第百九十回国会　衆議院　内閣委員会議録　第十号

平成二十八年三月三十日（水曜日）

午前九時開議

出席委員

委員長　西村　康稔君

理事　亀岡　偉民君　理事　平　将明君

理事　武井　俊輔君　理事　中根　一幸君

理事　平井たくや君　理事　緒方林太郎君

理事　柿沢　未途君　理事　後藤　祐一君

理事　佐藤　茂樹君

青山　周平君　池田　佳隆君

石﨑　徹君　岩田　和親君

大隈　和英君　岡下　昌平君

勝俣　孝明君　神谷　昇君

木内　均君　北村　茂男君

高木　宏壽君　武部　新君

中山　展宏君　長尾　敬君

ふくだ峰之君　牧島かれん君

松本　洋平君　宮崎　政久君

若狭　勝君　大串　博志君

小宮山泰子君　篠原　孝君

鈴木　義弘君　高井　崇志君

古本伸一郎君　江田　康幸君

濱村　進君　真山　祐一君

池内さおり君　島津　幸広君

河野　正美君

国務大臣　遠藤　利明君

内閣府副大臣　松本　文明君

総務副大臣　松下　新平君

外務副大臣　木原　誠二君

経済産業副大臣　鈴木　淳司君

内閣府大臣政務官　牧島かれん君

内閣府大臣政務官　酒井　庸行君

内閣府大臣政務官　高木　宏壽君

総務大臣政務官　森屋　宏君

総務大臣政務官　古賀　篤君

厚生労働大臣政務官　太田　房江君

経済産業大臣政務官　星野　剛士君

衆議院庶務部長　鹿村謙太郎君

参議院庶務部長　木下　博文君

最高裁判所事務総局情報政策課長　安東　章君

政府参考人（内閣官房内閣審議官）　谷脇　康彦君

政府参考人（消費者庁審議官）　井内　正敏君

政府参考人（総務省大臣官房審議官）　宮地　毅君

政府参考人（総務省大臣官房審議官）　猿渡　知之君

政府参考人（国税庁長官官房審議官）　柴﨑　澄哉君

政府参考人（文部科学省大臣官房審議官）　松尾　泰樹君

政府参考人（文部科学省生涯学習政策局生涯学習総括官）　岩本　健吾君

政府参考人（厚生労働省大臣官房情報政策・政策評価審議官）　安藤　英作君

政府参考人（厚生労働省大臣官房年金管理審議官）　福本　浩樹君

政府参考人（経済産業省商務情報政策局長）　安藤　久佳君

政府参考人（原子力規制庁次長）　荻野　徹君

内閣委員会専門員　室井　純子君

委員の異動

三月二十九日

辞任　岸本　周平君

補欠選任　真山　祐一君

同日

辞任　勝俣　孝明君　青山　周平君

篠原　孝君　阿部　知子君

補欠選任　勝俣　孝明君　青山　周平君

阿部　知子君　篠原　孝君

同月三十日

辞任　青山　周平君

同日

理事柿沢未途君同日理事辞任につき、その補欠として後藤祐一君が理事に当選した。

三月二十九日

特定秘密保護法の撤廃に関する請願（池内さおり君紹介）（第一〇五三号）

同（梅村さえこ君紹介）（第一〇五四号）

同（大平喜信君紹介）（第一〇五五号）

同（笠井亮君紹介）（第一〇五六号）

同（穀田恵二君紹介）（第一〇五七号）

同（清水忠史君紹介）（第一〇五八号）

同（塩川鉄也君紹介）（第一〇五九号）

同（島津幸広君紹介）（第一〇六〇号）

同（田村貴昭君紹介）（第一〇六一号）

同（高橋千鶴子君紹介）（第一〇六二号）

同（藤野保史君紹介）（第一〇六三号）

同（堀内照文君紹介）（第一〇六四号）

同（真島省三君紹介）（第一〇六五号）

同（宮本岳志君紹介）（第一〇六六号）

同（宮本徹君紹介）（第一〇六七号）

同（本村伸子君紹介）（第一〇六八号）

国の保育・教育・子育て支援施策の拡充に関する請願（中川正春君紹介）（第一一二三号）

は本委員会に付託された。

三月二十九日

伊勢志摩サミットに関わるテロ対策の強化並びに関係機関相互の協力及び連携強化を求める意見書（三重県議会）（第一五五九号）

緊急事態基本法の早期制定を求める意見書（長野県諏訪市議会）（第一五六〇号）

警察官の増員を求める意見書（岐阜県議会）（第一五六一号）

国民生活の安全・安心を支える国の行政機関等の体制・機能の充実を求める意見書（愛媛県上島町議会）（第一五六二号）

「子ども・子育て支援新制度の充実」を求める意見書（愛知県豊橋市議会）（第一五六三号）

子ども・子育て支援新制度に対する意見書（愛知県碧南市議会）（第一五六四号）

子ども・子育て支援新制度に対する意見書（愛知県弥富市議会）（第一五六五号）

子ども・子育て支援新制度に対する意見書（兵庫県加古川市議会）（第一五六六号）

子ども・子育て支援新制度に対する意見書（岡県大牟田市議会）（第一五六七号）

子ども・子育て支援新制度に対する意見書（岡県行橋市議会）（第一五六八号）

子ども・子育て支援新制度に対する意見書（岡県太宰府市議会）（第一五六九号）

子ども・子育て支援新制度に対する意見書（岡県宇美町議会）（第一五七〇号）

子ども・子育て支援新制度に対する意見書（岡県糸田町議会）（第一五七一号）

子ども・子育て支援新制度に対する意見書（岡県苅田町議会）（第一五七二号）

子どもの貧困対策の具体的推進を求める意見書（大分県臼杵市議会）（第一五七三号）

手話言語法制定を求める意見書（沖縄県浦添市議会）（第一五七四号）
「青少年健全育成基本法の制定」を求める意見書（茨城県笠間市議会）（第一五七五号）
「青少年健全育成基本法の制定」を求める意見書（茨城県潮来市議会）（第一五七六号）
「青少年健全育成基本法の制定」を求める意見書（茨城県坂東市議会）（第一五七七号）
「青少年健全育成基本法の制定」を求める意見書（茨城県阿見町議会）（第一五七八号）
「青少年健全育成基本法」の制定を求める意見書（神奈川県厚木市議会）（第一五七九号）
「青少年健全育成基本法の制定」を求める意見書（神奈川県伊勢原市議会）（第一五八〇号）
青少年健全育成基本法の制定を求める意見書（大津市議会）（第一五八一号）
「青少年健全育成基本法の制定」を求める意見書（和歌山県有田市議会）（第一五八二号）
青少年健全育成基本法の制定を求める意見書（熊本県宇土市議会）（第一五八三号）
青少年健全育成基本法の制定を求める意見書（熊本県宇城市議会）（第一五八四号）
青少年健全育成基本法の制定を求める意見書（宮崎県日南市議会）（第一五八五号）
青少年健全育成基本法の早期制定を求める意見書（鹿児島県出水市議会）（第一五八六号）
地域手当の級地区分及び支給割合の見直しを求める意見書（東京都武蔵村山市議会）（第一五八七号）
テロ対策の強化についての意見書（愛知県議会）（第一五八八号）
テロに対する国民の安全確保を求める意見書（熊本県議会）（第一五八九号）
特定教育・保育施設における利用者負担額多子世帯軽減の拡充を求める意見書（大阪府泉大津市議会）（第一五九〇号）
保育士の確保並びに保育施設整備等に関する意見書（滋賀県湖南市議会）（第一五九一号）
北海道警察の警察官の増員を求める意見書（北海道奈井江町議会）（第一五九二号）
北海道警察の警察官の増員を求める意見書（北海道上砂川町議会）（第一五九三号）
マイナンバー制度の円滑な運用についての意見書（愛知県議会）（第一五九四号）

は本委員会に参考送付された。

本日の会議に付した案件

理事の辞任及び補欠選任
政府参考人出頭要求に関する件
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（内閣提出第一一号）

◇◇◇

○西村委員長　これより会議を開きます。

理事の辞任についてお諮りいたします。

理事柿沢未途君から、理事辞任の申し出があります。これを許可するに御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○西村委員長　御異議なしと認めます。よって、そのように決しました。

引き続き、理事の補欠選任についてお諮りいたします。

ただいまの理事の辞任に伴い、現在理事が一名欠員となっております。その補欠選任を行いたいと存じますが、先例によりまして、委員長において指名するに御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○西村委員長　御異議なしと認めます。よって、そのように決しました。

それでは、理事に後藤祐一君を指名いたします。

○西村委員長　内閣提出、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。

この際、お諮りいたします。

本案審査のため、本日、政府参考人として内閣官房内閣審議官谷脇康彦君、消費者庁審議官井内正敏君、総務省大臣官房審議官宮地毅君、総務省大臣官房審議官猿渡知之君、国税庁長官官房審議官柴崎澄哉君、文部科学省大臣官房審議官松尾泰樹君、文部科学省生涯学習政策局生涯学習総括官岩本健吾君、厚生労働省大臣官房情報政策・政策評価審議官安藤英作君、厚生労働省大臣官房年金管理審議官福本浩樹君、経済産業省商務情報政策局長安藤久佳君、原子力規制庁次長荻野徹君の出席を求め、説明を聴取いたしたいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○西村委員長　御異議なしと認めます。よって、そのように決しました。

○西村委員長　次に、お諮りいたします。

本日、最高裁判所事務総局安東情報政策課長から出席説明の要求がありますので、これを承認するに御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○西村委員長　御異議なしと認めます。よって、そのように決しました。

○西村委員長　これより質疑に入ります。

質疑の申し出がありますので、順次これを許します。平井たくや君。

○平井委員　おはようございます。自由民主党の平井たくやです。

きょうは、質問をさせていただきまして、ありがとうございます。

今回、サイバーセキュリティ基本法の改正ということでございますが、皆さん、この法律は議員立法で、自公民そして維新にも協力をいただきまして提出をさせていただいて、成立の運びになったものでございます。そういう意味で、サイバーセキュリティーに関しては与党も野党もないということで、協力しながら進めていかなきゃいけないというふうに思っています。

この法律のまず位置づけなんですけれども、なぜこの議員立法が必要になったかということを少しお話しさせていただきますと、高度情報通信ネットワーク社会形成基本法、これは二〇〇〇年に成立して、そして二〇〇一年に施行されたんです。二〇〇〇年というとちょうど私が初当選した年なんですが、いわばＩＴ基本法というものです。

しかしながら、このＩＴ基本法の中の第二十二条に「安全性及び信頼性の確保」という文言が入っているんですが、その当時、振り返ってみると、今のようなサイバーに対するリスクみたいなものを想定していたわけでは全くありません。ですから、ＩＴ基本法というのがＩＴの世界の憲法だとしたら、それでは今の世の中の変化にもう対応できなくなっているということでございます。

当時は、セキュリティーだけじゃなくて、ビッグデータとかデータの利活用なんというような考え方、クラウドもありませんでした。それから、テクノロジーの進歩で、世の中は物すごく変わっているわけですよ。

一方で、個人情報の漏えいに対する懸念みたいなものもあり、データの利活用をやらなきゃいかぬということもあり、セキュリティーは両面で非常に重要だということで、個人情報保護法の改正、今行政の方のもやっていますが、セキュリティーの面とかデータ利活用とかいろいろ考えると、このＩＴ基本法を補完する新たな法律が要るというふうに思っています。

それは恐らく、国民のためにデータを利活用するということを基本的に担保するような法律がやはりないと、今、個人情報保護法というのは、データの利活用に配慮はするものの、個人情報を保護するということが法律の一番の目的になるわけです。そのこともまた、こういう話も与野党は関係ない、やはり国民のために進めていく、対決法案ではない、新たな時代に挑戦する法律としての枠組みをつくるというようなことを冒頭御提案させていただきたいなと思います。

そんなことで、まず最初に質問をさせていただくのは、今回の改正は、日本年金機構における百二十五万件の個人情報流出事案を受けての改正ということになります。そして、監視、監査、原因究明調査の範囲を特殊法人等に拡大するということです。では、今回の改正によって年金機構事案のようなインシデントが再び起きるか起きないか。起きないようにしてほしいということですが、遠藤大臣にお尋ねしたいと思います。

○遠藤国務大臣　お答えいたします。

今回の改正は、今委員御指摘のように、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づけ、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。

これによりまして、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り組みが義務づけられるとともに、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ってまいります。

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を行うことにより、十分なサイバーセキュリティー対策がと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まいります。

サイバー攻撃は質、量ともに深刻さを増しておりまして、予断を許さない厳しい状況ではあるものの、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ます。

○平井委員　では、年金機構の情報流出の事案というのはどのレベルのサイバー攻撃かというと、お恥ずかしい限りで、実際は大したことないわけですね。

つまり、対策が十分でなかったところと、そういうリスクに対するガバナンスが不十分だったこと等が見直されていくんだというふうに思います。

今、遠藤大臣の方からいろいろな対策をお話しいただきましたけれども、それでも一〇〇％とは言い切れませんから、そこがサイバーに対する非常に難しいところで、できるだけ全ての手を尽くした上で、もし何か起きたときには迅速に対応して、被害を最小化していく。つまり、そういうことが起きることが前提でいろいろな対策を今後考えていただきたいというふうに思います。

今回の改正によって監視の対象として拡大されるもののうち特殊法人や認可法人については、全部でなく、戦略本部が指定することになっています。特殊法人とか認可法人といいましても業務や持っている情報というのはさまざまなんですが、どのような基準で指定することを考えているのか、まずお聞かせ願いたいと思います。

○谷脇政府参考人　お答え申し上げます。

今回の改正法案により、国による不正な通信の監視等の対象とする特殊法人、認可法人につきましては、当該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、サイバーセキュリティ戦略本部が指定をすることといたしております。

具体的には、当該法人の業務と国の業務の一体性、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どうかといった要素を踏まえまして、サイバーセキュリティ戦略本部において決定することとしております。

なお、現時点におきましては、今お話がございました、平成二十七年五月に情報流出事案が発生いたしました日本年金機構を指定することを想定しておりますけれども、他の法人につきましては、関係省庁とも協議の上、今御説明申し上げました判断基準に照らしながら引き続き検討してまいりたいと考えております。

○平井委員　今御答弁いただいたような基準で指定法人を指定するとした場合、いつまでにどのような形で指定をしていくかということについて我々はぜひ知りたいと思いますので、お聞かせ願いたいと思います。

○谷脇政府参考人　お答え申し上げます。

今回の改正法案につきましては、一部の規定を除きまして、公布後六月を超えない範囲で政令で定める日より施行するとされているところでございます。

指定法人につきましては、改正法案の施行後できるだけ速やかに、先ほど申し上げました指定の考え方に照らしましてサイバーセキュリティ戦略本部において決定することを想定しているところでございます。

○平井委員　指定していろいろな対策をするといっても、本来それぞれの組織が自分の責任で自分をきっちり守るという前提がないと、ＮＩＳＣが幾ら頑張ったって意味がないんですね。そのようなことが、逆に言うと、指定されればそれで安心だというような勘違いにつながらないような周知徹底もお願いしたい。まず、一義的にはそれぞれの組織がやはり責任を持つということが重要だと思います。そういうようなことを前提として指定するということであれば、私もそれはそれでいいというふうに思います。

そうなると、指定されるかされないかなということでいうと、私がどうしても関心を持つのは、何といってもマイナンバーの基盤を担うＪ―ＬＩＳということになるんですね。

マイナンバー制度というのは、セキュリティーの確保が一番重要だと思います。一方で、マイナンバーというものは、世の中全体の情報管理のセキュリティーレベルを上げるんですね。

このことも実は結構誤解されているところがあって、今までアナログで管理されていた文書、デジタルで管理されていた文書は、ではどっちがセキュリティーレベルが高いかというような話。

ちょっと横に行っちゃいますけれども、そのこともぜひ皆様方に意識していただきたいのは、アナログだと、誰がいつ見たかわからないんですね。のぞかれても何してもわからない。つまり、誰が閲覧したか把握できない。閲覧者を制限することもできない。そして、データが紛失しちゃった場合、誰でも見ることが可能なんですね。持ち出しだって容易です。

一方、デジタルになると、今回のマイナンバー制度の中でもマイナポータルからできるわけですけれども、誰がデータを閲覧したか履歴が残るわけですよ。そして、アクセス管理により閲覧者が制限される。データが紛失しても、暗号化によって閲覧を制限できる。各種セキュリティー対策によって、持ち出しというようなものも制限できる。

というようなことで、実は世の中に誤解があるのは、マイナンバーを入れると情報漏えいのリスクが高まる、これは逆で、入れることによってそれは下がる。なぜなら、それぞれの情報共有機関の情報が漏れるのがリスクであって、マイナンバーはあくまでも符号でつながるだけで、なおかつ、これは限定をされているし、誰がいつ見たかもわかるし、おまけに分散管理なんですよ。

ですから、マイナンバーを導入することを奇貨として全体の情報管理のレベルを上げていくというのが基本、ベースにあるというふうに思うんですね。

そんな中で、私はかつてを思い出しました。マイナンバーというのは、我々が野党の時代から、民主党からバトンを受け取ったのがマイナンバーで、当時私は、ウオーニングを鳴らす意味で、マイナンバーというのが、Ｊ―ＬＩＳのＪ―ＬＩＳによるＪ―ＬＩＳのためのマイナンバーになっちゃいかぬぞということを再三言っておりました。

それはそうだと思います。公的個人認証そしてマイナンバーの基盤を担うＪ―ＬＩＳという組織は、非常に重要な組織になるわけですね。そのセ

キュリティーレベルを上げるということになった場合、今回、指定法人にするかしないかということがやはり非常に重要になってくると思うんです。

現時点で、Ｊ―ＬＩＳを指定法人とすべきだと私は思いますが、どのように御検討なさっているか、お聞かせ願いたいと思います。

○谷脇政府参考人　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され、かつ、その設立に当たって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いたします。

このＪ―ＬＩＳを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、当該法人それか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考えております。

○平井委員　いや、これはすべきだと思います。

しかし、私から見ると、Ｊ―ＬＩＳは、指定するしない以前のレベルでいろいろな問題を起こしているというふうに思うんですね。

Ｊ―ＬＩＳが運用するマイナンバーカードを交付するシステムについて、これまで機能停止に至る障害が七回発生しているんですよ。また、類似のシステム障害が発生して、カードの交付に大きな支障が生じています。これは、本当にマイナンバー制度の根幹を揺るがすような問題なんですね。

このＪ―ＬＩＳに対するガバナンスを総務省はどう考えているかという問題もあるんですが、オール・ジャパンのベンダーに発注をしてこのていたらくは、あり得ないんですよ。あり得ない。これはＪ―ＬＩＳの責任だと言って逃げられる話じゃないです。総務省として今一番やらなきゃいけないのは、このＪ―ＬＩＳで起きているいろいろな事案に対しての適切な対応と、説明責任を果たしていくということであります。

