第百九十回国会 参議院内閣委員会会議録第十号

平成二十八年四月十四日（木曜日）

午前十時開会

委員の異動

四月七日

辞任　補欠選任

堀井　巌君　岡田　広君

藤本　祐司君　前田　武志君

四月八日

辞任　補欠選任

前田　武志君　藤本　祐司君

四月十三日

辞任　補欠選任

山東　昭子君　舞立　昇治君

風間　直樹君　大野　元裕君

藤本　祐司君　芝　博一君

四月十四日

辞任　補欠選任

福岡　資麿君　山田　修路君

芝　博一君　藤本　祐司君

出席者は左のとおり。

委員長　神本美恵子君

理事

井上　義行君

上月　良祐君

相原久美子君

山下　芳生君

委員

石井　準一君

岡田　広君

岸　宏一君

酒井　庸行君

世耕　弘成君

二之湯武史君

福岡　資麿君

舞立　昇治君

山田　修路君

大野　元裕君

藤本　祐司君

牧山ひろえ君

山本　香苗君

江口　克彦君

山田　太郎君

山本　太郎君

国務大臣

国務大臣　遠藤　利明君

内閣官房副長官　世耕　弘成君

内閣官房副長官　松本　文明君

副大臣

内閣府副大臣　若宮　健嗣君

厚生労働副大臣　黄川田仁志君

防衛副大臣　三ッ林裕巳君

大臣政務官

外務大臣政務官　熊田　裕通君

厚生労働大臣政務官　藤田　昌三君

防衛大臣政務官

事務局側

常任委員会専門員　土生　栄二君

政府参考人

内閣官房内閣審議官　向井　治紀君

内閣官房内閣審議官　谷脇　康彦君

内閣官房内閣審議官　河内　隆君

内閣府大臣官房審議官　山本　哲也君

警察庁警備局長　沖田　芳樹君

総務大臣官房審議官　宮地　毅君

総務大臣官房審議官　池永　敏康君

総務省総合通信基盤局電気通信事業部長　大橋　秀行君

外務大臣官房審議官　水嶋　光一君

文部科学大臣官房審議官　生川　浩史君

経済産業省商務情報政策局長　安藤　久佳君

原子力規制委員会原子力規制庁次長　荻野　徹君

防衛大臣官房審議官　笠原　俊彦君

防衛省地方協力局次長　谷井　淳志君

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及び情報処理の促進に関する法律の一部を改正する法律案（内閣提出、衆議院送付）

○参考人の出席要求に関する件

○委員長（神本美恵子君）　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、堀井巌さん、風間直樹さん、藤本祐司さん及び山東昭子さんが委員を辞任され、その補欠として岡田広さん、大野元裕さん、芝博一さん及び舞立昇治さんが選任されました。

○委員長（神本美恵子君）　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及び情報処理の促進に関する法律の一部を改正する法律案の審査のため、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土生栄二さん外十四名の出席を求め、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（神本美恵子君）　御異議ないと認め、さよう決定いたします。

○委員長（神本美恵子君）　サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律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。

○井上義行君　自由民主党の井上義行でございます。

今回のサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の中身についてお伺いをしたいんですが、ＩＴの時代に当たって、私が役所に入ったときにはまだワープロの時代でございまして、それから随分、非常にＩＴの分野が広がったというふうに思っております。一方で、年金流出という形で、世界各国とつながることによってこうしたサイバーセキュリティーの重要性というのは非常に高まっています。

今回の改正で年金流出のような事案が起きないような対策を十分取っていただけるというふうに思っておりますが、そこで、今回、情報処理安全確保支援士というものを資格としてつくるということでございますが、これは多分高度な、実践的な知識、技能が求められるというふうに思ってお

りますが、一般的な国民に対してどういうような具体的業務内容を行うのか、簡単に説明をお願いします。経産省、お願いします。

○政府参考人（安藤久佳君）　お答え申し上げます。

今先生御指摘のように、サイバーセキュリティーに関します高度かつ実践的な知識や技能を備えた専門人材というものを想定をさせていただいております。

具体的な業務といたしましては、様々な組織におきますセキュリティーシステムの構築、組織内の体制の整備、これは言わば平時からの対応でございます。また、いざ現実に攻撃が行われた際におきますサイバー攻撃の分析、そして緊急事態の対応、こういったもろもろの業務に関します専門的な観点からの調査とか指導、助言、そしてこれに関する人材の教育、こういったものを想定させていただいております。

○井上義行君　この資格制度ができることによって、その資格に合った能力、知識というのが分かるということだというふうに思っております。

そして、サイバーテロを起こす人々というのはどんどんどんどん技術を変えていくわけですね。いずれ人工知能的なものができれば、その人工知能でどんどんどんどんそれを先に行ってしまうということが考えられるというふうに思っております。そこで、やはり事案が発生をしたときにいかに早くそれを伝えるかということが非常に大事だと思いますが、そのスピーディーな伝達方法というのはどういうものが考えられますでしょうか。

○政府参考人（安藤久佳君）　大変重要な御指摘だと思います。まさにサイバーセキュリティーに関します攻撃技術は日進月歩だと思っておりますので、それを守るサイドの専門人材の知識、技能というものを最新のものにしていかなければいけないというのは御指摘のとおりでございます。

メールマガジンとかあるいはウエブサイト、こういったようなものをＩＰＡの方でしっかりと整備をさせていただきまして、情報処理の支援士の皆様方に最新かつ実践的なサイバーセキュリティーに関する様々な情報の提供ということを日々行わせていただきたいと思っております。

また、制度といたしまして、資格者に対しまして最新のサイバーセキュリティーの事例あるいはその対策方法などの内容を含めた講習を定期的に受講していただく、こういったことを資格制度そのものの条件といたします更新制度を導入させていただきたいと、かように考えております。

○井上義行君　そして、国内にかかわらず、海外との連携強化というものが必要になってくるというふうに思います。二国間という形もあれば国際会議という場もあるでしょうし、あるいは多国間ということもあります。こうした取組は政府としてどのように考えているか、遠藤大臣、よろしくお願いします。

○国務大臣（遠藤利明君）　おはようございます。お答えいたします。

サイバー空間を取り巻くリスクが大変深刻化しておりますが、国境を越えた自由な情報の流通を可能とするサイバー空間の便益を享受するとともに、国家の安全保障、危機管理上の課題でもありますサイバー攻撃に迅速かつ的確に対応するためには諸外国等と効果的に連携することが必要と認識をしております。

政府としましては、管理や規制を過度に行うことはなく、開放性や相互運用性を確保することにより、情報の自由な流通が確保された安全で信頼できるサイバー空間を構築することを基本的方針として関係国との国際連携に取り組んでおります。こうした認識の下に、昨年九月に閣議決定をされましたサイバーセキュリティ戦略においても、多様な主体との国際的な連携により、サイバーセキュリティーの確保及びサイバー空間におけるグローバル規模の情報の自由な流通の確保に向け取り組むこととしております。

具体的には、米国、イギリス、オーストラリア等との二国間の協議、対話を通じ各国と連携を強めるとともに、国連の政府専門家会合や官民を含む幅広い参加者を得たサイバー空間に関する国際会議等の多国間の国際会議への積極的な参加を通じまして、サイバー空間に関するルール作りや意識啓発、ＣＳＩＲＴ間協力、情報共有の強化等に積極的に貢献しているところであります。

今後とも、サイバーセキュリティ戦略に基づき、関係各国との連携を積極的に深めるとともに、多国間の議論にも積極的に貢献してまいりたいと考えております。

○井上義行君　そして、今まで内閣サイバーセキュリティセンターが担ってきた仕事が、今度、独立行政法人情報処理推進機構、ＩＰＡ、ここに委託をするわけですが、やはり今までやってきた国の仕事をこのＩＰＡに委託をするので、より慎重に仕事を進めていく必要がある、そのためにはＮＩＳＣとそしてＩＰＡが一緒に連携を深めていく必要があるのではないかというふうに思っております。

そこで、その連携の在り方について、内閣官房の審議官にお伺いをしたいと思います。

○政府参考人（谷脇康彦君）　お答え申し上げます。

今回の改正法案を踏まえまして、サイバーセキュリティ戦略本部が行います監査あるいは原因究明調査の事務の一部を、独立行政法人情報処理推進機構、ＩＰＡに委託をすることを予定をしております。

ＩＰＡに事務を委託するに当たりましては、ＮＩＳＣとＩＰＡとの間におきまして攻撃情報を始めとする脅威情報等について情報共有を行うことに加えまして、ＩＰＡからＮＩＳＣへの職員の任用を通じた人的な交流についても積極的に行いまして、委員御指摘のＮＩＳＣとＩＰＡとの間の連携を密にしていくこととしております。

なお、ＮＩＳＣとＩＰＡとの間で円滑、適切に連携を取ることができるよう、今回の改正法案におきましては、併せて、委託事務に従事する職員の守秘義務と、これに違反した場合の罰則を盛り込んでいるところでございます。

○井上義行君　そこで、ＮＩＳＣの方々は公務員が多いので、私も公務員だったので、多分、採用するときにある程度の身元がはっきりしている部分があるんですが、今度のこのＩＰＡですね、ここは民間が多分多くなると。そうすると、採用時に当たってより慎重な身分の身元確認であるとかこうしたことが、犯罪が起きないような人を採用しなきゃいけないと。

その対策、出入り管理とかあるいは職員の管理のセキュリティー、こうしたことをどういう形でやっていくのかをお伺いしたいと思います。経産省、お願いします。

○政府参考人（安藤久佳君）　お答え申し上げます。

委託業務の実施に当たりましては、まさに様々な分野から極めて優秀な人材を採用させていただくとともに、情報管理を徹底することが大切だと思っております。

今回の法改正におきまして、ＩＰＡの役職員には法律上の秘密保持義務、こういったものを掛けさせていただくということを想定をしております。これは、ＩＰＡを退職した後も秘密保持義務は適用されるということでございます。

また、職員の現実の採用の際には慎重に人物の面談をして、身分の確認などこういったことを徹底して行いたいと思っております。また、現実の委託業務に任用する際には、重ねて面談などを行いまして業務の担当として信頼できる人物かを確認をしていく、こういったことを徹底させていただきたいと思っております。

○井上義行君　そしてもう一つ、この法案でポイントになるのがサイバーセキュリティ・情報化審議官だというふうに思います。あの年金流出のときに、話を聞いて、すぐに何かこれはおかしいなという形になっていれば防げたものがあったという教訓があると思います。この中で、今度はこの審議官が高度な知識を持っていないと結局同じ過ちを犯してしまうと。我々事務方というか、技術屋と多分分かれていくと思うんですが、やはりこ

うした審議官がある程度の知識を持って配置されないと、下からこういう事案が起きているというときに反応ができないと思うんですね。

そこで、大臣の構想の中でこうした審議官の配置をどう考えているのか、お尋ねしたいと思います。

○国務大臣（遠藤利明君）　サイバーセキュリティ人材育成総合強化方針において、各府省庁は、平成二十八年度に新設したサイバーセキュリティ・情報化審議官等の主導の下、セキュリティー、ＩＴに係る体制の整備や人材の拡充等に取り組むこととしております。

これらを踏まえ、当該審議官等においては、組織の規模や所管するシステム等の実情を踏まえつつ、これらの取組を円滑に進めるための司令塔としての総合調整力が求められております。また、セキュリティー、ＩＴに関する更なる知識も必要であることから、当該方針において、当該審議官等も含めた管理職向けにセキュリティー、ＩＴについての研修等を実施していくこととしております。

内閣官房においても、当該審議官等が各府省庁において主導的な役割を果たしていくことができるよう、各府省庁との連携の強化に努めてまいります。

○井上義行君　そして、国民の間でマイナンバーは果たして大丈夫なんだろうかというような声があるというふうに思います。

今回、監査、監視、原因の究明調査の対象が国の独法、特殊法人、認可法人に広がったわけですね。マイナンバーというのは地方公共団体情報システム機構になるわけで、そうすると、そのマイナンバーを管理しているところが、じゃ果たして今回の対象になるのか、それとも独自に総務省でやっていくのかという関心になるというふうに思いますが、このマイナンバーの運用をする地方公共団体情報システム機構、これは対象になるんでしょうか。内閣官房、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。

委員御指摘の地方公共団体情報システム機構、いわゆるＪ－ＬＩＳは、地方公共団体情報システム機構法に基づきまして設立をされております。かつ、その設立に当たっては総務大臣の認可を要することから、今回御審議をいただいておりますサイバーセキュリティ基本法上の認可法人に該当をするところでございます。

サイバーセキュリティ戦略本部による指定の対象とするか否かにつきましては、当該機構及び所管省庁である総務省と調整、検討をしてまいりたいと考えてございます。

○井上義行君　そして、何もかも国が監視をするとどこかの国と同じようになってしまうという危険性から、それぞれ、国の機関はＮＩＳＣが担う、で、独立行政法人とか認可法人は今回のＩＰＡがやると。

そして、日本を見渡すと、サイバーセキュリティーに関わるいろんな、病院だとか、あるいは金融機関、あるいは交通機関、こういうものもあるんですね。多分、こうした分野は当然自前で自分たちの防衛のためにやっていると思うんですね。しかし、それだけでは足らない場合が出てくるというふうに思っております。そのときのＮＩＳＣの支援というのはどういう形が考えられますでしょうか。内閣官房、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。

社会経済システムを始めあらゆるものがネットワーク化されつつある中、個人情報の窃取、経済的な犯罪から重要インフラシステムの破壊に至るまで、サイバー攻撃等によるリスクはますます深刻化をしてきているものと認識をしております。

委員御指摘の病院、金融機関、それから交通機関等のいわゆる重要インフラに係るサイバーセキュリティー対策につきましては、この三月末に開催をされましたサイバーセキュリティ戦略本部におきまして、重要インフラの情報セキュリティ対策に係る第三次行動計画の見直しに向けたロードマップが決定をされたところでございます。

具体的には、経営層における取組の強化の推進などのサイバー攻撃に対する体制の強化、情報共有範囲の拡大など重要インフラに係る防護範囲の見直し、国際連携等多様な関係者間の連携強化、こういった点を柱といたしまして、重要インフラ防護の更なる対策の強化に向けましてこのロードマップに従い検討を進め、行動計画の見直しについては平成二十八年度、今年度末を目途に結論を得ることとしております。また、このロードマップにおきまして早急に対処すべき事項につきましては、先ほどの行動計画の見直しを待たずに対処をすることとしているところでございます。

今後とも、関係機関が互いに緊密に連携しながら、重要インフラ事業者等と一体となってサイバーセキュリティー対策を進めてまいりたいと考えてございます。

○井上義行君　そこで、サイバーテロを防ぐにはどのぐらいの人が必要で、あるいは予算が必要になってくるのか。私が想像しても分からないんですね。お金を掛ければいいというものでもないし、人を多く取ればいいという、無限にやれば一番いいんでしょうけど、そこは財政事情からいろいろ絞っていかなきゃいけない。その中でもしっかり対応していかなきゃいけない。

そうすると、適正な予算の規模というのは大体どのぐらいのイメージを持っているんでしょうか。大臣、難しいと思いますが、お願いします。

○国務大臣（遠藤利明君）　政府機関に対するものを始めとして、サイバー攻撃は質量共に大変深刻を増しておりますし、予断を許さない状況にありますから、サイバー攻撃の対応は国家の安全保障、危機管理上の重要な課題と認識しております。

そうした中で、サイバーテロの脅威に対しましては、警察において関係機関と連携した国内外の情報収集、分析等の対策を推進するなど、関係省庁においても取組を進めております。それらの取組を含めまして、サイバーセキュリティーに関する予算については、政府全体として、平成二十七年度補正予算において五百十四億円を確保していただき、また平成二十八年度当初予算として四百九十九億円を計上しているところであります。

委員から御質問ありましたように、サイバーセキュリティーに関する適切な予算の規模については一概に申し上げるのは大変難しいわけでありますが、引き続き、政府として最適な予算や人員の確保に取り組むとともに、御審議いただいておりますサイバーセキュリティ基本法改正法案に盛り込んでおります情報処理安全確保支援士制度の円滑、実効ある運用等を通じ、サイバーセキュリティー対策の強化を図ってまいりたいと考えております。

○井上義行君　今言われたその予算あるいは人の配置、この中で私一番心配しているのが、これは答えなくていいんですけれども、あくまでも要望として聞いていただきたいんですが、例えば事務の管理は、管理職から見て、ああ、あいつこうだなとか、ちょっと最近生活が乱れているなとか、ある程度目に見えるものなんですが、でも、こういうものというのは、目に見えない、どういうものをやっているかというその管理というものが重要になってくると思いますので、こうした研修とかあるいは内部犯罪の防止についてちょっと御検討をいただければというふうに思っております。

そして、何もかもが、先ほど申し上げたとおり、国で管理をしていると何もできなくなってしまうということもあって、やはりこれからはサイバーセキュリティーの分野の産業化というものを考えていく必要があるのではないかというふうに思っております。こうしたサイバーセキュリティーの関連産業の育成を政府としてはどのように考えているでしょうか。経産省、お願いします。

○政府参考人（安藤久佳君）　お答え申し上げます。

まさに御指摘のとおり、我が国のサイバーセキュリティーを確保していく上におきましては、企業のサイバーセキュリティー投資を現実に促していきまして、サイバーセキュリティー関連産業

がまさに成長産業となる、こういった環境整備を促していくことが大変重要であると思っております。

企業のサイバーセキュリティー投資を促すためには、まず企業の経営者自身が攻撃リスク等対策の必要性、こういったことについて十分認識をしていただいて、経営の最重要事項として取り扱うと、こういったことが重要であるというふうに思っております。このため、今年度から、重要インフラ事業者の制御システムを中心にいたしまして、高度なサイバー攻撃に対する現実の防御力を確認するためのある種のテストをＩＰＡが中心となって実施をしていきたいと、このように考えております。

またさらに、企業の対策の実施がいわゆる市場から評価をされる、こういった仕組みなどによりまして対策への投資に対しますインセンティブを高めていく、こういったことも大事だと思っております。例えば企業の対策の度合いに応じましてサイバーセキュリティー保険の保険料を割り引く仕組み、こういったものの普及を働きかけていきたい、かように考えております。

○井上義行君　最後になりますけれども、こうしたサイバーセキュリティーの分野、専門分野ですね、技術もあればあるいは内面の部分もあると思います。こうしたことを初等教育からやはりしっかりと教えていく必要があるのではないかというふうに思っております。将来の課題として、遠藤大臣、非常に教育部門に今まで尽力を尽くしていただいた方でございますので、そうした経験を是非このセキュリティー分野にも生かしてもらいたい。その意味で、こうした教育の分野をどう考えていくのか、大臣に最後にお伺いしたいと思います。

○国務大臣（遠藤利明君）　今委員御指摘ありましたように、サイバーセキュリティーの人材育成こそ最大の課題だと思っておりますし、そうした育成については技術面と倫理面の両方が重要と認識をしております。

サイバーセキュリティ人材育成総合強化方針に基づいて、産学官連携した教育、演習環境の整備、資格制度の整備等、知識と実践力を身に付ける取組を推進していくこととしております。また、委員御指摘のように、高い倫理観も同時に身に付ける必要があるために、初等中等教育段階から情報セキュリティーを含む情報モラルの理解等を促す取組も併せて進めているところであります。

