第二百十二回国会　衆議院　総務委員会議録　第三号

令和五年十一月九日（木曜日）

午前九時開議

出席委員

委員長　古屋　範子君

理事　井原　巧君　理事　田所　嘉徳君

理事　田中　良生君　理事　根本　幸典君

理事　石川　香織君　理事　奥野総一郎君

理事　中司　宏君　理事　中川　康洋君

東　国幹君　石田　真敏君

尾身　朝子君　金子　恭之君

川崎ひでと君　国光あやの君

小森　卓郎君　斎藤　洋明君

坂井　学君　島尻安伊子君

新谷　正義君　橘　慶一郎君

寺田　稔君　中川　貴元君

西野　太亮君　葉梨　康弘君

長谷川淳二君　藤井比早之君

古川　直季君　本田　太郎君

保岡　宏武君　おおつき紅葉君

岡本あき子君　神谷　裕君

重徳　和彦君　道下　大樹君

湯原　俊二君　阿部　司君

中嶋　秀樹君　吉田とも代君

平林　晃君　西岡　秀子君

宮本　岳志君　吉川　赳君

総務大臣　鈴木　淳司君

総務副大臣　渡辺　孝一君

総務大臣政務官　小森　卓郎君

総務大臣政務官　長谷川淳二君

政府参考人（内閣官房内閣審議官）　飯島　秀俊君

政府参考人（総務省大臣官房総括審議官）　湯本　博信君

政府参考人（総務省自治税務局長）　池田　達雄君

政府参考人（総務省国際戦略局長）　田原　康生君

政府参考人（総務省総合通信基盤局長）　今川　拓郎君

政府参考人（総務省サイバーセキュリティ統括官）　山内　智生君

参考人（国立研究開発法人情報通信研究機構理事長）　徳田　英幸君

総務委員会専門員　阿部　哲也君

委員の異動

十一月九日

辞任

補欠選任

石田　真敏君　橘　慶一郎君

西野　太亮君　東　国幹君

同日

辞任

補欠選任

東　国幹君　西野　太亮君

橘　慶一郎君　藤井比早之君

同日

辞任

補欠選任

藤井比早之君　石田　真敏君

本日の会議に付した案件

政府参考人出頭要求に関する件

参考人出頭要求に関する件

国立研究開発法人情報通信研究機構法の一部を改正する等の法律案（内閣提出第六号）

○古屋委員長　これより会議を開きます。

内閣提出、国立研究開発法人情報通信研究機構法の一部を改正する等の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、参考人として国立研究開発法人情報通信研究機構理事長徳田英幸さんの出席を求め、意見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〕

○古屋委員長　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、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飯島秀俊さん、総務省大臣官房総括審議官湯本博信さん、自治税務局長池田達雄さん、国際戦略局長田原康生さん、総合通信基盤局長今川拓郎さん及びサイバーセキュリティ統括官山内智生さんの出席を求め、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〕

○古屋委員長　御異議なしと認めます。よって、そのように決しました。

○古屋委員長　これより質疑に入ります。

質疑の申出がありますので、順次これを許します。川崎ひでとさん。

○川崎委員　おはようございます。自由民主党の川崎ひでとです。

今日は、質問の機会をいただき、ありがとうございます。

私自身は、今、自由民主党のサイバーセキュリティープロジェクトチームに所属しており、今回のこの法案、通称ＮＩＣＴ法改正案については大変興味があります。今日は時間の限り精いっぱい質問させていただきますので、よろしくお願いいたします。

まず、スマホが普及し、あらゆるものがネットと接続するＩｏＴ社会が広がる現代において、サイバーセキュリティーの重要性は日に日に増しております。

一方で、サイバーアタックの脅威については、国民の方の理解が果たしてあるかというと、ちょっとそこは甚だ疑問が生じます。ニュース等でサイバーアタックがあったということは知れますが、どのような被害があったのか、あるいは危険性がどういうものであったのかという部分については余り教示されていないのか、国民の理解度が低いというふうに思います。逆に、詳しく説明してしまうと横文字だらけになって懸念されてしまう、こういう部分もあると思います。

まずは、一つ目の質問として、今回の法案の対象となっているＩＤ、パスワードに脆弱性のある機器、これが一体何なのかという、この定義と、それに対するサイバーアタックの発生で一体何が起こってしまうのかというのを、我々の目線、つまり生活者の目線で是非お答えいただきたいというふうに思います。

この質問については、自民党で共にデジタル関係をやっておりました小森大臣政務官にお伺いしたいと思います。

○小森大臣政務官　御質問をいただき、ありがとうございます。

御質問のありましたＩＤ、パスワードに脆弱性のあるＩｏＴ機器でございますけれども、こちらにつきましては、例えば御家庭ですとか企業でルーターですとかネットワークカメラといったようなＩｏＴ機器が使われているわけでありますけれども、このうち、ＩＤですとかパスワードというのがこれらに設定されているものがありますけれども、これが単純な英数字の羅列など容易に推測されやすいものでありますと、脆弱性があるものとして念頭に我々は置いているところでござい

ます。

こうしたＩｏＴ機器の問題でございますけれども、悪意のある者によってこれらがマルウェアに感染させられた場合には、利用している人たちが知らないうちにサイバー攻撃にこうした機器が加担してしまうといった危険性があるところでございます。

そしてまた、それにとどまらず、ＩＤ、パスワードに脆弱性がある場合の問題としては、例えばネットワークカメラで撮影された映像が外部に漏れてしまうなど、機密情報あるいは個人情報を窃取されるリスクもあるといったものでございます。

○川崎委員　ありがとうございます。

まず、実は、サイバーアタックの脅威の共有というのが一番重要だというふうに思っています。何となく、パスワードやＩＤを抜き取られると、国民の目線からすると、何だか知らないものを買われてしまうんじゃないかとか、あるいは自分の銀行からお金がなくなってしまうんじゃないかとか、自分としてのリスクばかりを考えてしまいますが、実は、広く見ると、本当に日本の国力にも大きく影響がある、まさに国益を損なうものでありますので、まずはこの部分を皆様と共有させていただきたく、一つ目にこの質問をさせていただきました。

では、二つ目の質問をさせていただきます。

今回、この法案は、令和五年度が期限となりますが、それを延期するというのが本法案改正の趣旨だというふうに理解しております。

延期をするということは、この法案そもそもに効果があったからなのではないかというふうに理解をしておりますが、現行のこの法案が施行した後のＮＯＴＩＣＥの成果並びに評価についてお伺いいたします。

○山内政府参考人　お答え申し上げます。

ＮＩＣＴでは、二〇一八年に成立をした今御指摘の改正ＮＩＣＴ法に基づきまして、二〇一九年から、今年度末までの時限の業務として、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査を実施してまいりました。

この調査は、国内のインターネットに直接接続されております約一億台のＩｏＴ機器を対象に実施しております。ＩＤ、パスワードに不備のある機器が接続されたＩＰアドレスを今までに累計十万件以上、電気通信事業者に通知しております。

通知を受けた電気通信事業者においては、不備のあるＩＤ、パスワードの変更等を行うよう、個別の利用者への注意喚起を行っております。

また、設定に不備が多く見つかった機器、調査の過程の中でこういう機器が見つかった場合にはメーカーにも働きかけを行い、初期パスワードの変更をしなければその後の操作ができないなどのセキュリティー機能の強化をした製品の提供にもつながっております。

これらの取組によりまして、少なくとも数万台規模と推定をしておりますこのようなＩｏＴ機器について、ＩＤ、パスワードの脆弱性の解消に資する成果が上がったものと受け止めております。

他方で、サイバー攻撃の手法も年々巧妙化をしております。従来になかった通信経路、それから新たなＩＤ、パスワードの組合せを狙った攻撃というものも発生しているということが分かっております。したがいまして、調査対象を拡大しながら対応してきておりまして、結果として、調査で見つかっている脆弱性のある機器の数はなかなか減らない状況にございます。

このため、少なくとも脆弱性のあるＩｏＴ機器の数が増えないようにするため、こうした取組を粘り強く続けていく必要があると考えております。

○川崎委員　ありがとうございます。

確かに、ＩｏＴ端末がどんどん増えれば増えるほどそうした危険性があると思いますので、私自身もこの法案を延長すべきだということは強く感じております。

一方で、じゃ、ずっとそのままほっておいて、ＮＯＴＩＣＥの方で検知をしていくかというと、やはりそこは根本的な解決にはならないというふうに思っております。脆弱性の高い機器をやはり減らす、これをやっていかなければならない。

脆弱性の高い機器を減らす方法として、やはり件数を減らすためには、一つ目には、端末のセキュリティーを高めるようにメーカー、ベンダーにそれぞれ御協力いただいて、しっかりと機器の安全性を保つということ、それ以上に、ＩＤ、パスワードを設定する個人個人の意識、これを高めないことには件数は減らないというふうに思っています。総務省として、私が今御提示したこの二点について相違はありますでしょうか。まず、この辺りをお伺いいたします。

○山内政府参考人　お答え申し上げます。

今委員御指摘のとおり、実際に機器を減らす取組を行うためには、メーカー、作っている方、それから利用する方、利用者の双方の取組が重要であるというふうに認識をしてございます。

特に、メーカーにつきましては、機器の脆弱性に関する情報、それからセキュリティーに関する対策プログラムの提供、場合によって製品のサポートが終わる場合がございますので、こういう場合には終わるということを周知していただく、利用者が対応するために必要なサポートを提供していただくということと、利用者が意識をしなくともセキュリティーが確保される製品の開発などに取り組むということが求められるというふうに考えてございます。

メーカーと利用者による取組に加えまして、例えば利用者が法人、いわゆる企業ユーザーの場合でございますが、ＩｏＴ機器の設置、管理を外部委託しているというケースが多くございます。こういう場合には、設置、管理等を担っているシステムベンダー等の方においてＩｏＴ機器に適切なセキュリティー対策を講じていただくこと、これを促すことも効果があるというふうに考えてございます。

これらを踏まえまして、今回の法案では、通信事業者への通知を今まで、従来行ってまいりましたが、これに加えまして、メーカーやシステムベンダー等の関係者への情報提供それから助言についてもＮＩＣＴの業務として法的に位置づけることとしております。これによりまして幅広い関係者を巻き込んだ対策を一層促進いたしまして、より大きな成果を上げるべく取り組んでまいりたいと考えております。

○川崎委員　ありがとうございます。

これまでは、ＩｏＴ機器のメーカーであったり、あるいはＩＳＰ事業者の方に訴えをされていたというふうに御発言いただきましたが、今回のこの法案において、それ以外にアプローチする先というのは改めてあるんでしょうか。

○山内政府参考人　ありがとうございます。

今申し上げましたとおり、今まで、従来ですと、特に利用者、個別の利用者に対する注意喚起ということを行ってまいりました。先ほど申し上げましたが、これに加えまして作っている方、ベンダーの方、そして今まで注目をしてまいりました法人ユーザーの方がなかなか、実際に責任を持っている方がどなたかお分かりにならないという場合がございます。この場合には、管理に責任を持っているシステムベンダーの方、こういう方を巻き込みます。情報を持っている関係の方にはセキュリティーのベンダーといった方々もいらっしゃいますので、こういう幅広い関係者の方を是非巻き込んで対応していきたいというふうに考えております。

○川崎委員　ありがとうございます。つまり、今回の法案は、単に延期するだけではなくて、しっかりと通知の対象者も増やして、より強固なセキュリティーを図っていくということで理解いたしました。

一番最初に申し上げましたけれども、サイバーアタックの具体的な脅威、これを小森政務官に共有いただきましたが、この質問をした意図は、今日ここに参加されている総務委員の皆様に対して、サイバーアタックの具体的な脅威、これをしっかりと共有するということが非常に大切だと

いうふうに思っております。

実は、私は地元でここ最近国政報告会を何度かさせていただいておりますが、この国政報告会の中で、今話題になっているマイナンバー制度、これについて丁寧に説明すると、ああ、なるほどねと、すごく理解を示してくれます。いかに政治家が情報共有をしっかりとするかというのが大切なのかということを改めて理解いたしました。

そうした観点からすると、ＩＤ、パスワードを設定する個人の意識を高めるためにも、共有というのは非常に重要なんだと思います。総務省として、なぜサイバーセキュリティーが重要なのか、なぜ一人一人が意識を高めなければならないのか、これを国民の皆様にしっかり共有していただきたいというふうに思います。この点において、総務省としての意気込みを小森政務官から是非お伺いしたいと思います。

○小森大臣政務官　御指摘いただきましたとおり、ＩｏＴ機器のセキュリティー対策を推進していく上で、我々の取組のＮＯＴＩＣＥに関する情報発信を強化して国民の理解を向上させていくことは重要な課題であるというふうに認識しているところでございます。

国民の皆様には、先ほど申し上げましたが、御自身が利用するＩｏＴ機器がサイバー攻撃に加担するおそれがあるということを広く知っていただいて、セキュリティー対策を自分事としてしっかり行っていただきたいというふうに考えております。

そのため、ＮＯＴＩＣＥの情報発信の強化とともに年度内に新たな広報戦略を策定することを考えておりますけれども、これを通じまして、ＩｏＴ機器のセキュリティー対策の重要性について国民の皆様の誰もが理解できるような周知啓発を進めるなど、理解の向上に取り組んでまいりたいと思っております。

○川崎委員　ありがとうございます。あらゆる手段を使って、国民の皆様に総務省の取組やサイバーセキュリティーの重要性がきちんと届くように是非努めていただきたいというふうに思います。

次の質問に参ります。

今回、ＩＤ、パスワード以外に脆弱性を有するファームウェアというものも対象になったというふうにされておりますけれども、実は、このファームウェアという単語が、更にまたぴんとこない単語になっています。具体的にどういうものを指すのか、これを例示いただけますでしょうか。

○山内政府参考人　お答え申し上げます。

御指摘のファームウェアとは、分かりやすく申し上げますとソフトウェアとハードウェアの中間的な存在、具体的に申し上げますと、ＩｏＴ機器を制御するために搭載されているソフトウェアのことを指しております。今御指摘がございましたが、ファームウェアを狙いますと制御権を取られてしまうということが起きるものですから、この脆弱性を狙ったサイバー攻撃が増加している状況にございます。

○川崎委員　御説明ありがとうございます。理解はさせていただきましたけれども、非常に難しい単語だったというふうに思いました。これこそまさに分かりやすく、例えばウィンドウズの古いＯＳだとか、こういう表現をしっかり使っていかないと国民の方は理解できないというふうに思います。是非、難しい単語ではなくて、分かりやすい啓発をよろしくお願いしたいと思います。

それでは、最後の質問にいたします。

今回、マルウェアに感染した機器も検知し、その機器を有する会社に連絡するという運用だというふうに理解しておりますが、まず、この方法で私の理解は合っていますでしょうか。その辺り、確認させてください。

○山内政府参考人　お答え申し上げます。

運用としては、今までと基本的には変わりません。まず電気通信事業者を通じて利用者の方に対して注意喚起を行うという、このメカニズム自身は変わりません。ただ、実効性を上げるために、先ほど申し上げましたとおり、関係者の方々、特に作っている方、利用者の方が実際に対策を行う前にセキュリティー対策を高めるといったこと、それから、管理者として、ユーザー以外に存在する方に直していただくということもございますので、こういう幅広い取組を是非進めていきたいというふうに思っているところでございます。

○川崎委員　ありがとうございます。

実際にＮＯＴＩＣＥの方でそうした通知をされたとしても、実は、連絡を受けた会社というのは必ずしもＩＴに詳しい人材がいるわけではございません。中小零細企業ではただでさえ人材不足がありますので、ＩＴ、デジタル人材が常に常駐しているというわけではないです。そういった状況ですので、ＮＯＴＩＣＥのサポート体制というのは本当にしっかりと努めていかなければいけないというふうに思っております。人材が足りないのであれば、ＮＯＴＩＣＥ側にもしっかりと人材配置を行う、そのための予算繰りもしっかりやる、これをお願いしたいというふうに思います。

また、実は、民間でも感染検知を行ってくれている企業というのがございます。これは一例ですけれども、大阪の商工会議所はサイバーセキュリティーに対してリテラシーがすごく高くて、このような感染検知を行ってくれている企業に委託して検知を行っております。是非、こうした企業もありますので、より強力な体制を構築するためには、総務省だけでやらずに、こういう民間企業ともタイアップをしながらやっていただければというふうに思います。

改めてこの部分も強くお願いをし、私の質問を終了させていただきます。ありがとうございました。

○古屋委員長　次に、平林晃さん。

○平林委員　公明党の平林晃と申します。

今国会から総務委員会の配属となりました。どうぞよろしくお願い申し上げます。

サイバー攻撃がサプライチェーンを寸断したり、あるいは社会インフラの機能が停止させられたりする事態を目の当たりにする昨今におきまして、サイバーセキュリティーの強化は喫緊の課題と考えております。このような状況の下、今回のＮＩＣＴ法改正案では、令和五年度末に時限を迎えるＩＤ、パスワードに脆弱性があるＩｏＴ機器の調査を令和六年度以降も継続的に実施する、また、脆弱性があるファームウェア等を搭載しているＩｏＴ機器及びマルウェアに既に感染してしまっているＩｏＴ機器を新たに調査の対象とすることとしております。この理解の下に、以下、質問をさせていただければと存じます。

まず、今回の法改正では調査対象が拡充され、また、ＩｏＴ機器は今後も更なる増加をすると考えます。そうしますと、ＮＩＣＴのセキュリティー部門の体制強化は必須であると考えております。この点についてのお考えを総務大臣にお伺いいたします。

○鈴木（淳）国務大臣　総務省では、サイバーセキュリティー分野をＮＩＣＴの重要研究開発分野の一つに位置づけておりまして、ＮＩＣＴのサイバーセキュリティー担当部門の体制強化は大きな課題であると認識をしております。

私自身も、先日、ＮＩＣＴを視察させていただきまして、サイバー攻撃の脅威が高まる中で、ＮＩＣＴのサイバーセキュリティー関連業務の重要性はますます高まっていると実感をしたところであります。

現在、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査は、平成三十一年の調査開始に伴ってＮＩＣＴに設置した専門の組織で実施しております。

ＩｏＴ機器数の増加が続く中で、今回の法案では、調査対象を拡充するとともに、幅広い関係者への情報提供や助言を新たにＮＩＣＴの業務として位置づけることとしておりまして、更なる体制強化が必要になるものと考えております。

総務省としましては、令和六年度に向けて、体制強化に必要な予算を増額して要求しておりますので、ＮＩＣＴのサイバーセキュリティー関連業

務の実効性が上がるように、しっかりと取り組んでまいりたいと思います。

委員はまさに御専門でございますので、これからも引き続き御指導を賜りますよう、どうぞよろしくお願いします。

○平林委員　大臣、丁寧な御答弁をいただきまして、大変ありがとうございます。予算措置を含めて体制強化を考えておられるとのことであり、しっかりと取組を進めていただきたいと考えます。よろしくお願いいたします。