そういう意味で、Ｊ―ＬＩＳがしっかりとシステムを運用できることが前提で指定法人じゃないと、つまり、システムというのは構築、運用、セキュリティーが一体なんですよ。今、その運用の段階でこれだけつまずいているというのは、セキュリティー以前の問題だ。

そのあたりのところで、どのような認識で、これからどのように対応していくのか、総務省にお聞きしたいと思います。

○松下副大臣　平井たくや筆頭理事におかれましては、マイナンバー制度全般にわたって、党派を超えてこれまで早くからまとめ役としてお取り組みをいただいておりまして、まさに伝道師としての役割に敬意を表したいと思います。

御指摘いただきました、Ｊ―ＬＩＳのカード管理システムの一時不安定な状態により、多くの市区町村においてマイナンバーカードの交付等の業務が行えなくなった事案が複数回発生いたしました。

ただいま原因の詳細につきましてはＪ―ＬＩＳにおいて調査中ですけれども、当面の対応といたしまして、住民の方に御迷惑をおかけすることのないように、まず、カード管理システムの中継サーバーを増設するとともに、何かあったときの対応を即座にするということで、影響の最小化に努めております。

また、これまでのシステムのふぐあいに関する調査結果を踏まえまして、カード管理システムのサーバーについて改修を実施し、その後の稼働状況について慎重に監視しているところでございます。

総務省といたしましても、市区町村がこの年度末そして年度初めの繁忙期を迎えることを踏まえて、高市大臣からＪ―ＬＩＳに対して、ふぐあいの早急な原因究明と再発防止に取り組むよう改めて要請を行いました。

理事から御指摘いただきましたとおり、総務省として、このＪ―ＬＩＳ、市区町村そして関係事業者と密接に連携をとりながら、心配されないように取り組んでまいりたいというふうに思います。

以上です。

○平井委員　私から見ると、まだまだ危機感が全く足りないと思いますよ。理由がわからないで、ふぐあいが起きる状態のままなんですね。だから、これはやはり政務が主導して徹底的にやらないと、後で大きく後悔すると思います。

その意味で、要するにガバナンスをどのようにきかせていくかというようなことも含めて総務省でさらに御検討いただかないと、今まで頑張ってきたことが全部水の泡になりかねない状態だと思います。

私の周りにも、カードを申請したのに来ないと文句を言う人がたくさんふえてきちゃった。本来だったら、年度末までに一千万枚は国民の手元になきゃおかしい話なんですよ。申請したけれども届かないという状態は、我々は全く看過できるものではありません。

ですから、総務省挙げてこれはきっちりやってもらわないと、与党も野党もなく進めてきたマイナンバーというものがシステムのふぐあいによってリスクにさらされる事態は、私はもう耐えられないです。そのことを松下副大臣はぜひ先頭に立って頑張っていただくことをお願いしたいというふうに思います。

そして同時に、地方公共団体は、国が持っているいろいろな情報を持っているんですね、自治体が。階層の深いいろいろな住民のデータを持っているのは自治体なんです。

結局、リスクはどこにあるかというと、情報管理の甘いところにリスクはやはり大きくなってしまうということを考えると、現行法も、地方自治の本旨ということもあり、これをつくるときにも我々はちょっと迷ったところでございます。地方公共団体との協力規定は書きましたけれども、地方公共団体のセキュリティー対策というようなことに関して、今までなかなか国がいろいろできるものではなかったんですね、地方自治は地方自治ですから。

そういう中で、ＮＩＳＣとしてはこの地方公共団体のセキュリティーに対してどのように考えているのかということをお聞きしたいと思います。

○谷脇政府参考人　お答え申し上げます。

地方公共団体につきましても、その行う業務は国民生活と密接な関係を有するものであり、サイバーセキュリティー対策を充実させる必要が当然のことながらございます。

他方、委員も御指摘のとおり、地方自治の本旨を踏まえ、国による関与については一定の配慮が必要と考えられるところでございます。

このため、地方自治体の提供する行政サービスにつきましても、いわゆる重要インフラの一分野と位置づけ、所要の対策について国として支援をしているところでございます。

また、基本法の規定に基づきまして、サイバーセキュリティ戦略本部は、地方公共団体の長に対しまして、資料の提出、意見の開陳、説明その他必要な協力を求めることができるとされております。

したがいまして、戦略本部の本部長である内閣官房長官は、提出された資料等を踏まえ、必要があると認めるときは、関係行政機関の長に対し勧告をすることができるところでございます。

委員が御議論になっておられますように、マイナンバー制度の本格稼働を踏まえまして、地方自治体のセキュリティー対策の強化は極めて重要でございますので、総務省を初め関係府省と連携しながら対策を進め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。

○平井委員　そうです。地方自治体のセキュリティーということに関して、平成二十七年度の補正予算で二百五十五億円を計上しました。

これは、やはり何とかこういう予算を確保すべきだということで我々も応援させていただいたんですけれども、その二百五十五億円を計上して、具体的にどのように地方公共団体のセキュリティー対策に取り組んでいるのか、まずそれをお聞きしたいと思います。

○猿渡政府参考人　お答え申し上げます。

地方自治体の情報セキュリティー対策の抜本的な強化につきましては、ＮＩＳＣ等の支援をいただきながら、昨年十一月二十四日に取りまとめられました自治体情報セキュリティ対策検討チームの報告を踏まえまして、次の三層から成る対策を全ての自治体にお願いしております。

一つ目は、既存住基、税、社会保障などのマイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより個人情報の流出を徹底して防ぐこと。

二つ目は、マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティーを確保するため、財務会計などＬＧＷＡＮを活用する業務用のシステムと、ウエブ閲覧やインターネットメールなどのインターネット用のシステムとの通信経路を一旦分けた上で、両システム間で通信する場合には、ウイルス感染のない無害化通信を図ること。

三つ目には、インターネット接続系におきましては、都道府県と市区町村が協力して、まずは都道府県単位でインターネット接続口を集約した上で自治体情報セキュリティクラウドを構築し、高度なセキュリティー対策を講じることでございます。

これらの対策のために必要な経費につきまして、平成二十七年度補正予算に二分の一の補助として二百五十五億円を計上していただいたところでありますけれども、残りの地方負担分につきましても、補正予算債で一〇〇％対応するなどにより支援をしているところでございます。

去る三月八日には、各自治体で補正予算を計上された上で交付申請をされました千六百七十一市区町村及び四十五道府県に対しまして約二百三十六億円の補助金の交付決定を行うとともに、対応する補正予算債の手続も終えたところであります。

なお、今回申請のなかった団体につきましては、来年度早々申請するものと伺っております。

また、補助金につきましては、各自治体のセキュリティー対策の実施実績を確認の上交付することになりますけれども、それまでの間も各自治体において円滑に情報セキュリティー対策が実施されていくよう、それぞれの自治体と緊密に連携を図りながら進めてまいりたいと存じます。

○平井委員　随分立派な御答弁ではございますが、これは実行が伴うかというと、甚だ疑問符がつくんですね。

こういう予算の執行は物すごく難しいです。それぞれの自治体はそれぞれ違う事情がある、また人材に関してもいろいろある、ベンダーも違う、予算の重点、優先順位も違う中で、やれと言って、金をつけるからと言って簡単にできると思ったら大間違いなんです。何かまだ、私から見ると、事を随分甘く見ているように思います。

ですから、全体の工程表とか、要するにどのような進みぐあいをしているかをやはり報告していただく必要が今後あろうかと思います。予算を用意したのにやらなかったからおまえらが悪いというような話で逃げられたのでは困るんです。

どうですか、審議官、そのあたりについての御決意は。

○猿渡政府参考人　今お話しいただきましたように、補助金の交付で、最終的に実績を確認するまでの間においても、適切に工程表等を作成して継続的にフォローしながら、自治体の意見をさまざまにお伺いしながら、また御報告してまいりたいと思います。

○平井委員　楽しみにしておりますが、いろいろな自治体から大きな反発もあるやり方であるということも十分御配慮いただいた上で、総務省としては、これは一丁目一番地なので、省挙げてお取り組みいただくようにお願いをしたいと思います。

それでは、セキュリティーの法案の方に戻ります。

リスクがますます深刻化して複雑化する中で、重大なインシデントの発生に伴う緊急事態に備えて政府は周到な準備をする必要があるんですが、どのような場合に重大なインシデント、今回、年金機構の問題が特定重大事象になったと思いますが、ほかにはあったのか。まあなかったのではないかと思うんですが。今後、この特定重大事象というようなものにどのような対応がとられることになるのか、そこを説明いただければと思います。

○谷脇政府参考人　お答え申し上げます。

どのようなインシデントがいわゆる特定重大事象に当たるかにつきましては、平成二十七年の二月にサイバーセキュリティ戦略本部で決定をいたしました、サイバーセキュリティ戦略本部重大事象施策評価規則において規定をしております。

戦略本部長である官房長官がこの要件に該当すると判断した場合には、サイバーセキュリティ基本法に定める原因究明調査の対象になるわけでございます。

具体的には、国の行政機関で発生したサイバーセキュリティーに関する事象のうち、行政事務の遂行に著しい支障を及ぼし、または及ぼすおそれのあるもの、国民生活または社会経済に重大な影響を与え、または与えるおそれがあるもの、または、我が国のサイバーセキュリティーに対する国内外の信用を著しく失墜させ、または失墜させるおそれがある事象、これらを想定しているところでございます。

年金機構事案につきましては、この規則にのっとりまして、平成二十七年五月二十九日に、ＮＩＳＣからの報告を踏まえ戦略本部長が特定重大事象に当たると判断し、同年六月一日、原因究明調査を開始したところでございます。

他方、インシデントが特定重大事象に該当しない場合であっても、インシデント発生時には、情報セキュリティ緊急支援チーム、いわゆるＣＹＭＡＴの派遣等により迅速な対応が可能になっているところでございます。

今後、こうした支援体制の強化に取り組むとともに、各省庁や独立行政法人、指定法人におきまして、ＣＹＭＡＴ派遣等による支援や助言の受け入れを迅速かつ適切に行い、ＮＩＳＣと協力して適切にインシデント対応に当たるよう、私どもとしても積極的に働きかけてまいりたいと考えております。

○平井委員　サイバーセキュリティーを確保するということは、情報システムを所管する各省庁がまず自主的に責任を持って取り組むことが基本であるということは言うまでもないんですが、しかし、それでも、小さな省庁においてはそれを行う必要な人材も予算も不足しているという実態もあります。

それぞれの組織においてＣＩＳＯを初めとする体制整備を図るためには人材、予算面の充実が必要だと考えるんですが、遠藤大臣、いかがでしょうか。

○遠藤国務大臣　サイバーセキュリティーに関する予算につきましては、政府全体として、平成二十七年度補正予算で五百十四億円を確保していただき、また平成二十八年当初予算で四百九十九億円を計上しております。

引き続き、政府として、最適な予算や人員の確保など、サイバーセキュリティー対策の強化を図ってまいります。

また、政府における人材育成については、各省庁に置かれているＣＩＳＯが実効ある働きができるよう、その補佐役となる審議官等の新設を行うこととしており、今年度中に策定予定のサイバーセキュリティ人材育成総合強化方針のもとで、新設審議官等を中心に政府一体となって取り組みを進めてまいりたいと思っております。

なお一層、平井先生ほか皆様方の御支援をお願い申し上げる次第であります。

○平井委員　今回の改正によりサイバーセキュリティ戦略本部の事務が拡大されることに伴って独立行政法人情報処理推進機構、ＩＰＡ等に委託することが可能になったということでございます

が、行革の議論もある中で、ＩＰＡがまた焼け太りするんじゃないかというふうな指摘があってもおかしくないと思います。

どうしてＩＰＡが受託者として適切なのかをまず明らかにしてほしいのと、ＩＰＡ等という、この等にほかの想定されるものがあるのかどうなのか、その点についてまずお聞かせ願いたいと思います。

○谷脇政府参考人　お答え申し上げます。

サイバーセキュリティ戦略本部の事務を委託する法人につきましては、十分な技術的能力及び専門的な知見を有するとともに、当該事務を確実に実施することができるものであることが必要でございます。

ＩＰＡは、サイバー攻撃に関する情報の収集、分析や、サイバー攻撃を受けた組織における不審な通信等の分析を行うとともに、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などを行っており、これらの要件に適合すると認められるところでございます。

また、ＩＰＡは、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ものと認識をしております。

なお、法律上は、ＩＰＡその他政令で定める法人に委託することができるとしておりまして、ＩＰＡのほかに能力がある法人がある場合、その法人に委託する余地そのものは否定されていないところでございます。

他方、純粋な民間企業につきましては、その業務運営や継続性につきましての国の関与など、継続的、安定的に国の事務を行う担保がなされていないことから、現時点におきましては、ＩＰＡに委託することが最も適切である、他の選択肢というものは持ち合わせていないという認識でございます。

○平井委員　もう時間もなくなってきたので、これからちょっとＩＰＡの話をするんです。

遠藤大臣には、オリンピックも担当なさっていて大変だと思うんです、これはまた別の機会に質問をさせていただくということで。

きょうはせっかく経産省の方から来ていただいていますので、今回、ＩＰＡにスポットライトが当たっちゃうんですね。サイバーセキュリティ戦略本部の事務の一部を受託して、サイバーセキュリティー確保上極めて重要な業務を担うことになる。

ＩＰＡというのは、中が一体どうなっているのかというのを私は最近余り知らないんですね。本当に十分な能力があるのかどうなのか。受託した仕事をきっちりやるためのＩＰＡの体制の強化が絶対必要だというふうに思うんですが、人員の増加等は行革の観点から抑制するという努力も求められる中でどのように対応していくのか、お聞かせ願いたいと思います。

○鈴木副大臣　ＩＰＡは、サイバーセキュリティー対策に関して、これまで、暗号の安全性確認、ＩＴ製品のセキュリティー評価及び認証、ウイルスやサイバー攻撃の分析、情報提供及び被害実態調査など幅広い取り組みを行ってきた実績がありまして、サイバーセキュリティ戦略本部の委託業務の実施に必要な能力を十分に有しているというふうに思っているところであります。

当該業務の実施に当たりましては、既存の人員の配置転換などを含め、可能な限り人員の増加を抑制していく所存でありますが、サイバーセキュリティー対策業務を確実に実行、実施するためには、現時点での想定では、今後、五十名程度の体制強化が必要となる見込みでございます。

○平井委員　ＩＰＡには、人材の確保そして教育等、これからきっちりと頑張っていただかなきゃいかぬというふうに思います。

それと、経産省も来ていただいていますので、ＩＰＡと並んで、先ほど理事会の懇談の中での雑談で出ましたけれども、ＣＳＳＣ、技術研究組合制御システムセキュリティセンターというものがあるんですね。その視察に行かれたかどうかわかりませんけれども、これは、重要インフラの防御対策の拡充に向けて非常に重要な施設だと私は思うんですよ。

さらに、エストニアの方もあそこに視察に行ったりいろいろしているんですが、海外と連携して、よりハイレベルな技術開発に取り組むべきだと思うし、それはそのままオリンピックまた重要インフラを守るというようなことに生かされていくと思うんです。

経産省として、多賀城にあるＣＳＳＣに関してどのようにこれから取り組んでいかれるのか、そのことについてお聞かせ願いたいと思います。

○鈴木副大臣　御指摘のＣＳＳＣは、重要インフラの制御系システムに特化した研究開発機関として非常に高い専門性を持ち、米軍のサイバー部隊でありますサイバーコマンドや、あるいは欧州の経済界のトップの来訪を受けるなど、世界各国から注目を受けております。

経済産業省としましては、ＣＳＳＣを今後の重要インフラのサイバーセキュリティー対策のハブとして機能強化していく所存でございます。

一方、ＣＳＳＣは、制御系の機器メーカーやシステムベンダーが主体でございまして、重要インフラ事業者等のユーザーの参加が少ないため、ユーザー側の課題というものを踏まえた研究開発とはならず、実装につながりにくいという課題があるのが現状でございます。このため、ＣＳＳＣへのユーザーの参加を急速に拡大して対策のサイクルを回していくことが必要となります。

加えて、米軍やイスラエル等、国内外の一流の研究機関との人材交流を通じて実践力のある高度な人材を育成して、研究の質を高めてまいりたいと思います。

このような重要インフラのサイバーセキュリティー対策を進めるためのより統合的な枠組みづくりに向け、体制を具現化、具体化して、産業界におきましてサイバーセキュリティー対策が自律的、継続的に進むようなエコシステムを構築してまいりたいと思います。

○平井委員　ＣＳＳＣは復興予算でつくったものなんですが、これが宝の持ち腐れにならないように、ちゃんと責任を持って今後のことを考えていただきたいと思います。

あと、情報処理安全確保支援士という名称を今回つくりますが、これはいかにもセンスがないというか、ＮＩＳＣさんが攻殻機動隊をＰＲに使って、あれはセンスがいいなと思ったんですけれども、情報処理安全確保支援士、これは若い人がなりたいと思わないですよ。覚えにくい。

例えば、米国ではＣＩＳＳＰ、サーティファイド・インフォメーション・システム・セキュリティー・プロフェッショナル、これは日本でも千人以上の方が資格を取っていますから、何か取りたいなというふうに思いますし、国際的に通用する名前として我々もすぐ言葉にできるんです。

これはちょっと、幾ら何でもセンスが悪過ぎると思うので、何か、若い人たちがそれを目指したいというような、例えばレジスタード・インフォメーション・セキュリティー・スペシャリスト、ＲＩＳＳですか。実は、このことに関して、名前も大事なんですよ。

センスの悪さを何とかしてくれというのが私のお願いでございますが、経産省、どうですか。

○鈴木副大臣　センスの御指摘をいただきました。

御指摘のとおり、法律の規定上では情報処理安全確保支援士というものが正式名称でございます。

なお、情報処理安全確保支援士は、国家資格として登録した資格者の信頼性を担保するため、法律上の名称独占規定を設けているところであります。

他方、委員御指摘のとおり、よりわかりやすい呼称、通称を検討し、より多くの方々に利用していただく制度としていくことが重要であると考えておりまして、議員御提案の名称、ＲＩＳＳですか、これも有力な候補として今後検討してまいりたいと存じます。

○平井委員　オリンピックもある、サイバーセ

キュリティー対策の予算はこれからどんどんふえるということですが、一方でシーリングの枠もかかってしまっていて、要するに、補正予算でいろいろなものを実装して、あとの予算はかき集めるというようなのが実態です。

ここで遠藤大臣にお願いしたいのは、サイバーセキュリティーというのは物すごく優先順位の高い政策テーマであって、予算も必要なので、その予算獲得に向けて、今までとは違う考え方で特にオリンピックに向けて頑張っていただきたいという要望をお伝えして、私の質問を終わりたいと思います。