今後とも、セキュリティー人材の確保、育成については、産学官の連携を十分に行いつつ積極的に取り組んでまいります。

○井上義行君　是非そういう取組をしていただきたいと思います。

これで終わります。

○委員長（神本美恵子君）　この際、委員の異動について御報告いたします。

本日、芝博一さんが委員を辞任され、その補欠として藤本祐司さんが選任されました。

○大野元裕君　民進党・新緑風会の大野元裕でございます。

久しぶりに内閣委員会に来させていただいて、質問をさせていただくことになりました。理事各位、委員の皆様の御協力ありがとうございます。

さて、サイバーセキュリティ基本法でございますが、二年前に議員立法で作られたものであって、民間における経済活動分野から安全保障分野まで幅広く対象としております。したがって、一元的に対応するところときめ細かく分野ごとに対応するところ、両方あると思っています。

政府の一元的なサイバー対応についてちょっとお伺いしたいんですが、この法律に基づいてサイバーセキュリティ戦略本部が法制化をされまして、その事務を担う内閣サイバーセキュリティセンター、いわゆるＮＩＳＣは内閣官房組織令で設置をされることにより推進をされたというふうに理解をしています。そこで、大臣、サイバーセキュリティ戦略本部及びＮＩＳＣの権限強化の成果についての評価を、簡潔で結構でございますので、教えていただきたいと思います。

○国務大臣（遠藤利明君）　サイバーセキュリティ戦略本部は、基本法制定により、ＩＴ総合戦略本部決定に基づいて、情報セキュリティ政策会議から法律に基づき内閣の下に直接設置される本部となったものであります。これにより、権限や所掌事務などの位置付けが明確にされました。簡単にということでございますから。

こうした具体的な戦略本部は、各省庁に対する監査、事案発生時の原因究明調査に関する事務等を所掌することとされ、加えて、本部長による監督権等が規定されたことにより、従来の枠組みに比べ各省庁に対するサイバーセキュリティーに対する権限が強化をされました。昨年の年金機構の情報流出事案についても、厚生労働大臣に勧告を行ったところであります。

情報セキュリティ政策会議が決定していたサイバーセキュリティ戦略も、基本法に基づき戦略本部が案を作成し、閣議決定、国会報告を行うこととされました。現在、昨年九月に閣議決定、国会報告を行ったサイバーセキュリティ戦略に基づき、内閣サイバーセキュリティセンターでは年次計画等を策定し、戦略の着実な推進に努めているところであります。

サイバーセキュリティ戦略本部及びその事務局でありますＮＩＳＣとしましては、基本法の趣旨を踏まえ、サイバーセキュリティーの司令塔としてサイバーセキュリティー対策の強化を図ってまいりたいと考えております。

○大野元裕君　ありがとうございます。副本部長として大臣にも御活躍を期待しますし、今のまさに成果は全く私も同じように共有をしており、そこは感謝をさせていただきたいと思っています。

他方、大臣、現行法の附則第二条におきましては、内閣官房に置かれるＮＩＳＣの法制化を含む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を求めています。内閣官房組織令でＮＩＳＣが規定されたことは重々承知していますが、条文は法令化ではなくて法制化、法律によってＮＩＳＣを制定しろと、そういうふうに求めていますけれども、この附則第二条のＮＩＳＣの法制化はいかに実現されたか、教えてください。

○国務大臣（遠藤利明君）　委員御指摘のように、情報セキュリティセンターの法制化を含む必要な法整備を行うということが基本法の附則で、二条で盛り込まれておりまして、これを踏まえて政府としましては、昨年一月、基本法の施行に合わせて内閣サイバーセキュリティセンターを設置をいたしました。

具体的には、内閣法第二十五条において、内閣官房の所掌事務を遂行するため必要な組織については政令で定めるとされていることから、内閣官房組織令を改正し、内閣官房セキュリティセンターを法令上位置付けたところであります。

○大野元裕君　内閣官房に設置されているＮＩＳＣの権限強化というものは国会の意思です。与野党が一致して議員立法で発議をし、そして審議をし、各行政機関に関する監査を含むＮＩＳＣの事務については法制化、法律でやれということを要求をいたしました。

資料でお配りしていますけれども、基本法成立に先立つ平成二十六年ですか、の五月の十九日の情報セキュリティ政策会議においても、政府としてサイバーセキュリティ政策会議を強力、迅速に補助するためとしてＮＩＳＣの法制化が承認をされています。

そして、冒頭、大臣がおっしゃられたとおり、年金機構に関するサイバー事案への対処を現実的にしたり、ＮＩＳＣがしっかりと機能をするということは実際の現場でも重要であったというふうに答弁されたと私は理解をしておりますけれども、そういった権限強化も実績もあります。だからこそ、我々は議員立法として、国会の意思を明確にしたこの基本法の附則において、法律でＮＩＳＣの権限を明確にすることを求めました。私が聞いている範囲では、法制局の方で、法技術

的に組織令でこれ規定すれば十分ではないかという、そういうこともあったようですが、ただ、大臣、法技術でそこに法律ではなくて政令で定めればいいということであれば、これまでも総理大臣命令でＮＩＳＣは設置されていましたから、それで十分だといえばそれで十分で、そのままになってしまうわけですよね。我々国会の意思というのは、法律でこれをしっかりと定めること、そして、今回の現実の世界でも一元的な対処というものの成果が出ているわけですから、これやはり法律で私は定めるべきだと思いますよ。

そして、それどころか、今回新しく出てきた法律を見ると、ＮＩＳＣの法制化は見送られています。政令だけです。しかしながら、ＮＩＳＣから独法に事務を委託することだけは法令化されているんです。アンバランスだとお思いになりませんか。しかも法律が、明文化して、明文として要求している国会の要求を無視して、そして今回、法律からその附則文は削除されています。こういった形を内閣提出の法律で削除するというのは国会軽視ではないでしょうか。

大臣、アンバランスで、国会軽視のこういった法律の書き方というのは、私はとても不適切だと思いますけれども、大臣の御見解を賜りたいと思います。

○国務大臣（遠藤利明君）　今委員から御指摘がありました附則第二条の中に、「情報セキュリティセンターの法制化を含む。」というふうな文言になっておりますが、この法制化には法律と政令と両方あると承知をしております。そこで、内閣法の第二十五条には「内閣官房の所掌事務を遂行するため必要な内部組織については、政令で定める。」と書いてありますので、そのような形で決めたということでありますので、アンバランスではないと承知をしております。

○大野元裕君　しかしながら、ＮＩＳＣは法律で定められておらず、そこが委託をする独法、この規定は法律で定められている。要するに、一番上は法律です。一番下も法律です。真ん中は法律じゃないんですよ、大臣。だから申し上げているんです。というのは、我々は先ほど申し上げたとおりしっかりと、大臣、皆様の仕事をサポートさせていただきたい。そういった意味で、自民党さんの方から提示された議員立法ですから、自民党さん自体も私これ疑問に感じるべきだと思っていますよ。我々、これ賛成したんです。その上で、法令化ではなくて法制化ということを盛り込んでいます。

大臣、今回法律出ていますし、私、委託すること自体は我が党としても賛成でありますので、そこについては評価をしますけれども、しかし、ここ、つまりＮＩＳＣの権限をしっかりとしていただいて、これから万が一の場合に対処するためにも、ＮＩＳＣの法制化については、この法律通ったら、大臣、是非法制化検討していただけないですか。政治家として、是非政治主導でお願いしたいです。

○国務大臣（遠藤利明君）　これからの進め方については、引き続き検討していきたいと思っております。

○大野元裕君　よろしくお願いします。

余り引っ張ると中身の話できないので、少し中身の話をさせていただきたいと思います。

それと同時に、実は一昨年のサイバーセキュリティ基本法が採択された際には参議院でも附帯決議が付されています。その第三項には、情報通信関連機器等の安全性に関する基準については防護対象の重要性の段階に応じたものにするということが求められています。つまり、政府の統一基準だけでは駄目だというふうに言っているんです。

防衛省は別途本件について検討しているようですけれども、サイバーセキュリティ戦略本部としては防護対象の重要性の段階に応じた機器等の安全性に関する基準を定めるために何を行ったんでしょうか。

○国務大臣（遠藤利明君）　政府機関につきましては、サイバーセキュリティ戦略や政府統一基準に基づき、防護対象の業務や情報の重要性に対して適切な対策を取るように求めております。一例を挙げれば、特に重要な情報を扱うシステムについてはインターネットから分離を求め、残るインターネットに接続するシステムについては業務のリスクに応じて優先順位を付した上で多重防御を図ることとしております。また、政府全体としてインターネット接続口の集約化を図ることにより、監視や防御をより効果的、効率的にする取組を進めているところであります。

一方、重要インフラに係るサイバーセキュリティー対策については、重要インフラの情報セキュリティ対策に係る第三次行動計画において、重要インフラサービスの持続的な提供のため、経営層がリスク源の評価及びそれに基づく優先順位を含む方針を決定するということとしております。さらに、重要インフラとしての機能保証の考え方に立脚し、サイバー攻撃に対する体制強化を推進するため、平成二十八年度末を目途に行動計画を見直すこととしております。

今後とも、官民の関係機関が互いに緊密に連携し、サイバーセキュリティー対策を進めてまいりたいと考えております。

○大野元裕君　私、今大臣のお話を私なりに理解をすると、重要インフラについては別途基準を作ったと、しかしそれ以外については、特に安全を必要とするものやアクセスポイント等については運用でやれということを決めているということだと思いますので、私は、若干これ、大臣、我々が求めた附帯決議とは違うと思っています。

さらに、この機器等の安全性に関する基準についてですけれども、具体的にちょっとお伺いしますが、例えばハードウエア・トロージャン・ディテクション、つまり、国内技術でこれ実は対処されていないと私は理解していますが、半導体のチップは今海外から輸入するものがどんどん多くなっています。こういったチップの中に不正なもの、あるいは悪意のあるものが埋め込まれている、こういったものを検知する技術というものは日本で確立を私はされていないと理解をしていますけれども、附帯決議を実現するためには、こういった新たな要請に対して技術の確立をすることが必要になっていると思います。

したがって、大臣、是非お伺いしたいのは、附帯決議を実施する前提として、こういった技術の確立に向けてどのような行動を政府は取ってきたんでしょうか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

政府統一基準など安全性に関する基準を定めるに際しては、技術的な知見を適宜反映させていくことが大変重要でございます。

昨年九月に閣議決定をいたしましたサイバーセキュリティ戦略におきまして、ＩＣチップを含むハードウエアの真正性の検証等に係る技術開発を行うという方向性を出しているところでございます。また、本年一月に閣議決定をいたしました第五期の科学技術基本計画におきましても、ハードウエアの真正性を確認する技術等の開発、それからその社会実装を推進することとしております。

これに関連しまして、戦略的イノベーション創造プログラム、ＳＩＰの課題としまして、重要インフラ等におけるサイバーセキュリティの確保に係るプロジェクトを実施しており、この取組の中で製造段階での不正機能の混入を確認する機器テスト技術に係る研究開発を進めることとしているところでございます。

○大野元裕君　つまり、進めることとしている方向性を定めるということでございますので、安全性の基準を定める以前の問題でまだとどまっているというふうに私は理解をせざるを得ないと思っています。

更にお伺いをしますが、やはり附帯決議の防護対象の重要性の段階に応じた対応で、これ、たしか内閣委員会で私、前回質問をさせていただいたと思いますが、例えば韓国などではインフォコンというシステムを持っていて、現実の世界で安全保障上の脅威が起きたときにはレッドアラートとかイエローアラートとか、こういった段階を設け

て、いわゆる現実の世界に対応したサイバー上の危機対応を行っていますけれども、附帯決議を受けて、政府は段階に応じた対応、これ実施をする方向で検討したんでしょうか。

○国務大臣（遠藤利明君）　先ほども申し上げましたとおり、新たなサイバーセキュリティ戦略の下、政府機関については政府統一基準に基づき、また重要インフラについては重要インフラの情報セキュリティ対策に係る第三次行動計画に基づき、各々取組を進めております。あわせて、先ほど政府参考人からお答えしましたように、機器等の安全性に関する基準を定めるための技術開発等の取組を進めることとしております。

　これらの取組を通じて、今後とも官民の関係機関が互いに緊密に連絡し、サイバーセキュリティー対策を進めてまいりたいと考えております。

○大野元裕君　要するに、やっていない、重要インフラのところは。そこは分かりました。それはおっしゃるとおりです。しかし、それ以外については検討もしていないということなんではないかなと私は思いますけれども。

　もう一つ附帯決議について、これ総務省所管だと思うので総務省にお伺いしますが、やはり附帯決議では実効性のある帯域制御の在り方を検討するということが求められています。平時における帯域制御の運用基準に関するガイドラインについては既に何度も説明いただいていますので、これは結構です。そうではなくて、前提がサイバーセキュリティーですから、有事の際のＩＳＰ側での帯域制御についてはどんな検討を行って、どんな措置を施したんでしょうか。

○政府参考人（大橋秀行君）　総務省において、平成二十五年十一月から、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会というものを開催をしております。これは、サイバー攻撃が巧妙化、複雑化する中、電気通信事業者が攻撃への対策や取組を新たに講じることができるようにということで検討を進めてきているものであります。

　この検討会の中で附帯決議にもあります帯域制御の在り方についての検討というものが行われて、例えば通信の秘密に属する情報を利用する場合について、これを正当業務としてみなせる場合についての整理を行うなどの対策を講じることによって、事業者によるサイバーセキュリティー対策というものの実効性を高めるという取組を進めてきているところでございます。

○大野元裕君　それは平時の話ですよね。しかも二〇一五年からでありますから、我々の附帯決議を受けてという話では毛頭ありません。

　大臣、先ほどの話に戻りますが、附則第二条では、法律では規定をしない。それから、段階に応じた、政府統一基準だけではないものについては、重要インフラはやるけれども、ほかはやらない。そして、技術の確立についてはまだ道半ばである。それから、重要性の段階に応じた防護対象の対応については、やはりやっていない。それから、ＩＳＰ側の実効性のある帯域制御の在り方については、別途有事については検討していない。これが我が国会が求めたことに対する政府の対応の現状であります。新しく内閣が提出する法律があるのであれば、こういったものはしっかりと対応してから法律出すというのは当然の話だと私は思います。

　大臣、改めてお伺いをさせていただきますけれども、国会が要求をいたしました法律そして附帯決議について、真摯にもう一度御検討いただけるということを明確に御答弁をいただけないでしょうか。

○国務大臣（遠藤利明君）　委員御指摘のように、附帯決議を踏まえて引き続き検討を進めてまいりたいと考えております。

○大野元裕君　大臣、オリンピック・パラリンピックで本当に御苦労されていること分かりますし、これ技術的なことが多いので、これ以上正直突っ込みません。いや、正直、大変だとよく分かっていますから。

　だけど、真摯にお願いしたいと思うんです、是非。というのは、これサイバーの話は真剣に、万が一の場合が起こったときには我が国の安全保障を根底から覆す可能性がある、だからこそ平時だけではなくて有事も含めて我々は議論をしなきゃいけないということを申し上げているので、恐らくこの後の附帯の御提案もあろうかと思いますけれども、そこについては真摯に御対応いただきたいということをお願いをして、次の質問に移らさせていただきますが。

　大臣、少し質問の順番を変えて、三問飛ばしますが、本法におきましては、独法の監査業務を委託する法人が今後業務を実施することに、あるいはできるということになっています。国の行政機関によっては、その保秘の在り方、あるいはインシデント発生の際の関連企業等の特約条項などについて、省庁ごと、行政機関ごとに差があります。例えば、防衛省の関連企業による情報漏えいが発生した場合などはまさにそういった対応を行うというふうに以前改正されたと私は理解しています。

　だとすると、大臣、お伺いしたいんですが、想定される監査業務を委託する法人が、この法律では独法等に対してですけれども、仮にこれらの行政機関の監査業務を行うとすれば、これらの秘密事項や異なる特約事項の義務をそれぞれ履行するということができるんでしょうか。そこは大臣の御見解を賜りたいと思います。

○国務大臣（遠藤利明君）　今回の改正法案におきましては、第三十条第一項の規定において、サイバーセキュリティ戦略本部から委託を受けた法人は、独立行政法人及び戦略本部が指定する特殊法人、認可法人に対する監査、原因究明調査事務の一部を行うこととしております。

　したがって、改正後の規定においても、委託する法人に行政機関への監査業務を行わせることは想定しておりません。

○大野元裕君　私もそれが適切だと思います。だとすると、独法等についてはどうなのかということが今度問題になります。

　そこで、これは防衛省にお伺いをしたいんですけれども、政務官、エルモというのがありますですよね。これは米軍で勤務をする職員の個人情報等を扱っています。これらの独法に対し、この法律では守秘義務が委託される独法に課せられることになりますけれども、ほかの独法と同じような守秘義務条項で十分に我が国、国際の安全、米軍等のオペレーション、これらについて安全を担保するということができるというふうにお考えかどうか、教えていただきたいと思います。

○大臣政務官（熊田裕通君）　お答えいたします。

　先ほど、エルモの質問でございますが、在日米軍施設に勤務する駐留軍等労働者の雇入れ、提供、労務管理、給与及び福利厚生に関する業務は、雇主である防衛省及びエルモ、独立行政法人駐留軍等労働者労務管理機構が行っております。これらの業務は在日米軍に必要な労働力を確保する上で必要不可欠な業務であり、エルモでは駐留軍等労働者の給与の支給に必要となる情報や福利厚生の実施に関する情報等、人事管理上必要となる個人情報を保有しております。

　エルモが保有している当該個人情報には、在日米軍の部隊運用に関わる情報は含まれていないものの、当該個人情報の漏えい等はあってはならず、情報の保全については防衛省及びエルモにおいて日本の法令及び基準等にのっとり万全を期しておるところでございます。

　今後、サイバーセキュリティ基本法が改正され、エルモがＩＰＡにより不正な通信の監視、監査、原因究明調査等の対象となる場合にはエルモの情報セキュリティー対策が強化されることになると認識しておりますが、いずれにいたしましても、防衛省としても引き続きエルモにおける情報保全に万全を期するように努めてまいりたいと思っております。

○大野元裕君　政務官、おっしゃっていることの意味分かりますか。先ほど大臣にもお伺いしましたけれども、行政機関によってはそれぞれ機微な

ものがあって、これはやはり行政機関にはなかなか独法が監査をするというのはなじまないだろうと先ほど大臣おっしゃいました。

エルモに関して申し上げると、例えばサイバー上の世界ではこんな事件が起きています。米軍では高官がフェイスブックなんかで書き込みをしています。そのフェイスブック等の書き込みを見た人が、悪意のある人が、そのフェイスブック等の書き込みからポジションを類推をして、米軍の高官だということをフェイスブック上の書き込みからそこで知った。そして、その高官は当然軍事や安全保障に影響力を行使することができる人ですから、そういった人がどこにいるのかということを実はサイバー上では探すことができるんです。

エルモは、もちろん運用については全く承知していないと思っています。ところが、米軍の運用情報等は持っていませんが、米軍の基地労働者、配置、その家族、そういったものまで一元化して持っているんですよ。つまり、悪意のある、悪意のあるですよ、攻撃者やそういった人たちが、万が一、こういった人たちの全体の情報を把握してしまった、そして仮に在日米軍の活動や我が国の安全保障に影響が出るような事態が起こった際に、政務官、防衛省として、あるいはエルモとして、いや、その情報は実は独法が監査していました、しかも、その監査を行っている守秘義務あるいは保秘に関する規定は、例えば年金を扱っているとか、ほかの政府の機関と全く同じでした、これで話、言い訳が付くんでしょうかね。胸張っていらっしゃるんでしょうか。

危機感が余りに欠如しているように私には思えるんですけれども、もう一度、政務官、ここについては別途やはり私は基準を設けるべきじゃないかと思いますけれども、いかがでしょうか。