続きまして、ＮＩＣＴの調査、これにより見つかった脆弱性のあるＩｏＴ機器に関しましては、機器の利用者にセキュリティー対策をお願いすることとなります。ここで連絡を受け取った利用者の機器操作についての知識が十分でない場合も十分考えられます。このような利用者に対するサポートを総務省はどのように考えておられるのか、見解を伺います。

○山内政府参考人　お答え申し上げます。

利用者に対するサポートという観点で、ＩｏＴ機器の利用者の知識が不十分であった場合、お願いしてもなかなか正しい設定を行うということが難しいということが想定されます。

このため、総務省では、利用者に対して通知を行う際には、実際に見つかった機種ごとの設定資料を作成して、具体的に何をするかということをお教えする、こういう内容をまず提供させていただくといったこと、それから、電話対応可能なサポートセンターを用意いたしまして、ＩｏＴ機器に対する知識が不十分な方であっても正しく設定ができるよう、御利用者の支援に取り組んでおります。

その観点では、先ほど、メーカーやシステムベンダーといった方々との連携強化の取組の一環として、設定変更を行わなくても一定のセキュリティーを確保できるようにということを申し上げましたが、こういう方々、メーカーや業者の方に対して設置、販売の時点でセキュリティーの確保に協力を求めるといったことを含めて、利用者の負担の軽減の取組についても検討をしてまいりたいと考えております。

○平林委員　ありがとうございます。

ただいま御答弁にあった電話のサポートの件ですけれども、私もちょっと調べさせていただいたんですが、固定電話用と携帯電話用、二種類の番号が用意してあるというふうに認識をしております。それ自体は非常に丁寧と思っていますけれども、時間が午前十時から午後六時までということで、本業と重なる時間帯かなと思いました。保守業務というのは意外に本業と違うところでやる操作であったりもするので、そういった時間以外、チャットとかウエブフォームによる問合せもあるので、そういった対応もしておられますけれども、より丁寧な対応をお願いできればと思いますので、よろしくお願いをいたします。

続きまして、セキュリティー人材の確保、これは一般企業や団体においても重要であり、私の地元でも様々困っているという声をたくさん伺っております。こうしたサイバーセキュリティー分野における人材確保及び育成について総務省はどのような取組を行ってきたのか、御見解を伺います。

○山内政府参考人　お答え申し上げます。

委員御指摘のとおり、企業や団体といった各組織におけるセキュリティーの人材の育成、確保は大変重要な課題だというふうに認識をしてございます。

このような課題に対応するため、総務省では、ＮＩＣＴにおいて、その豊富な技術的知見を活用いたしまして、政府機関、地方自治体、重要インフラ事業者等を対象といたしまして、実践的なサイバー防御演習、ＣＹＤＥＲと申し上げます、ＣＹＤＥＲを実施しております。

ＣＹＤＥＲは、受講者の事案対処能力を向上させるために、サイバー攻撃による事案の検知から回復までの一連の対処方法を実際に体験いただく演習でございます。二〇一七年度以降、毎年度、全都道府県の会場において計百回、三千名程度の規模で実施をしております。各組織内でのセキュリティー人材の育成、確保に貢献をしております。

また、二〇二一年度から、各都道府県の会場だけではなくて、自職場等から受講ができるＣＹＤＥＲのオンラインコースというものを開設いたしまして、受講者の裾野の拡大を図っているところでございます。

総務省といたしましては、引き続き、ＮＩＣＴと連携をして、サイバーセキュリティー分野における人材の育成、確保に取り組んでまいります。

○平林委員　ＣＹＤＥＲプログラムを通じて、年間三千人ということで、本当に多くの人材を育てていらっしゃるということ、また、オンラインも使ってより広範な取組をしておられるということで、大変重要な取組をしてきておられると考えます。

その上で、なおも人材が不足しているというのが現場の実感でもあろうかと思います。その場合、海外に目を向けることも必要かと考えております。総務省は、既に、ＡＳＥＡＮに対してＣＹＤＥＲプログラムの英語版を提供するなど、この五年間で千二百人程度の人材を育成してきているということも伺いました。こうした人材に、現在はＡＳＥＡＮ十か国それぞれの国で活躍することを想定しておられるとのことですけれども、我が国で活躍してもらってもいいのではないか、こんなふうにも考えております。

自国の安全は自国で守る、これも重要な考え方ですけれども、需要に対して供給が余りにも不足しているというのがサイバーセキュリティー人材であります。中小企業においては、是非力をかしてほしいとの声もあろうかと思います。御検討いただければと思いますので、よろしくお願いを申し上げます。

続きまして、インターネットにおける脅威という意味では、サイバー攻撃とともに偽情報やフェイクニュースへの対策が、生成ＡＩなど技術の急速な発展によりますます重要になってきています。先週末には、岸田総理のフェイク動画が問題になっております。それ以前にも、アメリカ国防総省、いわゆるペンタゴン付近で爆発が起きたとする偽の画像がネット上で拡散をし、株価が一時下落するなどの騒動に発展をしております。

偽情報やフェイクニュースのこうした問題が更に悪質と考えられるのは、こうした情報を発信することによって閲覧者を獲得すれば、偽情報を発信した側が広告収入を得ているということであります。うそでお金を稼いでいるという、とんでもないことであります。また、一部の研究によりますと、偽情報は正しい情報よりも早く拡散をしてしまう、しかも、より広範に拡散するということも指摘をされております。

このように深刻化していく偽情報問題への対策に関しまして、総務省はどのような取組を進めておられるのでしょうか。見解を伺います。

○湯本政府参考人　お答え申し上げます。

委員御指摘のとおり、生成ＡＩによる巧妙な偽・誤情報の拡散といった新たな課題が顕在化しておりまして、サイバー攻撃と同様に、これらの対策がますます重要になっているものと認識しているところでございます。

インターネット上のいわゆる偽・誤情報への対応につきましては、プラットフォーム事業者を含む幅広い関係者による自主的な取組を総合的に推進することが重要だと考えているところでございます。例えば、偽・誤情報を含む投稿の削除またアカウント停止といったプラットフォーム事業者が自主的に講じている取組に対する透明性、アカウンタビリティーを確保することが重要でございます。また、偽・誤情報をうのみにしないような利用者のＩＣＴリテラシーの向上も重要な事項であると考えているところでございます。

こうした認識の下、総務省におきましては、これまでも、プラットフォーム事業者による自主的な取組に対してモニタリングを実施したり、リテラシー向上策として、偽・誤情報に関する啓発教育教材及び講習用ガイドラインの開発やインター

ネットトラブル事例集の作成などに取り組んでまいりました。

また、偽・誤情報への対応につきましては、関連技術の開発、実証の推進など、技術の進展については技術で対応する、こういった観点も重要でございまして、今後も引き続き、関係省庁等とも連携しつつ、偽・誤情報対策に取り組んでまいります。

○平林委員　ありがとうございます。是非しっかりと進めていただきたいと思いますので、よろしくお願いいたします。

続きまして、ＮＩＣＴのその他の取組についても伺います。

今回の法改正に関係するサイバーセキュリティー分野以外におきましても、ＮＩＣＴは多種多様な研究の取組を進めておられると認識しております。

私は以前大学の教員をしておりましたが、その頃にお世話になったＮＩＣＴ研究者の方は、関西にあります未来ＩＣＴ研究所で、脳コンピューターインターフェース、いわゆるＢＣＩの研究を行っておられます。御当地を訪問させていただいたとき、ＭＲＩ装置の中でも日本有数の七テスラの装置、これは病院などにあるものよりもずっと強力なものですけれども、あるいは脳内の微弱な磁場の変化を計測できるＭＥＧ装置も見学させていただきました。こうした経験を通しまして、ＮＩＣＴの幅広い研究テーマに対する取組を拝見してきたところでございます。

そこで、伺います。研究機関としてのＮＩＣＴの取組を概括的に御教示いただき、今後目指すもの、その中でも特に力を入れていく内容について、総務省に伺います。

○田原政府参考人　お答え申し上げます。

ＮＩＣＴは、科学技術・イノベーション基本計画などの各種の政府戦略などを踏まえまして、現在は、電磁波先進技術、革新的ネットワーク、サイバーセキュリティー、ユニバーサルコミュニケーション、フロンティアサイエンスといった重点五分野において中長期的視点に立って自ら最先端の研究開発を実施するとともに、民間企業などによる研究開発の支援やオープンイノベーションの創出のための取組を進めております。また、日本標準時、標準周波数の決定、送出など、公的サービスの提供も担っているところでございます。

具体的に幾つか御紹介させていただきますと、御指摘のサイバーセキュリティー分野のほか、自ら実施する研究開発分野として、防災・減災などの社会的課題に向けた、光や電波を用いて対象物の状況を判別するリモートセンシング技術の研究開発、次世代の情報通信インフラ、ビヨンド５Ｇの実現に必要な超高速、大容量通信等を可能とする有・無線の通信技術の研究開発、長年の研究により蓄積してきたＡＩ技術や良質な日本語データを生かしたビジネス、国際会議で使えるリアルタイムな同時通訳、日本語に特化したテキスト生成ＡＩの研究開発、さらに、今委員からも御紹介がございましたが、脳波を測定、分析し、人間の認知過程を可視化、フィードバックすることによって学習や運動の改善、向上に役立てる脳情報通信技術の研究などの取組を実施しているところでございます。

さらに、令和四年度第二次補正予算で新たに造成した情報通信研究開発基金を活用させていただきながら、企業などが進めるビヨンド５Ｇの実現及び我が国の国際競争力の強化や経済安全保障の確保に資する技術の研究開発の支援を始めているところでございます。

総務省といたしましては、ＮＩＣＴには、引き続き中長期的視点に立った研究開発によって我が国の情報通信分野をリードいただくとともに、大学や産業界と連携して、研究開発成果を社会全体のイノベーション創出に積極的につなげていただくことを期待しております。

以上でございます。

○平林委員　ありがとうございました。

今、日本の研究力が相対的地位の低下に苦しんでおります。その挽回にも御貢献いただくことを御期待申し上げまして、私の質問を終わります。大変にありがとうございました。

○古屋委員長　次に、湯原俊二さん。

○湯原委員　おはようございます。立憲民主党の湯原俊二です。よろしくお願いします。

それでは、今回のＮＩＣＴ法の改正について質問させていただきます。

今回の法改正で、ＩｏＴ機器の調査を令和六年度以降も継続的に、対象も拡大してということでありますし、延長していくということです。ＮＩＣＴの観測によれば、サイバー攻撃関連通信のうちＩｏＴ機器を対象にしたものが全体の三割、その先の攻撃の踏み台にもなっているということで、先ほど来の議論になっているのかなというふうに思います。

お手元に資料を配付させていただきました。

先ほど、研修等、人材のこともあったわけですけれども、前段として、サイバー防御の関係の人員を各国と比較した資料をお手元にお渡ししております。もちろんＮＩＣＴだけで日本のサイバー防御をしているわけではありませんけれども、全体の中の一部分といいますか、先ほどあったように、研修の部分では主要なところであります。

お手元にあるように、中国、北朝鮮、ロシア。ロシアの場合は、軍が千人程度で、ほかには参謀本部であったりいろいろ、対外情報庁等々の人数もありますので分かりません。アメリカでも、軍が六千二百人、それ以外には三千人超ということで、これは表へ出てこない数字もあると思いますので、外へ出ている数字でこういう状況だということです。

防衛三文書も出ましたけれども、自衛隊の場合、現在は八百九十名で、これを今年度内に二千二百三十人、そして四千人、こういうふうな計画もあるわけであります。ＮＩＣＴの場合は現在百十二人。ＮＩＳＣの方、内閣官房の方ですけれども百八十人、警察庁が三百四十二人、こういう状況でありまして、先ほどは三千人研修ということでありますので、自治体を含めれば幾分増えるわけでありますけれども、人員体制について鈴木大臣はどのようにお考えであって、今後どうしていきたいか。人員体制について御答弁いただけたらと思います。

○鈴木（淳）国務大臣　サイバー攻撃が複雑化、巧妙化する中で、セキュリティー人材の確保は重要な課題でありまして、政府全体で取組を進めておるところでございます。

サイバーセキュリティー分野を含めて研究開発を実施しているＮＩＣＴ全体の職員数は、本年一月時点で千三百八十一名でございます。

各国でサイバーセキュリティーに関わる機関やその機関が果たす役割は多様でありまして、個別の機関の職員数を単純に他国と比較することはできませんけれども、サイバー攻撃の脅威の増大に対応する体制強化の必要性、重要性は各国で広く認識されているところと承知しております。

今回の法案では、ＮＩＣＴが実施するＩｏＴ機器の調査対象を拡充するとともに、幅広い関係者への情報提供や助言を新たにＮＩＣＴの業務として位置づけることとしておりまして、ＮＩＣＴのサイバーセキュリティー担当部門について、人員を含めて更なる体制強化が必要になると思っております。

総務省としましては、令和六年度に向けまして、体制強化に必要な予算を増額して要求しておりまして、ＮＩＣＴのサイバーセキュリティー関連業務の実効性が上がるようにしっかり取り組んでまいります。

○湯原委員　ありがとうございます。

おっしゃったように、体制強化が必要だということ、サイバー防御で、重要インフラというところはそれぞれでやるということですし、全体としてはＮＩＳＣがあり、自衛隊が人数を増やすということであります。これも、最初は自衛隊と関連産業をまずは防御していくということであります。

先ほど来あったように、古いＩｏＴ機器等々とか、あるいは中小企業とか地方の小規模の自治体

のことを考えれば、ＮＩＣＴがいかに研修してボトムアップを、強いところが一か所だけあればいいというものじゃなくて、全体がかさ上げしていかなきゃいけないものですから、そういう意味では役割は重要でありますので、人員体制についても引き続いて御尽力いただきたいと思います。

その一方で、いろいろな文献、識者の話を聞いておりますと、警察でも自衛隊でもそうであるようでありますけれども、サイバーセキュリティーの国際的な資格認定制度であるＣＩＳＳＰ、こういう資格があるようでありますけれども、資格を取った後、退職をされていく、それで民間に行く、こういう状況が一方であるんじゃないかということでありまして、ＮＩＣＴの方でも、こういったある意味での危機感、この辺についてどのようにお考えか、御答弁願いたいと思います。

○山内政府参考人　お答え申し上げます。

今御指摘のあったような、サイバーセキュリティーに関連するほかの組織と同じように、ＮＩＣＴにおいても、高度な知識、技術を有するサイバーセキュリティー分野の研究者、技術者を所内に維持、確保することは大変重要だというふうに思っております。

このため、ＮＩＣＴにおいては、サイバーセキュリティーの研究開発に携わる職員の待遇の改善を進めるとともに、世界最大規模のサイバー攻撃観測網を有しております、このようなものを使った最先端のサイバーセキュリティー研究開発環境を整備しているというふうに承知をしております。

総務省としても、ＮＩＣＴが高度な知識、技術を有するサイバーセキュリティー人材を維持、確保し続けることができるように、サイバーセキュリティーの研究開発に取り組む場としてのＮＩＣＴの魅力の向上に努めてまいります。

○湯原委員　待遇の改善とか、環境を整備していって、ある意味で引き止めると言ったらおかしいですけれども、引き続いて働いてもらいたい、こういう御答弁であったかと思います。

いろいろ私なりに勉強させてもらうと、先ほど申し上げたように、民間のレベルもアップするためには、やはり一定のスキルを蓄えた人が民間との交流、韓国ではそういうふうにやって全体的にボトムアップしているということをやっておりますので、一定程度は認めますけれども、民間へ行く、それ以降ですね。先般も質問がありましたけれども、倫理面で今度は、スキルアップをした人が今度は民間どころか悪用してしまう、こういった倫理面での対応ですね。いかに抑えていくか、抑制していくか、この辺、どのようにお考えでしょうか。

○山内政府参考人　お答え申し上げます。

今御指摘のあったような、サイバーセキュリティーの知識や技術でございますが、これは、セキュリティー対策の向上に役に立つのと同時に、悪用される、そういうおそれもあるというふうに思っております。

このため、総務省では、ＮＩＣＴを通じて実施をしているセキュリティー人材育成プログラムの中で、知識や技術についての教育と併せて倫理教育にも力を入れております。

また、ＮＩＣＴ内部の職員に対しても、サイバーセキュリティーに関する研究データ、これを適切に管理するという旨を指導しているところでございます。

総務省としては、こうした取組を通じて、サイバーセキュリティーの知識や技術を適切に活用できる人材の育成を引き続き推進してまいります。

○湯原委員　御答弁いただきました。倫理教育に力を入れるという御答弁があったので了としますが。

ただ、どこまで教育しても、最終的には本人が悪用に転じる可能性もあるわけでありますので、了とはしますけれども、引き続いてこの面は是非、力を入れていただくということでありましたけれども、力を入れていただきますようにお願いを申し上げたいと思います。

倫理面に関連してですけれども、今ＮＯＴＩＣＥでＩｏＴ機器をチェックしているわけですけれども、これは以前から、通信の秘密との整理、すみ分けのことで、今回は六年度以降も延長でありますけれども、最初の改正のときからずっと議論になっていることであります。

私も、今日までの国会答弁等を読ませていただいております。ＩｏＴ機器チェックということは不正アクセスにはならないという認識であって、どうやって歯止めをかけるかというと、実施計画を総務大臣に出して、総務大臣が認可をして、そして罰則の規定がある、その後、ＩｏＴ機器を調査した後はログを保存する、こういう歯止めをかけているから大丈夫だということを答弁されておりますけれども、改めて、ＩｏＴ機器チェック、調査に入ってＩＤとパスワードを取った後に、その中身について知り得たり、漏えいする懸念ですね、通信の秘密に対して侵すような、この担保、保証の仕方、改めて答弁願いたいと思います。

○山内政府参考人　お答え申し上げます。

まず、特定アクセス行為によって収集する情報でございますが、これはＩｏＴ機器の利用者とＮＩＣＴとの当事者の通信内容でございますので、第三者間の通信の内容を含まないため、通信の秘密には該当しないということになります。

また、特定アクセス行為は総務大臣が適正かつ確実に実施されると認めた計画に従って行うこととしておりますので、計画で認められた以上の操作、情報収集は行いません。

例えば、具体的には、特定アクセス行為の実施に当たりましては、計画に基づいて可能な限りシステムで調査を自動化して、必要以上の情報を収集する余地がないように運用することとしております。

また、実施に際して、計画に基づいた全ての特定アクセス行為に係る通信記録は定期的に監査をしております。これによって不正な利用がないことを確認するとともに、特定アクセス行為を行うＮＩＣＴ職員についても毎年セキュリティー研修を実施して、職員の高い倫理観の維持にも努めることとしております。

改正後においても、これらの取組を計画に記載することで、特定アクセス行為について引き続き適正かつ確実な実施を担保してまいります。

○湯原委員　分かりました。引き続いてお願いしたいと思います。

サイバー防御という観点から、その先に関連して、私は能動的サイバー防御について続けて質問をさせていただけたらというふうに思っております。

岸田総理は、今年の四月、防衛三文書についての代表質問に答えて、今年の一月末に内閣官房にサイバー安全保障体制整備準備室を設置したところであり、スピード感を持って具体化に向けた議論を進めてまいりますというふうに答弁されております。つまり、一月に内閣官房にこの準備室をつくったということでありますけれども、十一月、十か月たったわけですけれども、その進捗状況、体制整備の状況、お答え願いたいと思います。