ありがとうございました。

○西村委員長　次に、濱村進君。

○濱村委員　公明党の濱村進でございます。

本日は、サイバーセキュリティ基本法改正ということで御質問させていただきます。

まず冒頭に、遠藤大臣にぜひ御質問させていただきたいというふうに思います。何かと申し上げますと、サイバーテロの関連でございます。

大臣はオリンピック・パラリンピックも担当されておられる、その中でこうしたＩＴについても、なぜなのかというと、やはりサイバーテロにしっかりと対処していく、そういう使命を担われておられるんだというふうに思っております。

二〇二〇年に向けてしっかりと体制整備をしていく、準備を行っていくということでございますが、このサイバーテロ、二〇二〇年にいきなりどんとやるというわけではなくて、実は、二〇一九年ラグビーワールドカップ日本大会におきまして試行的にまずはやりましょうというような話になっておるというふうに聞いております。

過去の話でいえば、ロンドン・オリンピックであれば、一億六千五百万回セキュリティー関連のイベントがあって、その中でテクノロジーオペレーションセンターに上げられた件数は九十七件、大分絞られるんですけれども、ＣＩＯにさらに上がっていく、エスカレーションされたというのは六件のインシデントがあったというふうに聞いております。

ですので、非常に膨大な数のイベントが発生するということでありますが、当然、一九年も同様のことが想定されるわけでございます。ぜひラグビーワールドカップに向けて対策をまとめなければいけないというふうに思います。

二〇一五年のイングランド大会での対策についてもヒアリングを行われたりとか、あるいはリオのオリンピック・パラリンピックについても同様に、どのような体制をとられているのか、こうしたことについてもヒアリングを行って万全の体制をとる必要があるかと思いますけれども、政府としてのお考えを確認させてください。

○遠藤国務大臣　お答えいたします。

ラグビーワールドカップ二〇一九、また二〇二〇年の東京オリンピック・パラリンピック、大会の成功の条件はいろいろありますが、とりわけ安心、安全な運営が大事だと思っております。そうした中で、現下の厳しいテロ情勢に鑑みて、その中のとりわけサイバーセキュリティーの確保は、大会成功の条件として極めて重要だと認識をしております。

このため、安倍総理大臣を本部長とする東京オリンピック競技大会・東京パラリンピック競技大会推進本部において、オリンピック・パラリンピックに加え、ラグビーワールドカップ二〇一九に関係する施策についても連携して今準備を進めることとしております。

このため、安倍本部長のもとで設置をされましたサイバーセキュリティワーキングチームにおいて、関係組織の的確な情報共有を担うオリンピック・パラリンピックＣＳＩＲＴの体制等のあり方について議論を進めておりまして、二〇一九年のラグビーワールドカップ開催時の稼働を目指しております。

さらに、これらの取り組みに資するよう、オリンピック・パラリンピック・ロンドン大会及びラグビーワールドカップ・イングランド大会の教訓について、ヒアリング等を通じて情報収集を実施しており、オリンピック・パラリンピック・リオデジャネイロ大会の準備状況についても、現地に担当者を派遣して、現在、情報収集を実施中であります。

今後とも、今委員から御指摘がありましたように、関係機関が互いに緊密に連携をし、政府全体が一体となってサイバーセキュリティー対策に万全を期し、大会の成功に向けて努力してまいりたいと思っております。

○濱村委員　ラグビーに対する熱い思いは誰よりも強い遠藤大臣でおありだと思います。国会ラグビークラブの一員として一緒にイングランド大会に、国会議員同士の試合が実はワールドカップのときには行われるわけですが、昨年は残念ながら行けませんでした。なので、次はホスト国として迎えるわけですので、しっかりと万全の体制をとってまいりたいという意味では、私もしっかり汗をかいてまいりたいというふうに思っております。

公明党にはサイバーセキュリティ戦略委員会というものがございまして、私、事務局長をやっておりますが、先日、月曜日、ＮＩＣＴとＩＰＡの視察をさせていただきました。その中で、ＮＩＣＴでは、攻撃にどうやって対処するのか、無差別型の攻撃であるとか標的型の攻撃であるとかさまざまな攻撃があって、それに対して、ｎｉｃｔｅｒであったりとかＤＡＥＤＡＬＵＳとか、あるいはＮＩＲＶＡＮＡ改とか、そういった、研究をベースとしながらもサイバー攻撃に対して検知できるような状況をつくっているというわけでありました。

基本的に、今回の法律でＩＰＡが第二ＧＳＯＣという形で監査、監視、原因究明調査ができるようになるというわけでございます。そもそもこの法案は、ＧＳＯＣで検知することを独法や特殊法人、認可法人に拡大するということでございます。それ自体非常に大事だなというふうに思うわけですが、全部が全部ＮＩＳＣが見られるわけではありません。ですので、ＩＰＡに委託していくというのは非常に現実的な解決策であるというふうに思っております。

いずれにしても、本来であれば各法人が自分の責任の中でもってしっかりと対策を行うというのが筋なんだろうと思っております。ですが、ＮＩＳＣがしっかりと前面に立つ、あるいはＩＰＡが第二ＧＳＯＣとして検知をしていく、こうした体制というのは、今の移行段階では非常に現実的なのだなというふうに思っております。

その上で、今後のことを考えたとしても、各法人が個別でしっかりと対策を行っていけるように練度が上がっていくというような形になっていったとしても、初動としての被害拡大の防止ぐらいしかできなくて、原因究明のところについてはなかなか自前ではやり切れないんじゃないかしらというふうには思っております。

ＮＩＳＣについてはこの業務を将来的に担っていくのかどうかわかりませんけれども、サイバーテロの対象、実はサイバーテロという言葉の定義は何なんだろう、サイバー攻撃とサイバーテロというのは何が違うんだろうというふうに思って、一応、警視庁のホームページにはこのように書いてあるんです。「サイバーテロとは、重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの」云々、いろいろあるんですが、そういうふうに言われている。重要インフラなんですね。重要インフラをどうやって守っていくかということを考えなければなりません。

では、今どういうことをやっているのかというと、私、これも以前取り上げたことがありますけれども、セプターカウンシルというものを形成しています。これは、ＮＩＳＣが事務局的にやりながら、いろいろな重要インフラの機関、企業も含めて情報共有できる体制をつくっていますよということなんですが、非常に現実的な取り組みで、いい取り組みだなと私は思っております。

検知した不正を独法に提供しました、そうした

ら、独法は独法で大概どちらかのＳＩｅｒにシステム委託をしているので、そういうところが調査をして原因究明に当たらなければいけないということになるかと思います。

それはそもそも、今ＳＩｅｒに業務委託していますよというような話の中でいえば、委託契約の範囲内に入っているのかどうか、あるいは確実に入っているような状況を環境としてつくっていかなければいけないと思うんですけれども、御所見をお伺いできればと思います。

○谷脇政府参考人　お答え申し上げます。

例えば、日本年金機構の事案でございますけれども、この際には、情報システムを運用しているベンダーとの契約はございましたけれども、事案が発生した後のインシデント対応、あるいは原因究明についての契約関係が必ずしも明確ではなかったといったようなこともあったわけでございます。

そういった意味では、委員御指摘のとおり、事案が発生した場合、ＳＩｅｒ等との間でどのようなインシデントハンドリングを行うのか、あるいはどのように指示をするのか、こういった契約を明確に各府省それから独立行政法人においても定めをしていくことは極めて重要なことだというふうに考えております。

○濱村委員　そうなんです。年金機構の事案でも、ＳＩベンダーとの契約においては曖昧さがあった。これをどこまで委託範囲にしていくのかということはしっかりと明確にしていかないと、お互い不幸なことになってくるかと思います。

もう一つ、さらに確認していきたいんですが、ＩＰＡでは、重要インフラ事業者、経産省所管の七分野でしたか、七業種七十二組織について情報共有する仕組みがあるというふうに聞いております。このＩＰＡを中心にやっている情報共有の取り組みについては、実はＮＤＡ、秘密保持契約を結んでいるんですね。この秘密保持契約があるがゆえに外部には漏らしませんという状況がしっかりとできているわけですけれども、ＮＩＳＣ中心のセプターカウンシルではＮＤＡを結んでいるのかどうか、確認したいです。

○谷脇政府参考人　お答え申し上げます。

ＮＩＳＣが事務局を務めますセプターカウンシルにおきましては、標的型攻撃メールに関する情報共有体制を構築しているところでございます。

この情報共有体制におきましては、事務局に情報提供がございました標的型攻撃メールにつきまして、情報セキュリティー関係機関と連携して解析を行いまして、その解析結果を一定の匿名化措置を講じた上で重要インフラ事業者等に周知することによりまして、同様の攻撃の未然防止等を図っているものでございます。

本情報共有体制への参加に当たりましては、個別のＮＤＡ締結ではございませんけれども、運用規程に合意し遵守することを求めているところでございます。

○濱村委員　運用規程をしっかり定めていて、それを遵守するということでありました。

そういう形で、外部に漏らしてしまうと非常にまずい情報もあるかと思うんです。そういう中で、こういう標的型攻撃がありましたよということを横横で共有していくのは非常に大事な話でありますし、このセプターカウンシルの取り組みをさらに充実した形に持っていっていただきたいという思いで確認をさせていただきました。

国内での情報共有の体制というのは整備をされてこられているというふうに思うわけですが、海外との連携、情報共有についてはどのようになっているのかはＮＩＳＣさんに、もう一個、あわせて、脆弱性情報の公開については、ソフトウエア開発者が海外の場合に、公表に関しては個別に協議を行うということで認識しておりますが、確認をできますでしょうか。

○谷脇政府参考人　前段の部分についてＮＩＳＣの方からお答え申し上げます。

サイバー攻撃は、容易に国境を越えて行われる可能性がございます。サイバー空間における脅威のグローバル化が進んでいる中、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的確に対応するためには、やはり諸外国等とも効果的に連携することが必要だと考えております。

現在、二国間や多国間での協議、対話や国際会議、またＣＳＩＲＴ間協力等を通じまして情報交換を積極的に行い、関係各国間で連携を進めているところでございます。

○安藤（久）政府参考人　後段の部分についてお答え申し上げます。

ＩＰＡのソフトウエア脆弱性情報の公表についての海外との関係でございますけれども、ＩＰＡが脆弱性情報を受け付けまして、海外の場合には、一般社団法人ＪＰＣＥＲＴコーディネーションセンターに連絡をいたしまして、こちらがソフトウエアの開発者と協議を行う、こういうことでやらせていただいております。ＩＰＡは、その調整状況を受けまして、公表判定委員会で審議をした上で脆弱性情報を公表しております。

今先生御指摘のとおり、海外に存在する場合であっても、基本的には、同様に個別に協議を行うということでございます。

これまで、全体で千件の公表の中で、海外の開発事業者の案件は約三百件ということでございます。しかしながら、なかなか連絡がとれないケースもございます。最大限のネットワークを活用いたしまして協議をしっかりと行ってまいりたい、このように考えております。

○濱村委員　質問としてさらにお伺いしたかったのは、多国間、二国間のサイバー外交とか、あるいはサイバー対話について現状のお取り組みをちょっとお伺いしたかったんですが、時間の都合上、きょうは割愛いたします。

次のテーマに行きます。

先ほど平井先生からもありました情報処理安全確保支援士。

非常に名前がよろしくないということで、ぜひ平井先生御提案の名称に変えていただきたいなというようなことも思ったりするわけですが、この情報処理安全確保支援士は、本当に言いにくいなと思いますが、新たな制度になります。

ＩＰＡが実施する情報処理技術者試験は、どちらかというと実践的ではないんですね。記述式で、論述とかはあったりするんですけれども、サイバーセキュリティーの対策というのは、実際の方法論がわからないと手が動かせないというふうに思うわけでございます。

知識を試すだけではない、実技を踏まえたような試験にする必要性についてはどのようにお考えなのか、確認させてください。

○安藤（久）政府参考人　実技が大変重要な点については、先生御指摘のとおりでございます。

現状の情報処理技術者試験では、実際のサイバー攻撃事例に基づいた出題を行わせていただいております。実技では必ずしもございませんけれども、実務に即した内容を最大限入れさせていただいていると思っております。

加えまして、今後の情報処理安全確保支援士制度におきましては、サイバーセキュリティー対策の実務経験を有し実践的な能力があると認められる者については、資格の更新に必要な講習を一部免除するなどの措置を検討しております。

こうした評価を通じまして、実践的な能力を持つ方ほど結果として安定的に資格の更新が行いやすい、こういうような制度設計で進めてまいりたいと思っております。

○濱村委員　これは更新の部分にも非常に工夫を入れていこうと。要は、この支援士になったときには、更新制をとります、そのときには実務的なレベルをチェックしていこうという話でございますが、実は、実務でちゃんとセキュリティーに携わっているかというと、結構限られてくるかと思います。

実は、セキュリティービジネスというのはまだまだ大きな市場になってはおらなくて、しっかりとビジネス環境として広げていく、そして裾野を広げて人材を育成していけるような環境を民間の中でもしっかりとつくっていかなければいけない

んじゃないだろうかというふうに思います。
ですが、どこからどうやったらいいのかということを考えると、なかなか難しいんです。セキュリティー対策を企業として余りやりたくない。ですが、やらなきゃいけない状況なんです。
なので、サイバーセキュリティーへの投資をやればやるほど企業は何か恩恵が受けられるとか、そういった助成をするとか、そういうことも含めて考えていかないと、なかなかサイバーセキュリティービジネスの裾野が広がらないと思っております。
このビジネス環境を広げるための施策についてどのようにお考えなのか、確認したいです。

○星野大臣政務官　お答えさせていただきます。
企業のサイバーセキュリティーに対する投資を促し、関連ビジネスを振興することは、我が国のサイバーセキュリティー対策を着実に実施していく上で極めて重要な課題であると認識をしております。
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、企業の経営者が攻撃リスクと対策の必要性について認識を持つことが極めて重要だと思っております。
このため、来年度、重要インフラ事業者の制御システムを中心に、高度なサイバー攻撃に対する防御力を確認するためのテストをＩＰＡが中心となって実施することとしておりまして、これにより経営者の認識をまず高めてまいりたいというふうに考えております。
さらに、対策の実施が市場から評価される仕組みなどにより、対策への投資に対するインセンティブを高めていくことも必要だと考えております。例えば、企業の対策の度合いに応じてサイバーセキュリティーの保険料を割り引く仕組みの普及などを進めてまいりたい、これがインセンティブに大きくなってくるかなというふうに思っております。
御指摘の点は大変重要だと考えておりまして、さまざまな制度を通じてセキュリティービジネスの振興を促進してまいりたいと思っております。極めて重要な点でございます。
ありがとうございます。

○濱村委員　時間が来たので終わりますが、私はＩＰＡのＩＴストラテジストという資格を一応持っております。なかなかそれを持っている国会議員はいないんじゃないかと思いますが、そういう見地から見ても、まだまだこの分野は発展途上というか移行段階だと思っております。さらなる予算づけ等々をぜひお願い申し上げて、質問を終わります。
ありがとうございました。

○西村委員長　次に、高井崇志君。

○高井委員　岡山から参りました民進党の高井でございます。
民進党としては初めての質問になりますが、どうぞよろしくお願いをいたします。
先ほど平井先生が大変鋭い厳しい質問をされて、かなり重なっておりまして、全く同感だなと思いながら聞かせていただきました。ちょっと重なる部分も多々あると思いますけれども、御了解いただきたいと思います。
私は、最初に、遠藤大臣がなぜセキュリティー担当をされているのかなと。先ほど濱村委員からも東京オリンピック・パラリンピックとの関連、これは非常に重要な関連でうなずけるところもあるんですが、ただ、過去を見ると大体ＩＴ担当大臣が、去年も山口大臣が兼務をされておりました。私は、遠藤大臣はＩＣＴに大変造詣が深くて、教育の情報か何かを一生懸命ずっと先頭に立ってやっていただいていたので、まさにＩＣＴも、今は島尻大臣なんですけれども、遠藤大臣がやっていただいた方がよかったんじゃないかなと。
これは、本当に、ＩＣＴとセキュリティーの担当が分かれているというのは、ちょっと不都合な面もあるんじゃないか。例えば、今回セキュリティーの審議官が新設されますけれども、あれはセキュリティーとＩＣＴの、つまりＣＩＯとＣＩＳＯの補佐官が審議官であります。ところが、その上司の大臣になると別々に分かれるというのはちょっといかがなものかなと思います。ただ、これは遠藤大臣にお聞きしても、任命したのは総理でしょうから、ちょっと聞いてもしようがないので、指摘するにとどめたいと思います。
私は、去年、このサイバーセキュリティーの関係は、日本年金機構の漏えい事件が五月末に起こり、六月の頭に発覚して、それ以来、この内閣委員会で実に八回この問題を取り上げて質問しました。それから総務委員会でも二回、計十回委員会でこのサイバーセキュリティーの問題を取り上げ、そしてまた、維新の党として、サイバーセキュリティ基本法の改正案というのも出させていただいた。非常に思い入れがあります。
今回、その点も踏まえて政府として改正案が出てきたわけでありますが、その中で、去年もずっと指摘し続けてきたんですけれども、ともかく、もちろん法律も大事ですけれども、やはり予算と人だ。このＮＩＳＣにいろいろな仕事を任せるに当たって、今の人ではとても足りないし、あと政府全体の予算も少ないじゃないかと。内閣委員会は菅官房長官も御出席いただけるので、菅長官はセキュリティ本部長ですから、菅長官に二回私はこのことを強く申し上げて、菅長官もかなり大きくうなずいていただいたと思っております。
今回、予算も、当初予算ベースでいうと、平成二十七年に三百二十五億だったものが四百九十九億と、一・五倍以上の増加ということで補正予算もかなりついておりますので、一定の評価はいたします。
ただ、その中身を見ると、この予算全体の資料を見ると、例えば防衛省については九十億も予算がついている、ふえています。あるいは、年金機構の担当の厚生労働省の予算もぐっとふえている。一部のそういったところの予算はふえていますが、全体として、私は去年、倍増どころか一桁違うんじゃないかということを菅本部長に申し上げたんですけれども、それからするとまだまだ足りないのではないかと思いますけれども、御見解はいかがでしょうか。

○谷脇政府参考人　お答え申し上げます。
サイバーセキュリティ戦略本部におきましては、昨年の八月、サイバーセキュリティ関係施策に関する平成二十八年度予算重点化方針というものを決定いたしまして、重点化を図るべき分野として、関係府省及び産学官の連携等、また政府機関の防御能力の強化等、さらには人材育成や研究開発等の横断的施策、この三つを重点分野として特定したところでございます。
ＮＩＳＣにおきましては、各府省の概算要求がこの方針を踏まえたものとなるよう施策の具体化を促す等、所要の措置を講じたところでございます。
毎年度、関係予算については波動性が出る部分もございますけれども、平成二十八年度予算につきましては、必要な予算を確保していただいているものと認識をしております。