○大臣政務官（熊田裕通君）　様々今御指摘をいただきました。

まずエルモは元々、先ほど委員御指摘ありましたように、労務上必要な情報を共有するということで、米軍の部隊の運用等のそういった秘密のものについては情報は取っておりませんので、御指摘をいただきました、今新しいインターネット等のお話もありましたけれども、先ほど大臣がお答えをさせていただいたように、様々なことを考えながら、またこれは引き続き検討していかなきゃならないことだと思っておりますので、よろしくお願いいたします。

○大野元裕君　そこは応援しますので、是非お願いします。

次の質問ですけれども、これ今度は警察庁にお伺いしたいと思っています。

サイバーセキュリティーの世界では、サイバー上で全てが完結するわけではありません。日米のガイドライン等でも議論になりましたけれども、属性や足跡、いわゆるアービトレーションとか、あるいはアトリビューションと呼ばれるところが大変重要でございます。こういった属性や足跡、いわゆるリアルの世界については警察がやはり秀でている分野だと私は理解をしています。他方で、警察は刑事訴訟法の第四十七条で情報の提供の制約というものも当然あります。

そんな中で、サイバーインシデント、特に国際的なテロ組織によるものや国家的な関与が疑われているようなものがあった場合、警察庁は、監査を委託されている法人が監査、調査、原因究明、応急対処、こういったものを行う際に、今までは恐らくＮＩＳＣと協力してきたと思いますけれども、独法との間でこういった捜査情報を含めた秘密情報をこれまでと同様に十分に共有ができるか、教えていただきたいと思っています。

○政府参考人（沖田芳樹君）　委員御指摘のとおり、刑事訴訟法第四十七条におきましては、訴訟に関する書類は公判の開廷前にはこれを公にしてはならないとされ、ただし書として、公益上の必要その他の事由があって相当と認められる場合はこの限りではないとされております。

したがいまして、事案の解明及び同種事案の拡大防止に必要であると認められる場合には、このただし書の趣旨を踏まえまして、監査を委託された法人と捜査情報を共有することは十分に可能であると考えております。

○大野元裕君　そこで、改めて遠藤大臣にお伺いしますけれども、先ほど行政機関にまで法人の事務対象の委託を拡大するというのはやっぱりよくないんじゃないかという話を大臣からもいただきましたが、今のように、やはり実は行政機関だけではなくて、独法も含めて単純に、行政機関もそうですが、拡大するというのは、私は若干問題があるのではないかと思いますけれども、大臣の改めての御見解を賜ります。

○国務大臣（遠藤利明君）　先ほどもお答え申し上げましたが、監査を委託する法人による監査の対象を行政機関にまで拡大することは想定しておりません。

○大野元裕君　それでは、次の質問ですが、今回の法律では監査業務の委託先法人としてＩＰＡが例示をされています。ただ、例示されているんですけれども、ＩＰＡ以外とも書いてあって、その他のと書いてあるんですが、想定されているＩＰＡ以外の法人組織はどこなんでしょうか、教えてください。

○国務大臣（遠藤利明君）　改正法案では、サイバーセキュリティ戦略本部が行う監査及び原因究明調査について、ＩＰＡのほか、サイバーセキュリティー対策について十分な技術的能力及び専門的な知識、経験を有し、当該事務を確実に実施できる法人に委託することを可能としております。委託する法人については、サイバーセキュリティーに関する十分な技術力及び専門性に加え、国の事務を継続的かつ安定的に行うことができるということが必要であると考えております。

ＩＰＡについては、長年にわたりサイバー攻撃に関する情報の収集、分析の実施をするとともに、サイバーレスキュー隊によるサイバー攻撃への初動対応支援を行っていること、また、業務運営や組織の継続性において国の関与があるなど、国の事務を継続的かつ安定的に行うことができることから委託法人として適当であると考えております

が、現時点ではＩＰＡと同等の法人は存在しておらず、他の法人に委託することは考えておりません。

○大野元裕君　ＩＰＡと同等の法人があったら潰せばいいんですから、同じものがあったら。それは同じじゃないですよね。

しかしながら、ＩＰＡができないような分野での長所を持っているところも多分あるんじゃないかと思います。例えば、総務省所管のＮＩＣＴなどは、空きパケットを利用してサイバー上の悪意ある活動をモニターするｎｉｃｔｅｒなどが有名であります。あるいは、ＡＰＴ28や30といったこれまでの攻撃については、果たしてＩＰＡだけで対処できるかどうかについては私は若干疑問とするところもありますけれども。

総務省にお伺いすればよろしいんでしょうか。こういった空きパケットを利用したネットワークトラフィックに対する監視については、ＮＩＣＴなどはそれなりの能力をお持ちで長所があると思いますけれども、いかがでございましょうか。

○政府参考人（池永敏康君）　お答えをさせていただきたいと思います。

総務省所管の国立研究開発法人情報通信研究機構、ＮＩＣＴにおきましては、サイバー攻撃の地理的情報や攻撃量、それから攻撃手法等をリアルタイムに可視化するサイバー攻撃観測・分析・対策システム、ｎｉｃｔｅｒというふうに申し上げておりますが、こうしたものの開発であるとか、それから、委員御指摘のＡＰＴ28そのものについては実施をしておりませんけれども、サイバー攻撃で使用されるプログラムの分析、いわゆるマルウエアの分析ですとか、こうしたサイバーセキュリティーに関する研究開発を実施しているところでございます。

○大野元裕君　そうなんです。ネットワークトラフィック等についてはｎｉｃｔｅｒが強みを持っていると私も思います。

そうすると、独法や指定法人に関するネットワークトラフィックに対する監視はどの組織が今

後行うことになるか教えてください。

○政府参考人（谷脇康彦君）　お答え申し上げます。

ＮＩＳＣにおきましては、各府省等の情報システムのいわゆるインターネットの接続口にＧＳＯＣセンサーを設置をいたしまして、不正な通信等を監視をしているところでございます。改正法案が成立した後におきましては、独立行政法人及び指定法人の情報システムのインターネット接続口に同様のセンサーを設置をいたしまして、ＩＰＡが不正な通信等を監視することを想定してございます。

○大野元裕君　ちょっと理解できていないんですが、教えていただきたいんですが、それジーオー・ドット・ジェーピーのドメインだけじゃないんですか、ＧＳＯＣがやっているのは。

というのは、例えばですけれども、今後対象となり得る組織の中には、国立女性教育会館、宇宙航空研究開発機構、大学評価・学位授与機構、高齢・障害・求職者雇用支援機構などはジーオー・ドット・ジェーピーのドメインではないんじゃないですか。そうだとすると、例えば先ほどのＮＩＣＴでいえば、ＤｏＳ攻撃の跳ね返りを検知するわけですよね。そうすると、早期に違法なトラフィックを見るためにはＧＳＯＣの現時点での能力の外になってしまうのではないかと思うんですけれども、いかがでしょうか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

私どもＮＩＳＣにおきまして、先ほど申し上げたＧＳＯＣセンサーを設置をして不正な通信の感知を行っているわけでございますけれども、これはドメイン名で区別をしているものではございません。すなわち、ジーオー・ドット・ジェーピー以外のドメインを有する法人につきましても、当該法人の情報システムのインターネットの接続口にセンサーを設置する、それによって不正な通信等の監視を行うと、これは可能でございます。

他方、委員御指摘のように、ＮＩＣＴにおいてｎｉｃｔｅｒで得られた攻撃情報、その他脅威情報については、昨年の五月にＮＩＳＣとＮＩＣＴとの間でパートナーシップ協定を結んでおりまして、これに基づいて様々な情報共有を行っているところでございますので、引き続きＮＩＣＴとの間でも連携を図ってまいりたいと考えております。

○大野元裕君　大臣、実は私の問題意識は、今回、監査を委託するわけですね。監査ということは、最初に基準を決めます。そうすると、この基準をＩＰＡができることに定めて、それで監査をさせるのであれば、これはマッチポンプと一緒なわけですけれども、想定のところしかできないんです。

ところが、サイバーというのは、これまでも今までもたくさんいろんな話があるとおり、実は想定外がたくさんある。しかも、想定外どころか、今私が申し上げたように、実は広い分野で想定できることがあるんです。そこについての基準をしっかりとまず定めて、それを幅広く監査をさせるためには、ＩＰＡは僕は評価しています、すばらしいと思っています、ただ、それだけではなくて、それぞれの長所があるところをオールジャパンで固めていく必要がある。だからこそ、一番最初に申し上げた、政府が一元的にコントロールできるというものを上に置いておいて、そして様々な長所があるところを使っていくというのが本来の理想だと私は思うんです。分かります、つまり、何か起こって、それ以外は想定外でしたということが今から想定できるような話だけは是非やめてほしいんですよ。

そこで、実質的にＩＰＡにしか委託を今想定していませんとおっしゃいましたけれども、実はもう既に想定できる脅威ありますから、やはりその外、例えばＮＩＣＴもそうかもしれない、あるいは、質問しませんがＪＰＣＥＲＴ／ＣＣなんかもそうかもしれませんけど、様々な機関を使えるような法律にするべきではないかと、大臣、思うんですが、是非御感想をお聞かせいただきたいと思います。

○国務大臣（遠藤利明君）　大野先生はまさしく専門家でいらっしゃいますから、そうした知見を大変今御披瀝をいただきました。そうした先生始め多くの皆様方の知見また御意見をいただきながら、引き続き検討していきたいと思っております。

○大野元裕君　大臣、ＩＰＡは監査の委託を受けられるように、ＩＰＡ側での実は組織令の変更も一緒に出されています。そうだとすると、これＮＩＣＴの方も組織令変更するべきですよね。大臣、いかがですか。

○国務大臣（遠藤利明君）　今回は提出しておりません。

○大野元裕君　べきですよねと聞いているんですけれども、組織令、ＮＩＣＴ側も変えるべきですよね。

○国務大臣（遠藤利明君）　必要だと考えております。

○大野元裕君　ありがとうございます。

ところが、今回、ＮＩＣＴの組織令は今国会に提出されているんです、改正が。ところが、その中には受けられるような改正が入っていないんです。幅広くやるためには、当然向こうの組織令も改定をする。委託するかどうかは別な話です。先ほど申し上げた想定される危機がある限りにおいては、長所があるところの組織令は変更するべきですよね。

ところが、今回、その組織令が提出されているにもかかわらずこの改正が含まれていないというのは、政府にとって瑕疵じゃないですか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

今委員御指摘のＮＩＣＴ法の改正につきましては、サイバーセキュリティー関連の人材育成等の観点から法改正を行うものでございます。

現時点におきましては、サイバーセキュリティ戦略本部の事務の一部を委託する先につきましてはＩＰＡのみを想定をしております。将来的にＮＩＣＴがその対象になり得るというふうに判断できた場合には、ＮＩＣＴ法の所要の法改正も検討の視野に入ってくるものと理解しております。

○大野元裕君　また話戻します。

先ほど申し上げた、ＩＰＡはそのとおり私はすばらしいと思っています。しかしながら、基準をＩＰＡに合うように定めて監査させても仕方がないんです。想定はなるべく幅広く取ってやるのであれば、今回、しっかりと広げられるような可能性というのは置いておくべきだと。しかも、今回出ていなきゃいいんですよ。ＮＩＣＴの法律に関する改正が出ているんですから、そこは、しかも審議官、お立場は総務省じゃないですから、内閣官房としてお立ちになっていらっしゃいますから、そうだとすると、やはりこれは改正を、今国会出ているんですから、やるべきではなかったんですかと聞いているんです。

○政府参考人（谷脇康彦君）　お答え申し上げます。

ＮＩＣＴは、いわゆる研究開発法人ということでございます。したがいまして、監査等の業務を今後ＮＩＣＴにも委託をするということであれば、この独立行政法人としての位置付け、性格というものも含めて改めて評価をしていく必要があるというふうに考えております。

ただ、今回、このサイバーセキュリティ基本法の改正法案におきまして、ＩＰＡはあくまで例示でございますので、将来的にはそれ以外の委託先はあり得るということを改めて申し上げさせていただきたいと思います。

○大野元裕君　これ法律ですから、悪意のある攻撃者はこれ見ていて、ああ、想定はそれなのかというふうに思う可能性すらありますよ。これで万が一ここに攻撃があったときには、責任そちらですよ。そこは是非しっかりと御認識をいただいた上で、法律立ては分かっています、今後そういったことができることも分かりました、是非早急に御対処をいただきたいし、そこは政治主導で大臣にもお願いをしたいと思っています。

時間がないし、今日は黄川田先生にもお越しを

いただいているので、ちょっと別な話を次にさせていただきますけれども、外務省にお伺いいたしますが、ネットの話というのは日進月歩でございます。サイバー上の環境も大きく変化をしています。サイバー上の安全保障が現実の世界において大規模な被害をもたらす、こういった可能性もいろんなところで指摘をされているところでございますが、その一方で、サイバー攻撃って僕ら余りよく定義として分からないところがあります。

そんな中、一昨年ですか、五月だったと思いますが、NATOの、北大西洋条約機構のウェールズ・サミットにおきまして、NATO加盟国一か国に対する攻撃は他国に対する攻撃とみなして、NATO憲章の第五条適用、つまり集団的自衛権の適用だということを実は宣言しているんです、NATOはサミットにおいて、首脳会議において。

つまりこれ、とても権威ある機関がそういうことを言ったというのは物すごくやっぱり重い話だと私は理解をしていますけれども、仮にNATOが、NATO構成国に対するサイバー攻撃を受けた、そのときに五条適用であるということを言う場合のサイバー攻撃の定義、及び我が国として、国際法上の解釈ですけれども、許容されるサイバー攻撃上の集団的自衛権の行使の範囲というのはどこだというふうに今我が国は考えておられるんでしょうか。

○大臣政務官（黄川田仁志君）　大野委員にお答えいたします。

御指摘のとおり、二〇一四年の九月のNATOウェールズ・サミットにて採択された首脳宣言において、サイバー攻撃についていろいろと議論がされましたが、このサイバー攻撃の定義に関する記述はございませんでした。また、サイバー攻撃が北大西洋条約第五条の援用に当たるか否かについての決定は、北大西洋理事会によりケース・バイ・ケースにて行われる旨、記述がされております。

サイバー攻撃と自衛権の関係におきましては、個別具体的な状況を踏まえて判断すべきものであり、一概に述べることは困難であると考えております。いずれにせよ、これまでサイバー攻撃に対して自衛権が行使された事例はなく、サイバー攻撃に対する自衛権行使の在り方については国際的にも様々な議論が行われている段階であるというふうに承知をしております。

一般国際法上、ある国家が集団的自衛権を行使するための要件などもいろいろなところで申し上げておりますが、武力攻撃を受けた国からの要請又は同意があること、ほかに適当な手段がないこと、必要最小限の実力行使であることというふうに一般的に考えております。

○大野元裕君　済みません、五月じゃなくて九月でしたね。失礼いたしました。

黄川田先生、とすると、我が方これ確認したんですか、NATOに。一般的にとおっしゃいましたが、聞いたんですか、これ。教えてください。

○大臣政務官（黄川田仁志君）　聞いているということではなくて、このNATOウェールズ首脳宣言がございまして、そこの中からこういうことが読み取れるということでございます。

○大野元裕君　それは少し無責任ではないんでしょうか。攻撃をされたときに跳ね返りで攻撃を我が方受けるかもしれない、そういうものです。しかしながら、それがケース・バイ・ケースで分からないとすれば、我が国サイバー上の話ですから、これ何かまだ分からないわけですよね。

実は私、聞きに行っているんです、NATOまで行って。余りにもやっぱりこれ危険ですから。是非、やはり政府としては、どういうケースなんですかというのは聞くのは当然の話じゃないですか。そうじゃないと、我が国攻撃受けるかもしれないんですよ、NATOの条約に当てはまれば。

それはそうじゃないんですというならそれで結構です、もちろん。それは我が国が安全をきちんと守るのは当然の話ですから、政府として。ただ、分からないのなら聞くべきじゃないですか。もう一度教えてください。

○大臣政務官（黄川田仁志君）　このサイバー攻撃についてはいろんなものが想定されるわけでございまして、その様々なケースでどういうことができるかというのは、先ほども申し上げましたが、議論の最中でございますので、ここで申し上げることはできません。

○大野元裕君　さっき聞いていないとおっしゃったんじゃないでしたか。

もう一度確認します。聞いたんですか、聞かなかったんですか。

○大臣政務官（黄川田仁志君）　聞いてはございませんが、国際的にこういう形で様々な議論がなされているという段階でございます。

○大野元裕君　サミットの首脳会議の最終宣言で、これ、採択された文章の中に入っています。だとすれば、これは確かに議論されているものでありますから、明確に文章として表れているものですから、聞くぐらいは当然じゃないんでしょうか。

是非、最後、政務官、私もうこれで質問終わりますけれども、最後に、これから聞きますということは是非御対処いただきたいと思います。

○委員長（神本美恵子君）　時間ですので、簡潔に答弁お願いします。

○大臣政務官（黄川田仁志君）　委員御指摘のとおり、確認いたします。

○大野元裕君　ありがとうございました。

サイバーセキュリティーに関して政府のこれからのしっかりとした対処を望みまして、私の質問とさせていただきます。ありがとうございました。

○山本香苗君　まず最初に、遠藤大臣にお伺いをさせていただきたいと思います。

今回の改正というのは昨年の日本年金機構の個人情報流出事案を踏まえてのものということでございますが、あの事案におきましては、年金機構とそれを所管する厚生労働省との間で標的型攻撃に対する緊急体制も定められていなかった、また、機構がどういうセキュリティー対策をやっていて、それをちゃんと遵守しているかどうかということも事案を発生した後に把握しているというような非常に不十分なものでございました。本来あってはならないことでありましたので、その後の厚生労働省の総括においては、所管法人等に対する監督と情報セキュリティー対策の強化を図って、日常的な対策やインシデント発生時などに緊急対応を行うということを図っております。

この点について政府統一基準ではどう書いてあるのかというと、こうした法人の中でも、各省庁と一体となって公的業務を行う特殊法人等その他機関に対して必要な指導、助言を行うかということについては、行政事務従事者が職制及び職務に応じて与えられている権限と責務を理解した上で負うべき責務を全うすると、このように書いてあるわけです。要するに、どうとでも取れると、意識によっては。高いところはそれなりのことをやるかもしれないけれども、低い意識のところであればこの文言を見てどう取るかと。各省庁に、そこは裁量に任されているんですが、非常に一般的な書き方になっていると思います。

年金機構というのは今回の改正法が成立すれば指定法人と位置付けられますけれども、厚生労働省を始め各省庁はそのほかにも多くの法人を所管しております。各省庁が所管法人の情報セキュリティー対策というのをきちっと監督、確認して、そして日常的にも緊急時にも連携していくということをこれは政府統一基準でしっかりと明示的に書いていくべきではないかと考えるんですが、大臣、いかがでしょうか。

○国務大臣（遠藤利明君）　山本委員につきましては、当時、副大臣として大変御苦労されたとお伺いをしております。

今委員から御指摘がありましたとおり、政府機関やその所管法人は、所掌の業務において機微な個人情報を含む多くの重要情報を取り扱っている場合があり、その適切な管理を国民から期待されていることについて各職員がしっかりと認識を共有した上で所管法人等の指導監督に当たることが重要であります。その観点から、昨年九月にサイバーセキュリティ戦略本部長である内閣官房長官

より厚生労働大臣宛てに出された勧告の中にも今申し上げた趣旨の内容が含まれております。

こうした教訓を広く政府機関で生かしていくためにも、現在見直し作業を進めている政府統一基準群の中に、基本認識をしっかり踏まえた上で、今委員御指摘のように、日常時及び緊急時に連携の取れた対応を取ることの重要性について規定したいと考えております。

○山本香苗君　ありがとうございます。当時、この点が非常に希薄だったということが一つの教訓であると思いますので、是非しっかりとこの基準に書き込んでいただきたいと思います。