○飯島政府参考人　お答えを申し上げます。

昨年十二月に閣議決定した国家安全保障戦略におきましては、サイバー安全保障分野での対応能力の向上のため、情報収集、分析能力の強化や、能動的サイバー防御の実施のための体制などを進めることとしております。これらの検討に当たっては、委員御指摘のとおり、本年一月に内閣官房にサイバー安全保障体制整備準備室を設置したところであります。

この準備室におきましては、具体的に申し上げますと、官民の情報共有の強化や民間に対する支援の強化、通信に係る情報を活用した攻撃者による悪用が疑われるサーバーなどの検知、重大なサイバー攻撃を未然に阻止するための政府に対する必要な権限の付与といったことを取り組むということとしております。

また、こうした取組を実現、促進するために、内閣サイバーセキュリティセンター、ＮＩＳＣを発展的に改組し、サイバー安全保障分野の政策を

一元的に総合調整する新たな組織を設置することとしております。

我が国のサイバー対応能力を向上させることは喫緊の課題であります。様々な角度から政府全体で検討を進めているところ、可能な限り早期に法案をお示しできるよう検討して、引き続き取り組んでまいります。

○湯原委員　飯島さんから今御答弁があったわけですけれども、いろいろな権限を付与して、そしてＮＩＳＣを発展的に改組、バージョンアップしてということで、体制を整えていくということで、できるだけ早くということであります。

私は、今までの委員会等での質問で申し上げていたんですけれども、やはり諸外国と比べて十年近く日本の体制は遅れているというふうに認識を持っております。ほかの先進国は、やはり十年ぐらい前にこういう体制を整えております。できるだけ早く、岸田総理はスピード感を持ってと言う。具体的に、いつ頃までをめどにして考えていらっしゃいますか。

○飯島政府参考人　お答えを申し上げます。

先ほど申し上げましたとおり、まさに様々な角度から政府全体で検討を進めているというところでございます。

可能な限り早期に法案をお示しできるよう、引き続き取り組んでまいりたいと考えております。

○湯原委員　可能な限り早くというと、いつまでですかと聞いて可能な限り早くということで、もうそれ以上答弁がないのかなと思いますが、でも、やはり、体制整備をするということであれば、一定のめどを持ってやらなきゃですね。言葉で抽象的に可能な限り早く、可能な限り早くと言いながら、何年も先、五年も十年も先で果たしていいのか、こういう思いを持つわけであります。

本当に、先ほど来あるように、サイバー攻撃を受けている状況があるわけでありますので、その辺のところを踏まえて、いつまでをめどにということを、目標を持って対応できるようにしていただきたいというのを、これは要望させていただきたいと思います。

次の質問ですけれども、以前も申し上げておりますけれども、憲法の通信の秘密と能動的サイバー防御との論点整理といいますか、国民に見える形で、有識者会議を早く立ち上げて、国民の皆さん方にこういうところは議論があると、こういうことをちゃんと皆さん方に知らしめることが必要なんじゃないかなというふうに思っております。この点について、どのようにお考えなのか。有識者会議の設置についてお答え願いたいと思います。

○飯島政府参考人　お答え申し上げます。

委員御指摘の点も含めまして、まさに、我が国のサイバー対応能力を向上させることは、現在の安全保障環境を考えますと喫緊の課題でございます。安全保障上の必要性はもとより、憲法を始めとした現行法令との関係などを含む様々な角度から、今、政府全体で精力的に検討を進めているところでございます。

委員から御指摘のございました有識者会議の設置につきましては、こうした検討の進捗状況を踏まえ、判断してまいりたいと考えております。

○湯原委員　飯島さんがおっしゃるように、喫緊の課題だというのは認めていらっしゃるんですね、皆さん方、サイバー攻撃を受けていらっしゃる。

ところが、一方で、体制整備とか、あるいは通信の秘密との整合性、憲法論議も含めてこの辺のところ、有識者会議はできるだけ早くと言いながら全然明らかになってきていない、こういう状況であります。一方で、総務行政で、大臣は所信で、国民に一番身近なところと。今、皆さんがＩｏＴ機器を含めてインターネットを使っていらっしゃるわけでありますので、そこの一番コアな部分、一番大切な部分、通信の秘密の部分に絡む問題でありますので、やはり前広に、有識者会議を立ち上げて、こういう問題がありますということを国民の議論も併せてしていただくような体制を取らなきゃいけないんじゃないかなと私は申し上げておきたいと思います。

なぜならば、昨年末に防衛三文書が出ました。それまで国会で、どうなっているんですか、どうなっているんですか、検討状況は、こういう質問を野党側は再三してまいりましたけれども、一向に出てこない。国会が閉じた後、昨年末にいきなり防衛三文書が出て、予算がこうですみたいな話で閣議決定していくという。国民の議論がないままに、どんどんどんどん進んでいく。国民の通信の秘密の部分についても、いきなり出して、いきなり閣議決定で既成事実化する。こういう姿勢はやはりよくないんじゃないかというふうに私は思っております。

この点について、前広に議論をしていく、有識者会議を立ち上げて前広に議論はしていきますということを改めてどのように考えていらっしゃるか、御答弁願いたいと思います。

○飯島政府参考人　お答えを申し上げます。

まさに今、具体的な内容というのは、安全保障上の必要性はもとより、憲法その他の現行法令との関係も整理しつつ検討を進めておるというところでございます。

そういうような検討の状況を踏まえて、繰り返しにはなりますが、有識者会議につきましては、その進捗状況を踏まえて判断してまいりたいというふうに考えております。

○湯原委員　飯島さんがおっしゃったように、有識者会議を立ち上げてということは、その有識者会議を早く立ち上げないとそういう議論を公にできないわけですので、是非、これはもう時間もないので要望にさせていただきますけれども、可能な限り早く立ち上げて国民の議論を進めていただきたい、こういうことは申し上げておきたいと思います。

時間がないので一つ飛ばして、通信傍受法の場合、通信傍受の手続がありますね。改正になりましたけれども、通信傍受のターゲットを決めて、裁判所の許可を得て通信を傍受する、こういうことであります。能動的サイバー防御では、ふだんから、多分、先ほどのＩｏＴ機器ではありませんが、パトロールをするわけでありますけれども、この手続については必要なのか、どういった手続があるのか。それとも、全く必要なくて一方的に能動的サイバー防御をしていくのか。この点について、どのようなお考えなのか。

○飯島政府参考人　お答えを申し上げます。

国家安全保障戦略におきましては、国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバーなどを検知するために所要の取組を進めるということとしております。これについても、まさに現行法令との関係なども含め、今、政府全体で検討を進めているところであります。

その実施のために必要となる手続も含めて、現時点で具体的な取組の内容が決定しているものではありませんが、いずれにしても、国民の権利や自由が不当に侵害されないという観点も含めて、様々な角度から検討を進めるところであります。

○湯原委員　なかなか中身について教えていただけないんですけれども、論点はやはり明らかにしてもらわないと、国民の理解が得られないと思います。有識者会議も立ち上げない、中で今議論をしている最中です、しかし、こう決まりましたといって有識者会議もその方向で決まっていくということになると、なかなか論点について国民の皆さん方の理解が、逆に結果的に後々になって理解を得られないんじゃないか、こういうことを懸念するわけであります。

この辺のところは、再三になりますけれども、有識者会議をできるだけ早く立ち上げていただいて、こういう論点がありますよねということを知らしめて、そして国民の議論を呼んで、その上で決定していく、こういうプロセスを踏んでいくべきじゃないかな、こういうふうに、改めて、同じようなお願いになりますけれども、申し上げておきたいと思います。

一つ戻って、能動的サイバー防御と憲法の関連で、専守防衛についてであります。

四月に岸田総理は、能動的サイバー防御は武力行使ではないので専守防衛の対象外ということで答弁されております。

しかし、私の見方でありますけれども、国家安全保障戦略では、この能動的サイバー防御についてこういうふうに書いてあります。未然に攻撃者のサーバー等への侵入、無害化ができるように政府に権限を付与すると。未然にそのサーバー、相手のサーバーになると思いますけれども、あるいはどこかのサーバーになると思いますけれども、侵入していって無害化できるように政府に権限を付与する。

これは、私の見方ですと、まだ国内であれば警察権限とかいろいろあると思いますが、海外にあるサーバーを無害化するということは、果たしてこれが専守防衛に当たるのかどうなのか。この辺について、どのようなお考えを持っていらっしゃいますか。

○飯島政府参考人　お答えを申し上げます。

まさに今御指摘がございましたとおり、国家安全保障戦略におきましては、国、重要インフラなどに対する安全保障上の懸念を生じさせる重大なサイバー攻撃につきまして、可能な限り未然に攻撃者のサーバーなどへの侵入、無害化ができるよう、政府に対し必要な権限が付与されるようにすることとしております。

まさにこの侵入、無害化というのは、武力攻撃に至らない場合の措置として実施するということを考えております。そういうこともございますので、武力の行使に該当することは想定をしていないというところでございます。そういうことを踏まえますと、まさに専守防衛に反するものではないというふうに考えております。

○湯原委員　飯島さんは専守防衛の範囲内だとおっしゃいますが、実際、ロシアがウクライナへ侵攻する場合でも、ミサイルをドンパチ撃つ前には情報戦と称してサイバー攻撃をするわけです。つまりは、戦争の中の一つの部分、一番、前段としてあるわけです、戦争のカテゴリーの中のですね。そういうことを考えると、やはり専守防衛との位置づけ、これも前広に議論をしていくべきというふうに思います。

あと一言だけ要望として申し上げておきたいと思います。

これから有識者会議等々で議論をするわけでありますけれども、能動的サイバー防御を行う、その事後ですね、ＩｏＴ機器はログを保存するとかいろいろありましたけれども、このチェック体制、特に国会で、何を能動的サイバー防御でやってきたのかということを国会に報告する義務を持たせる、このことは絶対必要だということで申し上げておきますので、要望とさせていただきます。

以上で質問を終わりたいと思います。ありがとうございました。

○古屋委員長　次に、おおつき紅葉さん。

○おおつき委員　立憲民主党・無所属のおおつき紅葉と申します。

早速、質問に入らせていただきます。

改めまして、先ほどから皆さんが議論されているＮＯＴＩＣＥの取組、重要かつ評価すべき取組であるとまず冒頭に申し上げさせていただきます。

ただ、このＮＯＴＩＣＥと呼ばれる取組、先ほどもありましたが、お世辞にも国民に広く浸透されているとは言えない状況であります。

例えば、この取組、広げようとどういうことをしているのかなと、私はインターネットで検索してみましたけれども、総務省が認定している第三者機関のＩＣＴ―ＩＳＡＣ、このＩＣＴ―ＩＳＡＣが作っているＹｏｕＴｕｂｅチャンネルがあるんですけれども、この再生回数、皆さん御存じでしょうか。四十二回とか六十五回とか、もうちょっと多いのもあるんですけれども、正直、関係者しかもしかしたら見ていないんじゃないかなというような数字でございます。もちろん、ＹｏｕＴｕｂｅが広げるための全ての手段だとは思いません。ただ、やはり浸透していないのは事実だと思います。

また、ネットワークに接続された機器の脆弱性を管理者に通知しても、通知を受けた管理者などには十分に対処されていない事例も少なくないと伺っております。これまでネットワークに接続する機器の脆弱性を放置した結果が、その機器がほかのネットワーク機器に対するサイバー攻撃の踏み台にされてしまって、機器の管理者がサイバー犯罪の被疑者と疑われる可能性があるなど、一時的又は長期的に甚大な不利益が放置した管理者等に生じる可能性があることをこの場で指摘をさせていただきたいと思います。

情報通信行政においては、諸外国の取組の結果を十分に検討した上で、我が国の制度として整備していく。よく言えば、慎重かつ安全で失敗の少ない行政運営、悪く言えば、諸外国の後追いのみで先進的な取組に乏しいとの印象があります。しかしながら、ＮＯＴＩＣＥの取組に関しては、諸外国で余り例を見ない中、四年前から実施してきた希有な事例ということで大変評価されているということなんですけれども、そこでまず伺います。

実際にＮＯＴＩＣＥ同様の取組を行っている事例が海外にあるのかどうか、また、この取組に対する他国の評価について、例えば他国から視察の申入れがありましたなど、大臣就任後、大臣は就任後間もないんですけれども、これまで政務官や副大臣も務められていたことを踏まえて、サイバーセキュリティー対策に資する対策として、鈴木大臣にお伺いいたします。

○鈴木（淳）国務大臣　御質問ありがとうございます。

サイバー攻撃に悪用され得る脆弱性のあるＩｏＴ機器に対する対処の必要性については、世界の多くの国においては認識されておりますけれども、継続的に脆弱性のあるＩｏＴ機器を調査した上で、通信事業者の協力の下で利用者への注意喚起まで実現している例というのは我が国のほかにはないものと承知しております。

ＮＩＣＴでは、このＮＯＴＩＣＥプロジェクトの活動に基づく論文を多数発表しておりまして、これらの論文は、サイバーセキュリティーに関する世界的に権威のある国際学会においても、個人や事業者のセキュリティー対策の動機に着目したという点で高い評価を受けているものと承知をいたしております。

○おおつき委員　ありがとうございます。まさに高い評価を受けている取組、是非、先進的な例として進めていただきたいと思っております。

ＮＯＴＩＣＥの対象機器についてなんですけれども、これまで、ＩＤ、パスワードに脆弱性を有するネットワーク機器のみでしたが、先ほど御説明があったと思います、現在総務省などにおいて、ネットワークに接続されている機器のファームウェアという、機器に内蔵されたソフトウェアに問題が存在するもの、また、既にサイバー攻撃へ悪用できる状態となった機器など、つまり、ほかのネットワーク機器に対してサイバー攻撃に加担させることができる状態となったものが想定されると伺っております。

そして、これまで、ＮＯＴＩＣＥの取組によって通知、注意喚起を行った先は、一般家庭から法人まで様々あったかと思います。しかし、これまで開催された総務省の情報通信ネットワークにおけるサイバーセキュリティ対策分科会において、注意喚起を受けても対処が進まない、つまり、注意喚起の効果が表れていないのは実は一般家庭の利用者よりは法人の方が多数であるということが指摘されております。

更に問題と考えられているのが、サイバーセキュリティーを軽視する事業者がいる、こういう実情があるんですね。一般社団法人、先ほど言ったＩＣＴ―ＩＳＡＣが分科会に提出した資料を拝見させていただきました。すると、事業者がコストを抑えるために意図的に中古のルーター、古いルーターを継続して利用したりだとか、あるいは遠隔で管理しやすいようにあえて脆弱な状態を容認している、こういう実情があるということなん

です。したがって、パスワードは強力なもの、もっと複雑なものにしていきましょう、設定しましょうというような初心者向けの広報だけでは、これまでのこういった事業者の皆さんの悪習を改める機会にはなり得ないと私は思います。

そこで、お伺いいたしますが、脆弱性のあったネットワークに接続する機器の利用形態や利用状況について分析した統計は総務省の方で作成されているのでしょうか。分析の結果であれば、その状況をどのように評価しているのでしょうか。お答えください。

○山内政府参考人　お答え申し上げます。

ＮＯＴＩＣＥによる注意喚起の対象となった脆弱性のあるＩｏＴ機器については、その発売年について分析をしております。その結果、十年以上前に発売された機器が全体の約半分、それから、このプロジェクトが始まった二〇一九年以前に発売された機器が全体の九割以上を占めているということが明らかになっております。

注意喚起を受けた利用者の中では、先ほど委員御指摘のとおり、法人ユーザーが多い。法人の比率が個人の比率の三倍以上になっているということが分かっております。また、注意喚起を行った企業においてＩｏＴ機器の管理者が明確でないということが、これも課題として分かっておりまして、こういうものが、なかなか、実効性を上げる意味での課題になっているというふうに承知をしております。

○おおつき委員　まさに、それらを総括すると、今までの総務省やＮＩＣＴ等が呼びかけの対象としてきた基礎知識のない管理者ではなく、本当にアプローチすべき相手というのは、情報システムを管理する事業者、いわゆるシステムインテグレーターとかＳＩｅｒとか言われる方々などの、ある程度サイバーセキュリティーに対する知見を持った者でありまして、総務省等が行ってきたアプローチはやはり見直していく必要があると私は考えます。

更に伺います。

システムインテグレーター等の知見のある者によって意図的に生じる脆弱性のある機器を今後どのように削減していく予定でしょうか。又は、サイバーセキュリティー対策を軽視する事業者に対する実効性のある支援だとか対応策だとか、是非伺いたいと思います。

○山内政府参考人　お答え申し上げます。

今委員御指摘のとおりですが、法人利用者につきましては、法人利用者そのものというよりも、機器の設置や管理にシステムインテグレーターが関与しているということが多いと承知をしております。したがいまして、利用者に対する注意喚起も必要でございますが、システムインテグレーターによる取組を進めるということが重要だと思っております。

ＮＯＴＩＣＥのプロジェクトで観測結果が分かりまして、脆弱性のあるＩｏＴ機器についての情報が把握できますと、対応すべき脆弱性、それを解消する方策を技術的に、具体的に分かる形でシステムインテグレーターに対して助言それから情報提供を行うという形を考えてございます。これによりまして、分からないといった、そういう状態をまず解消して、システムインテグレーターが積極的に対応いただける、こういう効果的な対策を是非推進していきたいというふうに思っております。

○おおつき委員　まさにその通知の仕方について、これから伺いたいと思います。

ＮＯＴＩＣＥのウェブサイトで公表されている今年八月度の実施状況によりますと、この取組による注意喚起が五千五十五件実施されました。ただ、そのうち三千四百六件は今年の七月に検知したものであったと伺っております。すなわち、約三分の二は前の月の通知からの繰越しであって十分な対処がされておらず、脆弱性のある機器がネットワークに接続されたままの状態、すなわち脆弱性のある状態が放置されてしまっているとも受け取れると思います。

そこで、まず伺います。現在、ネットワークに接続する機器の脆弱性に対する注意喚起の通知方法はメールや郵送と伺っているんですけれども、その通知方法についてお伺いします。

○山内政府参考人　お答え申し上げます。

今御指摘がございましたとおりでございますが、通常、電気通信事業者を通じた注意喚起については主にメールや郵送によって実施をされるという形になってございます。これは実際には事業者によって判断をされるというものでございますが、私どもが承知をしている主な方法はこの二つということでございます。

○おおつき委員　メールや郵送で本当に十分なのかどうか、やはりこの改正案を受けて見直すべき点があるんじゃないかなと思っております。

先ほどのＩＣＴ―ＩＳＡＣの資料によりますと、注意喚起に基づく対処が進まない背景というのが、法人において問題のある機器の管理者等が特定できない場合や、業務の都合で意図的に外部から管理できるようにしているだとか、様々な要因があるようなんですけれども、メールや郵送ではやはり詐欺かなと思われるときがあるんじゃないかなと思うんですよね、それだけだと。いずれにしても、ＩＤやパスワード等に脆弱性があることでどういった問題が起こっているのか、あるいは将来どういった問題が起こり得るのか、その点がなかなか理解されていない表れなのではないかなと思っております。