○高井委員　それでは、人員の方ですね、ＮＩＳＣの人員も私は大幅にふやすべきだということを提案したんですけれども、今年度、この一年でどのくらいＮＩＳＣの人数はふえているんでしょうか。

○谷脇政府参考人　お答え申し上げます。
内閣サイバーセキュリティセンターにおきましては、質、量ともに増強に努めてきたところでございますけれども、数字で申し上げますと、平成二十六年度当初が、ＮＩＳＣの職員数は約八十名でございます。これが平成二十七年度当初で約百二十名、さらに今年度、今々現在におきまして約百六十名ということで、人員の増強また質の強化に努めているところでございます。

○高井委員　二十六年から比べれば倍増ということで、去年から比べても四十名ですか、ふえているということで、一定の評価はしたいと思います。
ただ、去年、私は菅セキュリティ本部長にこう提案をしています。というのは、アメリカは何と

六千名いるそうです、ＮＩＳＣに相当する、厳密に相当、イコールとは言えないかもしれませんが。ただし、このアメリカのＮＩＳＣ相当の機関というのは、電力とかガス、水道、鉄道、そういった重要インフラ、これも全て所掌している、それだけ間口も広いですから六千名と。

フランスは、五百名いたのが去年七百名に増員した。イギリスはちょっと数字がわからないんですが、イギリスも実は、こういった重要インフラも全て国というかセンターに集中して、それぞれの部署がやるというよりもセキュリティーの分野はとにかく一極集中して、専門家の数というのはそんなにたくさんいませんから、やはり、限られた専門家を一カ所に集めてやるということが望ましいんじゃないかということを提案いたしました。

そういったことからすると、私は、セキュリティーの関連予算も人員も、一定の評価はしますけれどもまだまだ足りないんじゃないか。しかし、そうはいっても政府の中にそんなにセキュリティーの専門家がいるとは思えませんので、やはり、加えて民間のセキュリティーの専門家とかそういった方をどんどん登用していくべきではないかと考えますが、これは大臣、いかがですか。

○遠藤国務大臣　委員御指摘のように、私、担当しまして、いろいろ皆さん方の話を聞くと、アメリカは大体一桁、人員も予算も違うんじゃないかと言われております。

今、サイバー空間におけるこうした脅威が深化する中で、我が国におけるサイバーセキュリティー推進体制の強化が不可欠であることはもちろんでありますから、平成二十七年一月九日に、内閣官房の情報セキュリティセンターを改組し、内閣サイバーセキュリティセンターを発足いたしました。

人員につきましては、今委員御指摘のように、国家公務員のみならず、サイバーセキュリティーに精通した学識経験者や民間事業者等からも専門性を有する職員を登用するなど、質、量ともに増強に努めたところでありますが、平成二十八年三月現在、約百六十人の職員がその任についており、平成二十八年度には百八十人程度を目指して増強に努めてまいります。

引き続き、優秀な人材の確保や、業務の専門性に鑑みた長期間の職員採用に努めるなど、増大するサイバーセキュリティーの脅威に適切に対処していくために、委員初め皆さん方の御協力をいただいて、所要の予算措置を含め必要な措置を講じてまいりたいと考えております。

○高井委員　定員の範囲でやろうとすると、私も役所に勤めていましたから、スクラップ・アンド・ビルドでどうしても定員を大幅にふやせないということなので、やはりここは工夫が要ると思うんですね。今、民間から出向のような形で来ていただいているんでしょうけれども、しかし、それも恐らく定員としてカウントして、給料も税金で払うということ。そこは、どう工夫の余地があるかというのはなかなか難しい面もあります。

ただ一方で、例えばＩＰＡであるとかあるいはＮＩＣＴであるとか、あと、この後話題にしますけれども、Ｊ－ＬＩＳ、地方公共団体の情報システム機構、まさに今回の法律もそういう一環だと言えばそうなんですけれども、やはり、こういったところと一緒になってＮＩＳＣの体制を強化するということは、もうちょっと踏み込んで検討していただいてもいいのかなというふうに思っております。

今回、情報セキュリティーの審議官を創設される、これは大変いいことだなとは思います。ただ、これは情報セキュリティーと情報化推進審議官ということで、ＩＣＴ全般の推進とセキュリティーと、両方を担当する審議官だと思います。

審議官といえば、局長の次、部長級、課長よりは上の、なかなか権限を持ったポストであります。しかし、ここに情報化とセキュリティーを担当する審議官を置くというのは、一体どういう人物像を想定しているのか。まだ発令されていないと思うので、こういう人とはっきり言えないと思いますけれども、どういう人物像の方を想定し、そして、きちんとその下には部下がいるのか。

というのは、実は、ＣＩＯ補佐官というのはこれまでもいるわけですね。ＣＩＯというのは、大体、各省庁の官房長がやっているケースが多くて、ほとんど官房長はＩＣＴのことなんかわからない。しかし、ではそのＣＩＯ補佐官という人が、官房長直属で、すぐに機動的に動け、そして課長とかに対して指示ができるのかというと、そういう役職でもないしそういう人物でもないということで、実質的になかなか機能してこなかったという経過があるわけですが、今回の情報セキュリティーそして情報化推進の審議官というのは、そういう点で機能はするんでしょうか。

○谷脇政府参考人　お答え申し上げます。

今委員御指摘のように、各府省庁におきましては、平成二十八年度から、サイバーセキュリティー対策や情報化推進を統括する新しい審議官として、サイバーセキュリティ・情報化審議官を新設いたしまして、情報システムの適切な運用管理とサイバーセキュリティー対策、そしてこれらと一体となった業務改革等につきまして、各府省庁内を指揮監督できる強力な体制を構築することとしております。

また、政府におけるセキュリティーに関する人材育成につきまして、今年度中に策定予定のサイバーセキュリティ人材育成総合強化方針のもとで、この新設する審議官等を中心に、政府一体となった取り組みを進めてまいりたいと思っております。

また、委員御指摘の体制の問題でありますけれども、各府省庁のセキュリティー、ＩＴに係る部局の体制の強化につきましても、まずは官房部局から、さらにそれを広げる形で政府全体として段階的かつ積極的に取り組んでまいりたいと考えております。

○高井委員　これは本当に、こういう職を置いた、しかもきちんとスクラップ・アンド・ビルドもして、審議官のポストを一個各省庁につくるというのは大変な努力だったと思います。

そこまでしてつくったせっかくのポストでありますけれども、機能するかどうかというのは、それぞれの省庁において、ＣＩＯをやる官房長なり、やはりそういったところがしっかりと部下に対して指示を出せるかどうかというところだと私は思います。しかし、正直言って官房長というのは大変忙しい仕事であり、情報化、ＩＴのことばかりやるわけにはいかない。

そうなりますと、やはり、セキュリティ本部なりＩＴ戦略本部なりがしっかりと官房長に対して指示を出すということ、そして、ちゃんと官房長から各省の中で指示系統をつくって、あるいはきちんと部下も配置をして取り組むということが極めて大事だと思いますので、そこは、セキュリティーの面でいえば遠藤大臣はセキュリティ副本部長になるんですか、そこはしっかり取り組んでいただきたいと思います。

それでは、少し話はかわりますが、今回の法律というのは、日本年金機構の情報漏えいを受けたという側面が強いと思うんですね。そういったサイバーアタックというか情報漏えいというようなものについての対策という面が強いと思います。

サイバーテロと言われる、これは、情報漏えいというレベルを超えたもっと脅威的な、まさに戦争に匹敵するといいましょうか、アメリカなんかでも、サイバーアタックというものを第五の戦争分野だというふうに認識して、だからこそ先ほど言った六千名という人員にもなるのかもしれません。

このサイバーテロの脅威というものを、セキュリティーを担当する大臣として、また、東京オリンピック・パラリンピックも本当に格好のテロの標的になる。あと、伊勢志摩サミットもあります。今のところ、物理的なテロというか、人がいわゆる爆弾を仕掛けて云々という方がやはりどうしても心配され、クローズアップされますが、私は、今の時代、サイバーテロというものが同じぐらいの脅威を発揮し得るんだろうと思います。

そういった点から見て、遠藤大臣は、サイバーテロというものに対してどういった認識をされておられ、そしてまた、直近である伊勢志摩サミットや、あるいは御担当である東京オリンピック・パラリンピックへの備えというものは十分備えられているんでしょうか。お聞きいたします。

○遠藤国務大臣　先ほども回答申し上げましたが、こうした大きな大会あるいはいろいろなイベントにつきまして、やはり安心、安全が最大の成功の要因だと思っております。

今、社会経済システムを初めとしてあらゆるものがネットワーク化されつつある中で、個人情報の窃取、あるいは経済的な犯罪から情報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していると認識しております。

とりわけ、我が国は、目前に伊勢志摩サミット、また三年後にはラグビーのワールドカップ、そして四年後には東京オリンピック・パラリンピックを控えておりますので、現下の厳しいテロ情勢に鑑みて、サイバーセキュリティーの確保は極めて重要な課題であると認識をしております。

この中で、伊勢志摩サミットについては、内閣官房副長官を座長とする伊勢志摩サミット準備会議のもとにサイバーセキュリティーワーキングチームを設置して、会議主催府省庁等におけるサイバーセキュリティー対策の徹底を図っております。

また、東京オリンピック・パラリンピック競技大会については、安倍総理を本部長とする東京オリンピック競技大会・東京パラリンピック競技大会推進本部のもとに設置されたサイバーセキュリティワーキングチームにおいて、関係者間の脅威情報の共有体制の確立などに向けて検討を進めております。

伊勢志摩サミット及び東京オリンピック・パラリンピック、ラグビーワールドカップを成功させるためにも、今後とも、関係組織が互いに緊密に連携をしながらサイバーセキュリティー対策に万全を期してまいりたいと考えております。

○高井委員　ロンドン・オリンピックのときも、サイバーアタックはかなり物すごい数があったと。しかし、あれはある意味愉快犯的なところもあって、例えば競技の記録を何か改ざんしてやろうとかですね。もちろんそれも大変重大な犯罪であり、取り締まらなければならないんですが、やはり、私はそれ以上に、テロ、人が死ぬ、しかも大勢の人が死ぬ可能性のあるテロもこのサイバーという手段が起こし得るんだということをぜひ認識していただきたい。

警察ももちろん、そういった面もやっていると思いますが、警察は警察でやはり物理的なというか人による犯罪の方にどうしても注力しがちだと思いますので、そこは本当にセキュリティ副本部長の遠藤大臣が、ましてや東京オリパラの御担当でもあるので、ぜひそこの面はしっかり意識をして、何でもかんでもＮＩＳＣにとなると大変なんですけれども、しかし、やはりＮＩＳＣにセキュリティーの専門家が集まっていますので、ＮＩＳＣと警察がよく連携していただいて、そこはしっかりやっていただきたいと思います。

実は、私が一番恐ろしいと思っているのは、原発じゃないか。今回のベルギーも、原発にＩＳが侵入する計画もあったと。私は、物理的な侵入というのはなかなか大変な、それだけの防御をしていると思うんですけれども、では、サイバーテロという点の備えを果たして原発施設が行っているのかというのが非常に疑問であるわけなんです。

これは、担当は原子力規制庁だとお聞きしたので、きょう来ていただいていますけれども、原発関連施設へのサイバーテロというのはどのくらいの備えをしていて、あるいは最悪の場合どういう事態にあるかとか、そういった想定はしているんでしょうか。

○荻野政府参考人　お答え申し上げます。

原子力発電所における情報セキュリティーについてのお尋ねでございます。

これにつきましては、原子炉等規制法に基づいて原子力規制委員会が制定いたしました規則におきまして、原子力発電所においては、まず、情報システムが電気通信回線を通じて破壊行為、妨害行為を受けることがないように、外部からのアクセスを遮断することを求めております。

また、この規則では、情報システムに対する破壊、妨害行為が行われるおそれがある場合、また行われた場合において、迅速かつ確実に対応できるよう情報システムセキュリティ計画を作成することを事業者に求めておりまして、事業者は、情報システム妨害行為が発生した場合等においては、その旨を規制機関に直ちに連絡するという仕組みになっております。

なお、こういったことを含めまして、事業者が行う防護措置の内容や体制について核物質防護規定といったものを定めることになっているわけでございますけれども、これの遵守状況につきましては、原子力規制委員会におきまして定期的に検査し、確認を行っているところでございます。

○高井委員　今のお答えを聞いても、遠藤大臣、ちょっと何か生ぬるいというか、本当に大丈夫かなという気がするんですね。では、原子力規制庁に果たしてどれだけセキュリティーの専門家がいて、かつ、原発施設というのは、日本は民間企業、電力会社がそれぞれ担当していますが、では、その電力会社がどこまでサイバーセキュリティーに対して知見を持ち、そして責任を持てるのか。

電力会社は重要インフラ事業者ですから、もちろんこのサイバーセキュリティ法の所掌の範囲ではあります。しかし、その位置づけとすれば、国の政府機関をＮＩＳＣが監査したりすることと比べると、やはり位置づけが一歩下がるんですね。

ほかの重要インフラ、鉄道とか水道とかももちろん危険はありますけれども、やはり原子力発電というのは非常に恐ろしい可能性がある。ですから、あらゆるサイバーセキュリティーの専門家にこういう可能性もあるというようなものをもっとしっかり洗い出してもらって、それについて一個一個潰していくという対応が、これはやはり原子力規制庁に任せるのではなくて、ＮＩＳＣが、今の法体系のもとではおせっかいなことかもしれませんけれども、そんなことは言っていられないわけで、やはりセキュリティ本部として取り組んでいただきたいと私は思っております。

似たような話として、先ほど平井委員からも再三指摘がありましたけれども、地方自治体。これは、私は、実は去年の日本年金機構の情報漏えい事件があったときに、真っ先に地方自治体だと。年金機構の問題はもうそこそこにして、地方自治体、これからマイナンバーがスタートして、あるいは、当時何度も私は紹介したんですけれども、総務省出身の神戸市長、久元さんという局長をされた方が市長なんですけれども、ブログに書かれていたんですね。年金機構の問題よりも自治体の方がはるかに、何十倍、何百倍と個人情報を扱い、そしてセキュリティーの危機にさらされていると。

であるから、総務省に私は再三この強化をしてくださいということをお願いし、そしてまたＮＩＳＣにも、今の法律の中では地方自治体に対しての権限というか関与が不十分なので、地方自治の本旨はわかりますけれども、しかし、現実にサイバーセキュリティーの専門家をそんなに、千七百以上ある地方自治体にそれぞれ配置できるわけはありませんので、やはりそこは中央集権的にＮＩＳＣがやるべきではないかということを提案し、そしてまた、法改正の提案も維新の党としてさせていただいた。

その結果、今回の法律になっているわけですが、私は、やはり今のこの法律でもこの部分は不十分ではないかと思っています。これは大臣、ぜひ、地方自治体のセキュリティー対策に対して、ＮＩＳＣとしてどのようにかかわっていくのか。法律上は、先ほども答えておられましたけれども、求められたときは対応するというのはありますけれども、そのくらいの関与では弱過ぎる、もっと積極的にかかわるべきだと私は考えます

が、いかがでしょうか。

○遠藤国務大臣　お答えいたします。

地方公共団体の行う業務は国民生活と密接な関係を有するものであり、サイバーセキュリティー対策を一層充実させる必要があると思っております。このため、地方自治体の提供する行政サービスについても、重要インフラの一分野と位置づけ、主要な対策について国として支援をしているところであります。

また、基本法においては、サイバーセキュリティ戦略本部は、地方公共団体の長に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることが可能であり、本部長は、提出された資料等を踏まえ、必要があると認めるときは、関係行政機関の長に対し勧告することができるよう規定をされております。

他方、今委員御指摘のように、地方自治の本旨も踏まえて、国による関与については一定の配慮が必要だと考えられ、そのため、サイバーセキュリティ戦略本部への求めがあった場合に、それに応じて規定されているところであります。

とはいえ、マイナンバー制度の本格稼働を踏まえて、地方自治体のセキュリティー対策の強化は極めて重要であり、関係府省と連携をしつつ、地方自治体に対する支援を含めた対策をなお一層推進してまいりたいと考えております。

○高井委員　最後のなお一層というところをぜひ。

今の御答弁は、現時点ではそういう御答弁しかできないとは思う。しかし、先ほど申し上げましたように、地方自治体から必要に応じて求めがあったりとか、あるいは何か起こってから、では資料の提出をしなさい、それを見て勧告しますとかいうのでは、サイバーテロとか個人情報漏えいというのは一瞬にして起こるわけですから、やはり事前の監視活動が大事であって、その監視が地方自治体には及ばないというところは私は大変不安だと思います。

ただ、ＮＩＳＣの方と話すと、現実にそうなって、やろうと思っても、今の人と予算ではとてもできませんということでありますから、冒頭申し上げた予算とか人とも連動してきます。しかし、いずれにしてもこれは国家としてやらなきゃいけない、政府としてやらなきゃいけないことだと思いますので、ぜひ、遠藤大臣のリーダーシップでそこは進めていただきたいと思います。

今の話でいうと、もうちょっと具体的な提案をすると、今回の特殊法人、認可法人まで対象を広げる、これは日本年金機構を想定しているという説明なんですけれども、ここにＪ―ＬＩＳ、地方公共団体情報システム機構、ここは地方自治体がお金を出し合ってつくった組織でありますから地方自治体の扱いということなんでしょうけれども、しかし認可法人ではあります。そのほか、例えば健康保険とか医療保険とか、こういったものをそれぞれやっている団体の中で認可法人もありますし、私は別に認可法人じゃなくても、この際、そういった非常に重要な国民の個人情報を扱っているような団体は広く対象とすればいいんじゃないかと思いますけれども、大臣、いかがですか。

○遠藤国務大臣　改正法案により、国による不正な通信の監視の対象とする特殊法人、認可法人については、当該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、サイバーセキュリティ戦略本部が指定することとしております。

具体的には、当該法人の業務と国の業務の一体性、二つ目には、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、三つ目には、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、四番目には、ＮＩＳＣの技術的能力、知見が活用可能であるか等の要素を踏まえ、サイバーセキュリティ戦略本部において決定することと考えております。

現時点では、平成二十七年五月に情報流出事案が発生した日本年金機構を指定することを想定しておりますが、委員御指摘の地方公共団体情報システム機構、Ｊ―ＬＩＳを初め、本法案に基づく指定法人の対象とするか否かについては、当該法人自身及び所管省庁と調整、検討していくことになると考えております。