その上で、今回の法改正におきましては、今申し上げたように日本年金機構が指定法人と位置付けられるというわけでありますけれども、先ほど井上理事の方の御質問の中にもありました、J―LISは今後総務省と調整、検討するということでございますけれども、J―LISというのは、そもそも今どういうセキュリティーポリシーに基づいて、どういう運用を行っておられるんでしょうか。

○政府参考人（宮地毅君）　お答え申し上げます。

地方公共団体情報システム機構、J―LISは、住基ネットやLGWAN、公的個人認証といったマイナンバー制度の根幹を担うシステムを運用しておりまして、多くの住民の個人情報を保有する法人でありますので、セキュリティー対策は非常に重要であると認識をしております。

J―LISでは、NISCの政府統一基準群等に倣いまして、情報セキュリティ管理規程などによる情報セキュリティポリシーを定めますとともに、このポリシーと併せまして、個人情報を扱う重要な業務につきましては、住民基本台帳法、公的個人認証法などの法令により定めております規定に沿って情報セキュリティー対策を行っているところでございます。

○山本香苗君　ということは、指定法人ではないけれども、今指定法人が求められているようなことは遜色ない形でできているということなんでしょうか。

○政府参考人（宮地毅君）　お答え申し上げましたように、政府統一基準群等に倣いながらセキュリティポリシーを定めております。また、法律に基づく規定に沿いながら、具体的な運用につきましても、組織、体制等につきまして、常勤理事の一人がCISOとして担当しておりまして、また内部のリスク管理課がその事務局としてインシデント時の対応を行うCSIRTの機能も含めて対応しているというふうに承知をしております。

○山本香苗君　先ほどのお話にもありましたけれども、現時点においてはこのJ―LISを指定するということは考えておらず、検討されているということでございましたが、今の時点でこの指定を検討していると。機構のように、認可法人ですから、これ大事ですから指定しましょうとならない具体的な理由をお伺いできますでしょうか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

今回の改正法案によりまして、国による不正な通信の監視等の対象となります特殊法人、認可法人につきましては、その法人におけるサイバーセキュリティーが確保されない場合に生じる国民生活や経済活動への影響を勘案してサイバーセキュリティ戦略本部が指定をするということとしております。

具体的には、法人の業務と国の業務の一体性、それから当該法人が実施する業務に係る保有情報の機微性や、サイバー攻撃等による当該業務の国民生活、経済活動に与える影響、当該法人による自主的なセキュリティー対策のみに委ねることが適切であるかどうか、さらにはNISCの技術的能力、知見が活用可能であるか、こういった要素を踏まえてサイバーセキュリティ戦略本部において決定をしてまいりたいというふうに考えております。

したがいまして、J―LISを戦略本部による指定の対象とするか否かにつきましては、繰り返しで恐縮でございますけれども、J―LIS自身の意向を踏まえながら、所管省庁である総務省と調整、検討をしてまいりたいというふうに考えてございます。

○山本香苗君　総務省としてはどうお考えなんですか。

○政府参考人（宮地毅君）　J―LISをサイバーセキュリティ戦略本部によります指定の対象とするか否かにつきましては、J―LIS自身の意向を踏まえることも必要だと思いますが、この意向を踏まえながら総務省としてもNISCの検討に協力をしてまいりたいと考えております。

○山本香苗君　ということは、まだJ―LISの意向というのは確認されていないということですか。

○政府参考人（宮地毅君）　まだ最終的な意向というのは確認をしておりません。

○山本香苗君　是非ともしっかりと、J―LISの意向もということではありますけれども、大変、マイナンバー制度の根幹を担う法人でございますので、速やかに指定できるように、ただ、いろいろと仕組みを伺っておりますと、普通の法人を指定するのとはちょっと違う配慮が必要なのではないかと思っておりますが、是非ともここはよろしくお願いしたいと思います。

その上で、J―LISは地方自治体の情報セキュリティー支援ということも行うこととなっております。具体的に今、何されていますか。

○政府参考人（宮地毅君）　J―LISの方では、以前から地方公共団体の情報セキュリティー対策の支援を行っております。

平成二十八年度の例で申し上げますと、地方公共団体のホームページの脆弱性の自動診断やウエブ感染型マルウエア等の検知、そしてセキュリティー研修としましては情報セキュリティーに関するe―ラーニングの実施など、そしてまた、情報セキュリティ対応ハンドブックを活用した訓練ツールの作成、配付、NISCの方から提供されるIT障害等の情報を全地方公共団体に一斉配信する業務などの事業を予定をしているところでございます。

○山本香苗君　今年度におきましては、J―LISにおいて独自にLGWANのところに集中監視機能を設けるということになっていると伺っております。そうなりますと、J―LISがNISCのように不審な通信を感知したというふうになった後に、当然のことながら、それが出元が地方自治体のところであったら地方自治体に対するサポート体制というものも必要となってくるんじゃないかと思うんですが、その辺りをお伺いしますと、まだ何も定まっていないというようなお話を伺いました。

CYMATみたいなものもないということなんですが、是非、J―LISにおいてそうした集中監視機能をお持ちになるという、予算も通っているのでやるということでありますけれども、そうした形のものを、しっかり地方自治体を支援していくというような仕組み、体制を取っていただきたいと考えますが、いかがでしょうか。

○政府参考人（宮地毅君）　J―LISの運営につきましては、地方公共団体情報システム機構法に基づきまして、地方三団体の代表や有識者が参画をいたします意思決定機関の代表者会議のガバナンスの下に行われることとなっておりまして、ここにおいて自治体の要望あるいはニーズなどを踏まえながら事業を行っていくのが基本ではございますが、情報セキュリティーに関しましては、地方公共団体のニーズもますます強くなってくると考えているところでございますので、総務省といたしましてもJ―LISの情報セキュリティー支援事業の在り方の検討に協力をしていきたいと考えております。

○山本香苗君　是非ここを充実をさせていただきたいと思います。

今の段階だと、インシデント発生時の対応は総務省の地域情報政策室ですか、そちらの方でやっていて、J―LISはかまないんだというふうな話も伺いまして、だったら、じゃこの集中監視機能は何で置くんだというような話にもなってきま

すので、しっかりとここのＪ－ＬＩＳがそうした機能もお持ちになっていただきたいと考えております。

今回、この法改正、大事な法改正でございますけれども、やはりサイバーセキュリティーを支えるのは製品とかそういうものではなくて人材であります。現在、日本においては、スキルが足りない技術者の再教育も含めて約二十四万人のサイバーセキュリティー人材が足りないというようなことも言われておりますが、中でも政府部内における人材不足というのは、今言われることじゃなくて、前から非常に深刻であったわけです。

ＮＩＳＣにおいては今年度末までに四十名を増員されて百八十名体制になるということでありますけれども、今、セキュリティー人材は民間でももう引く手あまたで、とにかく足りないんだというようなお話でありまして、使命感だけでいい人が集まるものかということはないと思うんです。

大臣に是非ともよくお考えいただきたいんですが、今ＮＩＳＣに任期付きで来ていただいている方々、本当に優秀な方々来ていただいておりますけれども、辞めた後、保障はないけど、まあいろんなところはありますけれども、極めて、兼業も駄目だし、いろんな形で制約された中で来られております。待遇面で今よりも更に特別な対応を取っていただくことが必要なのではないかと思うんですが、どうでしょうか。

○国務大臣（遠藤利明君）　御指摘いただきましたように、高度な能力を有する人材を民間から登用し、対処能力の向上を図ることは大変重要でありまして、そのためには処遇面での配慮が必要だと認識をしております。

そこで、公務に有用な専門的な知識、経験等を有する者を任期を定めて採用し、高度の専門的な知識、経験等を有する者についてはその専門性等にふさわしい給与を支給することができる制度を用い、高度な能力を有する人材の採用を開始したところであります。

引き続き、優秀な人材にとって民間と遜色のない魅力的な待遇となるよう改善に努めていきたいと思っております。

○山本香苗君　是非お願いしたいと思います。

それで、三月三十一日に、サイバーセキュリティ人材育成総合強化方針というものが策定をされました。その中で、先ほどもお話ありましたけれども、サイバーセキュリティ・情報化審議官というのが新設されて、この方が要するにＩＣＴ全般、セキュリティーの司令塔として機能することが期待をされているわけですけれども、実際これの任命、配置の状況というのはどうなっていますでしょうか。そして、ちゃんと本当に担える人がなっているということは御確認していただいておりますでしょうか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

今委員御指摘のサイバーセキュリティ人材育成総合強化方針におきまして、各府省庁は、平成二十八年度、今年度に新設をいたしましたサイバーセキュリティ・情報化審議官等の主導の下に、セキュリティー、ＩＴに係る体制の整備や人材の拡充等に取り組むこととしております。

その配置状況でございますけれども、各府省庁におきましては、この方針に基づきまして、この年度当初において当該審議官等の配置を行ったというふうに承知をしているところでございます。先ほど大臣からも御答弁ございましたように、総合調整能力に優れており、かつ、更にＩＴあるいはセキュリティーについての知見を高めていただくことも必要でございますので、私ども内閣官房といたしましても、こうした審議官等を集めた研修あるいは打合せ、こうしたものを定期的かつ頻繁に開催をいたしまして、それぞれの知見の底上げを図ってまいりたいというふうに考えてございます。

○山本香苗君　ただ単に新たなポストが一つ増えたで終わってもらっては困ると思いますし、また、ここが要するに官房長が多くなっているＣＩＯのところの部分の補佐にもなるわけでありますので、かつここは専任ですよね、専任でしっかりと機能するような形を是非取っていただきたい。機能していないところがあったら、しっかりと助言、指導していただけるような体制も取っていただきたいと思います。

そして、この人材育成の中には、政府部内において二〇二〇年までに一千人超の職員を育成をすることを目指すとされておられます。一千人の根拠がちょっとよく分からないんですが、本当にこれで十分なのかという思いもありますし、まず、この一千人、根拠は何なんでしょうかということと、今後具体的にこれをどういう形で実現していくのか、大臣にお伺いしたいと思います。

○国務大臣（遠藤利明君）　本年三月のサイバーセキュリティ戦略本部において、サイバーセキュリティ人材育成総合強化方針を決定し、政府におけるセキュリティー・ＩＴ人材の育成に当たっては、今委員御指摘ありました研修受講者数を今後四年間で一千人を超える規模を目指すとしているところであります。

一千人を超える規模についての今根拠という話がありましたが、この算出に当たりましては、各府省庁において、まずはセキュリティー、ＩＴに係る統括部局の体制整備等を行い、さらに社会的な影響力が大きいシステムを所管する部局についても体制整備等を行っていくこととしていることから、それらを勘案して目標を定めたものであります。

具体的には、ＮＩＳＣ及び総務省行政管理局等においてセキュリティー及びＩＴに係る役職段階別の研修を実施し、修了者にスキル認定を行うなどの取組を進め、実現を図ってまいりたいと考えております。また、各府省庁においては、サイバーセキュリティ・情報化審議官等の主導の下、セキュリティー、ＩＴに係る体制の整備や人材の拡充等に取り組むこととしております。

○山本香苗君　大丈夫かなという大変心配がありますけれども、もう一つ心配なことがありまして、是非遠藤大臣に聞いておいていただきたいと思うんですけど、大学ですね。大学等というのは研究成果のもう極めて重要な情報を保有していまして、サイバー攻撃の標的となりやすいというふうに言われていて、実際被害が出ていたということも二月ぐらいに報道で流れておりました。

文部科学省は、こうした大学等におけるセキュリティー対応状況の実態をそもそも把握していらっしゃるんでしょうか。そして、インシデント発生時とかどういうことをやろうとしているのかと。具体的にどうセキュリティー対策を講じているのか、よろしくお願いします。

○政府参考人（生川浩史君）　お答えいたします。

まず、状況の把握をしているのかという点でございますが、文部科学省の方としましては、大学等におきまして不正アクセス等の事案が発生をしているということについては私どもとしても把握をさせていただいているところでございます。

これに対しまして、セキュリティー対策の現状でございますけれども、大学におきましては、先生御指摘のように、学内の教育研究あるいは管理運営上の各種データを守るなどのために、各大学の責任において情報セキュリティー対策を講じることが極めて重要であるというふうに考えております。

文部科学省では、これまでも大学に対して通知や各種会議等の機会を通じて必要な情報提供を行うとともに、セキュリティー対策の徹底を要請をしてきたというところでございます。それに加えまして、学術情報ネットワーク、ＳＩＮＥＴというのがございますが、これを構築、運用いたします国立情報学研究所におきまして、本年度からでございますが、ＳＩＮＥＴに接続する全機関を対象に大量のデータ送信を行う異常トラフィックを監視をするということとともに、国立大学につきましては、情報の漏えいを防止するためサイバー攻撃をＳＩＮＥＴ上で監視をして、それが検知された場合にはその情報を当該大学に提供するということを始めることとしたところでございます。

また、国立大学の技術職員を対象としてサイ

バー攻撃への対処能力を高度化させるための研修を実施することといたしておりまして、現在、国立情報学研究所においてその準備を進めているというところでございます。

文部科学省としては、国立情報学研究所が運営をいたしますＳＩＮＥＴに係る取組を通じて大学における情報セキュリティー体制の構築を支援をしてまいりたいというふうに考えているところでございます。

○山本香苗君　終わります。ありがとうございました。

○江口克彦君　おおさか維新の会の江口でございます。

全て遠藤大臣に御質問というか、お尋ねしたいというふうに思います。

今回の改正の背景といたしまして、サイバーセキュリティーに対する脅威の一層の深刻化が指摘されておりますけれども、国民にとってサイバーセキュリティーに対する脅威の深刻化とは具体的にどのような事態をいうのか。また、サイバーセキュリティーの確保がなされない場合に国民の安心、安全にどのような危険が生ずるのかということについては、なかなか国民の皆さん方、具体的にはお分かりにならないんじゃないかと、多くの。そのことにつきまして、どのような危険が生ずるのかということについて、遠藤大臣のお考えをお尋ねしたいというふうに思います。

○国務大臣（遠藤利明君）　委員御指摘のように、サイバーセキュリティーという事案、言葉そのものもまだまだ浸透が薄いんだろうと私も承知をしております。

そこで、様々な分野におけるＩＴの利活用の発展に伴い、ＤＤｏＳ攻撃や標的型メール攻撃による社会インフラ等の機能障害や、窃取された情報の悪用等がこれまで以上に懸念される状況にあると認識をしております。

このようなサイバーセキュリティーに対する脅威が深刻化する中において、サイバーセキュリティーの確保がなされない場合には、例えば昨年の日本年金機構事案のように大量の個人情報の流出による国民生活への影響、また知的財産を窃取されることによる企業等による経済活動の悪影響、さらに重要インフラ事業者等が提供するサービスの停止による我が国の社会経済活動や安全保障への影響などが考えられます。

政府としましては、国民の安心、安全を確保する観点から、これまで以上に積極的にサイバーセキュリティー確保のための取組を進めてまいりたいと考えております。

○江口克彦君　警察や消費者庁による積極的な注意喚起にもかかわらず、おれおれ詐欺というものやその類似犯罪の被害がなかなか消えないというか、なくならないと。収束しない要因の一つに、国民一人一人が、まさか自分は詐欺には引っかからないだろうというような、そういう他人事意識があるのではないだろうかというふうに思われます。

サイバーセキュリティーに関しても同様でありまして、その脅威というのは実感している国民はまだまだ少ないのではないかというふうに思っているわけでありますけれども、法制度を整えることは必要なことだとしても、多くの国民が日常的にＰＣやモバイルツールを用いてインターネットにアクセスし、情報ネットワークに接続している状況を踏まえると、国民一人一人にサイバーセキュリティーへの脅威についての意識がなければ法制度は絵に描いた餅になりかねないのではないかというふうに思いますが、こうした問題意識について大臣はどのようにお考えになっておられるのか、お話伺いたいと思います。

○国務大臣（遠藤利明君）　物理的なテロ攻撃と違って、なかなか目に見えないというようなことも一般の国民の皆さんにとって理解しにくい部分があるかと思っております。そういう意味でも、私たちの役割をしっかり進めていかねばならないと。

またさらに、サイバー攻撃が高度化、複雑化している中で、国民一人一人がサイバーセキュリティーへの関心や理解を高め、対応力を強化していただくことが必要だと認識をしております。サイバーセキュリティ戦略においても、「利用者たる個人や企業・団体が、自ら進んで意識・リテラシーを高め、主体的に対策に取り組む努力も欠かすことはできない。」としております。そのためにも、産学官民が一体となって、国民一人一人の皆様に対するサイバーセキュリティーへの意識向上を取り組むとともに、サイバーセキュリティー対策の強化を遅滞なく図ってまいりたいと考えております。

○江口克彦君　そのサイバーセキュリティーということについて、また後で御質問させていただきますけれども、繰り返し申し上げていますけど、サイバーセキュリティーというのは何ぞやという多くの国民の方々のことを意識しますと、存在を考えますと、やっぱり特別に国民に対する、まあ教育と言うと語弊があるかもしれませんけれども、そういう啓蒙といいますか、サイバーセキュリティーとは何ぞやというようなことを政府も対応していかなければ、要するに個人のサイバーセキュリティーしっかりしていないと、個人の方から公的機関の方に入り込んでしまうというような可能性も、一気に公的なところへの攻撃だけではなくて、そういう迂回攻撃というものもあり得ると思いますので、その辺のことを十分に考えていかなければいけないんじゃないかというふうに思うんですけれども、後で御質問します。

情報通信技術を利用した諜報活動、サイバーインテリジェンスの脅威は、私は非常に深刻だというふうに思うんであります。昨年のあの日本年金機構による個人情報漏えいを始めとしまして、アメリカでも実に四百万件以上の政府職員の個人情報が盗まれているわけですね。また、特定秘密保護法により保護される政府の外交や防衛に関する特定秘密はもとより、原子力発電に関する情報、それから医薬品の研究開発に関する情報など、民間にも多くの機密情報が存在するというのはこれ事実でございますね。こうした情報が盗まれたとなれば、国の安全保障の問題や国益を損ないかねないというふうに、損失といった問題に発展しかねないというふうに思うんです。

サイバーインテリジェンスへの対応も喫緊の課題だというふうに思いますけれども、大臣の認識をちょっとお伺いしたいと思います。よろしくお願いします。

○国務大臣（遠藤利明君）　江口委員御指摘のとおり、今やサイバー空間は経済活動のみならず安全保障やインテリジェンス活動の舞台ともなり、組織的かつ周到に準備された高度なサイバー攻撃により破壊行為や機密情報の窃取、データの改ざんは現実の脅威となっておりまして、サイバーインテリジェンスへの対策を含むサイバーセキュリティー対策は緊喫の課題だと認識をしております。

政府機関等では、政府機関における統一的な基準の策定及びその運用を中心としてサイバーセキュリティーの確保に取り組んでおり、新たに直面した脅威、課題についても基準に逐次反映するとともに、監査や平素からの教育などの取組によりその徹底を図っているところであります。

また、重要な情報を保有する重要インフラ事業者に対しましては、重要インフラの情報セキュリティ対策に係る第三次行動計画に基づきＮＩＳＣが中心となって各種施策を推進しているほか、本年三月にはサイバーセキュリティ戦略本部において同行動計画の見直しに向けたロードマップを取りまとめたところであります。

この見直しを具体的に申し上げますと、経営層における取組の強化の推進等のサイバー攻撃に対する体制強化、そして情報共有範囲の拡大等重要インフラに係る防護範囲の見直し、さらに国際連携等多様な関係者間の連携強化、こうしたことを柱として重要インフラ防護のための更なる対策強化に向け本ロードマップに従い検討を進め、行動計画の見直しについて平成二十八年度末を目途に結論を得ることとしております。