そこで、これまでの電子メールや郵送による注意喚起だけでは対処が十分に進んでいない理由を調査するとともに、電話や個別訪問など、より確実な手段で通知を行う必要があると考えますが、現状どのくらい危機感を持たれているのか、総務省の見解と具体案とともに政務官にお伺いしたいと思います。

○小森大臣政務官　先ほど参考人の方からも答弁がございましたとおり、電気通信事業者を通じた注意喚起については主としてメール若しくは郵送でなされているというところであります。

注意喚起の方法につきましては、電気通信事業者、当該事業者に適切に判断していただくものでありますけれども、総務省といたしましては、議員御指摘の利用者による対応が進まないケースにおきましては、利用者のセキュリティー意識が十分でないことや、あるいは、これも御指摘がありましたけれども、企業においてＩｏＴ機器の管理者が明確でないこと、これらも一因ではないかというふうに考えているところでございます。

このため、利用者による対応を進めるため、注意喚起の実効性を高めるための取組としては、今後、利用者への周知啓発を充実させることが大事であるというふうに考えておりまして、新たな広報戦略の策定も含めまして取り組んでまいりたいと思いますし、企業における管理者の問題についても考えてまいりたいというふうに思っております。

そしてまた、利用者に対する働きかけにとどまらず、メーカーやシステムインテグレーターなどの関係者とも連携することによりまして、利用者による行動のいかんにかかわらず、ＩｏＴ機器の安全性を向上するための取組を進めてまいりたいというふうに考えております。

○おおつき委員　まさに意識を上げていく、これが必要になってくると思います。是非、新たな取組、通知の仕方についても十分に検討していただきたいと思っております。

次に、サイバー攻撃の対処協会への委託についてお伺いします。

サイバー攻撃でＩｏＴ機器等が悪用されることがないように管理者等へ通知や注意喚起をする業務というのは、現在、認定送信型対電気通信設備サイバー攻撃対処協会という協会に委託することができるんですけれども、この協会に所属しているのが、今、先ほどから申し上げているＩＣＴ―ＩＳＡＣだけが認定されているという状況です。

そこで、現状、このサイバー攻撃対処協会がＩＣＴ―ＩＳＡＣのみである理由は何でしょうか。また、新たにＩＣＴ―ＩＳＡＣ以外の団体から認可申請があった場合は電気通信事業法第百十六条

の二に規定する条件を満たす限り総務大臣は認定するとの理解でよろしいでしょうか。答弁をお願いいたします。

○山内政府参考人　お答え申し上げます。

まず、管理者への通知業務を行うに当たっては、サイバー攻撃に悪用されるおそれのある機微な情報を扱っているということから、情報の適切な管理を行うための適切な制度的、技術的知見を有する組織に委託する必要があると認識をしてございます。

したがいまして、本法案では、上記要件を満たす組織として、サイバー攻撃に関する情報共有の体制を持っている委員御指摘の協会、認定送信型対電気通信設備サイバー攻撃対処協会、これを定義いたしまして、委託可能な組織として規定しているという状態でございます。

この協会とは、サイバー攻撃への対処に関する業務を適正かつ確実に行うことができる能力を有するなど、所要の要件を満たす団体として、これも御指摘がございました電気通信事業法に基づいて総務大臣が認定するという形になってございます。

したがいまして、所要の要件を満たす団体については、総務大臣に対して申請を行うことによって認定を行うことができます。

したがって、今御質問の二つ目にございました、ほかに能力を持っている方がもし申請をしたらどうなるかということでございますが、要件を満たす限り認定をされるということは可能だというふうに認識はしてございます。ただ、今まで実例として申請がなされ、認定を受けているのは、一般社団法人ＩＣＴ―ＩＳＡＣの一者ということでございます。

○おおつき委員　では、次の質問に行きます。

先ほど人員体制については湯原委員からも質問がありましたが、ＮＩＣＴの取組において実際ある程度の自動化がなされているようなんですけれども、調査結果の分析や精査、判定、そして問題となったネットワークに接続する機器の管理者等に注意喚起を行うに当たっては、サイバーセキュリティーに対する知見を有する者が必要となります。

管理者等への通知をするにはやはり工夫が求められる中で、実績を見ると相当な数を通知しているようですし、相当な御苦労がうかがえます。そして、今回の改正案だけでは、その改善も踏まえて、ネットワークに接続する機器の製造事業者等を含む関係者に伝えて、より実効的かつ効率的に対策していこうという考えかと思っております。

そこで、現在、デジタル人材の不足と盛んに言われている中で、ＮＩＣＴ、先ほど湯原委員の方では百十二人ということだったんですけれども、そのほか、ＩＣＴ―ＩＳＡＣ、そしてインターネットサービスプロバイダー等、本取組における注意喚起について、業務量に照らし合わせた上で、参加しているこれらの組織において体制や人員が十分であるかどうか、見解を伺います。

○山内政府参考人　お答え申し上げます。

まず、サイバー空間の環境を見ますと、ＩｏＴ機器の利用はどんどん拡大をしている、ＩｏＴ機器を悪用するサイバー攻撃も多様化をしている。これも御指摘がございましたが、ＮＯＴＩＣＥの業務量は開始当初から比較いたしますと増大する傾向にございます。

また、サイバー攻撃の多様化に対応するため、注意喚起の対象も拡大をしてまいりました。したがいまして、体制や人員の拡充が必要になるということを認識してございます。

今後とも、ＮＩＣＴそれからＩＣＴ―ＩＳＡＣとも連携をして、予算等によるそういう強化も含めて、体制、人員の強化に努めてまいりたいというふうに考えてございます。

○おおつき委員　本当に業務量がどんどん増えていくと思います。それによって、やはりこの国のセキュリティー体制、守られる点が多いと思うんですけれども、やはり一人の業務量が多くなってくるとだんだんミス等も出てくると思いますので、人員の確保に向けては予算の確保も是非お願いいたしたいと思います。

次の質問は、ＮＯＴＩＣＥのサポートセンターの運営について伺います。

さて、ＮＯＴＩＣＥについては、ネットワークに接続する機器へのアクセスによってサイバー攻撃に悪用されるおそれのある機器の利用者に対して、ウェブサイトや電話による問合せ対応を目的としたサポートセンターというものが設けられています。このサポートセンターの業務は、これまで申し上げてきた特定アクセス行為等とは異なって、ＮＩＣＴではなく総務省が実施しております。

そこで、確認いたします。ＮＯＴＩＣＥサポートセンターの業務を総務省からＮＩＣＴに今後移管することとなるのか、そういう可能性があるのか、是非お答えください。

○山内政府参考人　お答え申し上げます。

ＮＩＣＴ法において、ＮＩＣＴは特定アクセス行為とその結果に基づく電気通信事業者への通知を行うということとされております。利用者への注意喚起はＮＯＴＩＣＥに参加する電気通信事業者の負担によって行っている、こういう構造でございます。

注意喚起の方法は個々の事業者に委ねられておりますが、共通的な部分、例えばＩｏＴ機器の設定マニュアルの作成、それから利用者からの一般的な問合せの窓口の運営というものについては、総務省が一括して支援することで業務の効率化を進めてございます。

御指摘がございました改正法の第十四条第七号のロにあります助言及び情報の提供、これはＮＩＣＴの専門的な知見を必要とするものを想定しております。これに対比となる、先ほど申し上げたマニュアルの作成それから問合せの窓口といった運営等の業務の効率化に関する業務は、役割分担をいたしまして、引き続き総務省が担うということを想定しております。

○おおつき委員　引き続き総務省が行うということなので、是非しっかり行っていただけたらと思います。

次に、関連して、ＮＯＴＩＣＥサポートセンターの運営予算について伺います。

まず、電波利用料というのは、電波法の第百三条の二第四項で規定されております、無線局全体の受益を直接の目的として行う事務の処理に要する費用として、無線局の免許人等が負担している共益費用という位置づけであります。

この電波利用料については、二〇〇八年の電波法改正でその使途を限定列挙することとなりましたが、その発端は、当時の総務省総合通信局においてレクリエーション物品やフラワーアレンジメントの費用を電波利用料から支出していた事実が二〇〇八年の五月に発覚したことでした。

電波利用料の使途の限定列挙は、政府提出の電波法改正案では盛り込まれておらず、当委員会における法案修正によって盛り込まれたものであります。

そして、総務省のＮＯＴＩＣＥサポートセンターの業務というのは、総務省が公表している令和五年度の行政事業レビューシートによると、電波法第百三条の二第四項第十二号を根拠としたＩｏＴの安心、安全かつ適正な利用環境の構築という事業の一環として行われているとしています。

同項の第十二号の規定の中には、電波の能率的な利用を確保し、又は電波の人体等への悪影響を防止するために行う周波数の使用又は人体等の防護に関するリテラシー向上のための活動に対する必要な援助となっておりまして、二〇〇八年の改正当時こそ第十号でしたが、内容は当時から全く変わっておりません。

修正案提出者の代表であった原口一博衆議院議員は、同法の趣旨について、二〇〇八年四月十七日の本委員会で、混信等の妨害を生じさせずに無線設備を使用する方法、例えば違法機器の見分け方、あるいは電波から人体、電子機器を守る方法、例えば近くに心臓のペースメーカーをつけていらっしゃる方がいらしたら、その電波が心臓のペースメーカーに影響を与える、こういったこと

などに関して国民のリテラシー、理解能力の向上を図るための周知、広報、啓発、教育等を意味しているものでございますと答弁されております。

そうなると、このＮＯＴＩＣＥサポートセンターの運営が、どのように、電波の能率的な利用確保、そして電波の人体等への悪影響を防止するために行う周波数の使用又は人体等の防護に関するリテラシーの向上のための活動に対する必要な援助に該当するというのでしょうか。

ＮＯＴＩＣＥの取組を進めて、ＤＤｏＳ攻撃によって生じる不必要なトラフィックを低減させることによって、回り回って電波の能率的な利用の確保につながると解釈することもできるかもしれませんが、その場合、無線局全体の受益を直接の目的として行う事務という規定との整合性に疑問が生じます。

そこで、伺います。ＮＯＴＩＣＥサポートセンターの経費を電波利用料から拠出している理由、あわせて、その拠出が電波利用料の使途を限定した規定に抵触しないと言える根拠についてお答えください。

○山内政府参考人　お答え申し上げます。

ＩｏＴ機器を対象にしているというふうに申し上げておりますが、ＩｏＴ機器とは、そもそも、インターネット・オブ・シングス、物がインターネットにつながっているという状態でございまして、ここには電波、無線ＬＡＮ等の無線技術に関わりが深いというものが多数ございます。したがいまして、電波の適正な利用を確保するためには、ＩｏＴ機器に係るセキュリティーの確保を図っていくということが不可欠だというふうに考えてございます。

この取組においては、無線技術を活用したＩｏＴ機器の利用者に対する注意喚起を通じて基本的な理解を深めることで、感染通信、攻撃通信などによる不要な電波の発射が抑制されるというふうに期待をしております。

これによって、安心、安全に電波を利用できる環境が整備されて、もって効率的な電波の利用の促進がされるという観点から、先ほど御指摘のあった電波利用料の使途、電波法第百三条の二の第四項第十二号でございます、電波の能率的な利用を確保するリテラシーの向上のための活動に該当するということで、電波利用料の財源から支出をすることとしております。

○おおつき委員　時間が参りました。

改めて私から申し上げたいのは、この法案、やはりサイバー攻撃から守ることによって何が得であるかというのをしっかりと説明して取組の認知度を上げていくこと、また、詐欺だとかと思われないように、その通知の仕方ですね、信用される通知の仕方を工夫することをお願いいたしまして、私の質問といたします。

ありがとうございました。

○古屋委員長　次に、岡本あき子さん。

○岡本（あ）委員　立憲民主党・無所属の岡本あき子でございます。

委員長を始め、今日質問の機会をいただきましたこと、感謝を申し上げたいと思います。

私からも今回の法改正について確認をさせていただきたいんですが、今ほど同僚議員が質問されました。資料一を御覧ください。今まさに、おおつき議員がおっしゃったと思います。

八月時点で五千五十五件、ＮＯＴＩＣＥの注意喚起、要は脆弱ですよということを一か月で把握しました。下にあります棒グラフを見ていただきたいんですが、これのうち、濃い赤、濃いオレンジ、濃い青、これが、前月も同じように脆弱だという指摘をしていて、また今月も対象になりましたという棒グラフでございます。先ほど三分の二という話がありましたが、せっかく通知をしているのに改善がなされていないというところは、やはり本来の施策の目的を果たしていないんじゃないかと思わざるを得ません。

今後新たにサイバー攻撃に悪用されるおそれがあるＩｏＴ機器を調査対象にしていくという今回の法改正です。その中に既にマルウェアに感染している機器も対象になっていくということを考えると、注意喚起をしましたよ、この後は電気通信事業者の努力ですとかシステムインテグレーターの努力ですではなくて、どれだけ改善をされたのか、そこまで総務省として目的を達成させる、この任務をすることこそ必要ではないかと思います。この点について、先ほどの答弁ではセキュリティー意識構築とか対策を考えていくという話なんですが、法改正に伴って、やはりこれは、どれだけ改善させていくのか、その決意も示していただきたいと思います。お答えください。

○山内政府参考人　お答え申し上げます。

御指摘いただきましたとおり、通信事業者への通知、機器の利用者への注意喚起については、ＩｏＴ機器のセキュリティー対策に対する利用者の意識が十分でないこと、ＩｏＴ機器の管理者が不明であるということから、対応が進まない場合が多数あるというふうに認識をしてございます。

今御指摘のあったＩｏＴ機器の適正な管理に向けた周知啓発の強化、これはもちろんでございますが、これに加えまして、累次にわたって注意喚起に応じない場合、通信事業者が利用者の機器の接続を拒否できる要件それから手続等を定めたガイドラインを策定して、基準の明確化を図ることで対策の実効性を向上させていきたいというふうに考えてございます。

また、通信事業者への通知、機器利用者への注意喚起によって地道に一台ずつ対処するのに加えて、メーカーへの働きかけというものによって、実際の成果としても、数万台規模でＩＤ、パスワードの脆弱性が解消されたということを私どもの方では経験してございます。

これらを踏まえまして、今回の法案では、通信事業者への通知だけではなくて、メーカー等の関係者への情報提供や助言についてＮＩＣＴの業務として法的に位置づけることにしております。これによりまして幅広い関係者を巻き込んだ対策を一層促進して、より大きな成果を上げるべく取り組んでまいりたいと考えております。

○岡本（あ）委員　是非大臣にも伺いたいと思うんですけれども、先ほどのサイバー攻撃の懸念、国家の安全保障上も非常に深刻な中で、一方で、今、ランサムウェア攻撃というのが非常に深刻になっています。要は、政府機関はもちろんですけれども、民間も含めてデータですとかに通信障害を起こさせて、その企業に身の代金を要求するというものです。

米国の調査ですけれども、報道によれば、スプランク社というところがまさに十月の末に二〇二三年版ＣＩＳＯレポートというのを公表されました。世界十か国を調査している中に日本の企業も入っております。世界中なので、日本がどのくらいの実数なのかというのが分からないんですが、実に九〇％の組織が過去一年間に大規模な攻撃を一回以上受けている、八三％がランサムウェア攻撃を受けて実際にお金を払ってしまっているという、ちょっと衝撃なレポートが公表されております。

今月一日に国際ランサムウェア対策イニシアティブという会議で身の代金を払わないようにしようという共同誓約が交わされており、日本も参加をしております。こういうサイバー攻撃の対策ということが、今回の法改正も一つの対策になるということを望んでいます。

せっかく脆弱性やサイバー攻撃に悪用されるおそれのある特徴とか、こういう分析は多分ＮＩＣＴさんは得意なんだと思うんですね。どういう機器に脆弱があって、あるいはどういう使われ方をしているところにリスクが高いのか、こういうところをＮＩＣＴさんのこれまでの知見や蓄積、技術で分析もできるはずです。先ほど助言とありましたけれども、対策をして結果として改善がなされる、このためにも取り組むべきだと思います。

この点は、是非、決意も含めて、総務大臣に伺わせていただければと思います。

○鈴木（淳）国務大臣　今回の法案に基づきＮＩＣＴが行うＩｏＴ機器の調査は、ＤＤｏＳ攻撃のように情報通信サービスの安定的な提供に支障を生じさせ、利用者に広く影響を及ぼすようなサイ

バー攻撃への対策を主な目的とするものであります。

他方、御指摘のランサムウェア攻撃のように特定の者を標的とした攻撃による被害は、直近においても本年七月に名古屋港の全ターミナルが一時的に停止する事案が発生するなど、深刻な状況が続いているものと認識をしております。

こうした状況を踏まえれば、例えば、ＩｏＴ機器が侵入経路となったサイバー攻撃の発生が確認された際に、同様の脆弱性があるＩｏＴ機器について緊急でセキュリティー対策を促すなど、ＮＩＣＴが行うＩｏＴ機器の調査で得られた情報や知見をＮＩＳＣや警察庁などの関係省庁とも共有、連携を進めまして、ランサムウェアを始めとした様々なサイバー攻撃への対策強化に貢献するなど、我が国全体として実効性があるサイバーセキュリティー対策につなげていくように取り組んでまいりたいと思います。

○岡本（あ）委員　関係機関とも是非連携をしていただいて、やはり総務省としては、ＮＩＣＴという専門レベルの機関を持っていますので、知見を生かして、結果としてリスクが減るように、実際に対策が実行されるまでしっかりチェックをしていく、その決意で取り組んでいただきたいと思います。

続きまして、ＮＩＣＴそのものについて幾つか伺わせていただきたいと思います。非常に私はこのＮＩＣＴに期待をかけているところでございます。

まず、資料三を御覧いただきたいんですけれども、先日、予算委員会で同僚の米山委員が、研究機関の科学論文が非常に評価が低下しているのを懸念している、ネイチャーに載ってしまったという紹介がなされておりました。ネイチャーの英文の記事でしたので、せっかくですので、ＮＩＣＴが持っているＶｏｉｃｅＴｒａという翻訳ソフトがありますよね、これを使って是非翻訳をしてみようと思ったんです。

本当はここで成果を披露しようと思ったんですが、アプリはあって、とても日本語らしい表現がされているということをとても感心しているところなんですが、残念ながらここで音声を御披露することが、残念ながら委員会の理事会で許可をいただけなかったので、議会の質疑の在り方もデジタルの活用ということも含めて今後の課題にしていただければと思います。

この中で、ＶｏｉｃｅＴｒａさんはすごいなと思ったのは、特に、今日の資料の後ろの方についているんですが、後ろといいますか、今日は一ページ目しか、タイトルしか載せておりませんけれども、年号ですとか数字が入ったりしている場合、ほかの翻訳ソフトも実は幾つか試したんですが、日本語としては正しく表記をされない、ＶｏｉｃｅＴｒａさんはきれいにちゃんと翻訳をされている。