○高井委員　今、所管省庁と検討、相談をするということだと思いますけれども、それでは、総務省はＪ―ＬＩＳを指定することに対してどういう考えを持っておられるか。前向きに相談する考えはありますか。

○古賀大臣政務官　Ｊ―ＬＩＳについての御質問でございますが、今遠藤大臣から御答弁ございましたように、Ｊ―ＬＩＳを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いては、Ｊ―ＬＩＳ自身の意向も踏まえまして、総務省としてもＮＩＳＣの検討に協力していきたいというふうに考えております。

○高井委員　前向きと捉えていいんでしょうか。これは本当に、私は非常に大事なことだと思います。今回、昨年の年金機構の事案を受けて、地方自治体は大丈夫かと。

では、総務省にセキュリティーの専門家というのは何人いるんですか、地域情報をやっている地域情報政策室というところがありますけれども、何名いて、セキュリティー専門家は何人ですかと聞いたら、七名いて、セキュリティーの専門家はゼロですという答えだったんですね、去年は。ことしは四人ふやしましたということで、そのうち一人の企画官がセキュリティーの専門家ですと高市大臣がこの間、総務委員会で答弁されましたけれども、それで千七百以上ある自治体のセキュリティーを所管するなんてことは到底できない。

だからこそＪ―ＬＩＳという組織があるわけですが、これは通告しているので、では、果たしてＪ―ＬＩＳにはどのくらいセキュリティーの専門家というのはいるんですか。

○宮地政府参考人　お答え申し上げます。

Ｊ―ＬＩＳでのセキュリティー対策につきましては、情報セキュリティー管理規程に基づきまして、組織的な側面とそれから人的な側面の双方で対応を講じております。

組織的な部分としましては、Ｊ―ＬＩＳの管理部門に情報セキュリティー管理の専門部署を設置したりしております。一方、人的なセキュリティーの対策といたしましては、情報セキュリティスペシャリスト等のセキュリティー関連の資格取得者を配置しているところでございます。

○高井委員　何名いるとか、そういう答えはなかったわけですけれども。

私は、正直余りいないと思うんですね。

ですので、ここも、つまり、やはりＮＩＳＣの力をかりる。Ｊ―ＬＩＳだけで千七百八十の自治体のセキュリティー対策はとても担えない。そして、総務省の先ほどの十一名でも担えない。やはりここはＮＩＳＣに協力を要請すべきだと私は思いますので、ぜひ、これは総務省として、ＮＩＳＣとよく相談していただいて、一刻も早くこれは対象にすべきだというふうに私は思います。

私が去年指摘をして、今回地方自治体のセキュリティー対策に二百五十五億円の補正予算をつけていただいた、このことは評価したいと思うんです。ただ、先ほど平井委員も苦言を呈されていましたけれども、必ずしも、使い方というか、これで十分なのかと。

まず金額面で、私は前回総務委員会でも質問しました。そのときは、一つ、二つの自治体から聞いた話、実は補正予算で示されている額よりも四倍ぐらい高い金額をベンダーから提示されて困っている、それを質問したんですけれども、その質問をした後にさらに、私の質問を聞いた人とかいろいろな、相当複数の自治体から、やはり三倍から四倍高いんだ、困っていると。しかし、もうやらなきゃいけないから、自治体は自分たちの予算を捻出して何とかやりますよと言っていますが、私はやはり、そもそもこの見積もりが甘いというか、逆に、ベンダーを厳しくたたいてぎりぎりの値段で予算をつくっておいて、しかし、実際に各ベンダーが自治体に営業に行くと、確かに今、マ

イナンバー特需もあって、ＳＥが、人が足りなくてどんどん値段が上がっているというような状態なんですね。

それと、もう一つ問題だと言われているのが、先ほど猿渡さんから、三層構造のセキュリティー対策をしっかりやっていますと。しっかりはいいんですけれども、しっかりやり過ぎるがゆえに、極端に言えば、職員は二台パソコンを置かなきゃいけないとか、あるいは課に一つ共有パソコンを置いて、インターネットを見たい人はそこから見てくださいなんという、何十年前の仕事なんだと。そんな仕事が今どき行われていたら、自治体は大変なことになるわけです。そういった面。

実は、これは仮想化する技術というのがあるんですけれども、その仮想化技術を導入するにはやはりお金が非常に高くかかるということで、この予算とそれから総務省が求めているセキュリティーの三層構造というのはちょっと無理があるんじゃないかというふうに、前回総務委員会で指摘させていただきました。

その後、こういった自治体の声を総務省としては聞かれているんでしょうか。

○古賀大臣政務官　ただいま高井委員から御質問をいただいた自治体のセキュリティーですけれども、今お話がありましたように、二十七年度の補正予算で、必要経費の二分の一ということで二百五十五億を措置、計上しているところであります。

不十分じゃないかというような御指摘の点ですが、自治体独自に、より高度な情報セキュリティー対策を実施する、そういった場合には、補助金対象経費に基準額で設定していることもありまして、一定の自治体負担が発生せざるを得ないというようなことも想定されるところでありまして、見積もりの方法等も含め、これまでも自治体からの問い合わせに緊密に対応してきたところであります。

先日、三月八日でありますけれども、この二百五十五億の補正予算、各自治体の補正予算において必要経費を計上していただいた上で、交付申請のあった千六百七十一市区町村及び四十五道府県に対しまして、対策支援のための補助金約二百三十六億円の交付決定を行ったところであります。今回申請のなかった残りの七十団体についても、来年度早々に申請するものと伺っているところであります。

今後、この補助金を活用していただいて、各自治体によって十分な情報セキュリティー対策が実施されるように、引き続き自治体ともいろいろな情報交換、把握をしながら支援をしていきたいと考えているところです。

○高井委員　総務省に聞くと必ずそういう答えで、自治体がよりハイスペックなものを入れて、そこは自治体の負担なんだと。でも、そうじゃないんですね。そんなハイスペックなものを入れようとしているんじゃなくて、本当に最低限のものを入れようとしても高くなっているという現場の声を私は何自治体からも聞いていますから、ぜひそこは、政務官、もう一度自治体の声をしっかり聞いていただきたいと思います。

この件について、セキュリティーを自治体に求めるという、総務省にももちろん、猿渡さんはセキュリティーの専門で十分理解されていると思いますけれども、やはりより専門である谷脇さん初めＮＩＳＣのメンバーがいるわけですけれども、自治体のセキュリティー対策をやるに当たって、総務省とＮＩＳＣで相談はされたんでしょうか。

○谷脇政府参考人　お答え申し上げます。

地方自治体の情報セキュリティー対策の抜本的強化に関して検討を行いました総務省の自治体情報セキュリティ対策検討チームには、ＮＩＳＣもオブザーバーとして出席をしており、報告の内容についても把握をさせていただいているところでございます。

インターネット接続系とＬＧＷＡＮの接続系の分割につきましては、セキュリティー対策一般においても有効な手段の一つであるというふうに私どもは考えております。

総務省におきましても、地方自治体において扱う情報の重要性ですとかシステム構成等を勘案し、円滑な業務プロセスの確保を図った上で検討しているものと理解しておりますので、今後とも、自治体のセキュリティー対策の強化に向けて、総務省と連携しつつ必要な対策を推進してまいりたいと考えております。

○高井委員　自治体の現場が非常に今不便になっているという声も届いているんじゃないかと思いますので、総務省の方がより届いていると思いますから、ぜひそこは改善に向けて検討していただきたいと思います。

きょうは、実はＪ－ＬＩＳ、マイナンバーの故障の話もしたかったんですが、これは先般総務委員会で指摘して、総務大臣から理事長に再度指導していただいたと聞いておりますので、それはもうきょうは行いません。

それから、経産省と文科省にも来ていただいたのに、質問できなくて時間になってしまいましたので、申しわけありませんでした。

以上で質問を終わります。ありがとうございました。

○西村委員長　次に、島津幸広君。

○島津委員　日本共産党の島津幸広です。

まず確認をしたいんですけれども、法案の提案理由で言っているサイバーセキュリティーに関する重大な事象、これはどういう事態なんでしょうか。

○谷脇政府参考人　お答え申し上げます。

いわゆる特定重大事象と言われるものでございますけれども、これにつきましては、サイバーセキュリティ戦略本部で決定をしておりますサイバーセキュリティ戦略本部重大事象施策評価規則において規定しております。そして、戦略本部長である官房長官がこれに該当すると判断した場合には、サイバーセキュリティ基本法に定める原因究明調査の対象になります。

具体的には、国の行政機関で発生をいたしましたサイバーセキュリティーに関する事象のうち、行政事務の遂行に著しい支障を及ぼし、または及ぼすおそれがあるもの、また、国民生活または社会経済に重大な影響を与え、または与えるおそれがあるもの、我が国のサイバーセキュリティーに対する国内外の信用を著しく失墜させ、または失墜させるおそれがある事象、こうしたものを想定してございます。

〔委員長退席、中根（一）委員長代理着席〕

○島津委員　あってはなりませんけれども、個人情報での、今回の年金の流出のような重大な事象などの際、こうした場合には国民に説明する規定というのはあるんでしょうか。

○谷脇政府参考人　お答え申し上げます。

事案が発生した際の国民への公表につきましては基本法上明示的な規定が設けられているわけではございませんけれども、公表することにより攻撃者を利する可能性があること、他方、公表しないことによる国民生活や経済社会活動への深刻な影響等を慎重に比較考量し、公表できるものは公表すべきということが基本的な姿勢であるというふうに考えているところでございます。

○島津委員　年金の個人情報が流出したわけです。これからマイナンバーも万全のセキュリティーが求められているわけです。万が一こうした個人情報が流出してしまえば、その方の権利侵害の可能性は将来にわたって残り続けていくわけです。さまざまな形で未来にわたって悪用される危険がある。

今御答弁があったのは、基本法の第三条六項の国民の権利を不当に侵害しないように留意するということの中にも含まれていると思うんですけれども、セキュリティーというのはあくまでも国民の大事な情報を守る、不利益が生じないようにしっかりやらなきゃいけないということです。そういう点では、やはりきちんと国民の皆さんに説明、報告していくということを確認しておきたいと思うんです。

大臣、通告していませんけれども、ＩＴ推進のためというだけじゃなくて、国民のためにやるん

だという認識がやはり一番大事だと私は思うんですけれども、これはどうでしょう。

○遠藤国務大臣　今、政治経済の複雑化した中で、こうした対策については、組織を守るためじゃなくて、やはり国民を守るためということは当然であると考えております。

○島津委員　そういう立場でぜひ進めていってほしいと思うんです。

次に、今回の法改正の理由に、年金情報の流出事件があるわけです。

この年金機構の流出の問題、これまでもいろいろなところで議論されてきていますけれども、改めて、この教訓は何か。いろいろあると思いますけれども、ポイントを簡潔にお願いしたいと思います。

○谷脇政府参考人　お答え申し上げます。

昨年の五月二十八日、日本年金機構が保有をしておりました個人情報の一部である約百二十五万件が外部に流出したことが判明したことを受けまして、六月一日、ＮＩＳＣは、客観的、専門的立場から事案の原因究明を実施するため、原因究明調査チームを設置いたしまして事案の解明を行い、これを踏まえ、サイバーセキュリティ戦略本部として、八月二十日、日本年金機構における個人情報流出事案に関する原因究明調査結果を決定、公表しております。

この調査から、具体的な教訓といたしまして、年金機構のセキュリティーポリシーにおいて、インシデント対処体制に関して、サイバー攻撃を想定した具体的な対応が明確化されておらず、事案発生時の報告、連絡が適切になされていなかったこと、また、年金機構においてＣＳＩＲＴ体制が構築されていなかったこと、さらに、標的型攻撃からの有効な遮断機能を有すると考えられるインターネットに接続していない業務系から、インターネットに接続している情報系に個人情報を移して取り扱っていたこと、こうしたことが結果として個人情報の流出につながったというふうにこの報告書の中でも明記をしているところでございます。

○島津委員　今お答えがあったように、やはり年金機構の中でいろいろなずさんなことがやられていたわけです。

今回、この年金の問題について言えば、年金機構がまずセキュリティー対策を講じなきゃいけない主体であったんですけれども、それが不十分だったということです。

ただ、この年金の情報流出の問題は、業務のあり方も反映していると思うんです。年金の給付の管理だけなら年金機構内のオンラインシステムの中でできるんですけれども、ＬＡＮシステムの共有サーバーに移さないとできない仕事もあった。未納者に督促状を送るだとか、ねんきん定期便を送るだとか、そういうリストをつくる仕事があるんですけれども、そうした仕事が外部委託でやられている。そして、その中で、今もお話がありましたけれども、機構の端末にＵＳＢメモリーを使用してデータを移したり、こういうことがやられていたわけです。

業務経費の削減で、外部委託が拡大しています。職員も削減された。非正規化も進んでいる。社会保険庁が解体されて日本年金機構が発足したんですけれども、その際には正規職員が二千二百人も減らされている、そして労働強化。こういう職場環境の中で起きたということも言えるわけです。

こういう問題にもメスを入れなきゃいけないと思うんですが、どうでしょう、これは通告していませんけれども。

○福本政府参考人　お答え申し上げます。

日本年金機構の情報セキュリティー体制がどうであったかという観点でお答えをいたしたいと思いますけれども、情報が流出した当時のセキュリティー対策に関して申し上げますと、今先生の御指摘にもございましたが、年金の個人情報はインターネット環境から隔離された基幹系システムというところで取り扱うことが基本でありましたけれども、一部の情報については、業務の必要上、インターネット環境に接続された機構ＬＡＮシステムの中でその共有フォルダに保管し使用するということをしておりました。

また、この共有フォルダにあるファイルでありますけれども、パスワードを設定するというようなルールを設けておりましたけれども、必ずしもそれが徹底されていなかったというような問題もございます。

さらに、標的型メール攻撃、今回はこれを受けたわけですけれども、個人情報を標的型メール攻撃から防ぐための対策、あるいはその対処の手順ということについても定めが十全でなかったというようなこともございます。

そして、さらに加えて、情報セキュリティーについての組織体制でありますけれども、これも十分ではなかったという話もありますし、先生御指摘のような、機構全体で体制が十分であったかどうか、職員の資質あるいは研修ということについても、外部との関係も含めて十全であったかどうかというようなことも今回改めて我々は検証し、その体制の確保に努めていかなければならないと考えておるところでございます。

○島津委員　やはりこうしたところも、行革でただ人を減らせばいいということだけじゃなくて、しっかりやらないとセキュリティーの問題にも影響するということだと思うんです。

年金の問題は、第一義的には年金機構に責任があるわけですけれども、それでは、所管している厚労省はどのような対策をしていたのか。

厚労省が出した「情報セキュリティ強化等に向けた組織・業務改革」で、「機構を監督する厚労省自身の長きにわたっての意識の欠如が、機構の個人情報流出につながった大きな要因。」こう反省しています。これは間違いありませんね。

○安藤（英）政府参考人　お答え申し上げます。

今回の日本年金機構の情報流出事案を受けまして、発生直後から、厚生労働省におきましては、外部有識者による検証委員会を設置し、徹底した原因究明と再発防止策の検討を行うとともに、先ほど御説明がございましたとおり、サイバーセキュリティ戦略本部におきましても原因究明調査をいただいたところでございます。

その結果、日本年金機構及び厚生労働省のいずれにおきましても、サイバー攻撃に対する危機意識が低く、インシデントに対処する体制や技術的対応が不十分であったことが明らかになったということでございます。

今先生から御指摘を受けたとおりということでございます。

○島津委員　厚労省は意識が欠如していたというわけです。

では、ほかの省庁はどうだったかということで、国税庁に来ていただいていますので聞きたいんですけれども、確定申告や法人の納税などをパソコンで行うことができるｅ－Ｔａｘを初め、納税という国民の皆さんにとって最も重要な情報の一つを扱っているわけです。このセキュリティー対策を簡潔に教えてください。

○柴﨑政府参考人　お答え申し上げます。

国税庁におきましては、基幹システムで管理しております納税者情報が外部に流出することがないように、納税者情報を管理する基幹システムに接続しております職員の業務用パソコンとインターネット用のパソコンを物理的に分離いたしまして、インターネットを通じて外部から納税者情報に不正アクセスを受けることがないようにしているところでございます。

また、納税者情報を取り扱う全ての事務処理は業務用のパソコンで行っておりまして、インターネット用のパソコンで納税者情報を取り扱う事務処理は行ってございません。

これに加えまして、インターネット用パソコンに納税者情報を持ち込み保管することは禁止しております。

また、納税者情報以外の情報を業務用パソコンからＵＳＢメモリー等を利用して取り出す必要がある場合には管理者の許可を必要としており、さらに、取り出し可能なものをシステム的に制限し

ているところでございます。

○島津委員　私も事前に説明を今の説明に加えて聞いたんですけれども、なるほどなということでした。

人為的なミスもありますから、絶対ということはないわけです。しかし、それを防ぐために、今お答えがあったように、ＵＳＢメモリーを使う場合でも二重、三重の仕組みがある、インターネットにつながったパソコンでは仕事ができない、こうした徹底した対策をとっている。年金機構の問題が発覚した後には、こうしたルールの再徹底を行ったということも聞きました。納税情報というのは本当に漏えいしてはならない情報で、絶対に外に出さないという意識で皆さんが業務されていた、既にそのシステムを組んでいたということをお聞きして、実感しました。

大臣、サイバー戦略では、セキュリティーはその組織が自律的に行うことを基本とするとうたっています。ですから、今、国税庁の例が出たわけですけれども、こうした対策をより徹底することこそサイバーセキュリティーの中心に据えるべきじゃないかと思うんですけれども、どうでしょう。

○遠藤国務大臣　お答えいたします。

委員御指摘のように、サイバーセキュリティーの確保については、情報システムの構築、運用とセキュリティー対策を一体として行うべきものであると思いますし、各組織の特性に応じた業務継続性の確保の観点からも、まずは各主体が自律的に取り組むべきものと考えております。

なお、政府機関のサイバーセキュリティー確保については、政府機関の情報セキュリティ対策のための統一規範において、各機関がみずからの責任において対策を図ることにより、もって全体の情報セキュリティー対策の強化、拡充を図る旨を明確化しているところであります。

○島津委員　改めて、年金機構にかかわらず、独立行政法人や認可法人、特殊法人は、行政改革で省庁とは切り離されたとはいえ、重要な仕事を省庁と協力してやっているわけです。所管している省庁がしっかりとセキュリティーについても指導監督をしていくということでこれからやっていくと思うんですけれども、やはり、重大事案が起きたからＮＩＳＣが一足飛びに監視対象にする、すればいい、こういうことではないと思うんです。

個人の情報流出というのは、厚労省や年金機構そのものの業務のあり方も反映したものです。サイバーセキュリティーについての監査、監視があれば起こり得なかったというものでもありません。セキュリティーはその組織が自律的に行うことが基本であり、まず自分たちで自主的な取り組みを進める、それが十分であるかどうか所管省庁がしっかりと監督する、これをやはり基本としてまずやるべきだということを指摘しておきたいと思うんです。