今後とも、引き続きこうした取組を着実に進め

て、国の安全保障の問題や国益の損失といった問題が生じないよう、関係機関と連携しつつサイバーセキュリティー対策の着実な推進に努めてまいりたいと考えております。

○江口克彦君　繰り返し申し上げて恐縮ですけれども、そういう専門機関だとか、それから企業、組織、団体とかというところは私はいいと思うんですね。それは、それぞれが組織防衛、企業防衛、あるいはまたいろんな自分のところのプラスマイナスというか、そういうふうな問題が出てきますから、自然にサイバーセキュリティーに関して一生懸命取り組むでしょうし、あるいはまた、政府等がそういう対策を講じたら、それに呼応する、あるいはまたそれ以上の対策というものを、企業にしても集団にしても組織にしても自分の存続に関わってくるわけですから一生懸命やるはずなんですね。それはそれでいいんですよ。もちろん協力してやっていただきたいと、やっていくべきだと思いますけれども、問題は個人なんですよね。個人がどうなんだという、その個人への、国民一人一人への、サイバーセキュリティーへの関心といいますか、そういうサイバー攻撃に対する当事者意識の喚起のために、やっぱり個人、国民一人一人に対してのそういう対策を講じていかないと大変ですよということを私は繰り返し申し上げているわけですよ。

　要するに、おれおれ詐欺じゃないですけれども、自分のPCは大丈夫だろうとか、自分のセキュリティーは、自分のところにはそんなことを考えなくてもいいだろうというふうに、大体国民皆さんそう思っておられるというふうに私は思うんですけれども、だけれども、そうじゃないんだと。こういうネットワーク社会ですから、どこからどういうふうに公的機関のコンピューターに入り込むかも分からないということになってくると、国民への啓蒙というものをもっとやっていかなければならないんじゃないかと。先ほどのお話では、言ってみれば組織とか団体とか、あるいはまた企業とかという、そういうふうなところをイメージされるわけですけれども、そうじゃなくて、やっぱり一人一人、国民ということを意識した政府の啓蒙活動というものを新たに付け加えるなり、あるいはまた考えて、対策というか対応をしていく必要があるのではないだろうかというふうに思うんですね。

　そういう具体的な対策を講じておられるんですか。おられるかもしれません。とするならば、具体的に国民一人一人に対してどのような対策を講じておられるのか、どのような施策を講じていこうとしているのか、是非お答えというか教えていただきたいなというふうに思うということです。

○国務大臣（遠藤利明君）　委員御指摘のとおり、まだそうした啓蒙活動が必ずしも浸透していないということは事実でありますし、そうしたことをこうした法律の制定も含めてしっかり進めていかなきゃならないと改めて認識をしております。

　国民一人一人のサイバーセキュリティーの意識あるいはリテラシーを高めるためには、年齢層や所属、ライフスタイルが異なる多様な国民のニーズにやはりきめ細かに対応しなきゃならないと。そのためには、学校教育での取組、そして家庭や会社などのニーズに合わせたウエブサイトの充実、また国民に親しみやすいメディアの活用など、そうした取組を推進して国民全体の意識の向上をなお一層進めてまいりたいと考えております。

○江口克彦君　是非国民に向かっての具体的なサイバーセキュリティーに関する啓蒙活動というものをしていただきたいということを――どうぞ、追加があればどうぞ。

○国務大臣（遠藤利明君）　具体的なという話がありましたので。

　例えば、二月一日から三月十八日までをサイバーセキュリティ月間と定め、関係機関、業界団体等、産学官民が一体となって、シンポジウムやセミナーの開催、情報セキュリティハンドブックの配布、メディアを活用したイベント開催やコンテンツ作成、ソーシャルメディア等を活用した情報発信など様々な取組を実施をしております。

　引き続きこれらの啓発活動を推進していき、国民一人一人の皆様がサイバーセキュリティーについて自ら具体的な行動を起こそうとする、そんな機運が高まることを強く期待し、そうした取組を進めてまいります。

○江口克彦君　よろしくお願いいたします。

　今回の法改正によって、特に民間部門におけるサイバーセキュリティーの向上や官民連携によるサイバーセキュリティーの対策の向上についてどのような効果があるのか、考えておられるのか、御教示いただきたいと思います。

○国務大臣（遠藤利明君）　企業等がサイバーセキュリティーを確保する上では、その対策を担う専門人材の活用を推進することが重要であります。本法案による情報処理安全確保支援士制度の創設を通じ、特に民間部門において高度かつ実践的な知識、技能を備えた専門人材の活用が進んでいくことが期待をされております。

　また、複雑、巧妙化するサイバー攻撃に適切に対処していくためには官民の協力が一層重要となっております。昨年九月に閣議決定したサイバーセキュリティ戦略においても、総合的な対策強化に際しては専門的知識を有する関係法人との連携体制の整備を図ることとされております。今回の改正法案を踏まえ、戦略本部の事務の一部をIPA等に委託することにより、当該事務をより迅速かつ効果的に実施することが可能になってまいります。

　なお、NISCは、従前よりIPA、NICT、産業技術総合研究所等とのパートナーシップを構築しており、これらの機関の知見を生かしながらサイバーセキュリティー対策の効率的、効果的な推進を図ってまいりたいと考えております。

○江口克彦君　サイバーセキュリティーにおける国際協調についてお尋ねしたいと思います。

　サイバーセキュリティ基本法は、第三条第四項において、サイバーセキュリティーに関する施策の推進は国際的協調の下に行われなければならないと定めていますけれども、国際的協調として具体的にどのような取組が行われているのでしょうか。

○国務大臣（遠藤利明君）　今具体的にというお話がありましたが、米国、イギリス、オーストラリア等との二国間の協議、対話を通じ各国との連携を強めるとともに、国連の政府専門家会合や官民を含む幅広い参加者を得たサイバー空間に関する国際会議等の多国間の国際会議への積極的な参加を通じて、サイバー空間に関するルール作りや意識啓発、CSIRT間協力、情報共有の強化等に積極的に貢献しているところであります。

○江口克彦君　もう時間がありませんので最後ですけれども、二〇二〇年東京オリンピック・パラリンピック開催に向けたサイバーセキュリティー対策についてもお伺いしたいと思います。

　物理的なテロへの備えももちろん重要でありますけれども、大会そのもののスケジュール管理や記録の管理、国際通信、オリパラ関連施設の運営や入場者管理等、あらゆる場面でコンピューターによる情報システムが稼働していることを考えますと、サイバー攻撃を受けた場合の大会の混乱は必定であります。二〇二〇年オリパラに向けたサイバーセキュリティー対策は万全を期すべきと考えていますが、もう時間がありませんので、一言、万全を期して、大丈夫ですねということでお答え、まあ大丈夫じゃないと言われるかもしれませんけれども、結構です。

○国務大臣（遠藤利明君）　成功の条件の最大の課題の一つは安心、安全な運営でありますし、そのためには、物理的なテロもそうですが、とりわけサイバーセキュリティーに対してはしっかりと取り組んでまいります。これは私のオリンピック・パラリンピック大臣としての最大の課題でありますから、ここは万全を期して取り組んでまいります。

○江口克彦君　ありがとうございました。

○山田太郎君　日本を元気にする会の山田太郎でございます。

　今日は、いろんな多岐にわたるセキュリティー

の話がありました。大野議員の方からかなり軍事上のところで詳しいやり取りがありまして、私はそこまで専門の分野は分からないんでありますが、ただ、私も、実は元々米国外資の三次元ＣＡＤの本社の副社長をやっておりまして、千六百社の日本のお客さんがいまして、ＣＡＤ情報が漏れれば会社は吹っ飛んでしまいますので、半端ないほど世界中からアタックがあった会社でありまして、セキュリティー対策、当時、極東責任者として頭を痛めていました。

また、私が上場企業をつくったときも、製造業のコンサルティングをやっていましたので、設計情報、原価情報、それから取引情報、お客様三百社預かっておりまして、これまたいろいろ大変でありまして、セキュリティー上でそういうところのお客様情報が漏れなかったのでよかったんですが、ただ、私も苦い経験がありまして、ＩＲで、実は私の部下というかＩＲ担当が転送しなきゃいけないところを返信してしまいまして、それが魚拓になって炎上しまして、役員会で私は一年間三〇％も減俸という憂き目に遭いました。いや、逆に言うと、セキュリティー、社長まで上る、極めてリスクの高い、これがもしお客様情報だったら、これはもう我が社は飛んでいたということであります。

そういう意味で、人の問題というのがやっぱり大きいんだなということは、私は実は民間ではあったんですけれども、セキュリティーに関する責任を持ってやっておりまして、それに比べてちょっと国の在り方はアマチュアじゃないかなというような、今日は苦言も含めていろいろ質疑させていただければというふうに思っております。

まず、この法律の元々のスタートになったのは、厚労省さん配下の年金機構の流出事件をきっかけにしております。やっぱり反省点から始めないといけないと思いますので、今日は厚労副大臣にも来ていただいていると思いますが、なぜこの流出事件が起こってしまったのか。今回、厚労省さんの方からも資料をいただきながら、お手元に皆さんの方お配りしているんですけれども、本当に簡単で結構でございます、概要を全部言い出すと多分質疑終わらなくなってしまいますので、ポイントだけ絞って教えていただければと思います。

○副大臣（とかしきなおみ君）　まずは、質問にお答えする前に、昨年の五月、百二十五万件の情報流出をしてしまったことをおわびを申し上げたいと思います。

それに当たりまして、厚生労働省におきましては、昨年の九月に再発防止を取りまとめさせていただきまして、厚生労働省及び所管の法人等における情報セキュリティー対策の強化に向けて、組織、そして先ほど委員御指摘の人的、そして業務運営、技術的対策、それぞれの観点から取組を進めさせていただいております。今日お配りいただきました資料に結構きちっとまとまっておりますので、これを見ていただければ、防止対策の方はまとめさせていただいております。

具体的に言いますと、専門性や即効性の向上の観点から、外部専門員の人材の確保、ＣＳＩＲＴの体制強化、あと、次は標的型メールの攻撃を始め職員の危機管理及びリテラシーの向上のための教育訓練、そして厚生労働省の所管法人等においてインシデント等が発生した場合の担当部局から速やかな幹部等への報告、連絡体制の構築、情報セキュリティポリシー等の改定、そして個人情報の重要性を、インターネットから分離するなど必要なシステム上の措置、これらに取り組んできたところであります。

○山田太郎君　質問は、取組の前に、何が問題だったかということだったんですが、紙にまとめてあるということで、これを見ていただいたということなんですが、やっぱり私、この中でもいろいろ問題だなと思うのは、この三番の四月二十二日の標的型攻撃についての厚労省の対応ということで、これは四月二十二日に攻撃されていまして、五月の八日、一番流出したんですけれども、これはもう分かっていたというか、このときの二十二日に対処していれば五月の八日はもう完全に防げたわけでありまして、ここはもう本当に人的としか言いようがないのかなというふうに思うんですね。

それ以外、厚労省さんと話をしていまして、置いてはいけないサーバー上に個人情報を置いていたとか、メールを受信しても怪しいと思っても無視すればよかったものをわざわざＵＲＬにアクセスまでして見てみたとか、いろんな人に依存する問題が多かったんじゃないかなというふうに思っています。

実はセキュリティーの問題で有名な話がありまして、ある会社のセキュリティーを監査するときに、一番簡単にその会社のセキュリティーを破る方法は何かというと、超簡単でありまして、その会社の駐車場にウイルス入りの、入ったＵＳＢメモリーを置いておくことなんですね。ばらまいておくことなんです。そうすると、人というのは興味がありまして、差してみて中に何が入っているんだろうと開けた瞬間に終わってしまうと。実はこれ、単純ではあるんですが、この手でかつてかなり多くの会社がセキュリティーを破られたという事実もありまして、つまり、どんなにハード面で頑張ったところで、やっぱり人が情報を持っていますので、その人が開けてしまえばもう仕方ないんですよね。どんなに鍵を立派にしても、泥棒がピンポン押して、何か興味がある人がドアを開けちゃえば入ってくるわけでありまして、やっぱり何だかんだ言って人の問題なのかなと、こういうふうに思っているわけであります。

そんな観点で、今厚労省さんの方からもいろいろ今後やるということをおっしゃっていましたし、問題点も、今回はもう本当にこれはマスコミでも相当たたかれた問題なので明らかだと思いますが、さて、この法案が本当に通ることによって今後年金流出事件のようなことが起こらないのかどうか。私は必ずしも、ちょっとこの程度では厳しいのではないかなとも思っているんですが、その辺り、遠藤大臣の御見解をまず聞きたいと思います。

○国務大臣（遠藤利明君）　今回の改正案、日本年金機構のような一部特殊法人等について指定法人と位置付け、国による不正な通信の監視及び監査等の対象に加えようとするものであります。これにより、指定法人においては、セキュリティー確保のために政府と同様の取組が義務付けられるとともに、十分なインシデント対応体制の整備がなされることとなり、結果として不正な通信の検知に対して迅速かつ適切な対応を行うことが可能となります。加えて、重大事象の場合は戦略本部による原因究明調査の対象となります。

また、指定法人に対して政府統一基準群が適用されるため、これを踏まえた監査等が行われることにより十分なサイバーセキュリティー対策が取られているかを評価し、必要な措置を講ずるよう求めることも可能となっております。

サイバー攻撃は質量共に深刻さを増しており、予断を許さない厳しい状況でありますが、これらの対策を着実に実施することにより、日本年金機構の個人情報流出事案のようなサイバー攻撃事案の再発防止、被害最小化に向けて政府一丸となって対策を強化してまいりたいと考えております。

○山田太郎君　もう一つ資料を、二枚目を見ていただきたいんですが、ＮＩＳＣのガイドラインというのがありまして、最低年一回の研修を義務付けているということでありますが、一方で、着任、異動後も三か月以内に受講せよということで、きちっとセキュリティーの勉強をしなさいということなんです。

ちょっと済みません、遠藤大臣に、余りクイズみたいなことはしたくないんですが、例えばウイルスに感染したときに実は二つすぐやらなきゃいけないというふうに決まっていることがございまして、その二つを実は大臣自身が御存じなのかどうか。余り私クイズみたいなことはしたくはないんですが、念のためお聞きしたいと思いますが、いかがでしょうか。

○国務大臣（遠藤利明君）　詳細について、二つ、詳しく存じてはおりませんが、一つはネットワー

クを切るということかと思います。

○山田太郎君　ありがとうございます。まずそれをやっていただければ漏れませんので。済みません、本当に大臣にクイズなんか出して申し訳なかったんですけれども、まさにＬＡＮケーブルを抜くということなんです。それから、セキュリティー本部に連絡をすると。二次被害、つまり年金機構の件はこれだったんですよね。一回目攻撃されて、二回目が本格的に出ましたので。ということで、遠藤大臣の下では大丈夫だと。常識的に考えればそうだよねということなんですが、そうやっていなかったというのが今回の流出だったというふうに思っています。

ただ、教育の方もしっかりやられているかということで、もう一枚目の紙を見ていただきたいと思っているんですが、先ほど厚労副大臣の方からは徹底的にやっているということで、確かにこれだけ年金機構大きな問題になりました。対処としてはｅ―ラーニングとかその他の受講とか教育ということなんですが、ｅ―ラーニングも九八％、大臣を含めた階級別研修を実施ということで、しっかり大臣も受けていますよということをレクの段階ではお聞きしたんですが、実は問題は、済みません、そういう意味で今日は世耕副長官に来ていただいたんですけれども、内閣官房さんでございまして、ｅ―ラーニングの受講も、内閣官房は一千八百六十人中僅か三十八名、二％しか受けていないと。内閣総務官室の方でセキュリティーに関する資料は作っているんですが、それを職員に送っているだけで、特にその後のフォローもしていないということを実はレクで聞きました。

やっぱり国家の中枢、機密を担うところでもありますし、そもそもＮＩＳＣは内閣官房にあるわけですから、そのＮＩＳＣさんがある内閣官房自身がもっとしっかりきちっと教育をしていただきたいなと。本来であれば、私は、世耕官房副長官の部屋にお伺いしたときも、かなりＩＴまでお詳しいということは知ってはいるんですけれども、足下こんな状態になっておりますので、ｅ―ラーニングだけではなくて集合教育も含めてきちっとやっていただきたい。第二の年金流出、まさか官邸からこんなことがあれば日本政府に対する信頼は全く失ってしまいますので、この辺り、世耕副長官の方、よろしくお願いします。

○内閣官房副長官（世耕弘成君）　内閣官房そして官邸は、やはり情報セキュリティーは徹底的にやっていかなければいけないと。そういう意味では、ハードとかシステムといった面では、逆に、私も毎日使っていて、はっきり言って使い勝手が悪いぐらいがちがちのセキュリティーが組まれているわけであります。

ただ、一方で、やはりそれを使う人がきちっとした知識を、リテラシーを持っていなければいけないというのは当然のことであります。ですから、今日、山田委員から質問通告をいただきまして、私もチェックをしましたが、ＮＩＳＣの勉強会への参加ですとかあるいは総務省が用意をしているｅ―ラーニングの受講者数、これ本当にお寒い内容であって、これは私は問題だと思っております。早速、今朝、私の方から事務方に対して、ＮＩＳＣや総務省が実施をしている既存の研修の受講、あるいはｅ―ラーニングの実施、こういったことをできるものから直ちに徹底をして取り組むように指示をしたところであります。

今後とも、こういった人の教育といった面を情報セキュリティーの面で徹底してまいりたいというふうに思います。

○山田太郎君　ありがとうございます。さすが世耕官房副長官だというふうに思っております。

対処が早いというのが最もセキュリティーでは重要でございますので、この政府であれば大丈夫だなというふうに思いたいんですが、もう一つありまして、ただ、やっぱり現場の方、なかなか言い訳をいろいろされるんですね。一つは、出入りが激しいというのが官房の宿命だということですが、出入りが激しくてもこれやっぱりきちっと、着任三か月以内というふうに書いてあるわけですから、それをお願いしたいということと、もう一つちょっと気になるのは、標的型メール訓練をやられたということで、一斉に十月二十八、十一月十六日、十一月三十日、去年やったということなんですが、確かにそれでいわゆる仮想感染したのが一五％から三％弱まで減ったということで胸を張られて説明をされていたんですが、実はゼロ％にしないとこれも終わりなんですね。

私の先ほど言った会社の常識では、たった一人でも漏れればもうそれは会社が飛んでしまうし、そこから全部漏れてしまいますので、ほぼ一桁台だから大丈夫だろうというのがやっぱりまだ認識なのかなと。この辺りが特に教育というか認識なんだと思います。民間であれば当然もう滅俸ということになりますが、国はなかなかそういうことでそれに対する罰だとかマイナスのインセンティブだとかということは付けにくいと思いますが、民間レベルはもう徹底して今常識ではそこまでやっている状態でありますから、私が感じた観点ですね。

つまり、言い訳はいろいろあると思います。大変なんだとも思います。ただ、それだからといっても、やっぱり本当に実際のテロでミサイルが飛んでくる危機よりも、まずその前に必ずサイバーテロされるというのが当然なわけでありまして、これだけ防衛省でお金と手間といろいろ使ってやっている割には確かに本当に国のセキュリティー大丈夫なのかということになりますが、それは先ほど言ったやっぱり意識の問題だと思いますので、もう一度この辺り、世耕副長官、それから遠藤大臣にも改めて、全省庁同じ状況でございますので、お伺いしたいと思います。よろしくお願いします。

○内閣官房副長官（世耕弘成君）　標的型メール攻撃訓練というのを最近実施をしておりまして、そういう意味で、これをうっかり開けてしまおうとした、一回開けて注意をされるわけですから徐々に減ってきております。ただ、やっぱりおっしゃるようにゼロにならないと意味がないというふうに思いますので、これからもこういう訓練を徹底していくとともに、一方で、先ほど申し上げたように、講習をちゃんと受けて、標的型メールにはこういうパターンがあるんだと、こういうふうに信用できそうに見えるけど危ないものもあるんだということを徹底をしていくことで、この数字をゼロにするよう目指していきたいというふうに思います。

