだけチェックしてくださいということで、その後控えているものに対して、ひょっとして雨漏りするような、何というんですか、部品が使われている家かもしれないし、建設予定の家かもしれないし、そういう部品のチェックというのも多少は流していただけたらいいのになと思うんですよね。

そういうものなんだよと言われればもうそれまでで、もう質問を終わらせていただきますという話になっちゃうんですけどね、済みません。（発言する者あり）済みません、ありがとうございます。骨組みがおかしいという質問をするべきだ、勉強させていただきます。

不正アクセス禁止法のとき、警察の主張に反して総務省がずっと賛成しなかったためにログ保存というものが入らなかったんだよという話を聞いているんですけれども、人々の権利のために当時郵政省は、今の総務省は闘ってくれていたんですね。このことに対して御存じの方。

○政府参考人（吉田眞人君）　平成十一年当時でございましたけれども、不正アクセス禁止法制定に際しまして、通信履歴の保存に関しましては、当時、捜査の必要性と通信の秘密との関係、あるいはプライバシー保護への配慮、あるいは事業者等への負担、当時の国際的な動向等、様々な観点を踏まえまして、総合的に判断をいたしまして通信履歴の保存に係る規定が盛り込まれなかったというふうなことになったというふうに承知をしているところでございます。

○山本太郎君　ありがとうございます。

でも、今回は転んじゃったんですかね、これが、こういう話が進んでいくということは。

この個人情報の収集、保全に関してヨーロッパではスタンスが変わったよと、先ほどもお話がありました。ヨーロッパでも、アメリカがヨーロッパの首脳に対していろいろ盗聴とかしていたということがばれて激怒していたけれども、実際は自分たちの国でもやっていたんだと、いろんな盗聴が行われていたんだというような、メールの内容とかも見ていたんだというような話が表沙汰になったと。

そのヨーロッパでは、二〇一四年の四月八日、

ヨーロッパの司法裁判所、これ最高裁よりも上ですよね、上の裁判所になるヨーロッパの司法裁判所、通信会社などに通話や電子メールの送受信の記録保持を義務付けた現行制度について、私生活の尊重と個人情報保護という基本的権利を侵害するとして無効を言い渡したと。結局、そういう使われ方をしちゃうんだと。結局、それは、司法裁判所の方でそれはないだろうと、やっぱりまずい、無効だという話にしちゃったという話なんですよね。

当然ですよね、プライバシーですから。それを守ろうとした、それを守ろうとする成熟した社会が確かに存在するんですよね、世界には。我が国がサイバー基本法を端緒として個人情報の収集、簡単に行える方向に行くんだったら、これ今の世界の流れと逆行するんじゃないかなと思うんですね。

時間もないようですので、ちょっと先に進みたいと思います。

もし、ウィキリークスのような活動にプロバイダーがサーバーを提供するようなことがあったとしたら、犯罪に便宜を図ったとして国家への協力義務違反とされるということはあるんですかね。あるかないかでお答えいただけると助かります。

○委員長（大島九州男君）　どなたが答弁しますか。

○山本太郎君　御存じの方。どなたが御存じか分からないんですよね。多分、法案提案者の方が一番御存じなのかなとは思うんですけど、そういうサーバー、おまえ提供したなということで、それ。

○衆議院議員（遠山清彦君）　委員、済みません。委員の今のお話は、ウィキリークスのようなところに個人が、あるいは企業が情報を……

○山本太郎君　サーバーとして、企業だったり……

○衆議院議員（遠山清彦君）　プロバイダーですね。

○山本太郎君　はい。ごめんなさい。

○衆議院議員（遠山清彦君）　プロバイダー会社がウィキリークスのようなところに情報を提供したら、この法律に規定されている国に対する民間会社の協力義務違反になるのかということでもし質問がよろしいのであれば、それは、この法律で求めている民間企業に対する協力義務というのは、基本的にはサイバー空間における安全を確保することに資する情報の提供でございますので、このプロバイダーがウィキリークスのような組織に情報を流したことをもって、ここの協力義務違反にはなりません。

ただ、指摘しておかなければならないのは、そのプロバイダーがウィキリークスのような外部の団体に提供した情報の内容によっては、別の法律で違反事項として見られる可能性はあるかと思います。

○山本太郎君　国会議員の存在価値の要だと思うんですけど、国政調査権が脅かされるというようなことにつながらないですか、質問変わりましたけど、この法律が、先々。

○衆議院議員（遠山清彦君）　結論から申し上げますと、サイバーセキュリティーを確保することを目的とし、情報の自由な流通が阻害されないようにするための法律でございますので、私ども立法府の一員である議員の国政調査権には全く影響を与えないと、このように認識をいたしております。