次に、情報処理推進機構、ＩＰＡについてお聞きします。

今回、ＮＩＳＣが監査、監視、調査などの対象に加えるのは、年金機構だけでなく、独立行政法人も行われます。しかも、その広げた部分は、ＮＩＳＣがやるんじゃなくて、ＩＰＡに事務を一部委託するというわけです。

このＩＰＡの職員数と、そのうちの非正規職員数、民間からの出向、派遣の職員の人数を教えていただけますか。

○安藤（久）政府参考人　お答え申し上げます。

ＩＰＡの職員数は、本日現在で二百六十五名となっております。このうち、民間からの出向者は七十九名でございます。ＩＰＡで採用された方が百七十一名、国からの出向が十五名、こういったことでございます。今お尋ねの派遣につきましてはこの外数になっておりまして、派遣の職員数が百二十八名ということでございます。

○島津委員　非正規職員というのはいないんですか。

○安藤（久）政府参考人　いわゆる常勤と非常勤ということで申し上げますと、非常勤職員は二百六十五名の職員のうち八十九名でございます。

○島津委員　今回業務として新たに追加される監査、監視や原因究明調査にも民間からの出向や派遣の方はかかわるんでしょうか。

○安藤（久）政府参考人　お答え申し上げます。

民間からの出向者につきましては、ＩＰＡの職員になるということでございます。本法案に基づきまして、秘密保持義務が課せられる対象となります。サイバーセキュリティ戦略本部から委託される今御指摘の独法などへの監査、調査の業務にも従事をする予定でございます。

他方、派遣の職員につきましては、サイバーセキュリティ戦略本部から委託される御指摘の業務については従事をしないという予定でございます。

〔中根（一）委員長代理退席、委員長着席〕

○島津委員　ただ、そういう仕事には従事しなくても、秘密保持規定があるように、いろいろな情報をやはり知り得るわけです。

ＩＰＡの職員でなくなった後も秘密保持義務は今言ったようになくならないわけですけれども、しかし、出向期間が終わって自社に帰った後、ＩＰＡで知り得た秘密を利用して自社で仕事をしたとしても、誰にもわからないんじゃないでしょうか。これはどうでしょう。

○安藤（久）政府参考人　民間出向者が民間企業に戻った後も、法律上、ＩＰＡへの出向中に業務上知り得た秘密については、刑事罰のかかる形で、漏えい、盗用してはならないということになります。

したがいまして、これが発覚するかどうかというのは、一般の事案と同様に、さまざまな事案の発生を受けた捜査の世界に入ってくると思いますけれども、厳密な意味でもともとの職員と同様の法律上の秘密保持義務がかかるということで、強い牽制力になると思っております。

○島津委員　情報漏えいに対する罰則が設けられているわけですけれども、疑ったら切りがないということもあるかもしれませんけれども、やはり新たな情報拡散を招く疑念というのは否定できないと思うんです。

全ての独立法人や特殊法人に演習だとか監視、調査対象を広げていってもＮＩＳＣがやり切れないのでこの事務をＩＰＡにやってもらう、そしてその業務は今後さらに政令で法人を指定していくことも検討されているわけですけれども、そんなことをしなくても、各省庁や各組織がしっかりと体制をとって対策を進めていくことがやはり必要だと改めて思います。

最後に、ＮＳＣ、国家安全保障会議との関係についてお聞きしたいと思います。

基本法に基づいて策定されたサイバーセキュリティ戦略、これは二〇一五年九月四日に閣議決定されているわけですけれども、この中で、総務省における、米国とのサイバー攻撃に関するデータの共有及び研究開発の協力関係の加速化、情報の共有の強化などが盛り込まれています。

これはどういうことなんでしょう。どういうことをするんでしょうか。

○谷脇政府参考人　昨年の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の中では、さまざまな国際的な連携を強化していくということで、多様な施策を盛り込んでいるところでございます。例えば、日米間におきましても、サイバーセキュリティーに関する研究開発のプロジェクトなどにつきまして、お互いの意見交換、情報の交換などを積極的に推進していく、こういったことも盛り込まれているわけでございます。

○島津委員　具体的に、今回、いろいろ事象が起きた場合には調査したり原因究明したりするわけですけれども、そういう情報も共有するということになるんでしょうか。

○谷脇政府参考人　お答え申し上げます。

サイバー事案の概要ですとか、あるいは政策面でのさまざまな動向については、サイバー空間というものは国境がございません関係上、国際連携を強化し、また情報を共有していくということが極めて重要な課題でございます。

そういった観点から、米国それからオーストラ

リアあるいは英国等々、さまざまな国々とサイバー協議などを開催し情報の共有を図っております。

そういった文脈の中で、サイバー事案についても、必要な範囲内で情報を他国と共有するということを行っているところでございます。

○島津委員　その情報の内容というのは当然攻撃側に知らせてはならないものもあると思うんですけれども、必要なものというのはしっかりとやはり開示もされて、国民も含めて、国会議員も含めて開示されていくんでしょうか。

○谷脇政府参考人　お答え申し上げます。

例えば、日本年金機構の事案でございますけれども、私ども、昨年の八月に年金機構事案の原因究明調査報告をまとめたところでございます。

その中身につきましては、当然のことながら、国民に対する説明責任ということで、その内容を開示したところでございます。そして、この開示に当たりましては、一部、我々ＮＩＳＣの対処能力を明らかにする部分は正直ございましたけれども、説明責任という公益性を重視してこれを公表したところでございます。

同様の情報については、その範囲内で他国とも共有をしている、こういうことでございます。

○島津委員　ＮＳＣとの情報交換が今度あるわけですけれども、そういう内容も含んできちんと必要なものは開示していくということでいいんですね。

○谷脇政府参考人　お答え申し上げます。

サイバーセキュリティ基本法におきましては、サイバーセキュリティーに関する政策課題等について、安全保障にかかわる問題についてＮＳＣと緊密に連携する旨の規定が盛り込まれているところでございます。

したがいまして、こうした安全保障にかかわるサイバーセキュリティーに関する政策のさまざまな動向ですとか事態の推移等につきまして、ＮＳＣとＮＩＳＣとの間で情報を交換し、あるいは意見を交換しているということでございます。

○島津委員　ですから、ＮＳＣとの情報交換の中身についてもわかる、開示するということでいいんですね。

○谷脇政府参考人　お答え申し上げます。

個別具体的な協力内容につきましては、事柄の性質上、お答えできないことを御理解いただきたいと存じます。

○島津委員　今回、ＮＳＣと緊密連携ということになるわけですけれども、どんな情報がやりとりされていくのかは事柄の性質上答えられないと。これは安全保障上の問題だということなんですけれども。

どんな情報がアメリカ、米国に伝わるのかわからない。一方で、監視調査の対象を広げていく。もちろん、テロというのは、サイバーであれ何であれ絶対に許されないものなんです。しかし、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づけて、サイバー攻撃に対しては、現実空間での反撃、攻撃も辞さない、こういう立場です。軍事の対応というのは、憎しみを広げてテロをさらに引き起こす、悪循環につながるわけです。

我が党は、一昨年、サイバーセキュリティ基本法の審議の際、サイバーセキュリティーを軍事や安全保障に密接に結びつけるものであるとして反対しました。しかし、きょう、今議論しましたけれども、やはりアメリカのサイバー戦略に巻き込む、こういう土台づくり、土壌づくりだという懸念は拭い切れません。このことを最後に指摘して、質問を終わります。

○西村委員長　次に、河野正美君。

○河野（正）委員　おおさか維新の会の河野正美でございます。

まず、今回の法改正は、先ほど来お話もあっておりますように、日本年金機構による情報流出事案を契機として行われるものであり、早急に検討しておかなければいけない課題だというふうに考えております。

ただ、国の行政機関等を対象とする法律でありますが、衆参両院の立法府であるとか、あるいは最高裁判所以下の司法が対象の範囲外となっております。

サイバー攻撃を初めとしたセキュリティー対策が必要なのは、行政機関に限りません。これら対象外のサイバーセキュリティー対策についての現状と課題、実際どのようなリスクにさらされているのかについて、それぞれの立場でお答えいただきたいと思います。

○鹿村参事　本院におきましても、サイバーセキュリティー対策の重要性は十分認識しているところでございます。

ネットワークなどの監視強化や、新たなセキュリティー対策機器の設置、セキュリティーに係る意識啓発を図るための訓練等、さまざまな対策を実施してきております。

また、セキュリティーを確保するためには、内閣サイバーセキュリティセンターを初めとした政府機関との連携が極めて重要であると考え、立法府の独立性に配慮しつつ、従来から同センターとは緊密な連携を図ってきております。

同センターとの連携によって得られたさまざまな情報などを踏まえまして各種対策を実施することにより、中央省庁等の政府機関と同水準のセキュリティー対策を実施しているものと考えております。

以上でございます。

○木下参議院参事　お答え申し上げます。

本院におきましても、セキュリティー対策の重要性を認識し、立法府の独立性に配慮しつつ、政府機関と同水準の対策の実施に努めております。

具体的には、内閣サイバーセキュリティセンターを初めとした各機関と連携し、政府機関の情報セキュリティ対策のための統一基準群を踏まえ、各種セキュリティー対策製品の導入及び運用を行っているところであります。

以上でございます。

○安東最高裁判所長官代理者　お答え申し上げます。

裁判所といたしましても、サイバーセキュリティー対策の重要性は十分に認識しているところでございます。

事柄の性質上、詳細なお答えは差し控えさせていただきますが、サイバー攻撃に備えまして、物理的な対策、不正な通信の監視、分析等の技術的な対策をとるとともに、情報セキュリティーに関するルールを職員に遵守させる取り組みも行っております。

また、裁判所は、関連の政府会合にオブザーバーとして参加いたしまして情報を収集しますとともに、内閣サイバーセキュリティセンターとの間でも、種々の情報を相互に提供し合うなどして連携を図っているところでございます。

今後とも、関係機関と情報交換をしつつ的確な対策を講じてまいる所存でございます。

以上でございます。

○河野（正）委員　遠藤大臣に伺いたいと思いますが、立法、司法、行政それぞれがセキュリティー対策を進めるとともに、縦割りに陥ることなく、日々さらされているリスクにしっかりと向き合って、情報を共有し連携して取り組むことが国全体の情報セキュリティーの向上につながると考えますが、御見解はいかがでしょうか。

○遠藤国務大臣　お答えいたします。

今委員御指摘のとおり、サイバー攻撃が一層深刻化、巧妙化している中で、衆議院、参議院や最高裁判所を含め関係機関と情報連携をすることは大変重要であります。

政府においては、サイバーセキュリティ戦略本部のもとに設置されているサイバーセキュリティ対策推進会議にこれら立法、司法機関等にオブザーバー参加をしていただき、政府の取り組みについて随時情報提供の機会を提供するなど、情報共有体制を構築しているところであります。

さらに、情報セキュリティーインシデントに関して、標的型メール及び不正プログラムの分析並びにサイバー攻撃に関する最新情報の提供等を含め、関係機関に対して随時必要な助言を行ってお

ります。

今後とも、政府として、必要な協力を行うなど関係機関と連携してサイバーセキュリティーを確保し、国民が安全で安心して暮らせる社会の実現を図ってまいります。

○河野(正)委員　次に移りますが、立法府、司法以外でも、地方自治体もこの改正の対象から外されております。

こういったことから、日本年金機構の情報流出事案を受けて、総務省は、自治体情報セキュリティ対策検討チームを発足させ、昨年十一月には「新たな自治体情報セキュリティ対策の抜本的強化に向けて」と題する報告書を取りまとめていると思います。

しかしながら、その直後の十二月に、大阪府の堺市で過去最大規模の住民情報の流出事案というのが明らかとなっております。約六十八万人分の選挙関連データなど個人情報が流出したと言われております。

まず、総務省として、これまで取り組んできた自治体の情報セキュリティー対策の取り組み、そして堺市の情報流出事案を受けての対応をお聞かせいただきたいと思います。

○猿渡政府参考人　お答えします。

自治体情報セキュリティー対策の抜本的強化につきましては、まず、最高情報セキュリティー責任者、ＣＩＳＯの設置などを徹底するとともに、徹底したインシデント即応体制を強化するとともに、職員の訓練等の徹底等による人的な情報セキュリティーの確保体制の強化とともに、端末からの情報持ち出しの不可設定及び例外的持ち出しの際の明確なルールの設定及びチェック体制の確保など、さまざまな多角的かつ総合的な対策により、攻撃リスク等の低減のための抜本的強化策を進めているところであります。

先般の堺市の事案を教訓といたしまして、私どもは、改めて、端末からの情報持ち出しの不可設定やルールの明確、チェック体制の確保等々が必要であるということを再認識したところであり、これまで以上に自治体情報セキュリティー対策に万全を期していきたいと覚悟したところであります。

○河野(正)委員　堺市の事案が最初に発覚したのは、外部からの通報があった昨年六月の時点というふうに言われております。一旦は内部調査を進めましたが、外部流出なしという判断をされていたというような問題がありました。自治体内部のリスク管理体制の不備というのがあるんじゃないかと思わざるを得ません。

事故を完全にゼロとすることが難しい以上、不測の事態が生じた場合、いかに早急に問題を把握して対策をとり、リスクを減らしていけるかが大切なことだと思います。

そうした観点からの自治体情報セキュリティー対策が必要と考えますが、どのように捉えているか、お聞かせください。

○猿渡政府参考人　お答え申し上げます。

情報の流出が起こらないようにということで、平成二十七年度補正予算の補助金などを活用してセキュリティー対策の抜本的強化などを図っているところでございますが、絶対ということはあり得ないわけでありますので、流出を前提とした対策も当然必要でございます。

そこで、昨年の日本年金機構の事案等を踏まえまして、まず、標的型攻撃に係るインシデント初動マニュアルの作成を初め、インシデント連絡ルートの再構築、多重化などの即応体制の強化、また攻撃リスク等の低減のための抜本的なシステム強化及び、何といっても重要なのは人的セキュリティーの強化と職員の訓練の徹底ということでございまして、そういうふうな形での多重的、総合的な強化を図っているところでございます。

○河野(正)委員　今回の例では、外部通報者、通報者へのいわれなき中傷があったというふうにも聞いております。こうした情報提供者、通報者を守る仕組みなどは現在どのようになっているかを伺いたいと思います。

○井内政府参考人　お答え申し上げます。

今先生から御指摘がありましたように、行政機関外部からの通報は、行政機関の不祥事の発覚やその被害の拡大防止に重要な役割を果たすものと考えておりまして、このような通報の機能を生かすためには、行政機関の迅速かつ適切な対応とともに、通報者が安心して通報できる環境の整備が必要であります。

この点に関しましては、公益通報者保護制度を消費者庁が所管しておりますけれども、国におきましては、行政機関のガイドラインというものがございます。また、昨年六月から公益通報者保護制度の実効性の向上に関する検討会というのを実施しておりまして、検討会からは、地方公共団体向けのガイドラインの策定についても検討するようという意見が出されております。

○河野(正)委員　先ほど来、今回国家資格として導入される情報処理安全確保支援士のような専門人材を育成するということが言われておりますが、こういった待遇面での一定の評価などといった人材登用のための方策や、自治体における情報セキュリティーに関する専門人材のあり方について、政府、総務省の見解を伺いたいと思います。

○猿渡政府参考人　お答え申し上げます。

自治体における情報セキュリティー人材の育成につきましては、全ての自治体において、ＣＩＳＯ、最高情報セキュリティー責任者及びＣＳＩＲＴ、インシデント対応チームの設置を徹底するなど、各自治体の司令塔機能の強化をまず図ったところであります。

さらに、自治体情報セキュリティ支援プラットフォームなどを通じまして、各自治体における専門的人材と申しますか、そういう方々の育成を図るとともに、外部の高度な専門人材との通常時からの交流等により、専門知識のさらなる向上とインシデント発生時の即応能力の強化を図っているところであります。また、緊急時対応訓練の逐次実施や標的型攻撃などに対する訓練の徹底などにより、いわゆる職員の皆様全般の対応能力の向上にも努めているところであります。

なお、都道府県におかれましては、みずからの対策の充実とともに、市区町村に対する初動対応の支援体制を強化していただくことや、市区町村と協力して自治体情報セキュリティクラウドを構築し、市区町村とあわせて高度なセキュリティー対策をとるというような取り組みも進めておるところであります。

○河野(正)委員　時間が余りありませんので先に行きたいと思いますが、大規模な流出事案では、情報流出の被害を受けた住民が管理者である自治体を訴えて、一件につき一万円の慰謝料が認められたという例もあるようでございます。

政府として把握をされている実情を伺いたいと思いますし、あわせて、首長や職員個人が責任を問われる例があるのかどうか、お聞かせいただきたいと思います。

○猿渡政府参考人　お答え申し上げます。

今委員の方で御指摘いただいたのは、平成十一年の宇治市の個人情報流出事案の件だろうと思います。再々委託先のアルバイト従業員の行為につきまして、民法七百十五条の民事上の使用者責任に基づく宇治市の賠償責任が裁判によって認められたものでございます。

また、先ほど御指摘がありました昨年十二月の堺市の個人情報流出事案におきましては、事案を引き起こした職員に対しまして免職処分を科した上に、この三月二日付で、地方公務員法第三十四条、秘密を守る義務違反と、堺市個人情報保護条例第五十七条、不正盗用違反の刑事告訴がなされたものでございます。そういう事例は過去もあったかと思います。

ただ、このような刑事上、民事上の責任は当然のこととといたしましても、総務省といたしましては、地方公共団体における情報セキュリティポリシーに関するガイドラインにおきまして、情報セキュリティーの確保は住民に対する公的な重大な責務であるということを改めて確認を求めておりまして、各自治体におかれましては深く認識して対応していただくよう、繰り返しお願いをしてい

るところであります。

○河野(正)委員　最後にまた大臣にお伺いしたいと思いますが、先ほど来マイナンバーの取り扱いについてもお話がありました。国と同じ水準の情報セキュリティー対策のもと、そのセキュリティーの水準に、千を超える自治体があるわけですが、大きな差が生じることなく、国、地方を挙げた取り組みが重要であるというふうに思っております。

担当の遠藤大臣は、東京オリンピック・パラリンピック担当大臣でもいらっしゃいます。サイバーセキュリティー対策は二〇二〇年以降も国、地方とも継続してしっかりと取り組んでいかなければならない課題だと思いますが、見解を伺いたいと思います。

○遠藤国務大臣　お答えいたします。

地方公共団体についても、その行う業務は国民生活と密接な関係を有するものであり、サイバーセキュリティー対策を充実させる必要があります。他方、地方自治の本旨を踏まえ、国による関与については一定の配慮が必要と考えられます。