そこの文章でいくと、二〇二〇年の文科省の分析によると、二〇〇二年から二〇一八年の間に大学の研究者が科学に専念する時間の割合が四七％から三三％まで減少している。ネイチャーのこの資料の後半に出てまいります。ここが、ほかの翻訳ソフトですと、四十七年から三十三年間とか、数字が入った部分が日本語としては非常に正しくない部分もあるので、これを御披露したかったのですが、ちょっと残念でございます。

今申し上げました、科学の環境が日本は非常に脆弱になっている。それから、資料二を御覧いただくと、科学的論文のトップテン論文が日本は十三位に転落をしているということです。ＮＩＣＴさんも論文はどんどん出していらっしゃると思いますので、ＮＩＣＴさんの環境整備について伺いたいと思います。まず一つは、うれしいことに、ＮＩＣＴさんは女性研究者の採用に努力をしてくださっていると伺っております。今日は徳田理事長にお越しいただいておりますので、是非、その点、御披露いただければと思います。

○徳田参考人　お答え申し上げます。

ＮＩＣＴでは、優秀な人材の確保、イノベーションの創出、国際競争力の獲得等に資する観点から、ダイバーシティ推進室を設置し、女性を始め障害者等の雇用、参画及び活躍を推進しており、この一環としまして女性研究者の採用にも力を入れております。

具体的には、次の二つの取組を実施しております。

一点目として、今年度より、一般の公募とは別に、女性対象の公募を五月から八月にかけて実施しております。その結果、令和六年度の採用予定研究者に占める女性の割合は四〇％となりました。

二点目は、より多くの女性研究者にＮＩＣＴへ応募していただけるよう、ＳＮＳを通じ、ＮＩＣＴで活躍する女性研究者の働く姿を積極的に紹介しております。また、ＮＩＣＴのオープンハウスや女子大で開催されている外部イベントにおいてＮＩＣＴの女性研究者による職場環境等の紹介を行っており、女性研究者に対するＮＩＣＴの良好な研究環境のＰＲを進めております。

今後もこうした取組を通じて女性研究者の積極的な採用を進めてまいります。

○岡本（あ）委員　ありがとうございます。デジタルの分野でも是非女性の研究者の活躍を期待したいと思いますし、若手の研究者ということで、テニュアトラックについてもＮＩＣＴらしい取組をして、パーマネントに登用するという仕組みをされている御努力も伺っておりました。

もう一点伺わせてください。

先ほどの私の、研究環境の中で、今、研究者が三三％しか研究に没頭できないという状況なんだというのがこのネイチャーの記事です。記事の中では、ほかの研究者のビザの手続までも研究者自身がやらされているんだ、こういう環境が日本というのは非常に研究の評価を下げている、こういう位置づけになっているという指摘がありました。

今の資料二、資料三を御覧になった感想も含めてですけれども、ＮＩＣＴさんでは、こういう課題、研究者が研究作業にちゃんと専念できる環境をどのように努力されているのか。あるいは、大学等だと外部資金獲得とか、有期研究者の場合、そろそろ自分の期間が終わってしまうので、次の転職先のための要は履歴書送り、こういうために時間が取られて研究に没頭できないという御指摘をいただいております。この点、ＮＩＣＴさんはどういう御努力をなされていますでしょうか。

○徳田参考人　お答え申し上げます。

ＮＩＣＴでは次の二点において大学と比較して良好な研究環境が整っており、より研究に集中できる環境にあると認識しております。

まず一点目は、研究者一人当たりの研究補助者の数とその他の支援スタッフの数がそれぞれ〇・四三人と一・七三人であり、日本の大学の平均値の約八倍でございます。研究支援を担う、いわゆるバックオフィス機能が充実しております。特に、外部資金の獲得に関しましては、ＮＩＣＴには受託研究や助成金等を管理する専門の部署があり、公募の紹介から、応募、採択後の契約、終了後の受託研究費請求までを専門のスタッフがサポートしております。

二点目は、サイバー攻撃に関連した情報など、ＮＩＣＴの持つ中立性を生かして収集、蓄積した研究データや、補正予算等で整備した高度な計算リソースなど、ＩＣＴ技術の研究開発に必要な資源がそろっていることで、研究者にとって非常に魅力的で優れた研究環境にあると考えております。

このような研究環境により、極めて質の高い論文の発出や、一本の光ファイバーで世界最大の伝送容量となります毎秒二十二・九ペタビット、これまでの世界記録の二倍を達成したんですけれども、この実現など、社会的インパクトの高い成果が出ていると認識しております。引き続き研究環境の整備に努めてまいりたいと思っております。

○岡本（あ）委員　デジタルの分野、特にＮＩＣＴさんのような、今まさに必要、これから先、格段に研究分野としては最優先になるような研究分野というところになりますので、是非これからも優

秀な研究者をしっかり獲得できて、最初に戻りますけれども、通知だけじゃなくて、結果として、国民の皆さんの安全、事業を営んでいる方あるいはＩｏＴを使われている方々にとっても安心してインターネットあるいは機器を使われる、デジタル環境が整っていくところに貢献をしていただきたいと思いますし、是非、研究所ですので、ここにＮＩＣＴさんからの論文がトップテン論文で評価されることを期待申し上げたいと思います。

残りの時間で、ちょっと基金を飛ばして、ＮＴＴ法と自治の方を伺わせてください。

総務委員会ですので、今、ＮＴＴ法に関する議論が審議会で取り上げられていると思います。大臣に伺わせていただきたいと思います。

先日、直近の審議会の議事録を拝見しますと、一定の方向性が確認された事項等も整理されてきているところです。現実、固定電話のユニバーサルサービス、一方でブロードバンドのユニバーサル制度をやりますという方針も掲げて、必ずしも固定電話ではなくてデジタルを、誰も取り残さない社会をつくるということが大前提になりますし、それは進んで着手されていると伺っておりますが、固定電話のユニバーサルサービスの義務化というのが一定の役割を終えているんじゃないかという御指摘、あと、やはり外資の関係ですね、日本の重要インフラである通信の確保を考えると、外資の影響というところは、当然、日本の安全保障上も一定の国防として、あるいは経済安全保障上として、ここは守るべきところがあるんじゃないか、この指摘もあると思います。

今現在で総務省として考えられていること、審議会の受け止めも含めて、大臣、お答えください。

○鈴木（淳）国務大臣　ＮＴＴ法を含めた、時代に即した通信政策の在り方につきましては、多様な関係者が関わるものであることから、事業者、団体等の様々な意見を丁寧に伺いながら、情報通信審議会において精力的に御審議を賜っております。

特に、委員御指摘のユニバーサルサービスの確保につきましては、過疎地や離島などの不採算地域も含めて、国民が全国どこでも通信サービスを利用できることが重要と考えておりまして、固定電話中心からブロードバンドを軸としたユニバーサルサービスに見直す方向で御議論を賜っているところでございます。

また、経済安全保障の確保に関しては、外資規制が引き続き重要であると考えておりまして、ＮＴＴ法と外為法の両法による安定的なサービス提供を担保するための措置の必要性についても御指摘を賜っているところでございます。

総務省としましては、ユニバーサルサービスや経済安全保障の確保など、通信政策の理念や国民の利益がしっかり確保できますように、審議会の御議論を踏まえまして適切に対応してまいりたいと考えております。

○岡本（あ）委員　ありがとうございます。審議会の行方をこれからも注視していくということになると思います。改めて、やはり通信をしっかり確保して、国民の皆さんがそれを享受できるということを最優先に考えていただいた上での取組になることを御祈念申し上げたいと思います。

あともう一つ、総務委員会で、おとどい、大臣の所信表明に対する質疑の中で、所得税減税で地方に与える影響というところがかなり質疑がなされました。

資料四を御覧ください。全国市長会から、都市税財源の充実確保についてということで要望がまさに今月出されております。その中の一番上の項目、総合経済対策に伴う交付税減収に対する確実な補塡ということで、住民税の減税は総務省で責任を持って、地方に迷惑をかけないという御答弁があったと思います。

そのほかに、システム改修ですとか、事務負担の部分ということも、明確に、その分をしっかり、地方に負担をかけない、要はその分は国で責任を持っていただきたいということに加えて、来年六月、所得税が減税になりますと、所得税の収入がその分、見込んだよりは所得税の収入が減ることになります。そうなりますと、交付税法定分三三・一％、地方交付税として交付されますけれども、これの母数、そもそもの母数が減ることになると思います。これも地方にとっては減収になるということになるのではないかと思います。

是非、総務大臣、頑張っていただいて、単に住民税の減収分だけじゃなくて、事務負担、あらゆる地方自治体が負担しなきゃいけない経費、あわせて、所得税が減る分、地方交付税が減ってしまうよと、ここの点もしっかり国で責任を持って、減収前の金額を元に、地方に交付されるよう御努力をいただきたいと思います。この点、お答えください。

○鈴木（淳）国務大臣　まず、今般の総合経済対策におきましては、御案内のとおり、納税者及び配偶者を含めた扶養家族一人につき、令和六年分の所得税三万円、令和六年度分の個人住民税一万円の減税を行うこととされております。

税制につきましての詳細につきましては、今後、与党税制調査会で御議論されるものと承知しております。

なお、総合経済対策では、御案内のとおり、個人住民税の減収額は全額国費で補塡することとされております。

総務省としましては、地方団体が事務を円滑に実施できますように、地方の財政運営への支障や過度な事務負担が生じないよう留意しつつ、適切に対応してまいります。

地方交付税減収分につきましては、これも地方に影響を与えないように全力で取り組んでまいりますので、必要な予算確保に取り組んでまいります。

○岡本（あ）委員　是非、この点、総務大臣として、地方自治体あるいは地方議員御出身の立場としても声を出していただきたいと思います。

ちょっと懸念をしている中で、来年の六月に要は減税をするんだと。住民税に関してもきっと同じになるのかなと思うんですが、報道とか総理大臣の記者会見を聞いていると、ボーナスで相殺をする可能性があるんじゃないかというような受け止めになるんです。

実は、地元の企業から潤沢にボーナスを出せないんだという御相談とかもありまして、是非この点も国民に減税の部分で、多分、民間の企業でいくと、企業の給与システムも触らなきゃいけないということになるんだと思います、住民税を引き去る分においても同じことになると思いますので、この点も是非、地域で暮らしている方々、地域で事業を営んでいる方々に過度な負担がかからない、その方策についても御配慮いただきたいと思います。この点は要望として申し上げます。

もう時間が来ましたので、この点も含めて、来年の六月、住民税も減税する可能性があるときに、地方自治体だけでなく、地方で事業を営んでいる方、地方で働いている方、あるいはフリーランスの方、こういう方々の減税というところは非常に不安に思っております。地域で事業を営んでいる方、暮らしている方々が、減税効果があるんだとすれば、恩恵にあやかれなければ全く意味がないことですので、是非、地域の暮らしを支えていただきたいと思います。

最後に、もし大臣からありましたら、お願いしたいと思います。

○古屋委員長　簡潔にお願いいたします。

○鈴木（淳）国務大臣　様々な分野で関連もありますので、そごが生じないように、適切に配分をしてまいりたいと思います。

○岡本（あ）委員　ありがとうございました。

基金に関しては、是非、取崩しで実効が上がる基金の活用をということを申し上げて、質問を終わります。

ありがとうございました。

○古屋委員長　次に、阿部司さん。

○阿部（司）委員　日本維新の会、阿部司です。

お見苦しい姿をお見せしますが、実は今年の夏にお祭りで頑張っておみこしを担いでいましたら痛めまして、ちょっと御容赦をいただければと思

います。

内閣提出第六号、国立研究開発法人情報通信研究機構法の一部を改正する等の法律案について質問させていただきます。

今回の法案は、ＮＩＣＴが実施する特定アクセス行為を伴うＩＤ、パスワードに脆弱性のあるＩｏＴ機器調査を令和六年以降も実施できるようにすること及びその調査対象の拡充、そして二つ目にＮＩＣＴの債務保証業務等を規定した特定通信・放送開発事業実施円滑化法の廃止の二つを柱としておりますけれども、私からは一つ目の特定アクセス行為の方を中心に質問させていただきます。

先ほど来、様々な委員から御指摘があったと思いますが、ＮＯＴＩＣＥの事業というのは、サイバー上ではありますけれども、例えるならば日本全国でドアノックをしまくる、そういう行為であります。そうしたときに、いかにサイバー攻撃から国民を守っていくための実効性をどのように担保していくか。実効性を担保していくといったときに、もちろんテクノロジーですとかルールの効果を高めていくということと、川崎委員からも御指摘がありましたが、国民の意識を高めていく、この点が非常に重要だと思っております。

国民の意識を高めていくといったときに、まず、それがなぜ必要なのか、どんなリスクがあるのか、何のためにやるのか、ここをしっかりと分かっていただく。また、急にドアノックしてくるものですから、心配だなと皆さんは思うと思います。そこがいかに安心、安全なものかということ、ここを御理解いただくこと、これが非常に重要かと思いますので、その観点から質問させていただきたいと思います。

まず、立法事実についてお伺いをいたします。

今回、法改正により、時限措置が撤廃されると同時に、調査対象の範囲が広がることになります。このような措置が必要とされる立法事実について、具体的なファクトをお示しいただきたいと思います。また、もし仮にこの事業を実施しない場合、どのようなリスクが想定されるのか。それぞれ、鈴木大臣、お答え願えますか。

○鈴木(淳)国務大臣　ＮＩＣＴでは、平成三十年に成立をしました改正ＮＩＣＴ法に基づきまして、平成三十一年から今年度末までの時限の業務として、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査を実施してまいりました。

こうした取組を通じまして一定の成果は上がっておりますけれども、依然としてＩＤ、パスワードの設定に不備のあるＩｏＴ機器を標的としたサイバー攻撃が発生しておりまして、最近ではＩＤ、パスワード以外のソフトウェアなどの脆弱性を狙ったサイバー攻撃も増えているなど、ＩｏＴ機器を悪用したサイバー攻撃のリスクは引き続き高い状況にあると思っております。

こうした状況を踏まえまして、今回の法案では、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査を来年度以降も継続して実施可能としまして、また、ＩＤ、パスワード以外のソフトウェア等の脆弱性を有するＩｏＴ機器にも調査対象を拡充することとしたものであります。

サイバー攻撃が年々巧妙化していることを踏まえれば、こうした取組を行わなかった場合、脆弱性のあるＩｏＴ機器が増えまして、こうした機器を悪用したサイバー攻撃のリスクが更に高まるという可能性がありますので、ＩｏＴ機器のセキュリティー対策の強化に向けて取組を拡充してまいりたいと思っております。

○阿部(司)委員　ありがとうございます。

サイバー攻撃が年々増えてきているというお話だったと思うんですが、更に質問なんですけれども、増えていった先にどんな危険、脅威があるのか。大臣の御認識をお伺いできればと思うんですけれども。

○鈴木(淳)国務大臣　被害者が今度は加害者になっていってどんどん拡大しますので、そこは、小さく抑えるためにもそれは必要だと思います。

○阿部(司)委員　ありがとうございます。

まず、先ほど来ほかの委員からも御指摘がありましたが、世界中で、国際情勢も非常に大きな変化を迎えておりまして、戦争も起きていますし、そうしたサイバー攻撃の脅威というのが高まって、重要インフラが攻撃されて生活に重大な影響を及ぼしたりだとか、例えば医療機関が攻撃を受けて止まっちゃったりしたら命の危険にさらされるわけであります。このようなことをよく国民の皆さんに御理解いただくことというのは非常に重要かと思うので、その点をもう一度、目的、事業の効果、国民の命をさらさない、経済を止めない、ここをしっかりと御認識いただきたいなと思っております。

今申し上げたような重大インフラが攻撃を受けるような対策をしていく上で非常にこの事業は重要だと思うんですけれども、踏み台とされるおそれのあるルーター、ＩｏＴ機器というのは、大臣からも少し言及がありましたが、管理者、機器を持っている所有者は直接デメリットがないケースもあるように認識しておりますが、その中で悪用される、自分が直接悪影響を受けないかもしれないけれども、悪用されて、それが国や社会に重大な影響を及ぼしてくる、この点、非常に重要なポイントだと思っております。

サイバー攻撃は五年で三・四倍に増えているというお話もあり、本事業は私自身賛成の立場で、応援をしていきたいと思っておるんですけれども、そういった立場で、次に、これまでの成果及び法改正により見込まれる効果について参考人にお伺いをしたいと思います。

〔委員長退席、中川(康)委員長代理着席〕

○山内政府参考人　お答え申し上げます。

ＩＤ、パスワードに不備があるＩｏＴ機器の調査に関しましては、ＮＯＴＩＣＥのプログラムに参加をしている通信事業者、合計で七十九社でございます、この七十九社のネットワークの下で、インターネットに直接接続されている約一億台のＩｏＴ機器を対象に実施してまいりました。

この調査によりＩＤ、パスワードに不備がある機器が見つかった場合には、通信事業者への通知、機器の利用者への注意喚起を行って、ＩＤ、パスワードの変更対応をお願いしてまいりました。調査開始以来、これまでの累計で延べ約十万件の通知を行っております。

この結果として、通知それから機器利用者への注意喚起によって、直接的には数千台程度のＩｏＴ機器についてＩＤ、パスワードの脆弱性の解消につながったと考えております。

これに加えまして、ＩＤ、パスワードに不備が多く見つかった機器のメーカー、このメーカーの方々に働きかけを行うことによりまして、ＩＤ、パスワードの強化につながるセキュリティー機能の改善に向けた働きかけを行ってまいりました。

こういう取組によって、少なくとも数万台規模のＩｏＴ機器について、ＩＤ、パスワードの脆弱性の解消に資する成果が上がったと認識をしてございます。

この調査を通じて、先ほど来のお話にちょっとございますが、メーカーの方々に対する訴求、それから、法人の利用者の場合ですと、システムを実際に運営している方、こういう方々に対する働きかけということが非常に重要だということを認識するに至っております。

したがいまして、今回の改正案の中では、今までの調査、特定アクセス行為に加えて、実際に助言を行って、いわゆるプログラム、先ほど来ファームウェアという言葉が出ておりますが、このファームウェアに脆弱性が出ているものの調査を行うこと、それから、実際に感染通信を行ってしまっている方がいらっしゃいます、これもＮＩＣＴの観測網によって検知をすることが可能でございますので、こういうものを含めてこれから対応するという形になります。

〔中川(康)委員長代理退席、委員長着席〕

○阿部(司)委員　御答弁ありがとうございました。ＮＯＴＩＣＥの事業で脆弱性が見つかって通信事業者に通知をした件数が十万件、数千台のＩｏＴ機器の脆弱性解消につなげることができた、こんな成果があると。

ところが、ＮＯＴＩＣＥの実施状況を拝見しますと、先ほどもほかの委員から御指摘がありましたが、令和五年八月には五千五十五件の注意喚起がなされているものの、三千四百六件は同年の七月に検知されたものということで、注意喚起を受けた三分の二はそのまま稼働し続けているということになります。

こうした状況を見ますと、脆弱性の注意喚起を受けても、直接的な不利益を感じる局面が少ない機器管理者、利用者はアクションを起こさないケースが多いということではないのかなと思います。せっかく脆弱性の指摘をしても対処してもらえないというのは非常にもったいないことで、この部分の対処率を上げていく取組というのが課題ではないかと感じるところであります。そのためには広報啓発などが重要かと思っておりますが、後ほど質問をさせていただきます。