○山本太郎君　ありがとうございます。

それだったらいいんですけれども、でも、第三者機関を制定しないまま発足してしまうような状況ですよね、これ、このまま行くと。そういう状況の中で、じゃ、それを利用するのが誰なのか、そのときに権力を持った人が暴走する人であれば全く違う方向にも使えてしまうよなということを危惧しての質問でした。

ありがとうございます。

○委員長（大島九州男君）　他に御発言もないようですから、質疑は終局したものと認めます。

これより討論に入ります。

御意見のある方は賛否を明らかにしてお述べ願います。

○山下芳生君　私は、日本共産党を代表して、サイバーセキュリティ戦略基本法案に対して反対の討論を行います。

本法案は、サイバーセキュリティーを軍事、安全保障に密接に結び付けるものであります。法案は、目的に我が国の安全保障を明記し、新設するサイバーセキュリティ戦略本部がサイバーセキュリティ戦略案を作成する際に、国家安全保障会議、NSCの意見を聴かなければならないとしています。

政府が昨年十二月に決定した国家安全保障戦略は、アメリカとのサイバー防衛協力の推進を掲げ、先日公表された日米ガイドライン見直しの中間報告でもそのことが位置付けられています。アメリカはサイバー空間を、陸、海、空、宇宙に次ぐ第五の戦場に位置付け、攻撃と防御の両面から体制づくりを進めています。

衆議院における審議の中で、法案の提案者は、本法案は有事を想定した国家機能強化の中核の一つと答弁し、サイバー対策が真にできる国は自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の認識を示し、日米の連携を強調しました。こうした下で、サイバーセキュリティ戦略は、日米軍事同盟の強化の一翼を担うことになるものであり、極めて重大です。

また、法案は、サイバーセキュリティ戦略本部が、安全保障に係る重要事項に関してNSCと緊密な連携を図るとしています。提案者は、NSCとの連携について、外国政府等が関与したサイバー攻撃の場合が考えられると答弁してきましたが、本部にそのような関与の分析や判断ができないことは審議を通じて明らかとなりました。緊密な連携の内容も全く不明瞭なままであります。

そもそも、安全保障や日米軍事同盟に密接に関わる法案でありながら、議員立法として提出され、政府が責任を持たず、官房長官、防衛、外務などの関係大臣からの責任ある答弁もないまま成立させようとしていることは、到底許されません。

また、僅か一時間半の審議で採決するなど言語道断であることも述べて、反対討論とします。

○委員長（大島九州男君）　他に御意見もないようですから、討論は終局したものと認めます。

これより採決に入ります。

サイバーセキュリティ基本法案に賛成の方の挙手を願います。

〔賛成者挙手〕

○委員長（大島九州男君）　多数と認めます。よって、本案は多数をもって原案どおり可決すべきものと決定いたしました。

この際、藤本君から発言を求められておりますので、これを許します。藤本祐司君。

○藤本祐司君　私は、ただいま可決されましたサイバーセキュリティ基本法案に対し、自由民主党、民主党・新緑風会、公明党、みんなの党及び新党改革・無所属の会の各派共同提案による附帯決議案を提出いたします。

案文を朗読いたします。

サイバーセキュリティ基本法案に対する附帯決議（案）

政府は、本法の施行に当たり、次の諸点について適切な措置を講ずべきである。

一　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。

二　サイバーセキュリティ戦略本部と内閣情報通信政策監との連携の下、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。

三　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、高度情報通信ネットワークの特性を踏まえた総合的な視点から策定すること。

四　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。

五　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。

六　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。

七　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常域制御の在り方について検討すること。

八　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。

以上です。

何とぞ委員各位の御賛同をお願い申し上げます。

○委員長（大島九州男君）　ただいま藤本君から提出されました附帯決議案を議題とし、採決を行います。

本附帯決議案に賛成の方の挙手を願います。

〔賛成者挙手〕

○委員長（大島九州男君）　多数と認めます。よって、藤本君提出の附帯決議案は多数をもって本委員会の決議とすることに決定いたしました。

ただいまの決議に対し、山口国務大臣から発言を求められておりますので、この際、これを許します。山口国務大臣。

○国務大臣（山口俊一君）　ただいまの決議につきましては、その趣旨を十分に尊重して、サイバーセキュリティーの確保に努めてまいりたいと存じます。

○委員長（大島九州男君）　なお、審査報告書の作成につきましては、これを委員長に御一任願いたいと存じますが、御異議ございませんか。

〔「異議なし」と呼ぶ者あり〕

○委員長（大島九州男君）　御異議ないと認め、さよう決定いたします。

本日はこれにて散会いたします。

午前十一時四十三分散会

平成二十六年十一月七日印刷　　平成二十六年十一月十日発行

参議院事務局　　印刷者　国立印刷局

P