このため、地方自治体の提供する行政サービスについても、重要インフラの一分野と位置づけ、主要な対策について国として支援しているところであります。

また、基本法の規定に基づき、サイバーセキュリティ戦略本部は、地方公共団体の長に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることが可能であり、本部長は、提出された資料等を踏まえ、必要があると認めるときは関係行政機関の長に対し勧告することができることとなっております。

マイナンバー制度の本格稼働を踏まえ、地方自治体のセキュリティー対策の強化は極めて重要であり、関係府省と連携しつつ対策を推進してまいりたいと思います。

○河野(正)委員　時間が来ましたので、以上で終わります。ありがとうございました。

○西村委員長　次に、後藤祐一君。

○後藤(祐)委員　民進党の後藤祐一でございます。

まず冒頭、外国等による通信傍受について、最初は入りたいと思います。

きょうは木原外務副大臣にお越しいただいておりますが、昨年の八月ぐらいにウィキリークスから、米国の情報機関による通信記録が表に明らかになって、そこで報道されたことが事実だとすると、日本の大臣に対する通信傍受活動が行われていた、こういう報道がなされました。

これに対して、昨年の八月四日の岸田外務大臣の記者会見で「仮に報道されているようなことが事実であるとしたならば、極めて遺憾なことと思います。」「政府として、クラッパー米国家情報長官と連絡を取りあっているところですが、我が国としましては、引き続き事実関係の確認を強く求めていく所存です。」とお答えになられて、記者から、「その遺憾の意をアメリカの政府に伝えるということでしょうか。」と聞かれ、「まず、現段階では、事実を確認中であります。ですから、先ずは確認をしてからということだと思います。」というふうにお答えになられております。

それからしばらく時間がたったわけですが、日本の政府要人のどなたの通信傍受が行われていたんでしょうか。そして、行われていたということが事実なんだとすれば、これに対する米国側の説明があったのでしょうかということと、その時点からの今後について、通信傍受はしないというお約束は相手側からいただけたのでしょうか。その後のやりとりについて、木原副大臣から御説明いただきたいと思います。

○木原副大臣　お答え申し上げます。

今、八月四日の岸田外務大臣のお話を挙げていただきました。その後また、安倍総理とオバマ大統領との間でも本件について話をさせていただきました。

まず、幾つか御質問があったというふうに思いますが、米国の国家安全保障局による過去の日本に対する盗聴の有無につきましては、大変恐縮でございますけれども、政府の情報保全全般にかかわることでございますので、このことについて明らかにすることは差し控えさせていただきたいというふうに思います。

その上で、オバマ大統領に対して、安倍総理から、仮に日本の関係者が対象になっていたということが事実であれば、同盟国間の信頼関係を揺るがしかねないものでございまして、深刻な懸念を表明せざるを得ないということを伝達させていただきました。それに対しまして、オバマ大統領から、米国政府としては、二〇一四年の大統領令を踏まえ、しかるべく措置をとっており、現在、米国政府として、日米同盟の信頼関係を損なう行動は行っていないという趣旨の御回答をいただいているところでございます。

○後藤(祐)委員　過去何をやっていたかということがこの場で明らかにできないというのは、これについては、私は情報監視審査会の委員でもありますので、いろいろなやり方があると思います。

後段の方の、オバマ大統領側から、日米関係を損なう行動は行っていないという現在形でお答えになられたということは、将来にわたってこういった通信傍受活動は行わないという約束を米側がしたというわけではないということですね。

○木原副大臣　今、現在形で申し上げましたけれども、オバマ大統領が発言をされましたことは、二〇一四年の大統領令に従って米国は行動しているということでありますので、現在形でその時点ではお答えになったわけでありますから、当然、未来のことも含めてお答えになったというふうに理解をしてございます。

○後藤(祐)委員　理解をしておりますということは、その時点以降の将来に向けて、日本の政府要人に対して通信傍受活動は行わないとアメリカ側が約束したということでよろしいですか。

○木原副大臣　米国を含め他国の政策について、私どもが将来にわたってお話しすることはなかなか難しいということは御理解いただけるというふうに思いますが、少なくとも、二〇一四年の大統領令というのが出されて、それを現時点で改正していないということでございますので、この時点においては、将来に向けてそういう行動はとらないということを含意されているというふうに理解をしてございます。

○後藤(祐)委員　その二〇一四年の大統領令には、少なくとも、日本の政府要人に対しては通信傍受活動を行わないということが明記されているんですか。

○木原副大臣　米国の国家安全保障にかかわるものを除いて、外国の要人等に対するそうした行動については厳に慎んでいくということが示されていると理解をしてございます。

○後藤(祐)委員　そうすると、米国の国家安全保障にかかわることであれば通信傍受できるということですか。

○木原副大臣　米国の政策、そして大統領令の理解そのものについて、私がこの場で他国の法令について、その内容を事細かに申し上げるのはなかなか困難かというふうに思います。

ただ、国家安全保障上にかかわるものを除いてそういうことはやらないということを示されたというふうに理解をしております。

○後藤(祐)委員　非常に危うい状況であることが明らかになったと思います。

こういったこともあり得るので、政務三役の方も含めて、政府の要人、国家の安全保障を含めた機密情報に携わる可能性がある方々は、私的なメールあるいは私的な、特に携帯電話、こういったものを通じた機密情報のやりとりというのは大変危険なわけでありまして、これについて禁じる、メールだけじゃなくて、最近はネット上のさまざまなやりとりがありますが、メール等ネット上でのやりとりみたいなものと音声通話について、機密情報を扱う場合には私的な手段を用いてはならないということについて、政府全体のルールというものはどうなっているでしょうか。遠藤大臣、お願いします。

○遠藤国務大臣　後藤委員にお答えいたします。

私用の携帯電話端末による音声通話も含めて、適正な端末の利用が図られる必要があることは、政府としても当然認識しているところであります。

その上で、諸外国等により各種の情報収集活動が行われるおそれを念頭に、官房長官が議長を務める政府のカウンターインテリジェンス推進会議において、官房長官から対応に万全を期すよう指示が行われているところであり、各省庁はその指示に従って対応しているものと承知をしております。

例えば、機密性の高い情報を扱う職員に対しては、当該活動に対する危機意識を持つよう平素から厳しく指導するとともに、特に機密性の高い情報については暗号化の徹底を含む確実な漏えい対策を講じてきたところであります。

政府としても、今後とも情報の保全等に万全を期してまいります。

○後藤(祐)委員　やってくださいというお願いだけですか。政務三役を含めた政府要人の方々は私的メール及び私的携帯電話で機密情報を扱ってはならないということはルール化されているんですか。大臣、これは通告しています。

○谷脇政府参考人　お答え申し上げます。

まず、一般論として、政府に勤務する職員の業務上の情報というものを私用携帯等を用いて私的にやりとりするということにつきましては、統一基準に基づく各府省のセキュリティーポリシーでこれを禁止しているところでございます。

したがいまして、同様の取り組みが各府省政務においても徹底されることが当然に求められているというふうに考えております。

○後藤(祐)委員　つまり、政府統一ルールはないということですね。各府省に任せられているということですね。全二十二府省庁で定められているんですか。禁止されていますか、遠藤大臣。

○西村委員長　では、先にちょっと事務的に。

○谷脇政府参考人　お答え申し上げます。

私用携帯、スマートフォン等で業務上知り得た機微性のある情報を取り扱うということは、全府省において、これをセキュリティーポリシーにおいて禁じているというふうに承知をしております。

○後藤(祐)委員　これは通告しているんですから、大臣、はっきり答えてください。今の答弁を大臣がすればいいんですよ。

これは政務三役は全員知っていなきゃいけないはずなんです。この答弁を役所に任せるようでは、やっていないということなんじゃないんですか。だって、今のルールを政務三役の方は当然知っていて、こっちの携帯でかけなきゃ、常にそう思っていただかなきゃ困るはずで、それが各省庁で厳密なルールになっているということを遠藤大臣は知っていなきゃいけないと思いますよ。しかも、これは通告しているんですから。

我々の方からのディフェンスをきちっと上げていかないと、サイバーセキュリティーは守れません。

核セキュリティーサミット、ちょうど安倍総理が行っていますけれども、その中でサイバー攻撃についてもどの程度議論になるかわかりませんが、これについて一つだけちょっと、木原外務副大臣が来られていますので、お聞きしたいと思います。

実際、サイバー攻撃が日本に対してなされた場合、大変深刻な問題になり得ますが、これに対して何らかの反撃を日本側からする場合、これは国連憲章上の自衛権の行使に当たることがあり得るでしょうか。

○木原副大臣　サイバー空間を利用した侵害行為が発生した場合に、国連憲章上の自衛権の発動が許されるかどうかということは、すなわちそれが武力行使に当たるかどうかということであろうというふうに思います。

そのことについては、どのようなサイバー空間を利用した行為が武力行使や武力攻撃に該当するかということについて、今、核セキュリティーサミットの件も例に挙げていただきましたけれども、まさに国際的にもまだまだ、さまざまな議論が行われている段階でありますし、私たちのこの国においても、また各国において、まだまだ議論がされているところでありますので、現時点で一概にお答えするのはなかなか困難かというふうに考えております。

○後藤(祐)委員　実際、イスラエルがスタックスネットをやってイランをやっつけたというようなことも発生しているわけですから、これは現実にいつ起きてもおかしくない話。その場合に備えて、防衛省の中でもサイバー部隊がいるわけでありますから、これの法的な整理というのは既になされていなきゃおかしいんです。

今の答弁は、含まれる可能性を否定していないというふうに理解させていただきました。とするならば、これは自衛隊法に基づく防衛出動をかけるとか、そういう話にもなってくるわけですから、これについての整理は今後も議論していきたいと思います。

それでは、この法案の条文も含めて少し確認をしたいと思いますが、まず、情報処理安全確保支援士制度についてでございます。

先ほど平井理事から、名前が悪いというお話もありましたが、設置することはわかるんですが、各民間企業なんかにこの支援士を必ず置かなければならないといったような運用が将来仮になされたとすると、大変な負担になりますし、現実にそれだけの人材がいらっしゃるかどうかという問題もあります。

過剰にそこを義務づけるというのも、またこれは問題だと思いますし、この制度をどう定着させていくかというバランスもあると思いますが、将来的に必置にする考えというのがあるのかどうかを含めて、ここについての考え方を鈴木経産副大臣、お願いします。

○鈴木副大臣　企業等のサイバーセキュリティー対策を強化していく上では、経営者自身が取り組みの重要性を認識して、みずからの経営判断として、情報処理安全確保支援士やこれと同等レベルの専門人材を積極的に登用いただくことが重要であると思います。

したがって、情報処理安全確保支援士は必置義務ではなく、まずはサイバーセキュリティ経営ガイドライン等も活用しながら、企業経営者のサイバーセキュリティー対策の普及啓発を通じ、専門人材の活用を促進してまいりたいと思っております。

その上で、法施行後の状況等により、必置化の必要性は検討事項とはなり得るものの、その場合でありましても、全ての企業に必置を義務づけるのではなく、重要インフラなど、真に必要なところにのみ義務づけるべきと考えております。

以上です。

○後藤(祐)委員　最後のところは大事だと思うんですね。ごく少数の極めて重要なところの必置についての将来の可能性は否定しないけれども、それ以外の企業について必置にすることは考えていないということは、大変重要な答弁だと思います。

続きまして、今回の法案の中で、情促法の四十三条三項の改正ということについて質問したいと思います。

IPAは、サイバーセキュリティーに関する調査を行った場合、必要があると認めるときは、事業者その他の電子計算機を利用する者が講ずべき措置の内容を公表するものとすると、さらりと書いてあるんですが、何らの条件とか限定もしないで、IPAがサイバーセキュリティーに関する調査ですと言った場合には、何でも公表できてしまう。何でもというのは言い過ぎなのかもしれませんが、必要な場合には公表できてしまうという、非常に幅の広い規定であります。

念頭にあるのは、いわゆる脆弱性情報、このソフトにはこういうセキュリティーホールがありますよですとか、こういったことについては今までも通達レベルで実施をされてきておりまして、それはそれで意味のある運用だと思うんですが、法律で、機構に対し、何らの限定も付さないで、一

民間企業の、誰に対してもですよ、民間企業に限らないですね、どんな民間の方に対しても、おたくのこのソフト、こうけしからぬから公表しますという、ある意味非常に強い権限をこの法律でさらりと与えています。

これは、運用に関して、少なくともこういう目的だとか、例えば脆弱性情報しかやらないとかいう限定を何らか付さないと、ちょっとオールマイティー過ぎて、非常に危険な規定になりかねません。

この四十三条三項の運用に関して、例えば脆弱性に関する情報に限定するですとか、何らか、限定運用についての明確な指針を示していただきたいと思います。

○鈴木副大臣　公表を想定しております内容としては、ＩＰＡは平成十六年より、サイバー攻撃を仕掛ける際に使われるようなソフトウエア等の弱点、いわゆる脆弱性に関する情報の公表制度を実施しております。これにつきましては、法令の規定に基づくものとしてまいりたいと思います。

また、近年、利用者が入力した情報が意図せずソフトウエアの作成者に伝わる仕組みを持ったものが問題になっております。このようなソフトウエアにつきましても、脆弱性と同様に公表を行い、利用者に強く注意喚起をする必要がある。今後、法令の規定に基づく公表の対象として検討を進めてまいりたいと思います。

いずれにしましても、第四十三条第三項における公表につきましては、厳格にこれを解釈した上で、公表することの必要性について、専門家の判断も踏まえてその内容を限定してまいりたいと思っております。

○後藤（祐）委員　今の運用は、ソフトウエア等脆弱性関連情報取扱基準というものに基づいて脆弱性に限定した上で、公表判定委員会で審議、判定をするという極めて限定的な運用をされているとは理解しておりますが、今の答弁も、後段のところの広がる部分、脆弱性はないけれども何らかの危険性が発生するかもしれないというものを将来においてやる可能性があるということを私も否定はしませんが、例えばこういった判定委員会みたいなものできちっとチェックをするですとかいった運用をしっかりしていただくようお願いを申し上げたいと思います。

続きまして、いろいろ前後して申しわけありませんが、ＮＩＳＣの権限の話を先にしたいと思います。

今、各行政機関ですとか独立行政法人あるいは特殊法人等に対してＮＩＳＣはどういう権限を持っているかということについては、現行のサイバーセキュリティ基本法十三条で、「国の行政機関の情報システムに対する不正な活動の監視及び分析、国の行政機関におけるサイバーセキュリティに関する演習及び訓練」、これは「国は、」となっているので、各行政機関なのかＮＩＳＣなのかよくわからない形で条文があって、二十五条には、「所掌事務等」として、サイバーセキュリティ本部、この下にＮＩＳＣがあるということなんでしょうが、ここにおいて、「サイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）」こういう書き方になっております。

つまり、施策の評価は所掌事務でありますが、実際、各行政機関の中まで行って、そのシステムの内部における監視はできるのでしょうか。

事務方からの説明によりますと、各行政機関の外側に設置した、入り口部分に設置したもの、例えば先日の年金機構の件でも、入り口部分に設置したセンサーで、ＮＩＳＣが、これはおかしなことが起きているぞということに気づいてアラームを鳴らしたということですが、これは現行もやっているわけで、法律上もできるわけです。

この法律を見る限りにおいては、各行政機関なり独立行政法人なりのシステムの中における監視その他、不正な行動があったときに、ＮＩＳＣなりサイバーセキュリティ本部が何らか直接的な活動をするということはできない条文だと理解していますが、それでよろしいでしょうか。

○谷脇政府参考人　お答え申し上げます。

サイバーセキュリティ戦略本部及びＮＩＳＣが各省庁の同意なくしてシステムの内部に入り込んで監視等を行う権限は有していないと理解しております。

○後藤（祐）委員　同意があれば、ＮＩＳＣは、各行政機関あるいは独法の中に入って、みずから直接このシステムに対して手を加えたり、そういったことができるんですか、アドバイスとか勧告ではなくて。

○谷脇政府参考人　お答え申し上げます。

まず、できるかどうかということと、それが適切かどうかということ、二つの論点があろうかというふうに思っております。

一般論として申し上げますと、情報システムの構築及びそのセキュリティー対策というのは、組織の業務や取り扱われる情報に応じて最適化されるべき性質のものであるというふうに考えております。したがいまして、各府省庁におけるサイバーセキュリティー対策は、まずはみずからの問題として取り組むことが原則でございます。

もちろん、私どもの緊急支援チーム、ＣＹＭＡＴを派遣し助言を行う、あるいは場合によっては勧告を行う、こういったことによって対策の強化を促していくということも現行の枠組みにおいてできるというふうに理解をしております。

○後藤（祐）委員　ですから、そうではなくて、アドバイスですとか勧告ではなくて、ＮＩＳＣが直接行政機関内部のシステムをいじることが法律上可能かどうかという、法律の解釈を聞いております。

○谷脇政府参考人　お答え申し上げます。

各府省が構築、運用しております情報システムは、あくまでその府省の責任において構築、運用すべきものであるというふうに考えております。したがいまして、ＮＩＳＣがそこに出ていきまして、情報システムに直接タッチをし、そして遮断等の行為を行うということはないというふうに考えております。

○後藤（祐）委員　ないではなくて、法律上できないという理解でよろしいですか。遮断に限定しませんが。

○谷脇政府参考人　お答え申し上げます。

そのような事態を法律上想定していないというふうに理解しております。

○後藤（祐）委員　こういう建前を言っているから、サイバーセキュリティー問題が解決しないんですよ。

起きた場合に、自分たちで対応できない、緊急性があるようなときに、ＮＩＳＣが入っていって、みずから、こうやった方がいい、ああやった方がいいとアドバイスはできますよ。だけれども、そんなことをやっているよりもＮＩＳＣが直接やっちゃった方が早いという場合がもしかしたらあり得るかもしれないじゃないですか。それが法的に可能かどうか、その解釈を聞いているんです。あってはならない、想定していませんじゃなくて、そういうことがあった場合に法的に可能かどうかを聞いています。ごまかさないでください。これは通告していますから。

○谷脇政府参考人　お答え申し上げます。

各府省の情報システムを遮断するか、あるいは業務をその情報システムを使って継続するかどうか、これは各府省庁において判断すべきことでございます。したがいまして、ＮＩＳＣがサイバーセキュリティー上の観点からその省庁に乗り込み、同意を得たとしても、直接我々ＮＩＳＣが手を下して遮断するということは法律上は予定されていないというふうに理解しております。

○後藤（祐）委員　予定されておりませんという言い方ですが、要するに、できないんです。事務方にも、遮断に限らず監視行為も含めてこれはできないという説明をいただいています。