課題はありつつもＮＯＴＩＣＥの取組が一定の成果を上げているということについては十分理解しております。

それでは、今回、改正によりまして調査を継続して、今、調査の対象範囲を拡大することでどのような効果が見込まれるのか、この点についてお答えをいただきたいと思います。また、ＩＤ、パスワードに脆弱性があると判定された機器のうち約三割が機種の特定が困難と伺っていますが、こうした機種特定が困難なケースへの改善の方策があればお伺いをしたいと思います。

○山内政府参考人　お答え申し上げます。

ＩＤ、パスワード以外のソフトウェアなどの脆弱性を狙ったサイバー攻撃が増えているなど、ＩｏＴ機器を悪用するサイバー攻撃が年々巧妙化している状況だと認識してございます。

こういうものも含めてサイバー攻撃に機動的に対応するために、今回の法改正によって、従来のＩＤ、パスワードに不備があるＩｏＴ機器の調査に加えて、先ほど申し上げましたソフトウェアなどに脆弱性のあるＩｏＴ機器、既にマルウェアに感染しているＩｏＴ機器にも調査対象を拡大することで、サイバー攻撃に悪用されるおそれのあるＩｏＴ機器により総合的に対応することが可能になるというふうに考えてございます。

もう一点御指摘のあった機種特定が困難なものにつきましては、調査の過程で得られる情報、メーカーなどの関係者との連携によって得られた情報を組み合わせて分析することによって、機種が特定できる割合を今まで以上に高めていきたいというふうに思っております。これによりまして必要な対策が進むよう取り組んでまいりたいと考えております。

○阿部(司)委員　新たにソフトウェア等に脆弱性があるＩｏＴ機器、既にマルウェアに感染しているＩｏＴ機器に調査対象を拡大して調査を継続することで巧妙化するサイバー攻撃に対処していけるということで理解いたしました。また、いわゆる機種特定困難事例についても御答弁をいただきました。是非こうしたデータ解析を、今御答弁がありましたが、しっかり進めて有効策を打ち出していただけますよう要望いたします。

次に、個人保護の取組強化ということでお伺いします。

本来、様々なＩｏＴ機器にログインを試みる行為は、不正アクセス禁止法における不正アクセス行為に該当します。これをＮＯＴＩＣＥの一環としてＮＩＣＴが行うものに限って法で特定アクセス行為として位置づけて、適法な行為としております。このため、ＮＯＴＩＣＥにおけるログインは、先ほども申し上げましたが、ドアをノックするもので部屋の中には入らないものと理解していますが、しかし、ログインが可能なのであれば、通信の内容等を知り得ることも不可能ではないと思います。

もちろん、世界中でも珍しいとされるこのような調査の必要性、有効性については十分理解しておりまして、サイバーセキュリティー強化にもつなげていくべきと思いますが、前提として、個人情報の保護、先ほども冒頭でお伝えしたとおり、個人情報保護に関しては万全を期していて大丈夫であるという安心感を国民の皆さんに持ってもらうことが非常に重要であると考えております。

そこで、特定アクセス行為における通信の秘密保持のための具体的な方策と運用状況、及び個人情報保護の実効性を上げるための方策についてお伺いいたします。

○山内政府参考人　お答え申し上げます。

今御指摘がございましたＮＩＣＴが行う調査は、脆弱性のあるＩＤ、パスワードを利用していないかどうかを確認するための調査でございます。

この調査、ＮＩＣＴが行う調査で得られた情報の取扱いにつきましては、総務大臣の認可を受けた実施計画に基づいて、例えば、情報を取り扱う区域は、管理区域とよく言いますが、生体認証を含む多要素認証により入退室の管理をする、情報を取り扱うサーバーについては、外部からの接続ができないような設定を行うとともに、アクセスできる職員を限定して、その通信履歴、ログを監視いたします。こういう極めて厳格な安全管理措置を講じておりまして、二〇一九年の調査開始以来、ＮＩＣＴにおいて遺漏なく適切に情報管理が行われていると認識をしております。

さらに、情報の適正な取扱いを法的に担保する観点から、特定アクセス行為などに従事する者については、ＮＩＣＴ法上、秘密保持義務が課せられております。この義務に違反した場合の罰則も併せて設けられていることに加えて、ＮＩＣＴが実施計画で認められた以上の行為を行った場合には、不正アクセス禁止法上の禁止行為に該当することから、同法の罰則の適用を受けることになるというふうに考えております。

こうしたＮＩＣＴの取組、法的な枠組み、こういうものによって引き続き適切に業務が行われるものと認識をしております。

○阿部(司)委員　万全である、もし仮に違反を行った場合は罰則があるということで、今の御答弁で国民の皆様にも御安心いただけるのではないかなと思いました。

次に、ＮＯＴＩＣＥにおける国民理解と啓発ということでお伺いをしてまいります。

もし、私の家族ですとか友人が、プロバイダーを名のるところから、あなたのルーターのパスワードは脆弱ですよとかマルウェアに感染していますよという、こうした連絡を受けた状況を想像すると、果たして素直に、そうか、では対応しようとなるか非常に疑問なんですよね。

そうしたときに、今、日常的に、フィッシングメールを送ってきたり偽サイトで個人情報を取得しようとすることはよく起こっております。こうしたことを考えると、ＮＩＣＴの取組は有意義なものだとしても、脆弱性を指摘する連絡は無視される、警戒される確率が高いのではないかなと思います。重要なのは、ＮＯＴＩＣＥの事業において、ＩｏＴ機器のＩＤ、パスワードの脆弱性が狙われて大きなサイバー被害をもたらすおそれがあるということをしっかりと国民の皆さんにまず知っていただく、広報、周知していくことが重要なのではないかなと思います。

大変恐縮なんですけれども、私、本事業に対する国民の認知度は限りなくゼロに近いのではないかなと思っています。私も恥ずかしながら知りませんでした。通告していないんですけれども、大臣、国民の認知度が限りなくゼロに近いのではないかなということについて、御所見を少しお伺いできればと思います。

○鈴木(淳)国務大臣　あるいは国民性もあるかもしれませんけれども、確かに認知度は高くはないと思います。

ただ、実際、こうしたことで守られているのは事実でありますので、こうしたことの効果をしっかり周知しながら、国民の中で脆弱性に対する危機感であり対策の必要性をしっかり認識してもらえるように取り組んでまいりたいと思っています。

○阿部(司)委員　ありがとうございました。

パスワードが脆弱なＩｏＴ機器がサイバー攻撃の踏み台になってしまうことと、それゆえＮＯＴ

ＩＣＥという事業を展開していて国民の皆様に協力いただきたい、こうしたことをもっとキャンペーンでも張って周知徹底していくべきと思うんですけれども、国民向け啓発事業について具体的な取組状況を、政府参考人、お答え願えますでしょうか。

○山内政府参考人　お答え申し上げます。

ＮＯＴＩＣＥに関する普及啓発に関しましては、専用のホームページを設けております。ここの中で、具体的な内容それから調査結果に基づいて脆弱性のあるＩｏＴ機器の現状などの情報の提供をしております。このホームページの運用に千三百万を充てております。

今回の法案を踏まえまして、情報発信を強化するために新たな広報戦略の策定に取り組んでおります。このために、来年度の関係予算も増額して要求して、実際の活動をもう少し強化していきたいというふうに思っているところでございます。

○阿部(司)委員　事前にお伺いして、今、情報発信の費用として今年度は千三百万円でウェブサイトを運用したという話を聞きまして、ちょっと少ないなということで、是非強化をしていただきたいと思います。

ここで、これまでの議論も踏まえまして、総務大臣にお伺いしたいと思います。

情報発信強化、国民理解向上に向けた今の御答弁を受けて、この状況についてどういった御感想を持たれたのかということと、しっかり来年度予算もアップして広報を強化していくべきと思うんですけれども、意気込みも含めてお伺いをできればと思います。

○鈴木(淳)国務大臣　ＩｏＴ機器のセキュリティー対策を推進する上で、ＮＯＴＩＣＥに関する情報発信を強化し、国民の理解を向上させていくことは極めて重要な課題であると認識しております。

国民の皆様には、御自身が利用するＩｏＴ機器がサイバー攻撃に加担するおそれがあることをまず知っていただいて、セキュリティー対策を自分事としてしっかり取り組んでいただきたいと思っております。

そのために、ＮＯＴＩＣＥの情報発信の強化とともに、先ほど統括官からも御説明しました広報戦略を通じまして、ＩｏＴ機器のセキュリティー対策の重要性を誰もが理解できますように周知啓発を進めるなど、国民の理解の向上に取り組んでまいりたいと思います。

いずれにしましても、しっかりと我が国でもやっておりますけれども、やはり国民の理解と、ある面では応援も必要でありますので、それにしっかり取り組みたいと思います。

○阿部(司)委員　質問を一つ残してしまいましたが、時間が来ましたので、終わります。

ありがとうございました。

○古屋委員長　次に、中嶋秀樹さん。

○中嶋(秀)委員　日本維新の会の中嶋秀樹です。

本年十月十九日から衆議院議員となり、初めての経験が続いておりますが、本日も初めての質問となります。古屋委員長を始め与野党の先生方、鈴木総務大臣を始め総務省の皆様、どうぞよろしくお願い申し上げます。

それでは、ＮＩＣＴ法案について質問させていただきます。

今般の改正案について、サイバーセキュリティー関係と基金の廃止の大きく二つに分かれています。まずは、サイバーセキュリティー関係について幾つか確認をさせていただきます。

サイバーセキュリティー対策として、ＮＯＴＩＣＥと呼ばれる、ＮＩＣＴが中心となってサイバー攻撃に悪用されるおそれのある機器の調査及び機器利用者への注意喚起を行っています。

ＮＯＴＩＣＥの取組において、注意喚起を受けた利用者がパスワードの変更を行う際に必要なサポートを行うため、ＮＯＴＩＣＥサポートセンターを設置しています。このサポートの取組は必要なことであり、悪用される機器を減らすためにも是非実施してほしいと思いますが、このサポートセンターの運用はＮＩＣＴではなく総務省の運営となっています。なぜこのサポートセンターだけ総務省が直接運営しているのか、ＮＩＣＴがまとめて実施してもいいのではないかとも思います。

○山内政府参考人　お答え申し上げます。

御指摘のＮＯＴＩＣＥプロジェクトにつきましては、現行のＮＩＣＴ法で、ＮＩＣＴは、ＩＤ、パスワードに脆弱性のあるＩｏＴ機器の調査を行って、その結果を電気通信事業者に通知する業務を実施するとされております。これを踏まえまして、個別の利用者への注意喚起につきましては、ＮＩＣＴからの通知を受けた電気通信事業者が行っております。

また、電気通信事業者が個別の利用者に注意喚起を行うに当たっての手順書の作成、それから、注意喚起を受けた利用者からの問合せ対応、ＮＯＴＩＣＥに関する一般的な情報発信、周知啓発、こういう共通的なものに関しましては、効率的に進めるために一元的に実施することが適当だと思われるものがございます。こういうものに関しましては、総務省が委託によりＮＯＴＩＣＥサポートセンターを設置してこれらの業務を行うという構造にしてございます。

このように、関係者、総務省、それからＮＩＣＴ、電気通信事業者が適切に役割分担を図りつつ、ＮＯＴＩＣＥプロジェクトを効果的に進めてまいりたいと考えております。

○中嶋(秀)委員　ありがとうございます。

それから、サポートセンター運営費用については、電波の共益費である電波利用料財源で運営されています。ここも確認をしたいのですが、サポートセンターの運営について、電波法に照らして、電波利用料を財源とすることとした理由を教えていただきたいと思います。

○山内政府参考人　お答え申し上げます。

ＩｏＴ機器、インターネット・オブ・シングスの略称でございますが、この普及が進む中で、このようなＩｏＴ機器は無線ＬＡＮ等の無線技術に関わりが深いものでございます、そのようなものが使う電波の適正な利用を確保するためには、ＩｏＴ機器に係るセキュリティーの強化を図っていくということが不可欠でございます。

本取組では、無線技術を活用したＩｏＴ機器の利用者に対する注意喚起を行うことで基本的な理解を深めて、その結果として、感染通信や攻撃通信などによる不要な電波の発射が抑制されるというふうに期待をしております。

これにより、安心、安全に電波を利用できる環境が整備されて、もって効率的な電波の利用の促進がされるということから、電波利用料の使途に定めてあります、電波法第百三条の二第四項第十二号でございますが、電波の能率的な利用を確保するリテラシーの向上の活動に該当すると考えております。これによりまして、電波利用料財源から支出をするとしております。

○中嶋(秀)委員　ありがとうございます。

特に、特定アクセス行為について確認をさせていただきます。

特定アクセス行為とは、ＮＩＣＴが行っている、脆弱性を有するＩｏＴ機器を発見するためにＩｏＴ機器にアクセスし、ＩＤ、パスワードを入力してＩｏＴ機器を作動させる行為のことですが、この特定のアクセス行為での調査範囲がインターネットに直接接続されている機器に限られていると伺っております。多くのＩｏＴ機器がインターネットにつながっている中、果たしてこれで十分なのか心配となります。

そこで、お尋ねいたします。特定アクセス行為の対象が国内のインターネットに直接接続しているＩｏＴ機器に限られており、職場内や家庭内のネットワーク下にあり、インターネットに直接接続されていない機器は本調査の対象外となっています。これでＩｏＴ機器のセキュリティー対策として十分なのか、教えていただきたいと思います。

○山内政府参考人　お答え申し上げます。

今委員から御指摘のありました、インターネットに直接接続をされていない、例えば家庭内にある機器がそうでございますが、こういうローカルなネットワークに接続をされている機器に関しましては、一般的にインターネットに直接接続されている機器などによって管理をされております。

このため、このプロジェクトは、特定アクセス行為による調査の対象となっているインターネットに直接接続されている機器についてＩＤ、パスワードなどの適切な対策が講じられているのであればサイバー攻撃の多くを防ぐことが可能でございますので、ＮＯＴＩＣＥについてはセキュリティー対策として十分効果があると考えております。

一方、その上で、ローカルなネットワーク、先ほど申し上げた対象外になっている機器につきましては、特定アクセス行為で対象にしておりませんので、一義的には当該機器それからネットワークを持っている組織若しくは個人といった方々がセキュリティー対策を講じる役割を担っていると私どもは認識をしてございます。総務省としては、関係省庁と連携をして、ＩｏＴ機器全体、その適切な管理を促進するための国民向けの周知啓発にも併せて取り組むことによって、我が国全体としてのＩｏＴ機器のセキュリティー対策が強化されるよう努めてまいりたいと考えております。

○中嶋（秀）委員　ありがとうございます。

このＩｏＴ機器ですが、ＩｏＴ機器といっても多くの機器があります。事前の説明では、ルーターやネットワークカメラなどと聞いていましたが、法律上のＩｏＴ機器の定義を確認しておきたいと思います。山内統括官にお尋ねいたします。

○山内政府参考人　お答え申し上げます。

ＩｏＴ機器について厳密な定義があるわけではございません。実は、法律上でもＩｏＴ機器という言葉は使ってございませんが、今回、ＮＯＴＩＣＥのプロジェクトで調査の対象になっておりますのは、インターネットに直接接続されている機器でございます。ＩｏＴ機器とはインターネット・オブ・シングスでございますので、こういう、物がインターネットに接続されている状態を総称してございます。

このプロジェクトの中では、ＩＤ、パスワードに脆弱性のあるインターネットに直接接続されている機器を調査いたしまして、利用者への注意喚起を通じてセキュリティー対策を促進するということを目的としておりますので、この目的に照らしますと、ＩｏＴ機器、先ほど申し上げた総称の中に入るかどうかは別にしても、脆弱性のある機器は全て対象になるというふうに考えております。

他方、特定アクセス行為の調査によってＩＤ、パスワードに脆弱性があるとして注意喚起の対象となった機器につきましては、ルーターそれからネットワークカメラといったものが大多数を占めているという状況を踏まえますと、ＮＯＴＩＣＥのプロジェクトは、事実上、ＩｏＴ機器のセキュリティー対策の促進を主眼とした取組になっているというふうに考えております。

○中嶋（秀）委員　ありがとうございます。

事前の説明の際に、特定アクセス行為により特定できない脆弱性がある機器があるとお伺いしました。

この機器が特定できないからといって、そのままにしておいていいのか、疑問に思ったところでございます。脆弱性があると判定されたものの、機種を特定できなかったＩｏＴ機器について何らかの対策が必要ではないかと考えておりますが、今後どのように対策を行っていくのか、教えていただきたいと思います。

○山内政府参考人　お答え申し上げます。

今委員が御指摘のとおり、機種が特定できない場合には、私どもは利用者に対して通知をすることが困難な状態が今起きてございます。

したがいまして、今後、調査の過程で得られる情報、それから、メーカー等これから幅広い関係者と連携をしていきたいと思ってございますが、この連携によって得られた情報を組み合わせて分析することによって、機種が特定できる数を増やしていきたいというふうに思ってございます。さらに、機種特定がたとえできない場合であっても、一般向けの情報発信を行い、ある特徴を捉まえた注意喚起を行うことによって、少しでも対策が進むよう努力をしてまいりたいと考えております。

○中嶋（秀）委員　ありがとうございます。

最後に、基金の廃止について確認をさせていただきます。

今回の法案の説明を聞いたときに、この基金の廃止についてはしっくりこない感じがいたしました。当初の目的を達成したとの説明ではありましたが、今あるスキームや法律を廃止するのに本当に必要性がなくなったのか、やや検証が不足しているように感じます。例えば、検討会で廃止の是非を検討し、多方面からの検証を行い、廃止という結論が出た上で廃止決定をしたとか、もう少し対応の仕方があったのではないかとも思っております。

最後に廃止の理由を聞いてすっきりといたしたいので、鈴木総務大臣にお伺いいたします。よろしくお願いします。

○鈴木（淳）国務大臣　特定通信・放送開発事業実施円滑化法は、平成二年当時、通信・放送分野の新規事業の開拓等を通じて情報の円滑な流通を図ることを目的として制定されました。

その後、通信・放送分野の新規事業を行う企業の支援の一環として、ＮＩＣＴが信用基金を設け、債務保証、出資、助成金の交付、利子補給の四種類の業務を行いまして、新技術を通じた通信サービスやケーブルテレビの高度化などに活用されてまいりました。

これにより、地域における情報の円滑な流通の確保等に貢献しましたけれども、その後の金利低下等の環境変化によりましてそれらの支援事業に対するニーズが低下をしました結果、令和三年度末までに既存案件が終了しまして、所期の目的を達成したと考えられますことから、基金を清算し、同法を廃止したものでございます。