○国務大臣（遠藤利明君）　今、世耕副長官から話がありましたが、一番の課題はやっぱり意識を高めるということだと思います。それだけ民間は、それですぐ企業は潰れる。しかし、ここはやっぱりお役人意識というものがあるんだろうと。そういうことを含めて、しっかりと訓練、教育等について意識を高めていきたいと思っております。

○山田太郎君　最後の質問をしたいと思いますが、このセキュリティーの裏にある表現の自由といったところもちょっとしっかり見ておく必要があると思いますが、この法律によって表現の自由が侵されないようにしなきゃいけないと。特にインターネット上の自由というんですか、逆に萎縮してしまっても、要は情報を発信していくということも一つの官それから我々国の仕事でもありますので。もちろんセキュリティーは、何もしない、何もやらない、何も足さないというのが一番いいんですが、それでは仕事にはなりません。

だから、自由との駆け引きになるんですが、その辺りを配慮していただきたいのと、もう一つはサイバー空間の分断。よく、セキュリティー分野で強化をし出すと、私も会社で経験があるんですけれども、実は切ってきちっと管理した方が確かにいいんだということになりますと、いわゆる元々、今国の方でももう一つ進めようとしているネットワークの統合というんですかね、ＩＴによるやっぱり我が国の再武装というんですか、あるいは、私も実は今回、ＩｏＴという形でもって、実際のインダストリー四・〇みたいな形での話を随分積極的にやらせていただいたんですけれども、そういった社会インフラのＩＴ化にも、逆に萎縮してしまってはこれは意味がないと思います

ので、その辺りも観点として是非とどめていただきたい。

逆に言うと、今私も国会へ来て、一つ、新人議員としてもう、三年やっとなりまして、慣れちゃったのであれですけど、ファクスが当たり前みたいな、確かにファクスだと漏れにくいんですけれども、今どき民間企業はファクスもうありませんので、というようなものに回帰してしまってもやはりよろしくないと思います。そういった意味で、この辺の通信の自由というか表現の自由というか、この辺りの配慮、遠藤大臣の方からよろしくお願いします。

○国務大臣（遠藤利明君）　今回の改正案につきまして、内容の中で、とりわけ情報の自由な流通の確保、そして法の支配、開放性、自律性、あるいは多様な主体の連携という政策の立案等に当たっての基本原則を踏まえたものであり、表現の自由等について影響を及ぼすものとは考えておりません。

また同時に、今委員御指摘ありました、統合化と分断という話がありましたが、そこについても十分配慮して進めていきたいと思っております。

○山田太郎君　これで終わりにしたいと思います。ありがとうございました。

○山本太郎君　ありがとうございます。生活の党と山本太郎となかまたち共同代表、山本太郎です。

サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案の、主にサイバーテロ対策について質問いたします。

この法案の担当大臣は遠藤大臣なんですね。遠藤大臣といえば、東京オリンピック・パラリンピックの担当大臣でもあられます。しかし、今回はオリンピック担当大臣としてお越しではないので、残念ながらその件については大臣に質問をすることはできません。これ、お伝えしたいということだけで、オリンピックへのサイバーセキュリティー問題と併せて是非力を入れていただきたいことについて三十秒ほどでお伝えした後、本法案の質問に入っていきたいと思います。うそと利権と人権侵害のオリンピックになりつつあるという点だけです。

東京オリンピックがなぜ人権侵害か。新国立競技場建設のために、オリンピック憲章に明記された人間の尊厳保持、人種、宗教、性別、政治、そのほかの理由に基づく国や個人に対する差別は、いかなる形であれオリンピックムーブメントに属することとは相入れないというオリンピック根本原則を無視し、長年、東京都の明治公園で野宿生活をしていた人たちに対し、話合いをするという約束を破り、仮処分を申し立てて、今まさに権力で強制排除しようとしている重大問題が存在します。

安倍総理も沖縄の辺野古新基地問題で和解、話合いに応じました。JSCは話合いにも和解にも全く応じようとしないんですよね。私は、オリンピック憲章に反するJSCには東京オリンピック・パラリンピック推進する資格はないと思うんです。遠藤大臣、是非JSCに対して話合いと和解に応じるよう指示をしていただきたいと思います。

改めまして、本法案について遠藤大臣にお伺いをしたいと思います。

遠藤大臣は政府のサイバーセキュリティー対策の責任者であり、担当大臣なのでしょうか。基本的なことで申し訳ございません。そして、違うのであれば、誰がサイバーセキュリティー対策の責任者、担当大臣なのでしょうか。また、サイバーセキュリティー対策の政府の事務方の責任者は誰なのか。さらに、サイバーテロ対策の政府の責任者、担当大臣は誰なのか。また、サイバーテロ対策の政府の事務方の責任者は誰なのか。教えていただけますか、大臣。

○国務大臣（遠藤利明君）　政府におけるサイバーセキュリティー対策については、サイバーセキュリティー政策の取りまとめを行うサイバーセキュリティー戦略本部長であります内閣官房長官が政府の責任者となります。また、サイバーセキュリティ戦略本部の事務は内閣サイバーセキュリティセンターにおいて行うこととされており、事務方の責任者は内閣官房内閣サイバーセキュリティセンターの長であります高見澤内閣官房副長官補が当たります。

（委員長退席、理事相原久美子君着席）

サイバーテロ対策についても、サイバーセキュリティー対策の一環として、内閣官房においてサイバーセキュリティ戦略の取りまとめ等の全体的な施策の総合調整を行っており、その責任者についてはそれぞれ同様であります。具体的な取組につきましては、情報収集や捜査を行う警察を始めとして関係省庁が連携して取り組んでいるところであります。

○山本太郎君　ありがとうございます。

マイナンバー制度に対するサイバーテロ対策の責任者、担当大臣って誰なんですかね。また、事務方の責任者は誰になりますか。そして、マイナンバー制度がサイバーテロの対象となる可能性はあると認識をされているのか。お答えいただけますか。

○政府参考人（向井治紀君）　お答えいたします。

マイナンバー制度につきましては、所管は内閣府と総務省、このようになってございます。そういう中で、現在、マイナンバーの具体的な実施、例えば広報とかシステム・体制整備の進捗管理、セキュリティーの確保対策など、実施に伴う事務を担うのは高市国務大臣と承知してございます。

その上で、事務方につきましても、総務省、内閣府、それぞれ所掌がございますけれども、内閣も内閣官房がございます。

それで、内閣官房の立場は、マイナンバー制度を企画立案して法案を通させていただいたわけでございますけれども、法案成立後につきましては、総合的な内閣官房の調整機能を使いまして、それで総合調整を行っていると。そういう意味で、事務方の責任者という点で申しますと、内閣府の所管でございますので、内閣府は、担当室長は私でございますが、その上には事務次官というのが、事務次官が事務方の最高責任者であり、総務省におきましては総務省の事務次官が事務方の責任者になろうかと思います。

○山本太郎君　ありがとうございます。お久しぶりです。マイナンバーのときにお世話になりました。

五月二十六日と二十七日の伊勢志摩サミットに対するサイバーテロ対策の責任者、担当大臣は誰なのか、また事務方の責任者は誰なのか、教えていただけますか。そして、万全の対策、もちろん講じられているということでよろしいですよね。

○政府参考人（谷脇康彦君）　お答え申し上げます。

伊勢志摩サミットにおけるサイバーテロ対策を含むサイバーセキュリティー対策につきましては、サイバーセキュリティ戦略本部長であります内閣官房長官が政府としての責任者でございます。

一方、事務方についてもお尋ねがございました。サイバーテロ対策を含む伊勢志摩サミットに向けた政府の準備を検討してきております伊勢志摩サミット準備会議の中に、サイバーセキュリティー対策について、NISCのセンター長の下、NISC副センター長を座長とするワーキングチームにおいて実務的な検討をしているところでございます。

なお、サイバーテロ対策の具体的な取組につきましては、その情報収集や捜査を行う警察を始めとし、関係省庁が連携をして現在取組を進めているところでございます。

○山本太郎君　一体さっきから何を聞いているんだろうと思われた方もいらっしゃるかもしれませんけれども、有事に混乱が起こる原因の一つとして、誰が何の責任者なのか曖昧というケースがありますよね。例えば三・一一を思い出していただきたいんです。東電福島第一原発事故のとき、政府の事故担当責任者、司令塔は、原子力安全・保安院の寺坂院長なのか、原子力安全委員会の班目委員長なのか、伊藤内閣危機管理監だったのか、何かはっきりしないなみたいな、何かそういう状

態があったと思うんですね。

〔理事相原久美子君退席、委員長着席〕

そこで、今後のサイバーテロ対策について、責任者、担当大臣は誰で、事務方の責任者は誰なのか、これはっきりさせておくべきだと。もちろん厚労省、年金の問題、もう大問題でしたから、年金情報流出事件の後ですし、そこら辺はしっかり決まっているだろうと思いましたけれども、一応念のために確認したんですよね。

三日前、月曜日にお聞きしたときには、ＮＩＳＣは、サイバーセキュリティーの責任者は菅官房長官であると、事務方の責任者はＮＩＳＣ、すなわち高見澤センター長、サイバーテロ対策の責任者は国家公安委員長で、事務方の責任者は警察庁ということだったんですけれども、昨日聞いたときには、サイバーテロ対策の責任者は国家公安委員長ではなく菅官房長官で、事務方の責任者は警察庁ではなくてＮＩＳＣの高見澤センター長であると。そして、伊勢志摩サミットのサイバーテロ対策の責任者も菅官房長官で、事務方の責任者は谷脇ＮＩＳＣ副センター長ということになったんですよね。聞く度にこれ答えが二転三転するという、混乱されているんだなとちょっと心配したんですけれども、この質疑をきっかけにそういうはっきりとしたことというのがこの後決まっていくようでよかったです。

サイバーに関する事象が起これば、結局警察のお世話になるしかないんですよね、結局警察に最後それを伝えて捜査してもらうという、そういう段階になるわけですから。サイバーテロ、これ明らかに犯罪なんだから、もうこの責任者、国家公安委員長でいいんじゃないのって、事務方の責任者は警察庁長官とすべきなんじゃないかなと思うんですよ。

警察のこれ警察白書というのを見てみたんですけれども、特集として、サイバー空間の脅威への対処というような内容で、もう初めからこれ特集としてサイバー問題が組まれているんですけれども、すごいですね、警察。サイバー攻撃対策官、サイバーフォースセンター長というのを置いて、サイバー攻撃分析センターというのをトップに、そこに技術情報の提供というのが上がってくると。それと併せて、横で連携して捜査、捜査の成果も上がってくると。捜査の方で置かれているのがサイバー攻撃特別捜査隊、十三都道府県警察の公安部、警備部に設置と。サイバーフォース、これ情報通信部門、本庁、七管区、五十一都道府県、方面の情報通信部に設置って、もう完璧じゃないか、もう既にあるじゃないかという話なんですよね。

これ、ＮＩＳＣがここに関わっていくという意味合いがどれぐらいこのサイバーセキュリティーという問題に対して効果をもたらすのかという部分も考えなきゃいけないなと。もう既にあるんだから、ここをもっと拡大していけばいいじゃないかって、何かワンクッションつくる必要があるのかなというふうにも思っちゃうんですけれども。

先ほど私が言った、サイバーテロに関してはもう明らかに犯罪なわけですから、責任者は国家公安委員長、事務方の責任者は警察庁長官ということじゃまずいんですかね、大臣。遠藤大臣、いかが思われますか。

○政府参考人（谷脇康彦君）　お答え申し上げます。

サイバーテロを含むサイバー犯罪に関して、これを捜査をし検挙をしていく、これは当然警察庁が行うべき責務であるというふうに考えております。ただ、広い意味でサイバーテロ対策を考えました場合に、重要インフラ、鉄道、通信等に対するサイバー攻撃が生じた場合、あるいはそれを予防するための対策というものは重要インフラを所管している省庁でそれぞれ行っているところでございます。そして、こうした取組を政府一体として行っていくために私ども内閣官房が全体の政策調整を行っているわけでございまして、それぞれの役目に応じて、かつ責任分担を明確にしながら、政府の中でサイバーセキュリティー対策を講じているところでございます。

○山本太郎君　そうですか。

日本の原発に対するサイバーテロ対策の政府の責任者、担当大臣、誰になりますか。また、事務方の責任者は誰でしょうか。そして、原発に対するサイバーテロ対策というのはあるんですか、教えてください。

○政府参考人（荻野徹君）　お答え申し上げます。

我が国の原子力発電所におけるサイバーテロ対策ということでございますが、法令上、原子炉等規制法に基づきまして、いろいろな国としての規制がございます。情報システムが電気通信回線を通じて妨害破壊行為を受けないように所要の対策を講じなさいということを事業者に法令上義務付ける、その法令上の義務付けについて、原子力規制委員会として、事業者の防護措置の内容、体制の有効性について検査、確認をするといったことを平素からやっております。

そういった意味で、原子力規制委員会が原子炉等規制法に基づき責任をもって対応しているというところでございます。

○山本太郎君　なるほど、サイバーテロ対策というのはもうされているんだよというお話なんですよね。確かにそうなんですよね、防護措置規定九十一条の規定というのもあるんだと。何かあったときには電気通信回線というのは遮断されるようになっているんですよねというような話ですよね。

でも、世界見てみたら、回線遮断するなどでは原発へのサイバー攻撃というのは防げない話というふうになっているのは御存じですよね。だから、新たに何かが必要だということはもう明らかなんですよね。防護措置規定九十一条で回線遮断するんだということが可能だからそれでオーケーだという話ではなく、サイバー攻撃というのはもっともっと進化していくものなんじゃないんですか。一秒ごとにというような話だと思うんですけれども。

チャタムハウス、英王立国際問題研究所は、原発を標的とした重大なサイバー攻撃のリスクは増大していると警告をしています。世界中の多数の専門家は大規模なサイバー攻撃の脅威の危険性は低いと考えている、なぜならば原子力施設の重要なコンポーネントは空間的に隔離されているからだと問題を指摘し、チャタムハウスは世界中の多数の専門家の考えは間違いだと明言しています。このチャタムハウスの指摘を受けてＢＢＣは、一般的なインターネットと原子力システムのいわゆるエアギャップは単なるフラッシュドライブを用いて容易に突破できる、破壊的なコンピューターウイルスはこのルートからイランの原子力施設を感染させたということに着目してほしいと、そのように報じたそうです。

サイバーセキュリティー、サイバーテロに関して、新たに新規制基準では対策をどの程度まで求めているんでしょうか。規則に不正アクセス行為を防止すると書いてあるだけじゃないですか。何かもっと先にもあるんですかね、これ見ていけば。でも、文章上書かれているのはそれだけだったんですけどね。サイバーセキュリティー、サイバーテロ問題に原子力規制庁は付いていけているのかなと。

今回の法案でも原子力事業者は対象になっていません。旧来の手法で大丈夫ですか。日本の原発を保有するほかの先進国とでは、危機意識のレベル、余りにもちょっと違い過ぎないかと。特にアメリカ、原子力施設に対するサイバーテロ、十分に想定をしている。武力攻撃の対象だとまで言及していると。原発へのサイバーテロについて、現在エール大学教授のハロルド・コーは、国務省法律顧問だった二〇一二年当時、直接的に死者、負傷者、重大な破壊行為を引き起こすサイバー攻撃は武力行使となり得るとした上で、原子力関連施設のメルトダウンを引き起こす攻撃を武力攻撃相当として挙げている。

アメリカは、二〇一六年二月九日、サイバーセキュリティー・ナショナル・アクション・プランを発表、二〇一七年度予算案では対前年度比三五％アップ、百九十億ドル、約二兆円のサイバー

セキュリティー関連費用を盛り込んだ。日本はどうだ。かなり増額されましたよね。平成二十八年度当初予算で四百九十九・三億円、平成二十七年度補正予算で五百十三・八億円、合わせて一千億円程度だと。これ足りるのかなって。原発のサイバーセキュリティー、セイバーテロを真剣に考えるとすると、この予算で守り切れますかっていう話なんですけどね。結局、原発は廃炉を急いだ方が経済的にも安全保障上も正解なんじゃないのっていうことだと思うんですよ。

原発に対しても当然サイバー攻撃の危険性を十分に認識する国が存在している一方で、原発が存在するのにそれに対するリスクヘッジは最低限の国が存在している。政治の無策で犠牲になるのはその国に生きる人々であると。核施設が列島を取り囲むこの国でそれをターゲットにされてしまえば、現在収束不能な東電原発に加え、もう一か所事故原発を抱える余力というのはこの国にはあるんですかね。もうミスれないぞって。

日本年金機構の情報漏えい問題での対応を思い出すと、五月十九日に年金機構が警視庁へ通報したことをＮＩＳＣが知ったのは十日後の五月二十九日だった。これが原子力発電を狙ったサイバー攻撃だったらと考えると背筋凍りませんか。ＮＩＳＣでワンクッション置く必要あるのかなって。もう警察にあるんだから、警察のこの部分をもっと強化して力を入れた方がいいんじゃないのって、ワンクッションつくる意味あるかなって。この十日間の空白って恐ろしいですよね。

国家の存亡に関わるほどの威力を持った施設が日本には山ほどあるわけですから、せっかく法改正するんだったらもっと危機感を持った権限拡大を目指してほしいよなと思うんですよね。なので、修正案を準備させていただいたので、詳細は後ほどお話ししたいと思います。

話を戻します。

サイバーテロについては、私は、日本壊滅のリスクがある原発へのサイバーテロへの対策は非常に重大で、今回の法案においても特に原子力事業所については政府の責任で監視等を行うべきだと思うんです。遠藤大臣、見解はいかがでしょうか。

○国務大臣（遠藤利明君）　サイバーセキュリティーの確保を含む原子力事業所における安全の確保については、核原料物質、核燃料物質及び原子炉の規制に関する法律に基づき原子力規制委員会が対応しているものと承知をしております。サイバーセキュリティ戦略本部及びその事務局である内閣サイバーセキュリティセンターは、現行の基本法の枠組みの中において、原子力規制委員会等の関係行政機関との間において情報共有を行ってきており、必要に応じて助言等を行っております。

したがって、お尋ねの原子力事業所のサイバーセキュリティーの確保については、現行の法令の枠組みの中において対応することが適当であると思っております。

○山本太郎君　サイバーセキュリティー、サイバーテロを本気で防ぐんだったら本法案では不十分であるのはよく分かることだと思うんですけれども、車の両輪、これがそろっていなきゃいけない。もう片方、余り具体的にならない部分が改善されなきゃサイバーセキュリティー、サイバーテロを防げないと思うんです。どういうことか。政府、公共機関に働く非正規職員の皆さんの厳しい労働環境の話です。年金機構の問題、そこで働く人々のヒューマンセキュリティーがしっかりと守られなければならないということを教えてくれた事案だったと思うんですよね。

例えば年金機構、平成二十八年四月現在で、正規の職員数一万一千九百五十二人、非正規職員数は九千八百三十五人。現在の時給の平均、千百八十二円だそうです。上がったんですって、賃金。でも、一日八時間、二十日間働いたとしたら幾らでしょうか、十八万九千百二十円。余裕で官製ワーキングプアのままなんですよ。

同一価値労働同一賃金の原則に反する人権無視の労働環境を押し付けて、守秘義務だけは正規職員と同じ、厳しい罰則まである。年金機構法二十五条秘密保持義務、五十七条罰則、一年以下の懲役又は百万円以下の罰金。サイバーセキュリティーを担っているのは人間だと。サイバーセキュリティーは実はヒューマンセキュリティーなんだと。人間の安全保障の問題であると私は思うんです。