もちろん、各行政機関なり独法がみずから守るのが大原則、それは理解します。何でもかんでもＮＩＳＣにやって、それはよくない。だけれども、行政機関によっては、非常に人数が少ないところですとか、あるいは、物すごく高度な、予想

もしないような攻撃が起きて、各行政機関ではちょっと対応できないけれども、ＮＩＳＣは物すごい高度な対応能力を持っていて、直接手を下せばすぐにでもできるような状況ということもあり得るかもしれないじゃないですか。しかも、それを各行政機関なりの同意を条件にすれば、誰が困る話でもないじゃないですか。

だから、同意を条件にした上で、いざというときには、ＮＩＳＣは中に入っていって手を下すことができるということを法律上可能にしておくことは私は意味があると思うんですね。

これについては条文修正も含めていろいろな議論をしてきておるんですが、ぜひ、これは今後いろいろやっていく中でいろいろなことが起きると思います。余りかたくなになるのではなくて、こういうのは、想定していませんでしたは許されない世界ですから、どんなことがあっても法的にはできるようにしておけばいい話であって、法律をやる立法府では、そんな技術的な細かいことを我々は審議するべきではなくて、いざ何かが起きた場合に法的には対応できるようにしておくことが立法府としての務めだと思います。

遠藤大臣、今のやりとりを聞いて、今後、各行政機関あるいは独立行政法人等における内部のシステムに関して、緊急性ですとか対応能力の問題ですとかで直接手を下す必要が仮に発生をした場合にＮＩＳＣが対応できるように、今回の法案でどうするかということはちょっとおいておいて、将来におけるその検討はすべきだと思いますが、大臣としての所感を聞きたいと思います。

○遠藤国務大臣　お答えいたします。

基本的には、先ほどの谷脇審議官の答弁のとおりでありますが、インシデント発生時に各府省庁が適切に対処できるよう、ＮＩＳＣにおいてはまず各省庁における人材、体制等の能力構築を支援していくとしておりますが、インシデント発生時に講ずべき具体的な措置のさらなる可能性については、今委員御指摘の点もありましたので、引き続き検討してまいります。

○後藤（祐）委員　サイバーセキュリティ基本法は、先ほど平井理事もおっしゃっておりましたけれども、議員立法でできた法なんです。私は、本来、議員立法でできた法を閣法で直すのはいかがなものかと思いますけれども、ぜひ、これから安全保障との関係ですとかいろいろな課題が実はありますので、これは、議員立法で今後いろいろな論点を含めて修正していく、その中で今の話も改正をしていくべきではないかということを申し上げておきたいと思います。

それでは、日本年金機構における情報流出に関連して、それそのものというよりは、こういったことが二度と起きないようにするためにどういう体制がとられているかということについての確認をしていきたいというふうに思います。

まず、標的型メールによる攻撃というのは、先ほど平井理事もおっしゃっていましたけれども、レベルとしてはそれほど高いレベルの攻撃ではないというお話がございました。ところが、やられてしまったわけです。

これには幾つかの原因がありますが、昨年の八月二十一日の、日本年金機構における不正アクセスによる情報流出事案検証委員会というところが検証報告書というのを出しております。これは、私のような文系の人間でも非常にわかるように書いてありまして、役に立つんです。

これは遠藤大臣に伺いたいと思いますが、この中に、こういう原因があったんじゃないか、あるいはこういう対策を今後とるべきじゃないかとたくさん盛り込まれておりますが、この検証報告書で掲げられているような提言も踏まえて、昨年の日本年金機構に対して行われたようなサイバー攻撃と全く同じような攻撃が仮にあった場合、各行政機関、各独法、特殊法人等で防御することはできる状態になっているんでしょうか。

○遠藤国務大臣　お答えいたします。

さきの年金事案における原因究明調査を通して得られた教訓については、その重要度や対策に要する時間や費用を踏まえた上で、着実に対策として実施すべく、昨年九月に閣議決定されたサイバーセキュリティ戦略に盛り込まれたところであります。具体的な対策例としては、業務の内容や取り扱う情報の性質、量に応じた情報システムの分離や、政府機関の情報システムにおけるインターネットの接続口の集約化、インシデント対処能力の向上等が挙げられます。

ＮＩＳＣにおいては、これら対策について各種会議を通じて実施を促すとともに、実施状況や予算要求状況の調査、マネジメント監査やペネトレーションテストによる履行状況の確認等を行いつつ、各省庁における着実な実施を図っているところであります。

○後藤（祐）委員　やってくださいねということは言っているけれども、実際にこの攻撃が起きたときに、各機関で守られる状態になっているということを確認はしていないということですか。

○谷脇政府参考人　お答え申し上げます。

ただいま大臣の方から御答弁申し上げましたように、情報システムの分離ですとか、インターネット接続口の集約化、あるいはインシデント対処能力の向上といったようなことを各省庁に対策としてお願いをしているところでございまして、各年の予算要求、予算措置、あるいはシステムの入れかえ、こうした時期を捉まえまして、対策を順次講じてきていただいているというふうに理解しております。

○後藤（祐）委員　同じ答弁をしないでください。実際、それが終了して、同じ攻撃が起きたときに守れる状態になっているのかどうかを聞いているのであって。

大臣に伺います。これは通告しています。すごく重要な話なんです。大したレベルでない攻撃が、全く同じことが起きたときに、やはりやられちゃうかもしれないなんていうのはあり得ないですよ。ちゃんと守れる状態になっているかどうかということについて、もう一度、大臣、御答弁いただきたいと思います。

○遠藤国務大臣　今委員から、確認を行っているのかという御指摘がありました。

ＮＩＳＣは、マネジメント監査を実施した府省庁に対して監査結果を通知し、当該府省庁は改善計画をＮＩＳＣに提出することとしております。また、ＮＩＳＣは、後年度、当該府省庁の改善計画に基づく改善の状況について確認を行うこととしております。

○後藤（祐）委員　確認を行うこととしております、未来形。すなわち、現段階では確認できていないということでよろしいですか、大臣。

○遠藤国務大臣　時間がかかるものについては途上ではありますが、応急対策については済ませております。

○後藤（祐）委員　途上なんです。これが非常に深刻なんです。大したレベルの攻撃じゃないんです。それすら、まだ対策が途上であるということが今明らかになったわけです。

確かに、お金のかかる問題ですし、途上のものがあることはしようがないかもしれませんが、まず、こういうレベルの低いものですら守れない状況にあるという自己認識のもとに、しっかり講じていただきたいと思います。

では、どういうレベルに達すればそれができるのかということについて、先ほどマネジメント監査の話がありましたが、ＮＩＳＣから、このマネジメント監査について何をやっているんですかと聞いても、こういう項目について見ていますという御説明はいろいろいただけますが、それはふわっとした話なんです。

この検証報告書はもっと具体的なことが書いてあって、例えば、今お配りの資料の、字がいっぱい書いてある方のページに、私が素人なりにこの検証報告書から、こういったことが原因、あるいはこういった対策をとるべきではないかということがいろいろ書いてあって、十七個ぐらい挙げさせていただきました。

一つ目と二つ目は、その裏側にある、これは地方公共団体のセキュリティー対策でよく言われている、インターネット接続系統と大量な個人情報

が保管されている系統をちゃんと分離してくださいねという話と、大量な個人情報は持ち出し不可という形にしてくださいねと。まさにこういうことを自治体に対してもやっていただいているわけですが、それが字のいっぱい書いてある方のページの一つ目と二つ目で、これは先ほどの答弁にもありました。ほかにも、暗号化について、三ポツぐらいまでは答弁がありました。

ＣＳＩＲＴの制度が設けられているかとか、十分な権限を付与されているかとか、あるいは、標的型攻撃によるインシデントに対応できるような監視が常時行われているかですとか、サイバー攻撃等のインシデント発生時における緊急時対応に関する具体的なサービス内容についての明確な合意はなされているか等々、私みたいな文系の人間が読んでもそれなりにはわかる程度のものが幾つか並んでいて、こういったものがちゃんとできていますかというようなチェックをＮＩＳＣから各行政機関なり独法等に対して行っているんでしょうか。

これも通告していますから、大臣にお伺いしたいと思います。審議官に聞いても抽象的なことしか答えませんから、大臣にお聞きしたいと思います。

○谷脇政府参考人　お答え申し上げます。

委員がお配りいただいている資料でございますけれども、出典のところにございますように、これは厚生労働省の第三者検証委員会の報告書であるという点をまず言及させていただきたいと思います。ＮＩＳＣが取りまとめました原因究明の調査報告書につきましては、これとは別にまとめているということでございます。時期は、ほぼ同じ時期でございます。

なお、ＮＩＳＣの原因究明の調査報告書におきましても、さまざまな改善すべき措置というものを書いているところでございまして、これに基づきまして、短期的にとれる措置、それから中期的にやるべきことを分けて、中期的にやるものについては、先ほど申し上げたインターネット接続口の集約化のように戦略に盛り込み、今着実に実施している、こういった取り組みをしているところでございます。

○遠藤国務大臣　具体策につきましては、対応の選択肢の中から、システム、業務、情報に応じて各種組織において判断されております。

ＮＩＳＣ監査につきましては、判断の妥当性について、主にそのプロセスを確認しております。

○後藤（祐）委員　大臣、ぜひ、文系でもわかる程度のことですから、これをちゃんとやっているのかどうか調べろと部下に指示してください。どの程度できているかということについて、ここで言いにくいという事情があるのは私理解します。ですが、こういう項目についてお願いしていますという説明は余り意味がないんです。

実際、それでどれだけ完了していて、どれだけやり途中で、何が足りないのかということを大臣に報告させしめてください。そのために私は、検証報告書から、これだけじゃないと思いますけれども、比較的わかりやすい項目を抽出しましたので、別にこれに従う必要はありませんが、こういう項目についてチェックしていますじゃ意味がないんです。これを具体的にやっているかやっていないかというデジタルな基準にしていかないと、実際に守れることになりません。ぜひここは大臣のリーダーシップを発揮していただきたいと思います。

きょうは太田厚労大臣政務官にもお越しいただいておりますが、せめて厚生労働省は、年金情報の流出事件を受けて、所管の三十二法人について、この報告書を踏まえて、例えば今私が配付させていただいた基準を満たしているかどうか、こういったチェックをした上で、同じような攻撃を受けても、厚生労働省本省も含めて、所管法人では同じような事件は起きないということになっているでしょうか。

○太田大臣政務官　お答え申し上げます。

先ほど来御指摘いただいておりますような検証委員会での検証結果を踏まえまして、私ども、厚労本省と、年金機構を初めとした個人情報を扱う法人が全部で三十数個ございますけれども、それらを含めまして、サイバー攻撃を受けたときにしっかりした対応ができるように今体制を整えつつあり、また、指導もやっております。体制はほぼ整いました。

まず、ＣＳＩＲＴにつきましては、厚労本省の中において、これまでの四人体制から十人体制にいたしまして、責任の所在もはっきりさせました。それと同じようなことを年金機構にもやらせております。

それから、標的型のメール攻撃にしっかり職員が対応できるように、危機意識の醸成や、リテラシー向上のための教育訓練の充実も行いました。これはもうここ一年余りにわたりましてさまざまな教育訓練、研修を行ってきております。そしてまた、インシデントが発生した場合の連絡体制の迅速な稼働、これについても訓練等を含めて行っております。

そして、所管の法人に対しましても、インシデント発生時における当該法人と厚労省との役割分担の明確化、また、報告、連絡のオペレーションの改善等々についても力を入れて、これまでにも既に実施をいたしております。

先生おっしゃっておりますような、それほど高度なレベルでない攻撃型のサイバー攻撃に対してしっかりと対応できるように、これからも危機意識を持って対応していきたいと考えております。

○後藤（祐）委員　この検証報告書をぜひ読んでいただいて、そうすると、さっきの私のような項目が出てきますから、ちゃんとこれはできているのかとチェックしてください。よろしくお願いします。

最後に、私はもとは経済産業省にいたんですけれども、同じようなウイルス目的のメールをもらったことがあります。添付ファイルがついていました。何でこれが来たのかなというと、メールアドレスが単純なんです。ゴトウユウイチ・アット・メティ・ジーオー・ジェーピー。職員名簿なんて世の中にありますから、要は、悪いことをする人は、職員名簿さえあれば、ああ、ここの役所はこういうルールでやっているなというので、簡単に大量なメールを職員に対して送ることができちゃうんです。役所によっては、乱数を入れたりして簡単にできないようにしています。でも、役所によっては単に名前だけ。ハイフンで結んだり、下のバーだったりしますが。

私が調べたところ、二十二省庁のうち十一省庁は、単純に姓と名のアドレスをつけています。これは改めるべきじゃないでしょうか。少なくとも、標的型メールのディフェンスとしては、数がたくさん入るということはすごく重要なので。ちょっとメールアドレスが変わるというのは仕事上厄介なことではあるかもしれませんが、半分は対応しているんですから、残りのところについて、しかも重要な省庁が含まれますからあえて申し上げませんが、これは少し検討すべき課題だと思います。遠藤大臣、御見解をいただきたいと思います。

○遠藤国務大臣　先ほど、大臣として確認を受けろという話であります。私は文系ではありますが体育会系でもあって、後藤委員は大変優秀な文系でいらっしゃいますが、各省庁において講ぜられている多様な策については、今後、しっかり確認をし、報告を受けたいと思っております。

また、今委員御指摘ありました、メールアドレスを複雑にすることによって、外部からのメール攻撃を一定程度抑止する効果はあるものと考えております。

しかしながら、今御指摘のように、政府機関職員のアドレスは、職務上、外部に対して比較的広範囲に告知されているものであるため、攻撃を抑止するための効果は限定的と考えざるを得ない部分もあるかなと。

したがって、こうした対策は、業務上の要求と必要なセキュリティーを比較考量しつつ各組織において考えるべきものでありますが、今委員御指摘のように既に対応しているところもあるようで

ありますから、ＮＩＳＣとしても、こうした取り組み事例として推奨する等、各府省庁に対してよい取り組みを促してまいりたいと考えております。

○後藤（祐）委員　終わります。ありがとうございました。

○西村委員長　これにて本案に対する質疑は終局いたしました。

○西村委員長　これより討論に入ります。

討論の申し出がありますので、これを許します。池内さおり君。

○池内委員　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に対する国による監視、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、こうした国が行う演習、訓練、監視、監査、原因究明調査等の対象を、独立行政法人や指定する特殊法人等に拡大するものです。

昨年の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の問題は、厚労省や年金機構のそもそもの業務のあり方が反映したものであり、サイバーセキュリティーについての監査、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。閣議決定されたサイバーセキュリティ戦略でも、各省の主体的管理、自律的メカニズムの構築、運用が基本とされています。

年金流出のケースをもってして全独立行政法人や特殊法人に演習や訓練、監視、監査の対象を拡大することは、国の演習や訓練への動員、監視、調査を際限なく拡大することにつながり、認められません。

さらに、現行法の目的には「我が国の安全保障」が明記され、サイバーセキュリティーを軍事、安全保障に密接に結びつけ、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て、昨年四月の新日米防衛協力のための指針、いわゆるガイドラインは、サイバー空間に関する協力を初めて明記しています。

日米政府が、民間との情報共有、おのおののネットワーク及びシステムを監視する態勢を維持、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するとして、サイバーセキュリティ戦略の年次計画、サイバーセキュリティ二〇一五でも、米国とのサイバー攻撃に関するデータの共有及び研究開発の協力関係の加速化、情報共有の強化などとされ、実際に、戦略本部の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、アメリカにも共有をされており、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。

なお、更新制の情報処理安全確保支援士制度の創設などについては当然の措置と考えますが、そのことをもって法案全体に賛成できるものではありません。

以上、反対討論といたします。（拍手）

○西村委員長　これにて討論は終局いたしました。

○西村委員長　これより採決に入ります。

内閣提出、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いたします。

本案に賛成の諸君の起立を求めます。

〔賛成者起立〕

○西村委員長　起立多数。よって、本案は原案のとおり可決すべきものと決しました。

○西村委員長　この際、ただいま議決いたしました本案に対し、平井たくや君外三名から、自由民主党、民進党・無所属クラブ、公明党、おおさか維新の会の共同提案による附帯決議を付すべしとの動議が提出されております。

提出者から趣旨の説明を聴取いたします。緒方林太郎君。

○緒方委員　ただいま議題となりました附帯決議案につきまして、提出者を代表して、その趣旨を御説明いたします。

案文の朗読により趣旨の説明にかえさせていただきます。

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、本法の施行に当たっては、次の諸点に留意し、その運用等について遺漏なきを期すべきである。

一　内閣官房内閣サイバーセキュリティセンター及び独立行政法人情報処理推進機構は、サイバーセキュリティ対策を着実に実施するために必要かつ十分な人員、予算を継続的に確保し、サイバーセキュリティ戦略を着実に実施すること。

二　国の行政機関、重要社会基盤事業者等をはじめとする企業等においてサイバー攻撃からの防御を担う実践的かつ高度な専門人材の確保・育成に向け、産学官が連携して人材育成に取り組む体制を整備すること。

三　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行うため、インシデント発生時において緊急に必要となる措置、重要社会基盤事業者等におけるインシデント情報の迅速かつ省庁横断的な共有等、サイバーセキュリティ対策の実施に係る枠組みの更なる強化に向けて必要となる施策を講じること。

四　地方公共団体の扱う住民情報等の重要性に鑑み、地方公共団体のサイバーセキュリティに係る人的体制及び技術的体制の整備及び充実のため、必要な協力等を行うこと。

五　国の行政機関、独立行政法人及び指定法人の情報システムの内部におけ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、当該行政機関等が同意した場合には、内閣官房内閣サイバーセキュリティセンター及びその委託を受けた法人が必要な対応を行うこと。

六　この法律の施行後二年以内に、サイバーセキュリティ基本法の施行の状況及び五をはじめとした本附帯決議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ものとすること。

以上であります。

何とぞ委員各位の御賛同をお願いいたします。

○西村委員長　これにて趣旨の説明は終わりました。

採決いたします。

本動議に賛成の諸君の起立を求めます。

〔賛成者起立〕

○西村委員長　起立多数。よって、本案に対し附帯決議を付することに決しました。

この際、本附帯決議に対し、政府から発言を求められておりますので、これを許します。遠藤国務大臣。

○遠藤国務大臣　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思います。

ありがとうございました。

○西村委員長　お諮りいたします。

ただいま議決いたしました本案に関する委員会報告書の作成につきましては、委員長に御一任願いたいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○**西村委員長**　御異議なしと認めます。よって、そのように決しました。

〔報告書は附録に掲載〕

○**西村委員長**　次回は、来る四月一日金曜日午前八時五十分理事会、午前九時委員会を開会することとし、本日は、これにて散会いたします。

午後零時十二分散会

平成二十八年四月二十一日印刷
平成二十八年四月二十二日発行
衆議院事務局
印刷者　国立印刷局
K