以上です。

○中嶋（秀）委員　ありがとうございます。

すっきりしたといえば、すっきりしたという感じですけれども。ありがとうございました。

初めての質問で不慣れなところもあったと思いますけれども、鈴木大臣を始め皆様、今後ともどうぞよろしくお願い申し上げます。

少し早いですけれども、以上で質問を終わります。ありがとうございました。

○古屋委員長　次に、西岡秀子さん。

○西岡委員　国民民主党・無所属クラブ、西岡秀子でございます。

本日は、ＮＩＣＴ法改正案についての質疑ということで、質問の機会をいただき、ありがとうございます。どうぞよろしくお願いいたします。

これまでの質疑の中で、若干、同様の質問があるかと思いますけれども、どうぞよろしくお願いいたします。

今回の法改正につきましては、ＮＩＣＴのサイバーセキュリティー関連業務につきまして、今年度末に期限を迎えるＩＤ、パスワードに脆弱性のあるＩｏＴ機器の調査を来年度からも継続的に実施するようにという内容と、調査対象を拡充する、この二つの内容が盛り込まれております。

まず、鈴木総務大臣に、その立法趣旨、理由についてお伺いをさせていただきます。

○鈴木（淳）国務大臣　お答えします。

ＮＩＣＴでは、平成三十年に成立しました改正ＮＩＣＴ法に基づきまして、平成三十一年から今年度末までの時限の業務として、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査を実施してまいりました。

この取組により、少なくとも数万台規模のＩｏＴ機器につきまして、ＩＤ、パスワードの脆弱性の解消に資する成果が上がっているものと受け止めております。

他方で、依然としてＩＤ、パスワードの設定に

不備のあるＩｏＴ機器を標的としたサイバー攻撃が発生しておりまして、最近では、ＩＤ、パスワード以外のソフトウェアなどの脆弱性を狙ったサイバー攻撃も増えております。

このように、ＩｏＴ機器を悪用したサイバー攻撃のリスクが引き続き高い状況にあることを踏まえて、今回の法案では、ＩＤ、パスワードの設定に不備があるＩｏＴ機器の調査を来年度以降も継続して実施可能とし、ＩＤ、パスワード以外のソフトウエアなどの脆弱性を有するＩｏＴ機器にも調査対象を拡充するものとしたものでございます。

これによりまして、ＩｏＴ機器のセキュリティー対策を更に強化し、安心、安全なサイバー空間の確保に取り組んでまいりたいと思います。

○西岡委員　今大臣から御説明いただきましたけれども、ＮＯＴＩＣＥの事業でございますけれども、総務省、ＮＩＣＴ及びインターネットプロバイダーが連携をして、ＩｏＴ機器へのアクセスによるサイバー攻撃に悪用されるおそれのある機器に対する調査と機器利用者への注意喚起をプロバイダーを通じて行うものです。この枠組みにおける具体的な調査対象数と実際の調査カバー率につきましてお尋ねをさせていただきます。

○山内政府参考人　お答え申し上げます。

御指摘の調査につきましては、ＮＯＴＩＣＥのプロジェクトに参加をしている電気通信事業者七十九社のネットワークの下で、インターネットに直接接続をしている約一億台のＩｏＴ機器を対象に調査を毎月実施しております。

具体的な方法といたしましては、サイバー攻撃に利用されたことのあるＩＤやパスワード、単純な英数字の羅列など容易に推測をされやすいＩＤ、パスワードを用いて、コンピューターを用いて実際にログインを試すことによって脆弱性の調査を行っております。

御指摘の調査カバー率につきましては、具体的な数字を推計、公表はしておりませんが、主要な通信事業者が全てＮＯＴＩＣＥのプロジェクトに参加をしていることを踏まえますと、ＩｏＴ機器のセキュリティー対策を行うのに必要な調査範囲はカバーされているものと考えております。

○西岡委員　存在するＩｏＴ機器からすると、約半数ぐらいを対象としているというふうに思っておりますけれども、まず、この改正案が成立した場合には、これまで時限的な措置として実施していたものが、総務大臣の認可を受けた実施計画に基づいて定めた期間において実施できるということになりますので、事実上、令和六年度以降も継続的に恒久的に行っていくということになるというふうに認識をいたしておりますけれども、その前提としては、これまでの検証がしっかりと行われなければならないというふうに思っております。

実際に注意喚起が行われた対象機器の改善状況、また、その検証の状況について、総務省としてこれまでの成果をどのように総括しておられるのかということについてお伺いをさせていただきます。

○山内政府参考人　お答え申し上げます。

ＮＩＣＴが行う調査によりＩＤ、パスワードに脆弱性がある機器が見つかった場合には、電気通信事業者への通知、それから事業者を通じて機器の利用者への注意喚起を行って、ＩＤ、パスワードの変更等の対応をお願いしております。二〇一九年の二月から調査を開始いたしまして、これまでの累計で延べ約十万件の通知を行ってまいりました。

また、その通知対象となっている機器のうち、ルーター及びネットワークカメラがその大半を占めている状況だと判明しております。

通知を受けた電気通信事業者においては、脆弱性のあるＩＤ、パスワードの変更等を行うよう、個別の利用者への注意喚起を行ってまいりました。

また、個別の利用者への注意喚起に加えて、設定に不備が多く見つかった機器のメーカーにも働きかけを行い、初期パスワードを変更しないとその後の操作ができないなどのセキュリティー機能の強化の製品の提供につながっております。

これらの取組によりまして、少なくも数万台規模のＩｏＴ機器について、ＩＤ、パスワードの脆弱性の解消に資する効果が上がっているものと受け止めております。

○西岡委員　今御説明がありましたけれども、現在、インターネットに常時接続するＩｏＴ機器を始めとした機器が私たちの生活に幅広く普及して、社会に普及して進化を続けている中で、サイバー攻撃のリスクが常に私たちの生活と隣り合わせの中でサイバー攻撃の脅威にさらされている状況を考えますと、この取組は大変重要な取組であると認識をいたしております。

一方で、ＮＯＴＩＣＥ事業が開始されるときに、プライバシーの侵害ですとか通信の秘密に抵触するのではないかといった懸念の声が専門家を中心に発せられたことも事実でございます。現在までの間にそのような問題事案の発生というものはなかったのかどうか、このことについてお尋ねをさせていただきます。

○山内政府参考人　お答え申し上げます。

まず、ＮＩＣＴが行う調査に関しましては、脆弱性のあるＩＤ、パスワードを利用していないか否かを確認するための調査でございますので、個人情報、第三者の通信の内容を取得する内容ではございません。したがいまして、プライバシーや通信の秘密との関係で問題があるというものではございません。

また、ＮＩＣＴが行う特定アクセス行為による調査で得られた情報の取扱いにつきましては、総務大臣の認可を受けた実施計画に基づいて極めて厳格な安全管理措置を講じております。二〇一九年の調査開始以来、ＮＩＣＴにおいて遺漏なく適切に情報管理が行われており、法令違反事例はないと認識をしてございます。

御指摘のＮＯＴＩＣＥの情報発信につきましては継続して取り組んでまいりますが、ＮＯＴＩＣＥプロジェクトの実効性をより上げるためには利用者の十分な理解を得るということが極めて重要でございますので、そのための取組を強化してまいりたいと考えております。

○西岡委員　次の質問にもほぼお答えをいただいたというふうに思いますけれども、この調査業務は、誰がどのような法的な根拠に基づいて権限を持って行うのかどうか、また、情報アクセスは脆弱性のみの調査であって、データの閲覧等の目的外の行為は行われないということをしっかり担保していただいているかというのが次の質問だったんですけれども、今そのことについてもお答えをいただいたというふうに思っております。

その中で、守秘義務が課されているということで部会等のヒアリングでもお聞きをして、守秘義務違反があった場合には罰則もあるということで理解をいたしておりますけれども、ＮＩＣＴの当該調査業務というのは、本来、不正アクセス禁止法で処罰される行為の例外としてＮＩＣＴ法によって期限付で今の時点では認められているという状況を考えますと、この業務内容につきましては、先ほど御説明のあった守秘義務では、今後の対応としては不十分なことも出てくるのではないかというふうに思っております。

先ほど湯原委員の質疑の中でもあったんですけれども、現在、政府内で、セキュリティークリアランス、つまり国家の機密情報や先端技術の流出を防ぐために重要な情報を扱う政府の職員ですとか民間人の信頼性を確認するという制度でございますけれども、このことも議論が今なされております。

米国企業では、既にセキュリティークリアランスの有資格者しかアクセスできない情報というのがありまして、ＩｏＴ活用におけるセキュリティー強化も図られているというふうに聞いております。来年には法改正もということで今議論が進んでいるようですけれども、今後この議論も踏まえて対応すべきではないかというふうに考えますけれども、総務省の御見解をお伺いいたします。

○山内政府参考人　お答え申し上げます。

ＮＩＣＴが行う特定アクセス行為による調査で得られた情報の取扱いにつきましては、先ほど申し上げましたが、認可を受けた実施計画に基づいて極めて厳格な安全管理措置を行っております。それから、ＮＩＣＴ法の中でも、特定アクセス行為等に従事する者については、秘密保持義務、同義務に違反した場合の罰則に関する規定も設けている。

こういう枠組みの中で、今までＮＩＣＴの中で情報管理を遺漏なく適切に行ってまいりました。

御指摘のセキュリティークリアランスにつきましては、具体的な内容が現在検討が行われており、まだ結論が得られていない状況だと認識をしてございます。したがいまして、まだ御指摘のような対応が必要であるとまでは考えておりませんが、引き続きＮＩＣＴで適切に業務が行われるよう、総務省としても実施状況をしっかりフォローしてまいりたいというふうに考えております。

○西岡委員　やはり、信頼性というのが大変重要だと思います。この信頼性をしっかり担保した上で、我が国のサイバーセキュリティー対策を総合的に進めていくということが重要だと思いますので、今後議論が進んでいくというふうに思いますので、しっかり、このＮＯＴＩＣＥ事業にも、このことを踏まえて考えていただきたいというふうに思います。

続きまして、調査対象の拡充につきましては、総務大臣がサイバーセキュリティ戦略本部に意見を聴取した上で中期目標の策定を行うこととなっております。今日お配りしておりますポンチ絵に、ＮＯＴＩＣＥ関係のところでサイバーセキュリティ戦略本部ということが記載をされているわけでございます。

社会全体のデジタル化や安全保障上の観点からも大変重要な取組であり、現在政府内でいろいろな議論、検討がされておりますアクティブサイバーディフェンスとの関連についてはどのように整理をされているのかということをまずお聞きをしたいのが一点、そして、内閣サイバーセキュリティセンターを始めとする政府機関との連携というものはどのように今なっているのか、総務省にお伺いをさせていただきます。

○山内政府参考人　お答え申し上げます。

ＮＩＣＴが行っておりますＩｏＴ機器の調査につきましては、サイバー攻撃に悪用されるおそれのあるＩｏＴ機器のセキュリティー対策を促進するということを目的にしております。アクティブサイバーディフェンスを始めとするサイバー安全保障の取組と直接関係をするものではございませんが、一般論としてあえて申し上げますと、サイバー安全保障の取組が目指しているサイバー空間の安全にも資する面があるというふうに考えてございます。

また、本調査の実施に当たりましては、政府全体の取組と整合的になるように、サイバーセキュリティ戦略本部の意見を聴取しなければならないとされております。このような枠組みの下で、ＮＩＳＣ、内閣サイバーセキュリティセンターや関係省庁等と連携を図りながら、ＩｏＴ機器のセキュリティー対策の強化に引き続き取り組んでまいりたいと考えております。

○西岡委員　アクティブサイバーディフェンスにつきましては今検討が進められているところでありますし、今の法制や体制ではこのアクティブサイバーディフェンスというものは実行できない今現状でございます。

国民民主党としては六月にアクティブサイバーディフェンスも含むサイバー安全保障法案の骨子案というものを発表させていただいておりますけれども、今ＮＩＣＴでお取り組みになっていただいているサイバーセキュリティー対策も含めて、省庁の縦割りではなくて、信頼性をしっかり担保した上で、先ほども申し上げましたけれども、我が国のサイバーセキュリティー対策を総合的に進めていくことが大変重要だと考えますけれども、このことについて総務省から何か一言あれば、御見解をお伺いしたいと思います。

○山内政府参考人　お答え申し上げます。

委員御指摘のとおり、私どもはＩｏＴ機器のセキュリティー対策ということで進めておりますが、全体としてサイバー空間のセキュリティーのレベルを上げるということに関しましては、政府全体、サイバーセキュリティ戦略本部が目指す方向と合致をして進める必要があるというふうに考えてございます。

したがいまして、この観点から、関係省庁と連携をして、おっしゃるとおり、縦割りのない形でしっかりと進めてまいりたいというふうに考えております。

○西岡委員　是非、連携を強化して進めていただきたいというふうに思います。

続きまして、サイバーセキュリティー対策につきましては、利用者サイドのＩＤ、パスワードの改善だけでは解決できない問題も多くございます。同時に、製造機器メーカーに対しての協力を要請して、対策を講じる必要があります。

メーカー側が開発、製造する段階で適切なセキュリティー対策をより高度に講じるとともに、適切なサポート体制の在り方、機器のマニュアルにリスクとセキュリティー対策を利用者に分かりやすく表示する等の取組が大変重要になるというふうに思いますけれども、このことに対して総務省としてどのようにお考えか、今お取組があれば、お取組について、また、今後の方針をお伺いできればと思います。

○山内政府参考人　お答え申し上げます。

今委員御指摘をいただきましたとおり、通信事業者への通知それから機器の利用者への注意喚起について、一台ずつ対処するだけではなくて、ＩＤ、パスワードの脆弱性が多く見つかった機器のメーカー、こういう方々にも働きかけを行って、セキュリティー対策が適切に講じられた製品の提供につなげることで、より大きな成果が得られるということが明らかになってございます。

同じく、御指摘をいただきましたが、ＩｏＴ機器の適切な管理をするという観点で利用者への周知啓発を進めるに当たっては、私どもが直接周知啓発するだけではなくて、メーカーを始めとする関係者と連携して働きかけをするということが大変重要だというふうに考えてございます。

こうしたことを踏まえまして、今回の法案においては、通信事業者への通知だけではなくて、メーカーなどの関係者への情報提供それから助言についてもＮＩＣＴの業務として法的に位置づけることとしております。これにより幅広い関係者を巻き込んだ対策を一層促進して、より大きな成果を上げるべく取り組んでまいりたいと考えております。

○西岡委員　ありがとうございます。

続きまして、先ほどから、国民への理解、周知が大変重要だというお話がありましたけれども、一般社団法人デジタルライフ推進協会が二〇二三年三月に実施しましたＷｉＦｉルーター向けのアンケート結果によりますと、五七・八％の利用者がＷｉＦｉルーターのセキュリティーを意識したことがないというデータがあり、また、八一・七％の利用者が自宅のＷｉＦｉルーターがサイバー攻撃をされることを考えていないと答え、四二・七％が購入時のパスワードをそのまま利用しているというようなアンケート結果もございます。

やはり、利用者の意識改革が大変重要であるということがこの調査からも明確となるというふうに思いますけれども、ＮＯＴＩＣＥの取組についての広報の強化も含めまして、利用者側に対して、ＩｏＴ機器の適切な管理の重要性についての啓発、情報提供の強化が大変重要だと思いますけれども、総務省としてのお取組をお伺いさせていただきます。

○山内政府参考人　お答え申し上げます。

御指摘いただきましたとおり、ＩｏＴ機器のセキュリティー対策につきましては、利用者の意識が十分な状況ではない中、ＮＯＴＩＣＥに関する情報発信を強化して、ＩｏＴ機器の適切な管理の重要性について国民の皆様により御理解いただけるように周知啓発を進めていくということが非常

に重要な課題だというふうに認識をしてございます。

このため、来年度のＮＯＴＩＣＥの情報発信強化に向けて新たな広報戦略を検討しているところでございます。この観点では、先ほど来御指摘がございました点もありますが、私どもが知られていないというところも含めて、もっと知られる努力を恐らくするということも含め、国民の皆様に、御自身が利用するＩｏＴ機器がサイバー攻撃に加担をしてしまう、そういうおそれがあるということをまず広く知っていただいて、セキュリティー対策を自分のこととしてしっかり行っていただけるように、より効果的な周知啓発に取り組んでまいりたいと考えております。

○西岡委員　しっかりお取組をお願いいたします。

最後の質問になります。鈴木総務大臣にお伺いいたします。

サイバー攻撃の多様化、複雑化、そして日本社会、国民生活に与える影響の重大性に鑑みまして、今後一層、関係団体、事業者との連携強化を図り、ＮＩＣＴの体制、これは人員や財政面も含めて充実をしていただいて、サイバーセキュリティーの専門人材の育成強化、このことも進めていく必要があるというふうに思いますが、鈴木総務大臣の御見解をお伺いして、私の質問を終わらせていただきます。

○鈴木（淳）国務大臣　これまでも答弁してまいりましたけれども、総務省では、サイバーセキュリティー分野をＮＩＣＴの重点研究開発分野の一つに位置づけておりまして、ＮＩＣＴの体制強化は大きな課題であると認識をしております。

私自身も、先日、ＮＩＣＴを視察しましたけれども、サイバー攻撃の脅威が高まる中で、ＮＩＣＴのサイバーセキュリティー関連業務の重要性がますます高まっている、こう認識したところであります。

現在、ＩＤ、パスワードの設定に不備のあるＩｏＴ機器の調査は、平成三十一年の調査開始に伴ってＮＩＣＴに設置した専門の組織で実施しております。

今回の法案では、調査対象を拡充するとともに、幅広い関係者への情報提供や助言を新たにＮＩＣＴの業務として位置づけることとしておりまして、更なる体制強化が必要になるものと考えております。

総務省としましては、令和六年度に向けて、体制強化に必要な予算を増額して要求しておりまして、ＮＩＣＴのサイバーセキュリティー関連業務の実効性が上がりますように、しっかりと取り組んでまいりたいと思います。

○西岡委員　それでは質問を終わらせていただきます。ありがとうございました。

○古屋委員長　次に、宮本岳志さん。

○宮本（岳）委員　日本共産党の宮本岳志です。

我が党は、サイバーセキュリティー対策の重要性についていささかも軽視するつもりはなく、ＩＤ、パスワードに脆弱性がある機器を調査し、ユーザーに警告する制度は必要だと考えております。しかし、それを進める上で、この法案には大きな問題があると指摘せざるを得ません。

法案は、これまでＮＩＣＴが五年間に限って行うこととされてきたＩＤ、パスワードに脆弱性があるＩｏＴ機器の調査、特定アクセス行為の業務について、本則の恒常的な業務の範囲に規定し、継続的に実施することとするものであります。

そこで、まず、特定アクセス行為というものについて政府参考人に確認しますけれども、これをＮＩＣＴではなく一般の人が行ったらどういうことになりますか。

○山内政府参考人　お答え申し上げます。

今ＮＩＣＴが行っておりますＩＤ、パスワードに脆弱性のあるＩｏＴ機器調査、これは御指摘のあった特定アクセス行為になりますが、実際にＩＤ、パスワードを入力してログインを試みる必要がございます。これは、通常、不正アクセス禁止法で禁止をされている不正アクセス行為に該当するというものでございます。