年金機構など、非正規の人たちを正規職員にしていく必要があると思います。同一労働同一賃金を宣言した政府を挙げてこれに取り組むことがヒューマンセキュリティーのレベルを上げていく、サイバーセキュリティーのレベルを上げていくことになると思うんですけれども、厚労省、いかがですかということが一点。

そして、本法案を急ぐように、いや、それ以上にだと、もっと急いで職員の待遇改善が行われなきゃ、サイバーテロを防ぐ下準備というのがまだできていないんだよと。遠藤大臣、その厚生労働省の答えを受けた上で、この問題について厚生労働大臣にその件を提案していただけますかという、この二点についてそれぞれお答えいただけますか。お願いします。

○委員長（神本美恵子君）　時間が来ておりますので、答弁は簡潔にお願いします。

○大臣政務官（三ッ林裕巳君）　お答えいたします。

日本年金機構の職員体制については、正規職員のほか、効率的に業務を実施するという観点から、正規職員の指揮の下、年金相談や入力など業務の補助を行う職員として有期雇用職員を雇用しております。これらの職員は補助的業務であることから、賃金等は正規職員とは異なったものとなっております。

日本年金機構は、今般の情報流出事案を踏まえて業務改善計画を策定し、情報セキュリティー対策はもとより、人事制度の改革にも取り組むこととしており、その中では有期雇用職員についても、活性化の観点から、無期化制度の活用、評価の導入と意欲、成果に応じた処遇といった項目が盛り込まれていると承知しております。機構においては今後これらの具体化に取り組んでいくこととなりますが、厚生労働省としても必要な助言、指導を行ってまいる所存でございます。

○国務大臣（遠藤利明君）　今厚労省から話がありましたが、御指摘のとおり、処遇面での配慮が必要だと認識をしております。引き続き待遇の改善等について努めていきたいと思っております。

○山本太郎君　是非、厚生労働大臣にそのことを伝えてください。サイバーセキュリティーに一番大事な部分です。

ありがとうございました。

○山下芳生君　日本共産党の山下芳生です。

サイバーセキュリティ基本法に基づいて、サイバーセキュリティ本部が国家安全保障会議の意見を聴いて昨年九月公表、作成したサイバーセキュリティ戦略、ここには外国政府機関との情報共有を含む情報収集、情報分析機能の強化を図るとあります。その必要性について、サイバー攻撃とそれに対する抑止の特徴との関係で説明をしていただけますか。

○国務大臣（遠藤利明君）　サイバー空間を取り巻くリスクが深刻化する中で、国境を越えた自由な情報の流通を可能とするサイバー空間の便益を享受するとともに、国家の安全保障、危機管理上の課題でもあるサイバー攻撃に迅速かつ的確に対応するためには、諸外国等と効果的に連携することが必要と認識をしております。

政府としましては、管理や規制を過度に行うことなく、開放性や相互運用性を確保することにより、情報の自由な流通が確保された安全で信頼できるサイバー空間を構築することを基本方針として関係国との国際連携に取り組んでおります。こうした認識の下で、昨年九月にも閣議決定されましたサイバーセキュリティ戦略においても、多様な主体との国際的な連携により、サイバーセキュリティーの確保及びサイバー空間におけるグローバル規模の情報の自由な流通の確保に向け取り組むこととしております。

今後とも、サイバーセキュリティ戦略に基づき、

関係各国との連携を積極的に深めるとともに、多国間の議論にも積極的に貢献してまいりたいと考えております。

○山下芳生君　今基本的な認識、遠藤大臣に述べていただきましたけれども、ここでは遠藤大臣とそもそもサイバー空間の特徴について少し議論したいと思うんですが、一つはアクターの多様性ということが言われます。どの相手が攻撃してくるか分からない。非国家主体も高度な能力を保有している。軍事力を持つ必要はないんですね。高い能力を持つ個人でもサイバー攻撃はできる。

それから二つ目に、隠匿性、ボーダーレス性ということが言われております。攻撃者の特定が極めて困難です。国家の関与もなかなか決着が付きません。米中韓でもこれはもう論争になっております。アメリカへの攻撃は中国から発信されているじゃないかとアメリカが言っても、いや、それは経由しているだけであって中国も被害者なんだとか、いやいや、確実に中国から攻撃が発信されているじゃないかと、こう指摘しても、それは政府とは無関係だと、こういうふうに言われるわけですね。

このアクターの多様性、隠匿性、ボーダーレス性、これが特徴だということについて、大臣の御見解、どうでしょうか。

○国務大臣（遠藤利明君）　今委員御指摘のように、その発信がどこからなされたか、この追及はなかなか難しいと認識をしております。それだけに、なおさら国際間の協調が必要だと思っております。

○山下芳生君　それからもう一つ、サイバー空間に関する規範はいまだ形成途上であるということも大事だと思っております。サイバー攻撃に対して自衛権を行使することの合法性、あるいは自国内のアクターによるサイバー活動に対する国家責任等について、コンセンサスは今存在しておりません。その国の中のある個人がサイバー攻撃を行ったとしても、政府の責任とは言い切れないという現状にあります。

要するに、サイバー空間における規範、まだ確立されていない、途上である、この点いかがでしょうか。

○国務大臣（遠藤利明君）　今御指摘のように、規範についてまだ正確にこれだということになっていないと思いますが、そうしたことを国際間においていろいろ議論をしている最中だと認識をしております。

○山下芳生君　そうなんです、途上なんですね。

さらにもう一つ、サイバー攻撃に対する防御について、報復の信憑性ということも言われております。

どういうことかといいますと、どこまで攻撃されればレッドラインとして反撃できるのか、この設定がなかなか難しい。報復能力の証明、つまり、これぐらい攻撃されたら報復する能力を有していますよということをどのように伝えるか、どの相手に伝えるか、これもなかなか難しい。それから、通常戦力による報復というのが許されるのか、非国家主体に対する報復などが一体できるのかどうか、困難ではないか。

こういう報復の信憑性ということも問題になっておりますが、この点、大臣、いかがでしょうか。

○国務大臣（遠藤利明君）　委員御指摘のように、技術が進めば進むほど特定化は難しいと、それだけになおさら国際間の情報の共有、連携が必要だと思っております。

○山下芳生君　そこで、じゃ、その国際間の連携なんですが、安倍政権が策定した国家安全保障戦略には米国とのサイバー防衛協力の推進がうたわれております。それから、昨年四月の新日米ガイドラインにはサイバー空間に関する協力という項目が初めて設けられました。

遠藤大臣、なぜこの分野で米国との協力が必要なんでしょうか。

○国務大臣（遠藤利明君）　米国は日米安全保障体制を基軸にあらゆるレベルで緊密に連携する我が国の同盟国であり、サイバー分野においても様々なチャンネルにおける緊密な情報共有と連携を図る必要があります。

これまで両政府間においては、平成二十五年五月、平成二十六年四月、平成二十七年の七月の三回にわたり日米サイバー対話を実施してきており、日米双方のサイバーセキュリティー関係省庁が参加する形で、双方の政策動向、情勢認識等につき協議を実施しております。

○山下芳生君　もう既に日米サイバー対話というものが三回行われたということであります、今御報告があったとおりですが。

では、米国のサイバー戦略とは一体どういうものかについて伺いたいと思います。

二〇一一年十一月、国防省サイバー空間政策報告書は、拒否的抑止、これは何とか攻撃されないようにする抑止とともに、懲罰的抑止、報復型の抑止ですね、これについても言及しております。それから、通常兵力を用いた報復も選択肢とするというふうにあります。

この懲罰的抑止、通常兵力を用いた報復とは一体どういうことでしょうか。

○政府参考人（水嶋光一君）　お答え申し上げます。

米国のサイバー戦略につきましては、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認識しているものと承知をしてございます。

その上で、今御指摘のございました国防省によります二〇一一年十一月のサイバー空間政策報告書でございますけれども、ここにおきましては、サイバー空間におけます抑止について、ほかの領域と同様に、攻撃者の目的達成を拒否するとともに、必要に応じて攻撃者にコストを課すとの考え方に基づくものであるというふうに述べられているものと承知をしてございます。

また、加えまして、その報告書におきましては、サイバー空間での一定の活動、これは武力の行使を構成し得るものであり、また、合法的な自衛権を発動し得るものであるという旨述べているものだと承知をしてございます。

○山下芳生君　サイバー攻撃に対して武力行使もやりますよということをアメリカはそういう戦略でもうはっきりうたっているわけですね。

それから、二〇一二年十月十一日、パネッタ国防長官の演説で、サイバー攻撃による大規模な被害が差し迫っている場合にはサイバー空間で先制攻撃を行う可能性に言及しています。サイバー空間での先制攻撃を行うとはどういう意味でしょうか。

○政府参考人（水嶋光一君）　御指摘の、二〇一二年十一月、パネッタ国防長官の講演でございますが、この中では、国防省といたしましてはサイバー攻撃の抑止に取り組んでいると言った上で、米国が攻撃者を特定できて、また米国の強力な防御によって攻撃が失敗するというふうに承知していれば米国が攻撃される可能性は低くなるというふうに述べていると理解をしてございます。

ただ、その中で、また仮に米国に重大かつ物理的な破壊をもたらして、又は米国市民を殺害するサイバー攻撃の切迫した脅威を察知した場合には、米国は、大統領が指示した際には、国家を守るために攻撃者に対して措置をとる選択肢を持たなければならないと、そういうふうに述べられていると承知をしてございます。

○山下芳生君　先制攻撃戦略、サイバー空間における戦略、取っているということですね。察知したら先制攻撃すると、相手を殺傷することも含めてですね。これは、イラクに対する、大量破壊兵器を持っていると察知したはずだったけれども、それは間違いだったということを想起させられるものであります。

二〇一二年、オバマ大統領は、大統領政策指令20、米国のサイバー作戦政策に署名をしていまして、そこでは重大な帰結（人命の喪失等を含む）をもたらす作戦ということが言われておりますが、こういうことも言われているわけですね。先ほど述べられたとおりです、殺傷ということも含めて、サイバー攻撃、先制攻撃も戦略として取ら

れている。

それから、ニューヨーク・タイムズが、二〇一三年二月三日、オバマ政権が検討中とされるサイバー作戦に関する交戦規則の内容を報道しております。先制攻撃を命じる権限を大統領に付与、そういう中身の交戦規則があると言われておりますが、こういう交戦規則あるんですか。

○政府参考人（水嶋光一君）　今御質問にございました新聞報道、それから交戦規則でございますが、米国政府としましてはこれは対外的に明らかにしたものだとは我々承知しておりませんので、お答えは差し控えさせていただきたいと思います。

○山下芳生君　アメリカと緊密に協力する、サイバー攻撃に対する対処をと言いながら、アメリカのこの戦略の交戦規則について承知しない。余りにもこれは無責任だと言わなければなりません。

遠藤大臣、安倍政権の下で、昨年の安保法制の審議の中でも安倍総理はサイバー攻撃に対する日米同盟の強化ということを答弁されています。それから、中谷防衛大臣もこう言っております。武力攻撃の一環として行われたサイバー攻撃に対して武力を行使して対応することも法理としては考えられる。

遠藤大臣に伺いますが、政府はサイバー攻撃に対して武力を行使して対応するという立場ですか。

○副大臣（若宮健嗣君）　今質疑をなされている中で、やはり様々な見解がもうお示しをされているかと思います。また、山下委員の御質問でも、また御自身の意見でも出されておられますけれども、現在、確かに高度化、巧妙化するサイバー攻撃の態様を実際踏まえますと、今後、サイバー攻撃によって極めて深刻な被害が発生する可能性というのはこれは否定できないのはもう委員も御承知のところだと思っております。

このサイバー攻撃への対応というのは、我が国にとりましても安全保障に関わります重要な課題であるというふうに認識をしているところでございます。また、今日、弾道ミサイルや航空機等による武力攻撃が行われる場合には、もちろんその一環としてこれは同時にサイバー攻撃ということが行われる可能性というのも想定をしておかなければいけないのではないかというふうにも考えているところでございます。

その上で、私ども政府といたしましては、従来、サイバー攻撃が武力攻撃の一環として行われた場合、自衛権を発動して対処することが法理としては可能であるというふうには御説明申し上げているところではございますけれども、現在、これまでにはサイバー攻撃に対しまして自衛権が行使された事例というのはございませんでして、サイバー攻撃に対します自衛権行使の在り方につきましては、委員も御指摘でございましたが、国際的にも様々な議論が行われている段階でございます。このため、現実の問題といたしましては、サイバー攻撃に対します自衛権の行使の在り方につきましては、国際的な議論を見据えながら更に検討を進めてまいりたいと、このように考えているところでございます。

○山下芳生君　要するに、まだ決めていないけれども法理としてはあり得るという立場なんですね、ずっと。これは非常に、この方向でいいのかということを私は危惧するわけですね。

実際に日米間では共同演習の中でサイバー攻撃に対する訓練も行われております。防衛省に伺いますが、これまで二〇一三年から毎年やっていますけれども、どのような訓練が行われましたか、報告してください。

○政府参考人（笠原俊彦君）　お答えいたします。

議員御指摘のとおり、二〇一三年から二〇一五年、日本で実施をされた日米共同方面隊指揮所演習というのがございますが、そちらにおきまして、各種事態における実効的な対処能力の向上を図る一環として、自衛隊と米軍に対してサイバー攻撃が行われたという状況を想定をいたしました対処要領及び連携要領について演練を行ったところでございます。

○山下芳生君　もう漠としかお答えにならないんですが、具体的にどういう訓練をやったのかと聞いても、これは答えられないんですよ。――あっ、どうぞ。

○政府参考人（笠原俊彦君）　失礼いたしました。

訓練の内容でございますけれども、不審メールを受信した際に受信者である情報システム使用者が行うべき対処要領や、原因究明、被害拡大防止のために情報システム担当部署が行う対処要領の確認などを実施しているところであります。また、サイバー攻撃による被害拡大を防止するためには日米の連携が重要でありますことから、その連携要領についても確認をしたところでございます。

以上です。

○山下芳生君　要領が確認されたということであって、どういう具体的な話がされているのかということについては幾ら聞いても答えが返ってこないということで、国民からは見えないところで、サイバー攻撃に対する対処という下で訓練が日米間で毎年やられているということなんです。その米国は、サイバー攻撃に対して先制攻撃、通常兵力による攻撃、これもいとわないという戦略を持っているわけですから、それに対して、今防衛副大臣が答弁されたように、サイバー攻撃に対する武力の行使についてはしっかりと拒否するという立場ではないわけですね。そういう方向に行っていいのかということを私は本当に危惧します。

これは、アメリカや日本がサイバー攻撃、確かにいろんなインフラ、電力だとか工場だとか、そういうものに対するサイバー攻撃は大変な被害を与えますから、それに対して防御すること、備えることは必要でしょう。しかし、備えることによって、先制攻撃する、通常兵器による攻撃まで検討する、また備えるということでやりますと、これはアメリカや日本がそういうふうに備えれば、恐らく他の国々あるいは勢力、個人かもしれません、そういう勢力もそういう方向に備えざるを得ないと思うんですよね。お互いにサイバー空間のリスクを高め合う方向で、サイバーセキュリティーといいながらリスクが高まるという心配が当然起こってくると思うんですが、その点、遠藤大臣、いかがですか。

○国務大臣（遠藤利明君）　備えあれば憂いなしという言葉がありますが、それぞれの国がそれぞれの対応をしておりますので、国としてしっかり取り組まなきゃならないと考えております。

○山下芳生君　いや、私が聞いたのは、それぞれの国がしっかりやると相手の国もしっかりやる、そうすると非常に高いリスクが相互に高まり合うということになるんじゃないかと。要するに、米ソ間で核兵器がどんどんどんどん増えていくような、あるいはテロに対する報復としてテロが一層拡散するような、そういう悪循環になる危険がこの分野でももう生まれているんじゃないかということを私は危惧するわけですね。

国連の情報セキュリティーに関する政策専門家会合、ＧＧＥがサイバー空間における信頼醸成措置、ＣＢＭについて検討していますが、どのように述べていますか。

○政府参考人（水嶋光一君）　今御指摘ございました国連のサイバー政府専門家会合、ＧＧＥと申しますが、これは二〇〇四年以来今まで四回の会期で開催をされてございます。

こちらでは、責任ある国家の行動規範、また信頼醸成措置、それから国際協力、能力構築支援、それからＩＣＴの利用に関する国際法の適用などの国際安全保障の文脈におけます情報通信技術の進歩に関します幅広い議題について議論が行われてきております。最近では、二〇一五年七月に最終的な報告書が公表されているところでございます。

このうち今お尋ねございました信頼醸成措置につきましては、この信頼醸成措置が国際の平和及び安全を強化するんだという前提の下で、各政府におきましてコンタクトポイントを特定をするとか、あるいは二国間、多国間の協議メカニズムを構築するとか、あるいは透明性を向上する努力を続けるとか、あるいは学術研究機関の間での交流を促進する、あるいはＩＣＴを用いた犯罪・テロ

対策協力を進める等についての提言が行われていると承知してございます。

○山下芳生君　非常に重要な指摘だと私は思いました。

遠藤大臣、防御という名の下での先制攻撃まで一つのブロックが高めるという方向をお互いに各国がやり始めますとリスクが高まる。そうじゃなくて、信頼醸成をやる必要があるというこの国連の専門家会合の指摘、非常に重要だし、日本もその立場でどういうルールが必要なのか。今、世界の実態踏まえた積極的なこういう信頼醸成についての関与必要だと思いますが、いかがですか。

○委員長(神本美恵子君)　遠藤大臣、時間ですので、簡潔にお願いします。

○国務大臣(遠藤利明君)　はい。

信頼醸成は極めて大事だと認識をしております。

○山下芳生君　そういう方向で努力せずに、アメリカと一緒になってサイバー空間における先制攻撃までやるような軍事優先のやり方は極めて危険だということを申し上げて、終わります。

○委員長(神本美恵子君)　この際、委員の異動について御報告いたします。

本日、福岡資麿さんが委員を辞任され、その補欠として山田修路さんが選任されました。

○委員長(神本美恵子君)　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。

本案の修正について山本太郎さん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。山本太郎さん。

○山本太郎君　ありがとうございます。

私は、サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案に対し、修正の動議を提出いたします。その内容は、お手元に配付されております案文のとおりでございます。

これより、その趣旨について御説明いたします。

東日本大震災から五年がたった今も、東京電力福島第一原子力発電所では放射性物質の放出が続き、コントロールできない汚染水との闘いが続いています。年間一ミリシーベルト以下に抑えるはずだった被曝を年間二十ミリシーベルトにまで引き上げられたという不条理も続いています。福島第一原発事故等による福島県民の避難者は、今年二月現在で今なお九万八千七百六十二人。避難指示区域についても、区域見直しが行われたり、一部の区域で解除されたりしたものの、依然として多くの市町村で設定されたままです。

このように、一たび原子力災害が発生すると長期間にわたり広範囲で甚大な影響が続くこととなりますが、自然災害のみならず、サイバー攻撃が原子力災害を引き起こすおそれもあります。実際、二〇一〇年、イランにおいて、ウラン濃縮施設へのサイバー攻撃により遠心分離機が全て停止したという事案が報道されております。

現行のサイバーセキュリティ基本法第十四条では、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ーに関し、自主的な取組の促進など必要な施策を講ずるものとすると定められておりますが、原子力災害が甚大で過酷であることを踏まえ、サイバーセキュリティ基本法上、原子力災害の発生を防止するためのサイバーセキュリティーの確保について特に定める必要があると考えます。現在でも、規則により、電気通信回線のアクセス遮断などの措置がとられていますが、十分ではありません。英国の王立国際問題研究所は、原発を標的とした重大なサイバー攻撃のリスクは増大していると警告をしています。