したがいまして、ＮＩＣＴが実施計画において認められた範囲によって実施を可能とするもので、不正アクセス禁止法の適用除外として、ＮＩＣＴ法において行為者がＮＩＣＴとして実施をするという形になってございますので、仮にＮＩＣＴ以外の者が行った場合には、先ほど申し上げた不正アクセス禁止法の禁止行為に該当することになりまして、同法の罰則の適用を受けることになります。

○宮本（岳）委員　要するに、外形的、形式的には不正アクセスなんですね。それを、ＮＩＣＴがこの法律に基づいて実施する特定アクセス行為である限りにおいて認められているということになるわけですね。

今後のＮＯＴＩＣＥの取組の方向性等について議論を行った総務省の有識者会議である情報通信ネットワークにおけるサイバーセキュリティ対策分科会、第一回の分科会では、ＮＩＣＴの井上大介サイバーセキュリティ研究所サイバーセキュリティネクサス長が、調査実施機関のＮＩＣＴとしては調査体制の維持、人員確保も大きな課題となっていると発言されたことが議事録に残っております。

ＮＩＣＴが特別に五年間に限って行うこととされてきた特定アクセス行為を恒常的な業務の範囲に規定し、継続的に実施することとするならば、人的リソースの確保が課題であることは想像に難くありません。調査を行うための体制や人員確保はどうするつもりなのか、お答えいただけますか。

○山内政府参考人　お答え申し上げます。

今御指摘のありましたとおり、私どもの関係する会合の中でＮＩＣＴの方から、人員、体制について強化する必要があるということを申し上げたのはまず事実でございます。

その上で、実際に、先ほど来の答弁の中にもちょっと出てまいりましたが、体制を強化するということが必要であり、これはＮＩＣＴだけではなくて、実際の対策を立てるためには、通信事業者、先ほどの協会、ＩＣＴ―ＩＳＡＣといった幅広い方々の取組が必要になります。こういうものを含めて体制の強化を行うことによって、これからの取組を強化するということを考えてございます。

○宮本（岳）委員　先日、私もＮＩＣＴの関係者から直接話を聞きました。特定アクセス行為というこの業務について、研究員が、兼務で、限られた人しか入れない場所で厳格にやっておられます。そもそも、ＮＩＣＴにおけるこの業務の位置づけですけれども、これは研究なんですか、それとも研究ではないのか。これも、政府参考人、答えていただけますか。

○山内政府参考人　お答え申し上げます。

研究に付随をする業務として、ＮＩＣＴは研究開発法人でございますので、御指摘のとおり、研究開発を主とする業務でございます。ただ、今回のＩＤ、パスワードの調査に関しましては、技術的な知見を必要といたしますので、今までの研究開発に付随する行為としてＮＩＣＴは行っております。

○宮本（岳）委員　付随する行為ということは、研究そのものではないということですよね。

現場の方は、研究とは厳格に区別してやっている、こうはっきり言っておられました。研究者がリーダーとなり、調査は企業から出向していただいた方を職員採用して進めているが区別している、これは言っておかなければなりません。研究者の方は誇りを持ってこの業務にちゃんと当たっておられます。そういう大事な仕事だということをおっしゃっていました。

ただ、それが研究の重荷になりはしないだろうかという危惧も感じるわけですね。現在、この業務をＮＩＣＴでは何人の体制で行っておられるのか、また、この業務がこの改正により恒常的な業務の範囲となって継続的に実施することになればどれだけの職員採用が必要になるのか、政府参考人、お答えできますか。

○山内政府参考人　お答え申し上げます。

現状、特定アクセス行為に係る調査に関わっているＮＩＣＴの方は全部で十一名でございます。（宮本（岳）委員「十一名」と呼ぶ）はい。

この上で、これからの業務の拡大につきましては、今いろいろと見積りを行っているところでございます。恐らく何らかの形で増強は要るかと思いますが、まだ具体的な人数の算定に至っておりませんが、恐らく何らかの形で体制の強化は必要になるというふうに考えております。

○宮本（岳）委員　体制の強化は必要だということでございます。

当然、人員確保が課題というなら、ＮＩＣＴの恒常的な業務の範囲としていくためには、職員をきちんと増員する、これが筋だと思うんですね、大臣もうなずいておられますけれども。ところが、ＮＩＣＴが実施する業務を特定アクセス行為と通信履歴等の電磁的記録の作成に定義分けして、特定アクセス行為は委託しないものの、後者の記録の作成に限って委託も可能とする仕組みを導入する、ここが問題だと思うんですね。なぜ委託を可能とする仕組みを入れるのか、お答えをいただけますか。

○山内政府参考人　お答え申し上げます。

現行法におきまして、特定アクセス行為に係る業務に関しましては、通信事業者への通知業務以外に外部委託に関する規定が特段ありませんでした。したがいまして、実行上、ＮＩＣＴにおいても外部委託を行ってまいりませんでした。

今般、ＮＯＴＩＣＥの調査対象の拡大が行われまして、体制の強化も必要になるということがございます。特定アクセス行為による調査が引き続き厳格な条件に基づいて適切に実施されるということを確保しながら、ＮＩＣＴにおいて体制の確保をするために、外部委託が可能な範囲や要件について新たに定めるということにしております。

具体的には、今委員御指摘のとおり、特定アクセス行為自体については委託は不可といたします。その上で、得られた情報の処理、分析に係る業務については、総務大臣の認可事項に係る実施計画の中で、委託先の選定基準が定められていることですとか、情報の安全管理措置が委託先においても適切に講じられているということが確認できた場合に限って委託するということを考えてございます。

○宮本（岳）委員　いやいや、これまではしていなかったわけです。少なくとも通信履歴等の電磁的記録の作成も委託はしていなかった。そもそも、特定アクセス行為の中に両方含んでいたものをわざわざ切り分けて、これはできるというふうにするわけですね。だから、元々そういう規定がなかったと冒頭おっしゃったけれども、規定はなかったけれどもしていなかったんですよ。

二〇一八年の前回の法案審議の際、特定アクセス行為に関わる業務について、我が党の本村伸子議員の質問に対して当時の野田聖子総務大臣は、ＮＩＣＴが行う特定アクセス行為について外部委託することは想定しませんと答弁されました。この特定アクセス行為というのは今回の特定アクセス行為だけでなくて、当然その当時は含まれていた通信履歴等の電磁的記録の作成についても外部委託はしません、こういうふうに答弁された。このとき、総務省はどういう認識でこうした判断をしたのか。これはひとつ大臣からお答えいただけますか。

○山内政府参考人　お答え申し上げます。

先ほど御説明をいたしましたが、当時、まず、特定アクセス行為、実際にＩＤ、パスワードを入力して調査を行った結果を得ること、それから、その結果に基づいて電気通信事業者に対して通知を行うこと、大きく、御指摘のとおり、二つの行為がございます。

これに関して明確な切り分けが、まだ当時、始める前の状態で、そこまで認識ができていないこともあって、当時の関係者の方からの御答弁があったと認識をしてございますが、この度、先ほど御質問もいただいたとおり、体制の強化をする必要がある、業務を拡充するといった観点で、それぞれ、法律との整合性を考えながら、委託ができる範囲、委託がやはり不可能ではないかと考える場合を分けて対応するということを考えているところでございます。

○宮本（岳）委員　だから、体制の強化は必要だと言っているじゃないですか。体制の強化が必要なのに、職員の強化ではなくて委託にしようとするからそういう話になるんですね。

はっきりしているのは、これまで外部委託していなかった行為の中に通信履歴等の電磁的記録の作成は含まれておりましたね、参考人。

○山内政府参考人　お答え申し上げます。

先ほどお答えを申し上げておりますが、まず、特定アクセス行為そのものというのは、実際にＩＤ、パスワードを入力して結果を得ることというのが特定アクセス行為でございます。実際にそれを通知することというのがＮＩＣＴの法律の中でも決まっていて、ここの部分については明確な定めが見えていなかったことがございますので、これに関して私どもの中でも議論をした上で、そこの部分を委託が可能ではないかということで、規定を切り分けて今作っているという形になってございます。

○宮本（岳）委員　通信履歴等の電磁的記録の作成という業務はどのようなものか。これは、つまりは、セキュリティーが脆弱で容易に不正アクセスができるＩＰアドレスの一覧表を抽出して作るという業務なんですよ。だから、これは、委託なんかできないということで、ＮＩＣＴ本体でやってきたわけですね。

もしも作成されたセキュリティーが脆弱で容易に不正アクセスができるＩＰアドレスの一覧が悪意ある第三者に渡った場合には、どのようなことが起こると予想されますか、参考人。

○山内政府参考人　お答え申し上げます。

仮に委託をした者が悪意を持って漏えいするようなことがあった場合には、御指摘のとおり、非常に大きな問題が生じるというふうに認識をしてございます。

したがいまして、ＮＩＣＴが仮に委託を行う場合には、ＮＩＣＴが行っている情報の安全管理措置と同様の措置が講じられるということを実施計画において定めた上で、総務大臣は委託先における当該情報の適切な取扱いの確保の措置の内容の妥当性を判断した上で実施計画の認可を行うということを考えてございます。

さらに、特定アクセス行為で得られた情報の処理、分析に係る業務の委託に従事する者については、ＮＩＣＴ職員と同等の秘密保持義務が課されるとともに、違反した場合の罰則規定も設けられるということになります。

本法案の制度的な枠組みの中で外部委託が行われる場合でも、情報が厳格に管理をされ、適切に業務が行われるというふうに考えているところでございます。

○宮本（岳）委員　この資料が流出すると、とんでもないんですね。セキュリティーが脆弱で容易に不正アクセスができるＩＰアドレスの一覧なんですから、最も効率的に悪意ある不正アクセスが可能となるわけです。だからこそ、これまでは当然のことながら外部委託を避けてきたんですね。これを委託して、絶対に悪意ある第三者にこのような情報が漏えいしないと断言できるかどうか。これはひとつ大臣にお答えいただきたい。大丈夫ですか。

○鈴木（淳）国務大臣　その辺りをしっかりと厳格に切り分けた上での判断でありますので、御理解を賜りますようお願いします。

○宮本（岳）委員　私はそうは思わないんですね。発注書や契約書に明記しようが、罰則や賠償責任をかけようが、それだけでは防げないんです。

最近も、企業や自治体が業務委託していたＮＴＴ西日本の子会社で働いていた元派遣社員が、サーバーに不正アクセスして、ＵＳＢに顧客情報を保存し、十年近くで九百万件の顧客情報を流出させたという事件が発生しております。

十一月七日の会見でＮＴＴの島田社長が語っておりますが、記録媒体は持ち込んではいけない、振る舞い検知のソフトを入れないといけない、ロ

グをしっかり残さないといけないなどのルールはできていたが、実際のガバナンスが利いていなかったのは非常に反省していると述べております。

これらの情報漏えい事案が示しているのは、当然、守秘義務がかかり、ルールはあっても、それだけでは決して漏えいは防げないということなんですね。

では、聞きますが、新たに外部委託が可能となる通信履歴等の電磁的記録の作成、これはＮＩＣＴの中でやるのか、外でやるのか、はっきりお答えをいただきたい。

○山内政府参考人　お答え申し上げます。

今委員御指摘のとおり、情報をしっかり管理するということが非常に大切でございます。したがいまして、当該情報の管理はＮＩＣＴ内で行うということを想定しております。

○宮本（岳）委員　これは、外でやるわけにいかない業務だと思うんですね。厳格な管理が必要で、中で行う。

では、重ねて聞きますけれども、外部委託をした場合に、ＮＩＣＴの研究員や職員がその委託業者の社員に指図できるのか。ＮＩＣＴの内部で指示をしたら、偽装請負になりませんか。

○山内政府参考人　お答え申し上げます。

今の関係が生じるのは、特定アクセス行為を行っているＮＩＣＴから実際にその情報を活用して通信事業者に対する提供を行う委託事業者に対する関係というふうに認識しておりますが、この関係に関しましては、実施計画の中で何を指図するかということを決めることになりますので、それ以外は、逆に言うと、法律に定められた行為に基づいて様々なことを行うということと認識してございます。

逆に、それ以外のことを、もし何らかの形で計画に外れたことをやるのであれば、計画と合わない、整合しないということになりますので、これは実施計画に違反をすることになります。

○宮本（岳）委員　もう一つだけ更問いしたいんですけれども、特定アクセスをやる場所と今の電磁的記録の作成をする場所とは同じですか、違うんですか。

○山内政府参考人　お答え申し上げます。

現状でここまで正確な区分ができておりませんが、外部委託を行う場合に当たっては、外部委託業者についてはＮＩＣＴの職員とはまず異なります。特定アクセス行為自体ができないということを考えますと、ＮＩＣＴで具体的な安全管理措置を今後検討いたしますが、恐らくは異なる、同じ場所には置くことが困難でございますので、安全管理措置を異なるところで行うということになるかというふうに想定してございます。

○宮本（岳）委員　当然、そういう管理でないとうまくいかないと思うんですね。

本来なら、採決前にＮＩＣＴを現地視察して、確かに情報漏えいが起こらないかどうか、現に特定アクセスを行っている場所や、今回外部委託も可能にしようとしている通信履歴等の電磁的記録の作成の現場を見極めたいところでありますが、どうやら後になってしまうようであります。

しかし、十四日に予定されていると聞いているＮＩＣＴの視察では、その場所、すなわち特定アクセスを行っている場所や電磁的記録の作成を行うことになる場所を私たちが見ることは可能なんですね。

○山内政府参考人　お答え申し上げます。

今の御希望は、この後の議論によるかというふうに思っておりますが、まず、私どもの定めに基づいてお話をいたしますと、実施計画に記載された極めて限られた職員を除いて、調査を実施する区画への入退室は禁じられているという形になってございます。これがＮＩＣＴにおける極めて厳格な安全管理措置の内容でございますので、私ども総務省の職員も含めて、ここの中の所在、それから、そこがどうなっているかということは承知をしていない状況でございます。こういう安全管理措置を実際には行っているところでございます。

○宮本（岳）委員　いやいや、どうしても、外部委託の可能性があるところは見せていただく必要があります。国権の最高機関であり、まさに本法案の審議を行っている国会に見せないということは通りません。外部委託はするが国会には見せないという話は認められない。国会議員にも見せられないような業務なら、外部委託などやめるべきであります。外部委託が可能なものなら、当然、我々を受け入れて、しっかり説明責任を果たさなければなりません。

委員長、是非ともお取り計らい願いたいと思います。

○古屋委員長　後刻、理事会で協議をいたします。

○宮本（岳）委員　しっかりと私たちのチェック、行政監視に応えていただけるように要求して、私の質問を終わります。

○古屋委員長　これにて本案に対する質疑は終局いたしました。

○古屋委員長　これより討論に入ります。

討論の申出がありますので、これを許します。

宮本岳志さん。

○宮本（岳）委員　私は、日本共産党を代表して、国立研究開発法人情報通信研究機構法の一部改正案に反対の討論を行います。

ＩＤ、パスワードに脆弱性がある機器を調査し、ユーザーに警告する制度は必要です。

しかし、本法案は、これまでＮＩＣＴが実施してきた特定アクセス行為を本来の業務とした上で、通信履歴等の電磁的記録の作成を切り出して定義分けし、この全部又は一部は委託を可能とするものです。

そもそも、特定アクセス行為は、不正アクセス禁止法が禁じた権限を持たない者が通信機器にアクセスする行為であり、ＮＩＣＴが行う特定アクセス行為は、ＩＤ、パスワードに脆弱性のあるＩｏＴ機器を調査する目的に限り、大臣認可の実施計画に基づき実施する例外行為です。厳格な運用が求められています。

ところが、法案は、委託を可能にしたばかりか、委託先における情報の適正な取扱いについては、実施計画の大臣認可の際に確認するものの、実施過程の中での適正な取扱いを検証する仕組みは確保されておりません。また、委託事業者との契約について縛る仕組みはなく、通信履歴等の電磁的記録やその加工データの漏えいの危険性を拡大しかねないものとなっています。

厳格な運営のための担保は極めて不十分であり、反対です。

総務省は、外部委託規定の新設について、ＮＩＣＴからの人的リソースの確保が課題との意見などがあると説明していますが、そうであるなら、ＮＩＣＴの事業を実施するための人員増、体制確保こそ取り組むべきであることを指摘して、討論を終わります。

○古屋委員長　これにて討論は終局いたしました。

○古屋委員長　これより採決に入ります。

国立研究開発法人情報通信研究機構法の一部を改正する等の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〕

○古屋委員長　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。

○古屋委員長　この際、ただいま議決いたしました法律案に対し、根本幸典さん外四名から、自由民主党・無所属の会、立憲民主党・無所属、日本維新の会、公明党及び国民民主党・無所属クラブの五派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求めます。石川香織さん。

○石川（香）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、その趣旨を御説明申し上げます。

案文の朗読により趣旨の説明に代えさせていただきます。

国立研究開発法人情報通信研究機構法の一部を改正する等の法律案に対する附帯決議（案）

政府及び国立研究開発法人情報通信研究機構は、本法の施行に当たり、次の各項の実施に努めるべきである。

一　政府は、インターネットに接続する機器の更なる普及等により、サイバー攻撃の脅威が一層高まることが予想される中、機構がサイバーセキュリティ対策に果たす役割の重要性に鑑み、機構の人員・予算等の充実及び技術・知見の更なる活用を図るとともに、我が国のサイバーセキュリティ人材の育成に努めること。

二　政府及び機構は、公的機関、民間事業者及び国民に対し、機構によるぜい弱性のある機器の調査・注意喚起等の取組に関して十分に周知を行い、サイバーセキュリティ対策の重要性と当該取組についての正しい理解を促進すること、幅広く関係者と連携を行うことなどにより、メーカーの開発・製造の段階における適切なセキュリティ対策の実施等、インターネットに接続する機器の安全性の確保をはじめとする我が国のサイバーセキュリティ対策の一層の充実・強化を図ること。

三　機構は、特定アクセス行為や新たに機構法に位置付けられる業務の実施に当たっては、これらの実施により取得した情報の管理を徹底すること。また、政府は、「特定アクセス行為等実施計画」を認可する際には、当該計画において、特定アクセス行為により取得した情報の取扱が適切なものであるか厳格に審査すること。なお、政府は、機構がサイバーセキュリティ対策に果たす役割の重要性に鑑み、機構の役職員等に課されている秘密保持義務が引き続き遵守されるよう適切に監督を行うこと。

四　機構は、機構に設置された基金が国民負担によって造成されていること及びこれまでに造成された他の様々な基金が必ずしも有効かつ適切に活用されていないとの指摘があることを踏まえ、機構の基金の適切な管理及び有効活用による成果の最大化に一層努めること。

以上であります。

何とぞ委員各位の御賛同をお願い申し上げます。

○古屋委員長　以上で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〕

○古屋委員長　起立総員。よって、本動議のとおり附帯決議を付することに決しました。

この際、総務大臣から発言を求められておりますので、これを許します。鈴木総務大臣。

○鈴木（淳）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。

○古屋委員長　お諮りいたします。

ただいま議決いたしました法律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〕

○古屋委員長　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〕

○古屋委員長　次回は、公報をもってお知らせすることとし、本日は、これにて散会いたします。

午後零時七分散会