また、原子力規制委員会は、原子力利用における安全の確保を図ることを任務としておりますが、原子力規制委員会設置法上、委員として求められる専門的知識等にサイバーセキュリティーが含まれるかが明確ではなく、現在の委員の経歴を見る限り、サイバーセキュリティーの専門家は含まれておりません。

そこで、修正案は、原子力事業所におけるサイバーセキュリティーを強化するため、国は、原子力事業所における安全の確保に関する基準においてサイバーセキュリティーの確保につき必要な定めをし、及びその遵守を確保することその他の必要な施策を講ずるものとすると定めるとともに、サイバーセキュリティ戦略本部の所掌事務に、この基準の策定等に関し、原子力規制委員会に対し必要な助言、情報の提供その他の援助を行うことを追加しております。

以上が修正案の趣旨であります。

何とぞ、委員各位の御賛同を賜りますようよろしくお願い申し上げます。

○委員長(神本美恵子君)　これより原案及び修正案について討論に入ります。

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基本法及び情報処理の促進に関する法律の一部改正案に反対の立場から討論を行います。

現行サイバーセキュリティ基本法は、国の行政機関を対象に、情報システムに対する不正な活動への国による監視・分析、演習・訓練の実施や監査、重大事案発生時における原因究明調査などを定めていますが、本法案は、こうした監視、調査等の対象を独立行政法人や指定する特殊法人等にも拡大するものであります。

日本年金機構の大量データ流出事案への対策を口実にしていますが、年金機構の個人情報流出問題は厚労省や年金機構のそもそもの業務の在り方の問題であり、政府のサイバーセキュリティ戦略でも主体的管理、自律的メカニズムの構築、運用が基本とされているのであり、監査、監視があれば起こり得なかったというものではありません。

サイバーセキュリティーが軍事、安全保障に密接に結び付けられている中で、全独立行政法人や特殊法人に演習や訓練、監視、調査の対象を拡大することは認められません。

現行法の「目的」には、我が国の安全保障が明記されています。安倍政権が策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、昨年四月の新日米防衛協力のための指針、ガイドラインはサイバー空間に関する協力を初めて明記し、日米政府が平時から緊急事態までのいかなる状況においてもサイバーセキュリティーのための実効的な協力を確実に行うために共同演習を実施、深刻なサイバー事案が発生した場合、日米政府は緊密に協議し、適切な協力行動を取り対処するとされています。

実際、ＮＩＳＣ、内閣サイバーセキュリティセンターの情報は、ほぼそのまま国家安全保障会議に報告をされ、アメリカにも共有されています。米国は、サイバー事案に対して武力行使をすること、場合によってはサイバー攻撃を先制的に行うことを表明しています。今回の対象拡大の措置は、アメリカのサイバー戦略に巻き込まれる土壌づくりとの懸念を拭い切れません。

国連では軍事的対応ではないサイバー空間における信頼醸成措置の在り方について議論がされているところであり、サイバー空間を民主的、平和的に維持するためにこそ力を注ぐべきであります。

以上、反対討論とします。

○委員長(神本美恵子君)　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。

それでは、これよりサイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案について採決に入ります。

まず、山本太郎さん提出の修正案の採決を行います。

本修正案に賛成の方の挙手を願います。

〔賛成者挙手〕

○委員長(神本美恵子君)　少数と認めます。よって、山本太郎さん提出の修正案は否決されました。

それでは、次に原案全部の採決を行います。

本案に賛成の方の挙手を願います。

〔賛成者挙手〕

○委員長(神本美恵子君)　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、相原さんから発言を求められておりますので、これを許します。相原久美子さん。

○相原久美子君　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及び情報処理の促進に関する法律の一部を改正する法律案に対し、自由民主党、民進党・新緑風会、公明党、おおさか維新の会及び日本を元気にする会・無所属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及び情報処理の促進に関する法律の一部を改正する法律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るべきである。

一　内閣サイバーセキュリティセンターは、サイバーセキュリティ対策を実施するために必要な経験と能力を備えた人員、予算、人材育成措置を継続的に確保し、サイバーセキュリティ戦略を着実に実施可能な体制を整備するとともに、業務を委託する法人に対しても、当該業務を着実に実施させるために必要な措置を講ずること。

二　サイバー攻撃の多様化等の環境変化に柔軟に対応したサイバーセキュリティ対策を適切に実施するため、内閣サイバーセキュリティセンターを中心とし、サイバー攻撃事案発生時における被害の抑制や迅速な対処のための支援措置、重要社会基盤事業者等における事案情報の迅速かつ省庁横断的な共有、被害の有効な回避のための措置の準備等、必要となる施策を講ずること。

三　平成二十二年十二月二十七日の情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せに基づき、初動対処訓練等を通じて即時対応可能な能力を確保するために必要な措置を実施するとともに、今後とも適宜シナリオ非提示型の訓練を実施し、各行政機関の効果的なサイバーセキュリティ体制の構築に役立てること。

四　国の行政機関等の情報システムに対する不正な活動の監視その他の当該情報システムを防御するために必要な措置を講ずるに際しては、各行政機関等における保秘の運用基準、サイバー攻撃事案発生時の関連企業等との約定事項等が異なり得ることを踏まえ、内閣サイバーセキュリティセンターから業務を委託される法人が、必要な範囲を超えて関係機関の所掌事務に関する情報に触れることがないよう留意し、その上で、同センターが不正な活動の痕跡情報や属性の調査も視野に入れた対応を実施できるよう、関係機関と事前協議を重ねるなどして協力関係を密にすること。

五　本法施行から二年を経た後に、内閣サイバーセキュリティセンターが監査業務を委託する法人による独立行政法人及び指定法人に対する業務の在り方を検証し、関係機関に対する監査業務の委託の是非を検討すること。

六　監査業務を委託する法人を選定するに当たっては、国立研究開発法人情報通信研究機構を始めとする各法人の特性と能力を見極め、事態を幅広く想定してきめ細かく精査するように努めること。

七　内閣サイバーセキュリティセンターが独立行政法人情報処理推進機構以外に業務を委託する場合には、その所掌業務、当該業務に係る秘密保持義務等の必要な規定の整備を行うこと。

八　内閣サイバーセキュリティセンターの設置根拠や所掌事務、権限等について、現行制度では業務遂行に重大な支障が生じる状況になった場合には、サイバーセキュリティ基本法とは別の法律に定めること等の法制上の措置の是非を検討し、適切に対応すること。

九　内閣サイバーセキュリティセンターは、我が国の組織に対するサイバー攻撃に関する情報のより迅速かつ効果的な共有の在り方について検討し、適切に対応すること。

十　サイバーセキュリティ戦略を検討するに当たっては、それがインターネット上の自由を阻害し、サイバー空間が分断される要因とならないよう、細心の注意を払うこと。

十一　本法には、平成二十六年十月二十三日の本委員会におけるサイバーセキュリティ基本法案に対する附帯決議の諸点のうち三及び七の観点を踏まえ、防護対象となる特定の行政機関や重要社会基盤事業者等について、サイバー攻撃事案の態様によっては我が国の安全と秩序に極めて深刻な影響を与えかねない対象となるかどうかを区別し、防護対象の重要性の段階に応じ、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措置することとともに、これらの対象に対する実効ある帯域制御の在り方について所要の検討を進めること。

十二　本法施行後二年以内に、サイバーセキュリティ基本法の施行の状況及び本附帯決議への対処の状況を踏まえ、サイバーセキュリティ基本法を見直す必要性について検討し、その結果に基づいて、必要な措置を講ずること。

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申し上げます。

○委員長（神本美恵子君）　ただいま相原さん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（神本美恵子君）　多数と認めます。よって、相原さん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、遠藤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。遠藤国務大臣。

○国務大臣（遠藤利明君）　ただいま御決議のありました事項につきましては、その御趣旨を十分に尊重してまいりたいと存じます。ありがとうございます。

○委員長（神本美恵子君）　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（神本美恵子君）　御異議ないと認め、さよう決定いたします。

○委員長（神本美恵子君）　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。

内閣の重要政策及び警察等に関する調査のため、参考人の出席を求め、その意見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（神本美恵子君）　御異議ないと認めます。

なお、その日時及び人選等につきましては、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（神本美恵子君）　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。

午後一時七分散会

〔参照〕

サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案に対する修正案

サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案の一部を次のように修正する。

第一条中第十三条の改正規定の次に次の改正規定を加える。

第十五条の次に次の一条を加える。

（原子力災害の発生を防止するためのサイバーセキュリティの確保）

第十五条の二　国は、サイバーセキュリティに対する脅威により原子力災害（原子力災害対策特別措置法（平成十一年法律第百五十六号）第二条第一号に規定する原子力災害をいう。）が生ずることを防止するため、原子力事業所（同条第四号に規定する原子力事業所をいう。）における安全の確保に関する基準においてサイバーセキュリティの確保につき必要な定めをし、及びその遵守を確保することその他の必要な施策を講ずるものとする。

第一条のうち第二十五条の改正規定中「加える」を『加え、同項第四号中「前三号」を「前各号」に改め、同号を同項第五号とし、同項第三号の次に次の一号を加える』に改め、同改正規定に次のように加える。

四　第十五条の二に規定する基準の策定等に関しサイバーセキュリティの確保の見地から原子力規制委員会に対し必要な助言、情報の提供その他の援助を行うこと。

第一条のうち第二十七条の改正規定中「第二十七条第三項中」の下に『「から第四号まで」を「、第三号若しくは第五号」に、』を加える。

◇

四月八日本委員会に左の案件が付託された。

一、保育の拡充等に関する請願（第一一九二号）（第一一九三号）（第一一九四号）（第一一九五号）

一、物価高騰をもたらす経済政策をやめることに関する請願（第一一九六号）（第一一九七号）（第一一九八号）（第一一九九号）

一、保育の拡充等に関する請願（第一二七一号）（第一二七二号）（第一二七三号）

一、物価高騰をもたらす経済政策をやめることに関する請願（第一二七四号）（第一二七五号）

一、プライバシー権侵害のマイナンバー制度中止に関する請願（第一二七六号）（第一二七七号）（第一二七八号）（第一二七九号）

一、マイナンバー制度の廃止に関する請願（第一三六二号）（第一三六三号）（第一三六四号）（第一三六五号）（第一三六六号）（第一三六七号）（第一三六八号）（第一三六九号）（第一三七〇号）（第一三七一号）（第一三七二号）

一、特定秘密保護法を速やかに撤廃することに関する請願（第一三七五号）（第一三七六号）（第一三七七号）（第一三七八号）（第一三七九号）（第一三八〇号）（第一三八一号）

第一一九二号　平成二十八年三月二十五日受理

保育の拡充等に関する請願

請　願　者　名古屋市　加藤つや子　外三百十七名

紹介議員　井上　哲士君

この請願の趣旨は、第五六七号と同じである。

第一一九三号　平成二十八年三月二十五日受理

保育の拡充等に関する請願

請　願　者　北海道稚内市　鎌田葉子　外三百二十八名

紹介議員　紙　智子君

この請願の趣旨は、第五六七号と同じである。

第一一九四号　平成二十八年三月二十五日受理

保育の拡充等に関する請願

請　願　者　京都市　瀬戸武之　外一名

紹介議員　田村　智子君

この請願の趣旨は、第五六七号と同じである。

第一一九五号　平成二十八年三月二十五日受理

保育の拡充等に関する請願

請　願　者　鳥取県米子市　砂口美千子　外三百二十七名

紹介議員　仁比　聡平君

この請願の趣旨は、第五六七号と同じである。

第一一九六号　平成二十八年三月二十五日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　愛知県岩倉市　佐藤加代　外三百十七名

紹介議員　井上　哲士君

この請願の趣旨は、第五七八号と同じである。

第一一九七号　平成二十八年三月二十五日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　埼玉県川口市　須田美津子　外三名

紹介議員　田村　智子君

この請願の趣旨は、第五七八号と同じである。

第一一九八号　平成二十八年三月二十五日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　北海道北斗市　神尾勝子　外三百十七名

紹介議員　紙　智子君

この請願の趣旨は、第五七八号と同じである。

第一一九九号　平成二十八年三月二十五日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　岡山県玉野市　内村加代子　外三百十七名

紹介議員　仁比　聡平君

この請願の趣旨は、第五七八号と同じである。

第一二七一号　平成二十八年三月二十九日受理

保育の拡充等に関する請願

請　願　者　新潟県長岡市　小林米子　外二十四名

紹介議員　井上　哲士君

この請願の趣旨は、第五六七号と同じである。

第一二七二号　平成二十八年三月二十九日受理

保育の拡充等に関する請願

請　願　者　群馬県太田市　森田久子　外十九名

紹介議員　紙　智子君

この請願の趣旨は、第五六七号と同じである。

第一二七三号　平成二十八年三月二十九日受理

保育の拡充等に関する請願

請　願　者　広島市　権藤延恵　外十九名

紹介議員　仁比　聡平君

この請願の趣旨は、第五六七号と同じである。

第一二七四号　平成二十八年三月二十九日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　群馬県館林市　水沼節子　外三十九名

紹介議員　紙　智子君

この請願の趣旨は、第五七八号と同じである。

第一二七五号　平成二十八年三月二十九日受理

物価高騰をもたらす経済政策をやめることに関する請願

請　願　者　広島市　権藤延恵　外三十九名

紹介議員　仁比　聡平君

この請願の趣旨は、第五七八号と同じである。

第一二七六号　平成二十八年三月二十九日受理

プライバシー権侵害のマイナンバー制度中止に関する請願

請　願　者　大阪市　吉田弘美　外八百三十九名

紹介議員　市田　忠義君

日本経済は、アベノミクスによる円安と資材高騰、消費税八％によって失速している。社会保障は切下げと負担増ばかりで、既に国民生活は限界である。多くの中小企業・零細業者は、消費税が転嫁できず赤字でも身銭を切って納税を続ける中で廃業の危機に迫られている。今必要なことは、

税率を五％に戻し景気回復につなげることである。逆に、一〇％再増税を強行すれば、日本経済は取り返しの付かない大打撃を受け、更なる財政悪化を招く。絶対にこの道は避けるべきである。酒類・外食を除く食料品を八％に据え置く軽減税率が導入されようとしている。税率一〇％が前提で、実際は軽減どころか一世帯平均で四万円の負担増である。そもそも、五％から一〇％で十四兆円もの大増税のうち一兆円分を下げるだけで、その財源は低所得者への医療・介護の負担軽減策を見送るなど、どこを取っても偽軽減である。また、二〇二一年からインボイス方式が導入されようとしている。複数税率では不正経理が起こる、インボイスにすれば益税がなくなると説明されるが、転嫁問題は何ら解決されず、大変な事務負担と徴税強化となり、中小業者の経営を悪化させるばかりである。さらに、インボイスを発行できない免税業者は、取引から排除されてしまう。共通番号、いわゆるマイナンバー制度が二〇一六年一月から実施となった。国民監視・選別化、徴税強化と福祉削減、情報漏えい・成り済まし犯罪の拡大など、日本社会に弊害と混乱を招くのは確実である。憲法第十三条が保障するプライバシー権の侵害として全国一斉訴訟まで起こっている。中小企業は番号記載と厳格な管理体制が求められ、漏えいには四年以下の懲役又は二百万円以下の罰則である。この対策に五人ほどの会社でも数十万円の費用負担がかかると言われ、正にマイナンバー増税である。国民の理解も進まず不安も拭えず、事業者も行政も対応が追い付かない中で、このような危険な共通番号制度は中止するべきである。

ついては、次の措置を採られたい。

一、プライバシー権侵害（憲法第十三条違反）のマイナンバー制度は中止すること。

第一二七七号　平成二十八年三月二十九日受理
プライバシー権侵害のマイナンバー制度中止に関する請願
請願者　堺市　井之上尚美　外八百四十二名
紹介議員　大門実紀史君
この請願の趣旨は、第一二七六号と同じである。

第一二七八号　平成二十八年三月二十九日受理
プライバシー権侵害のマイナンバー制度中止に関する請願
請願者　大阪市　野田豊子　外八百三十九名
紹介議員　辰巳孝太郎君
この請願の趣旨は、第一二七六号と同じである。

第一二七九号　平成二十八年三月二十九日受理
プライバシー権侵害のマイナンバー制度中止に関する請願
請願者　大阪市　山本浩子　外八百三十九名
紹介議員　山下　芳生君
この請願の趣旨は、第一二七六号と同じである。

第一三六二号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　三重県松阪市　民谷久美子　外三百十一名
紹介議員　井上　哲士君
この請願の趣旨は、第二六九号と同じである。

第一三六三号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　和歌山市　栗山康子　外三百十一名
紹介議員　市田　忠義君
この請願の趣旨は、第二六九号と同じである。

第一三六四号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　札幌市　須藤澄江　外三百十一名
紹介議員　紙　智子君
この請願の趣旨は、第二六九号と同じである。

第一三六五号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　東京都目黒区　小國アヤ子　外三百十一名
紹介議員　吉良よし子君
この請願の趣旨は、第二六九号と同じである。

第一三六六号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　京都市　後藤温子　外三百十一名
紹介議員　倉林　明子君
この請願の趣旨は、第二六九号と同じである。

第一三六七号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　東京都品川区　高橋さゆり　外三百十一名
紹介議員　小池　晃君
この請願の趣旨は、第二六九号と同じである。

第一三六八号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　東京都大田区　浅田光子　外三百十一名
紹介議員　田村　智子君
この請願の趣旨は、第二六九号と同じである。

第一三六九号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　和歌山市　是枝美代子　外三百十一名
紹介議員　大門実紀史君
この請願の趣旨は、第二六九号と同じである。

第一三七〇号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　大阪市　渡辺なぎさ　外三百十一名
紹介議員　辰巳孝太郎君
この請願の趣旨は、第二六九号と同じである。

第一三七一号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　愛媛県四国中央市　三宅敦子　外三百十一名
紹介議員　仁比　聡平君
この請願の趣旨は、第二六九号と同じである。

第一三七二号　平成二十八年三月三十日受理
マイナンバー制度の廃止に関する請願
請願者　大阪府大東市　香川昭子　外三百十八名
紹介議員　山下　芳生君
この請願の趣旨は、第二六九号と同じである。

第一三七五号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請願者　長野県中野市　小林裕子　外二百五名
紹介議員　井上　哲士君
この請願の趣旨は、第二七九号と同じである。

第一三七六号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請願者　仙台市　阿部真紀　外二百五名
紹介議員　紙　智子君
この請願の趣旨は、第二七九号と同じである。

第一三七七号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請願者　京都市　高橋美紀子　外二百五名
紹介議員　倉林　明子君
この請願の趣旨は、第二七九号と同じである。

第一三七八号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請　願　者　兵庫県芦屋市　岸田恵　外二百五名
紹介議員　大門実紀史君
この請願の趣旨は、第二七九号と同じである。

第一三七九号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請　願　者　堺市　山田加津美　外二百五名
紹介議員　辰巳孝太郎君
この請願の趣旨は、第二七九号と同じである。

第一三八〇号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請　願　者　山口県光市　宮本育子　外二百十二名
紹介議員　仁比　聡平君
この請願の趣旨は、第二七九号と同じである。

第一三八一号　平成二十八年三月三十一日受理
特定秘密保護法を速やかに撤廃することに関する請願
請　願　者　大阪府東大阪市　中山美喜恵　外二百五名
紹介議員　山下　芳生君
この請願の趣旨は、第二七九号と同じである。

平成二十八年四月二十六日印刷　平成二十八年四月二十七日発行　参議院事務局　印刷者　国立印刷局　P